AWS Cloud WAN User Guide

AWS Network Manager

AWS Network Manager: AWS Cloud WAN User Guide

Table of Contents

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. For key concepts and terms about global and core networks, see the section called “Global and core network key concepts”.

> **Note**
>
> AWS Cloud WAN is designed to work with a core network. You can create a core network at the time you create your global network, or you can create one later on. If you want to create a global network without using a core network, use AWS Global Networks for Transit Gateways. For more information, see the *AWS Global Networks for Transit Gateways User Guide*.

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 Quick start: Create a global and core network.

- **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 AWS Global Networks for Transit Gateways command line 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 *AWS Global Networks for Transit Gateways 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.*

Global and core network key 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. This is also known as 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 “Shared core network”. 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 policy change sets.
- Visualize maps of your network topology, including network resources such as attachments, sites, and devices.
- 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.

- **Peering**

  You can interconnect your core network edge and transit gateway in the same AWS Region using a peering connection. You can create one or more route table attachments over a peering connection to peer a transit gateway route table through a Cloud WAN network segment, allowing you to deploy end-to-end network segmentation across your transit gateway and Cloud WAN-based networks.

AWS PrivateLink support

Cloud WAN supports AWS PrivateLink to create private connectivity between Cloud WAN and your VPCs. Using PrivateLink, you can establish secure and private connectivity without the need for using an internet gateway or any NAT devices to communicate with your VPCs.

Costs associated with using PrivateLink are separate from any Cloud WAN costs you might incur. For more information, see AWS PrivateLink pricing.

Note

- PrivateLink only supports IPv6 dual-stack endpoints.
- Support for PrivateLink through Cloud WAN is currently available only in the us-west-2 and us-gov-west-1 Regions.

For more information on PrivateLink, see the *AWS PrivateLink Guide*.

IPv6 support

Cloud WAN supports Internet Protocol version 6 (IPv6) on dual-stack endpoints. Backwards compatibility is supported for IPv4 endpoints. For example, `networkmanager.us-west-2.api.aws`.

Home Region

The home Region is the AWS Region where data related to your use of your AWS Cloud WAN core network is aggregated and stored. Cloud WAN aggregates and stores this information in the home Region to provide you with a central dashboard with visualized insights into your global network by creating maps of your network topology. Currently, Cloud WAN only supports US West (Oregon) as the home Region.

Cloud WAN uses Amazon Location Service to create maps of your global network. For more information about Amazon Location Service, see Amazon Location Service.

Important

- Cloud WAN aggregates and stores Regional usage data associated with the core network edges specified in your core network policy from the AWS Regions you're using to the US West (Oregon) Region.
- When it has been established, you can't change the home Region.

AWS aggregates and stores this Regional usage data from the AWS Regions that you are using to US West (Oregon), using Amazon Simple Queue Service (SQS) and Amazon Simple Storage Service (S3). This data includes but is not limited to:

- Topology data for registered transit gateways
- Event data for transit gateways and VPNs
- Transit gateway IDs for registering transit gateways into a global network
- (Optional) Location data related to your device and site registrations
- (Optional) Provider and link data related to your link registrations

- (Optional) IP address and CIDR ranges used in Cloud WAN and transit gateway Connect peers

All movement and data aggregation occurs over a secure and encrypted channel and stored with encryption at rest.

Region availability

AWS Cloud WAN is available in the following AWS Regions:

AWS Region	Description
us-east-1	US East (N. Virginia)
us-east-2	US East (Ohio)
us-west-1	US West (N. California)
us-west-2	US West (Oregon)
af-south-1	Africa (Cape Town)
ap-northeast-1	Asia Pacific (Tokyo)
ap-northeast-2	Asia Pacific (Seoul)
ap-northeast-3	Asia Pacific (Osaka)
ap-south-1	Asia Pacific (Mumbai)
ap-south-2	Asia Pacific (Hyderabad)
ap-southeast-1	Asia Pacific (Singapore)
ap-southeast-2	Asia Pacific (Sydney)
ap-southeast-3	Asia Pacific (Jakarta)
ap-southeast-4	Asia Pacific (Melbourne)
ap-southeast-5	Asia Pacific (Malaysia)

AWS Region	Description
ca-central-1	Canada (Central)
ca-west-1	Canada West (Calgary)
eu-central-1	Europe (Frankfurt)
eu-central-2	Europe (Zurich)
eu-north-1	Europe (Stockholm)
eu-west-1	Europe (Ireland)
eu-west-2	Europe (London)
eu-west-3	Europe (Paris)
eu-south-1	Europe (Milan)
eu-south-2	Europe (Spain)
il-central-1	Israel (Tel Aviv)
me-central-1	Middle East (UAE)
me-south-1	Middle East (Bahrain)

Cloud WAN pricing

For information about Cloud WAN pricing, see AWS Cloud WAN Pricing.

Quick start: Create an AWS Cloud WAN global network and core network

With AWS Cloud WAN, you'll first create a global network framework, which eventually will contain 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” for the steps to register your events.
Transit gateways	A transit gateway must first be created on the Amazon Virtual Private Cloud console at https://console.aws.amazon.com/vpc/home. Transit gateways that you have created in Amazon VPC can then be registered in AWS

Prerequisite	Description
	Cloud WAN to be part of your AWS Cloud WAN global network.

Step 1: Create a global network

The first step in using AWS Cloud WAN is to create your global network. Your global network can contain a single core network, which in turn contains all of your attachments, transit gateways, site, and devices.

> **Note**
>
> If you're only creating and managing a global network without a core network, use AWS Global Networks for Transit Gateways. For more information, see the AWS Global Networks for Transit Gateways User Guide.

You can either create a global network using the AWS console or through the command line or API. You can create as many global networks as your account allows; however, each global network can have only one core network.

To create a global network using the AWS console

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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. Keep the **Add core network in your global network** check box selected, and then choose **Next** to set up your core network and policies.

   The **Global networks** page appears with a confirmation box that your global network was created successfully.

To create a global network using the command line or API

- create-global-network

You can also view dashboards of your global and core networks as topological trees and logical diagrams, and you can monitor and track events. See *Global and core network dashboards* for the ways you can visualize and monitor your global and core networks.

Step 2: Create a core network

After creating a global network, you'll be prompted to create a core network. You have the option to create the core network later, but until you create one you won't be able to deploy core network resources.

To create a core network after creating a global network

1. Access the AWS Cloud WAN console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Core network general settings**, enter a **Name** and **Description** identifying the core network.
3. (Optional) Choose Additional settings to add one more or more **Key** and **Value Tags** to help identify this network resource.
4. Under **Core network policy settings**, set the beginning and ending Autonomous System Number (ASN) **ASN range**. 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** identifying the segment. You can have up to 100 alphanumeric characters. White space is not allowed. For example, you might want this core network to be used for `development`. You might 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 and core network are created. During this time 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 up to 30 minutes to complete. During this time you can't create any attachments within your core network or create policy versions. Once the core network is deployed successfully, the **Policy versions** tab displays that the core network policy is LIVE and that the **Change set state** has succeeded when the policy has deployed successfully.

9. After your policy is LIVE and the core network was created, you can begin to add attachments to your core network. See the section called “Attachments”.

To create a core network using the command line or API

- create-core-network

(Optional) Step 3: Modify your global and core networks

Once you've created your global and core networks you can optionally modify your global and core network by completing any of the following tasks based on the needs of your network:

Task	Description	More information
Add attachment tags	Add tags to your attachments. This helps you to more easily identify and organize your attachment resources.	See Attachment tags.
Create attachments	Add attachments to your core network. Cloud WAN supports Connect attachments, Direct Connect attachments, VPC attachments, Site-to-Site VPN attachments, and Transit gateway route table attachments. In addition, Cloud WAN also supports Tunnel-less and GRE	See Attachments.

Task	Description	More information
	Connect peer connections with third-party appliances, such as SD-WAN appliances.	
Create a core network policy version	Create a core network policy if you want to make changes to your network, such as adding new segments or creating a network function group for routing secure traffic between VPCs. The policy version you deploy implements that policy version as your new core network. Policy versions can be created through the AWS Network Manager console or by modifying a JSON file.	See Core network policy versions.
Create a peering	A peering allows you to interconnect your core network edge with an AWS transit gateway in the same Region. Peering supports dynamic routing.	See Peerings.
Share attachments	Share any of your VPC or transit gateway route table attachments across AWS accounts.	See Shared attachments.
Share your core network	Share your core network across AWS accounts or across your organization.	See Shared core network.
Share peerings	Create and share a transit gateway peering that allows you to establish peering connections between your core network and transit gateways in the same AWS Region.	See Shared peerings.
Add devices	Add a physical or virtual device. Once you add a device, you can associate that device with a specific site.	See Devices.

Task	Description	More information
Create sites and links	Create one or more global network sites, which are physical network locations. You can then add create a link between that site and any devices you've added to your global network.	See Sites and links.
Register transit gateways	Register transit gateways you've created in Amazon VPC with your Cloud WAN global network.	See Transit gateways.
Monitor events and track metrics using Amazon CloudWatch.	Onboard CloudWatch Logs Insight, allowing you to monitor our Cloud WAN resources. Use Amazon CloudWatch Events to track CloudWatch metrics and to set threshold alarms on metrics.	See CloudWatch events and metrics.

(Optional) Step 4: View your global and core network dashboards

View dashboards of your global and core networks. Cloud WAN uses Amazon CloudWatch events and metrics, allowing you to monitor your global and core networks. You can use these events and metrics to set alarms notifying you when any threshold is reached or a change occurs; for example a change event might be when a VPC attachment is deleted from your core network.

To access the global network dashboards

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Global Networks**, choose the link for the global network you want to access the dashboard for.

The global network dashboard opens for that global network. For information on navigating this dashboard, see the section called “Access global network dashboards”.

To access the core network dashboards

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Global Networks**, choose the link for the global network that you want to view the core network dashboard for.
3. In the navigation pane choose **Core network**.

   The dashboard opens for that core network. For information on navigating this dashboard, see the section called “Access core network dashboards”.

(Optional) Step 5: View your transit gateway network and transit gateway dashboards

View dashboards of both your transit gateway network and your transit gateways to view logical diagrams, geographical representations, and topologies of your transit gateway network and transit gateways. You can also view CloudWatch metrics, as well as set threshold alarms on events.

To access the transit gateway network dashboards

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Global Networks**, choose the link for the global network you want to access the transit gateway networks dashboard for.
3. In the navigation pane, choose **Transit gateway network**.

   The transit gateway network dashboard opens. For information on navigating this dashboard, see the section called “Access transit gateway network dashboards”.

To access the transit gateway dashboards

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Global Networks**, choose the link for the global network that you want to view the transit gateway dashboard for.
3. Under **Transit gateway network** in the navigation pane, choose **Transit gateways**.

   The dashboard opens for that transit gateway. For information on navigating this dashboard, see the section called “Access transit gateway dashboards”.

Modify AWS Cloud WAN networks

After setting up your AWS Cloud WAN global and core networks set up, you can further modify these networks by performing a number of different tasks.

> **Note**
>
> Modifying a global network or a core network requires that both be set up first. If you haven't yet created either, see *Quick start: Create a global and core network* for the steps to create a global or core network.

Tasks you can perform to modify your global and core networks include:

- **Add attachments.**

  Add Connect, Site-to-Site VPN, VPC, or transit gateway route table attachments. In addition, you can create Connect peers.

- **Create a policy version.**

  Create and deploy a version of any policy to become your new core network. You can create a policy version through either the Network Manager console or by modifying a JSON file.

- **Add sites, devices, and links.**

  Add representations of physical devices and sites to your global network. You can then create a link that associates a device and a site.

- **Register transit gateways.**

  Register transit gateways you've created in Amazon Virtual Private Cloud (VPC) with your Cloud WAN network. This allows you to view and monitor transit gateway resources within the network.

- **Create a peering.**

  Create a peering connection to enable communication between your core network and transit gateways.

- **Share your core network.**

Share your core network across accounts or across your organizations. You can set permissions to allow users to view and modify network resources.

- **Share attachments**.

  Share your VPC and transit gateway route table attachments from your shared core network. You can set permissions to allow users to create new VPC or transit gateway route table attachments.

- **Access network dashboards.**

  Cloud WAN includes separate global network, core network, transit gateway network, and transit gateway dashboards. On these dashboards you can view logical trees and geographic maps of your networks, which includes attachments, sites and devices. You can also view monitoring and events dashboards, allowing you to view Amazon CloudWatch metrics and to set threshold alarms on these metrics.

Topics

Global and core networks in AWS Cloud WAN

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

For example, you might need to delete a global network if you've reached the maximum number of global networks for your account. The default number of global networks per account is 5, but

you can request an increase. If your global network has an associated core network, you'll first need to delete the core network and any of its network resources. Once deleted, a global network can't be retrieved. You'll need to create that global network again. See General on the AWS Cloud WAN Quotas page.

Each global network can have only one core network associated with it. You can't request an increase for more than one core network. If you want to add a new core network to an existing global network without creating a new global network, you'll first need to delete the existing core network. Before deleting the core network, you must first delete all network resources from that core network. A deleted core network can't be retrieved. You'll need to recreate that core network again.

Topics

View AWS Cloud WAN global network information

View details about a Cloud WAN global network. On the Details page of the global network you can add or modify tags as needed.

To view details about a global network

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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 an AWS Cloud WAN global network

Delete a Cloud WAN global network if you no longer need that network. Deleting a global can't 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”.

To delete a global network

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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.

View AWS Cloud WAN core network information

View information about a core network within a Cloud WAN global network. On this page you can also add or modify tags as needed.

To view or edit details about a core network

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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 an AWS Cloud WAN core network

Delete a core network if the core network is no longer needed. Deleting a core network can't be undone. Before you delete a core network you'll need to first delete any network resources associated with it.

To delete a core network

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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.

Network resource attachment tags in AWS Cloud WAN

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*.

If you are not the core network owner, any attachment tag that you add, modify, or delete might require acceptance on the part of the core network owner. These tags can be seen on the **Proposed Tags** tab until the time that the core network owner accepts or rejects them.

Supported resources

The following core network resources support tagging:

- Core network
- Core network attachments
- Connect peer

For tagging support resources in Network Manager, see Resources tags in AWS Global Networks for Transit Gateways.

Topics

Add or update an AWS Cloud WAN resource attachment tag

Add a tag to a Cloud WAN core network attachment or modify an existing tag.

To add or update attachment tags

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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. 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.

Remove an AWS Cloud WAN resource attachment tag

You can remove any resource tag that you've associated with an attachment.

To remove a tag

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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.

Attachments in AWS Cloud WAN

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.
- **Failed** — The attachment failed to attach to the core network. For example, this might be due to an input error or a service linked role issue.

The following are the supported core network attachment types.

- Direct Connect
- Connect

  You can also create a Connect peer through the Network Manager console.
-
- VPC
-
- Transit gateway route table

You can create an attachment using either using the Network Manager console or by using the command line or API.

Route evaluation

Cloud WAN evaluates routes at each core network edge in the following order:

1. The most specific route for the destination
2. For routes with the same destination IP address, but different targets, the following route priority is used:
   a. Static routes
   b. VPC-propagated routes in the same Region.
   c. For dynamic routes received at the core network with an *unequal* AS path length and/or MED BGP attributes, Cloud WAN evaluates them in the following order:

i. AS path length

ii. MED

d. For dynamic routes received at the core network with *equal* AS path length and MED BGP attributes, Cloud WAN evaluates them in the following order:

i. AWS Direct Connect gateway-propagated routes.

ii. Cloud WAN Connect-propagates routes in the same Region.

iii. Site-to-Site VPN-propagated routes in the same Region.

iv. Routes propagated from other sources, such as transit gateway peering and core network edges in other remote Regions over the AWS global infrastructure. If identical routes are received from two or more sources, a single attachment will be chosen in a deterministically random manner.

Topics

Connect attachments and Connect peers in AWS Cloud WAN

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 both the Generic Routing Encapsulation (GRE) tunnel protocol and Tunnel-less connect 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 or Tunnel-less Connect 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 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.

You can create a Connect attachment through either the AWS Network Manager console or using the CLI/SDK.

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

Tunnel-less Connect

AWS Cloud WAN supports Tunnel-less Connect for VPC Connect attachments. Tunnel-less Connect provides a simpler way to build a global SD-WAN using AWS. Third-party SD-WAN appliances can peer with Cloud WAN using Border Gateway Protocol (BGP) without needing to deploy IPsec or GRE-based tunnels between the appliance and Cloud WAN. This allows you to deploy a Cloud WAN core network across multiple AWS Regions and to connect one or more of your third-party SD-WAN appliances to core network edges in each Region. Because Tunnel-less Connect has no tunneling overhead, it provides better performance and peak bandwidth on TLC attachments. IPSec provides 1.25G, allowing you to combine up to eight tunnels while providing up to the entire VPC attachment bandwidth. GRE supports only 5G, which means you'd need to deploy specialized techniques, such as ECMP (Equal Cost Multi-pathing), for scaling bandwidth across tunnels.

You can use the console or API to specify the Tunnel-less Connect protocol.

In order to use Tunnel-less Connect, note the following:

- Your SD-WAN appliance must support BGP. The appliance must be deployed in a VPC and use a Connect attachment enabled for the tunnel-less operation in order to connect your SD-WAN appliance to a core network edge.
- Attachment policy tags or resource names are used to associate the Tunnel-less Connect attachment to the SD-WAN segment.
- Both Connect (GRE) and Connect (Tunnel-less) attachments can co-exist in the same VPC. There is a maximum of single Connect (Tunnel-less) attachment per VPC.
- Tunnel-less Connect and any underlying transport VPC attachments must be associated to the same core network segment.

- Inside CIDR blocks is not an input when creating a Tunnel-less Connect peer, but is instead taken from the connecting core network edge

Routing

Tunnel-less Connect uses BGP for dynamic routing. Therefore, any third-party SD-WAN appliance you want to use for Tunnel-less Connect must support BGP. SD-WAN appliances peer with a core network using the Connect attachment functioning in a tunnel-less manner. It uses native BGP to dynamically exchange routing and reachability information between SD-WAN appliance in the VPC and the core network edge. We recommend using a different autonomous number (ASN) on your SD-WAN appliance from the one configured on the core network edge.

Tunnel-less Connect also supports Multiprotocol extension for BGP (MP- BGP) in order to support both IPv4/IPv6 address families.

You'll need to configure the following in the VPC route table used for Tunnel-less Connect:

- The core network edge BGP IP address. This is necessary to bring up the BGP session between the core network edge and the SD-WAN appliance.
- If your third-party appliance is in a different subnet from the VPC attachment, you'll need to add all destination prefixes.

For more information about route tables, see Configure route tables in the *Amazon VPC User Guide*.

Third-party appliance limitations

An AWS Cloud WAN tunnel-less attachment peer (third-party appliance) can be located in the same subnet as the VPC attachment (transport attachment) subnet or a different subnet. The following limitations apply if your third-party appliance is located either in the same subnet as the Cloud WAN VPC attachment or in different subnets.

For third-party appliances in the same subnet as the Cloud WAN VPC attachment:

- When the third-party appliance is in the same subnet as the VPC attachment, routes are dynamically exchanged using BGP with the core network edge. For the dataplane to function correctly, no VPC route table modifications are required except for adding the core network BGP addresses to establish BGP peering.

- The BGP IPv4 prefixes advertised by the core network edge to your third-party appliance will have the core network attachment's Elastic Network Interface's (ENI) IPv4 address as the next-hop address, which differs from the core network BGP address peering.
- The BGP IPv6 prefixes advertised by the core network edge to your third-party appliance will use the EUI-64 Address of the core network attachment's ENI as the next-hop.

For third-party appliances in a different subnets from the Cloud WAN VPC attachment:

- If the third-party appliance is in a different subnet from the VPC attachment, you can still establish dynamic route exchange the core network edge using BGP. However, in addition to adding the core network BGP addresses for peering, you must modify the VPC route table for the dataplane to function correctly. This includes adding the prefixes received from the core network edge BGP peer into the route table. You can create a summary route that encompasses the longest prefixes advertised by the core network edge.
- The BGP IPv4 prefixes advertised by the core network edge to your third-party appliance will have the core network BGP address as the next-hop.
- The BGP IPv6 prefixes advertised by the core network edge to your third-party appliance will use IPv4-mapped IPv6 addresses of the core network BGP address as the next-hop.

It's recommended that you place your third-party appliance in the same subnet as the Cloud WAN VPC attachment for more seamless integration with Tunnel-less connect.

Topics

Create a Connect attachment for an AWS Cloud WAN core network

You can create a Connect attachment using either the Network Manager console or using the AWS CLI. Once you create a Connect attachment to your core network you can create a Connect peer. For the steps to create a Connect peer after creating the Connect attachment, see the section called “Add a Connect peer”.

Topics

- Create a Connect attachment using the console
- Create a Connect attachment or Connect peer using the command line or API

Create a Connect attachment using the console

The following steps create a Connect attachment for a core network using the console.

To create a Connect attachment using the console

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
3. On the **Global networks** page, choose the global network link for the core network you want to add an attachment to.
4. In the navigation pane under he name of the global network, choose **Attachments**.
5. Choose **Create attachment**.
6. Enter a **name** identifying the attachment.
7. From the **Edge location** dropdown list, choose the location where the attachment is located.
8. Choose **Connect**.
9. From the **Connect attachment** section, choose the Connect protocol. This will be either:
   - **GRE**
   - **Tunnel-less (No encapsulation)**
10. Choose the **Transport Attachment ID** that will be used for the Connect attachment.
11. (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**.
12. Choose **Create attachment**.

Create a Connect attachment or Connect peer using the command line or API

Use the command line or API to create an AWS Cloud WAN Connect attachment. When using the `CreateConnectAttachment` API pass the following:`"Protocol" : "NO_ENCAP"`.

To create a Connect attachment or Connect peer using the command line or API

- Use `create-connect-attachment`. See create-connect-attachment.

If you're creating a Tunnel-less Connect attachment, you must then use the following command line or API to create the Connect peer:

- `create-connect-peer`. See create-connect-peer.

View or edit an AWS Cloud WAN Connect attachment

You can view information about a Connect attachment. For an existing attachment you can create a GRE or Tunnel-less Connect peer, as well as edit the key-value tags associated with the attachment. If you want to add a new Connect attachment, see the section called "Connect attachments and Connect peers".

To view and edit a Connect peer attachment

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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**.
6. Details about the attachment are displayed, as well as any Connect peers and tags that are associated with the attachment. Here you can also add a new Connect peer, as well as add, edit, or remove tags.

    - To add a new GRE or Tunnel-less Connect peer attachment, choose the **Connect peers** tab and follow the steps here: the section called "Add a Connect peer".
    - 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. 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.

View a Connect or Connect peer attachment using the command line or API

Use the command line or API to view a Connect or Connect peer attachment.

To view a Connect or Connect peer attachment using the command line or API

- For a Connect attachment, see get-connect-attachment.
- For a Connect peer attachment, see get-connect-peer.

Create an AWS Cloud WAN Connect peer for a core network

You can create a either a GRE Connect peer or a Tunnel-less Connect peer for an existing Connect attachment using either the AWS Cloud WAN console or the command line/API.

Topics

- Add a GRE Connect peer using the console
- Add a Tunnel-less Connect peer using the console
- Add a Connect peer using the command line or API

Add a GRE Connect peer using the console

The following steps add a GRE Connect peer using the console.

To add a Connect peer using the console

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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**.

   The **Details** tab displays the **Connect protocol**. Make sure to choose a Connect attachment where the Connect protocol is **GRE**.
6. Choose the **Connect peers** 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 customer appliance. This is peer IP address (GRE outer IP address) on the appliance side of the Connect peer.

    This can be any IP address. The IP address can be an IPv4 or IPv6 address, but it must be the same IP address family as the transit gateway address.
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 any ASN in the `1-4294967294` 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 Tunnel-less Connect peer using the console

The following steps add a Tunnel-less Connect peer using the console.

To add a Tunnel-less Connect peer using the console

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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**.

    The **Details** tab displays the **Connect protocol**. Make sure to choose a Connect attachment where the Connect protocol is **NO_ENCAP**.
6. Choose the **Connect peers** tab.

7. Choose **Create Connect peer**.
8. Enter a **Name** to identify the Tunnel-less Connect peer.
9. For the **Peer BGP address**, enter the appliance's private IPv4 address.

> **Note**
>
> BGP peering primarily uses IPv4 addresses, but it does support IPv6 address exchange through MP-BGP. To establsih BGP sessions for IPv6 Unicast, you must have IPv4 Unicast addressing.

10. For the **Peer ASN**, specify the BGP 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 any ASN in the `1-4294967294` range. The default is the same ASN as the core network edge. If you configure the **Peer ASN** to be different from the core network edge ASN (eBGP), you must configure ebgp-multihop with a time-to-live (TTL) value of 2.
11. For **Subnet**, choose the subnet of the appliance.

> **Note**
>
> We recommend you run your appliance in the same subnet as your transport VPC attachment.

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 Connect peer**.

Add a Connect peer using the command line or API

Use the command line or API to create an AWS Cloud WAN Connect peer.

To create a Connect peer using the command line or API

- Use `create-connect-peer`. See create-connect-peer.

Direct Connect gateway attachments in AWS Cloud WAN

AWS Cloud WAN now supports native integration with AWS Direct Connect, simplifying connectivity between your on-premises networks and the AWS cloud. The new capability enables you to directly attach your Direct Connect gateways to Cloud WAN without the need for an intermediate AWS Transit Gateway, allowing seamless connectivity between your data centers or offices with Amazon Virtual Private Cloud (VPCs) across AWS Regions globally.

Cloud WAN allows you to build, monitor, and manage a unified global network that interconnects your resources in the AWS cloud and your on-premises environments. Direct Connect allows you to create a dedicated network connection to AWS bypassing the public Internet and provides improved application performance, greater privacy and security. Previously, you needed to deploy an intermediate transit gateway to interconnect your Direct Connect-based networks with Cloud WAN. Now you can directly attach your Direct Connect gateway to a Cloud WAN core network, simplifying connectivity between your on-premises locations and VPCs. Cloud WAN Direct Connect gateway attachments add support for automatic route propagation between AWS and on-premises networks using BGP (Border Gateway Protocol). Direct Connect gateway attachments also support existing Cloud WAN features, such as central policy-based management, tag-based attachment automation and segmentation for advanced security.

Prerequisites

The following are required before you can create a Direct Connect gateway attachment in a core network:

- You must have a Direct Connect account and a valid Direct Connect gateway. A specific Direct Connect gateway can't be used for any other gateway types as long as it remains associated with a core network. This includes virtual gateways, transit gateways, and private virtual interfaces.
- Only one core network can be associated with a Direct Connect gateway.

For more information about Direct Connect, see the *AWS Direct Connect User Guide*.

Limitations

The following limits apply to Direct Connect gateway attachments in a core network:

- You can't configure static routes pointing to a Direct Connect gateway attachment as the next hop in a core network policy. Routes must be dynamically advertised from the on-premises network to core network.

- Direct Connect Border Gateway Protocol (BGP) communities are not supported in a Cloud WAN network.
- You can't configure a list of allowed prefixes to be advertised over the Direct Connect gateway attachment from Cloud WAN to an on-premises network.
- The ASN of a Direct Connect gateway must be outside of the ASN range configured for the core network. For example, if you have an ASN range of 64512 - 65534 for the core network, the ASN of the Direct Connect gateway must use an ASN outside of that range.
- Private IP VPN and Connect attachments are not supported when a Direct Connect gateway attachment is the transport type.

Route propagation

A Direct Connect gateway attachments support BGP-based dynamic routing for both inbound and outbound directions.

For inbound routes,

- Cloud WAN learns BGP routes advertised from your on-premises location via the Direct Connect gateway and the transit virtual interface. Routes are learnt in the segment route-tables of the associated core network edges for the attachment.
- Routes learned in segment route table can be routed across all AWS Regions for that segment.
- Cloud WAN follows the route evaluation order for the same prefixes learned over multiple attachments. See the section called “Route evaluation” for more information.

For outbound routes,

- Cloud WAN propagates routes from the segment route table to the Direct Connect gateway, which in turn advertises these routes over transit virtual interfaces to your on-premises locations via BGP.
- Each core network edge associated with the Direct Connect gateway attachment advertises only its local routes towards the Direct Connect gateway.
- The AS_PATH BGP attribute is retained in these route advertisements to your on-premises locations. For more information about AS_PATH and BGP, see Private virtual interface and transit virtual interface routing policies in the *AWS Direct Connect User Guide*.

Pricing

As with other Cloud WAN attachments, there is a per-hour charge and per-gigabyte charge for using Direct Connect gateway attachments in a Cloud WAN core network. For more details about pricing, see AWS Cloud WAN Pricing.

Topics

- Create a Direct Connect gateway attachment for an AWS Cloud WAN core network
- View or edit an AWS Cloud WAN core network Direct Connect gateway attachment

Create a Direct Connect gateway attachment for an AWS Cloud WAN core network

You can add a Direct Connect gateway attachment using either the Network Manager console or using the AWS CLI. The Direct Connect gateway must first be created using the Direct Connect console before it can be added as an attachment in Cloud WAN. For more information about Direct Connect gateway attachments and Cloud WAN, see Direct Connect gateway attachments.

Topics

- Create a Direct Connect gateway attachment using the console
- Create a Direct Connect gateway attachment using the command line or API

Create a Direct Connect gateway attachment using the console

The following steps create a Direct Connect gateway attachment for a core network using the console.

To create a Direct Connect gateway attachment using the console

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network link for the core network you want to add an attachment to.
4. In the navigation pane under he name of the global network, choose **Attachments**.
5. Choose **Create attachment**.
6. Enter a **Name** identifying the attachment.

7. From the **Attachment type** drop-down list choose **Direct Connect gateway**.
8. For the **Edge locations**, choose one of the following:

   - **All** — Choose this option if you want to associate all edge locations in your core network with the Direct Connect gateway. When choosing this option, any new edge locations deployed in a core network policy version are automatically added to the Direct Connect gateway attachment and updated with the Direct Connect gateway. This does not automatically update any edge locations you might remove from the core network policy.
   - **Specific** — Choose this option if you want to associate only a subset of edge locations from your core network policy with the Direct Connect gateway. When choosing this option, you must manually add new or remove edge locations to the Direct Connect gateway attachment after deploying a core network policy version. A Direct Connect attachment will be attached to the core network edge according to the core network policy edge locations but will associated to the segment based on the segment edge locations..
9. In the **Direct Connect gateway attachment** section, choose the Direct Connect gateway to use for connecting Direct Connect to the Cloud WAN core network.

   > **Note**
   >
   > A Direct Connect gateway can be used for only one core network, and can't be used for any other Direct Connect gateway type.

10. Choose **Create attachment**.

Create a Direct Connect gateway attachment using the command line or API

Use the command line or API to create a Direct Connect gateway attachment.

To create a Direct Connect gateway attachment using the command line or API

- Use `create-direct-connect-gateway-attachment`. See create-direct-connect-gateway-attachment.

View or edit an AWS Cloud WAN core network Direct Connect gateway attachment

You can update the edge locations for a Direct Connect gateway attachment using either the Network Manager console or using the AWS CLI. The Direct Connect gateway attachment must first be created using the Direct Connect console. For more information about Direct Connect gateway attachments and Cloud WAN, see Direct Connect gateway attachments.

Topics

View or edit a Direct Connect gateway attachment using the console

Use the following steps he following steps to update the edge locations for a Direct Connect gateway attachment. The updated edge locations are automatically associated with the Direct Connect gateway on Direct Connect console.

To add a Direct Connect gateway attachment using the console

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network link for the core network you want to add an attachment to.
4. In the navigation pane under he name of the global network, choose **Attachments**.
5. Choose the Direct Connect gateway attachment you want to update, and then choose **Edit**.
6. In the **Direct Connect attachment** section, add or remove **Edge locations**, and then choose **Edit attachment**.

Update a Direct Connect gateway attachment using the command line or API

Use the command line or API to update a Direct Connect gateway attachment.

To create a Direct Connect gateway attachment using the command line or API

- Use `update-direct-connect-gateway-attachment`. See update-direct-connect-gateway-attachment.

VPC attachments in AWS Cloud WAN

When you attach a VPC to a core network edge in AWS Cloud WAN, 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 a VPC in the *Transit Gateway User Guide*.

> **Important**
>
> You cannot select a subnet from a Local Zone while creating a Cloud WAN VPC attachment. Doing so will result in an error. For more information about Local Zones, see the *AWS Local Zones User Guide*.

Appliance mode

If you plan to configure a stateful network appliance in your VPC, you can enable appliance mode support for the VPC attachment in which the appliance is located when you create an attachment. This ensures that Cloud WAN uses the same Availability Zone for that VPC attachment for the lifetime of the flow of traffic between a source and destination. It also allows Cloud WAN to send traffic to any Availability Zone in the VPC as long as there is a subnet association in that zone. While appliance mode is only supported on VPC attachments, the network flow can enter the core network from any other Cloud WAN attachment type, including VPC, VPN, and Connect attachments. Cloud WAN appliance mode also works for network flows that have sources and destinations across different AWS Regions in your core network. Network flows can potentially be rebalanced across different Availability Zones if you don't initially enable appliance mode but later edit the attachment configuration to enable it. You can enable or disable appliance mode using either the console or the command line or API.

Appliance mode in Cloud WAN optimizes traffic routing by considering the source and destination Availability Zones when determining the path through an appliance mode VPC. This approach enhances efficiency and reduces latency. The following are example scenarios.

Scenario 1: Intra-Availability Zone Traffic Routing via Appliance VPC

When traffic flows from source Availability Zone us-east-1a to destination Availability Zone us-east-1a, with Appliance Mode VPC attachments in both us-east-1a and us-east-1b, Cloud WAN selects a network interface from us-east-1a within the appliance VPC. This Availability Zone is maintained for the entire duration of the traffic flow between source and destination.

Scenario 2: Inter-Availability Zone Traffic Routing via Appliance VPC

For traffic flowing from source Availability Zone us-east-1a to destination Availability Zone us-east-1b, with Appliance Mode VPC attachments in both us-east-1a and us-east-1b, Cloud WAN uses a flow hash algorithm to select either us-east-1a or us-east-1b in the appliance VPC. The chosen Availability Zone is used consistently for the lifetime of the flow.

Scenario 3: Routing traffic through an appliance VPC without Availability Zone data

When traffic originates from source Availability Zone us-east-1a to a destination without Availability Zone information (e.g., internet-bound traffic), with Appliance Mode VPC attachments in both us-east-1a and us-east-1b, Cloud WAN selects a network interface from us-east-1a within the appliance VPC.

Scenario 4: Routing traffic through an appliance VPC in an Availability Zone distinct from either the source or destination

When traffic flows from source Availability Zone us-east-1a to destination Availability Zone us-east-1b, with Appliance Mode VPC attachments in different Availability Zone example us-east-1c and us-east-1d, Cloud WAN uses a flow hash algorithm to select either us-east-1c or us-east-1d in the appliance VPC. The chosen Availability Zone is used consistently for the lifetime of the flow.

Note

- When you create a VPC attachment you can't create a core network VPC attachment that uses only IPv6 subnets. A core network VPC attachment must also support IPv4 addresses.
- Appliance mode is only supported for VPC attachments.

DNS support

DNS support in Cloud WAN enables the resolution of public DNS host names to private IP addresses when queried across VPCs attached to the same core network edge similar to the DNS resolution capability available for transit gateways. This feature is enabled by default in your core network and can be configured in your core network policy by setting the `dns-support` parameter to either `true` or `false`, with the setting applying to all core network edges in the core network. You can view your DNS support configuration through the console in the core network policy or by using the `get-core-network` command.

> **Note**
>
> DNS support only works between VPCs attached to the same core network edge and does not function across different regions or between VPCs attached to different core network edges.

Security group referencing

You can configure security groups by specifying a list of rules that allow network traffic based on criteria such as IP CIDRs, prefix lists, ports and security group referencing. Security group referencing allows you to specify other security groups as references, or matching criterion in inbound security rules to allow instance-to-instance traffic. With this capability, you do not need to reconfigure security rules as applications scale up or down or if their IP addresses change. Rules with security group references also provide higher scale as a single rule can cover thousands of instances and prevents you from over-running security group rule limits.

Security group referencing is a regional feature for Cloud WAN, meaning VPCs must be connected to the same core network edge for this feature to work. When you create a VPC attachment, Cloud WAN automatically enables security group referencing for VPCs attached to the same core network edge.

> **Note**
>
> Security group referencing is enabled by default at the attachment level but disabled by default at the core network level.

With security group referencing support in Cloud WAN, you can:

- Reference security groups across VPCs connected to the same core network edge
- Simplify security group management for applications that span multiple VPCs
- Maintain security group references even as instances scale up or down
- Reduce the number of security group rules needed for cross-VPC communication

Limitations

The following limitations apply to security group referencing in Cloud WAN:

- Security group referencing only works between VPCs attached to the same core network edge. It does not work across different regions or between VPCs attached to different core network edges.
- Security group referencing is not supported for VPC attachments in the use1-az3 Availability Zone .
- Security group referencing is not supported for AWS PrivateLink endpoints. We recommend using IP CIDR-based security rules as an alternative.
- Security group referencing works for Elastic File System (EFS) as long as an allow all egress security group rule is configured for the EFS interfaces in the VPC.
- Security group referencing support can be configured for both core network and VPC attachments and will only work if it has been enabled for both a core network and its VPC attachments.

Topics

Create a VPC attachment for an AWS Cloud WAN core network

Create a VPC attachment using the console

The following steps create a VPC attachment for a core network using the console.

To create a VPC attachment using the console

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

2. Under **Connectivity**, choose **Global networks**.
3. On the **Global networks** page, choose the global network link for the core network you want to add an attachment to.
4. In the navigation pane under he name of the global network, choose **Attachments**.
5. Choose **Create attachment**.
6. Enter a **name** identifying the attachment.
7. From the **Edge location** dropdown list, choose the location where the attachment is located.
8. Choose **VPC**.
9. In the VPC attachment section, choose **Appliance mode support** if appliance mode is supported. For more information about appliance mode, see the section called “Appliance mode”.
10. Choose **IPv6 support** if the attachment supports IPv6.
11. By default, **DNS support** is enabled. This allows domain name system resolution for the attachment. Clear the check box if you don't want to enable DNS support. For more information, see the section called “DNS support”.
12. By default **Security Group Referencing support** is enabled. When you create a VPC attachment, Cloud WAN automatically enables security group referencing for VPCs attached to the same core network edge. This allows you to reference security groups across VPCs in your security group rules. Clear the check box if you don't want to enable security group referencing. For more information, see the section called “Security group referencing”.
13. From the **VPC IP** dropdown list, choose the VPC ID to attach to the core network.
14. 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.
15. (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**.
16. Choose **Create attachment**.

Create a VPC attachment using the command line or API

Use the command line or API to create an AWS Cloud WAN VPC attachment

To create a VPC attachment using the command line or API

- Use `create-vpc-attachment`. See create-vpc-attachment.

To enable appliance mode, add `--options ApplianceModeSupport=true` to the command.

View or edit an AWS Cloud WAN VPC attachment

You can view and edit configuration information for a VPC attachment . If you want to add a new VPC attachment, see the section called “VPC attachments”.

To view and edit a VPC attachment

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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.
6. (Optional) Choose **Edit** to modify any of the following options for the VPC attachment:
   - Enable or disable appliance mode support.
   - Enable or disable IPv6 support.
   - Enable or disable DNS support.
   - Enable or disable security group referencing support.
   - Add or remove subnet IDs.
7. After making any changes, choose **Edit attachment**.
8. To add, edit, or remove 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.
9. 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.

View a VPC attachment using the command line or API

Use the command line or API to view a VPC attachment.

To view a VPC attachment using the command line or API

- See get-vpc-attachment.

Site-to-Site VPN attachments in AWS Cloud WAN

Attaching a Site-to-Site VPN connection to your core network edge, first requires that you create a Site-to-Site VPN connection with **Target Gateway Type** set to **Not Associated**. See Create 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.

Topics

Create a Site-to-Site VPN attachment for an AWS Cloud WAN core network

You can create a Site-to-Site VPN attachment using either the Network Manager console or the AWS CLI.

Topics

Create a Site-to-Site VPN attachment using the console

The following steps create a Site-to-Site VPN attachment for a core network using the console

To create a Site-to-Site VPN attachment using the console

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
3. On the **Global networks** page, choose the global network link for the core network you want to add an attachment to.
4. In the navigation pane under he name of the global network, choose **Attachments**.
5. Choose **Create attachment**.
6. Enter a **name** identifying the attachment.
7. From the **Edge location** dropdown 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**.

Create a Site-to-Site VPN attachment using the command line or API

Use the command line or API to create an AWS Cloud WAN Site-to-Site VPN attachment.

To create a Site-to-Site VPN attachment using the command line or API

- Use `create-site-to-site-vpn-attachment`. See create-site-to-site-vpn-attachment.

View or edit an AWS Cloud WAN Site-to-Site VPN attachment

You can view and edit configuration information for a VPN attachment, as well as adding a new attachment. If you want to add a new VPN attachment, see the section called “Create a Site-to-Site VPN attachment”.

To view and edit a VPC attachment

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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. In this section, you can also edit the attachment Tags by choosing the **Tags** tab.
6. Choose **Edit**.
7. On the **Edit attachment** page, do any of the following:
   - Enable or disable appliance mode support.
   - Enable or disable IPv6 support.
   - Add or remove subnets IDs.
   - Add or remove 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.

View a Site-to-Site VPN attachment using the command line or API

Use the command line or API to viewt a Site-to-Site VPN attachment.

To view a Site-to-Site VPN attachment using the command line or API

- See get-site-to-site-vpn-attachment.

Transit gateway route table attachments in AWS Cloud WAN

Transit gateway route tables contain the rules that determine how your network traffic is routed between your VPCs and VPNs. A transit gateway route table can be added as an attachment type in your AWS Cloud WAN core network. You can create a transit gateway route table attachment through either the console or by using the command line or API.

Before creating the attachment you must first have created your transit gateway route table.

- For more information about transit gateway route tables, see Routing in the *AWS Transit Gateway User Guide*.
- For the steps to create a transit gateway route table, see Transit gateway route tables in the *AWS Transit Gateway User Guide*.

Topics

Create a transit gateway route table attachment for an AWS Cloud WAN core network

Add a transit gateway route table attachment to your AWS Cloud WAN core network.

Create a transit gateway route table attachment using the console

The following steps create a transit gateway route table attachment for a core network using the console.

To create a transit gateway route table attachment using the console

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
3. On the **Global networks** page, choose the global network link for the core network you want to add an attachment to.
4. In the navigation pane under he name of the global network, choose **Attachments**.
5. Choose **Create attachment**.
6. Enter a **name** identifying the attachment.
7. From the **Edge location** dropdown list, choose the location where the attachment is located.
8. From the **Attachment type** dropdown list, choose **Transit gateway route table**.
9. In the **Transit gateway route table attachment** section, choose the **Transit gateway peering** that will be used for the route table attachment. For information on creating a peering, see the section called “Create a peering”.

10. From the **Transit gateway route table** list, choose the route table to be used for the peering. For information about creating a transit gateway route table, see Transit gateway route tables in the *AWS Transit Gateway Guide*.
11. (Optional) In the **Tags** section, add **Key** and **Value** tags to 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**.

Create a transit gateway route table attachment using the command line or API

Use the command line or API to create an AWS Cloud WAN transit gateway route table attachment.

To create a transit gateway route table attachment using the command line or API

- Use `create-transit-gateway-route-table-attachment`. See create-transit-gateway-route-table-attachment.

View or edit an AWS Cloud WAN transit gateway route table attachment

You can view and edit the key-value tags associated with a transit gateway route table attachment, as well as adding a new attachment. For the steps to add a new transit gateway route table attachment, seethe section called “Transit gateway route table attachments”.

To view and edit a Connect peer attachment

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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 **Transit gateway route table**.
6. To add, edit, or remove 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.

View a transit gateway route table attachment using the command line or API

Use the command line or API to view a transit gateway route table attachment.

To view a transit gateway route table attachment using the command line or API

- See get-transit-gateway-route-table-attachment.

Accept or reject an AWS Cloud WAN core network attachment

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/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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 an AWS Cloud WAN core network attachment

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/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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 an attachment using the command line or API

- For a Connect, transit gateway route table, VPC, or Site-to-Site VPN attachment, see delete-attachment.
- For a Connect peer attachment, see delete-transit-gateway-connect-peer.

Core network policy versions in AWS Cloud WAN

Create a version of your current network policy any time you want to make changes to your network. Policy versions can be created using the console, through either the visual editor mode or directly in JSON, or you can download a version of any policy and make changes to that policy in any JSON editor. Once you create a new version of a policy you can compare that version against an older version to view changes.

New versions of policies are not automatically deployed, so once you create a policy version you can deploy that policy at a time of your own choosing. You can also restore any out-of-date policy to become the new current version.

The name of each policy version you create is numbered incrementally from the LATEST version. For example, if the LATEST 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 deploy.

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 deployed as the new LIVE policy. You can have multiple policy versions in this state, but you can only have one LIVE policy. When deployed, the policy change set state changes to **Execution succeeded**. For the steps to deploy a policy change set state, see the section called “Deploy a core network policy version”.
- **Execution succeeded** — The policy version was deployed 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 core network policy version”.
- **Failed generation** — An error prevented the policy from generating. Choose the Failed generation link to see details about the failure.
- **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**. If policy generation failed, this state changes to **Failed generation**.

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

Topics

- Core network policy sections
- AWS Cloud WAN service insertion
- Create an AWS Cloud WAN core network policy version using the console
- Create an AWS Cloud WAN core network policy version using JSON
- View an AWS Cloud WAN core network policy change set
- Compare AWS Cloud WAN core network policy change set versions
- Deploy an AWS Cloud WAN core network policy version
- Delete an AWS Cloud WAN policy version
- Download an AWS Cloud WAN core network policy
- Restore an out-of-date AWS Cloud WAN core network policy version

Core network policy sections

The following are the parts of a core network policy and describe how each of these work. If you're using either the console or a JSON file, a policy version is always composed of these sections.

Topics

Network configuration

Use **Network configuration** 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.

See the following for the steps to configure your network:

- To configure your network using the console, see the section called “Configure the core network settings”.
- To configure your network using a JSON file, see the section called “`core-network-configuration`” in the section called “Core network policy version parameters”.

Segments

The Segments section of a policy allows to divide your global network into separate isolated networks. Here 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.

See the following for the steps to add segments to your core network:

- To add a segment using the console, see the section called "Add a segment".
- To add a segment using a JSON file, see the section called "`segments`" in the section called "Core network policy version parameters".

Network function groups

A network function group is composed of a group of attachments used to steer those attachments to network security group functions. For example, you might create a network function group that steers traffic from a production segment through an inspection VPC directly to the Internet.

Optionally use the **Network function groups** page to create a group that allows you to insert AWS and third-party networking and security services on Cloud WAN using your policy document. After creating a network function group you'll create a segment action that defines how you want to steer the segments and attachments for the network function group.

- For the steps to create a network function group using the console, see the section called "Create a network function group".
- For the steps to create a network function group using JSON, see the section called "`network-function-groups`" in the section called "Core network policy version parameters".

Segment actions

Segment actions allow you to optionally share your segments, create routes, or create a service insertion action for a network functions group.

- **Segment sharing** — Segment sharing is bidirectional by default. When you create a segment share between two segments, routes from both segments are automatically advertised to each other. For example, you might share a segment named `test` with another segment named `dev`. Routes from `test` are advertised to `dev`, and vice versa. To make routes in shared segments unidirectional, create a deny list filter to share routes from one segment to the other, but not vice versa. Using the previous example, you could make a deny list filter that prevents

routes from `test` being advertised to `dev`. For more information on creating the deny list for a segment, see the section called "Add a segment".

- **Segment routes** — Create a segment route to define a static route within a segment.
- **Service insertion** — Create a service insertion action that allows you to insert a network function within a segment or across segments. This action can either be send via (east-west) or send to north-south). For more information about traffic actions and modes see the section called "Traffic actions and modes". You can additionally choose to specify which edge locations you want to use. Service insertion uses a default order for choosing the edgte locations. However, you can specify which edges you want to use as well as which edge is the preferred edge.

See the following for the steps to set segment actions:

- To add a segment using the console, see the section called "Add a segment action".
- To add a segment using a JSON file, see the section called "`segments`" in the section called "`segment-actions`" in the section called "Core network policy version parameters".

Attachment policies

Attachment policies control how your attachments map to your segments or network function groups. You create a network function group attachment policy using either the AND or OR subset of conditions along with either the full tag name or tag value.

See the following for the steps to create a network functions group attachment policy:

- To add an attachment policy using the console, see the section called "Create a core network attachment policy".
- To add an attachment policy using a JSON file, see the section called "`attachment-policies`" in the section called "`segment-actions`".

AWS Cloud WAN service insertion

Service insertion allows you to steer same-segment or cross-segment traffic using network functions deployed in VPCs or on-premises networks attached to Cloud WAN. Network functions can be third-party network or security appliances such as NGFW, IDS, IPS appliances or native AWS network firewall or Gateway Load Balancer services. Using either the AWS Network Manager

console or a JSON file, you'll create a version of one of your core network policies, create a network function group that contains a set of core network attachments where your network functions reside, and specify a segment or segment pairs for which traffic needs to be redirected to those network functions. Once the policy version is deployed and your new core network LIVE, Cloud WAN will automatically redirect network traffic between the segments to the specified core network attachments for the respective network function group. This redirection works for both same Region and cross-Region traffic on the core network. Service insertion works on both east-west (VPC to VPC) and north-south (VPC to the Internet or on-premises location) traffic.

To create a core network that includes service insertion, you'll need to do the following:

1. **Create a policy version of a current policy**. The initial policy you deploy when you create your first core network doesn't include any service insertion features. To do this you'll create a version of an existing policy and add the service insertion features. You can do this using either the AWS Network Manager console or through a JSON file.

   You can create a policy version containing the service insertion action using either the AWS Network Manager console or through creating a JSON file which you can also create using the console:

   - To create a policy version using the console, see the section called “Create a policy version using the console”.
   - To create a policy version using a JSON file, see the section called “Create a policy version using JSON”.
2. Using either the console or within the JSON file you'll do the following:
   a. **Configure your core network**. Set the BGP and ASN for this core network policy.
   b. **Add segments**. Add segments to your core network policy. Segments with cross-segment or same-segment traffic that must be steered via the network functions. Based on your policy configuration, Cloud WAN will automatically propagate routes from VPCs and networks associated to the network function groups and redirect VPC-to-VPC or VPC-to-Internet or on-premises traffic through a network functions group.
   c. **Create a network function group**. The network function group is a collection of attachments specifically used for network or security functions.

   > **Note**
   >
   > You can only have one attachment per network function group per Region.

d. **Set segment actions**. Segment actions allow you to share segments, create routes, and create a service insertion action.

   For the service insertion action, you can create a send via action which sends traffic east-west between all VPCs. Or you can create a send to action, which first sends traffic to a security appliance and then out from the appliance. For example, you might create segment action using send via. With this action, traffic is first routed to the Inspection VPC and then to the final destination, which could be another VPC, the Internet, or an on-premises location. See the section called “Traffic actions and modes” below for more information about traffic actions and modes.

   By default, Cloud WAN will select an attachment in one of the two Regions used for the network function. For example, if the network function is steering traffic to an Inspection VPC, and that Inspection VPC exists in only one Region, Cloud WAN uses the Region where the Inspection VPC resides to steer all cross-Region traffic. If the Inspection VPC exists in both Regions, service insertion will deterministically choose which Region to use based on the default Region priority list. However, when setting the segment actions, you can choose the Region priority order as well as choose the preferred Region to use. If the Inspection VPC doesn't exist in either Region, Cloud WAN uses the fallback Region specified in the segment policy. You can only specific a single fallback Region per segment policy.

e. **Create an attachment policy for the network function group**. Add the network function group to an attachment policy. The attachment policy then controls the order in which the network function group runs.

3. Deploy the policy version. See the section called “Deploy a core network policy version”.

Benefits

- **Simplified routing** — Service insertion allows for more simplified routing. You might need inter-VPC or VPC to internet or on-premises traffic to be routed through network appliances, such as network firewalls or load balancers. With Cloud WAN service insertion you can more easily steer network traffic to network or security appliances deployed in VPCs or in on-premises. This allows you to create and manage sometimes complex routing configurations or third-party automation tools.
- **Ease of deploying multi-Region inspection** — You might deploy Cloud WAN in multi-Region networks to support Region expansion or disaster recovery use cases. Service insertion simplifies mutli-Region deployment, allowing you to steer both intra-Region and inter-Region traffic

through your security infrastructure without having to set up complex multi-Region network configurations.

Traffic actions and modes

Service insertion supports the following traffic actions and modes for both east-west and north-south traffic.

- Send via — Traffic flows east-west between VPCs. All traffic for the service insertion action is first sent via a specific segment to the security appliance and then out to other VPCs.
  - Single hop — Traffic traverses a single intermediate attachment, using the deterministically preferred source or destination Region. You can set a list of Regions to use, as well as setting a preferred Region to use as a priority.
  - Dual hop — Traffic traverses inserted attachments in both the source and destination core network edges. For this option, the inspection attachment should be located in both Regions for each service insertion-enabled segment.
- Send to — Traffic flows north-south. That is, traffic flows into the network appliance, such as an Inspection VPC, and out to the Internet or to an on-premises location. Traffic does not re-enter the AWS cloud.

Attachments

Within a network function group you can specify a set of core network attachments where your network functions will reside. For example, the attachment might be a VPC that you use for inspection. You'll then add a segment or segment pair to this attachment that will be redirected to the network functions group and then to the security appliance. Cloud WAN automatically redirects traffic on any segment you add to that VPC when creating a service insertion action to that group both in the same Region and cross-Region within the core network.

In order to make an attachment be part of the network function group correctly, service insertion relies on the key-value pair tags added to an attachment. When creating an attachment you'll need to add the relevant tag to each attachment. For example, you might want to use a particular attachment as an Inspection VPC. You could add a tag with the key name *Inspection VPC* and then a key value of *InspectionVpcs*. The same tag should be applied to any attachment you add to that network function group. When you create a service insertion function, you'll add an attachment policy rule that relies on the key tags and values added to those attachments in order to process the tag key. In this example, you'd add a policy rule that identifies the tag *Inspection VPC* and

the key value of *InspectionVpcs*. Attachment policy rules can be created using either the AWS Cloud WAN console or through a JSON file. For the steps for either method, see the section called "Attachment policies".

> **Important**
>
> A network function group need not be associated with an attachment in order for the attachment policy to succeed. If you specify segment actions of **send-to** or **send-via** to a network function group with no attachments associated to it, the Cloud WAN policy execution will still be successful; however, all traffic destined to that network function group will be blackholed until you associate attachments to that group in appropriate Regions.

The following are the supported core network attachments:

- Connect
- Direct Connect gateway
- Transit gateway route table
- VPC
- VPN

Considerations

- **Attachments** — You can associate an attachment either with a segment or with a network function group, but it can't be associated with both.
- **Isolated mode** — Isolated mode is required for service insertion to work between attachments belonging to the same segment. This setting ensures there is no direct connectivity between attachments associated with the same segment by bypassing the network functions group.
- **Appliance mode** — Appliance mode must be enabled on the Inspection VPC to ensure that traffic moves in both directions.

Pricing

There are no additional charges for using service insertion other than the standard AWS Cloud WAN pricing charges. Information about Cloud WAN pricing can be found here: AWS Cloud WAN Pricing.

Create an AWS Cloud WAN core network policy version using the console

Use the Network Manager console to create a core network policy version. The console provides separate tabs for you to configure a network policy version. The following steps describe the high-level process.

1. the section called “Configure the core network settings”.

   You'll first set the network configuration parameters, including adding ASN ranges, CIDR blocks, and the edge locations to include in the policy.
2. the section called “Add a segment”.

   After defining the network configuration parameters, you'll add network segments and define the behavior for those segments. For example, you might want to include a segment that requires attachment acceptance.
3. the section called “Create a network function group”.

   The network function group provides an added level of security if you want to first steer specific segments to a third-party security device or an Inspection VPC. A network function group is the parent object for the segments you want to route to security appliances.
4. the section called “Add a segment action”.

   Define segment actions, such as sharing a segment, creating a segment route, or creating a service insertion action for the network function group.
5. the section called “Create a core network attachment policy”.

   Lastly, you'll create an attachment policy that defines the order when segments or network function groups should be run in the core network policy.

Topics

- Configure the core network settings in an AWS Cloud WAN policy version

- Add a segment to an AWS Cloud WAN core network policy version
- Create a network function group in an AWS Cloud WAN policy version
- Add a segment action in an AWS Cloud WAN core network policy version
- Create an attachment policy in an AWS Cloud WAN core network policy version

Configure the core network settings in an AWS Cloud WAN policy version

The following steps guide you through configuring a core network for a policy version using the **Policy versions** link on the AWS Network Manager console. For more information about a core network in a policy version, see the section called “Network configuration”.

To configure network for a policy version

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity** choose **Cloud WAN**.
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 any of the following:
        - **VPN ECMP support** if the core network should forward traffic over multiple-cost routes using VPN.
        - **DNS support** if you want to use DNS resolution for the core network.
        - **Security Group Referencing support** if you want to enable security group referencing for VPC attachments in the core network. For more information about security group referencing, see Security group referencing.
    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**.

> **Note**
>
> The **ASN range** is left-closed and right-open. This means that the leftmost number is included in the range but the rightmost number is not. For example, if you choose an ASN range of **64900-64903**, the actual available ASN range is **64900** through **64902**. **64903** is not included.

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.

> **Note**
>
> You can't change the ASN of a core network edge. Any transit gateway with the same ASN can't be peered to that core network edge. For example, if you have a core network edge with an ASN of 64512, you can't peer any transit gateway that also has an ASN of 64512.

    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**.

Add a segment to an AWS Cloud WAN core network policy version

The following steps guide you through configuring a core network for a policy version using the **Policy versions** link on the AWS Network Manager console. Before adding a segment you must first have configured your network settings. For more information, about network Segments, see the section called “Segments”.

To configure a segment

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity** choose **Cloud WAN**.
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.

> **Important**
>
> **Isolated attachments** is required if you're adding an intra-segment for use with service insertion.

12. For the **Segment filter**, choose if you want to **Allow all** shared routes from other segments, to **Allowed selected** segments, or to **Deny selected** segments. The default value is to **Allow all** segments.
13. (Optional) If you want to limit your edge locations for the segment, choose **Choose edge locations**, and then choose the edge locations you want to limit the segment to.
14. Choose **Create policy**.

Create a network function group in an AWS Cloud WAN policy version

The following steps guide you through configuring a core network for a policy version using the **Policy versions** link on the AWS Network Manager console. There are no prerequisites for creating a network functions group. For more information, about network function groups, see the section called “Network function groups”.

To route traffic using a network function group

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity** choose **Cloud WAN**.
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. Choose **Network function groups**.
8. Choose **Create**.
9. Enter a **Name** identifying this function, and then provide an optional **Description**.
10. If the attachment association requires acceptance, choose **Require acceptance**.

> **Note**
>
> An attachment can be associated only with a segment or a network functions group, but not both. You can't associate an attachment to a network functions group if that attachment is already associated with a segment.

11. Once you've created the network function group, you can create a service insertion segment action that routes your network functions from source segments to destination segments using this network function group. For more information on creating a segment action, see "Service insertion" in the section called “Add a segment action”.

Add a segment action in an AWS Cloud WAN core network policy version

The following steps guide you through optionally setting segment actions for a core network for a policy version using the **Policy versions** link on the AWS Network Manager console. Before setting segment actions you must first configure your network settings and add one or more segments. For more information, about segment actions, see the section called “Segment actions”.

Segment sharing

Create a shared segment between two segments.

Segment sharing is bidirectional by default. When you create a segment share between two segments, routes from both segments are automatically advertised to each other. For example, you might share a segment named `test` with another segment named `dev`. Routes from `test` are advertised to `dev`, and vice versa. To make routes in shared segments unidirectional, create a deny list filter to share routes from one segment to the other, but not vice versa. Using the previous example, you could make a deny list filter that prevents routes from `test` being advertised to `dev`. For more information on creating the deny list for a segment, see the section called “Add a segment”.

To create a shared segment

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity** choose **Cloud WAN**.
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 - optional**.
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 if you want to **Allow all** shared routes from other segments, to **Allowed selected** segments, or to **Deny selected** segments. The default value is to **Allow all** segments.
    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/networkmanager/home/.
2. Under **Connectivity** choose **Cloud WAN**.
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 - optional**.
7. (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**.

8. (Optional) Add **Attachment policies**. For more information, see the section called “Create a core network attachment policy”.
9. Choose **Create route**.

Service insertion

Create a segment route for a policy version.

To set up service insertion for a segment

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity** choose **Cloud WAN**.
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 - optional**.

> **Note**
>
> You must first have created your segments and network functions group.

7. If you want to create a service insertion action associated with a network functions group in the **Service insertion** section, choose **Create**, and then choose an **Action**. If you're not creating a service insertion action, this is an optional section.

Send via

This **Action** uses an east-west traffic pattern from attachment to attachment. For example, you might create a policy that directs all traffic between a segment named *Production* and all other segments via inspection VPC attachments.

1. For the **Mode**, choose one of the following:
   - **Single hop** — This option steers traffic through a single intermediate attachment.
   - **Dual hop** — Traffic traverses the inserted attachments in both the source and destination core network edges.
2. For **Segment from**, choose the source segment.
3. For **Segment to**, choose the destination segments.
4. For **Send traffic via**, choose the network functions group that you want to use for the service insertion.
5. (Optional) In **Edge overrides**, choose **Add**.
   - From the **Edge 1** and **Edge 2** drop-down lists, choose the edge locations for the overrides. the service the priority order for the edge locations to route traffic.
   - Choose the **Preferred edge** drop-down list to choose which edge location you prefer to use.
   - Choose **Add** to include additional edge overrides.

Send to

This **Action** uses north-south traffic, sending traffic to the security appliance, such as an Inspection VPC or firewall, and then out to the Internet or an on-premises location.

1. For **Segment from**, choose the segment coming into the security appliance. For example, you might have a segment named *production* that you want to first go to a security appliance.
2. For **Segment to**, choose one or more segments that traffic will flow to from the security appliance.
3. For **Send traffic via**, choose the network functions group that you want to use for the service insertion.
4. Optional) In **Edge overrides**, choose **Add**.

- From the **Edge 1** and **Edge 2** drop-down lists, choose the edge locations for the overrides. the service the priority order for the edge locations to route traffic.
- Choose the **Preferred edge** drop-down list to choose which edge location you prefer to use.
- • Choose **Add** to include additional edge overrides.

8. Choose **Create service insertion**.
9. (Optional) Add **Attachment policies**. For more information, see the section called “Create a core network attachment policy”.

Create an attachment policy in an AWS Cloud WAN core network policy version

The following steps guide you through configuring a core network for a policy version using the **Policy versions** link on the AWS Network Manager console. For more information about attachment policies, see the section called “Attachment policies”.

An attachment policy requires the following:

- The core network configured. See the section called “Configure the core network settings”.
- One or more segments. See the section called “Segments”.
- If you are optionally creating a service insertion action, you'll first need the following:
  - A network functions group. See the section called “Network function groups”.
  - At least one attachment. Supported attachment types are Connect, Direct Connect gateway, transit gateway route table, VPC, and Site-to-Site VPN. For more information about attachments, see the section called “Attachments”.

> **Important**
>
> An attachment is required when creating a policy that includes a service insertion action. If there is no associated attachment in the policy, traffic will be dropped instead of being redirected to a specified network function group.

To create an attachment policy

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

2. Under **Connectivity** choose **Cloud WAN**.
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 **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.
    - **Network function group** — creates an attachment policy rule for service insertion. Choose a network functions group for the service insertion policy. This option requires that you choose **Condition logic** and then the **AND** operator. For the **Type** you can choose the **Tag name** , **Tag value**, or both.
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.

> **Note**
>
> If `require-attachment-acceptance` is `false` for a segment, it's still possible for attachments to be added to or removed from a segment automatically when their tags

change. If this behavior is not desired, set `require-attachment-acceptance` to `true`.

12. (Optional) For **Condition logic**, further refine how the attachment is associated with the segment.

> **Important**
>
> **Condition logic** is required using **AND** for a network functions group attachment policy rule. The **AND** condition must use a **Tag name** or **Tag value** associated with the attachment.

- 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.

> **Important**
>
> **Tag name** and **Tag value** are the only supported and available **Conditions** for a **Network function group** attachment policy.

2. From the **Operator** dropdown list, choose one of the following operators. The operator determines the relationship of the Type.

> **Note**
>
> Operators are not supported when for a network function group attachment policy when the **Type** is **Tag name**. The full tag name must be used.

- **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**. If you're creating a network function group attachment policy, the full tag name or value are required. Partial C
4. Choose **Add** to include additional conditions or choose **Remove** to delete any conditions.

14. Choose **Create attachment policy**.
15. Choose **Create policy**.

Example condition logic for a network function group attachment policy

The following shows a partial JSON example using the OR operator for a network function group attachment policy.

- There are two segments, `production` and `development`.
- Rule numbers are manually assigned to each attachment policy for rule processing. Rules are then processed in numerical order according to the number assigned to them. In this example, the rule number is assigned `600` .
- Using the OR Condition logic, the network function group attachment policy looks for any segment with the value `production` or `development`.

For more information on the parameters used in the JSON file, see the section called “Core network policy version parameters”.

```
{
      "rule-number": 600,
      "condition-logic": "or",
      "conditions": [
        {
          "type": "tag-value",
          "operator": "equals",
          "key": "segment",
          "value": "production"
        },
        {
          "type": "tag-value",
          "operator": "equals",
          "key": "stage",
          "value": "development"
        }
      ],
      "action": {
        "add-to-network-function-group": "networkfunctiongroupone"
      }
    }
```

Example attachment policy

The following shows a JSON containing three attachment policies for a core network.

- There are three segments, `DevelopmentSegment`, `TestingSegment`, and `ProductionSegment`, which were first created on the **Segments** tab of the **Create policy** page. When these segments were created, `DevelopmentSegment` was set to automatically accept attachments, while `TestingSegment` and `ProductionSegment` were required to accept attachments. `ProductionSegment` was also limited to `us-east-1` only and only `TestingSegment` is allowed to advertise to this segment.
- Rule numbers are manually assigned to each attachment policy for rule processing. Rules are then processed in numerical order according to the number assigned to them. In this example, the following rule numbers are used: `100` for `DevelopmentSegment`, `200` for `TestingSegment`, and `300` for `ProductionSegment`. This indicates that rule `100` will be run first, followed by rule `200` and then rule `300`. Once an attachment matches a rule, no further rules are processed for that attachment. Rule `300` for `ProductionSegment` additionally

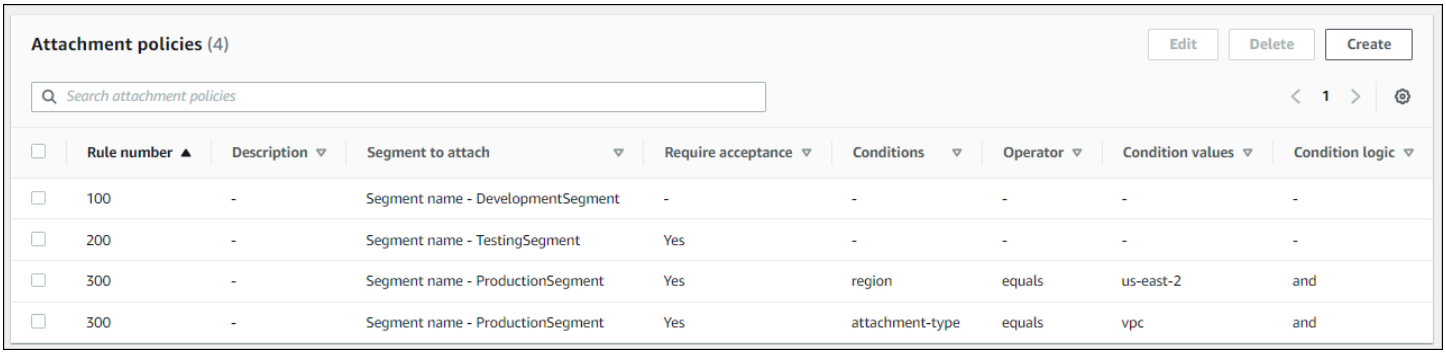
indicates that the policy will only accept `vpc` attachments and only if the request comes from `us-east-2`.

For more information on the parameters used in the JSON file, see the section called “Core network policy version parameters”.

```
{
  "version": "2021.12",
  "core-network-configuration": {
    "vpn-ecmp-support": true
  },
  "segments": [
    {
      "name": "DevelopmentSegment",
      "require-attachment-acceptance": false
    },
    {
      "name": "TestingSegment",
      "require-attachment-acceptance": true
    },
    {
      "name": "ProductionSegment",
      "edge-locations": [
        "us-east-1"
      ],
      "require-attachment-acceptance": true,
      "isolate-attachments": true,
      "allow-filter": [
        "TestingSegment"
      ]
    }
  ],
  "attachment-policies": [
    {
      "rule-number": 100,
      "condition-logic": "or",
      "conditions": [],
      "action": {
        "association-method": "constant",
        "segment": "DevelopmentSegment"
      }
    },
```

```
    {
      "rule-number": 200,
      "condition-logic": "or",
      "conditions": [],
      "action": {
        "association-method": "constant",
        "segment": "TestingSegment",
        "require-acceptance": true
      }
    },
    {
      "rule-number": 300,
      "condition-logic": "and",
      "conditions": [
        {
          "type": "region",
          "operator": "equals",
          "value": "us-east-2"
        },
        {
          "type": "attachment-type",
          "operator": "equals",
          "value": "vpc"
        }
      ],
      "action": {
        "association-method": "constant",
        "segment": "ProductionSegment",
        "require-acceptance": true
      }
    }
  ]
}
```

Using the **Visual editor**, the same policies display as follows:



Note that if an attachment policy uses the **and** condition, each condition appears on a separate row of the editor. In this example, since rule number 300 uses **region** and **attachment-type** conditions, each of those conditions appear on separate rows.

Create an AWS Cloud WAN core network policy version using JSON

You can create a core network policy by creating a JSON file. 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 version parameters”.

> **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/networkmanager/home/.
2. Under **Connectivity** choose **Cloud WAN**.
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. You can create a new policy version using a blank form, or copy and modify the contents of a policy version that you've downloaded.

- For the required and optional parameters in your JSON policy, see the section called "Core network policy version parameters".
- For the steps to download a previous policy version, see

8. Choose **Create policy**.

   A new policy version is generated.

   The **Change set state** on the **Policy version** page displays **Pending generation** while the new policy generates. The state changes when the policy either generates successfully or fails to generate.

Topics

- Core network policy version parameters in AWS Cloud WAN
- AWS Cloud WAN core network policy examples

Core network policy version parameters in AWS Cloud WAN

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 optional sections for defining network function groups and segment actions.

For example JSON policies, see the section called "Core network policy examples".

Topics

- core-network-configuration
- segments
- network-function-groups
- segment-actions
- attachment-policies

`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 can't be removed until the associated attachments are deleted. `core-network-configuration` is required.

Parameters

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

- General settings allow you to create the foundation of a core network, including whether VPN ECMP, DNS, and security group referencing are supported.
  - `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`. When set to `true`, traffic can be distributed across multiple VPN tunnels for better throughput and redundancy. The default is `true`.
  - `dns-support` — (Optional) Indicates whether DNS resolution is enabled for the core network. The value can be either `true` or `false`. When set to `true`, DNS resolution is enabled for VPCs attached to the core network, allowing resources in different VPCs to resolve each other's domain names. The default is `true`. For more information, see the section called “DNS support”.
  - `security-group-referencing-support` — (Optional) Indicates whether security group referencing is enabled for the core network. The value can be either `true` or `false`. When set to `true`, security groups in one VPC can reference security groups in another VPC attached to the core network, enabling more flexible security configurations across your network. The default is `false`. For more information about security group referencing, see Security group referencing.

- `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) Indicate whether the core network forwards traffic over multiple equal-cost routes using VPN. The value can either be `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`.

    Note

    You can't change the ASN of a core network edge. Any transit gateway with the same ASN can't be peered to that core network edge. For example, if you have a core network edge with an ASN of 64512, you can't peer any transit gateway that also has an ASN of 64512.

  - `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`.

    Note

    You can't delete the inside CIDR block once it's assigned to a core network edge.

For example, you might have the following core network configuration. This core network configuration establishes a Cloud WAN core network with VPN ECMP and DNS support enabled, while disabling security group referencing across VPCs. It allocates two internal CIDR blocks (`10.0.0.0/16` and `10.1.0.0/16`) for network connectivity, defines an ASN range of `65000-65100`, and deploys a single edge location in `us-east-1`, providing the foundation for a managed wide area network.

```
{
```

```
 "version": "2021.12",
 "core-network-configuration": {
    "vpn-ecmp-support": true,
    "dns-support": true,
    "security-group-referencing-support": false,
    "inside-cidr-blocks": [
        "10.0.0.0/16",
        "10.1.0.0/16"
    ],
    "asn-ranges": [
        "65000-65100"
    ],
    "edge-locations": [
        {
        "location": "us-east-1"
        }
    ]
 }
 ...
}
```

`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 separate 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 and 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, 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. The default value is `false`. When set to `true`, the only routes available will either be shared routes through the share actions, which are attachments in other segments, or static routes. 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 set the parameter to `true`.

> **Note**
>
> Routes coming from a route table attachment are not affected by the `isolate-attachments` parameter. You are responsible for managing routes propagating from their attached route tables. Routes flowing into the route table attachment from other attachments within the segment follow the standard `isolate-attachments` behavior

- `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`.

> **Note**
>
> If `require-attachment-acceptance` is `false` for a segment, it's still possible for attachments to be added to or removed from a segment automatically when their tags

change. If this behavior is not desired, set `require-attachment-acceptance` to `true`.

- `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.

`network-function-groups`

`network-function-groups` defines the container for the service insertion actions you want to include. This will include any attachment policies.

- `name` — Required. This identifies the network function group container.
- `description` — Optional description of the network function group.
- `require-attachment-acceptance` — This will be either `true`, that attachment acceptance is required, or `false`, that it is not required.

`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` can be any of the following:
  - `share` for a shared route
  - `create-route` for a route

- `send-via` for service insertion, indicating that traffic is sent from one Cloud WAN attachment to another (east-west).
- `send-to` for service insertion, indicating that traffic is sent out from the cloud and doesn't re-enter (north-south).

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, encapsulated within a `share-with` block. For example,

```
{
      "action": "share",
      "mode": "attachment-route",
      "segment": "segment",
      "share-with": {
        "except": [
          "dev",
          "prod"
        ]
      }
```

```
    }
```

- `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. This is the same case for multiple attachments that are defined across multiple remote Regions. Instead of an array of attachments, you can also provide a `blackhole`, which drops all traffic to the `destination-cidr-blocks`.

    Note
    - AWS Cloud WAN does not propagate blackhole routes.
  - `description` — (Optional) A user-defined description to help further identify this route.

- `send-via` and `send-to` parameters. If the network function group segment `action` is either `send-via` or `send-to`. Use `send-via` if you want to send east-west traffic between VPCs. Use `send-to` for north-south traffic; that is, traffic that first must come into your security appliance and then out to either the Internet or an on-premises location.

  The following are the required and optional parameters:

  - `segment` — Required. The name of an existing segment that can be used for the `send-via` or `send-to` action.

- mode — This only applies when the `action` is `send-via`, and indicates the mode used for packets. This will be either `single-hop` or `dual-hop`. `send-to` does not rely on `mode` for traffic.
- `when-sent-to` parameters are used to list the destination segments for the `send-via` or `send-to` action.
  - `segments` — The list of segments that the `send-via` action uses. `segments` is not used for the `send-to` action.
- `via` parameters describe the network function groups and any edge overrides associated with the
  - `network-function-groups` — The network function group to use for the service insertion action.
  - `with-edge-overrides` parameters describe any edge overrides and the preferred edge to use.
    - `edge-sets` — The list of edges associated with the network function group.
    - `use-edge` — The preferred edge to use.

The following example shows an example of the `send-via` action:

- Traffic is sent via a segment named `development`.
- the `via` parameter, which contains the details of the edge locations and overrides. It uses a network function group named `inspection-vpc` and has two defined `edge-sets`, `corenetwork1`and `corenetwork2`. `corenetwork2` is set as the preferred core network edge (`use-edge`).

```
{
        "segment": "SendToInspectionVPC",
        "action": "send-via",
        "mode": "single-hop",
        "when-sent-to": {
            "segments ": [
                "development"
            ]
        },
        "via": {
            "network-function-groups": [
                "inspection-vpc"
            ],
            "with-edge-overrides ": [
```

```
                {
                    "edge-sets ": [
                        ["corenetwork1", "corenetwork2"]
                    ],
                    "use-edge": "corenetwork2"
                }
            ]
        }
    }
```

The following example shows an example of the `send-to` action. In this example, traffic is sent to a segment named `development` through a network function group named `inspection-vpc`.

```
{
      “action”: “send-to”,
      “segment”: “development”,
      “via”: {
        “network-function-groups”: [
          “inspetion-vpc”
        ]
      }
    }
]
```

`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. The tags are then used to associate the attachment to the specified segment or network function group. A core network supports the following types of attachments:

- Transit Gateway Connect — `connect`
- Direct Connect gateway — `direct-connect-gateway`
- VPC — `vpc`
- VPN — `site-to-site-vpn`
- Transit Gateway route table — `transit-gateway-route-table`

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.

If you're creating an attachment policy that includes a network functions group for service insertion, an attachment is required. If you attempt to create a service insertion policy that doesn't include an attachment, policy generation will fail.

`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 `and` if you want to the rule to match on all of the conditions, or use `or` if you want the rule to match on one of the conditions.

  If you're creating a JSON policy for a network function group `and` and `or` are the only supported `condition-logic` options.
- `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.

   A network function group attachment policy requires that you use the `tag-exists` type and then either `tag-name` or `tag-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`.

     `operator` is not supported for tag-name in a network function group policy version.
   - `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.
- `add-to-network-function-group` — The name of the network function group to attach to the attachment policy. The network function group must use and for the `condition-logic` and have an associated `Conditions` tag.

  The following shows an example policy adding a network function group named `SendToInspectionVPC`. The rule-number for the service insertion policy `125`. It uses the and condition-logic with a `tag` type of `tag-exists` type and a `key` value of `Location`.

```
"attachment-policies": [
    {
      "rule-number": 125,
      "description": "Sends to Inspection VPC",
      "condition-logic": "and",
      "conditions": [
        {
          "type": "tag-exists",
          "key": "Location"
        }
      ],
      "action": {
        "add-to-network-function-group": "SendToInspectionVPC"
      }
    }
  ]
}
```

AWS Cloud WAN 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 version parameters".

Topics

AWS Cloud WAN 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": "mynetwork",
   "require-attachment-acceptance": false
  }
 ],
 "attachment-policies": [
  {
   "rule-number": 100,
   "condition-logic": "and",
   "conditions": [
    {
```

```
     "type": "any"
    }
   ],
   "action": {
    "association-method": "constant",
    "segment": "mynetwork"
   }
  }
 ]
}
```

AWS Cloud WAN 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": "nonSecured"
        }
```

```
    ],
    "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"
            }
        }
    ]
}
```

AWS Cloud WAN 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 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"
            }
        }
    ]
}
```

AWS Cloud WAN 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": "sharedServices"
  }
 ],
 "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"
   }
  }
 ]
}
```

AWS Cloud WAN 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"
            }
        }
    ]
}
```

AWS Cloud WAN 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 internalApps segment to the internet.

Similar to Example: Edge consolidation, 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 internalApps 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": "internalApps"
  },
  {
   "name": "firewall"
  },
  {
   "name": "onPremises"
  }
 ],
 "segment-actions": [
  {
   "action": "create-route",
   "destination-cidr-blocks": [
    "0.0.0.0/0"
   ],
   "segment": "internalApps",
   "destinations": [
    "attachment-deadbeef901234567",
    "attachment-eeeeee00000000000"
   ],
   "description": "Send all internet headed on-premises through the firewall"
  },
  {
   "action": "create-route",
   "destination-cidr-blocks": [
    "0.0.0.0/0"
```

```
    ],
    "segment": "onPremises",
    "destinations": [
     "attachment-deadbeef901234567",
     "attachment-eeeeee00000000000"
    ],
    "description": "Send all traffic received from the VPN through the firewall"
   },
   {
    "action": "share",
    "mode": "attachment-route",
    "segment": "firewall",
    "share-with": [
     "internalAapps",
     "onPremises"
    ]
   }
  ],
  "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": "internalApps"
    }
   },
   {
    "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": "onPremises"
    }
   }
  ]
}
```

AWS Cloud WAN example: Service insertion firewalls between on-premises and VPCs

In this policy, traffic on a segment named *development* is first sent to an Inspection VPC before being sent to a segment named *production* using a network function group named *InspectionVPC*. The on-premises attachment has already been set up and mapped to either the `development` or `production` segments. The segment action uses `send-via`, indicating that this is east-west traffic. The attachment policy rule uses the `and` condition logic with `InspectionVpcs` as the value of the key-value pair associated with the attachment.

```
{
    "version": "2021.12",
    "core-network-configuration": {
        "vpn-ecmp-support": true,
        "inside-cidr-blocks": [
            "10.0.0.0/16"
        ],
        "asn-ranges": [
            "64512-65534"
        ],
```

```
        "edge-locations": [
            {
                "location": "us-east-2"
            },
            {
                "location": "us-west-2"
            }
        ]
    },
    "segments": [
        {
            "name": "development",
            "edge-locations": [
                "us-east-2"
            ],
            "require-attachment-acceptance": true,
            "isolate-attachments": true
        },
        {
            "name": "production",
            "edge-locations": [
                "us-east-2"
            ],
            "require-attachment-acceptance": true,
            "isolate-attachments": true
        }
    ],
    "network-function-groups": [
        {
            "name": "InspectionVPC",
            "description": "Route segment traffic to the inspection VPC",
            "require-attachment-acceptance": true
        }
    ],
    "segment-actions": [
        {
            "action": "send-via",
            "segment": "development",
            "mode": "single-hop",
            "when-sent-to": {
                "segments": [
                    "production"
                ]
            },
```

```
            "via": {
                "network-function-groups": [
                    "InspectionVPC"
                ]
            }
        }
    ],
    "attachment-policies": [
        {
            "rule-number": 125,
            "condition-logic": "and",
            "conditions": [
                {
                    "type": "tag-exists",
                    "key": "InspectionVpcs"
                }
            ],
            "action": {
                "add-to-network-function-group": "InspectionVPC"
            }
        }
    ]
}
```

View an AWS Cloud WAN core network policy change set

View proposed changes to a policy before deploying those changes to become the new live policy.

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 view a core policy version change set

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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. In the **Policy versions section**, choose the check box that you want to see policy changes for.
6. Choose **View or apply change set**. This creates a new version of the policy. The policy version is incremented by one from the last policy version.

7. The **Change set** page displays the **Type** of change being affected, for example, a core network segment, and the **Action** that's associated with that type, for example, adding a new segment.
8. In **New Values** and **Previous values**, choose **Details** to view the change in a JSON format.
9. In the **Compare** column, choose **Compare** to view a line-by-line comparison of the current live policy with the proposed policy change.

Compare AWS Cloud WAN core network policy change set versions

Compare two policy versions against each other using the console. The comparison returns line-by-line changes between the two policies in JSON format with changes highlighted.

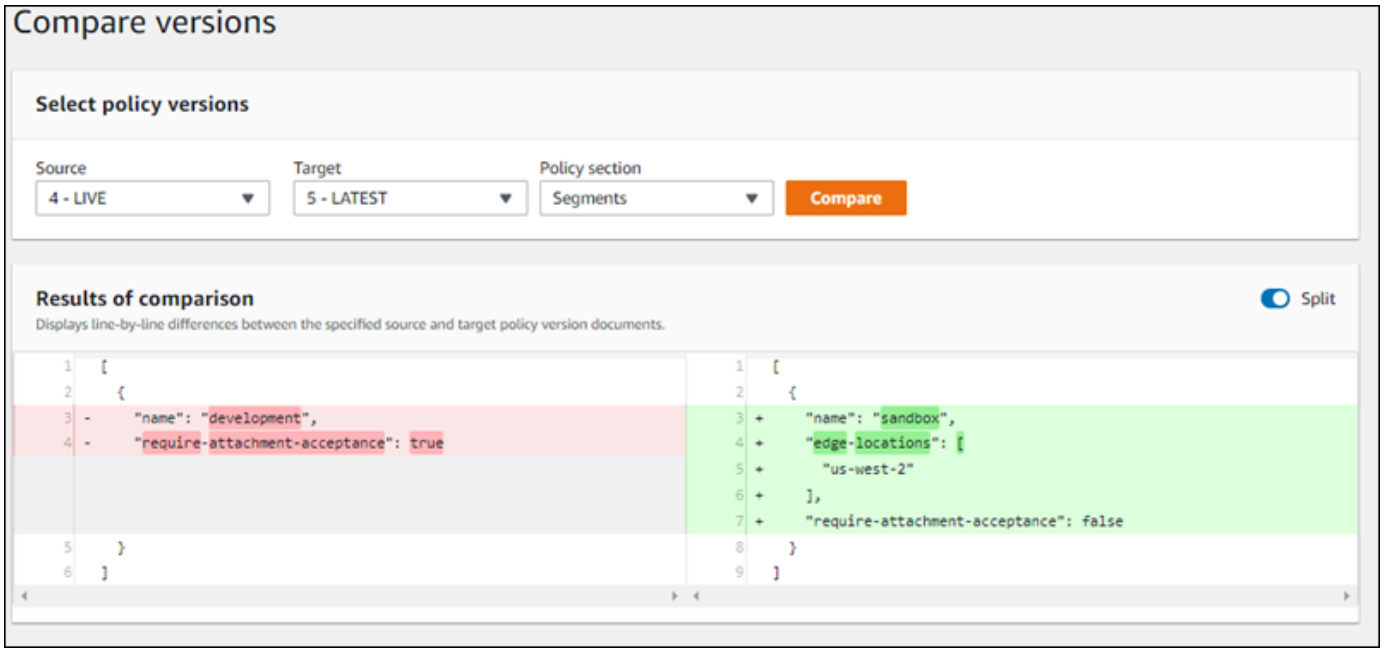
To compare policy versions

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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 compare against another policy.
6. Choose **View or apply change set**.
7. On the Change set page, choose **Compare with LIVE**.
8. From the **Source** and **Target** dropdown lists, choose the policy versions that you want to compare.
9. (Optional) From the **Policy section** dropdown list, choose a specific policy section to compare. Options are:

   - **All** — Compares all policy changes between the two policies. This is the default view.
   - **Network configuration** — Compares Border Gateway Protocol (BGP), Autonomous System Number (ASN), and core network edge locations.
   - **Segments** — Compares segment additions, deletions, or modifications.
   - **Segment actions** — Compares segment sharing and filtering.
   - **Attachment policies** — Compare how attachments map to segments.

10. Choose **Compare**.

The **Results of comparison** section displays the changes between the two policies. In the following example, the **Segments** of a current LIVE **Source** policy are compared against the segment changes to an undeployed **Target** policy. The comparison shows that a new segment, **sandbox**, will be added when deploying the **Target** policy version.



11. By default, the changes for each policy display in separate policy windows. To see the results of the comparison line-by-line in a single window, turn the **Split** toggle off.

Deploy an AWS Cloud WAN core network policy version

fter creating a version of a policy, you can deploy the policy version as your new **LIVE** policy. Deploying a new policy version never occurs automatically.

To implement a core policy version

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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. On the **Policy versions** page, choose the policy that you want to deploy.
6. Choose **View or apply change set**.

7. (Optional) Do either of the following:

   - To review the proposed changes to the policy, choose **Details** in the **New values** column.
   - To review the values of the original policy, choose **Details** in the **Previous values** column.
8. Choose **Apply change set** to deploy the policy to become the new LIVE policy.
9. On the Policy versions page, the status of the policy deployment is **Executing policy**.
10. To view the deployment details and progress, choose the policy link. The **Policy version - X** page appears.

    - The **Policy details** page displays information about the policy that you're deploying.
    - The **JSON** page displays policy information as a JSON file.
    - The **Execution progress** page displays the status of the policy deployment. You can view all events related to the deployment or you can view specific events. For example, you might want to view the deployment status of core network edges.
11. When finished, the **Alias** changes to **LIVE/LATEST** and the **Change set state** changes to **Execution succeeded**. The **Change set state** of any previous policies that were in a **Ready to execute** change set state change to **Out of date**. This indicates that those policies are now considered older than the current LIVE policy.

Delete an AWS Cloud WAN 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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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 an AWS Cloud WAN core network policy

Download any policy version or your current LIVE policy as a JSON file. You can open the downloaded file in any JSON editor.

To download a core policy

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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. You can create a new policy version using the contents of this file by pasting them into the Cloud WAN JSON editor. For the steps to create a policy using the JSON editor, see the section called “Create a policy version using JSON”.

Restore an out-of-date AWS Cloud WAN core network 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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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 one 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**.

Devices in AWS Cloud WAN

Devices represent a physical or virtual appliance. When you add a device to your core network, you can include optional information such as vendor, model and serial number to help you more easily identify the device.

In addition, you'll indicate whether the device is on-premises or in the AWS Cloud. If the device is on-premises you can specify optional information such as physical address. If the device is in the AWS Cloud, you can specify the zone, subnet ID, latitude and longitude, and physical address. Tags are also used to more help you identify this Network Manager resource.

Once added to your global network, a device can then be associated with a site. Before you can associate the device with a site using a link, you must first create the site. For more information on creating sites and linking the site to a device, see the section called “Sites and links”.

> **Note**
>
> A single device can't be associated with multiple sites.

Topics

Add a device to an AWS Cloud WAN global network

Add a device to your Cloud WAN global network. Devices can then be associated to sites using links.

To add a device

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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`**).

Delete a device from an AWS Cloud WAN global network

Delete a device that is no longer a part of your Cloud WAN global network.

To delete a device

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

2. Under **Connectivity**, choose **Global Networks**.
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 want to delete, and then choose **Delete**.
6. Confirm that you want to delete the device by choosing **Delete** again.

   Deletion occurs immediately.

Edit a device in an AWS Cloud WAN global network

Edit the details of a device, including changing whether the location type is either on-premises or AWS Cloud.

To edit a device

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the device check box, and then choose **Edit**.
6. Edit any of the following information as needed:

   - **Description**
   - **Model**
   - **Serial Number**
   - **Type**
   - **Router**
   - **Vendor**
   - **Location type**. This will be either **On-premises** or **AWS Cloud**, and then edit any related information for the **Location type** as needed.
   - **Tags**
7. Choose **Edit device**.

View device details in an AWS Cloud WAN global network

View details about a device. On the device details page you can access tabs:

- **Overview**

  This tab provides general information about the device, such as the device State, Vendor, and Model. You can also edit, delete, and associate or disassociate the device with a site,

- **Links**

  Associate or disassociate a link with a device.

- **On-premises associations**

  Associate or disassociate a device with a customer gateway. You must have at least one gateway set up and one link to create the association.

- **Connect peer associations**

  Associate a Connect peer with a device, allowing you to connect with a transit gateway. You must have at least one Connect peer and one link.

- **Connections**

  Create a connection between two devices using a link. You can create a connection between two devices in your global network. The connection can be between a physical or virtual appliance and a third-party appliance in a VPC, or between physical appliances in an on-premises network. A connection is created for a specific global network and cannot be shared with other global networks.

- **VPNs**

  View the VPNs associated with the device. On this tab you can only view the associations of a transit gateway with a device.

- **Monitoring**

  Monitor the device's data in, data out, and Tunnel down count average with CloudWatch metrics. You can modify the CloudWatch time frame as well as add these metrics to your global network dashboard.

Topics

- Associate or disassociate a device link in an AWS Cloud WAN global network

- Associate or disassociate an on-premises link in an AWS Cloud WAN global network
- Associate or disassociate a Connect peer link in an AWS Cloud WAN global network
- Create or delete a device connection in an AWS Cloud WAN global network
- View VPNs in an AWS Cloud WAN global network
- Monitor devices in an AWS Cloud WAN global network

Associate or disassociate a device link in an AWS Cloud WAN global network

Associate a link with a device in your Cloud WAN global network. In order to associate a link with a device, you must first create a link that can be used for the device connection. For more information on creating a ink, see the section called “Create a link”.

You can only associate one link with one device. If a link is already associated with a device, and you want to use that link with another device, you must first disassociate the link the device it's associated with.

To associate a link with a device

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the link for the device **ID** 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. Choose the **Links** tab, and then choose **Associate link**.
7. Choose the link that you want to associate with the device.
8. Choose **Associate link**.

   The link is available to use immediately.

If you to use a link with another device, you must first disassociate the link from its original device.

To disassociate a link from a device

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the link for the device **ID** 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. Choose the **Links** tab, and then choose **Associate link**.
7. Choose the check box for the link that you want to disassociate from a device.
8. Choose **Disassociate link**.

   Disassociation occurs immediately.

Associate or disassociate an on-premises link in an AWS Cloud WAN global network

Associate or disassociate an on-premises device link association in your Cloud WAN global network.

You can only associate one link with a customer gateway. If a link is already associated with a customer gateway, and you want to use that link with another gateway, you must first disassociate the link the gateway it's currently associated with.

To create an on-premises association

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the link for the device **ID** that you want to create an on-premises association for.

6. Choose the **On-premises associations** tab.
7. Choose **Associate**.
8. Choose the on-premises **Customer gateway**.
9. (Optional) Choose the **Link** used for the connection.
10. Choose **Create on-premises association**.

    The link is available to use immediately.

To disassociate an on-premises association

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the device **ID** link.
6. Choose the **On-premises association** tab.
7. Choose the check box for the on-premises association that you want to disassociate.
8. Choose **Disassociate**.

    Disassociation occurs immediately.

Associate or disassociate a Connect peer link in an AWS Cloud WAN global network

Associate or disassociate a Connect peer device link association in your Cloud WAN global network.

You can only associate one link with a Connect peer. If a link is already associated with a Connect peer, and you want to use that link with another Connect peer, you must first disassociate the link the Connect peer it's associated with.

To create a Connect peer association

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.

3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the link for the device **ID** that you want to create an on-premises association for.
6. Choose the **Connect peer** tab.
7. Choose **Associate**.
8. Choose the on-premises **Connect peer**.
9. (Optional) Choose the **Link** used for the connection.
10. Choose **Create Connect peer association**.

    The link is available to use immediately.

To disassociate a Connect peer association

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the device **ID** link.
6. Choose the **Connect peer** tab.
7. Choose the check box for the Connect peer that you want to disassociate.
8. Choose **Disassociate**.

    Disassociation occurs immediately.

Create or delete a device connection in an AWS Cloud WAN global network

Create or delete a connection between two devices in your Cloud WAN global network.

To create a connection

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.

4. In the navigation pane, choose **Devices**.
5. Choose the **Connections** tab, and then choose **Create connection**.
6. For the **Name** and **Description**, enter a name and optional description for the connection.
7. (Optional) For **Link**, choose a link to associate with the first device in the connection.
8. For **Connected device**, choose the ID of the second device in the connection.
9. (Optional) For **Connected link**, choose a link to associate with the second device in the connection.
10. Choose **Create connection**.

Delete the existing connection between two devices or delete a connection between two devices in your Cloud WAN global network.

To delete a device connection

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the **Connections** tab.
6. In the **Connections** section, choose the check box of the connection you want to delete.
7. Choose **Delete**.
8. Choose **Delete** again to confirm you want to delete the connection.

   The connection is deleted immediately.

View VPNs in an AWS Cloud WAN global network

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

To view device VPN connections

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.

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**.

Monitor devices in an AWS Cloud WAN global network

Monitor device Amazon CloudWatch events on the AWS Cloud WAN Monitoring page.

To monitor devices

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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.

Peerings in AWS Cloud WAN

AWS Cloud WAN peering connections allow you to interconnect your core network edge with an AWS Transit Gateway in the same Region. Peering connections between Cloud WAN and transit gateways support dynamic routing with automatic exchange of routes using BGP. You can use route table attachments on the peering connection to selectively exchange routes between a specific transit gateway route table and a Cloud WAN network segment for end-to-end segmentation and network isolation.

The peering connection supports policy-based routing to implement segment isolation across peering connections. Using this capability, routes are selectively propagated between a route table in transit gateway and a core network segment. You first need to create the peering connection and associate a policy table to the transit gateway peering attachment. A policy table contains rules for matching network traffic by a specific route table or segment, and then maps traffic that matches the rule to a target route table for determining routing behavior.

When you create a peering connection, you can either create a new policy table or use an existing policy table for association with the peering attachment. As you create your route table attachments, the policy table is populated automatically with the policy rules that match network traffic by a segment or routing domain, and then maps the traffic that matches the rule to a target route table. For more information about transit gateway peering, see Transit gateway peering attachments in the *AWS Transit Gateway Guide*.

Peering limitations

Limits apply when creating a transit gateway peering connection between your transit gateways in AWS Cloud WAN.

The following limitations apply when creating a peering:

- A transit gateway used for peering must be in the same Region as the core network.
- The Autonomous System Number (ASN) of a transit gateway and the core network must be different.
- A transit gateway connection to Cloud WAN only supports dynamically propagated routes. An error is returned if you try to add a static route.

Topics

- Create a peering in an AWS Cloud WAN core network

- View peering details in an AWS Cloud WAN core network
- Delete a peering from an AWS Cloud WAN core network
- Edit peering tags in an AWS Cloud WAN core network

Create a peering in an AWS Cloud WAN core network

Create a transit gateway peering.

Important

Before creating a peering, make sure that the account you use to create the peering has the following permissions:

- `ec2:CreateTransitGatewayPolicyTable`
- `ec2:AcceptTransistGatewayPeering`
- `ec2:AssociateTransitGatewayPolicyTable`

To create a peering

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Peerings**.
5. Choose **Create peering**.
6. (Optional) Enter a **name** identifying the peering.
7. From the **Edge location** dropdown list, choose the edge location where the peering is located.
8. From the **Transit gateway** dropdown list, choose a transit gateway to be used for the peering.

   Note

   The core ASN and the transit gateway ASN must be unique. ASNs must be unique for peerings to succeed.

9. Choose one of the following **Associate policy table** options:

- **New** — Creates a new policy routing table.
- **Existing** — Allows you to associate this peering with an existing policy table. If you choose this option, you'll be prompted to choose an existing **Transit gateway policy table** to associate with the peering. For information on creating a transit gateway policy table, see Transit Gateway policy tables in the *AWS Transit Gateway Guide*.

10. (Optional) If the transit gateway is not registered in your global network, choose **Register the specific transit gateway to the global network** to simultaneously register the transit gateway to the global network. If your transit gateway is already registered, this option does not display.
11. (Optional) In the **Tags** section, add **Key** and **Value** tags to help identify this resource. You can add multiple tags by choosing **Add tag**, or remove any tag by choosing **Remove tag**.
12. Choose **Create peering**.

    The **Create peering progress** displays the current status of the peering deployment. When deployment is complete, the **State** of the peering on the **Peerings** page displays **Available**. You can then use this peering to create a transit gateway route table attachment. See the section called “Transit gateway route table attachments”

View peering details in an AWS Cloud WAN core network

View information about a transit gateway used for peering.

To view peering details

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Peerings**.
5. Choose the **Peering ID** of the peer that you want to view details for.
6. In the **Details** section, choose the **Resource ID** link.

   The **Transit gateways** page appears in a new window. Depending on your permissions, you can add or modify your transit gateways or transit gateway route tables. For more information on working with transit gateways, see the *AWS Transit Gateway Guide*.

Delete a peering from an AWS Cloud WAN core network

Delete a transit gateway peering.

To delete a peering

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Peerings**.
5. Choose the **Peering ID** of the peer that you want to delete.
6. Choose **Delete**.
7. In the confirmation box, choose **Delete**.

   The **Peering** page displays a confirmation that you deleted the transit gateway peering.

Edit peering tags in an AWS Cloud WAN core network

Edit the tags that are associated with transit gateway peering.

To edit peering tags

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Peerings**.
5. Choose the **Peering ID** of the peer that you want to add or modify tags for.
6. In the **Peering name** section, choose the **Tags** tab.
7. Choose **Edit tags**.
8. Do any of the following:

   - To add a new tag, choose **Add tag**, and then add a new **Key** and **Value**.
   - To remove an existing tag, choose **Remove tag** for the tag that you want to delete.

- To edit an existing tag, change the **Key** or **Value** text as needed.

9. Choose **Edit tags**.

Shared attachments in AWS Cloud WAN

You can share attachments on any of your shared core networks. For more information on sharing core networks, see the section called "Shared core network".

When a core network owner shares their core network with your account, you are then able to create new VPC, transit gateway route table, or Direct Connect gateway attachments for the shared core network. You can also view the current attachments or delete an attachment from the shared core network.

> **Note**
>
> A shared core network currently supports only VPC, transit gateway route table, and Direct Connect gateway attachments.

Topics

- Create a shared VPC attachment in an AWS Cloud WAN core network
- Create a shared transit gateway route table attachment in an AWS Cloud WAN core network
- Create a shared AWS Direct Connect gateway attachment in an AWS Cloud WAN core network
- View shared AWS Cloud WAN attachments

Create a shared VPC attachment in an AWS Cloud WAN core network

Use the AWS Network Manager console to create a shared VPC attachment that can be used across accounts.

To create a shared VPC attachment

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.

3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, under **Shared by me**, choose **Attachments**.
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 that is where you want to create the VPC attachment.
8. From the **Edge location** dropdown list, choose the location where the attachment is located.
9. From the **Attachment type** dropdown list, choose **VPC**.
10. Optionally choose any of the following:

    - Choose **Appliance mode support** if appliance mode is supported. For more information about appliance mode, see the section called “Appliance mode”.
    - Choose **IPv6 support** if the attachment supports IPv6.
    - By default, **DNS support** is enabled. This allows domain name system resolution for the attachment. Clear the check box if you don't want to enable DNS support. For more information, see the section called “DNS support”.
    - By default **Security Group Referencing support** is enabled. When you create a VPC attachment, Cloud WAN automatically enables security group referencing for VPCs attached to the same core network edge. This allows you to reference security groups across VPCs in your security group rules. Clear the check box if you don't want to enable security group referencing. For more information, see the section called “Security group referencing”.
11. 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.
12. (Optional) In the **Tags** section, add **Key** and **Value** pairs to 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**.
14. 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**

15. Choose **Create attachment** to create a new shared VPC attachment.

Create a shared transit gateway route table attachment in an AWS Cloud WAN core network

The following steps guide you through creating a shared transit gateway attachment.

To create a shared transit gateway attachment

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, under **Shared by me**, choose **Attachments**.
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 that is 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. From the **Attachment type** dropdown list, choose **Transit gateway route table**.
11. From the **Transit gateway peering** dropdown list in the **Transit gateway route table attachment** section, choose an existing peering to share.
12. (Optional) In the **Tags** section, add **Key** and **Value** pairs to 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**.
14. 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**

15. Choose **Create attachment** to create the new shared VPC or transit gateway attachment. See the section called “Attachments”.

Create a shared AWS Direct Connect gateway attachment in an AWS Cloud WAN core network

The following steps guide you through creating a shared Direct Connect gateway attachment.

To create a shared Direct Connect gateway attachment

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, under **Shared by me**, choose **Attachments**.
5. Choose **Create attachment**.
6. Enter a **Name** identifying the attachment.
7. From the **Core network** drop-down list, choose the core network that you want to associate the Direct Connect gateway with.
8. From the **Attachment type** drop-down list choose **Direct Connect gateway attachment**.
9. For the **Edge locations**, choose one of the following:

   - **All** — Choose this option if you want to associate all edge locations in your core network with the Direct Connect gateway. When choosing this option, any new edge locations deployed in a core network policy version are automatically added to the Direct Connect gateway attachment and updated with the Direct Connect gateway. This does not automatically update any edge locations you might remove from the core network policy.

- **Specific** — Choose this option if you want to associate only a subset of edge locations from your core network policy with the Direct Connect gateway. When choosing this option, you must manually add new or remove edge locations to the Direct Connect gateway attachment after deploying a core network policy version. A Direct Connect attachment will be attached to the core network edge according to the core network policy edge locations but will associated to the segment based on the segment edge locations.

10. In the **Direct Connect gateway attachment** section, choose the Direct Connect gateway to use for connecting Direct Connect to the Cloud WAN core network.

> **Note**
>
> A Direct Connect gateway can be used for only one core network, and can't be used for any other Direct Connect gateway type. If the attachment between the Direct Connect gateway and the core network is removed, the gateway becomes available for other Direct Connect association types.

11. Choose **Create attachment**.

View shared AWS Cloud WAN attachments

View details about your shared VPC and transit gateway attachments.

To view shared VP and transit gateway attachments

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, under **Shared by me**, choose **Attachments**.
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. (Optional) You can edit some of the 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 attachment, choose **Edit attachment**. The **Attachments** page displays a confirmation that the attachment was modified successfully.

Shared AWS Cloud WAN 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 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 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 `list-core-networks` API to view information about the core networks you own. See list-core-networks.
- Run the APIs that create, view, and delete attachments:

> **Note**
>
> A shared core network supports only VPC and transit gateway route table attachments.

  - Create a VPC attachment: create-vpc-attachment
  - Get a VPC attachment: get-vpc-attachment
  - Delete a VPC attachment: delete-vpc-attachment
  - Create a transit gateway route table attachment: create-transit-gateway-route-table-attachment
  - Get a transit gateway route table attachment: get-transit-gateway-route-table-attachment
  - Delete a transit gateway route table attachment: delete-attachment
  - Create a Direct Connect gateway attachment: create-direct-connect-gateway-attachment
  - Get a Direct Connect gateway attachment: get-direct-connect-gateway-attachment
  - Update a Direct Connect gateway attachment: update-direct-connect-gateway-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, transit gateway route table attachments, and Direct Connect gateway 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.

Topics

Share an AWS Cloud WAN core network

The following steps guide you through sharing your core network with other AWS accounts or across your organizations.

To share a core network

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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**.

Stop sharing an AWS Cloud WAN core network

The following steps guide you through stopping sharing of your core network with other AWS accounts or across your organizations.

To stop sharing a core network share

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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**.

Shared peerings in AWS Cloud WAN

Shared peering allows you to establish peering connections between your Cloud WAN core network and transit gateways in the same AWS Region. You can dynamically exchange routing and reachability information between your core network edge and transit gateway over these peering connections, and interconnect your existing transit gateway-based network with your Cloud WAN network. You can create a new transity gateway policy table for this new shared peering or you can choose an existing transit gatewa policy table to use.

When a core network owner shares their core network with your account, you are then able to create new peerings for the shared core network, delete existing peerings, or manage the tags associated with a peering. When you create a shared peering you can choose the core network that you want to associate the peering with, the edge location, and any transit gateways you want to share in this peering. In addition, you can also choose whether to create a new policy table for the shared peering or to use an existing policy table. If you choose an existing table, you'll be prompted to supply the transit gateway policy table to use.

Topics

- Create a shared peering in an AWS Cloud WAN global network
- Delete a shared peering from an AWS Cloud WAN global network
- Edit shared peering tags in an AWS Cloud WAN global network

Create a shared peering in an AWS Cloud WAN global network

The following steps guide you through creating a shared peering in your core network.

> **Important**
>
> Before creating a peering, make sure that the account you use to create the peering has the following permissions:
>
> - `ec2:CreateTransitGatewayPolicyTable`
> - `ec2:AcceptTransitGatewayPeering`
> - `ec2:AssociateTransitGatewayPolicyTable`

To create a shared peering

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, under **Shared by me**, choose **Peerings**.
5. Choose **Create peering**.
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 that is where you want to create the peering.
8. From the **Edge location** dropdown list, choose the location where the attachment is located.
9. In the **Transit gateway** section, choose the transit gateway used for the peering.
10. Choose one of the following **Associate policy table** options:

    - **New** — Creates a new policy routing table.

- **Existing** — Allows you to associate this peering with an existing policy route table. If you choose this option, choose an existing **Transit gateway policy table** from the dropdown list to associate with the peering.

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

Delete a shared peering from an AWS Cloud WAN global network

Delete a transit gateway peering.

To delete a shared peering

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, under **Shared by me**, choose **Peerings**.
5. Choose the **Peering ID** of the peer that you want to delete.
6. Choose **Delete**.
7. In the confirmation box, choose **Delete**.

   The **Peering** page displays a confirmation that you deleted the transit gateway peering.

Edit shared peering tags in an AWS Cloud WAN global network

Edit the tags associated with a shared transit gateway peering.

To edit shared peering tags

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, under **Shared by me**, choose **Peerings**.

5. Choose the **Peering ID** of the peer that you want to add or modify tags for.
6. In the **Peering name** section, choose the **Tags** tab.
7. Choose **Edit tags**.
8. Do any of the following:

   - To add a new tag, choose **Add tag**, then add a new **Key** and **Value**.
   - To remove an existing tag, choose **Remove tag** for the tag that you want to delete.
   - To edit an existing tag, change the **Key** or **Value** text as needed.
9. Choose **Edit tags**.

Sites and links in AWS Cloud WAN

After you've added any devices to your global network, you can create a Cloud WAN site and associate any of your devices with that particular site using a link. For information on adding devices, see the section called “Devices”.

Sites

A site represents the physical location of your network, using location information such as latitude, longitude, and address. You can have multiple sites for each of your network locations. Sites are useful when viewing the global network dashboard, which provides you the geographical location of these sites based on location information you provided. Once you create a site you can view the devices associated with the site and create links between devices and sites. You can also view any VPNs associated with the site as well as monitor CloudWatch metrics for this site.

Links

A link represents the connection between a device and a site. Once you've added a device and created a site, you can create an association between the device and a site.

Topics

- Create a link for a site in an AWS Cloud WAN global network
- Edit a device link in an AWS Cloud WAN global network
- Delete a link from an AWS Cloud WAN global network

Create a site in an AWS Cloud WAN global network

A site represents the physical location of your network, using location information that you provide. Sites you add to your Cloud WAN global network appear in the geographical map of a Cloud WAN global network dashboard.

To create a site

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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**.

    Sites are created immediately and can be viewed on the global network dashboard. For more information on viewing sites on your global network dashboard, see the section called “Access global network dashboards”.

View site details in an AWS Cloud WAN global network

View details about a Cloud WAN global network site.

To view details about a site

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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”.
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 “Create a link”.
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 a site in an AWS Cloud WAN global network

You can edit any of an existing site's details as needed, including adding, editing, and removing tags.

To create a site

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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:
   - **Description**
   - **Address**
   - **Latitude**
   - **Longitude**
   - **Tags**
7. Choose **Edit site**.

Delete a site from an AWS Cloud WAN global network

Delete sites from your Cloud WAN global network that are no longer a valid or needed.

To delete a site

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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 want to delete, and then choose **Delete**.
6. Confirm that you want to delete the site by choosing **Delete** again.

Create a link for a site in an AWS Cloud WAN global network

Create a link that can be used to associate a device with a site.

To add a link

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Sites**.
5. Choose the link for the site **ID** 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. Choose the **Links** tab, and then 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 further identify this link.
13. Choose **Create link**.

Edit a device link in an AWS Cloud WAN global network

Edit the link between two devices in your Cloud WAN global network.

To update a link

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

2. Under **Connectivity**, choose **Global Networks**.
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**.

Delete a link from an AWS Cloud WAN global network

You can delete the link between two devices without deleting the devices.

To delete a link

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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.

Transit gateways in AWS Cloud WAN

You can choose from a list of and register the transit gateways you want to monitor for the chosen global network. You can select transit gateways from any AWS Regions. If multi-account is enabled you'll be able to choose transit gateways from each account shared with you. A transit gateway can only be registered to one global network.

Once registered, you can view details about that registered transit gateway on the Transit gateway dashboard. If you've registered multiple transit gateways in your global network, you can view

- For information about viewing the dashboard for a single transit gateway in your global network, see the section called "Access transit gateway dashboards".
- For information about viewing all transit gateways in your global network, see the section called "Access transit gateway network dashboards".

Topics

Register a transit gateway in an AWS Cloud WAN global network

Prerequisite: A transit gateway must first be created on the Amazon Virtual Private Cloud console at https://console.aws.amazon.com/vpc/home. For the steps to create a transit gateway, see Working with transit gateways in the *Amazon VPC Transit Gateways Guide*

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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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**.

AWS Cloud WAN global and core network dashboards

AWS Cloud WAN provides two dashboards, a global network dashboard and a core network dashboard. Each dashboard is composed sub-dashboards that allow you to view details about your global and core networks.

Cloud WAN global network dashboards

The AWS Cloud WAN console uses dashboard visualizations to help you view and monitor all aspects of your global and core networks. The following list describes just a few of the things you can do with Cloud WAN global network dashboards:

- View world maps that pinpoint where your network resources are located, including edge locations, devices, and attachments,
- Monitor data using CloudWatch Events to track 15-months' worth of statistics, giving you a better perspective on how your networks are performing.
- Track real-time global network events.
- View topological and logical diagrams of your global network topology.
- View network routes and sharing.

For the steps to access and use the Cloud WAN global network dashboards, see the section called “Access global network dashboards”.

Cloud WAN core network dashboards

The AWS Cloud WAN console provides a dashboard where you can visualize and monitor your core network. It includes information about the resources in your core network, including geographic locations and edge locations, You can also view and monitor CloudWatch metrics. The following topics describe the different core network dashboards on the Network Manager console. T he following list describes just a few of the things you can do with Cloud WAN global network dashboards:

- View world maps that pinpoint where your core network edge locations, segments, devices, sites, or network function groups are located.

- Viewing shared network resources.
- Topological graphs and trees displaying your core network topology.
- Track real-time core network events.
- Set monitor alarms on core network metrics using Amazon CloudWatch.

For the steps to use the Cloud WAN core network dashboards see the section called "Access core network dashboards".

Access AWS Cloud WAN global network dashboards

Visualize and monitor your global networks in the Network Manager console through a graphical representation of your global network topology, including a map showing the locations of transit gateways, edge locations, devices, and sites.

Use the following dashboards to view information about your Cloud WAN global network. For more information about the Cloud WAN core network dashboards, see the section called "Cloud WAN global network dashboards".

Global network dashboards

- Overview
- Details
- Topology graph
- Topology tree

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
Edge locations 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.
Transit gateways 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.
Devices 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.
Sites 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.

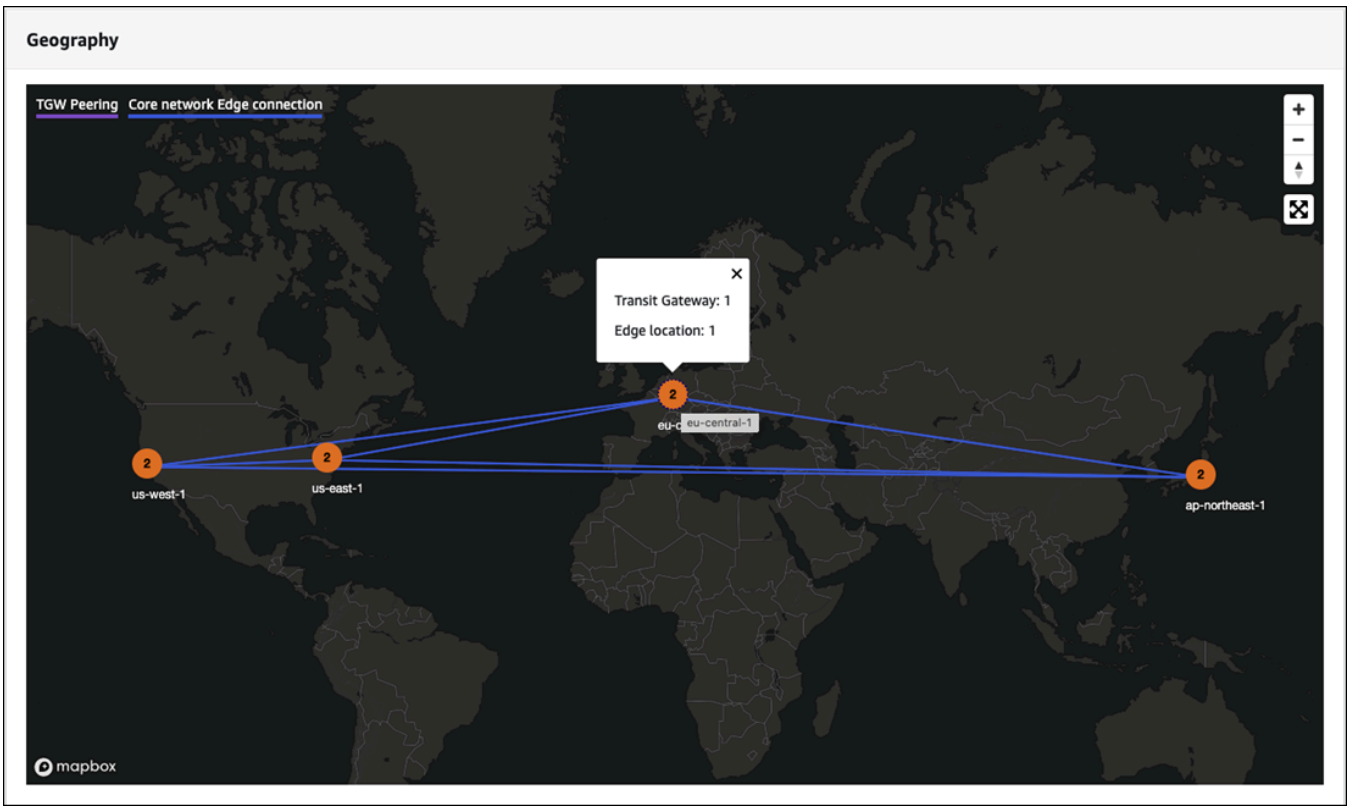
To access your global network resource inventory list

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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

Description
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.
VPN The VPNs in your global network.
Direct Connect Gateway The Direct Connect Gateways in your global network.
Regions The Regions in your global network.

To access the topology graph for a global network

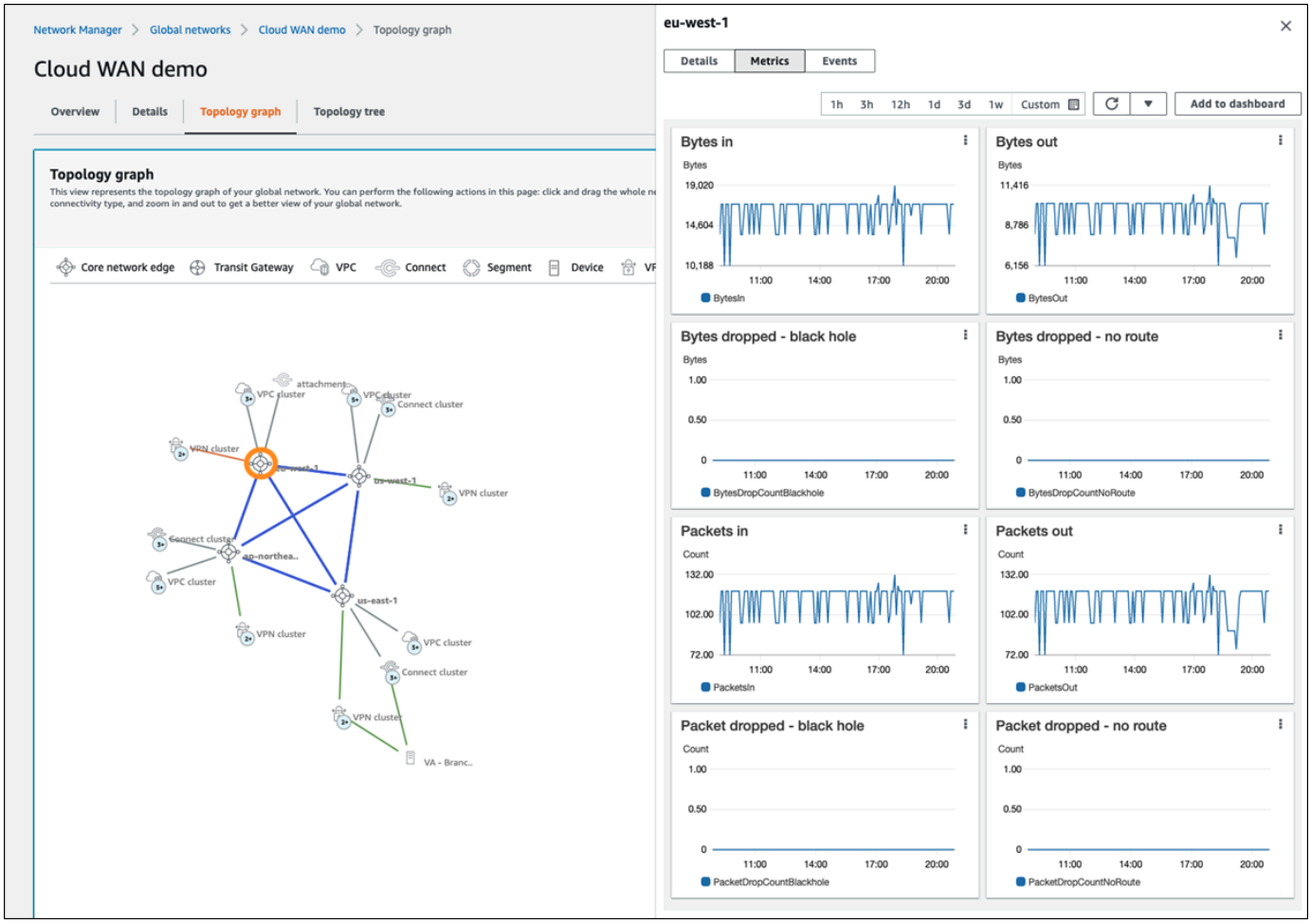
1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.

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* for more information about the types of events that can be tracked.
- **Transit gateway** — **Transit gateway details**.
- **VPC**, **Connect**, **VPC**, **VPN**, and **Direct Connect Gateway** — **Attachment details**.
- **Segment** — **Segment details** and **Routes**.
- **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.

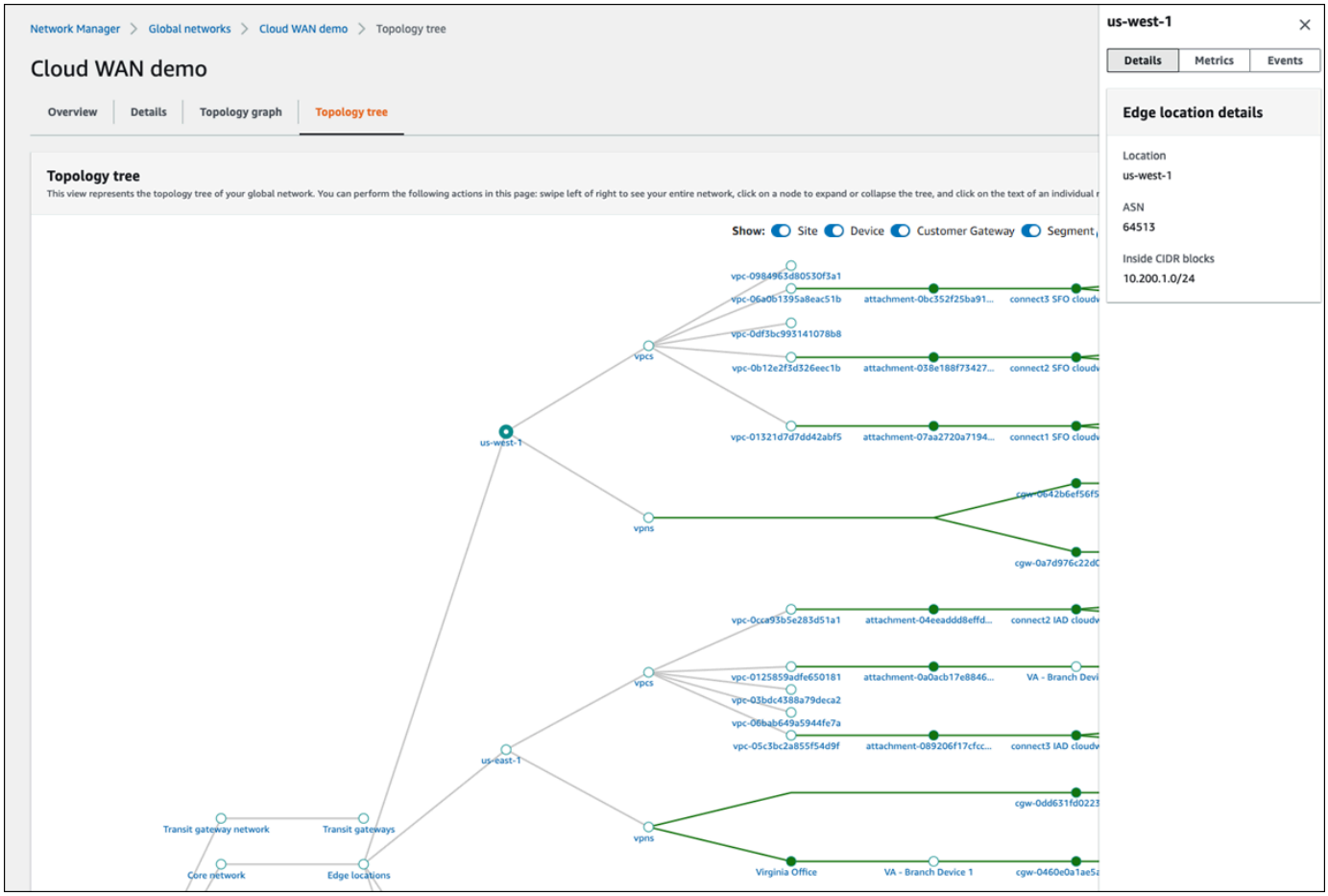
To access the topology tree for a global network

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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.
   - **Segment** — Turns the display of segments 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 location** — **Details**, **Metrics**, and **Events**. See *Events and metrics* for more information about the types of events that can be tracked.
- **VPC**, **Connect**, **VPC**, **VPN**, and **Direct Connect Gateway** attachments — **Attachment details** and **Events**.
- **Transit Gateways** — **Transit Gateway details**.
- **Device** — **Device details**.
- **Sites** — **Site details**.

Access Cloud WAN core network dashboards

Use the following dashboards to view information about your Cloud WAN core network. For more information about the Cloud WAN core network dashboards, see the section called “Cloud WAN core network dashboards”.

Core network dashboards

- Overview
- Details
- Sharing
- Topology graph
- Topology tree
- Logical
- Routes
- Events
- Monitoring

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.
- The number of network function groups used to route specific traffic to security appliances.

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

Description
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.
Network function groups The total number of network function groups 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/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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 “Shared core network” 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.
Direct Connect Gateway The Direct Connect Gateway attachments in your core network.

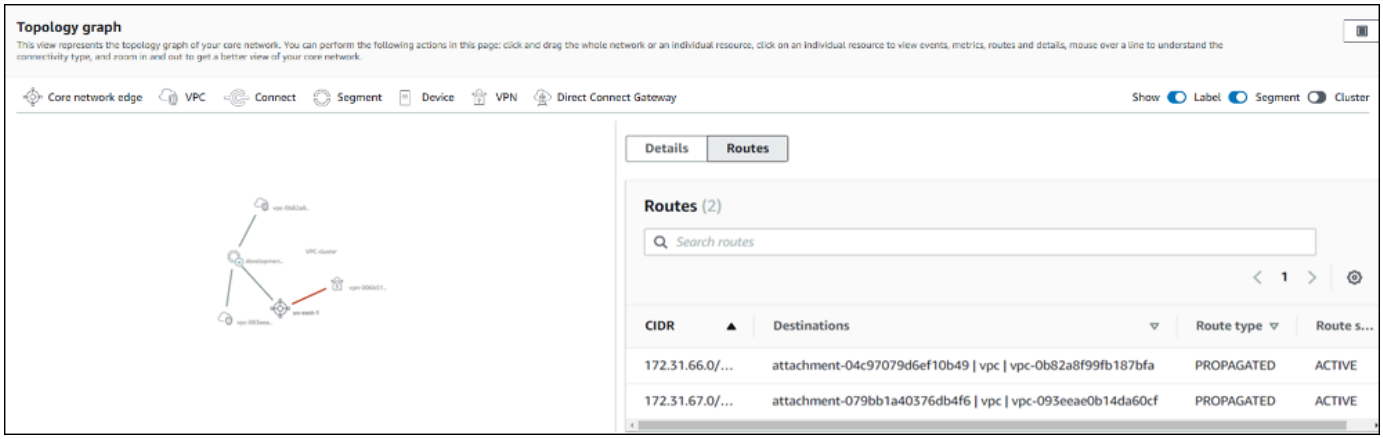
To view the core network topology graph

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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 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* for more information about the types of metrics and events that can be tracked.
- **VPC**, **Connect**, **VPN**, and **Direct Connect Gateway** — **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/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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.

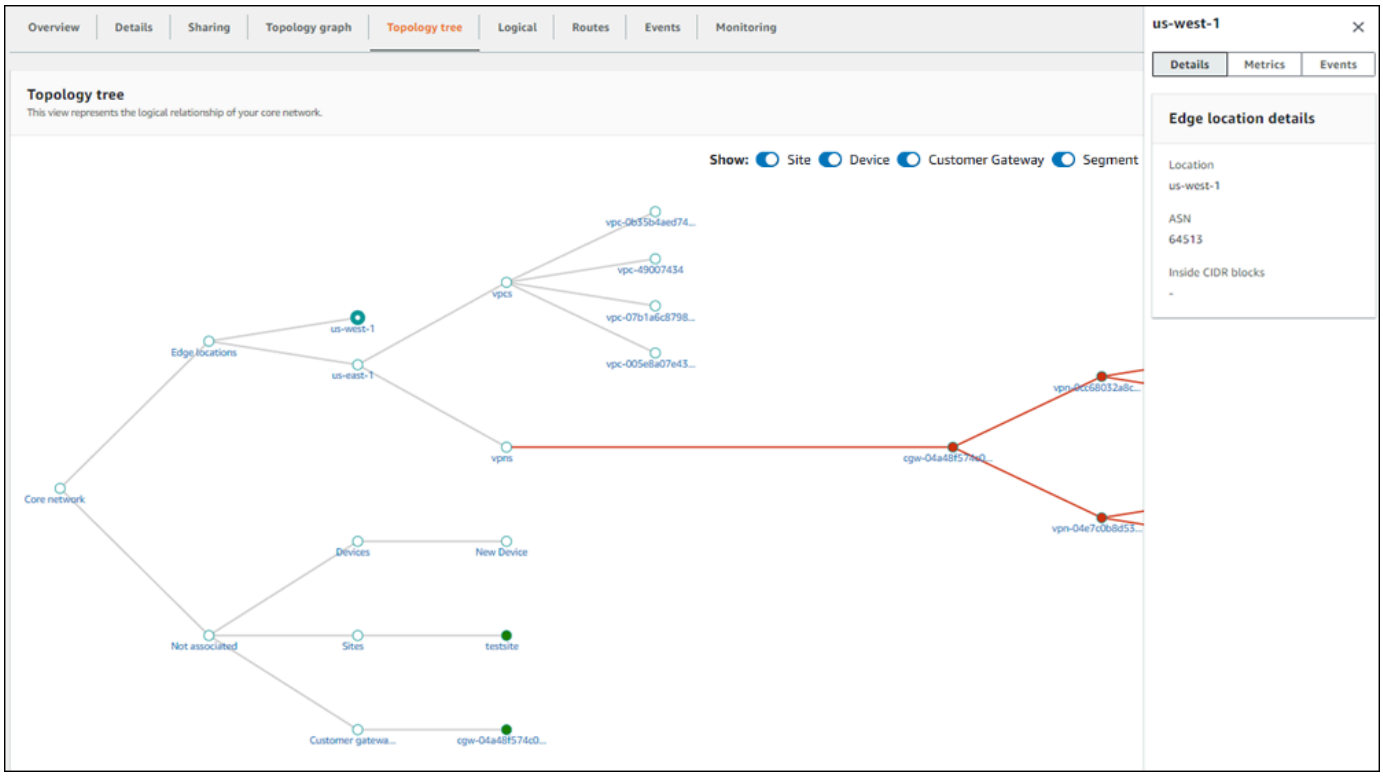
   A logical representation of your global network is displayed, along with the details of your global network configuration.

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.
   - **Segment** — Turns the display of segments 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. See *Events and metrics* for more information about the types of events that can be tracked.

- **Core network** - Core network details, including the **AWS account** and current **State** of the core network.
- **Sites** — **Details** and **Events**.
- **Devices** — **Details** and **Events**.
- **Customer Gateway** — **Details** and **Events**.
- **Segment** — **Details** and **Events**.
- **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
VPC The VPC attachments in your core network.
Connect The Connect attachments in your core network.
Segment The segments in your core network.
Network function group

Description
The network function groups in your core network.
VPN The VPN attachments in your core network.
Transit gateway route table The transit gateway route table attachments in your core network.
Direct Connect gateway attachment The Direct Connect gateway attachments in your core network.

To access the logical diagram for a core network

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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.

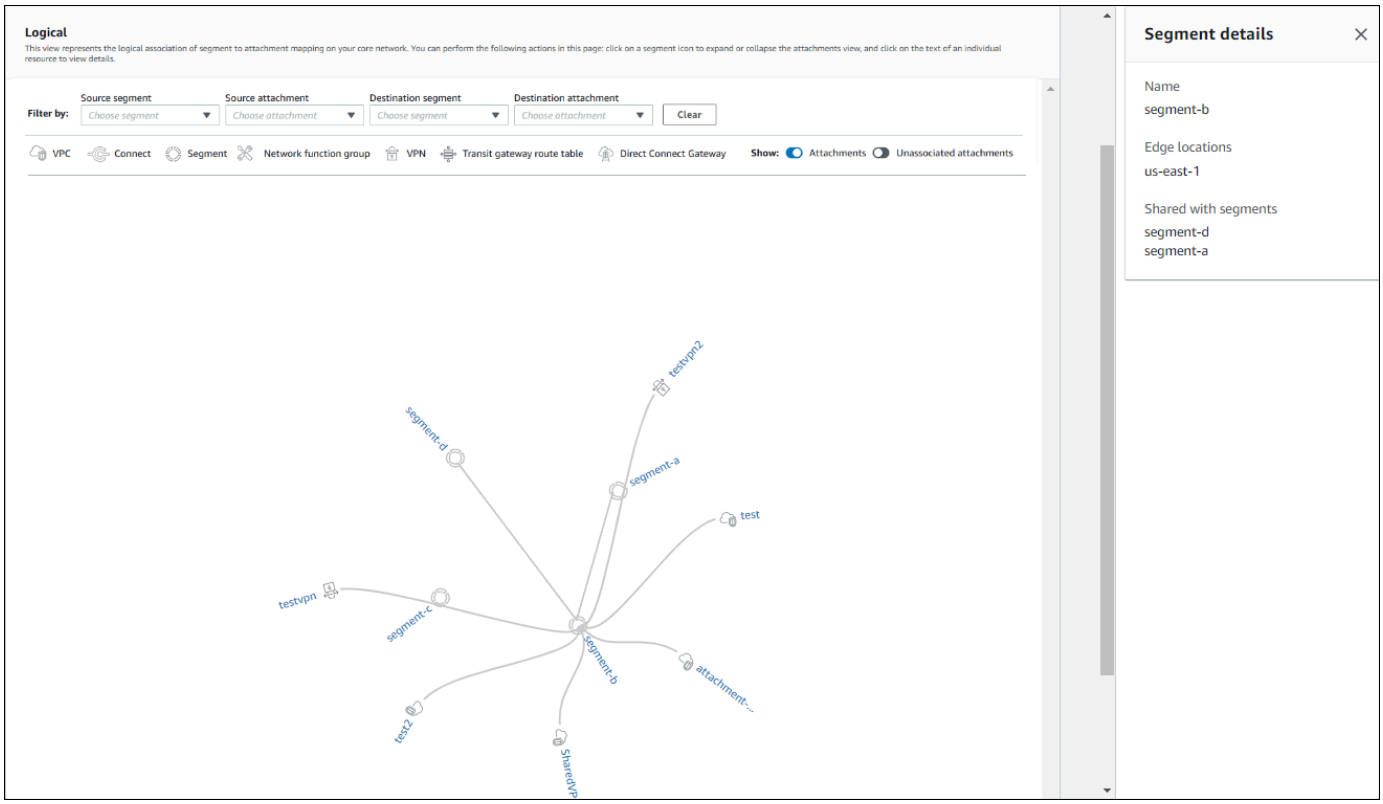
The logical graph updates based on your choices. Choose **Clear** to reset the page.

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**, **VPN**, **Transit gateway route table,** and **Direct Connect Gateway** — Attachment **Details** and **Events**. See *Events and metrics* for more information about the types of events that can be tracked.
   - **Segment** — **Segment details** and **Routes**.

- **Network function groups** — **Edge locations** and **Send to/Send via**.

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/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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, choose one of the following:

   - Chose **Segment**, and then from the **Segment** and **Edge** location drop-down lists, choose the segment and edge location.
   - Choose **Network function group**, and then from the **Network function group** and **Edge location** drop-down lists, choose the network function group and edge location that you want to create a route filter for.
8. Choose **Search routes**.

   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 Amazon EventBridge, 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, see the Amazon EventBridge User Guide.

Prerequisites: Before monitoring events, you must 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*.

To access core network events

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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 EventBridge 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 Amazon CloudWatch Events".

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 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/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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** 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**

AWS Cloud WAN transit gateway network and transit gateways dashboards

Cloud WAN transit gateway network dashboards

Use the transit gateway network dashboard to view details about all transit gateways in your global network. Some of the dashboards include:

- View a geographical map that pinpoints where your transit gateway resources, such as VPNs, VPCs, sites, and devices are located.
- View VPN and Connect peer status.
- Monitor data using CloudWatch Events to track 15-months' worth of statistics, giving you a better perspective on how your transit gateways are performing.
- Track real-time transit gateway network events.
- View topological diagrams of your transit gateways including sites, devices and gateways.

For the steps to access and use the Cloud WAN transit gateway networks dashboards, see the section called “Access transit gateway network dashboards”.

Cloud WAN transit gateway dashboards

Use the transit gateway dashboard to view details about the transit gateways in your global network. Some of the dashboards include:

- View attachment details, including VPNs and Connect peers, as well as network events.
- View onn-premises and Connect peer associations.
- Track real-time transit gateway events.
- View a topological diagram of your transit gateways.

For the steps to access and use the Cloud WAN transit gateway dashboards, see the section called “Access transit gateway dashboards”.

Access AWS Cloud WAN transit gateway network dashboards

View dashboard information about transit gateways registered registered in your AWS Cloud WAN global network. For more information about the Cloud WAN transit gateway dashboards see the section called “Cloud WAN transit gateway network dashboards”.

Transit gateway networks dashboards

- Overview
- Geography
- Topology tree
- Events
- Monitoring
- Route analyzer

Overview

The **Overview** page displays details about your Cloud WAN transit gateways, VPN and 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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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

Description
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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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 Amazon EventBridge, 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, see the Amazon EventBridge User Guide.

To track transit gateway events

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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 transit gateway 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 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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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.

Access AWS Cloud WAN transit gateway dashboards

View dashboard information about transit gateways registered in your AWS Cloud WAN global network. For more information about the Cloud WAN transit gateway dashboards see the section called “Cloud WAN transit gateway dashboards”.

Transit gateway dashboards

- Overview
- Topology tree
- Events
- Monitoring
- On-premises associations
- Connect peer

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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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
VPC The total number of VPCs attached to your transit gateway.
VPN The total number of VPNs attached to your transit gateway.
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 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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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 resources 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 Amazon EventBridge, 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, see the Amazon EventBridge User Guide.

To track transit gateway events

1. Access the Network Manager console at https://console.aws.amazon.com/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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 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 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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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**.

Authentication and access in AWS Cloud WAN

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-lined role, see AWS Global Networks for Transit Gateways service-linked roles.

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 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 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 How Network Manager works with IAM.

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 Condition keys.
- For example policies to manage, see Example policies to manage.

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 Identify 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.

AWS managed policies for AWS Cloud WAN

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the `ReadOnlyAccess` AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the *IAM User Guide*.

AWS managed policy: AWSNetworkManagerCloudWANServiceRolePolicy

You can attach the `AWSNetworkManagerCloudWANServiceRolePolicy` policy to your IAM identities. This policy allows AWS Network Manager to access resources associated with Cloud WAN. For more information, see the section called "Service-linked roles".

To view the permissions for this policy, see AWSNetworkManagerCloudWANServiceRolePolicy in the *AWS Managed Policy Reference*.

AWS managed policy: AWSNetworkManagerServiceRolePolicy

This policy is attached to the service-linked role named `AWSServiceRoleForNetworkManager` to allow AWS Cloud WAN to call API actions on your behalf when you work with global networks. For more information, see the section called "Service-linked roles".

To view the permissions for this policy, see AWSNetworkManagerServiceRolePolicy in the *AWS Managed Policy Reference*.

Cloud WAN updates to AWS managed policies

View details about updates to AWS managed policies for AWS Cloud WAN since this service began tracking these changes in July 2022.

Change	Description	Date
AWSNetworkManagerCloudWANServiceRolePolicy - New policy.	Added a policy to allow Network Manager to access resources associated with your core network.	July 12, 2022
AWSNetworkManagerServiceRolePolicy - New policy.	Added a policy to allow Network Manager to access	December 3, 2019

Change	Description	Date
	resources associated with your global networks.	

AWS Cloud WAN service-linked roles

AWS Cloud WAN uses the following service-linked roles for the permissions that it requires to call other AWS services on your behalf:

- AWSServiceRoleForNetworkManagerCloudWAN
- AWSServiceRoleForVPCTransitGateway
- AWSServiceRoleForNetworkManager

AWSServiceRoleForNetworkManagerCloudWAN

AWS Cloud WAN uses the service-linked role named AWSServiceRoleForNetworkManagerCloudWAN to create and announce transit gateway route tables, and then propagates transit gateway routes to those tables.

The AWSServiceRoleForNetworkManagerCloudWAN service-linked role trusts the following service to assume the role:

- `networkmanager.amazonaws.com`

This service-linked role uses the managed policy AWSNetworkManagerCloudWANServiceRolePolicy. To view the permissions for this policy, see AWSNetworkManagerCloudWANServiceRolePolicy in the *AWS Managed Policy Reference*.

AWSServiceRoleForVPCTransitGateway

Amazon VPC uses the service-linked role named AWSServiceRoleForVPCTransitGateway to create and manage resources for your transit gateway on your behalf.

The AWSServiceRoleForVPCTransitGateway service-linked role trusts the following service to assume the role:

- `transitgateway.amazonaws.com`

This service-linked role uses the managed policy AWSVPCTransitGatewayServiceRolePolicy. To view the permissions for this policy, see AWSVPCTransitGatewayServiceRolePolicy in the *AWS Managed Policy Reference*.

AWSServiceRoleForNetworkManager

AWS Cloud WAN uses the service-linked role named AWSServiceRoleForNetworkManager to call actions on your behalf when you work with global networks.

The AWSServiceRoleForNetworkManager service-linked role trusts the following service to assume the role:

- `networkmanager.amazonaws.com`

This service-linked role uses the managed policy AWSNetworkManagerServiceRolePolicy. To view the permissions for this policy, see AWSNetworkManagerServiceRolePolicy in the *AWS Managed Policy Reference*.

Create the service-linked role

You don't need to manually create these service-linked roles.

- Network Manager creates the AWSServiceRoleForNetworkManager role when you create your first global network.
- Amazon VPC creates the AWSServiceRoleForVPCTransitGateway role when you attach a VPC to a transit gateway in your account.

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

Edit the service-linked role

You can edit the descriptions of the AWSServiceRoleForNetworkManager and AWSServiceRoleForVPCTransitGateway roles using IAM. For more information, see Edit a service-linked role description in the *IAM User Guide*.

Delete the service-linked role

If you no longer need to use Network Manager, we recommend that you delete the AWSServiceRoleForNetworkManager and AWSServiceRoleForVPCTransitGateway roles.

You can delete these service-linked roles only after you delete your global network. For information about deleting your global network, see Delete a global network.

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

After you delete AWSServiceRoleForNetworkManager, Network Manager will create the role again when you create a new global network. After you delete AWSServiceRoleForVPCTransitGateway, Amazon VPC will create the role again when you attach a VPC to a transit gateway in your account.

Supported Regions

Service-linked roles are supported in all the AWS Regions where the service is available. For more information, see the section called “Region availability”.

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 EventBridge* delivers a near-real-time stream of system events that describe changes in AWS resources. EventBridge 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 EventBridge 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” for the onboarding steps.

Topics

CloudWatch metrics in AWS Cloud WAN

You can use the following features to monitor your Cloud WAN network, analyze traffic patterns, and troubleshoot issues with your Cloud WAN global network.

Cloud WAN metrics and dimensions

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

Amazon VPC measures and sends its metrics to CloudWatch in 60-second intervals.

For more information, see the Amazon CloudWatch User Guide.

The AWS/NetworkManager namespace includes the following metrics. All metrics are always reported.

Metric	Description
BytesDropCountBlackhole	The number of bytes dropped because they matched a blackhole route. **Statistics**: The only meaningful statistic is Sum.
BytesDropCountNoRoute	The number of bytes dropped because they did not match a route. **Statistics**: The only meaningful statistic is Sum.
BytesIn	The number of bytes received by the core network. **Statistics**: The only meaningful statistic is Sum.
BytesOut	The number of bytes sent from the core network. **Statistics**: The only meaningful statistic is Sum.
PacketsIn	The number of packets received by the core network. **Statistics**: The only meaningful statistic is Sum.
PacketsOut	The number of packets sent by the core network. **Statistics**: The only meaningful statistic is Sum.
PacketDropCountBlackhole	The number of packets dropped because they matched a blackhole route. **Statistics**: The only meaningful statistic is Sum.
PacketDropCountNoRoute	The number of packets dropped because they did not match a route. **Statistics**: The only meaningful statistic is Sum.

Metric	Description
PacketDropTTLExpired	The number of packets dropped because the TTL expired. **Statistics**: The only meaningful statistic is Sum.

Cloud WAN metric dimensions

Filter metric data by a combination of the following Cloud WAN core network metric dimensions.

Dimension	Description
CoreNetwork , EdgeLocation	Filters the metric data by core network.
Attachment , CoreNetwork	Filters the metric data by core network attachment.
AvailabilityZone , CoreNetwork , EdgeLocation	Filters the metric data by availability zone. This is only applicable for Direct Connect.
Attachment , AvailabilityZone , CoreNetwork	Filters the metric data by both core network attachment and availability zone.

AWS Cloud WAN usage metrics

Cloud WAN usage metrics correspond to AWS service quotas for Cloud WAN. You can configure alarms that alert you when your usage approaches a service quota. For more information about CloudWatch integration with service quotas, see CloudWatch usage metrics in the *Amazon CloudWatch User Guide*.

The AWS/Usage namespace reports the following metric for Cloud WAN:

Metric	Description
ResourceCount	The number of the specified resources running in your account. The resources are defined by the dimensions associated with the metric. **Statistics**: The only meaningful statistic is MAXIMUM.

AWS Cloud WAN metric dimensions

The following dimensions are used to refine the usage metrics that are published by Cloud WAN.

Dimension	Description
Service	The name of the AWS service containing the resource. For Cloud WAN usage metrics, the value for this dimension is NetworkManager .
Type	The type of entity that is being reported. Currently, the only valid value for Cloud WAN usage metrics is Resource.
Resource	The type of resource that is running. Currently, valid values for Cloud WAN usage metrics include RoutesPropagated/Inbound and RoutesPropagated/Outbound , which return the number of routes advertised and learnt over Direct Connect attachments.
ResourceID	The unique identifier for the resource, such as a core network attachmentId, and might include a region code prefix for region-specific resources.
Class	This dimension is reserved for future use.

Onboard CloudWatch Logs Insights for AWS Cloud WAN

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 (user) in your account has the appropriate permissions to onboard to CloudWatch Logs Insights. Ensure that the IAM policy contains the following permissions.

JSON

```
{
    "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/networkmanager/home/.
2. Under **Connectivity**, choose **Global networks**.
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:

- An EventBridge rule with the name `DON_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.
- An EventBridge rule is configured with the CloudWatch Logs group as a target.
- A 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 Amazon CloudWatch Events

You can monitor your core network using Amazon EventBridge, 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 EventBridge User Guide.

The following events can be sent to EventBridge:

- the section called “Topology changes”
- the section called “Route changes”
- the section called “Status updates”
- the section called “Policy updates”
- the section called “Segment update events”
- the section called “Network function group update events”

Topology changes

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

- An Edge location has been added to the Core Network.

- An edge location has been deleted from the Core Network.
- A Site-to-Site VPN attachment has been created for a Core Network.
- A Site-to-Site VPN attachment has been deleted for a Core Network.
- A VPC attachment has been created for a Core Network.
- A VPC attachment has been deleted for a Core Network.
- A Site-to-Site VPN attachment has been created for a Core Network.
- A Site-to-Site VPN attachment has been deleted for a Core Network.
- A Connect attachment has been created for a Core Network.
- A Connect attachment has been deleted for a Core Network.
- A Connect peer attachment has been created for a Core Network.
- A Connect peer attachment has been deleted for a Core Network.
- A Direct Connect Gateway attachment has been created for a Core Network.
- A Direct Connect Gateway attachment has been deleted for a Core Network.
- A Direct Connect Gateway attachment has been updated for a Core Network.

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

```
{
  "version": "0",
  "id": "13143a7e-806e-a904-300b-ef874c56eaac",
  "detail-type": "Network Manager Topology Change",
  "source": "aws.networkmanager",
  "account": "111122223333",
  "time": "2021-09-02T12:00:38Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:networkmanager::111122223333:global-network/global-
network-021345abcdef6789",
    "arn:aws:networkmanager::111122223333:core-network/core-network-abcdef01234567890"

  ],
  "detail": {
    "changeType": "VPC-ATTACHMENT-DELETED",
    "changeDescription": "A VPC attachment has been deleted from a Core Network.",
    "edgeLocation": "us-east-2",
```

```
    "attachmentArn": "arn:aws:networkmanager::111122223333:attachment/
attachment-1234567890abcdef0",
    "vpcArn": "arn:aws:ec2:us-east-2:212869205455:vpc/vpc-049a3a24f48fcc47d",
    "coreNetworkArn": "arn:aws:networkmanager::111122223333:core-network/core-network-
abcdef01234567890"
  }
}
```

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": "111122223333",
   "time": "2021-09-02T12:00:38Z",
   "region": "us-west-2",
   "resources": [
     "arn:aws:networkmanager::111122223333:global-network/global-
network-021345abcdef6789",
     "arn:aws:networkmanager::111122223333:core-network/core-network-
abcdef01234567890"
   ],
   "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": "attachment1234567890abcdef0",
             "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::111122223333:core-network/core-network-
abcdef01234567890"
   }
 }
}
```

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": "111122223333",
   "time": "2021-09-02T12:00:38Z",
   "region": "us-west-2",
   "resources": [
     "arn:aws:networkmanager::111122223333:global-network/global-
network-021345abcdef6789",
     "arn:aws:networkmanager::111122223333:core-network/core-network-
abcdef01234567890"
   ],
   "detail": {
     "changeType": "VPN-CONNECTION-IPSEC-UP",
     "changeDescription": "IPsec for a VPN connection has come up.",
     "region": "us-west-2",
     "attachmentArn": "arn:aws:networkmanager::111122223333:attachment/
attachment-1234567890abcdef0",
     "outsideIpAddress": "35.161.41.136",
     "coreNetworkArn": "arn:aws:networkmanager::111122223333:core-network/core-network-
abcdef01234567890"
   }
 }
```

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": "111122223333",
   "time": "2021-09-02T12:00:38Z",
```

```
   "region": "us-west-2",
   "resources": [
     "arn:aws:networkmanager::111122223333:global-network/global-
network-1234567890abcdef0",
     "arn:aws:networkmanager::111122223333:core-network/core-network-
abcdef01234567890"
   ],
   "detail": {
     "changeType": "CHANGE-SET-EXECUTED",
     "changeDescription": "A change-set has been sucessfully executed for a Core
 Network policy.",
     "policyVersionId":"1",
     "coreNetworkArn": "arn:aws:networkmanager::111122223333:core-network/core-network-
abcdef01234567890"
   }
 }
```

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": "111122223333",
   "time": "2021-09-02T12:00:38Z",
   "region": "us-west-2",
   "resources": [
     "arn:aws:networkmanager::111122223333:global-network/global-
network-021345abcdef6789",
```

```
     "arn:aws:networkmanager::111122223333:core-network/core-network-
abcdef01234567890"
   ],
   "detail": {
     "changeType": "ATTACHMENT-ASSOCIATION-MODIFIED",
     "changeDescription": "An attachment has been mapped to a different Segment.",
     "attachmentArn": "arn:aws:networkmanager::111122223333:attachment/
attachment-1234567890abcdef0",
     "previousSegmentName": "development",
     "segmentName": "production",
     "edgeLocation": "us-west-2",
     "coreNetworkArn": "arn:aws:networkmanager::111122223333:core-network/core-network-
abcdef01234567890"
   }
 }
```

Network function group update events

A network function group event occurs when any of the following changes occur:

- An attachment was associated with a different network function group.
- An attachment was mapped to a different network function group
- An attachment was disassociated from a network function group.

The following example shows a network function group update event where an attachment is associated with a different network function group.

```
{
   "version": "0",
   "id": "13143a7e-806e-a904-300b-ef874c56eaac",
   "detail-type": "Network Function Group Update",
   "source": "aws.networkmanager",
   "account": "111122223333",
   "time": "2024-06-12T12:00:00Z",
   "region": "us-west-2",
   "resources": [
     "arn:aws:networkmanager::111122223333:global-network/global-
network-021345abcdef6789",
     "arn:aws:networkmanager::111122223333:core-network/core-network-
abcdef01234567890",
     "arn:aws:networkmanager::111122223333:attachment/attachment-1234567890abcdef0"
```

```
   ],
   "detail": {
     "changeType": "ATTACHMENT_MODIFIED",
     "changeDescription": "An attachment is disassociated from network function group
 and associated with a new function group.",
     "attachmentArn": "arn:aws:networkmanager::111122223333:attachment/
attachment-1234567890abcdef0",
     "previousNetworkFunctionGroupName": "development",
     "newNetworkFunctionGroupName": "production",
     "edgeLocation": "us-west-2",
     "coreNetworkArn": "arn:aws:networkmanager::111122223333:core-network/core-network-
abcdef01234567890"
   }
 }
```

Monitor AWS Cloud WAN with Amazon CloudWatch Events metrics

You can monitor your core network and core network attachments using Amazon CloudWatch under the `AWS/NetworkManager` namespace, 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.

Note

CloudWatch metrics in the `AWS/NetworkManager` namespace are available only in the following Regions:

- US West (Oregon) for all Regions except AWS GovCloud (US)
- AWS GovCloud (US-West) for AWS GovCloud (US-West) and AWS GovCloud (US-East)

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/networkmanager/home/.
2. Under **Connectivity**, choose **Global Networks**.
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 usage metrics for the specified edge location during the chosen time frame. For more information about these metrics, see the section called “Cloud WAN metrics”.

AWS Cloud WAN 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	40	No
Retention duration (in seconds) for core network policies with out-of-date change sets	7776000	Yes
Number of policy versions per core network	10,000	Yes
Size of a core network policy	1 MB	No
Number of policy versions	10000	Yes
Number of attachments per core network	5000	Yes

Quota	Default	Adjustable
Number of core network Connect attachments	No limit, up to 5000 maximum attachments per core network	No
Number of core network attachments per VPC	5	No
Number of Connect peers per Connect attachment	4	No
Number of Connect peers per Tunnel-less 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
Number of connections per global network	500	Yes
Number of transit gateway peers	50	Yes
Number of transit gateway routing tables	No limit	
Maximum number of core network attachments per Direct Connect gateway	1	No

Quota	Default	Adjustable
Maximum number of Direct Connect attachments per core network.	40	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
Bandwidth per VPC attachment per Availability Zone	Up to 100 Gbps	Contact your Solutions Architect (SA) or Technical Account Manager (TAM) for further assistance.
Packets per second per core network VPC attachment per Availability Zone	Up to 7,500,000	Contact your Solutions Architect (SA) or Technical Account Manager (TAM) for further assistance.
Maximum bandwidth per VPN tunnel	Up to 1.25 Gbps	No

Quota	Default	Adjustable
Maximum bandwidth per Connect peer (GRE tunnel) per Connect attachment	Up to 5 Gbps	No
Maximum bandwidth per Connect peer (Tunnel-less) per Connect attachment	Up to 100 Gbps per availability zone	Contact your Solutions Architect (SA) or Technical Account Manager (TAM) for further assistance.

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 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
Routes advertised from core network over Connect peer	5,000	No
Maximum number of Tunnel-less Connect routes	5,000 outbound 1,000 inbound	No

Quota	Default	Adjustable
Maximum number of outbound routes per Direct Connect gateway attachment Quotas applicable to Direct Connect resources (virtual interfaces and Direct Connect gateways) behave in the same way when used with a Cloud WAN core network. For more information, see see AWS Direct Connect quotas in the *AWS Direct Connect User Guide*.	5000	Yes

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, including transit gateway peering and Tunnel-less Connect VPC attachments. 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 enforces Maximum Segment Size (MSS) clamping for all packets. For more information, see RFC879.
- Cloud WAN supports Path MTU Discovery (PMTUD) for traffic ingressing on VPC attachments. Transit gateway generates the `FRAG_NEEDED` for ICMPv4 packets and `Packet Too Big (PTB)` for ICMPv6 packets. Cloud WAN does not support PMTUD on Connect, Site-to-site VPN, Direct Connect and Peering attachments. For more information about Path MTU Discovery, see Path MTU Discovery in the *Amazon VPC User Guide*

Document history for AWS Cloud WAN

The following table describes the releases for AWS Cloud WAN:

Change	Description	Date
Removed the table of supported Regions for Direct Connect Gateway attachments	Direct Connect Gateway attachments are now supported in all Cloud WAN Regions listed here Region Availability.	June 24, 2025
DNS and security group referencing support	Cloud WAN now supports DNS and security group referencing	June 11, 2025
Support for dual-stack IPv6 endpoints	AWS Cloud WAN now supports dual-stack IPv6 endpoints	March 25, 2025
PrivateLink support	PrivateLink support in the us-west-2 and us-gov-west-1 Regions	March 25, 2025
Updated supported regions	AWS Cloud WAN now supports the `ap-southeast-5` Region	March 13, 2025
Updated supported attachments	AWS Cloud WAN now supports Direct Connect attachment types	November 25, 2024
Updated supported regions.	AWS Cloud WAN now supports additional Regions	October 3, 2024
Added a new feature, Cloud WAN service insertion	AWS Cloud WAN now supports Service Insertion, a	June 11, 2024

	feature allowing you to route traffic to security appliances	
Added a new available Region	ap-southeast-3 Asia Pacific (Jakarta) Region is now an available Region for AWS Cloud WAN	March 26, 2024
Support added for appliance mode	VPC attachments now support appliance mode in AWS Cloud WAN	December 14, 2022
Official launch date	The official launch of AWS Cloud WAN	July 12, 2022