



# Transit GateWay

By: Salma Salah

Guidance & Support: Eng. Saad El-Kenawy

# Why Use AWS Transit Gateway



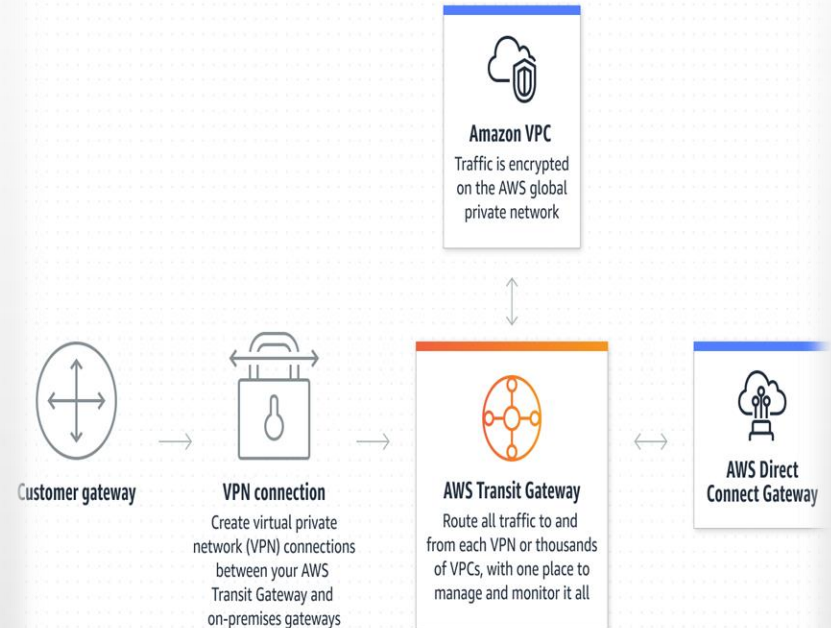
AWS Transit Gateway helps to design and implement networks at scale by acting as a cloud router.



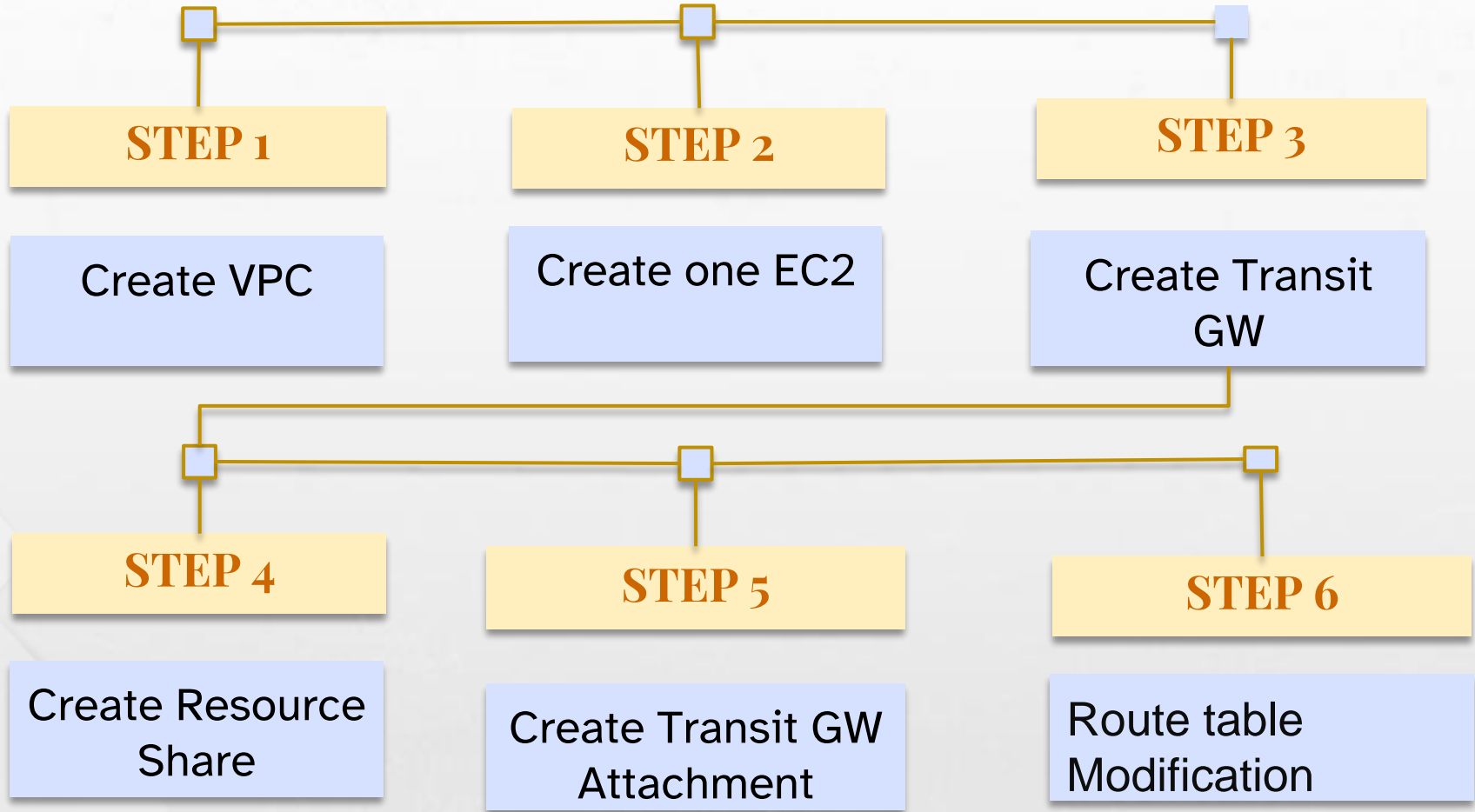
As the network grows, the complexity of managing incremental connections can slow the implementation down.



AWS Transit Gateway connects VPCs and on-premises networks through a central hub.



# Steps



# 1) Create a VPC

The screenshot shows the AWS Management Console interface for the 'Your VPCs' page. The top navigation bar includes the AWS logo, 'Services', a search bar, and the user's profile 'Salma\_Salah @ salma-salah'. The left sidebar lists various AWS services, with 'Virtual private cloud' expanded to show 'Your VPCs', 'Subnets', 'Route tables', 'Internet gateways', 'Egress-only internet gateways', 'Carrier gateways', 'DHCP option sets', 'Elastic IPs', 'Managed prefix lists', 'Endpoints', 'Endpoint services', 'NAT gateways', and 'Peering connections'.

The main content area is titled 'Your VPCs (1/2)' and features a search bar and a 'Create VPC' button. A table lists the VPCs:

	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/>	TGW-VPC-vpc	vpc-098c83289ed2b5c37	Available	10.0.0.0/16	-

Below the table, the 'Resource map' tab is selected, showing a diagram of the VPC resources. The diagram includes a 'VPC' box labeled 'TGW-VPC-vpc', a 'Subnets (1)' box labeled 'us-east-1a' containing 'TGW-VPC-subnet-public1-us-east-1a', and a 'Route tables (2)' box containing 'TGW-VPC-rtb-public' and 'rtb-05debbda28b566271'. A line connects the subnet box to the route table box. A feedback prompt asks 'Was the resource map helpful today?' with a 'Give us feedback as often as' link.

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

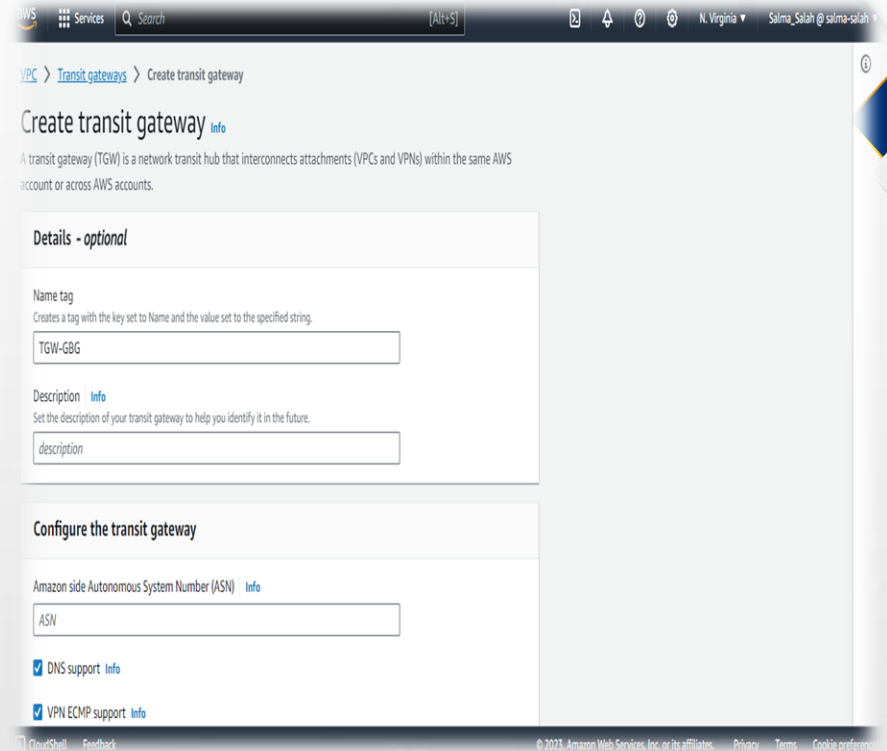
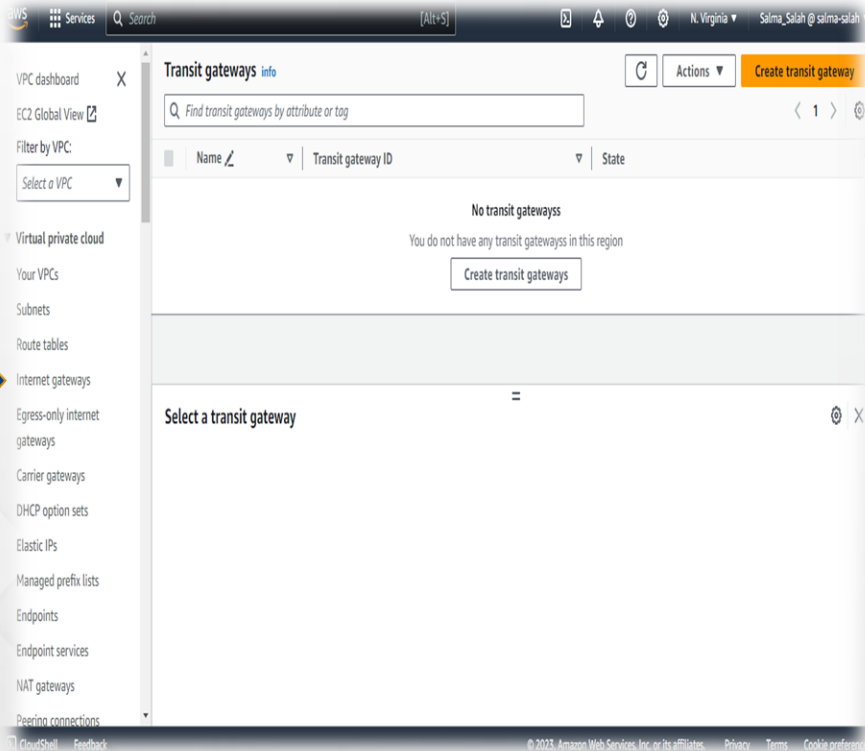
## 2) Create an EC2 instance

The screenshot displays the AWS Management Console interface. On the left, the navigation menu includes 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Instances', 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Capacity Reservations', 'Images', 'AMI Catalog', and 'Elastic Block Store'. The main content area is titled 'Instances (1/1) Info'. It features a search bar with the placeholder 'Find Instance by attribute or tag (case-sensitive)', a filter dropdown set to 'Instance state: running', and a 'Clear filters' button. Below this is a table with one instance listed: 'TGW-EC2' with Instance ID 'i-099f229dd69f98506', state 'Running', type 't2.micro', and status '2/2 checks passed'. The instance is located in 'us-east-1a'. Below the table, the 'Instance: i-099f229dd69f98506 (TGW-EC2)' details are shown, including tabs for 'Details', 'Security', 'Networking', 'Storage', 'Status checks', 'Monitoring', and 'Tags'. The 'Details' tab is active, showing an 'Instance summary' with the following information:

Instance summary Info		
Instance ID	Public IPv4 address	Private IPv4 addresses
i-099f229dd69f98506 (TGW-EC2)	3.238.2.91   <a href="#">open address</a>	10.0.1.120
IPv6 address	Instance state	Public IPv4 DNS
-	Running	ec2-3-238-2-91.compute-1.amazonaws.com   <a href="#">open address</a>
Hostname type	Private IP DNS name (IPv4 only)	
IP name: ip-10-0-1-120.ec2.internal	ip-10-0-1-120.ec2.internal	

At the bottom of the console, there is a footer with 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates, along with links for 'Privacy', 'Terms', and 'Cookie preferences'.

# 3) Create a Transit Gateway



# Transit Gateway configuration

Services Search [Alt+S] N. Virginia Salma\_Salah @ salma-salah

### Configure cross-account sharing options

☒ Auto accept shared attachments [Info](#)

### Transit gateway CIDR blocks

CIDR - optional [Info](#)

### Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="TGW-GBG"/>

[Remove](#)

[Add new tag](#)

You can add up to 49 more tags.

[Cancel](#) [Create transit gateway](#)

Services Search [Alt+S] N. Virginia Salma\_Salah @ salma-salah

### Transit gateways (1/1) [Info](#)

[Find transit gateways by attribute or tag](#)

<input checked="" type="checkbox"/>	Name	Transit gateway ID	State
<input checked="" type="checkbox"/>	TGW-GBG	tgw-091e05ac5de82155d	<span>Available</span>

#### Transit gateway: tgw-091e05ac5de82155d / TGW-GBG

Transit gateway ID tgw-091e05ac5de82155d	Transit gateway ARN arn:aws:ec2:us-east-1:821594020462:transit-gateway/tgw-091e05ac5de82155d	Owner ID 821594020462	Description -
State <span>Available</span>	Default association route table Enable	Default propagation route table Enable	Transit gateway CIDR blocks -
Amazon ASN 64512	Association route table ID <a href="#">tgw-rtb-0c1cfd976c428552</a>	Propagation route table ID <a href="#">tgw-rtb-0c1cfd976c428552</a>	Multicast support Disable
DNS support Enable	Auto accept shared attachments Enable	VPN ECMP support Enable	

# 4) Create a Resource Share

The screenshot shows the AWS Resource Access Manager console. The left sidebar has a 'Resource Access Manager' header and a 'Shared by me' section with links for 'Resource shares', 'Shared resources', and 'Principals'. The main content area is titled 'Shared by me: Resource shares' and includes a sub-header 'Resource shares owned by your account.' Below this, there is a 'Resource shares (0)' section with a search bar and a 'Create resource share' button. A table with columns 'Name', 'ID', 'Owner', 'Allow external principals', and 'Status' is shown, but it is empty with the message 'No resource shares found. Start sharing resources by creating a resource share.' and a 'Create resource share' button.

Resource Access Manager

Shared by me

Resource shares

Shared resources

Principals

Shared with me

Resource shares

Shared resources

Principals

Managed permissions library

Settings

Resource Access Manager > Shared by me: Resource shares

Shared by me: Resource shares

Resource shares owned by your account.

Resource shares (0)

Filter by text and property value

1

Name	ID	Owner	Allow external principals	Status
No resource shares found. Start sharing resources by creating a resource share.				

Create resource share

The screenshot shows the 'Specify resource share details' page in the AWS Resource Access Manager console. It includes a progress bar with four steps: 'Specify resource share details', 'Associate managed permissions', 'Grant access to principals', and 'Review and create'. The 'Specify resource share details' step is active. It has a section for 'Resource share name' with a 'Name' field containing 'TGW-RS'. Below this is a 'Resources - optional' section with a dropdown menu set to 'Transit Gateways' and a search bar. A table with columns 'ID', 'Name', 'Description', and 'State' is shown, containing one entry: 'tgw-091e05ac5de82155d', 'TGW-GBG', '-', and 'pending'.

Resource Access Manager > Shared by me: Resource shares > Create resource share

Step 1

Specify resource share details

Specify resource share details

Enter a name for the resource share and select the resources that you want to share.

Step 2

Associate managed permissions

Step 3

Grant access to principals

Step 4

Review and create

Resource share name

Name

Provide a descriptive name for the resource share.

TGW-RS

Resources - optional

Choose the resources to add to the resource share

Transit Gateways

Filter by text and property value

1

ID	Name	Description	State
<input checked="" type="checkbox"/> tgw-091e05ac5de82155d	TGW-GBG	-	pending



# Resource Share Configuration

AWS Services Search [Alt+S] N. Virginia Salma\_Salah @ salma-salah

Name	Description	Status
<input checked="" type="checkbox"/> tgw-091e05ac5de82155d	TGW-GBG	- pending

**Selected resources (1 selected)** Deselect

Filter by text

Resource ID	Resource type
<input checked="" type="checkbox"/> <a href="#">tgw-091e05ac5de82155d</a>	ec2:TransitGateway

**Tags - optional**  
Tags are key-value pairs that you can add to AWS resources to help identify, organize, and secure your AWS resources.

Key	Value - optional	
<input type="text" value="Enter key"/>	<input type="text" value="Enter value"/>	Remove

AWS Services Search [Alt+S] N. Virginia Salma\_Salah @ salma-salah

Associate managed permissions

Step 3  
Grant access to principals

Step 4  
Review and create

**Managed permission for ec2:TransitGateway**

Managed permissions  
For this resource type, only one managed permission is available.

Version  
You can use only the default version of a managed permission when creating a resource share.

**View the policy template for this managed permission**

Statement 1

Actions (4)

ec2:CreateTransitGatewayVpcAttachment	ec2>DeleteTransitGatewayVpcAttachment
ec2:DescribeTransitGateways	ec2:ModifyTransitGatewayVpcAttachment

Conditions (0)  
No conditions applied

# Resource Share Configuration

The image displays two side-by-side screenshots of the AWS Resource Access Manager (RAM) console, illustrating the 'Grant access to principals' configuration process.

**Left Screenshot (Step 1):**

- Navigation:** Resource Access Manager > Shared by me: Resource shares > Create resource share.
- Steps:** Step 1: Specify resource share details; Step 2: Associate managed permissions; Step 3: Grant access to principals; Step 4: Review and create.
- Section:** Grant access to principals.
- Description:** Specify the principals that are allowed access to the shared resources. A principal can be any of the following: An entire organization or organizational unit (OU) in AWS Organizations, an AWS account, IAM role, or IAM user.
- Principals - optional:**
  - ☒ Allow sharing with anyone: You can share resources with any AWS accounts, roles, and users. If you are in an organization, you can also share with the entire organization or organizational units in that organization.
  - ☐ Allow sharing only within your organization: You can share resources with the entire organization, organizational units, or AWS accounts, roles, and users in that organization.
- Principals:** You can add multiple principals of different types.
- Select principal type:** A dropdown menu showing 'AWS account'.
- Enter an AWS account ID:** A text input field.
- Text:** An AWS account ID is a 12-digit number.
- Add:** A button to add a principal.

**Right Screenshot (Step 3):**

- Select principal type:** A dropdown menu showing 'AWS account'.
- Enter an AWS account ID:** A text input field.
- Text:** An AWS account ID is a 12-digit number.
- Add:** A button to add a principal.
- Selected principals (3 selected):** A section showing the selected principals with a 'Deselect' button.
- Description:** The following principals will be allowed access to the shared resources.
- Filter:** A search bar with the text 'Filter by text'.
- Table:** A table listing the selected principals.

Principal ID	Principal type
<input checked="" type="checkbox"/> 214199940805	AWS account
<input checked="" type="checkbox"/> 487660541358	AWS account
<input checked="" type="checkbox"/> 112013099121	AWS account

- Buttons:** Cancel, Previous, Next.

# Review Resource Share

Resource Access Manager > Shared by me: Resource shares > Create resource share

Step 1  
[Specify resource share details](#)

Step 2  
[Associate managed permissions](#)

Step 3  
[Grant access to principals](#)

Step 4  
Review and create

## Review and create

Review the resource share configuration and make changes if needed. After you finish reviewing the configuration, choose **Create resource share**.

Step 1: Resource share details Edit

**Basic information**

Name  
TGW-RS

**Resources to share (1)**

< 1 > ⓘ

Resource ID	Resource type
<a href="#">tgw-091e05ac5de82155d</a> ⓘ	ec2:TransitGateway

Resource share successfully created

Resource Access Manager > Shared by me: Resource shares > Resource share 919e87bc-74e8-4ee4-bf74-63d593eea33a

## TGW-RS (919e87bc-74e8-4ee4-bf74-63d593eea33a)

Modify Delete

Details and information relating to this resource share.

**Summary**

Name TGW-RS	Owner 821594020462	Created on 2023/11/25	Status Active
ID 919e87bc-74e8-4ee4-bf74-63d593eea33a	ARN <a href="#">arn:aws:ramus-east-1:821594020462:resource-share/919e87bc-74e8-4ee4-bf74-63d593eea33a</a>	Allow external principals Yes	

**Shared resources (1)** Disassociate

< 1 > ⓘ

# After creating the resource share

- In Resource share the selected principals are the account IDs of accounts that want to connect VPCs through the Transit Gateway.
- After adding these accounts IDs a request will be sent to each of those accounts.
- Each account will have to accept the request to be able to connect through the Transit Gateway.
- After accepting the request each account will be able to create the Transit Gateway Attachment.

# 5) Create Transit Gateway Attachment

The screenshot shows the AWS Management Console interface for 'Transit gateway attachments'. The top navigation bar includes the AWS logo, 'Services', a search bar, and user information. The left sidebar lists various AWS services, with 'Virtual private cloud' expanded. The main content area is titled 'Transit gateway attachments' and shows a message: 'No transit gateway attachments. You do not have any transit gateway attachments in this region.' Below this message is a button labeled 'Create transit gateway attachments'. A table header is visible with columns: Name, Transit gateway attachment ID, Transit gateway ID, State, and Resource. At the bottom of the console, there is a footer with copyright information and links to Privacy, Terms, and Cookie preferences.

The screenshot shows the 'Create transit gateway attachment' page in the AWS Management Console. The breadcrumb navigation at the top reads 'VPC > Transit gateway attachments > Create transit gateway attachment'. The page title is 'Create transit gateway attachment'. A descriptive text states: 'A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.' The 'Details' section contains three fields: 'Name tag - optional' with a value of 'ATT-TGW', 'Transit gateway ID' with a dropdown menu showing 'tgw-091e05ac5de82155d', and 'Attachment type' with a dropdown menu showing 'VPC'. The 'VPC attachment' section has two checkboxes: 'DNS support' (checked) and 'IPv6 support'. The footer of the console shows copyright information and links to Privacy, Terms, and Cookie preferences.

# Transit Gateway Attachment Configuration

Select and configure your VPC attachment.

☒ DNS support [Info](#)

☐ IPv6 support [Info](#)

☐ Appliance Mode support [Info](#)

VPC ID

Select the VPC to attach to the transit gateway.

vpc-098c83289ed2b5c37

Q |

vpc-07e368fb8901161b4  
172.31.0.0/16

vpc-098c83289ed2b5c37 (TGW-VPC-vpc)  
10.0.0.0/16 ✓

us-east-1c No subnet available

us-east-1d No subnet available

us-east-1e No subnet available

us-east-1f No subnet available

subnet-0f99c901e7dba329c ✕

CloudShell Feedback

© 2023, Amazon Web S

VPC dashboard X

EC2 Global View

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

You successfully created VPC attachment tgw-attach-0a2bef6935eec8526 / ATT-TGW.

Transit gateway attachments (1/1) [Info](#)

Find transit gateway attachments by attribute or tag

1 >

<input checked="" type="checkbox"/>	Name	Transit gateway attachment ID	Transit gateway ID	State	Resource type
<input checked="" type="checkbox"/>	ATT-TGW	tgw-attach-0a2bef6935eec8526	tgw-091e05ac5de82155d	Pending	VPC

Transit gateway attachment: tgw-attach-0a2bef6935eec8526 / ATT-TGW

Transit gateway attachment ID	Transit gateway ID	Transit gateway owner ID	Subnet IDs
tgw-attach-0a2bef6935eec8526	tgw-091e05ac5de82155d	821594020462	subnet-0f99c901e7dba329c
State	Resource owner ID	DNS support	Resource type
Pending	821594020462	Enable	VPC
Resource ID	IPv6 support	Association state	Association route table ID
vpc-098c83289ed2b5c37	Disable	-	-
Appliance Mode support			
Disable			

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## 6) Route table Modification

aws Services Search [Alt+S] N. Virginia Salma\_Salah @ salma-salah

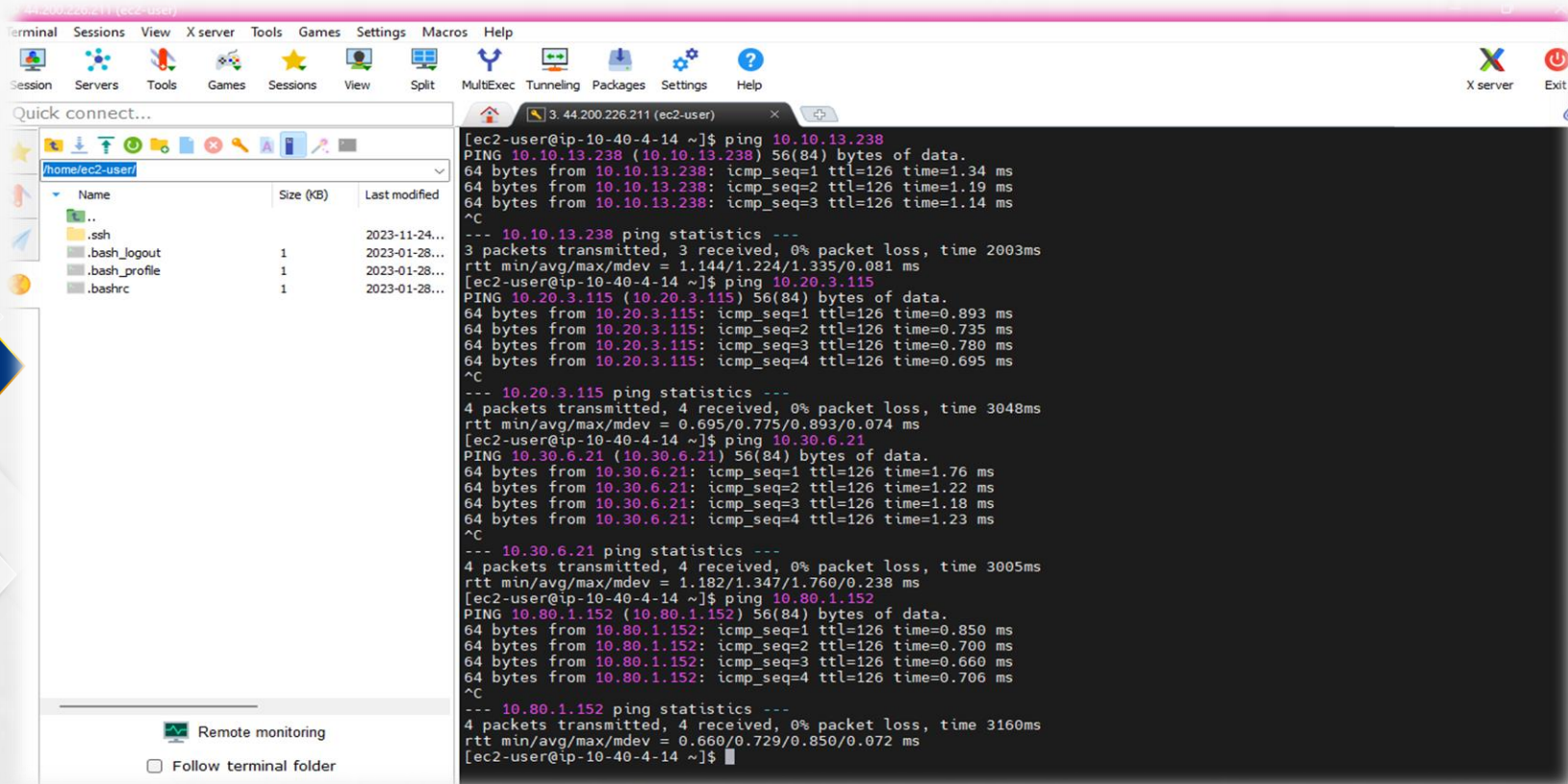
Destination	Target	Status	Propagated
10.0.0.0/16	local Q local X	Active	No
Q 0.0.0.0/0 X	Internet Gateway Q igw-0834af3928cf159b3 X Use: "igw-0834af3928cf159b3"	Active	No
Q 10.10.0.0/16 X	igw-0834af3928cf159b3 (TGW-VPC-igw) Q tgw-091e05ac5de82155d X	-	No
Q 10.20.0.0/16 X	Transit Gateway Q tgw-091e05ac5de82155d X	-	No
Q 10.30.0.0/16 X	Transit Gateway Q tgw-091e05ac5de82155d X	-	No
Q 10.80.0.0/16 X	Transit Gateway Q tgw-091e05ac5de82155d X	-	No

Add route

CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# 7) Testing Connection between all VPCs attached to the TGW



The screenshot shows a terminal window with a file explorer on the left and a terminal output on the right. The file explorer shows the contents of the `/home/ec2-user/` directory, including `.ssh`, `.bash_logout`, `.bash_profile`, and `.bashrc`. The terminal output shows the results of three ping tests:

```
[ec2-user@ip-10-40-4-14 ~]$ ping 10.10.13.238
PING 10.10.13.238 (10.10.13.238) 56(84) bytes of data.
64 bytes from 10.10.13.238: icmp_seq=1 ttl=126 time=1.34 ms
64 bytes from 10.10.13.238: icmp_seq=2 ttl=126 time=1.19 ms
64 bytes from 10.10.13.238: icmp_seq=3 ttl=126 time=1.14 ms
^C
--- 10.10.13.238 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.144/1.224/1.335/0.081 ms
[ec2-user@ip-10-40-4-14 ~]$ ping 10.20.3.115
PING 10.20.3.115 (10.20.3.115) 56(84) bytes of data.
64 bytes from 10.20.3.115: icmp_seq=1 ttl=126 time=0.893 ms
64 bytes from 10.20.3.115: icmp_seq=2 ttl=126 time=0.735 ms
64 bytes from 10.20.3.115: icmp_seq=3 ttl=126 time=0.780 ms
64 bytes from 10.20.3.115: icmp_seq=4 ttl=126 time=0.695 ms
^C
--- 10.20.3.115 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3048ms
rtt min/avg/max/mdev = 0.695/0.775/0.893/0.074 ms
[ec2-user@ip-10-40-4-14 ~]$ ping 10.30.6.21
PING 10.30.6.21 (10.30.6.21) 56(84) bytes of data.
64 bytes from 10.30.6.21: icmp_seq=1 ttl=126 time=1.76 ms
64 bytes from 10.30.6.21: icmp_seq=2 ttl=126 time=1.22 ms
64 bytes from 10.30.6.21: icmp_seq=3 ttl=126 time=1.18 ms
64 bytes from 10.30.6.21: icmp_seq=4 ttl=126 time=1.23 ms
^C
--- 10.30.6.21 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.182/1.347/1.760/0.238 ms
[ec2-user@ip-10-40-4-14 ~]$ ping 10.80.1.152
PING 10.80.1.152 (10.80.1.152) 56(84) bytes of data.
64 bytes from 10.80.1.152: icmp_seq=1 ttl=126 time=0.850 ms
64 bytes from 10.80.1.152: icmp_seq=2 ttl=126 time=0.700 ms
64 bytes from 10.80.1.152: icmp_seq=3 ttl=126 time=0.660 ms
64 bytes from 10.80.1.152: icmp_seq=4 ttl=126 time=0.706 ms
^C
--- 10.80.1.152 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3160ms
rtt min/avg/max/mdev = 0.660/0.729/0.850/0.072 ms
[ec2-user@ip-10-40-4-14 ~]$
```

At the bottom of the terminal window, there are two checkboxes: ☒ Remote monitoring and ☐ Follow terminal folder.