
TRANSIT GATEWAY

AWS Transit Gateway is a pivotal networking service provided by Amazon Web Services that simplifies the management of network connectivity at scale. It serves as a central hub for connecting Virtual Private Clouds (VPCs), on-premises networks, and other resources within an AWS environment. By consolidating multiple networking connections through a single gateway, AWS Transit Gateway facilitates efficient network management, improves performance, and enhances security.

Key features of AWS Transit Gateway include:

- **Centralized Network Management:** Simplify network design by consolidating multiple VPCs and VPN connections into a single gateway.
- **Scalability:** Efficiently handle large-scale networks with high throughput and low latency.
- **Segmentation and Isolation:** Enable network segmentation and isolation to improve security and compliance.
- **Flexible Routing:** Utilize advanced routing options and policies to control traffic flow between network resources.
- **Cost Efficiency:** Reduce operational costs by minimizing the need for complex peering arrangements and extensive network configurations.

Components Explained

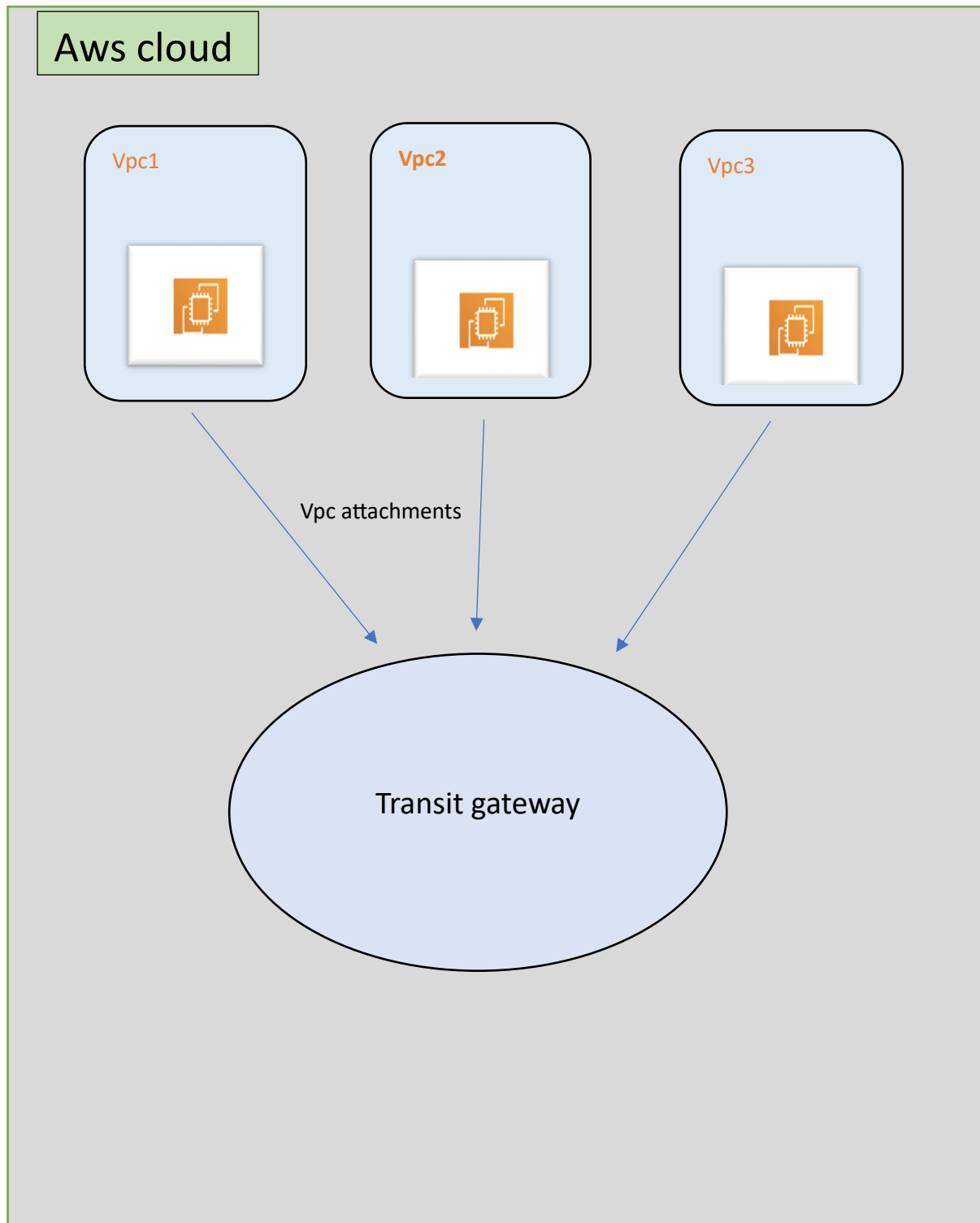
1. **AWS Transit Gateway:** Acts as a centralized router for network traffic between connected VPCs.
2. **VPC 1, VPC 2, VPC 3:** Individual VPCs with their own route tables and subnets. Each VPC connects to the Transit Gateway.
3. **Route Tables:**
 - Each VPC has a route table with routes to the Transit Gateway (TG). This enables traffic to be routed between VPCs via the TG.
 - The Transit Gateway also has its own route table to handle traffic between VPCs and ensure correct routing.

Key Points

- **Connectivity:** VPCs can communicate with each other through the Transit Gateway without needing VPC peering connections.
- **Routing:** Ensure each VPC's route table directs traffic intended for other VPCs to the Transit Gateway.

- **Scalability:** Adding more VPCs is straightforward; just connect them to the existing Transit Gateway.

Configuration diagram:



Connecting three VPCs with transit gateway

Open AWS console and select VPC and click on Create.

- I was created VPC in **Asia Pacific (Seoul) Region**.

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

☐ VPC only ☒ VPC and more

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate
vpc1

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.

10.11.0.0/16 65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

☒ No IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block

Preview

VPC Show details
Your AWS virtual network

vpc1-vpc

Subnets (2)
Subnets within this VPC

ap-northeast-2a

- vpc1-subnet-public1-ap-northeast-
- vpc1-subnet-private1-ap-northeast-

I Was created VPC1 in Zone(ap-northeast-2a) with 2 subnets (1 public, 1 private), 2 route tables (1 public, 1 private) and 1 internet gateway with IP address-10.11.0.0/16. Similarly, I was created another 2 VPCs (VPC2 & VPC3). VPC2 in ap-northeast-2b Zone with IP address as 10.12.0.0/16 and VPC3 in ap-northeast-2c Zone with IP address as 10.13.0.0/16 respectively.

VPC dashboard X

EC2 Global View

Filter by 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

Your VPCs (4) Info

Last updated less than a minute ago

Actions Create VPC

| | Name | VPC ID | State | IPv4 CIDR | IPv6 CIDR | D |
|--------------------------|---------|-----------------------|-----------|---------------|-----------|----|
| <input type="checkbox"/> | default | vpc-0543ea4df9721ffd3 | Available | 172.31.0.0/16 | - | di |
| <input type="checkbox"/> | vpc1 | vpc-0723b4c280606b2e3 | Available | 10.11.0.0/16 | - | di |
| <input type="checkbox"/> | vpc2 | vpc-035475e7448cd5099 | Available | 10.12.0.0/16 | - | di |
| <input type="checkbox"/> | vpc3 | vpc-08e3b7437e90c1c59 | Available | 10.13.0.0/16 | - | di |

Select a VPC above

3 VPCs were created in separate zones within the same region.

2. Creating Transit gateway:

VPC > Transit gateways > Create transit gateway

Create transit gateway [Info](#)

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

Details - optional

Name tag
Creates a tag with the key set to Name and the value set to the specified string.

Transit-gw

Description [Info](#)
Set the description of your transit gateway to help you identify it in the future.

description

Configure the transit gateway

Amazon side Autonomous System Number (ASN) [Info](#)

ASN

☒ DNS support [Info](#)

☒ VPN ECMP support [Info](#)

☒ Default route table association [Info](#)

Open Transit gateway and created with name as Transit-GW.

✓ You successfully created tgw-06d63d514a0462d50 / Transit-gw.

ⓘ You can visualize and monitor your Transit Gateway(s) from the [AWS Network Manager](#). Register your Transit Gateway by creating a [global network](#) to get started.

Transit gateways (1) [Info](#)

Find transit gateway by attribute or tag

Actions Create transit gateway

| | Name | Transit gateway ID | State |
|--------------------------|------------|-----------------------|-------------|
| <input type="checkbox"/> | Transit-gw | tgw-06d63d514a0462d50 | ✓ Available |

Once transit gateway created go to transit gateway attachments.

3. Transit gateway attachments: Create transit gateway attachments as shown in below.

[VPC](#) > [Transit gateway attachments](#) > [Create transit gateway attachment](#)

Create transit gateway attachment [Info](#)

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same account or across AWS accounts.

Details

Name tag - optional
Creates a tag with the key set to Name and the value set to the specified string.

Transit gateway ID [Info](#)

Attachment type [Info](#)

VPC attachment

Select and configure your VPC attachment.

☒ **DNS support** [Info](#)

☐ **IPv6 support** [Info](#)

☐ **Appliance Mode support** [Info](#)

Create Transit gateway attachment for VPC1: Go to Transit gateway attachments and click on create->give name->select Transit gateway ID->VPC ID and then create. Likewise for remaining 2 VPCs need to create transit gateway attachments (tg2 & tg3) as shown in below.

You successfully created VPC attachment tgw-attach-056089bdc6b2423bf / tg3.

You can visualize and monitor your Transit Gateway(s) from the [AWS Network Manager](#). Register your Transit Gateway by creating a [global network](#) to get started.

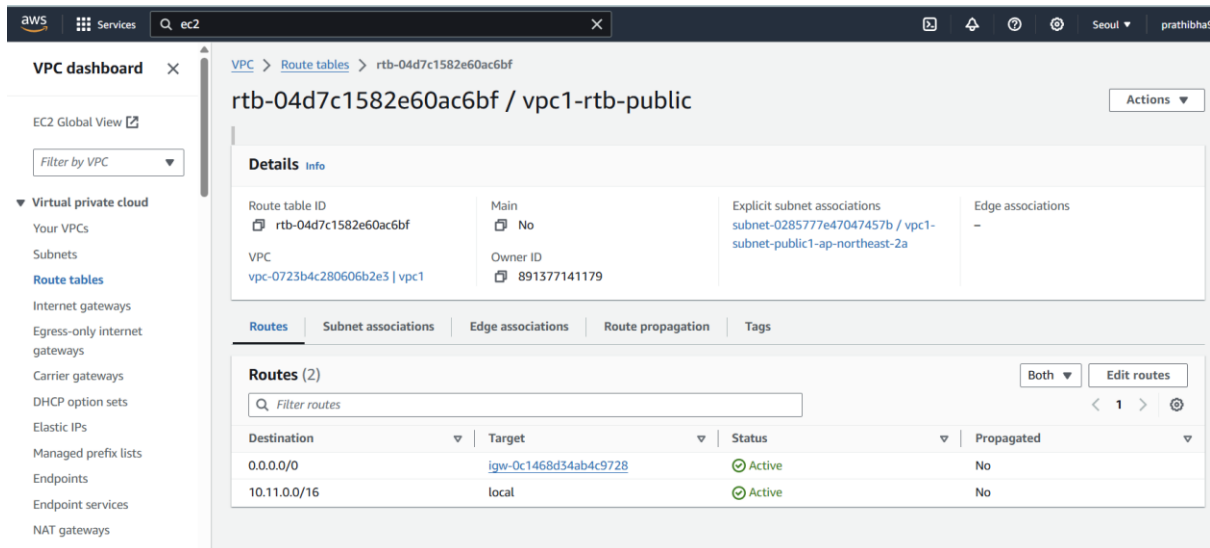
Transit gateway attachments (3) [Info](#)

| <input type="checkbox"/> | Name | Transit gateway attachment ID | Transit gateway ID | State | Resource type | Resource ID |
|--------------------------|------|-------------------------------|-----------------------|-----------|---------------|--------------|
| <input type="checkbox"/> | tg1 | tgw-attach-0c040e78dfee0d051 | tgw-06d63d514a0462d50 | Available | VPC | vpc-0723b... |
| <input type="checkbox"/> | tg2 | tgw-attach-0414a9ce12fd2affe | tgw-06d63d514a0462d50 | Available | VPC | vpc-03547... |
| <input type="checkbox"/> | tg3 | tgw-attach-056089bdc6b2423bf | tgw-06d63d514a0462d50 | Available | VPC | vpc-08e3b... |

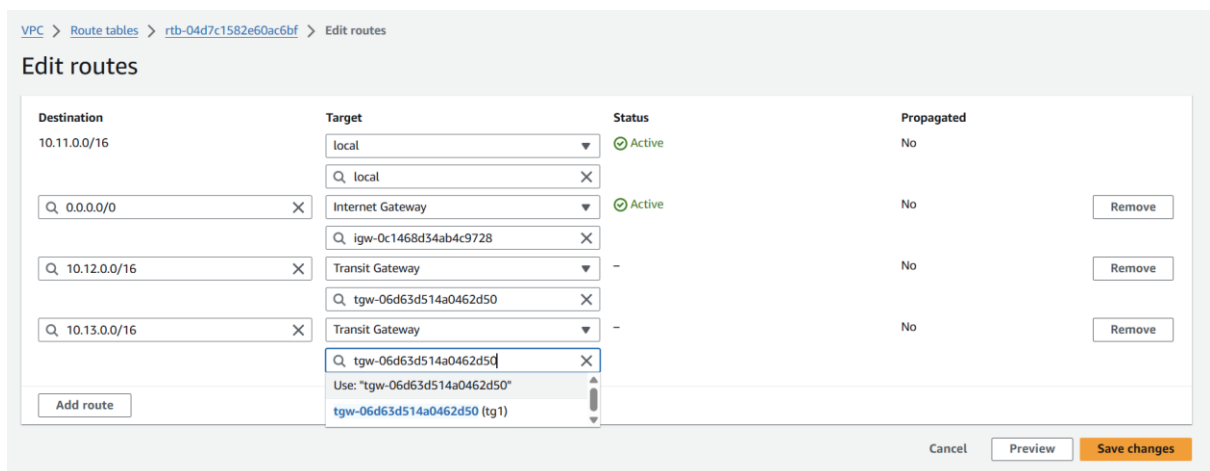
Select a transit gateway attachment

Once transit gateway attachments created go to the route tables.

4.Route tables:



I was taken VPC1 public route table and then go to edit routes. In that we need to add remaining 2 VPCs IP address and transit gateway attachments as shown in below diagram.



Like wise we need to add for remaining 2 route tables of VPC2 & VPC3. Once route table configuration done we need to create one EC2 instance for each VPC [VPC1, VPC2 & VPC3].

5.EC2 instance:

Go EC2 instance and click on launch instance. In that we need to give name for instance and then click on aws or ubuntu or etc -> create key pair as shown in below.

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents

Quick Start

Amazon Linux 2023

Ubuntu 22.04 LTS

Windows Server 2022

Red Hat Enterprise Linux 8

CentOS Stream 9

▼ Summary

Number of instances [Info](#)

Software Image (AMI)

Amazon Linux 2023 AMI 2023.5.2...[read more](#)

ami-045f2d6eeb07ce8c0

Virtual server type (instance type)


t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

 **Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which Free tier is available)

Cancel

Launch instance

[Review commands](#)

VPC - required

vpc-0723b4c280606b2e3 (vpc1)
10.11.0.0/16

Subnet

Info

subnet-0285777e47047457b
vpc-0723b4c280606b2e3 Owner: 891377141179
Availability Zone: ap-northeast-2a IP addresses available: 4090 CIDR: 10.11.0.0/20

Add assign public IP

Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Security group name - required

sg-vpc1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _~:/!@#%&*(){}\$*

Description - required

Info

Summary

Number of instances

Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.5.2...read more
ami-045f2d6eeb07ce8c0

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which you have access to the Free Tier.)

Cancel

Launch instance

Create the security group and allow the port numbers 22 for ssh and 80 for http as shown in below

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

Type [Info](#)

ssh ▼

Protocol [Info](#)

TCP

Port range [Info](#)

22

Source type [Info](#)

Anywhere ▼

Source [Info](#)

Q Add CIDR, prefix list or security

0.0.0.0/0 X

Description - optional [Info](#)

e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0)

Remove

Type [Info](#)

HTTP ▼

Protocol [Info](#)

TCP

Port range [Info](#)

80

Source type [Info](#)

Anywhere ▼

Source [Info](#)

Q Add CIDR, prefix list or security

0.0.0.0/0 X

Description - optional [Info](#)

e.g. SSH for admin desktop

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. X

Likewise create another 2 instances for VPC2 and VPC3. The overall configuration as shown in below diagrams for creating EC2 instance.

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name

vpc3-instance

Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-045f2d6eeb07ce8c0 (64-bit (x86), uefi-preferred) / ami-08271b263d7b4ae11 (64-bit (arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Architecture

64-bit (x86)

Boot mode

uefi-preferred

AMI ID

ami-045f2d6eeb07ce8c0

Verified provider

Key pair (login)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

vpc3

Create new key pair

Network settings

VPC - required

vpc-08a3b7437e90c1c59 (vpc3)

10.10.0.0/16

Subnet

subnet-091a1f588b47e29fb vpc3-subnet-public-1-ap-northeast-2c

VPC: vpc-08a3b7437e90c1c59 Owner: 891377141179 Availability Zone: ap-northeast-2c IP addresses available: 4091 CIDR: 10.10.0.0/20

Create new subnet

Auto-assign public IP

Enable

Additional charges apply when outside of free tier allowance

Firewall (security group)

Create new security group

Select existing security group

Security group name - required

sgpc3

This security group will be added to all network interfaces. The name can't be called after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _ (underscore) (0-9a-zA-Z_)

Description - required

launch-wizard-1 created 2024-08-01T16:40:53.048Z

Inbound Security Group Rules

Security group rule 1 (TCP: 22, 0.0.0.0/0)

Remove

Type

ssh

Protocol

TCP

Port range

22

Source type

Anywhere

Source

Anywhere

Description - optional

e.g. SSH for admin desktop

Security rules remain in effect 0.0.0.0/0

Dismiss

Number of instances

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.5.2 - read more

ami-045f2d6eeb07ce8c0

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 100 GiB of bandwidth to the internet.

Cancel

Launch instance

Review commands

Instances (3)

Find Instance by attribute or tag (case-sensitive)

All states

Name

vpc1-instance

i-0f8c4bb27faf62405

Running

t2.micro

2/2 checks passed

View alarms

ap-northeast-2a

ec2-43-202-40-225.ap-

Name

vpc2-instance

i-0793719406206415d

Running

t3.micro

2/2 checks passed

View alarms

ap-northeast-2b

ec2-43-203-171-53.ap-

Name

vpc3-instance

i-069fd5ce5a5f52888

Running

t2.micro

Initializing

View alarms

ap-northeast-2c

ec2-43-201-20-225.ap-

Once instances came to running or available state then click on connect and copy the ssh command in ssh client field as shown in below diagram.

EC2 > Instances > i-0f8c4bb27faf62405 > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-0f8c4bb27faf62405 (vpc1-instance) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID
i-0f8c4bb27faf62405 (vpc1-instance)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is vini.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 "vini.pem"
4. Connect to your instance using its Public DNS:
ec2-43-202-40-225.ap-northeast-2.compute.amazonaws.com

✔ Command copied

```
ssh -i "vini.pem" ec2-user@ec2-43-202-40-225.ap-northeast-2.compute.amazonaws.com
```

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel

After that go to git bash and connect to the server. Once connected install the nginx and create the html file. Likewise connect remaining 2 instances [VPC2-instance & VPC3 - instance] and create files in it. Once done try to connect from VPC1-instance server to remaining 2 servers. It will get connect because of transit gateway. The output was shown in below pictures.

Output from VPC1-instance:

```
[root@ip-10-11-0-46 html]# curl 10.11.0.46:80
Hi this is from vpc1
[root@ip-10-11-0-46 html]# curl 10.12.11.144:80
hi this is from vpc2
[root@ip-10-11-0-46 html]# curl 10.13.12.252:80
hi this is from vpc3
[root@ip-10-11-0-46 html]#
```

Output from VPC2-instance:

```
[root@ip-10-12-11-144 html]# curl 10.12.11.144:80
hi this is from vpc2
[root@ip-10-12-11-144 html]# curl 10.11.0.46:80
Hi this is from vpc1
[root@ip-10-12-11-144 html]# curl 10.13.12.252:80
hi this is from vpc3
[root@ip-10-12-11-144 html]#
```

Output from VPC3-instance:

```
[root@ip-10-13-12-252 html]# curl 10.13.12.252:80
hi this is from vpc3
[root@ip-10-13-12-252 html]# curl 10.12.11.144:80
hi this is from vpc2
[root@ip-10-13-12-252 html]# curl 10.11.0.46:80
Hi this is from vpc1
[root@ip-10-13-12-252 html]#
```

Conclusion:

utilizing an AWS Transit Gateway to connect three Virtual Private Clouds (VPCs) offers a highly efficient and scalable networking solution. The Transit Gateway simplifies the network architecture by providing a central hub for interconnecting multiple VPCs, thereby reducing the complexity and number of peering connections needed. This setup not only enhances network management and monitoring but also improves security and performance through centralized traffic routing.