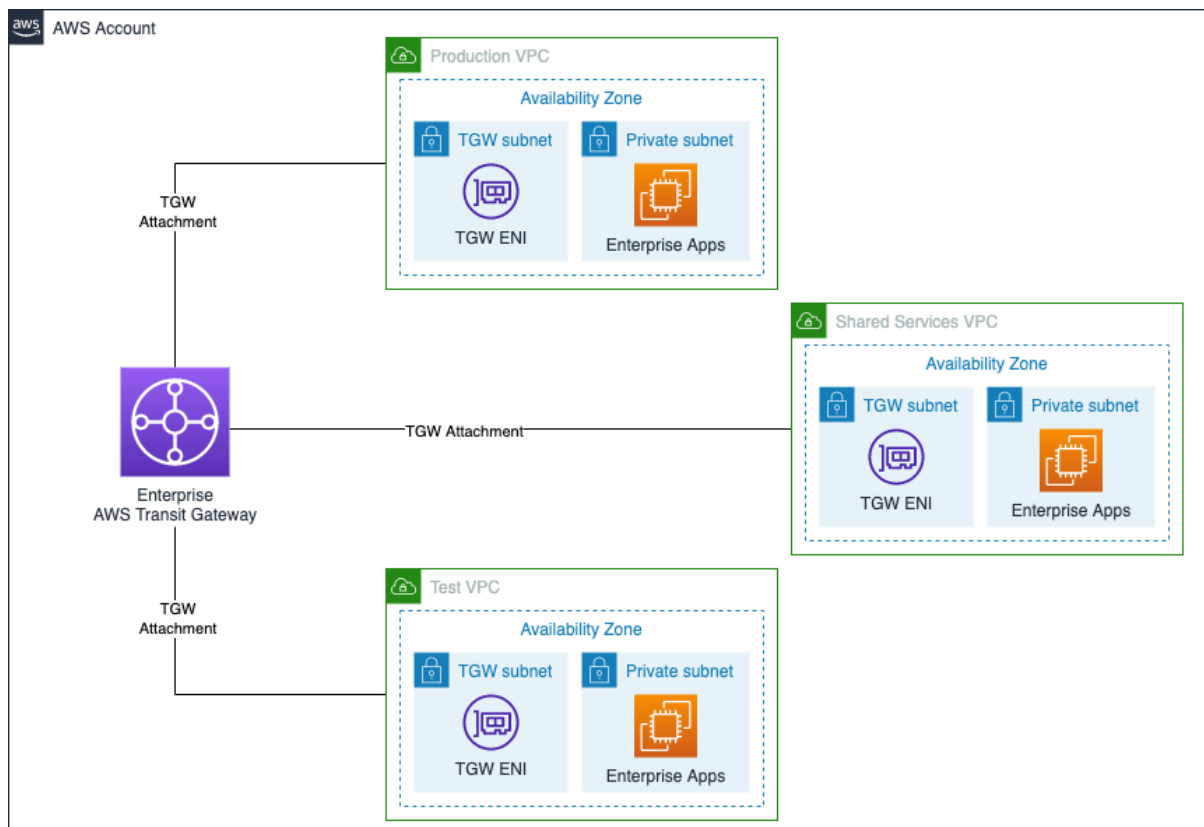


What is Transit Gateway

1. Transit gateway means interconnection between multiple VPC's
2. It acts as central hub

Transit Gateway Diagram



Steps to create Transit Gateway

Step 1:

1. Create three VPC'S
2. First create one VPC
 - Click on create VPC
 - Select VPC only
 - Give the name for VPC as VPC 1

- Give the CIDR block range as (10.0.0.0/16)
- Finally click on create VPC as shown in below figure

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 - optional
Creates a tag with a key of 'Name' and a value that you specify.

vpc1

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input ☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block ☐ IPAM-allocated IPv6 CIDR block ☐ Amazon-provided IPv6 CIDR block ☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Default

3. Create second VPC

- Click on create VPC
- Select VPC only
- Give the name for VPC as VPC 2
- Select the CIDR block range as (20.0.0.0/16)
- Finally click on create VPC as shown in below figure

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 - optional
Creates a tag with a key of 'Name' and a value that you specify.

vpc-2

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input ☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

20.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

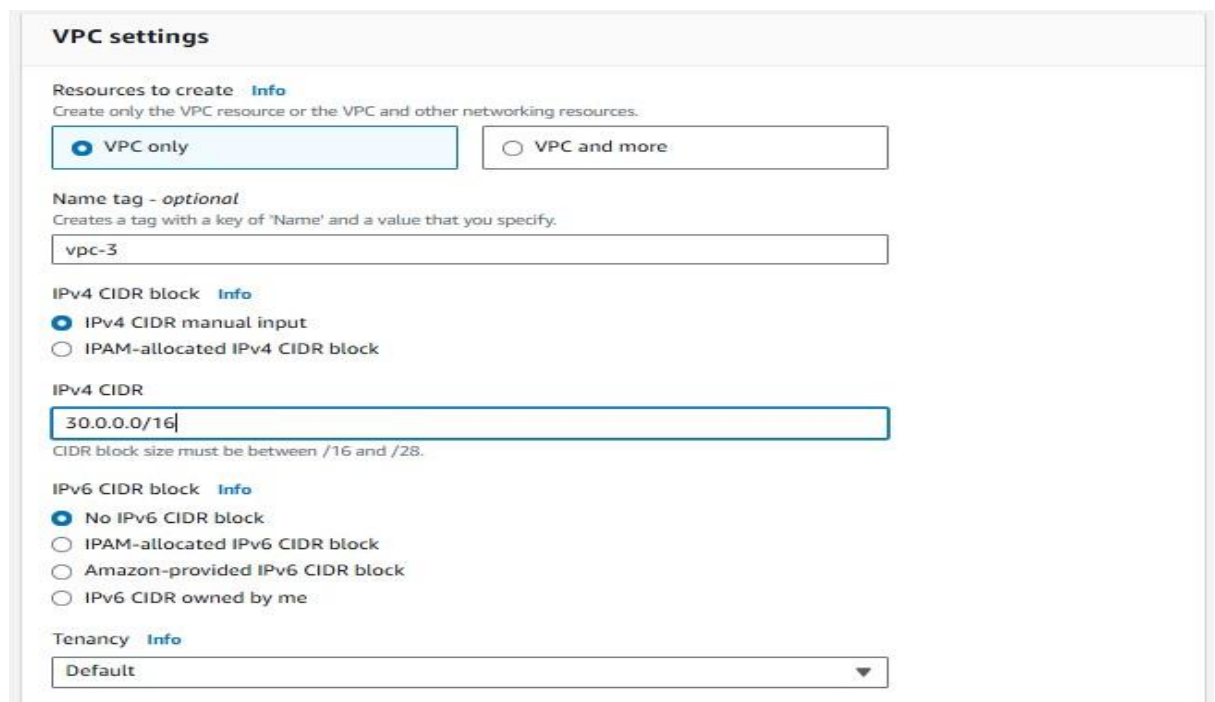
☒ No IPv6 CIDR block ☐ IPAM-allocated IPv6 CIDR block ☐ Amazon-provided IPv6 CIDR block ☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Default

4. Create third VPC

- Click on create VPC
- Select VPC only
- Give the name for VPC as VPC 3
- Select the CIDR block range as (30.0.0.0/16)
- Finally click on create VPC as shown in below figure



The screenshot shows the 'VPC settings' page in the AWS Management Console. It includes sections for 'Resources to create', 'Name tag - optional', 'IPv4 CIDR block', 'IPv6 CIDR block', and 'Tenancy'. The 'VPC only' option is selected under 'Resources to create'. The 'Name tag' is set to 'vpc-3'. Under 'IPv4 CIDR block', 'IPv4 CIDR manual input' is selected with the value '30.0.0.0/16'. Under 'IPv6 CIDR block', 'No IPv6 CIDR block' is selected. The 'Tenancy' is set to 'Default'.

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 - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

vpc-3

IPv4 CIDR block [Info](#)
☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
30.0.0.0/16
CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)
☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy [Info](#)
Default

Step 2:

1. Create subnets
2. First create one public subnet in VPC 1
3. Click on create subnet
 - Select the VPC as VPC 1
 - Edit subnet settings
 - Give the name for subnet as public-subnet
 - Select the availability zone
 - Give the CIDR block range for subnet as (10.0.0.0/27)
 - Finally click on create subnet as shown in below figure

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

 The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 32 IPs

▼ **Tags - optional**

4. Create two subnets, one subnet as public-subnet and second subnet as private-subnet in VPC 2
5. First create one public-subnet in VPC 2
6. Click on create subnets
 - Select VPC as VPC 2
 - Edit subnet settings
 - Give the name for subnet as public-subnet
 - Select the availability zone
 - Give CIDR block range for subnet as (20.0.0.0/27)
 - Finally click on create subnet as shown in below figure

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

 The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 32 IPs

▼ **Tags - optional**

7. Now create private-subnet in VPC 2

8. Click on create subnet

- Select VPC as VPC 2
- Edit subnet settings
- Give the name for subnet as private-subnet
- Select the availability zone
- Give CIDR block range for subnet as (20.0.1.0/27)
- Finally click on create subnet as shown in below figure

Subnet 2 of 2

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 32 IPs
< > ^ v

▼ **Tags - optional**

9. Create one public -subnet in VPC 3

10. Click on create subnet

- Select VPC as VPC 3
- Edit subnet settings
- Give the name for subnet as public-subnet
- Select the availability zone
- Give the CIDR block range for subnet as (30.0.0.0/16)
- Finally click on create subnet as shown in below figure

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 32 IPs

▼ Tags - optional

Step 3:

1. Go to route tables
2. By default, three route tables are created for three VPC'S
3. Give the names for three created route tables to avoid the confusions
4. Create one route table for private-subnet in VPC 2
5. Click on create route table
 - Give the name for route table as private-route
 - Select the VPC as VPC 2
 - Finally click on create route table
6. Select the private-route in route table
 - Click on subnet associations
 - Click on edit subnet associations
 - Select private-subnet
 - Click on save associations

Step 4:

1. Go to internet gateway

2. Create one internet gateway
3. Click on create internet gateway
 - Give the name for internet gateway
 - Finally click on create internet gateway
 - Attach the created internet gateway to VPC 1
4. Go to route table
 - Select VPC 1 created route table
 - Click on routes
 - Click on edit routes
 - Click on add routes
 - Select internet gateway and ID
 - Click on save changes as shown in below figure

Destination	Target	Status
10.0.0.0/16	local	Active
0.0.0.0/0	Internet Gateway	-

Add route

Step 5:

1. Select NAT gateway
2. Create one NAT gateway
3. Click on create NAT gateway
 - Give the name for NAT gateway
 - Select the subnet as public-subnet in VPC 2
 - Connectivity type is public
 - Click on allocate elastic IP
 - Finally click on create NAT gateway
 - As shown in below figure

NAT gateway settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

NAT

The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.

subnet-00b2dbaf670f71351 (public-subnet-vpc2)

Connectivity type
Select a connectivity type for the NAT gateway.

☒ Public
☐ Private

Elastic IP allocation ID [Info](#)
Assign an Elastic IP address to the NAT gateway.

eipalloc-097499f18c9008c35

[Allocate Elastic IP](#)

[▶ Additional settings](#) [Info](#)

4. Go to route table

5. Select private-route of VPC 2 in route table

- Click on routes
- Click on edit routes
- Click on add routes
- Select NAT gateway and ID
- Click on save changes as shown in below figure

Destination	Target	Status
20.0.0.0/16	local	Active
0.0.0.0/0	NAT Gateway	Active

[Add route](#)

Step 6:

1. Select transit gateway

2. Click on create transit gateway

- Give the name for transit gateway
- No need to select ASN leave as default

- Finally click on create transit gateway
- 3. Select transit gateway attachments
- 4. Create one transit gateway attachment
 - Give the name for transit gateway attachments
 - Select the transit gateway ID
 - Select the attachment type as VPC
 - Select the VPC ID as VPC 1
 - Finally click on create transit gateway attachments
- 5. Create the second transit gateway attachment
 - Give the name for transit gateway attachments
 - Select the transit gateway ID
 - Select the attachment type as VPC
 - Select the VPC ID as VPC 2
 - Finally click on create transit gateway attachments
- 6. Create the third transit gateway attachment
 - Give the name for transit gateway attachments
 - Select the transit gateway ID
 - Select the attachment type as VPC
 - Select the VPC ID as VPC 3
 - Finally click on create transit gateway attachments

Step 7:

1. Select the route tables
2. Select the public-route in VPC 1
 - Click on routes
 - Click on edit routes
 - Click on add route
 - Type VPC 2 CIDR block range ID as (20.0.0.0/16) to provide connection for VPC 1 to VPC 2
 - Select transit gateway and ID

- Finally click on save changes as shown in below figure

Destination	Target	Status
10.0.0.0/16	local	Active
0.0.0.0/0	Internet Gateway	Active
20.0.0.0/16	Transit Gateway	-
	tgw-07bc08af153fe0ddc	

Add route

3. Select the private-route in VPC 2

- Click on routes
- Click on edit routes
- Click on add route
- Type VPC 1 CIDR block range ID as (10.0.0.0/16) to provide connection for VPC 2 to VPC 1
- Click on add route
- Type VPC 3 CIDR block range ID as (30.0.0.0/16) to provide connection for VPC 2 to VPC 3
- Select transit gateway and ID
- Click on save changes as shown in below figure

Destination	Target	Status
20.0.0.0/16	local	Active
0.0.0.0/0	NAT Gateway	Active
10.0.0.0/16	Transit Gateway	-
30.0.0.0/16	Transit Gateway	-
	tgw-07bc08af153fe0ddc	

Add route

4. Select the public-route in VPC 3

- Click on routes
- Click on edit routes
- Click on add route

- Type VPC 2 CIDR block range ID as (20.0.0.0/16) to provide connection for VPC 3 to VPC 2
- Select the transit gateway and ID
- Click on save changes and shown in below figure

Destination	Target	Status
30.0.0.0/16	local	Active
Q 0.0.0.0/0	Internet Gateway	Active
Q 20.0.0.0/16	Transit Gateway	-
	Q tgw-07bc08af153fe0ddq	

Add route

Step 8:

1. Select the EC2 service
2. Create three instances with three VPC'S
3. First create one instance
4. Click on launch instance
 - Select the name for instance
 - Select the AMI as Amazon Linux
 - Select the key pair
 - Edit the network settings
 - Select the VPC as VPC 1
 - Select the subnet
 - Enable the auto assign public IP
 - Finally click on launch instance
5. Create second instance
6. Click on launch instance
 - Select the name for instance
 - Select the AMI as Amazon Linux
 - Select the key pair

```

pute.amazonaws.com
Warning: Permanently added 'ec2-13-126-198-68.ap-south-1.compute.amazonaws.com' to the list of known hosts.
X11 forwarding request failed on channel 0

#
~ \ #####
nn \ #####
nn \ ###|
nn \ #/
nn V~' ->
nnn
nn - .
  / \
 /m/ '

Amazon Linux 2023

https://aws.amazon.com/linux/amazon-linux-2023

[ec2-user@ip-10-0-6-7 ~]$ sudo -i

```

- Type `sudo -i` it will switch to root location
3. Select the second instance
- Copy the key pair and go to terminal
 - After switching into the root user
 - Type `vi` space key pair then `vi` editor will open and click `I` to enter into the insert mode then copy the key pair content and paste the content in `vi` editor save and come back to the terminal
 - Copy the `chmod 400 "raj.pem"` from `ssh` client in second instance and paste in terminal
 - Copy the example URL from `ssh` client in second instance and paste in terminal
 - Then it will ask yes/no then click yes and give enter
 - Then the second instance is connected as shown in below figure

```

pute.amazonaws.com
Warning: Permanently added 'ec2-13-126-198-68.ap-south-1.compute.amazonaws.com'
X11 forwarding request failed on channel 0

#
#####
#####\
#####|
\###/
\#/
V~' ->
https://aws.amazon.com/linux/amazon-linux-2023

[ec2-user@ip-10-0-6-7 ~]$ sudo -i
[root@ip-10-0-6-7 ~]# vi raj.pem
[root@ip-10-0-6-7 ~]# chmod 400 "raj.pem"
[root@ip-10-0-6-7 ~]# ssh -i "raj.pem" ec2-user@20.0.138.175
The authenticity of host '20.0.138.175 (20.0.138.175)' can't be established.
ED25519 key fingerprint is SHA256:55sZ1f8ubdnETz9Nz1AdE6MBoaZXky3/TFHH89Fff3E.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.0.138.175' (ED25519) to the list of known hosts.

#
#####
#####\
#####|
\###/
\#/
V~' ->
https://aws.amazon.com/linux/amazon-linux-2023

[ec2-user@ip-20-0-138-175 ~]$ sudo -i
[root@ip-20-0-138-175 ~]#

```

4. Select the third instance

- Copy the key pair and go to terminal
- After switching into the root user
- Type vi space key pair then vi editor will open and click I to enter into the insert mode then copy the key pair content and paste the content in vi editor save and come back to the terminal
- Copy the chmod 400 "raj.pem" from ssh client in third instance and paste in terminal
- Copy the example URL from ssh client in third instance and paste in terminal
- Then it will ask yes/no then click yes and give enter
- Then the third instance is connected as shown in below figure

[illegible]