AWS VPC creation

VPC and subnets

Name	Default	Adjustable	Comments
VPCs per Region	5	Yes	Increasing this quota increases the quota on internet gateways per Region by the same amount. You can increase this limit so that you can have hundreds of VPCs per Region.
Subnets per VPC	200	Yes	
IPv4 CIDR blocks per VPC	5	Yes (up to 50)	This primary CIDR block and all secondary CIDR blocks count toward this quota.
IPv6 CIDR blocks per VPC	5	Yes (up to 50)	The number of /56 CIDRs you can allocate to a single VPC.

Elastic IP addresses

Name	Default	Adjustable	Comments
Elastic IP addresses per Region	5	Yes	This quota applies to individual AWS account VPCs and shared VPCs.
Elastic IP addresses per public NAT gateway	2	Yes	

Gateways

Name	Default	Adjustable	Comments
Egress-only internet gateways per Region	5	Yes	To increase this quota, increase the quota for VPCs per Region. You can attach only one egress-only internet gateway to a VPC at a time.
Internet gateways per Region	5	Yes	To increase this quota, increase the quota for VPCs per Region. You can attach only one internet gateway to a VPC at a time.
NAT gateways per Availability Zone	5	Yes	NAT gateways only count toward your quota in the `pending`, `active`, and `deleting` states.
Private IP address quota per NAT gateway	8	Yes	You can assign private IP addresses only to private NAT gateways.
Carrier gateways per VPC	1	No	

Network ACLs

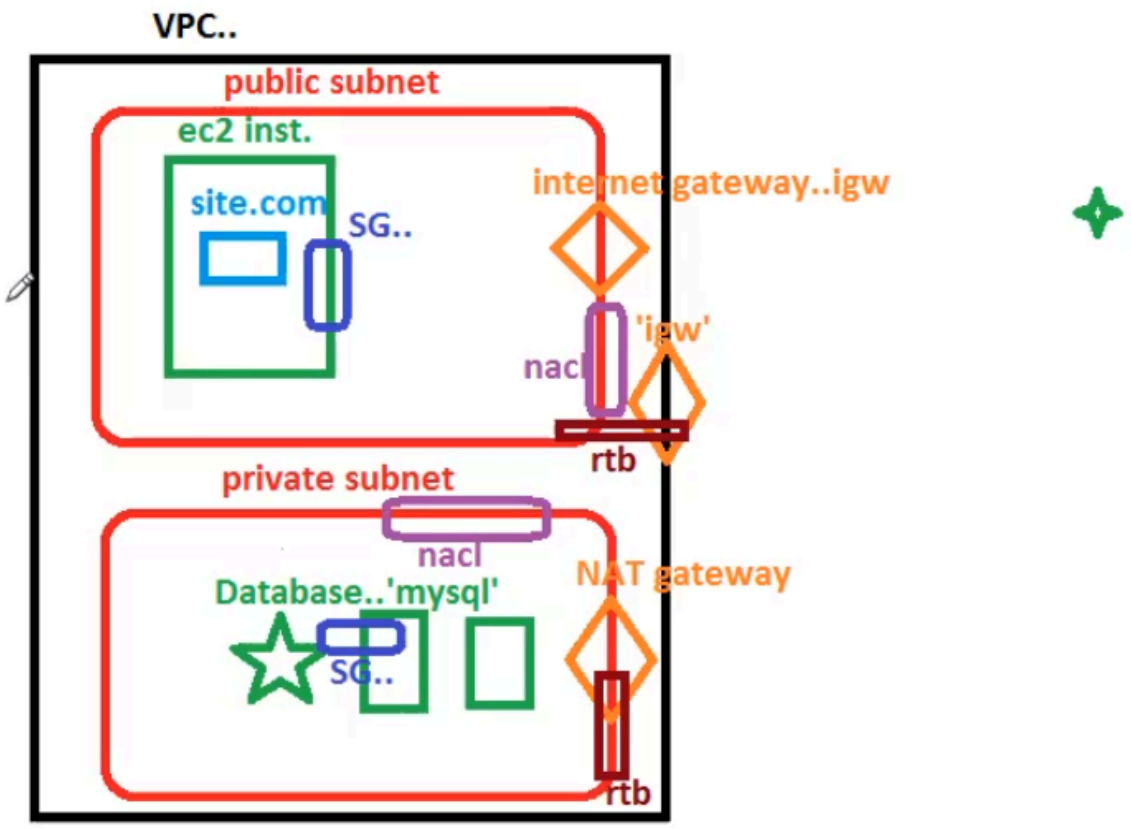
Name	Default	Adjustable	Comments
Network ACLs per VPC	200	Yes	You can associate one network ACL to one or more subnets in a VPC.
Rules per network ACL	20	Yes	This quota determines both the maximum number of inbound rules and the maximum number of outbound rules. This quota can be increased up to a maximum of 40 inbound rules and 40 outbound rules (for a total of 80 rules), but network performance might be impacted.

Route tables

Name	Default	Adjustable	Comments
Route tables per VPC	200	Yes	The main route table counts toward this quota. Note that if you request a quota increase for route tables, you may also want to request a quota increase for subnets. While route tables can be shared with multiple subnets, a subnet can only be associated with a single route table.
Routes per route table (non-propagated routes)	50	Yes	You can increase this quota up to a maximum of 1,000; however, network performance might be impacted. This quota is enforced separately for IPv4 routes and IPv6 routes. If you have more than 125 routes, we recommend that you paginate calls to describe your route tables for better performance.
Propagated routes per route table	100	No	If you require additional prefixes, advertise a default route.

Security groups

Name	Default	Adjustable	Comments
VPC security groups per Region	2,500	Yes	This quota applies to individual AWS account VPCs and shared VPCs. If you increase this quota to more than 5,000 security groups in a Region, we recommend that you paginate calls to describe your security groups for better performance.
Inbound or outbound rules per security group	60	Yes	This quota is enforced separately for IPv4 rules and IPv6 rules. Therefore, for an account with the default quota of 60 rules, a security group can have 60 inbound rules for IPv4 traffic and 60 inbound rules for IPv6 traffic. For more information, see Security group size. A quota change applies to both inbound and outbound rules. This quota multiplied by the quota for security groups per network interface cannot exceed 1,000.
Security groups per network interface	5	Yes (up to 16)	This quota multiplied by the quota for rules per security group cannot exceed 1,000.



- VPC is collection of subnets
- Two types of subnet are there : public subnet & private subnet
- Public subnet purpose : we create resources in a public subnet (resources like instance), because any public user/any user can access the resources.
- Private subnet purpose : we create a database (mysql) in a private subnet, because the database needs to be very secure and can not be accessed publicly. so public users can not access the database. we can also create instances/databases in private subnets, so no public user can access them.
- Suppose I have deployed a website in a public subnet's ec2 instance, then the user will request the information, then that request for the info is sent to the database from the public subnet's ec2 instance, and info is sent back to the public subnets website and then forwarded to the user.
- Can a user directly access the resource (database, instance) in a private subnet?
  -> NO

- How to differentiate whether a subnet is public or private?
  -> using gateways

Internet gateway : it is attached to the public subnet, it lets you access the resources publicly.

NAT gateway : it is attached to the private subnet.
This NAT gateway makes the private subnet more secure.
HOW? -> if a public user tries to access the private subnet, it rejects, it allows the resource in only one way. -> resources can access the internet through NAT gateway, but the internet can not access the resources in private subnets.

- Why does VPC need an internet gateway?
  -> The internet gateway is connected at two levels, namely the VPC (Virtual Private Cloud) and subnet levels. This configuration is essential because instances within the VPC send requests to a NAT (Network Address Translation) device. The NAT device then forwards these requests to the VPC's internet gateway, which ultimately routes the traffic to the broader internet.

- Internet gateway :internet -> IGW -> resources -> IGW -> internet (two way communication in public subnet via IGW)

- How does the user/internet access the database?
  -> user request is sent to the IGW of VPC then IGW of subnet then private subnet, the response from private subnet is sent back to the public subnet and then to the user.

- Security Group: security grp are attach at instance lvl
  Both private and public resources have security groups.

- NACL : NACL is attached at subnet lvl, for both public and private subnet.

- User -> public subnet
  User -> IGW -> public NACL (inbound rule in NACL, allowing this request) -> public instance SG (instance lvl, and inbound rule in SG, allowing this request)

- User -> private subnet
  user -> IGW -> public NACL (inbound rule in NACL, allowing this request) -> public instance SG (instance lvl, and inbound rule in SG, allowing this request) -> private NACL (inbound rule in NACL, allowing this request) -> private instance SG (instance lvl, and inbound rule in SG, allowing this request) -> resource (response) -> private instance SG

(instance lvl, and outbound rule in SG, allowing this request) -> private NACL (outbound rule in NACL, allowing this request) -> public instance SG (instance lvl, and outbound rule in SG, allowing this request) -> public NACL (outbound rule in NACL, allowing this request) -> IGW -> user

- How to attach gateways to subnets?
  -> route tables

  Route tables : bridge between gateways to the subnets

  Public subnet ->route tables-> IGW

  Private subnet ->route tables-> NAT

```
Today
=====
--VPC..virtual private cloud
--VPC and components/Arch./steps
        1.create vpc
        2.create subnet(public,private)
        3.create gateways..igw,nat
        4.route tables
        5.attach gateways to subnets via rtb
        6.create SG
        7.create nacl
        8.associate nacl to subnet and SG to resource(inst.)
```

Sure, I can explain these fundamental concepts related to networking in the context of Amazon Web Services (AWS) and similar cloud environments:

1. **VPC (Virtual Private Cloud):**
   - A VPC is a logically isolated section of the AWS cloud where you can launch AWS resources such as EC2 instances, RDS databases, and more.
   - It allows you to define your own network topology, including IP address ranges, subnets, route tables, and security settings.
   - VPCs provide control over your network environment and can be connected to your on-premises data centres or other VPCs.

2. **Subnet:**
   - Subnets are subdivisions of a VPC's IP address range. They allow you to segment your VPC into smaller, more manageable networks.
   - Each subnet is associated with a specific Availability Zone (AZ), and resources launched in a subnet are placed in the corresponding AZ.
   - Subnets can be either public (accessible from the internet) or private (not

accessible from the internet).

3. **IP Addresses (Internet Protocol Addresses):**
   - IP addresses are unique numerical labels assigned to devices on a network to identify and communicate with each other.
   - In AWS, you can allocate IP addresses to instances, load balancers, and other resources. Two types of IP addresses are commonly used: private IPs (within a VPC) and public IPs (for internet-facing resources).

4. **Security Groups:**
   - Security Groups are virtual firewalls that control inbound and outbound traffic for AWS resources.
   - They are stateful, meaning that if you allow inbound traffic from a specific IP, the corresponding outbound reply traffic is automatically allowed.
   - You can attach security groups to EC2 instances and other AWS resources to define the rules governing traffic to and from those resources.

5. **Routing Tables:**
   - Routing tables determine how network traffic is directed within a VPC.
   - Each subnet is associated with a routing table that specifies the routes for traffic leaving that subnet.
   - Routing tables contain rules that determine whether traffic should be sent locally within the VPC or forwarded to other destinations, such as an Internet Gateway or VPN connection.

6. **Internet Gateway:**
   - An Internet Gateway (IGW) is a horizontally scalable, highly available AWS resource that allows communication between instances in your VPC and the internet.
   - It serves as a gateway for traffic going in and out of your VPC to and from the internet.
   - To enable internet access for resources in a VPC, you must attach an IGW to the VPC and configure appropriate routing.

7. **Network Access Control Lists (NACLs):**
   - NACLs are network-level security devices that act as a firewall for controlling inbound and outbound traffic at the subnet level.
   - Unlike security groups, NACLs are stateless, meaning you must define both inbound and outbound rules separately.
   - NACLs are less granular than security groups but can provide an additional layer of security for your VPC.

Can we attach an internet gateway to a private subnet?
-> No

What is a NAT gateway?

-> A Network Address Translation (NAT) gateway is a networking component that allows resources in a private subnet to access the internet while keeping their individual IP addresses hidden. It acts as an intermediary, translating private IP addresses to a single public IP address when communicating with the internet, providing an extra layer of security.

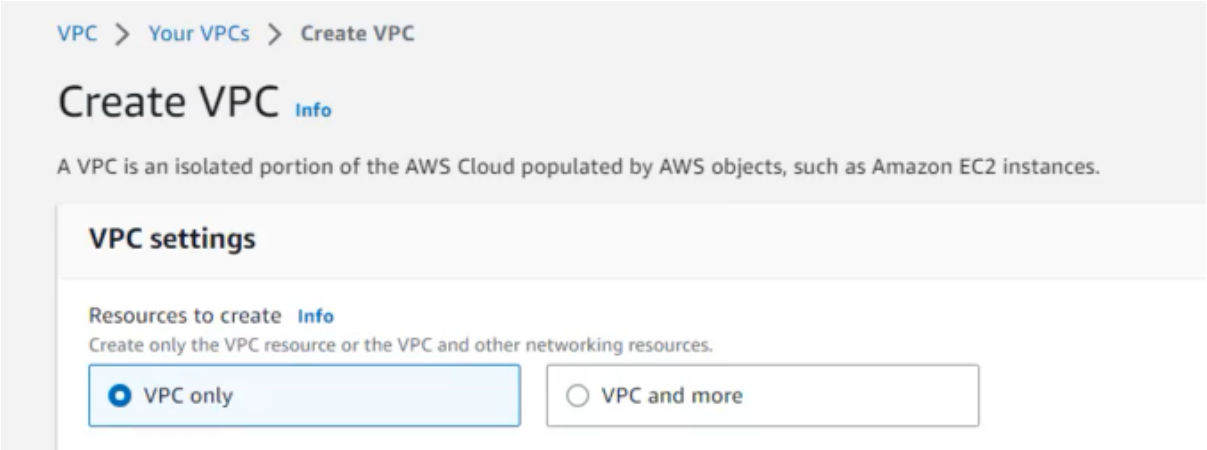
Why do we need an internet gateway at the VPC level?
-> An Internet Gateway is needed at the VPC (Virtual Private Cloud) level to enable communication between resources within your VPC and the internet. It acts as a bridge, allowing instances in your VPC to access and send data to and from the public internet. This is essential for scenarios like web servers serving content to users, downloading updates, or interacting with external APIs.

Why is a NAT gateway more secure than an internet gateway?
-> Because NAT allows traffic in one way , whereas an internet gateway allows traffic in both ways**.**

How do we differentiate private subnet and public subnet?
-> Private Subnet:
- Resources within a private subnet typically don't have direct internet access.
- They are used for sensitive services like databases or backend servers.
- Communication with the internet is usually mediated through a NAT gateway or NAT instance.
- Private subnets have route tables that direct outbound traffic to the NAT gateway for internet access.

Public Subnet:
- Resources in a public subnet can have direct internet access.
- These are commonly used for front-facing services like web servers.
- They can communicate directly with the Internet through an Internet Gateway.
- Public subnets have route tables that direct outbound traffic to the Internet Gateway.

What is VPC and VPC more?

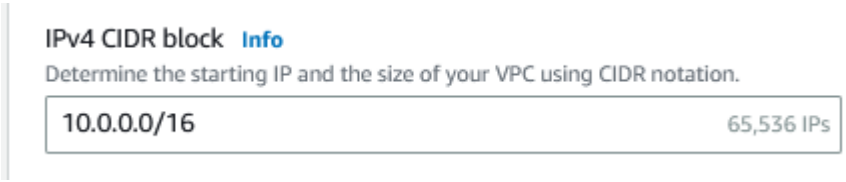


-> VPC means only VPC will get created
VPC and more means VPC as well as other components will get created.
Other components mean -> Subjects, nacl, etc

Which process should we follow ideally and why?
-> VPC only, because we can configure things on our own in VPC only. But if we select VPC and more all things are default, just one click and all things will get created.

What are the different ways we can create VPC?
-> 1)VPC
2)VPC and more
3)Terraform

What is a CIDR block?



What is 65536 IPs ?
It is the capacity.
10.0.0.0/16 => (32-16) -> 2 pow 16 => 65536

```
ex: 10.0.0.0/8..32-8....2pow24..16M
    10.0.0.0/16..32-16..2pow16..65536
    10.0.0.0/24..32-24..2pow8...256
```

Only 10.0.0.0/16 (this is class b type), 10.0.0.0/24 (this is class c type) is provided by cloud, 10.0.0.0/8 (this is class a type) is very big range, so no cloud provides this much CIDR range

-> CIDR block decides ip range.
The CIDR block decides how many instances can be launched in your VPC.

Again no of resources that can be deployed in the public or private subnet are decided by CICD

EXAMPLE
Your CICD block value is 16000 . Then your public + private subnet cannot deploy resources more than 16000.

Can we attach multiple NACL to the same subnet?

-> YES

Can we assign two security groups to a instance

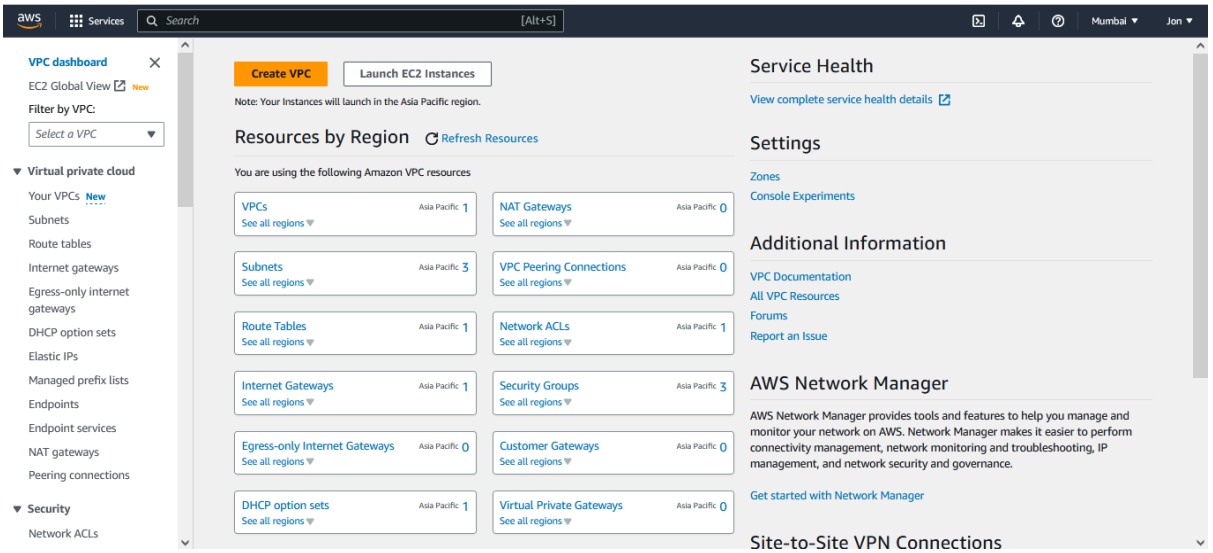
-> YES

Steps to create VPC

1.Creating VPC using VPC and more option

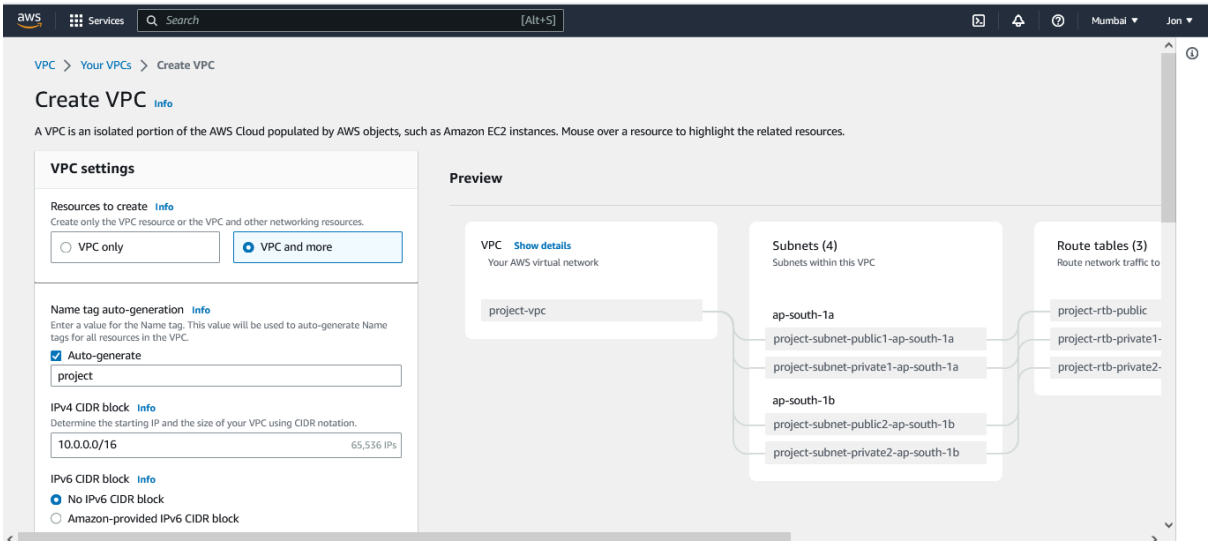
STEP 1

VPC dashboard -> Create VPC



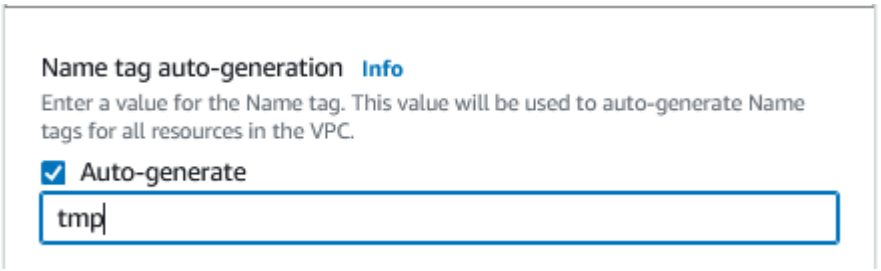
STEP 2

Create VPC ->VPC settings -> Select VPC and more



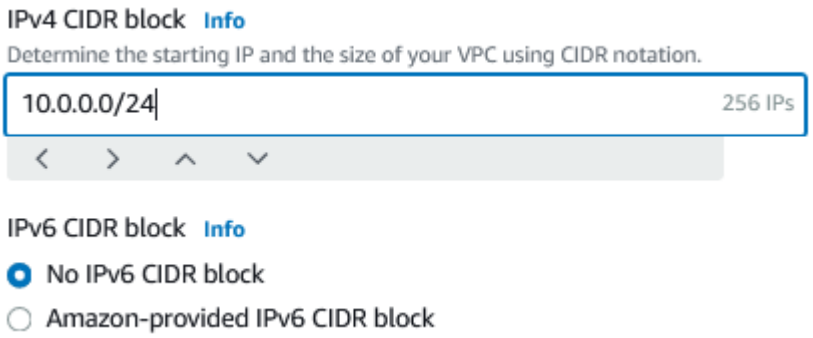
STEP 3

Give name or else you can keep auto generated



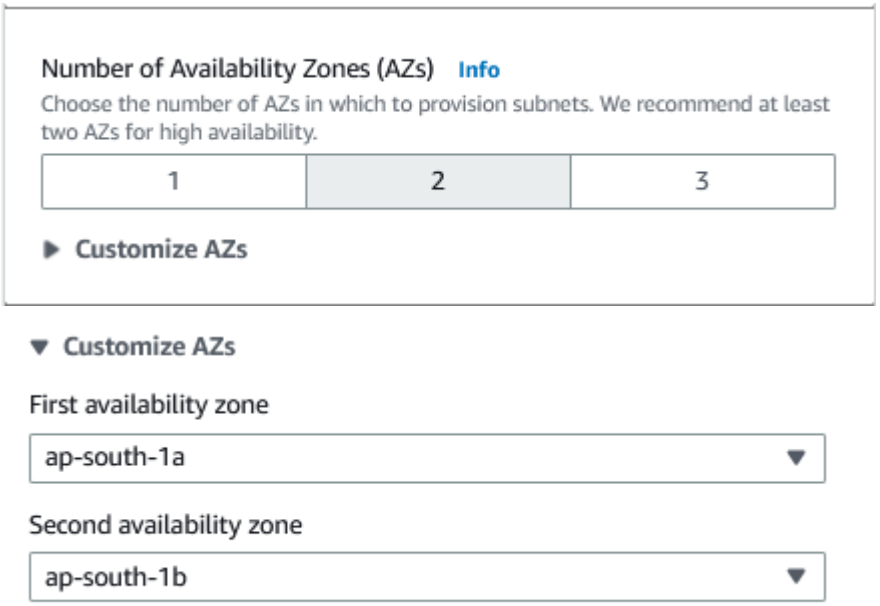
Decide CIDR value

STEP 4



*** Out Of 256 only 251 are available for us , 5 are reserved for AWS

STEP 5

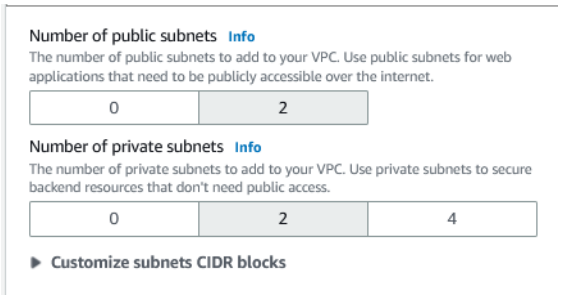


(You can even customise the availability zone)

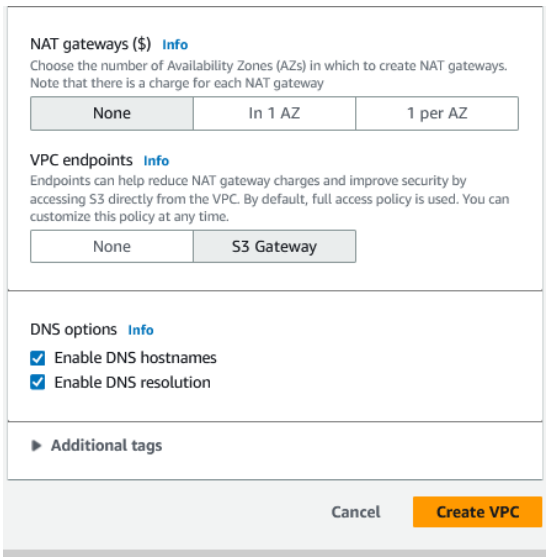
***** If you have 2 subnets then you have to select 2 availability zones. And make sure that both the availability zones are different . Different subnets have different availability zones.**

STEP 6

Select 2 public and 2 private subnets.

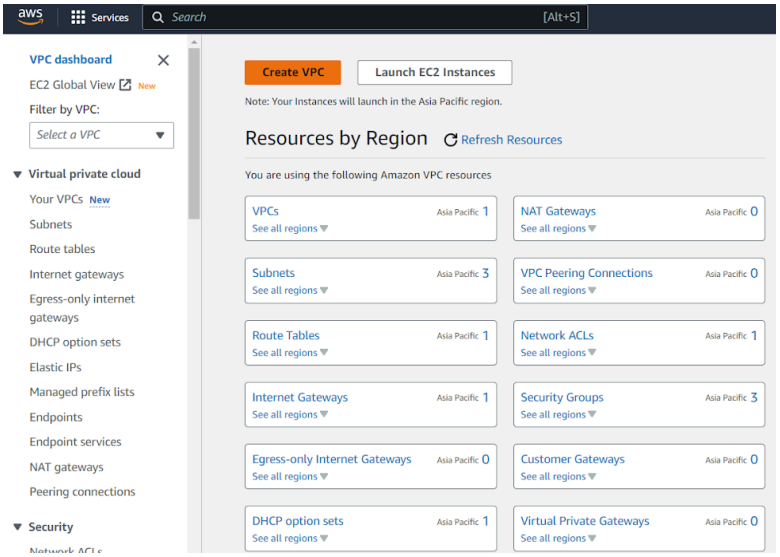


STEP 7
Click create VPC



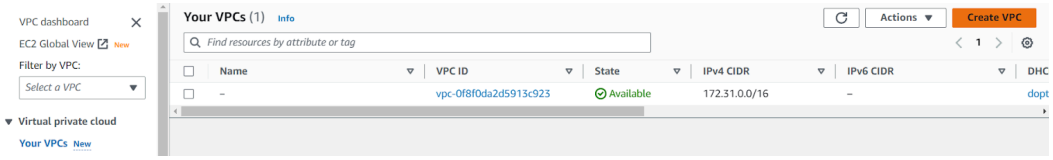
2. Creating Customised VPC

Services -> search for VPC -> create VPC



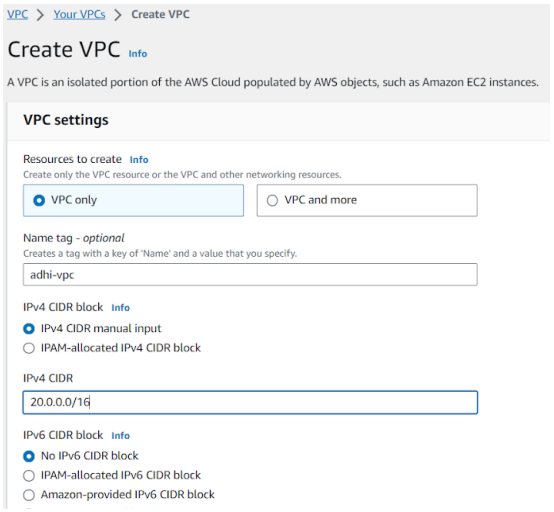
or

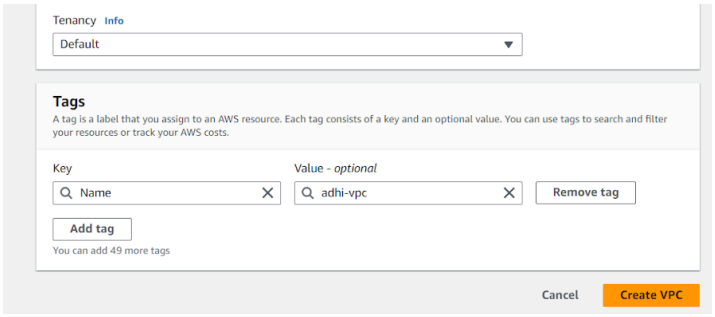
Services -> search for VPC -> Virtual Private Cloud -> Your VPCs -> create VPC



Two VPC must not have same CIDR

Services -> search for VPC -> Virtual Private Cloud -> Your VPCs -> create VPC -> VPC only

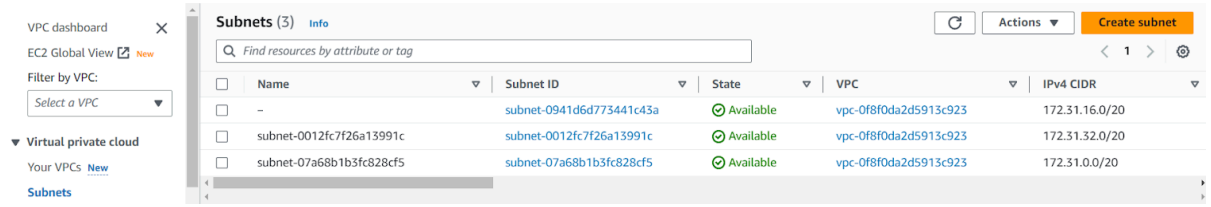




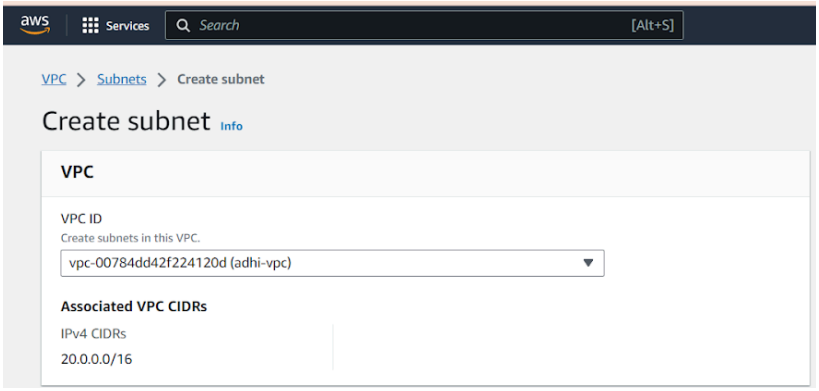
Successfully created VPC

2. Creating Subnets

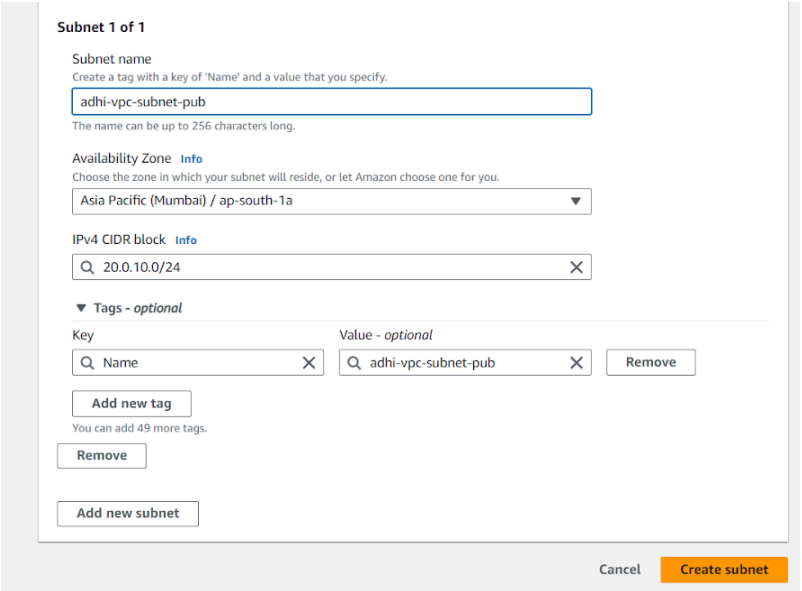
Services -> search for VPC -> Virtual Private Cloud -> Subnets -> create subnet



choosed recently created VPC

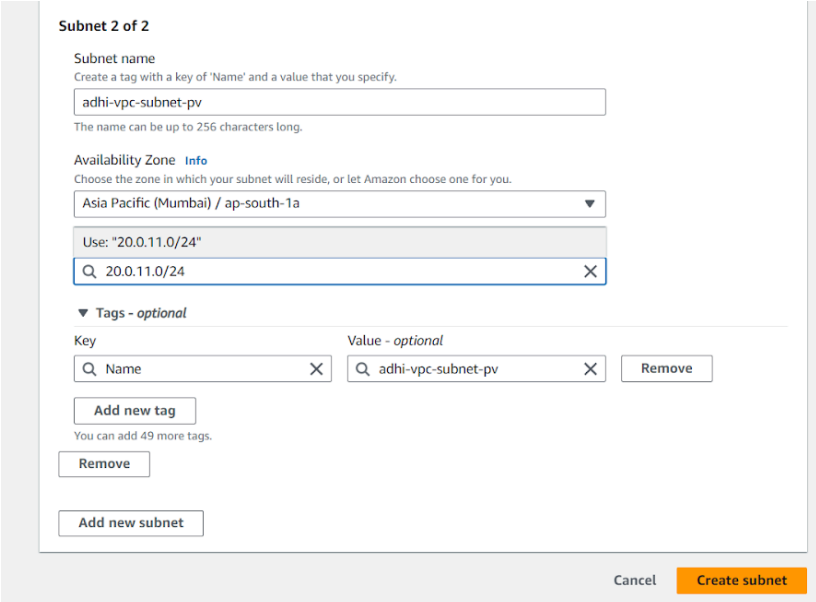


creating public subnet

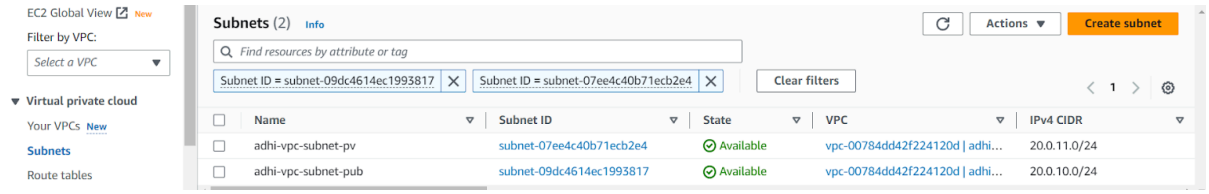


click on add new subnet

creating private subnet



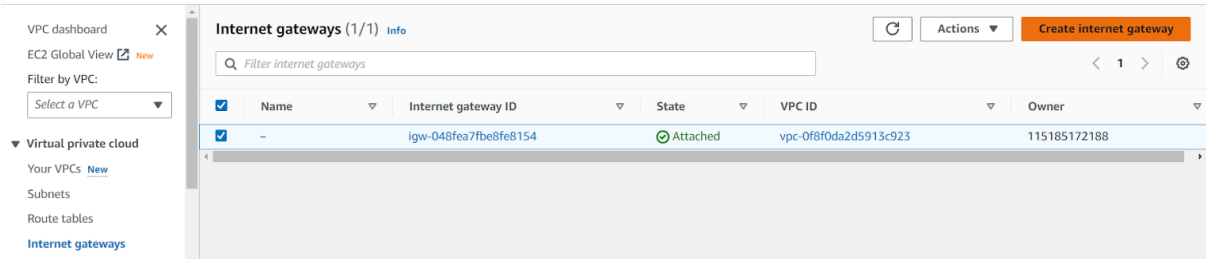
These are just names, public and private. Now these two are the same subnets, we will make them public or private later on by using gateways.

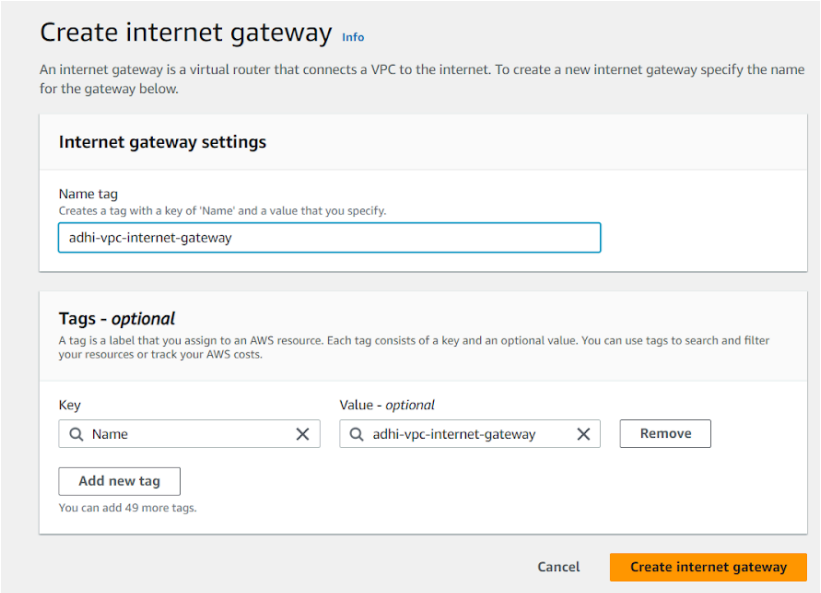


3. Creating Gateways

1. **Internet gateway for VPC**

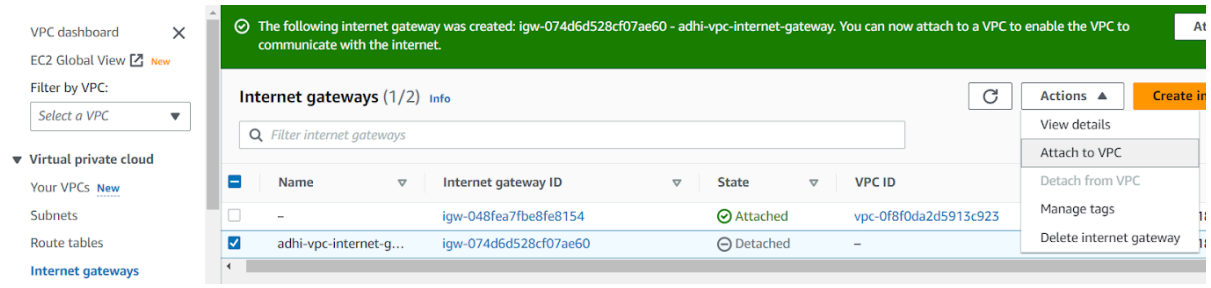
Services -> search for VPC -> Virtual Private Cloud -> Internet gateways -> create internet gateway



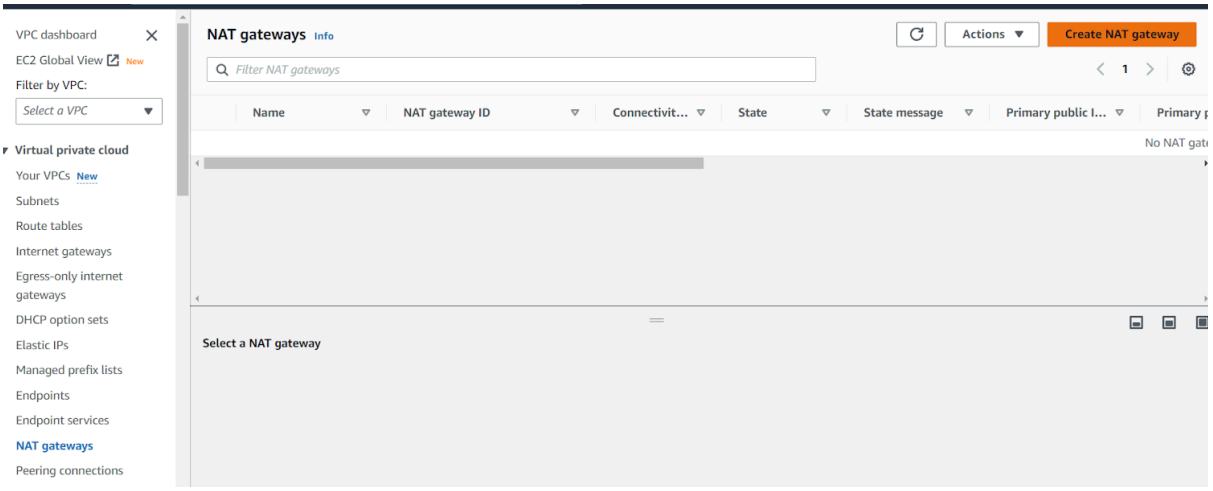


internet gateway created

now we have to attach that gateway to the VPC

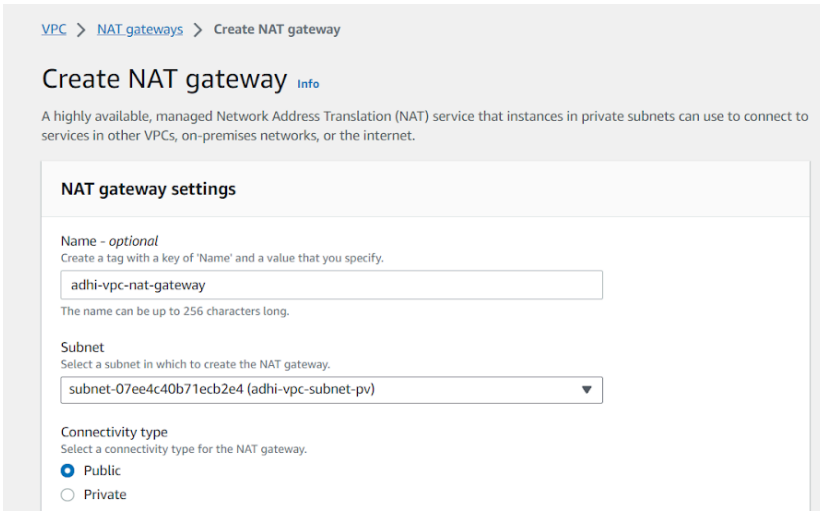


2. NAT gateway

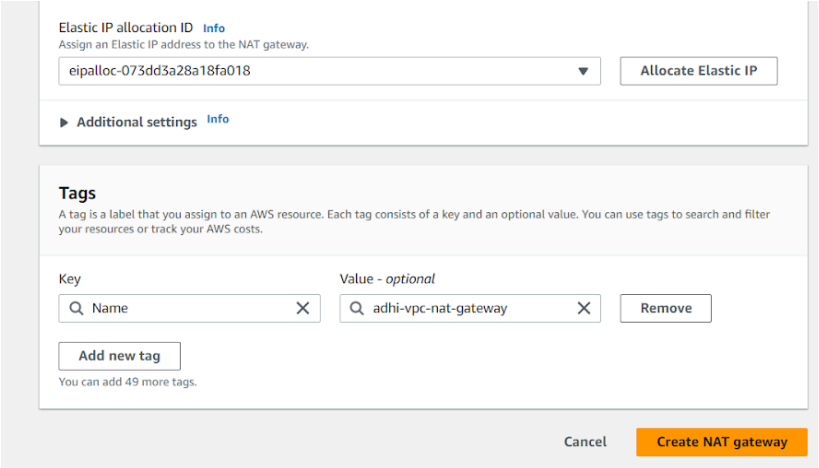


In NAT, we have option to attach the subnet while creating NAT, so here we will select

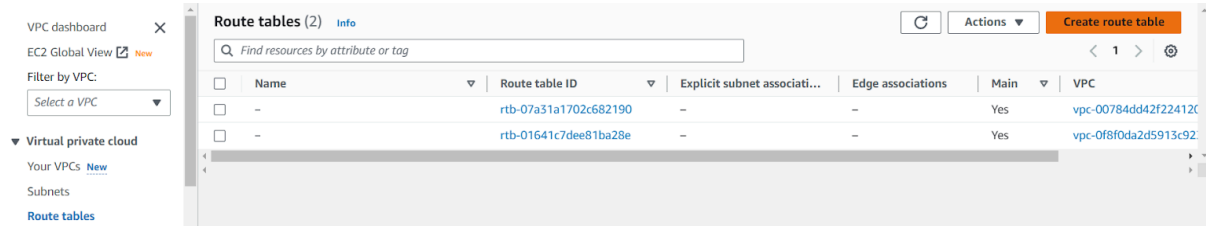
adhi-vpc-subnet-pv



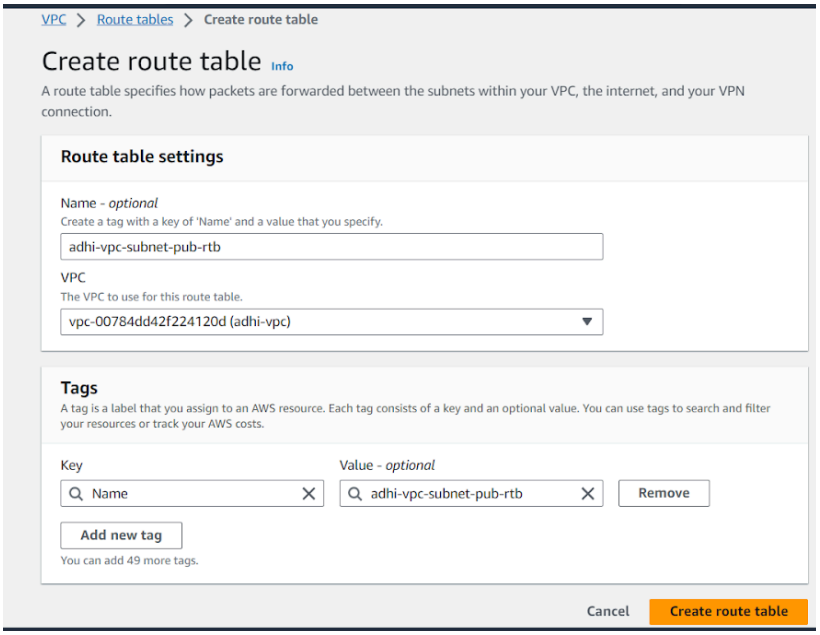
click on allocate elastic ip -> create NAT



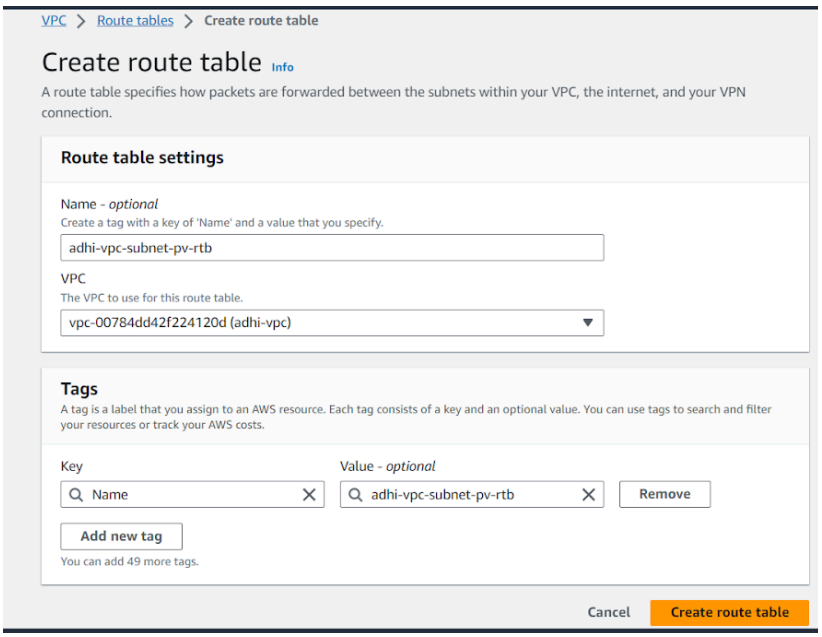
4. Creating Route tables



1. creating route table for public subnet

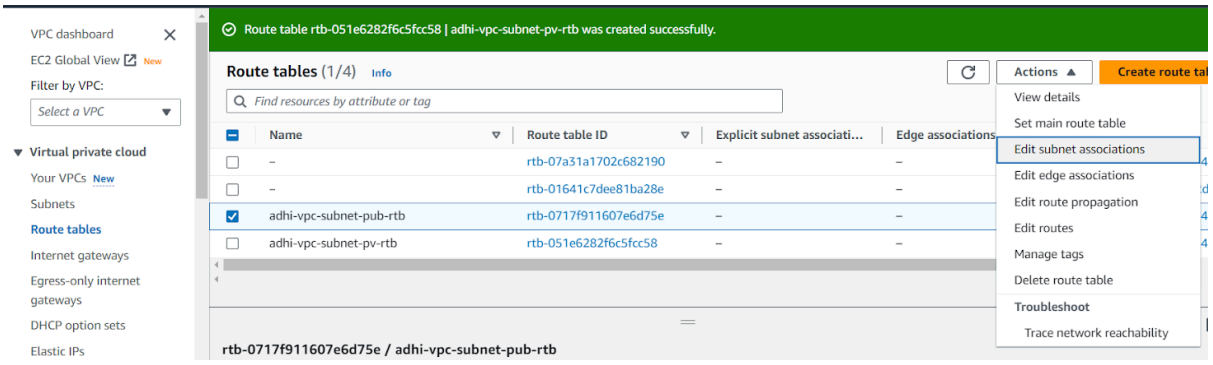


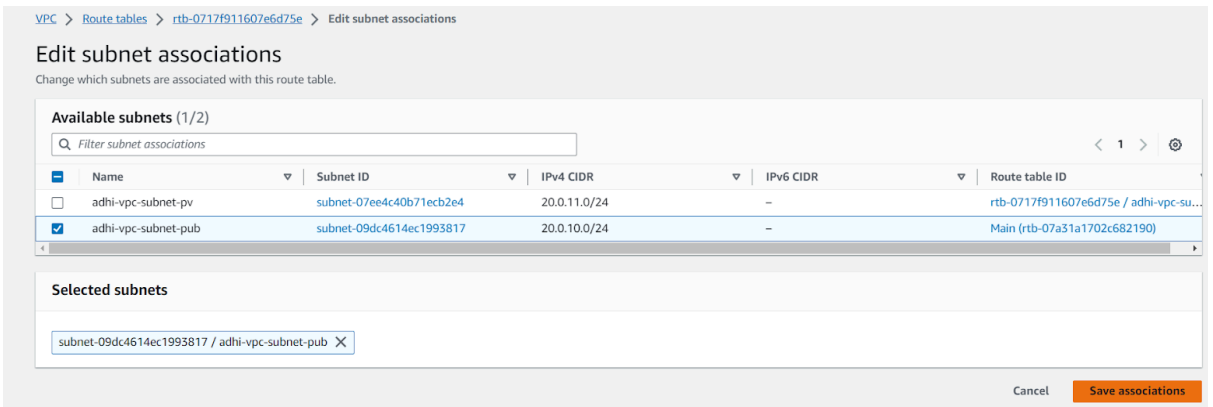
2. creating route table for private subnet



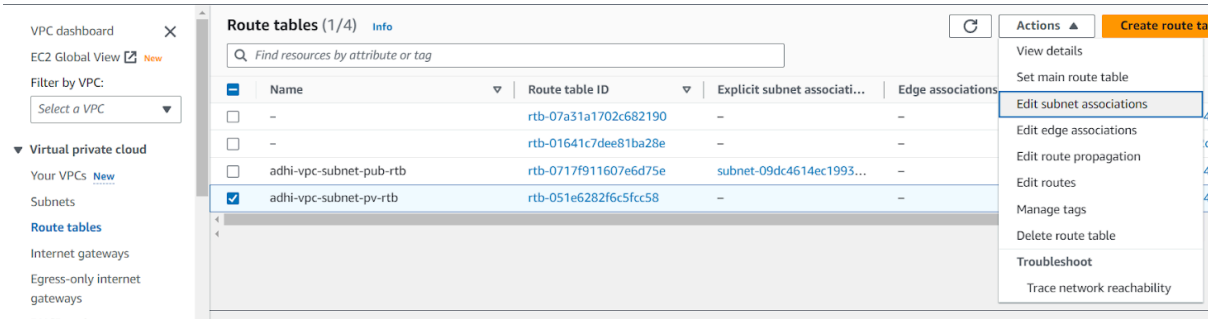
5. Attach gateways to subnet via rtb

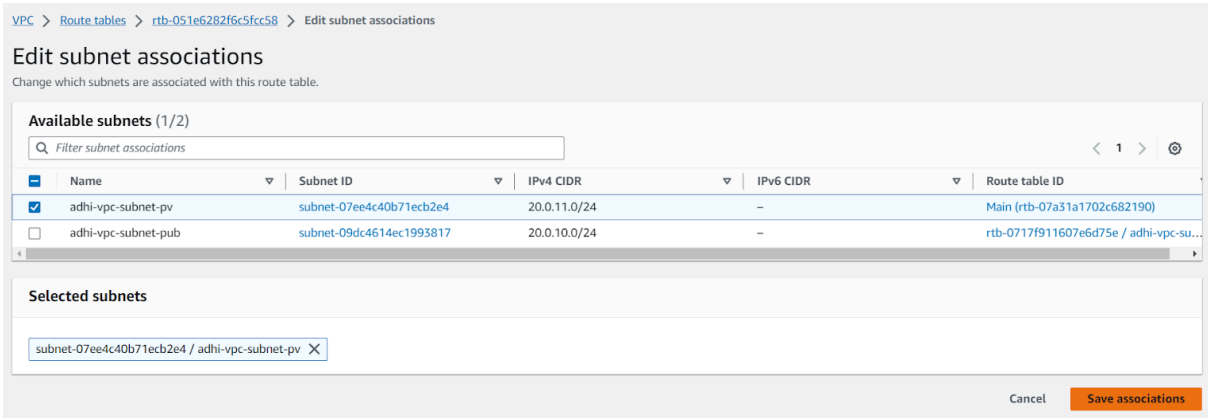
For public



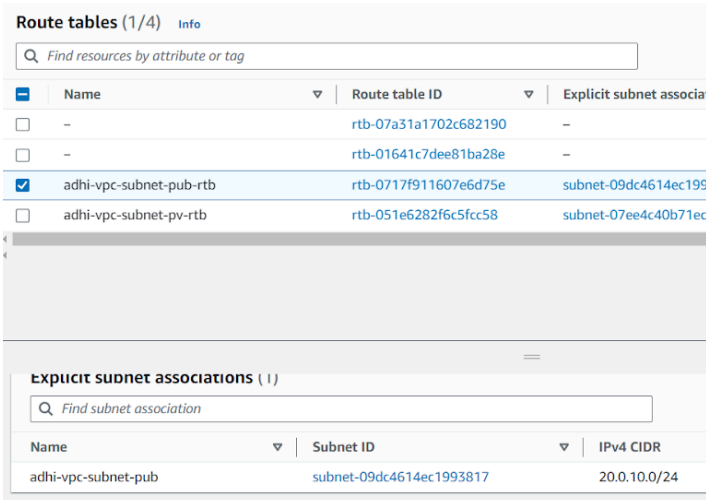


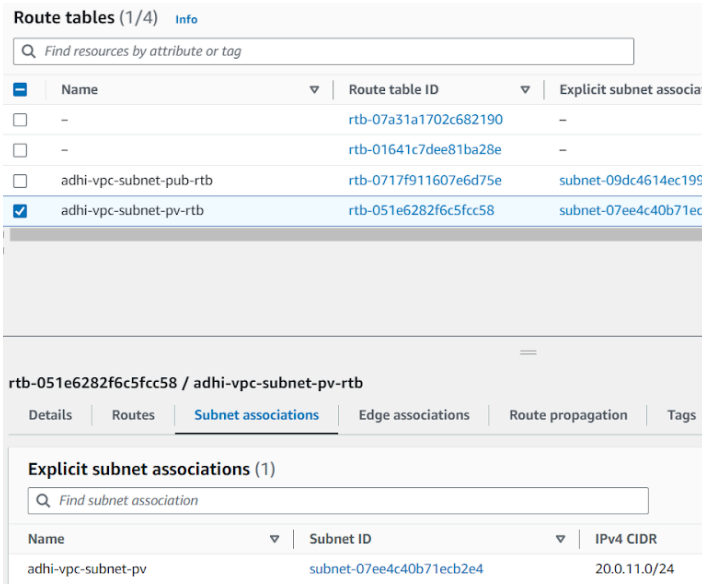
For private





it is associated, we can do this like below mentioned...

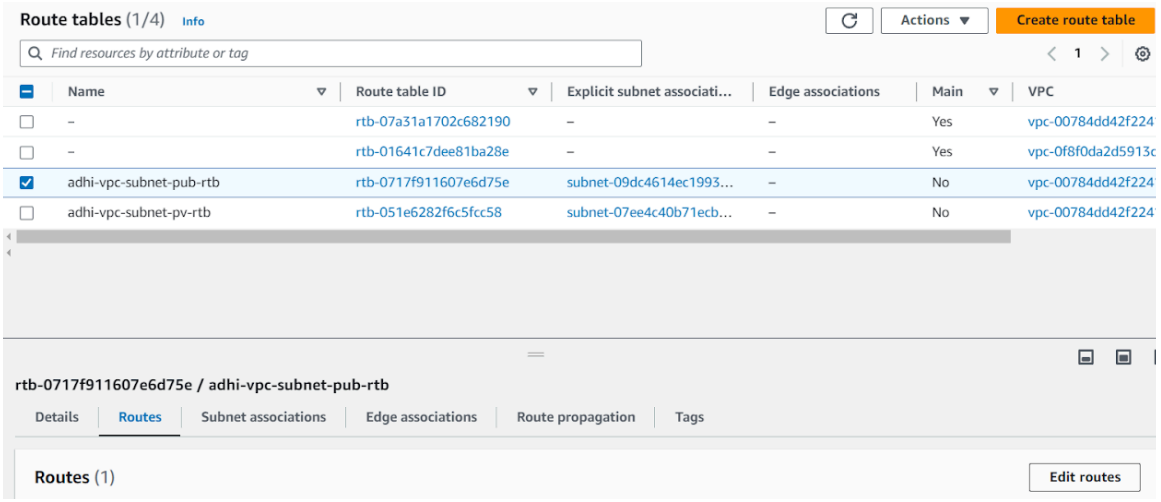


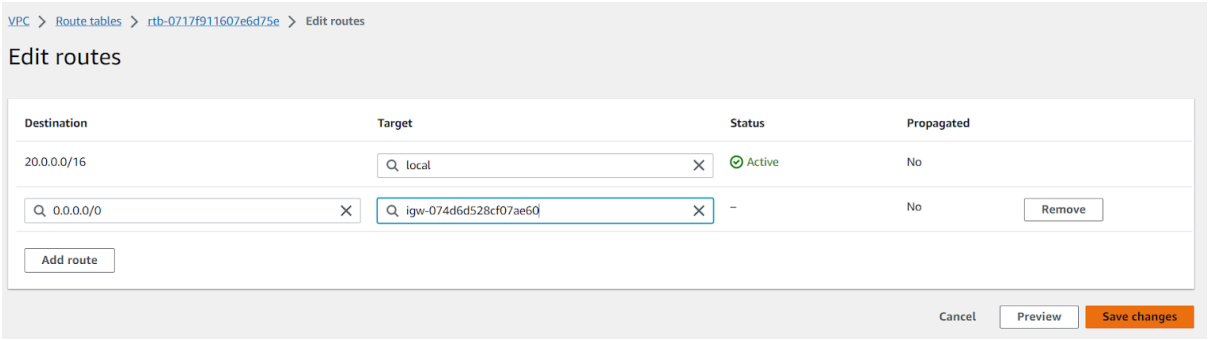


adding routes

1. for public route table

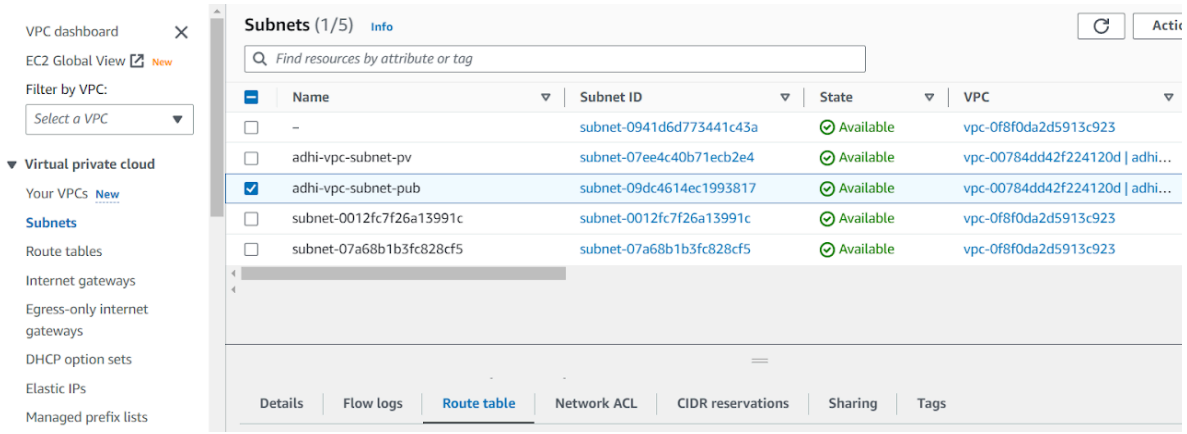
route tables -> pub rtb -> routes -> edit routes

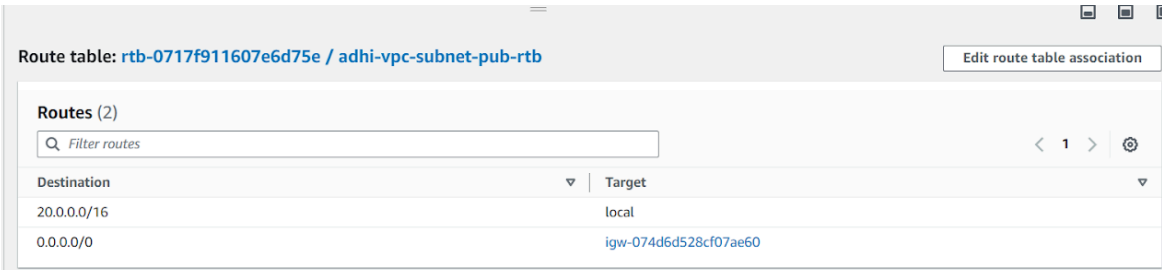




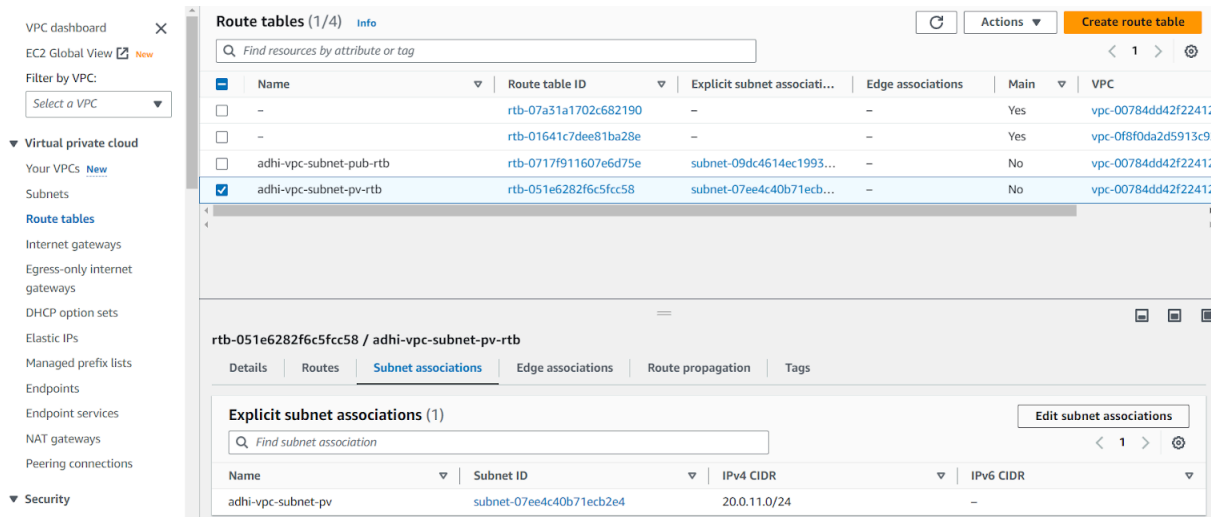
this is how we attach internet gateways to subnets

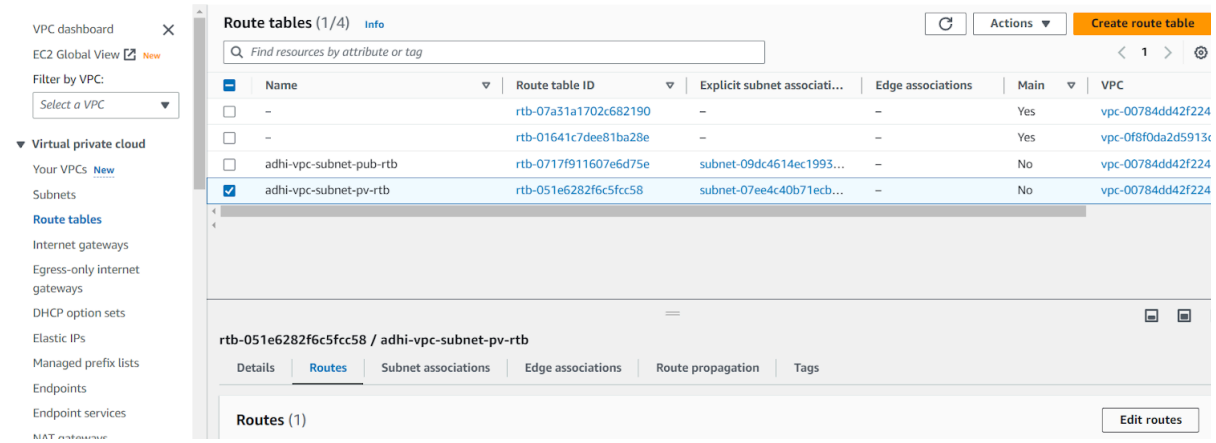
gateway attached to subnet successfully



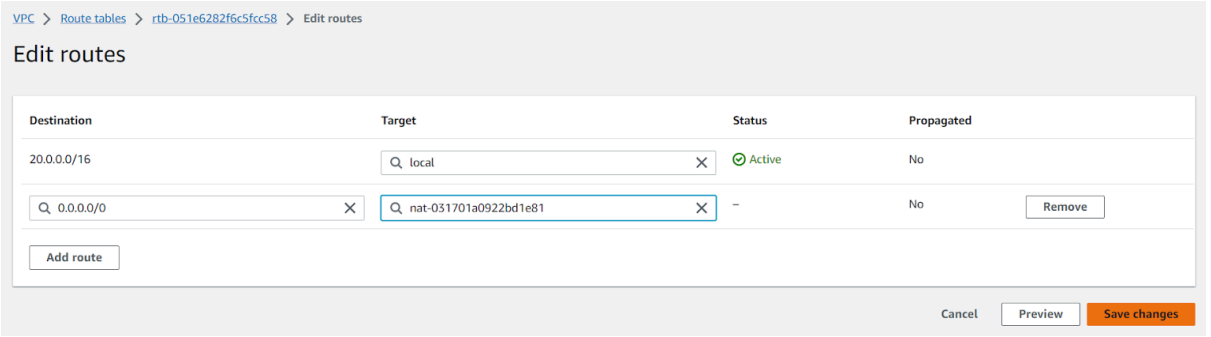


same for private rtb, we will attach private rtb to private subnet



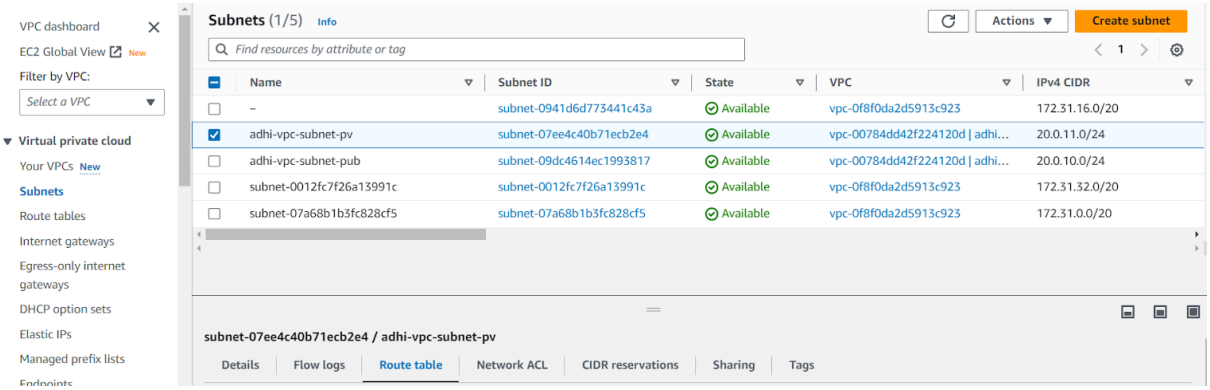


and select NAT



we can verify this like below...

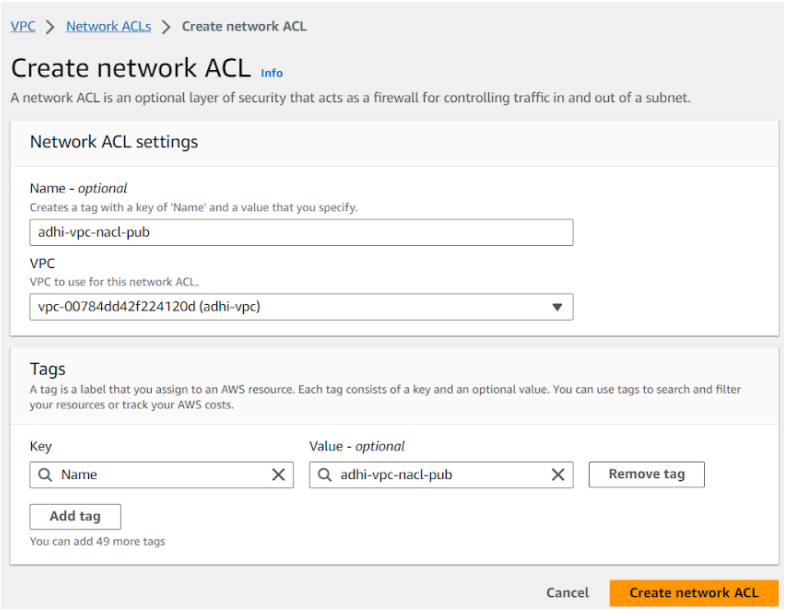
subnets -> select private subnet -> route table



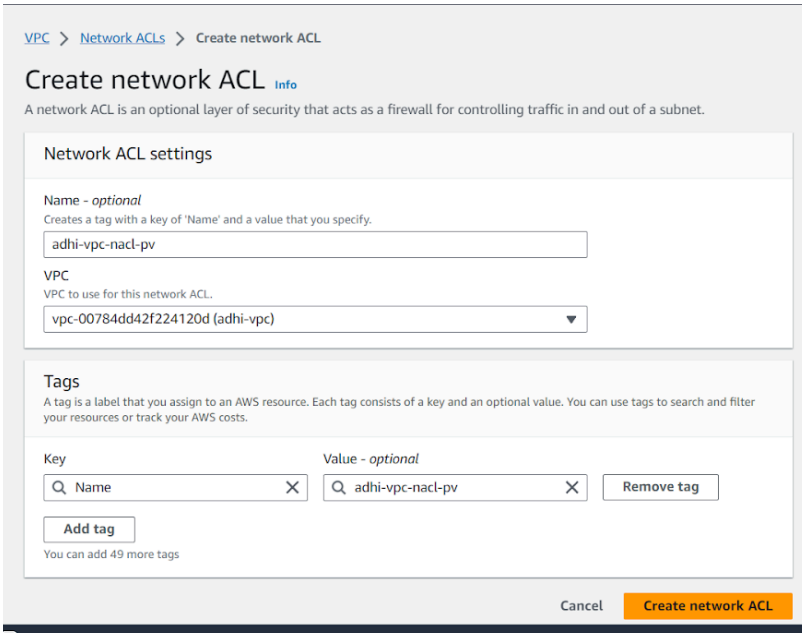
6. Create NACL

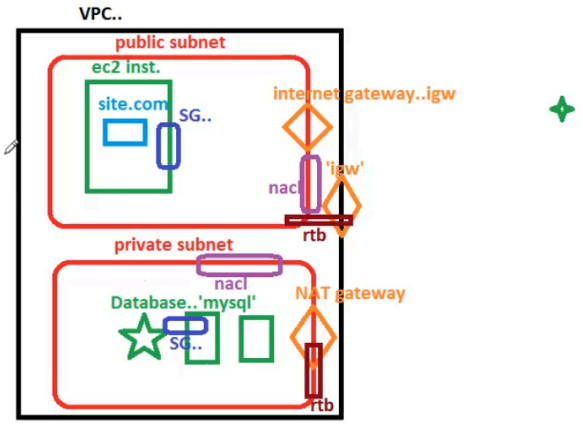
Security -> NACL -> create NACL

1. create public NACL



1. create private NACL

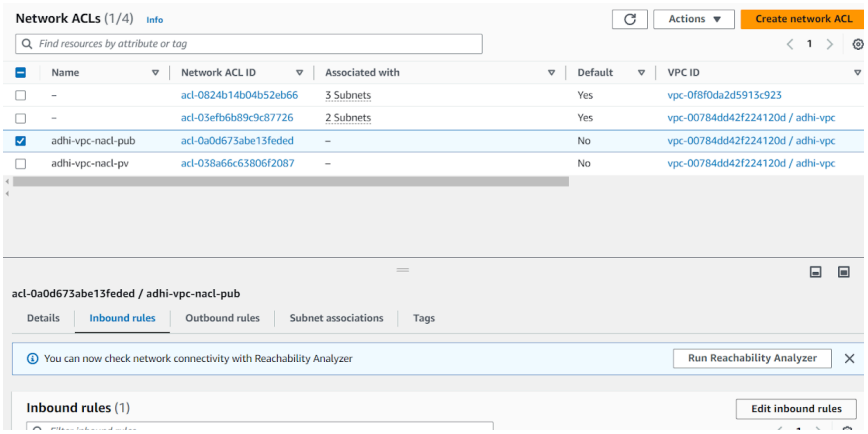




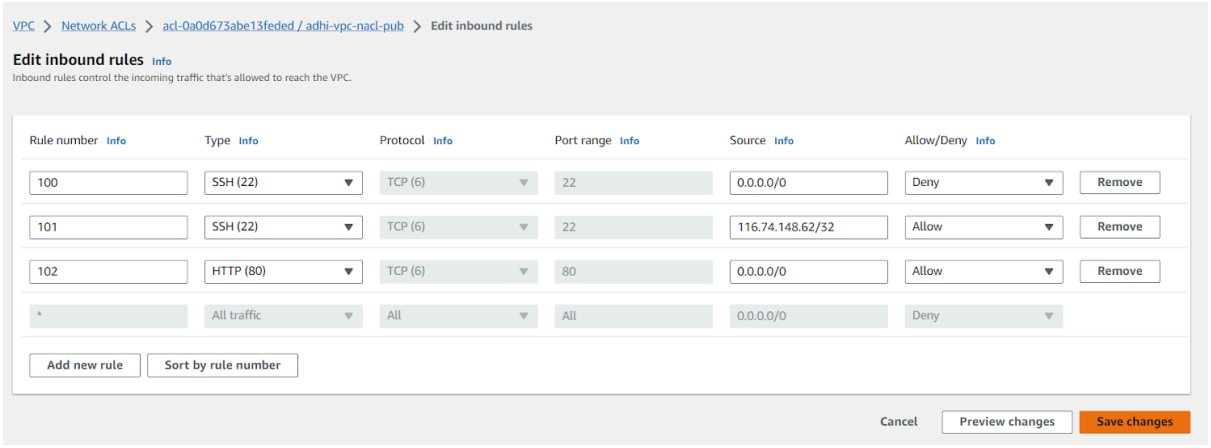
Editing inbound rules of NACL

1. **for public NACL**

select public NACL -> inbound rules -> edit inbound rules

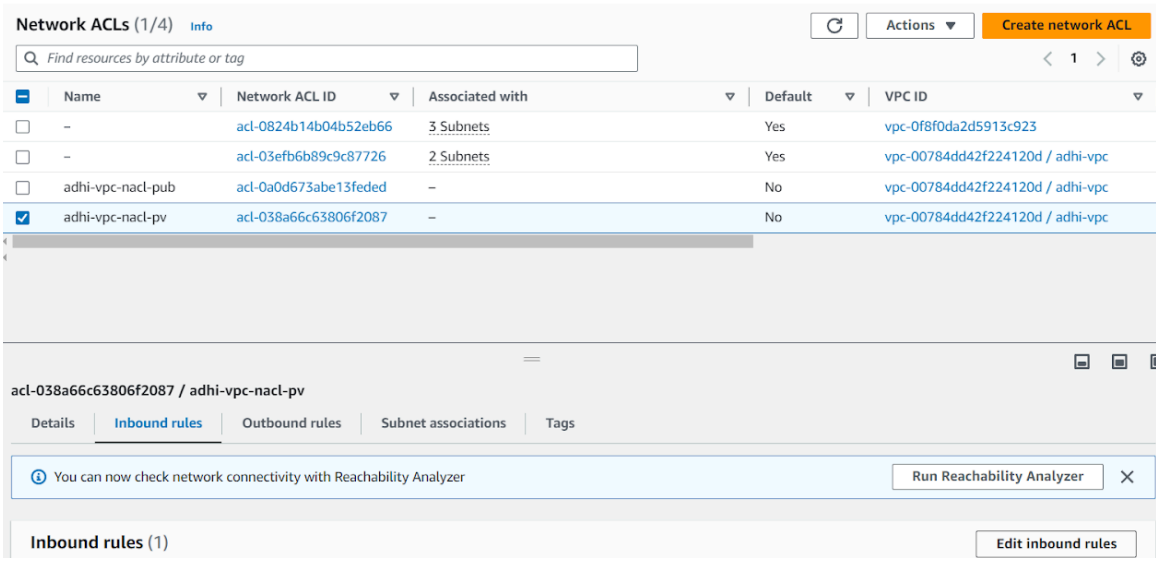


just adding some random rules

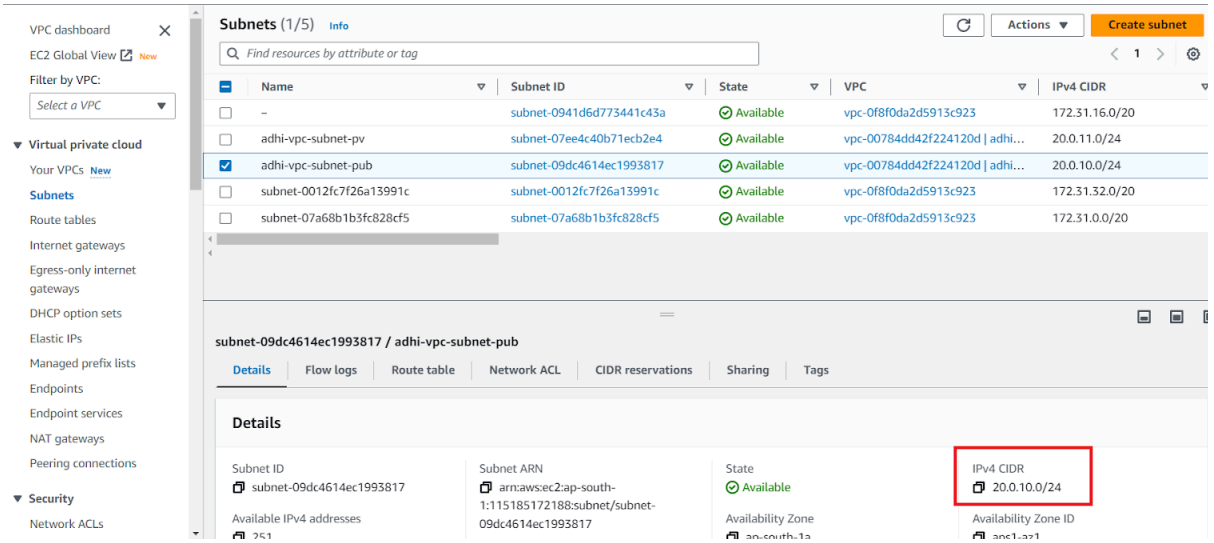


2. for private NACL

select private NACL -> inbound rules -> edit inbound rules

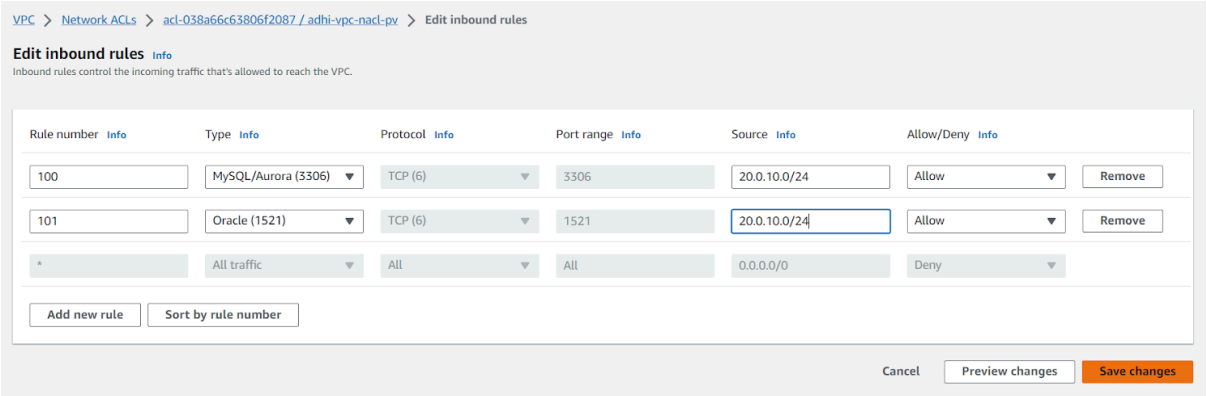


i want only adhi-vpc-subnet-pub can access my private NACL, so i will select public subnet and copy IPv4 CIDR



and paste it here.

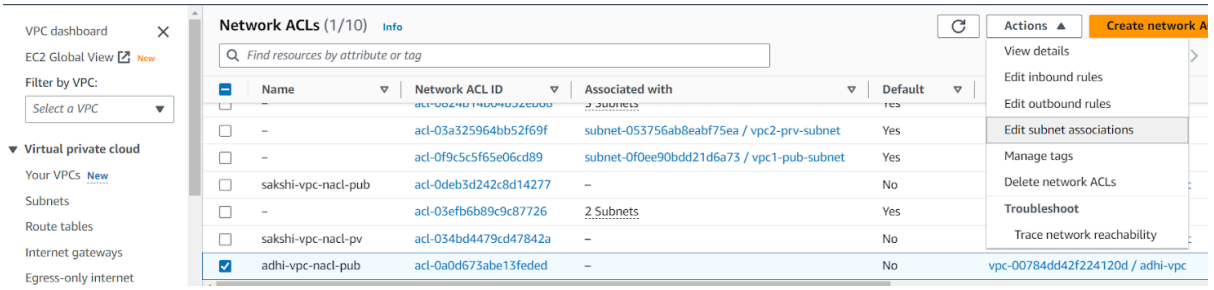
i want only my database to access my private NACL

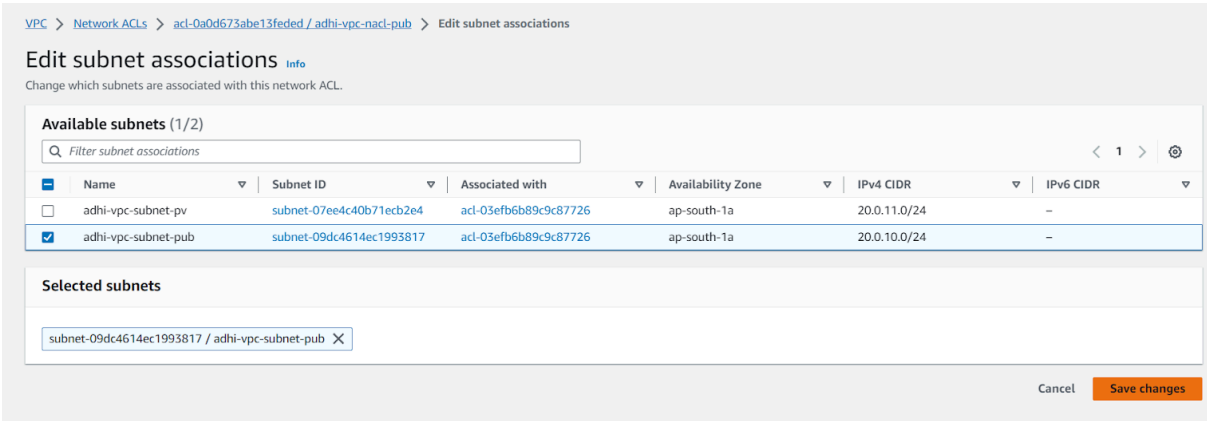


we have successfully set up NACL inbound and outbound rules

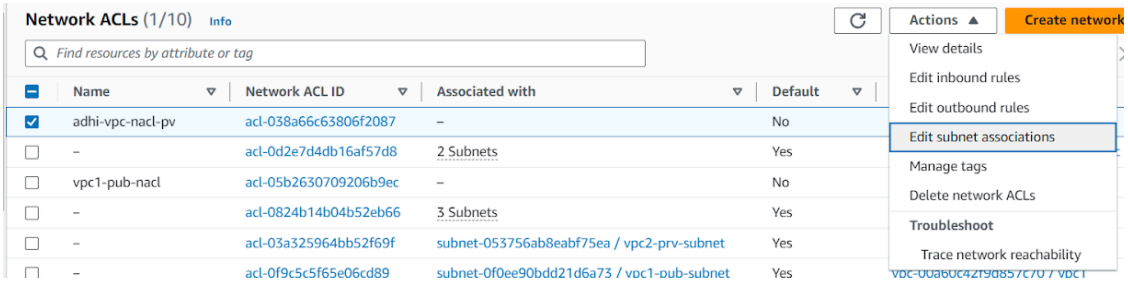
now we will associate our NACL to subnets

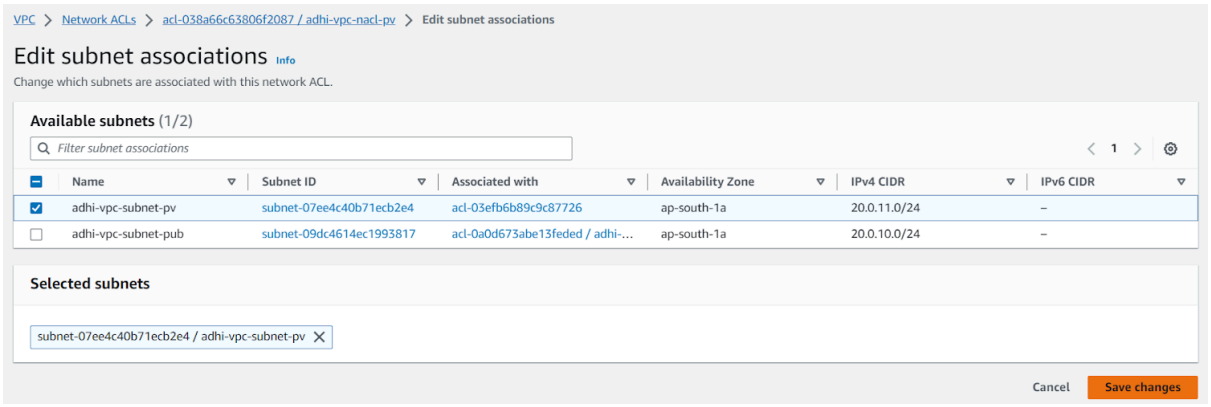
1. **for public NACL**



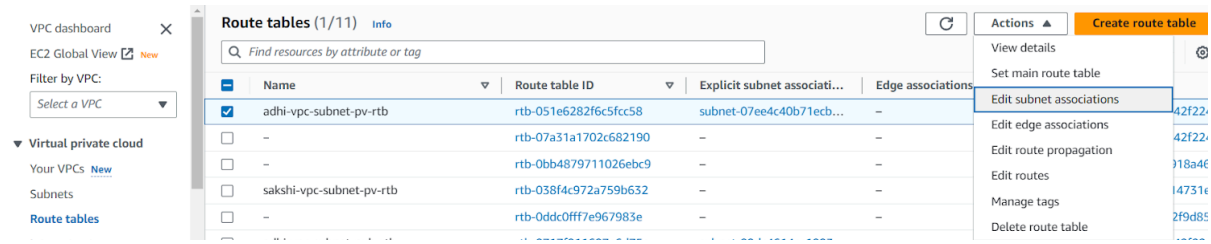


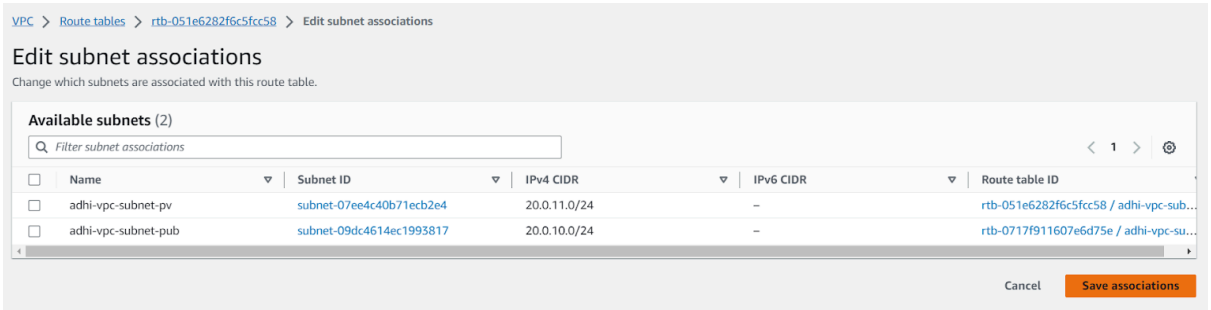
2. same for private NACL





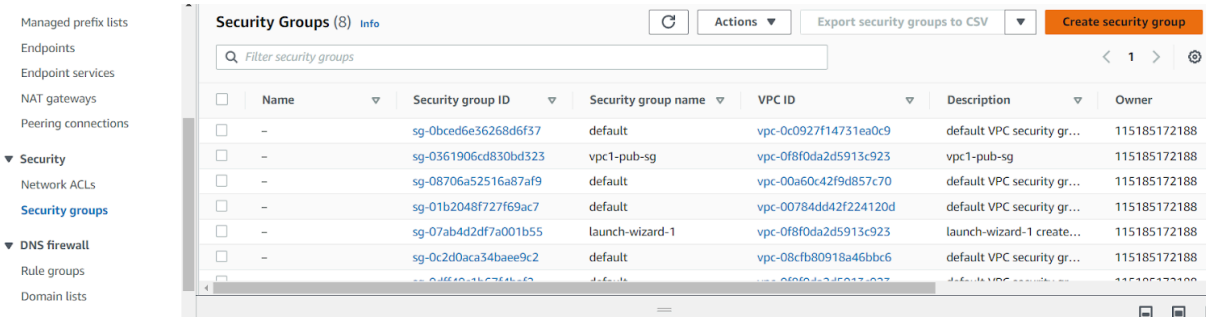
how to disassociate subnet



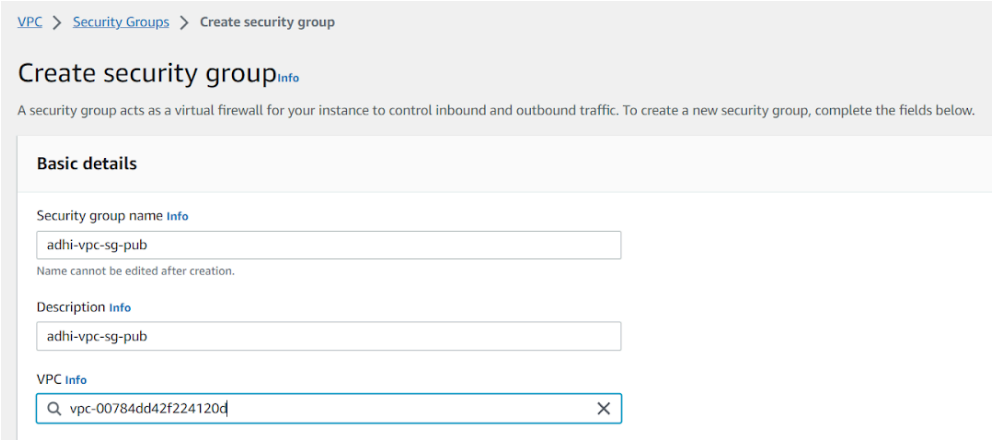


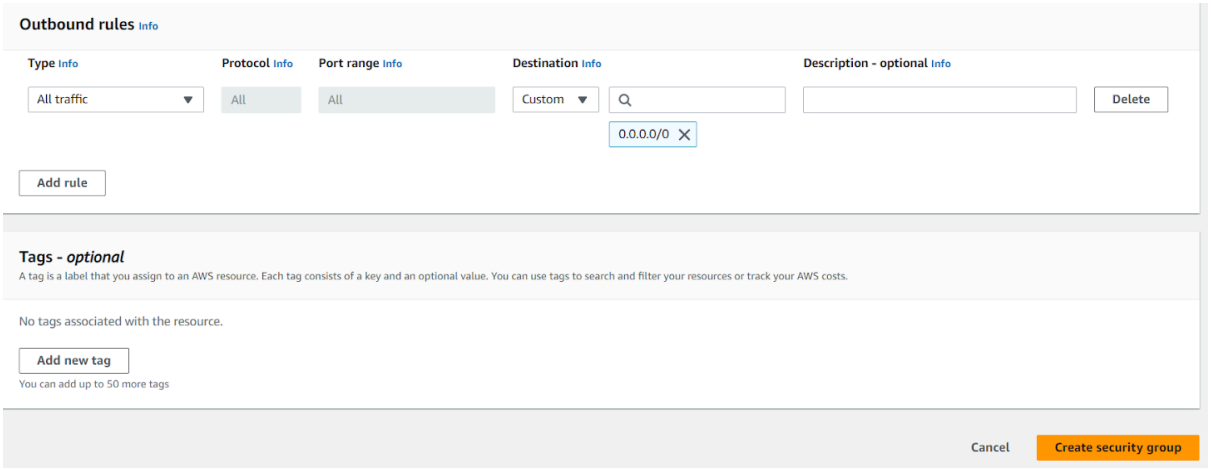
7. Create Security groups

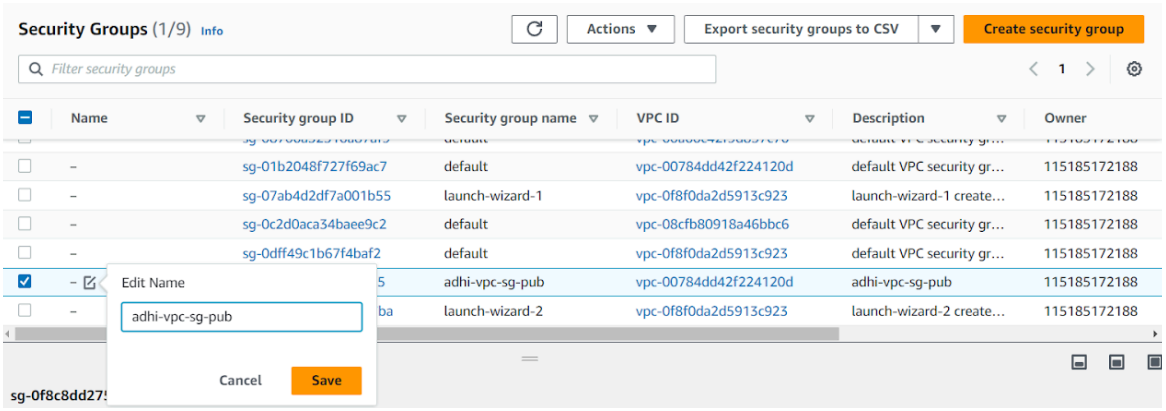
click on create security group



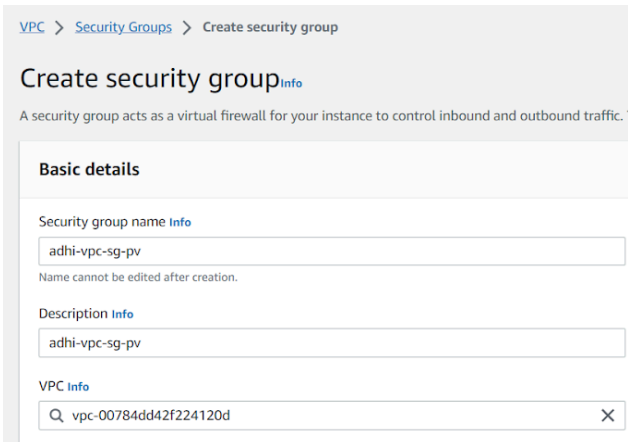
1. Public

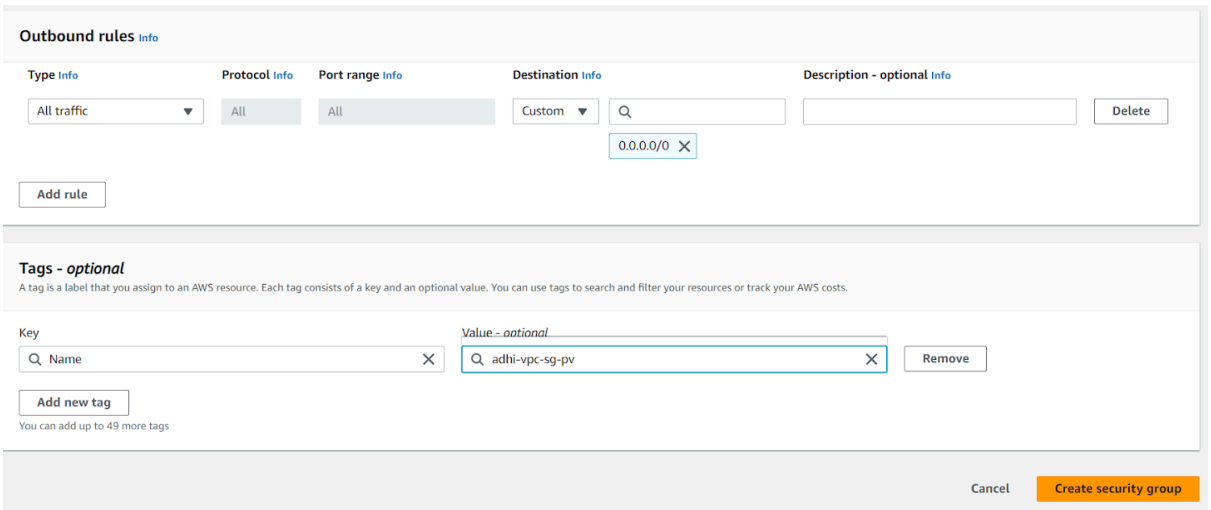





Security Groups (1/9) Info
Actions
Export security groups to CSV
Create security group
Filter security groups
Name
Security group ID
Security group name
VPC ID
Description
Owner
sg-01b2048f727f69ac7 default vpc-00784dd42f224120d default VPC security gr... 115185172188
sg-07ab4d2df7a001b55 launch-wizard-1 vpc-0f8f0da2d5913c923 launch-wizard-1 create... 115185172188
sg-0c2d0aca34baee9c2 default vpc-08cfb80918a46bbc6 default VPC security gr... 115185172188
sg-0dff49c1b67f4baf2 default vpc-0f8f0da2d5913c923 default VPC security gr... 115185172188
adhi-vpc-sg-pub vpc-00784dd42f224120d adhi-vpc-sg-pub 115185172188
launch-wizard-2 vpc-0f8f0da2d5913c923 launch-wizard-2 create... 115185172188
Edit Name
adhi-vpc-sg-pub
Cancel
Save

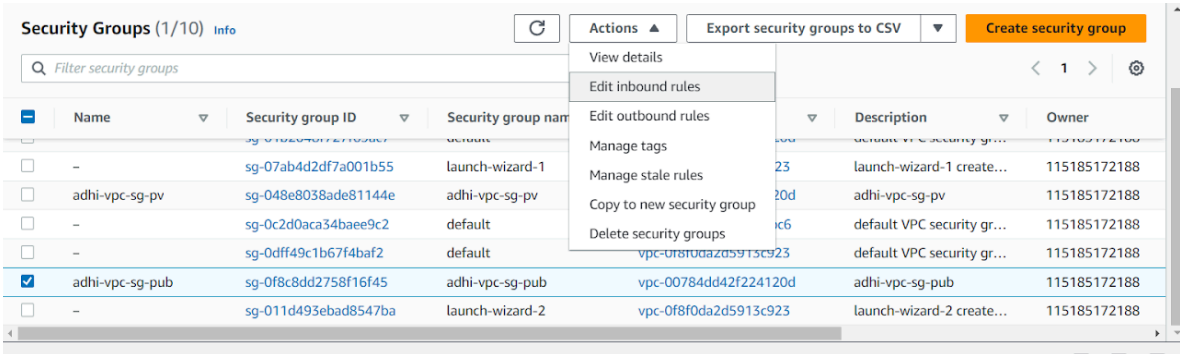
1. Private

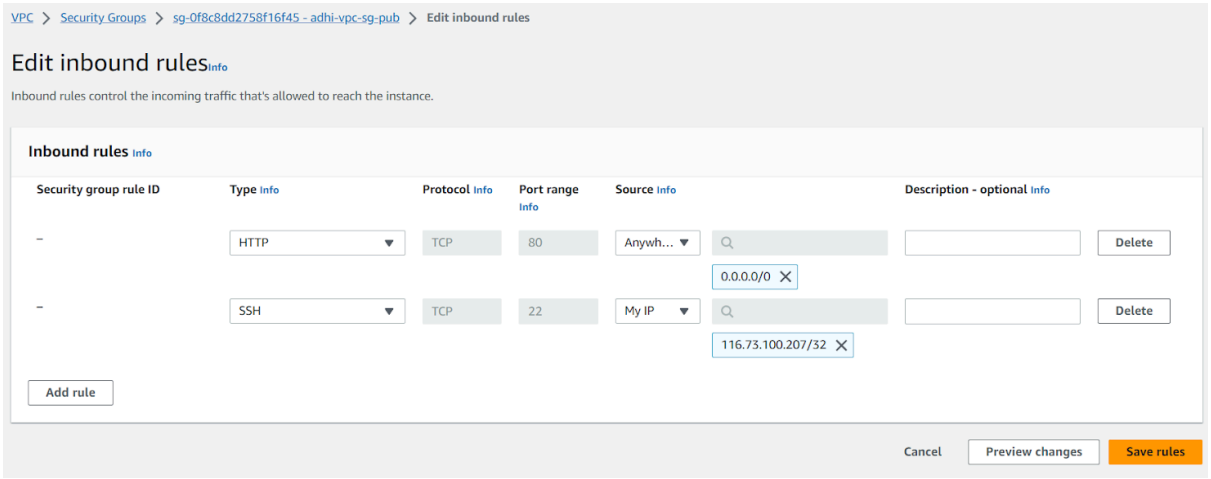

VPC > Security Groups > Create security group
Create security group Info
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.
Basic details
Security group name Info
adhi-vpc-sg-pv
Name cannot be edited after creation.
Description Info
adhi-vpc-sg-pv
VPC Info
vpc-00784dd42f224120d


Outbound rules Info
Type Info
Protocol Info
Port range Info
Destination Info
Description - optional Info
All traffic
All
All
Custom
0.0.0.0/0
Delete
Add rule
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
Name
adhi-vpc-sg-pv
Remove
Add new tag
You can add up to 49 more tags
Cancel
Create security group

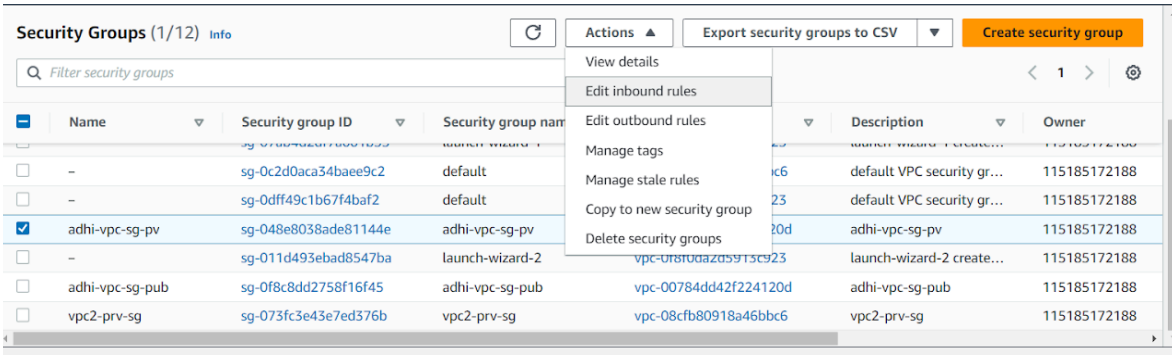
now we will change inbound rules

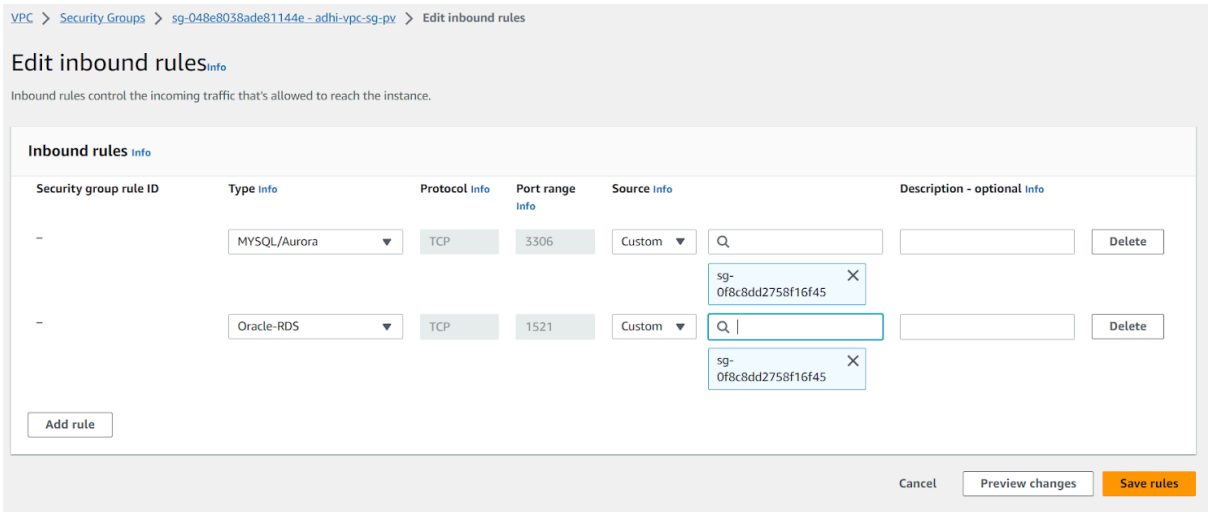
1. public





2. private





here, in source, we have added security group of public subnet, in source field

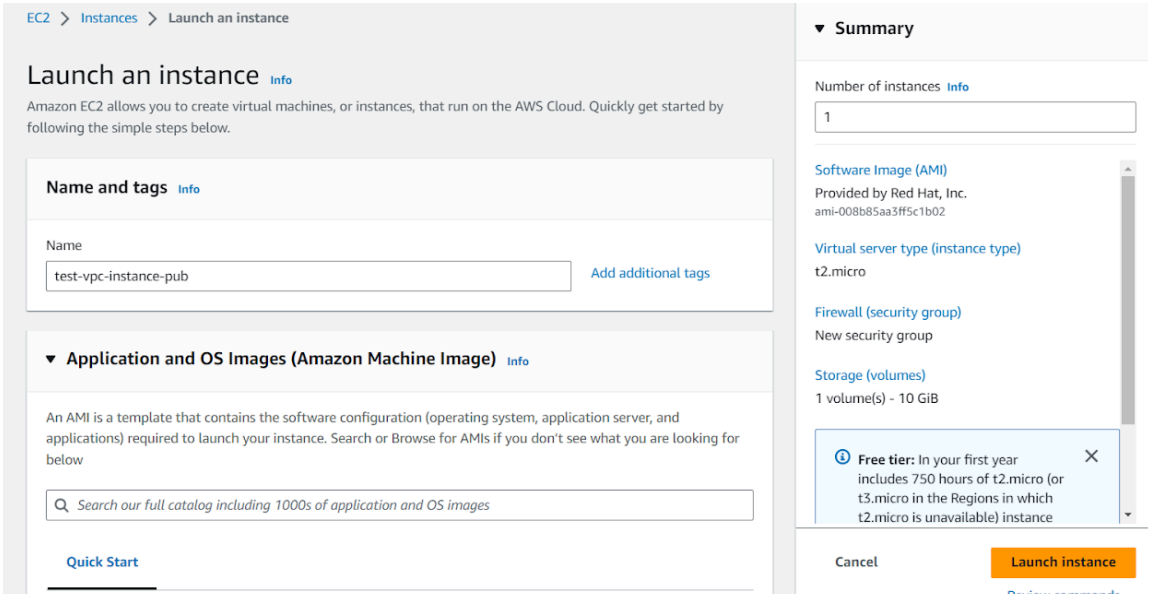
8. Associate NACL to subnet and SG to resource

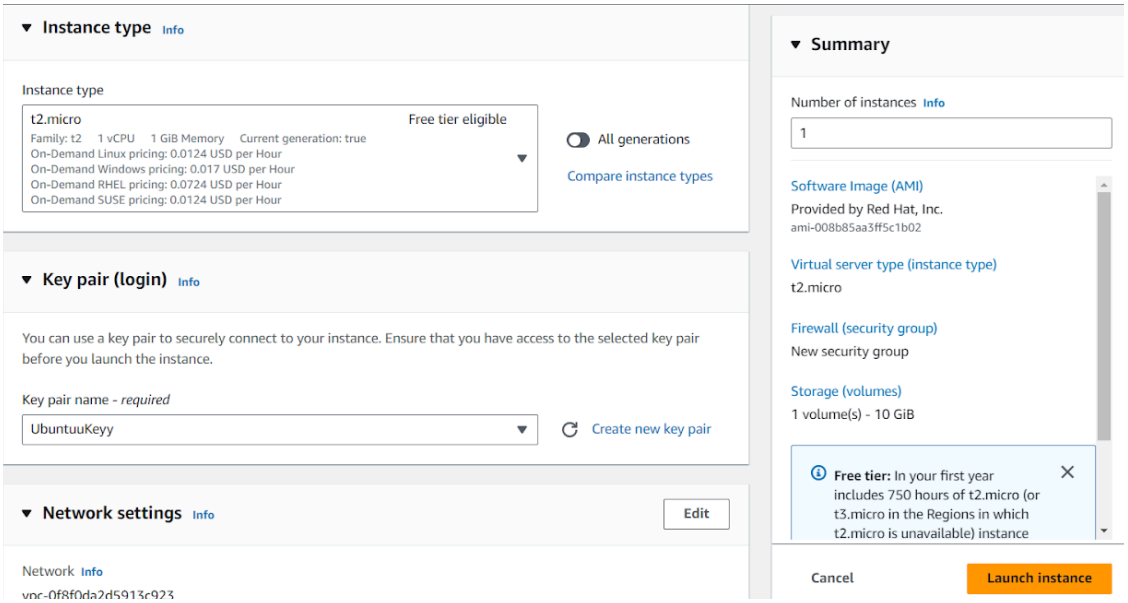
We have already associated NACL to subnet in step 6

And to associate SG to resource, we have to launch the instances into our custom VPC and then associate SG to resource

Go the EC2 -> Launch instance

1. Public





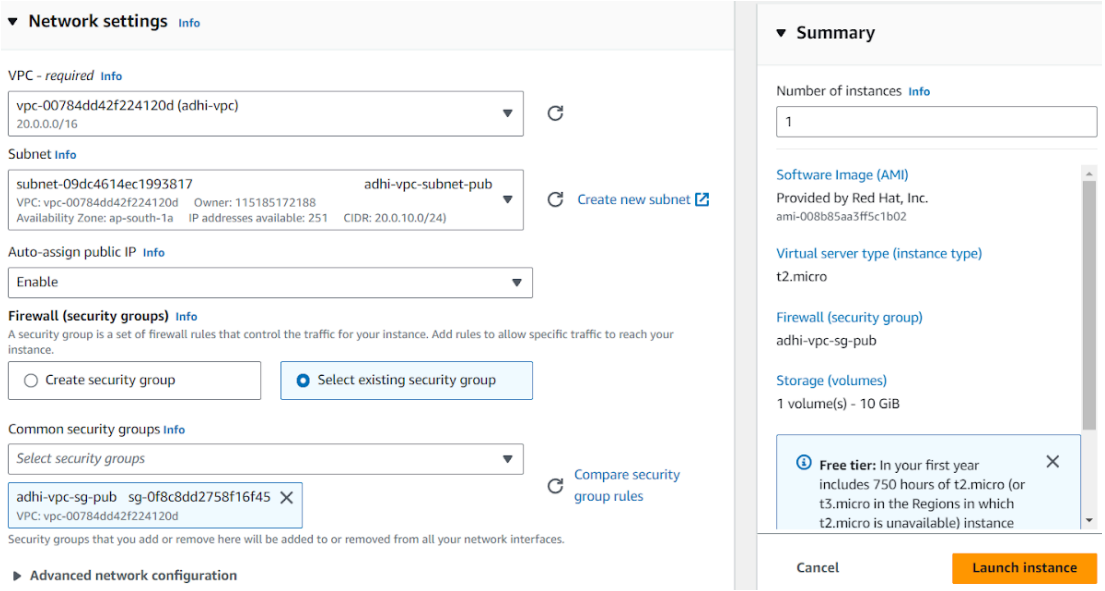
Network settings -> Edit

VPC : adhi-vpc

Subnet : adhi-vpc-subnet-pub

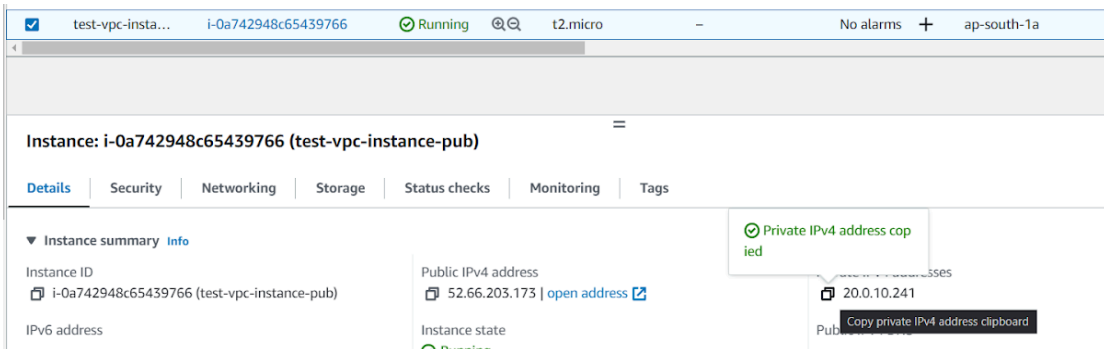
Auto-assign public ip : Enable

Firewall : Select existing security group -> adhi-vpc-sg-pub -> launch instance



Availability zones of instance totally depend upon the zones of the subnet, we can not change the availability zones of the instance while creating. While creating an instance, when we select the subnet, then the same zone is applicable for the instance too.

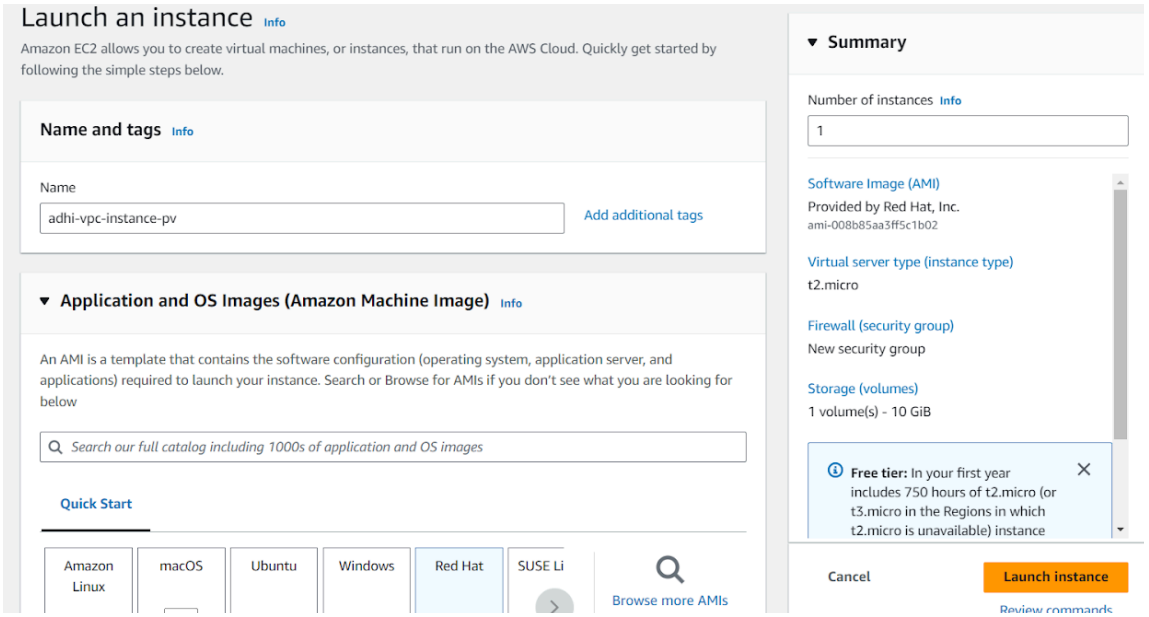
Private ip is in the range of CIDR of public

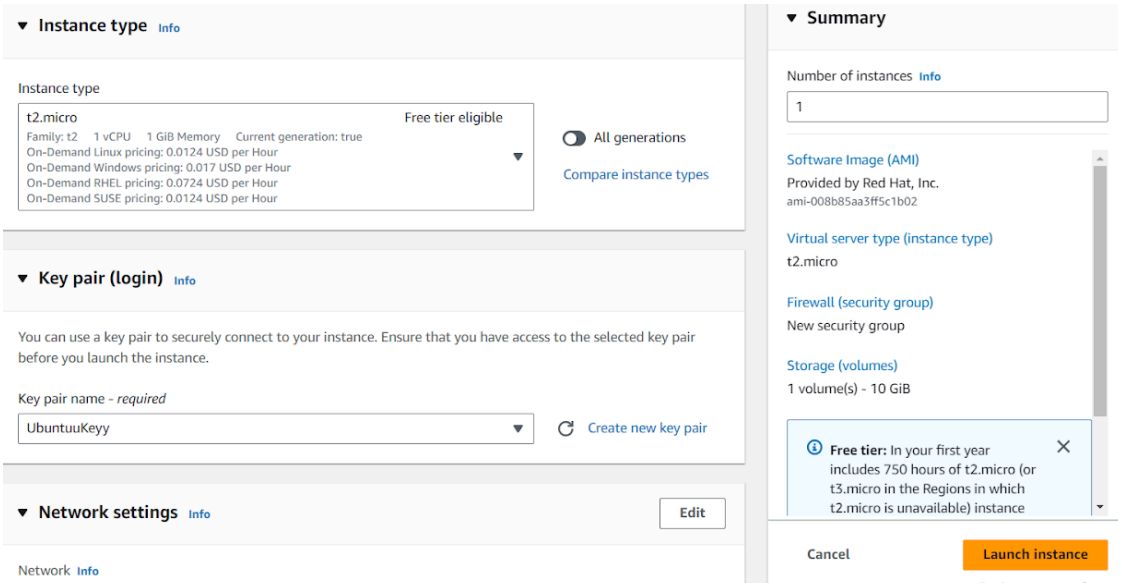


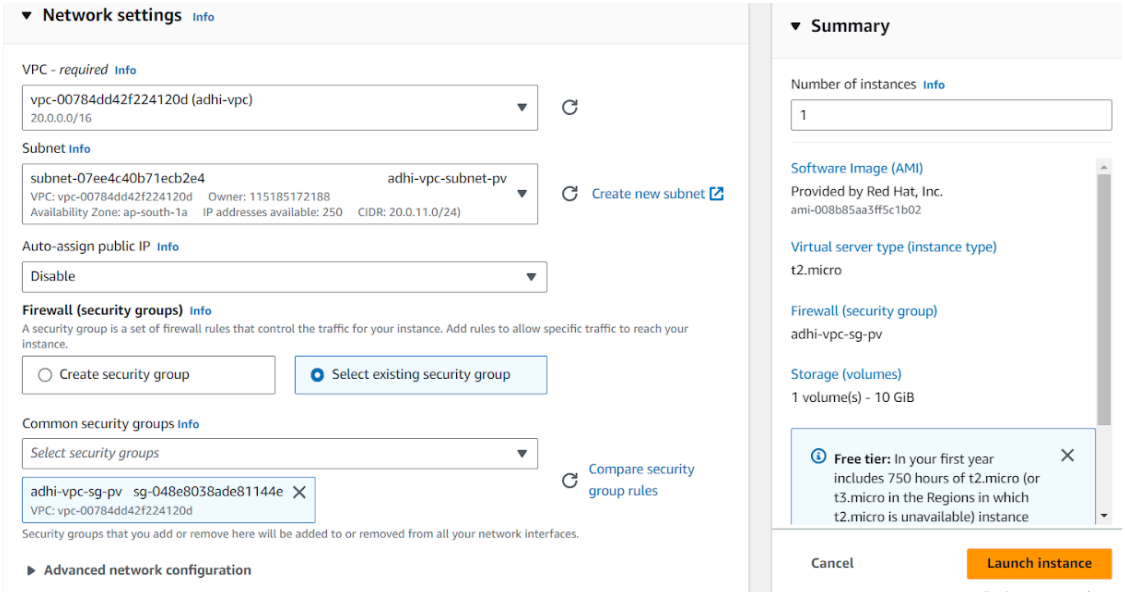
we can cross check everything for this instance now, out instance is created in our vpc, subnets, and in our security group.

1. Private

EC2 -> Instances -> Launch an instance







click on **Launch instance**