VPC:

VPC is the virtual networking environment for your AWS account. It is isolated from other virtual networks in AWS cloud, giving you control over a virtual networking environment. The main components of VPC:

Subnets - Divide your VPC into smaller networks. Subnets can be public or private:

- **Public Subnets**: Accessible from the internet.
- **Private Subnets**: Not directly accessible from the internet.

Route tables - Control the routing of traffic within your VPC.

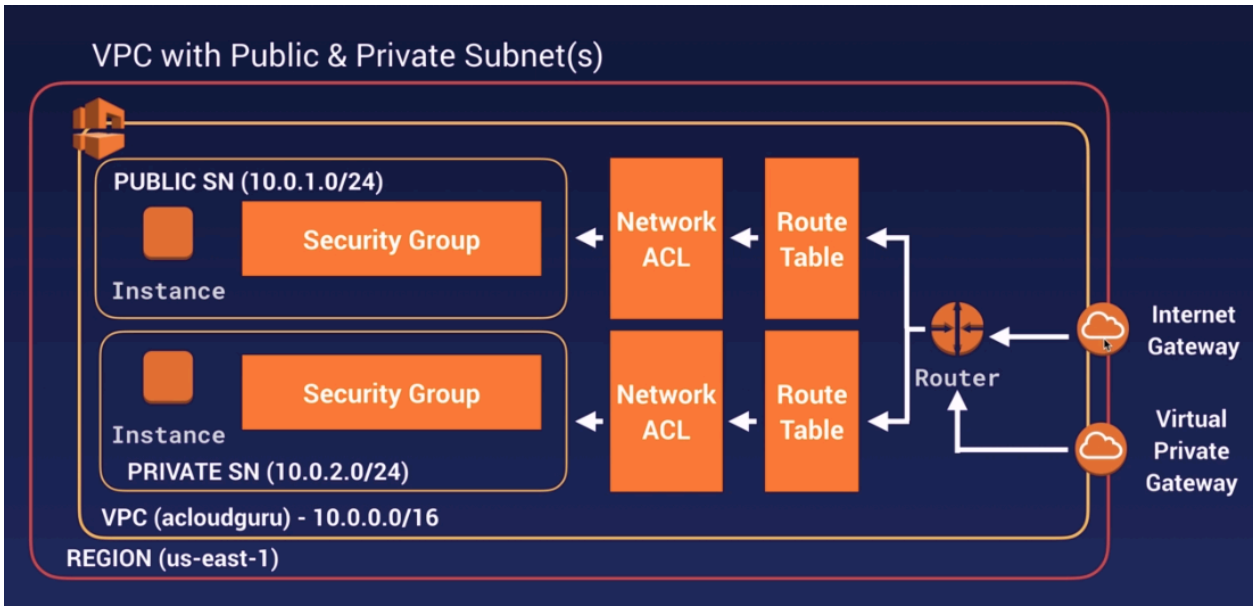
Internet Gateway - Allows communication between instances in your VPC and the internet.

NAT Gateway - Enables instances in a private subnet to connect to the internet or other AWS services but prevents the internet from initiating connections with those instances.

Security Groups - Act as a virtual firewall for your instances to control inbound and outbound traffic.

Network ACLs - Provide an additional layer of security at the subnet level.

The architecture of VPC:



Working of VPC:

Let's say you have a web application with a database backend.

Step-by-Step Setup

1. **Create a VPC**:
    - Choose an IP address range (e.g., 10.0.0.0/16).
2. **Create Subnets**:
    - **Public Subnet** (e.g., 10.0.1.0/24): For web servers that need internet access.
    - **Private Subnet** (e.g., 10.0.2.0/24): For databases and application servers that don't need direct internet access.
3. **Set Up Route Tables**:
    - **Public Route Table**: Routes traffic from the public subnet to the internet via the Internet Gateway.
    - **Private Route Table**: Routes traffic within the VPC and to the internet via the NAT Gateway.
4. **Attach an Internet Gateway**:
    - Allows instances in the public subnet to communicate with the internet.
5. **Create a NAT Gateway**:
    - Place it in the public subnet to enable internet access for instances in the private subnet.
6. **Launch Instances**:
    - **Web Servers**: In the public subnet, assigned public IPs.
    - **Database Servers**: In the private subnet, without public IPs.
7. **Configure Security Groups**:
    - **Web Server Security Group**: Allow HTTP/HTTPS traffic from the internet and SSH traffic from your IP address.
    - **Database Security Group**: Allow traffic only from the web server security group on the database port (e.g., MySQL port 3306).
8. **Configure Network ACLs**:
    - Add rules for additional security at the subnet level if needed.

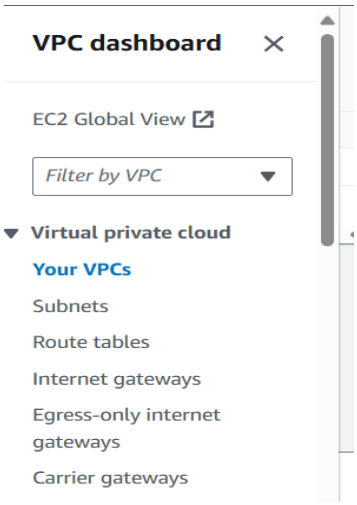
Traffic Flow

1. **User Access**: Users access your web application through the internet. Traffic hits the Internet Gateway and is routed to the web servers in the public subnet.
2. **Web to Database**: Web servers process requests and may need to query the database. They send traffic to the database servers in the private subnet.
3. **Database Access**: Database servers can respond to web server queries. If they need to download updates or access other AWS services, they use the NAT Gateway to access the internet without exposing themselves directly.

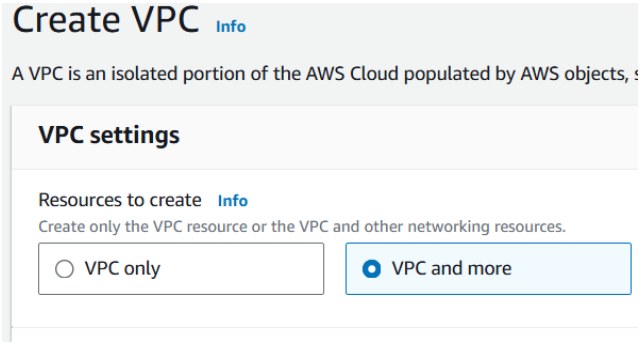
How to create VPC for your Account:

VPC Container Creation:

1. Search VPC Service in AWS and select it.
2. Then click on the “Create VPC” button . In VPC creation dashboard you will have to select following things:
    - Name
    - IPv4 CIDR block- This defines the range of ip addresses for your VPC. Usually we keep 10.0.0.0/16
    - After filling all these details click on Create VPC button at the bottom
3. After this you can see your newly created VPC in the “Your VPCs” option available in the VPC dashboard



(**Note:** When you are creating VPC you can see you have two options:



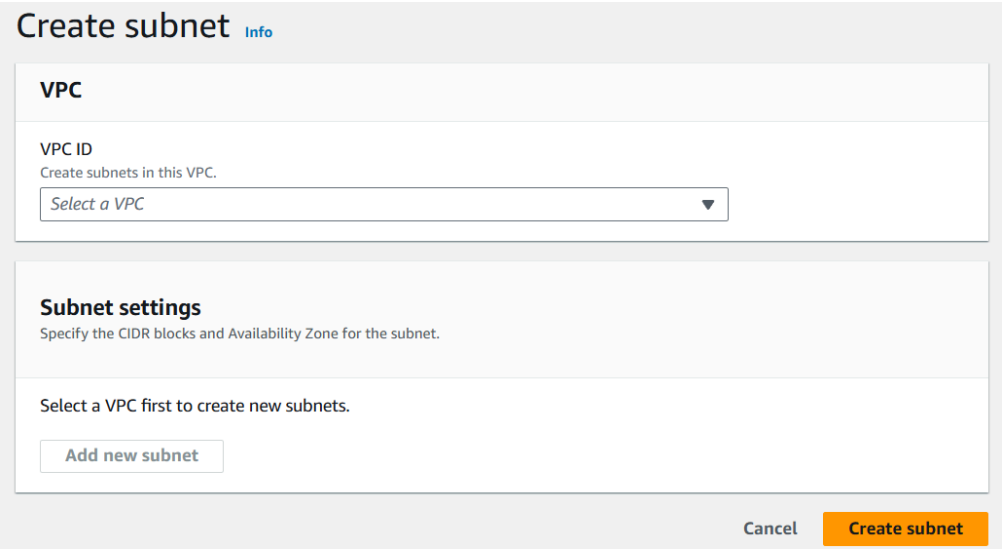
1. VPC only: This option creates only VPC
2. VPC and more: This option creates subnets, routes and internet access along with VPC. Basically in this everything is created for you and you do not need to set up anything.

)

Subnet Creation:

Now you have a Private cloud network for you. Next step is subnet creation. For this follow these steps -

1. Select “Subnets” from VPC Dashboard
2. Then click on the “Create Subnet” option available in the upper right hand side corner.
3. In this you have to fill only one thing i.e Your VPC in which you want your subnet:



4. Once you select the VPC you will be able to access Subnet Settings which you can see in the above image. In that fill in the details:
    - Name of your subnet
    - Availability Zone
    - IPv4 subnet CIDR block - The IP range for your subnet. This range should be within your VPC IP range.
      Example: If you gave your VPC range - 10.0.0.0/16
      Then your subnet can have this range - subnet1- 10.0.0.0/24
      subnet2- 10.0.1.0/24 and so on.
5. Once you are done with this. You can either create one more subnet by clicking on the “ADD New Subnet” button OR if you don’t want more subnets then just click on the “Create subnet” button.

Route Creation:

Now the next step is to create a route to your subnet. For this follow these steps -

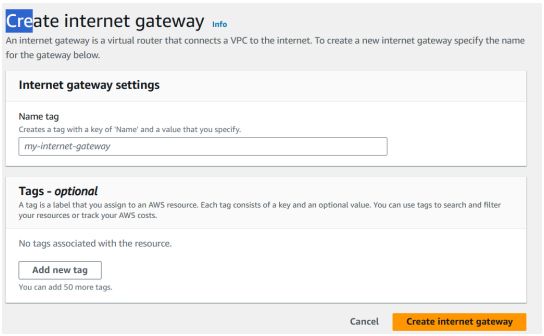
1. Select “Route tables” from VPC Dashboard
2. Then click on the “Create route table” option available in the upper right hand side corner.
3. In that fill the following details:
    - Name of the route
    - VPC - The VPC to use this route. The VPC which you created earlier
4. Then click on create route

Internet Gateway:

Now you need to attach an internet gateway to your public subnet. For this follow these steps -

Select “Internet Gateways” from VPC Dashboard.

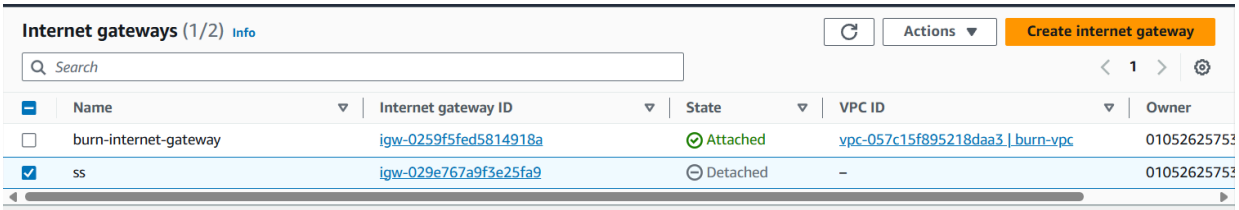
Then click on the “Create internet gateway” option available in the upper right hand side corner.



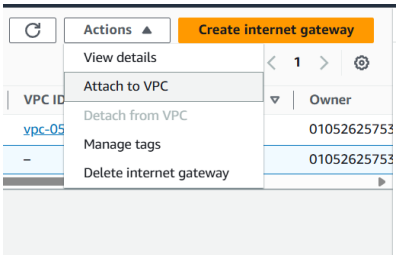
Name your internet gateway and click on click internet gateway below.

Attaching all the Components Created Till Now

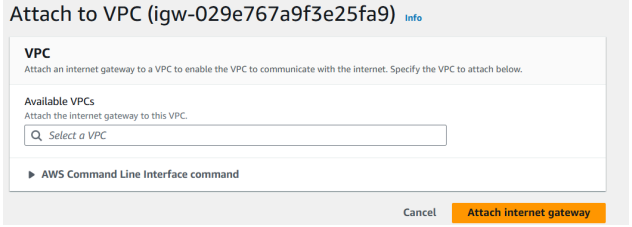
1. **Attaching VPC to internet Gateway**: Now we need to attach the Internet gateway we created to our initially created VPC. For this do the following steps:
   - Select the internet gateway you created from the internet gateway dashboard



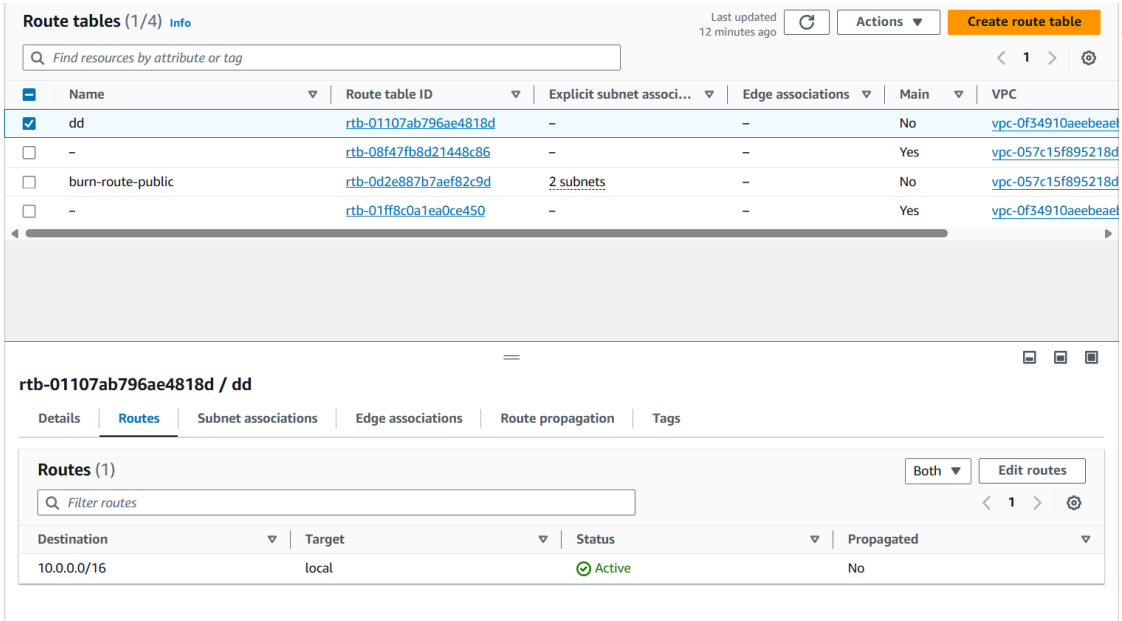
   - Then click on the “Actions” tab available in the upper corner side. In that select “Attach to VPC” option



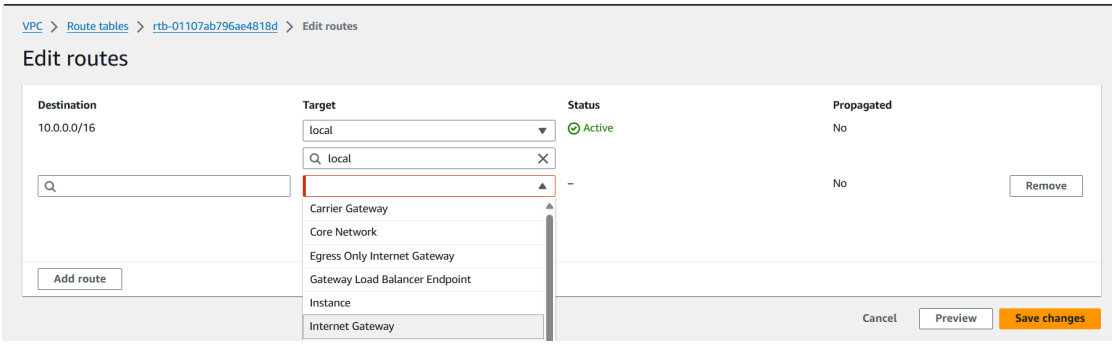
   - Then select your VPC and attach to it to internet gateway



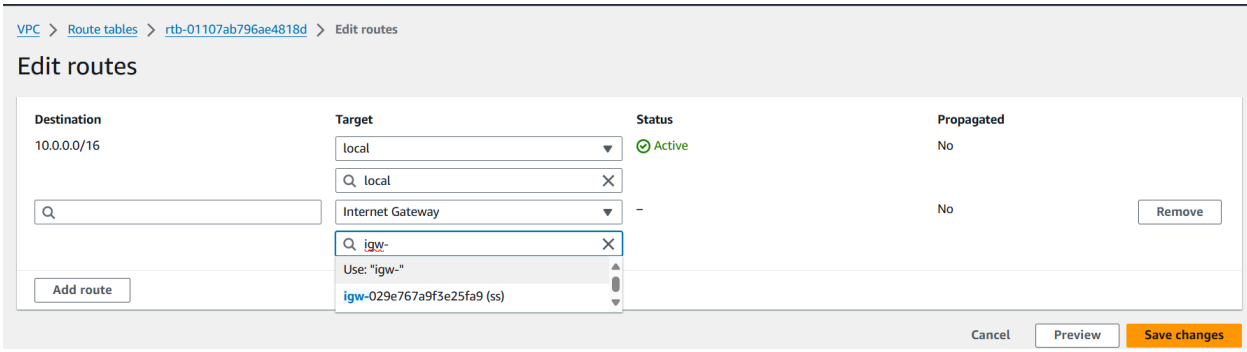
2. **Connect Internet Gateway to Route:** Now we need to connect our newly created internet gateway to Route which we created earlier. For this follow these steps:
    - Go to the “Route Tables” tab. In that select the table you created earlier.
    - On selecting it below you can see various options like Details, Routes, Subnet Associations, etc.



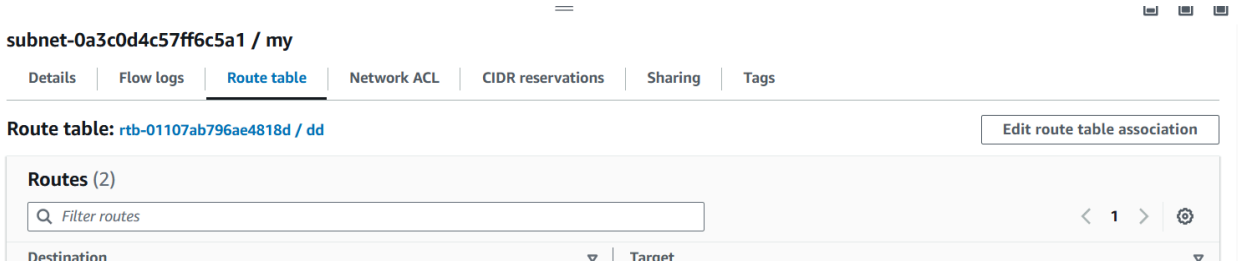
    - From that select the “Routes” option and click on the “Edit routes” button in the corner.
    - After clicking it click on “Add new route” button and select Internet Gateway option in that and also the IP address of your destination.



    - After that select the Internet Gateway you created and Click on “Save Changes”.



3. **Attach Subnet to Route Table** - Now we want to attach the route with Internet Gateway to Public Subnet (Note: For Private subnet you need to create NAT Gateway if you want internet access for it.). To do this follow these steps:
    - Go to the “Subnet” tab. In that select the table you created earlier.
    - On selecting it below you can see various options like Details, Flow Logs, Route tables, etc.
    - In that select “Route Tables” option “Edit Route table” option in the upper corner

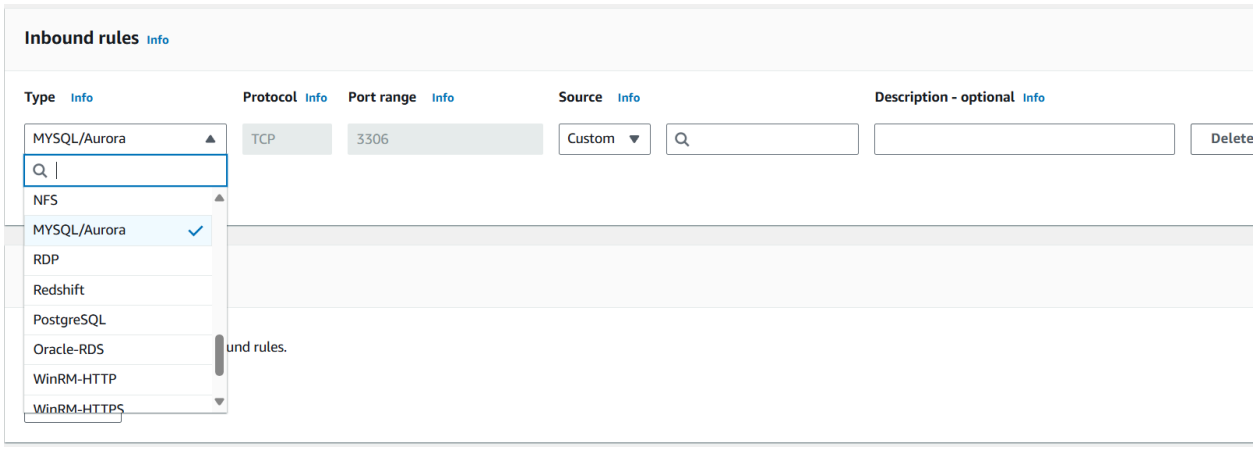


    - In that select the route you created earlier and click on save button.

Security Group:

Now we need to create a Security Group for our VPC , which will define Inbound and Outbound rules for our VPC.For this follow the following steps:

1. Select the “Security Groups” tab from the VPC Dashboard.
2. Then Click on “Create Security Group” . Fill in the basic details like name of the group and VPC you created earlier.
3. After that define the inbound rules. YOu can click on the add rule button and create your rule. For Database you can select MYSQL as Type in inbound rule.



4. You can work with this as you go further with your project. Means you can change these rules according to your project as you move forward with it.

Finally, we are done creating VPC for our Account. Now we can launch instances in this Environment and work on it.