**VPC (Virtual Private Cloud)**

* VPC is Isolated environment for data centre
* One of the important concepts in AWS
* It is used to get the more control on our AWS resources.
* To restrict the resources from outside to provide the fine and gained access to AWS resource.
* If you want to create network in AWS then you can create VPC.
* Every reason AWS provide one default VPC.
* Every reason you can create five VPC.
* By default, you can create 20 servers in each region

**Some important Components In VPC**

1. network -: collection or group of computers

2. subnet -: logical portion of network

subnets are nothing but a range of IP addresses in your VPC.

3. CIDR (Cross inter domain route) -: according to your requirement/system you can set the network.

Using this you can set the customize network

Subnetmask -: IP address followed by subnet mask. Subnet mask value is used to get the network of ip address (to get the actual network of system use subnet mask value)

Internet gateway -: used for allowing outside traffic to our network.

Route -: you want to collect multiple network, then you can use rout.

You want to create two different network the you use route

NAT (Network address translator)-: When any private system wants to communicate with public network then we use NAT

NAT gateway -: is logical device (aws provide NAT gateway)

Ingress -: nothing but incoming traffic

Egress -: nothing but outgoing traffic

Network ACL (network access control list)-> subnet level firewall

Allow subnet level traffic using network acl

*Hardware VPN Connection-:* A hardware-based VPN connection between your Amazon VPC and your datacenter, home network, or co-location facility.

*Virtual Private Gateway-:* The Amazon VPC side of a VPN connection. The Customer gateway is the customer side of a VPN connection.

*VPC Endpoint-:* Enables you to privately connect AWS services .

access from within your VPC without using an Internet gateway or NAT, and allows you to control the access using VPC endpoint policies.

Why we are creating vpc in aws?

To get the more control on our AWS resources.

To restrict the resources from outside to provide the fine and green access to aws resource.

VPC is Isolated environment for data center .

Data center we have server,route ,switches ,racks,networks same thing we can create in aws as well using VPC.

If you want to create network in aws then you can create VPC.

Every reason aws provide one default vpc.

Every reason you can create five vpc.

Budefault you can create 20 servers in each region

Component in VPC

1.subnet

2. Internet Gateway

3.Egress

4.Ingress

5.nat gateway

6.End Points

VPC with public and private subnets

1.create the vpc

2.create public subnet

3.create private subnet

4.create internet gateway

5.attach internet gateway to VPC

5.create Router for VPC

6.Assign VPC router to network

1.create VPC

-> Go to vpc

* Click on create vpc
* Give Name tag
* Define IPv4 CIDR block (ex .192.168.0.0/16)
* Click on create

2. Create public subnet

-> Goto VPC service

-> select Subnets

-> create subnet

-> give name tag

-> select vpc (which you have created)

-> select availability zone

-> define IPv4 CIDR block (ex.192.168.0.0/24)

-> click on create

3.create Private subnet

-> Goto VPC service

-> select Subnets

-> create subnet

-> give name tag

-> select vpc (which you have created)

-> select availability zone

-> define IPv4 CIDR block (ex.192.168.1.0/24 – define different than public)

-> click on create

4.Create Internet Gateway

-> goto VPC service

-> select internet Gatway

-> Create internet Gateway

-> Give Name tag

-> click on create

5.attach internet gateway to VPC

-> select created internet gateway

-> select Actions

-> Attach To VPC

-> Assign newly created VPC

-> click on attach

6.create router

-> By default VPC created its own route table

7.Assign VPC router to network

-> select Route Tables

-> select default route table which is created

-> select subnet association

-> click on edit subnet associations

-> select public subnet and save it

Testing Purpose

1. Create two instance one for public subnet and another for private subnets
2. For public instance,

* In third step (configure instance) select newly created VPC in in networks option
* Select Public subnet which is created for relevant VPC
* Enable auto assign public IP option
* Click on next
* Add Tag for this instance which you want

For Private instance

* In third step (configure instance) select newly created VPC in in networks option
* Select Private subnet which is created for relevant VPC
* disable auto assign public IP option
* Click on next
* Add Tag for this instance which you want

1. Then check the ip for both instance

* Public instance created with public and private ip with assigned subnets

Ex. Public mask is 192.168.0.0/24 then ip will be 192.168.0.(1-255)

* Private instance created with only private ip address

Ex. Ex. Public mask is 192.168.1.0/24 then ip will be 192.168.1.(1-255)

1. You can easily access you public instance from any where (your laptop), But you can not access Private instance from anywhere

You can access Private instance using any instance which is created in AWS

1. When you logged on to private instance that time you cannot internet for this, because its not for public

For accessing internet on it you have to do nating

**Create Elastic Ip address**

1. Go to VPC services
2. Select Elastic IP’s
3. Create Elastic IP’s
4. select Allocate new address
5. select IPv4 address pool (Amazon Pool)
6. click on allocate

**Create Nat Gateway**

1. Go to VPC services
2. Select Nat Gateways
3. Click on create NAT gateways
4. Select subnets (choose public )
5. Select Elastic IP Allocation ID
6. Click on create NAT Gateway

**Create New Route Table for Nat Gateway (Giving access to Private instance via public subnets)**

1. Go to VPC services
2. Select Route tables
3. Click on create Route Table
4. Give Name tag
5. Select VPC and
6. Click on create
7. Select newly create route table
8. Click on Actions -> Edit Routes -> Add route -> Destination(0.0.0.0/0) ->Target(select Internet Gateway which you created for this vpc) -> save
9. Go to Subnet Associations -> Edit Subnet Associations -> select private subnets under Associated Subnets option -> save

Note-: This time we selected private subnet because we have to allow routing between public instance and internet (outsider), if we choose Private subnet under nat gateways that mean it will be not private nw that time