**Exercise 7. To Configure Amazon Virtual Private Cloud (VPC) AIM:** To Create your own VPC

**PROCEDURE:**

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications. You can easily customize the network configuration for your Amazon Virtual Private Cloud.

**For example:**

you can create a public-facing subnet for your web servers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Features and Benefits

Multiple Connectivity Options Secure

Simple

Use All the Scalability and Reliability of AWS

Cases

Host a simple, public-facing website Host multi-tier web applications

Host scalable web applications in the AWS cloud that are connected to your Datacenter

Extend your corporate network into the cloud Disaster

Recovery

Amazon VPC enables you to launch AWS resources into a virtual network that you've defined. If you have a default VPC, you can skip this section and move to the next task,

Create a Security Group. Open AWS console Click on Services

1.Select Networking and Content Delivery Click on VPC

On VPC Dashboard panel

Click on Your VPC

Click on Create VPC button

A screenshot of a computer

Description automatically generated

On “Create VPC”, page

For Name tag -> HYD VPC

For IPv4 CIDR block -- 192.168.0.0/16

Leave on “Yes Create” button

A screenshot of a computer

Description automatically generated

2.To Create public & private subnet

For VPC -> HYDVPC

For IPv4 CIDR block -> 192.168.10.0/24 Click on Yes Create button

Verify

Hyd-pub-subnet got created

On create subnet page

For Name tag -> hyd-pvt-subnet

For VPC -> HYDVPC

For IPv4 CIDR block -> 192.168.20.0/24

Click on Yes Create button A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

3.Create an Internet gateway and attach to your VPC

In Create Internet Gateway, box For Name tag -> HYDIGW Click on “Yes, create” button A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

4.Create Pubic Routing Table, associate subnet and add routing rules

For Destination -> 0.0.0.0/0 For

Target ->select HYDIGW

Click on Save button

5.Create Private Routing Table, associate subnet and add routing rules

On “Create Route Table” box

For name tag -> hyd-pvt-route For

VPC -> HYDVPC

Click on “Yes, Create button”

A screenshot of a computer

Description automatically generated

**8.Aim**: To configure EFS

Procedure:

1.Students should have an AWS account or use the provided institutional AWS sandbox.

2.Navigate to Amazon EFS service.

Create an EFS File System:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Click on Create file system.

3.Select the VPC where the file system will reside.

Choose default settings or customize the performance mode (General Purpose) and throughput mode (Bursted).

Review and Create:

4.After creating the file system, take note of the File System ID and DNS name. You’ll need these for mounting EFS on an EC2 instance.

Create/Modify Security Group:

A screenshot of a computer

Description automatically generated

5.Ensure that the EC2 instance has a security group that allows outbound traffic to the EFS mount target. EFS uses the NFS (Network File System) protocol on port 2049.

6.Navigate to Security Groups in the EC2 console.

7.Select the security group associated with your EC2 instance, then edit the inbound/outbound rules to allow traffic on port 2049.

A screenshot of a computer

Description automatically generated