# Master level instructions (Project 4)

Step 1

Create 2 VPCs

# VPC-1

Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.

In VPC setting select VPC only

In Name – provide Name (VPC-A)

In IPv4 CIDR block select IPv4 CIDR manual input (10.0.0.0/16)

In tag –

Key=Name

Value= VPC-A

Leave all options as default and create VPC

# VPC-2

Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.

In VPC setting select VPC only

In Name – provide Name (VPC-B)

In IPv4 CIDR block select IPv4 CIDR manual input (20.0.0.0/16)

In tag –

Key=Name

Value= VPC-B

Leave all options as default and create VPC

Create Subnet

# Subnet-1

In Create Subnet

Select VPC (VPC-A)

In Subnet setting provide subnet name (my-subnet- VPC-A-private)

Select Availability zone

IPv4 CIDR block (10.0.0.0/24)

Create Subnet

# Subnet-2

In Create Subnet

Select VPC (VPC-B)

In Subnet setting provide subnet name (my-subnet-VPC-B-public)

Select Availability zone

IPv4 CIDR block (20.0.0.0/24)

Create Subnet

Create 1 Internet Gateway and Attach to VPC-B

Create Route-Table in VPC-A

Go to VPC and select Create Route Table

Provide name – (for ex. VPC-A-PrivateRoute)

Select VPC-A in VPC option

Go to subnet association attach subnet created in subnet-1

Create

Create Route-Table in VPC-B

Go to VPC and select Create Route Table

Provide name – (for ex. VPC-B-PublicRoute)

Select VPC-B in VPC option

Create

Select Route Table created in above step

Go to Routes and add routes

In destination select – 0.0.0.0/0

In Target select Internet Gateway

In subnet association

Click edit subnet association and select public subnet –created in subnet-2 step

Save the changes

Create Security group in VPC-A

Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>

In the navigation pane, choose Security Groups

Choose Create security group.

In Security group name enter name – SSHAccess

Enter description

Select VPC – (VPC-A)

In Inbond open SSH port

In tag –

Key=Name

Value= SSHAccess

Create Security group

Create Security group in VPC-B

Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>

In the navigation pane, choose Security Groups

Choose Create security group.

In Security group name enter name – SSHAccess

Enter description

Select VPC – (VPC-B)

In Inbond open SSH port

In tag –

Key=Name

Value= SSHAccess

Create Security group

Launch EC2 Instance in VPC-A

Launch one EC2 Instance in VPC-A in private subnet (created in subnet-1 step)

Select AMI

In Instance type select t2.micro

In Configure Instance Details select VPC-A in network

In subnet select – private subnet (created in subnet-1 step)

Auto-assign public IP – should be selected as Disable

In the Add Tags – give name to your EC2 machine

In security group -attach security group created above

Select Keypair

Launch

Launch EC2 Bastion Instance in VPC-B

Launch one EC2 Instance in VPC-B public subnet (created in subnet-2 step)

Select AMI

In Instance type select t2.micro

In Configure Instance Details select VPC-B in network

In subnet select – public subnet (created in subnet-2 step)

Auto-assign public IP – should be selected as Enable

In the Add Tags – give name to your EC2 machine

In security group attach security group created above

Select Keypair

Launch

VPC Peering

Create VPC Peering between VPC-A and VPC-B

Go to VPC console – Select Peering connection – create Peering connection

Give Name – Select Requestor and Accepter VPC

Create

Once Peering is created successfully, accepter need to accept the peering request

Go to VPC peering – select action – Accept request

Update Route Table

Go to Route table created in VPC-A

Go to Routes and add routes

In destination select – CIDR range of VPC - VPC-B

In Target select Peering connection

Save

Go to Route table created in VPC-B

Go to Routes and add routes

In destination select – CIDR range of VPC - VPC-A

In Target select Peering connection

In destination select – 0.0.0.0/0

In Target select Internet Gateway

Save

Note – To check ping connectivity open ICMP port in Security group

Testing