# Master level instructions (Project 3)

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 (PROD-VPC)

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

In tag –

Key=Name

Value= PROD-VPC

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 (DEV-VPC)

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

In tag –

Key=Name

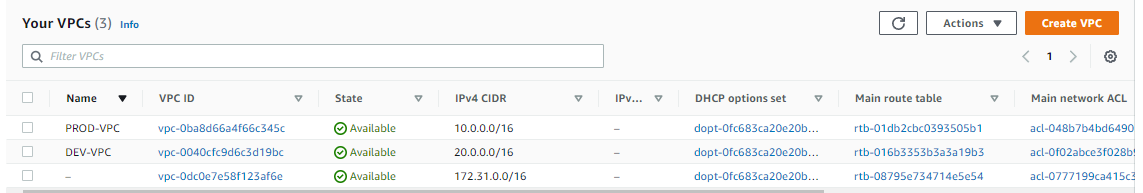
Value= DEV-VPC

Leave all options as default and create VPC

In tag –

Key=Name

Value= DEV-VPC



Create Subnet

# Subnet-1

In Create Subnet

Select VPC (PROD-VPC)

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

Select Availability zone (2a)

IPv4 CIDR block (10.0.0.0/24)

Create Subnet

# Subnet-1a

In Create Subnet

Select VPC (PROD-VPC)

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

Select Availability zone (2b)

IPv4 CIDR block (10.0.1.64/26)

Create Subnet

# Subnet-2

In Create Subnet

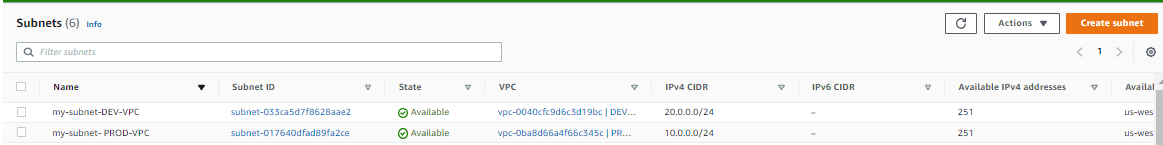
Select VPC (DEV-VPC)

In Subnet setting provide subnet name (my-subnet-DEV-VPC)

Select Availability zone (2a)

IPv4 CIDR block (20.0.0.0/24)

Create Subnet



Create Route-Table

Go to VPC and select Create Route Table

Provide name – (for ex. PROD-VPC-PUBLIC-ROUTE)

Select PROD-VPC

Create

Step to follow after creation of Internet gateway

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 1a step

Save the changes

Create Internet Gateway and Attach to PROD-VPC

Create Security group

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 – ElasticInterfaceSG

Enter description

Select VPC – (PROD-VPC)

In tag –

Key=Name

Value= ElasticInterfaceSG

Create Security group

Create Network Interface

Go to EC2 console and select Network Interface

Select Create Network Interface

Enter Description

In subnet select (my-subnet-PROD-VPC)

Select the Default security group (this need to be change)

In tag –

Key=Name

Value= additionalprivateIP

Launch EC2 Instance

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

Select AMI

In Instance type select t2.micro

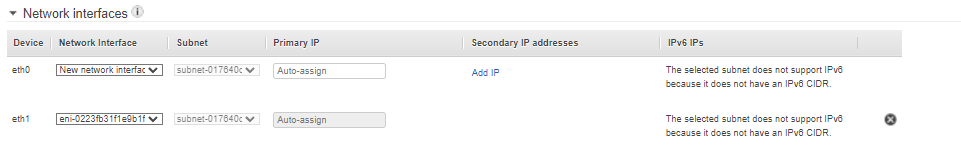
In Configure Instance Details select PROD-VPC in network

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

Auto-assign public IP – should be selected as Disable

Scroll down and select Network Interface

Click Add device – select the Network Interface create in above Step



In the Add Tags – give name to your EC2 machine

In security group create security group with default type ssh traffic

Select Keypair

Launch

Launch EC2 Bastion Instance (PROD-VPC)

Launch one EC2 Instance in Prod-VPC public subnet (created in subnet-1a step)

Select AMI

In Instance type select t2.micro

In Configure Instance Details select PROD-VPC in network

In subnet select – public subnet (created in subnet-1a step)

Auto-assign public IP – should be selected as Enable

In the Add Tags – give name to your EC2 machine

In security group create security group with default type ssh

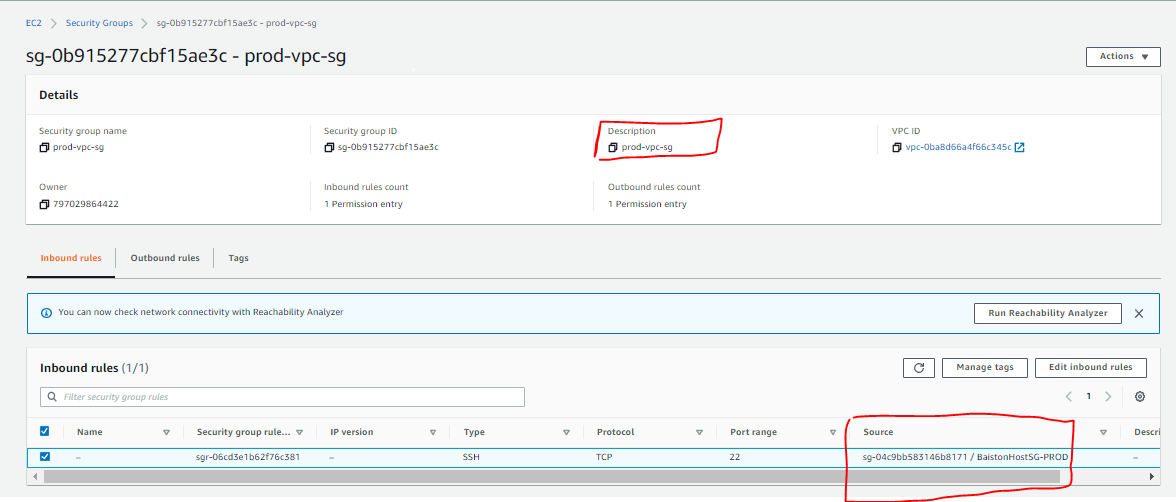
Select Keypair

Launch

Testing

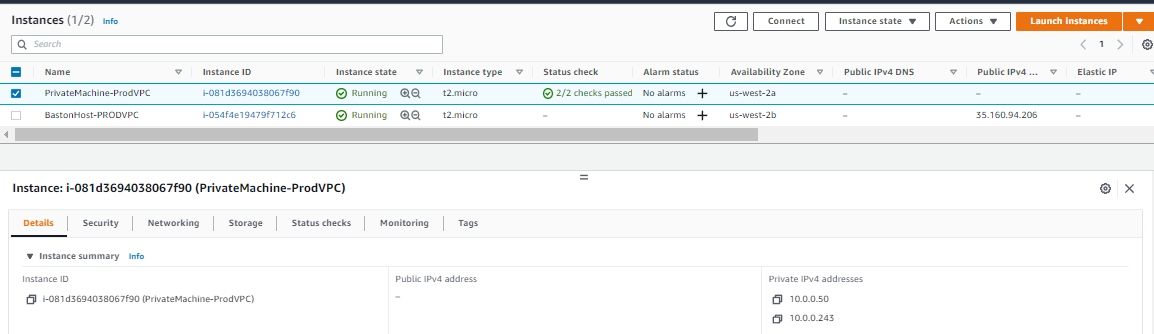
Make a note of the Security group attached to Bastion host and Private Machine (created in PROD-VPC)

Update the Security group connected to PROD-VPC machine with Bastion Host Security group in custom (ref screenshot below)



If everything fine you will able to connect to one of the private IP of Prod-VPC machine

Ref below screenshot (if everything followed correctly than one of the private IP able to connect with Bastion machine)



Step 2 of Demo

Create VPC Peering between PROD-VPC and DEV-VPC

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

Create Internet Gateway and Attach to PROD-VPC

Create Route Table

In Create Route Table

Provide name – (for ex. DEV-VPC-PUBLIC-ROUTE)

In VPC Select option - select DEV-VPC

Create

Go to Select Route Table

Go to Routes and add routes

In destination select – CIDR range of PROD-VPC (for ex . 10.0.0.0/16)

In Target select Peering connection

In destination select – 0.0.0.0/0

In Target select Internet Gateway

In subnet association

Click edit subnet association and select default subnet

Save the changes

Select Existing Route Table in PROD-VPC

Select PROD-VPC RT

Go to Routes and add routes

In destination select – CIDR range of DEV-VPC (10.0.0.0/16)

In Target select Peering connect

In subnet association

Click edit subnet association and select public subnet –created in subnet 1a step

Save the changes

Launch EC2 Bastion Instance (DEV-VPC)

Launch one EC2 Instance in DEV-VPC Default subnet (created in subnet-1a step)

Select AMI

In Instance type select t2.micro

In Configure Instance Details select DEV-VPC in network

In subnet select –subnet default subnet

Auto-assign public IP – should be selected as Enable

In the Add Tags – give name to your EC2 machine

In security group create security group with default type ssh

Select Keypair

Launch

Testing

Make a note of the Security group attached to Bastion (created in DEV-VPC) host and Private Machine (created in PROD-VPC)

Update the Security group connected to PROD-VPC machine with Bastion Host Security group in custom (ref screenshot below)