# Master level instructions (Project 2)

To create a VPC only

* Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>
* In the navigation pane, choose Your VPCs, Create VPC.
* Under Resources to create, choose VPC only.
* Specify the following VPC details as needed.
  + Name
  + IPv4 CIDR block - for example, 10.0.0.0/16, or 192.168.0.0/16
* Tenancy: Choose the tenancy option for this VPC. (Should go with Default)
  + **Select Default** to ensure that EC2 instances launched in this VPC use the EC2 instance tenancy attribute specified when the EC2 instance is launched.
  + **Select Dedicated** to ensure that EC2 instances launched in this VPC are run on tenancy instances regardless of the tenancy attribute specified at launch.
  + Choose Create VPC

To create a Subnet

* Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>
* In the navigation pane, choose Subnets. Then choose Create Subnet.
* In the Create Subnet dialog box, do the following:
  + Name (private-subnet)
  + For VPC, choose the VPC that you created previously.
  + For Availability Zone, choose the first Availability Zone in the list.
  + For CIDR block, type the CIDR block to use for the subnet. If you used the default values for the VPC in the previous procedure, then type 10.0.1.0/28.
  + Choose Yes, Create.
* Repeat above steps to create subnets for each remaining Availability Zone in the region. For the subnet CIDR blocks, you can use 10.0.2.0/28, 10.0.3.0/28, and so on.

To 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.

Enter a name and description for the security group. You cannot change the name and description of a security group after it is created.

From VPC, choose the VPC (created in above step )

You can add security group rules, or you can add them later.

For Inbound rules, create rules that allow specific traffic to reach your instance

* Choose Add rule. For Type, choose HTTP. For Source, choose Anywhere.
* Choose Add rule. For Type, choose SSH. For Source, choose Anywhere

For Outbound rules, keep the default rule, which allows all outbound traffic.

Choose Create security group

To create EC2 machines

Create Keypair first

Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

In the navigation pane, choose Key Pairs.

Choose Create key pair.

For Name, enter a descriptive name for the key pair.

For Key pair type, choose either RSA or ED25519.

Note that ED25519 keys are not supported for Windows instances, EC2 Instance Connect, or EC2 Serial Console.

For Private key file format, choose the format in which to save the private key.

To save the private key in a format that can be used with OpenSSH, choose pem.

To save the private key in a format that can be used with PuTTY, choose ppk.

Choose Create key pair.

The private key file is automatically downloaded by your browser. The base file name is the name

you specified as the name of your key pair, and the file name extension is determined by the file

format you chose. Save the private key file in a safe place.

Important –

This is the only chance for you to save the private key file.

If you will use an SSH client on a macOS or Linux computer to connect to your Linux instance, use the following command to set the permissions of your private key file so that only you can read it.

chmod 400 my-key-pair.pem

Launch an instance

Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

From the console dashboard, choose Launch Instance.

The Choose an Amazon Machine Image (AMI) – Select Linux AMI 2

On the Choose an Instance Type page - Select the t2.micro instance type, which is selected by default

On the Configure Instance page -

In **Number of instances – change it to 2**

In the Network section – Select VPC – select Subnet (private subnet create in above step)

Auto-assign Public IP – Disabled

Scroll down to the last and select user data – select as text – enter the below script to install Apache web server at startup

#!/bin/bash

yum install httpd -y

service httpd start

chkconfig httpd on

echo "Sample Content " > /var/www/html/index.html

Go with default setting in ADD Storage tab

Under Security Groups – select the security group created in above step

On the Review Instance Launch page, choose Launch.

When prompted for a key pair, select choose an existing key pair (select the key pair created in above step)

Choose Launch Instance

Step to create NAT Gateway

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

Choose NAT Gateways.

Choose Create NAT Gateway and do the following:

* 1. (Optional) Specify a name for the NAT gateway. This creates a tag where the key is Name and the value is the name that you specify.
  2. Select the subnet in which to create the NAT gateway.
  3. For Connectivity type, select Private to create a private NAT gateway or Public (the default) to create a public NAT gateway.
  4. (Public NAT gateway only) For Elastic IP allocation ID, select an Elastic IP address to associate with the NAT gateway.
  5. (Optional) For each tag, choose Add new tag and enter the key name and value.
  6. Choose Create a NAT Gateway.

Steps to create IGW

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

In the navigation pane, choose Internet Gateways, and then choose Create internet gateway.

Optionally name your internet gateway.

Choose Create internet gateway.

Select the internet gateway that you just created, and then choose Actions, Attach to VPC.

Select your VPC from the list, and then choose Attach internet gateway.

Step to create Route Table

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

In the navigation pane, choose Route Tables.

Choose Create route table.

(Optional) For Name tag, enter a name for your route table.

For VPC, choose your VPC.

Choose Create.

Step to create Load Balancer

Open the Amazon EC2 console.

Select Classic Load Balancer

Select the VPC and than Associate the **public subnets** with your load

Register the backend instances (created in private subnet ) with your load balancer

Select Security group ( created in above step )

Create LoadBalancer

Test with DNS Name

https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/