AWS Academy Learner Lab [28589] ID: 142475069537 prodrigo@student.42madrid.com

Practice 2
Cloud and Compute in AWS

Introduction

We are asked to create the next infrastructure:

- 1 VPC
- Two subnets within different availability zones, one must be public and one must be private, with its required table routes.
- Una instancia EC2 en cada una de las subredes con sus correspondientes Security Groups.
- An EC2 instance in every subnet with their required Security Groups.
- For each instance within a public subnet, the Security Group must allow SSH and HTTP access from anywhere.
- For each instance within a private subnet, the Security Group must ONLY allow SSH access from IP addresses within the public subnet, and not from anywhere else.
- Procedure of creating subnets and Security Groups can be done in the AWS Management Console, but instance creation must be done with AWS CLI. The EC2 instance within the public subnet must have the Apache web service installed with an user data script.

Procedure

We click on Start Lab in order to do so, and we also want to open the AWS Management Console tab (even though we are not really using it in this learner lab) so we can take our required screenshots. An AWS CLI shell will open after some time.

We need to read the AWS CLI documentation to know how to launch an EC2 Instance into a VPC (and create key pairs), and also look at the subnet/security groups documentation.

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-subnets-commands-example.html

https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/run-instances.html

https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/create-security-group.html

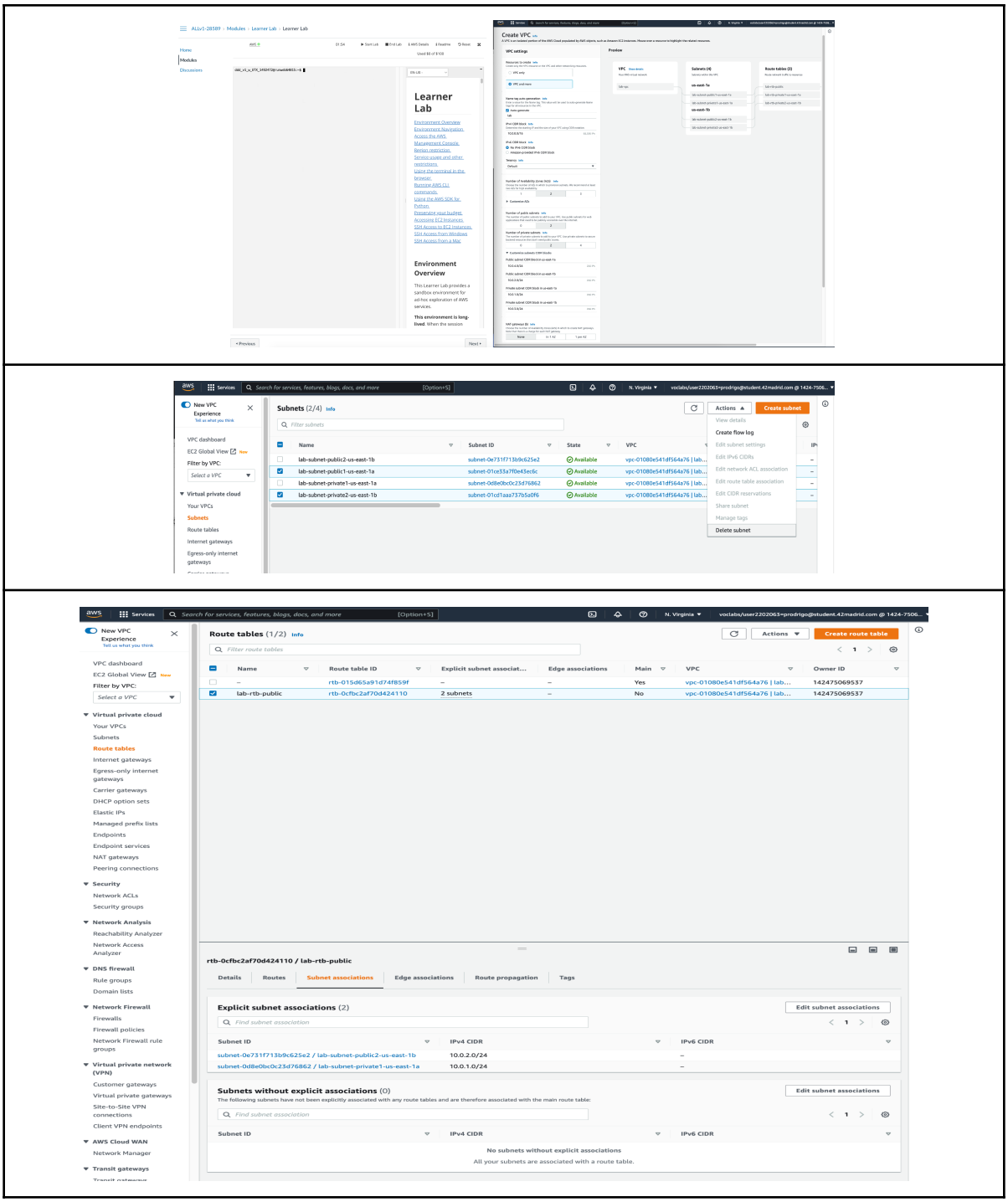
https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/authorize-security-group-ingress.html

I've chosen to do most of it in the AWS Management Console, as it's more eye-friendly and you can see most of the data immediately instead of scrolling through the JSON output.

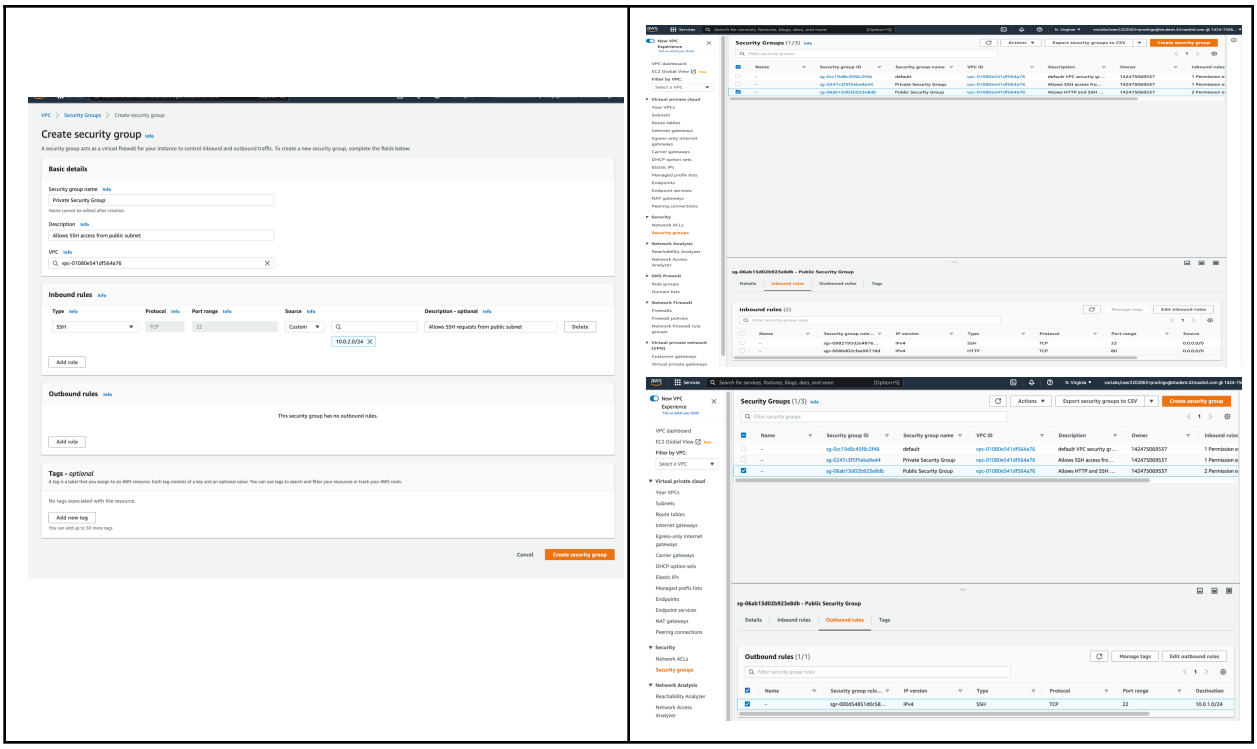
Start by creating the VPC by going to **Services > VPC.** Click on **Create VPC**

Configure the VPC following this template. We are going to delete two of the subnets later, as we aren't asked for those.

Associate both of subnets through the Route Table to end up like this:



Now go to **Security Groups** and create one Security Group for each subnet with its rules.



As our learner lab documentation says:

> **Amazon Elastic Compute Cloud (EC2) Restrictions**
>
> Key pairs - If you are creating an EC2 instance in any AWS Region other than us-east-1, the vockey key pair will not be available. In such cases, you should create a new key pair and download it when creating the EC2 instance. Then use the new key pair to connect to that instance.

It doesn't affect us, but let's create a key regardless.

So we need to create a key pair.

```
aws ec2 create-key-pair --key-name vpckey --query 'KeyMaterial' --output text > vpckey.pem

chmod 400 vpckey.pem
```

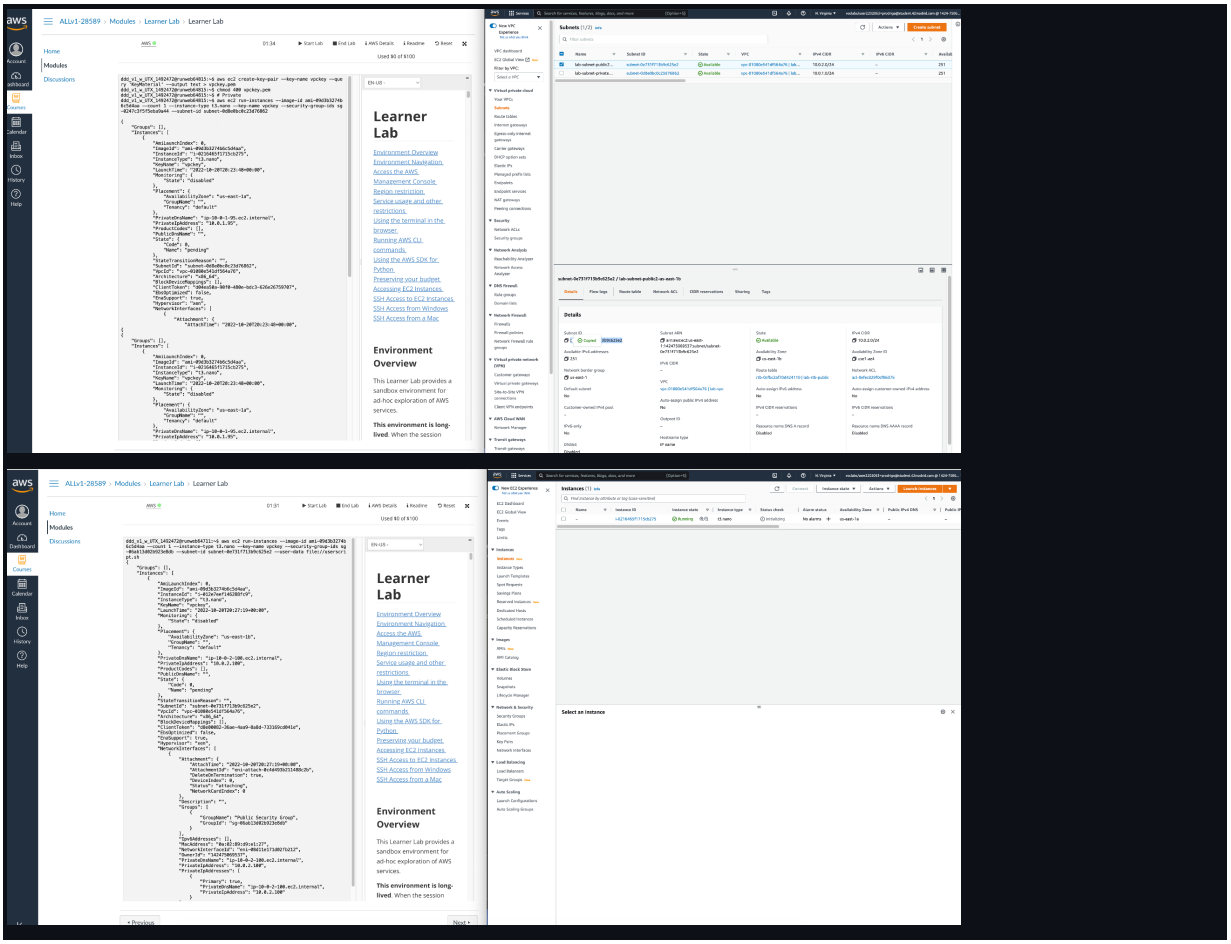
I recommend using scp command with ssh to get the key locally after creating it as you will want to use it later to connect to the instances

Let's create the user-data script which will be run by the public subnet instance.

`userscript.sh`

```
#!/bin/bash
yum update -y
yum install httpd -y
systemctl start httpd
systemctl enable httpd
```

And finally, let's create the instances with the AWS CLI gathering all the data we need from details tabs on AWS Management Console



```
# Private
aws ec2 run-instances --image-id ami-09d3b3274b6c5d4aa --count 1 --instance-type t3.nano
--key-name vpckey --security-group-ids sg-0247c3f5f5eba9a44 --subnet-id
subnet-0d8e0bc0c23d76862

# Public
aws ec2 run-instances --image-id ami-09d3b3274b6c5d4aa --count 1 --instance-type t3.nano
--key-name vpckey --security-group-ids sg-06ab13d02b923e8db --subnet-id
subnet-0e731f713b9c625e2 --user-data file://userscript.sh
```

Once we are done, we click on End Lab and Logout.