Module 5: VPC Security Groups Assignment

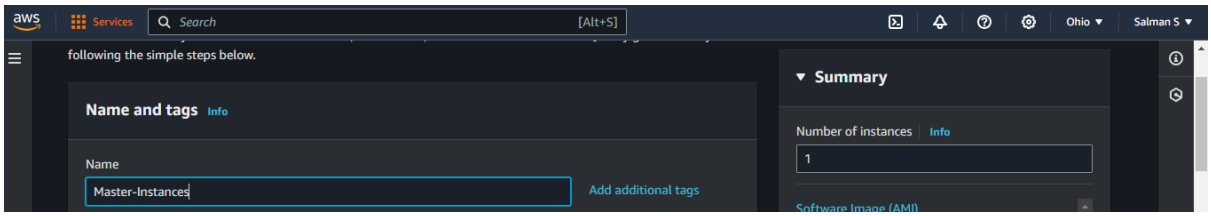
Problem Statement:

Working for an organization, you are required to provide them a safe and secure environment for the deployment of their resources. They might require different types of connectivity. Implement the following to fulfill the requirements of the company.

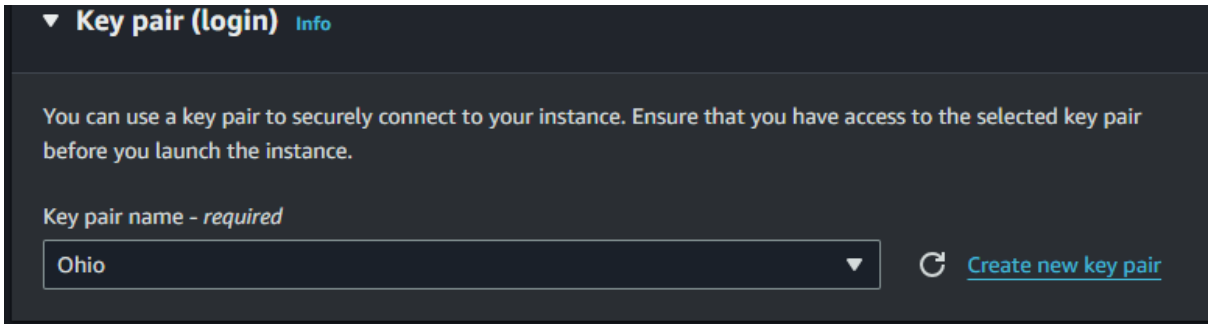
Tasks To Be Performed:

1. Create 2 EC2 instances in any public subnet of any VPC and name them Master and Client.
2. Using security groups, make sure that the Client instance can only be accessed (SSH) through the Master instance.

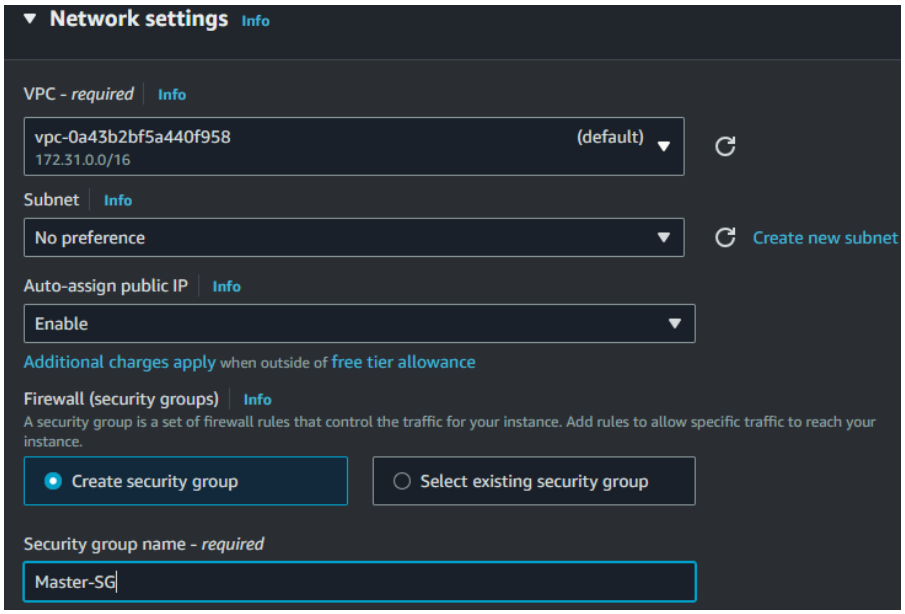
1. Create Master-Instances



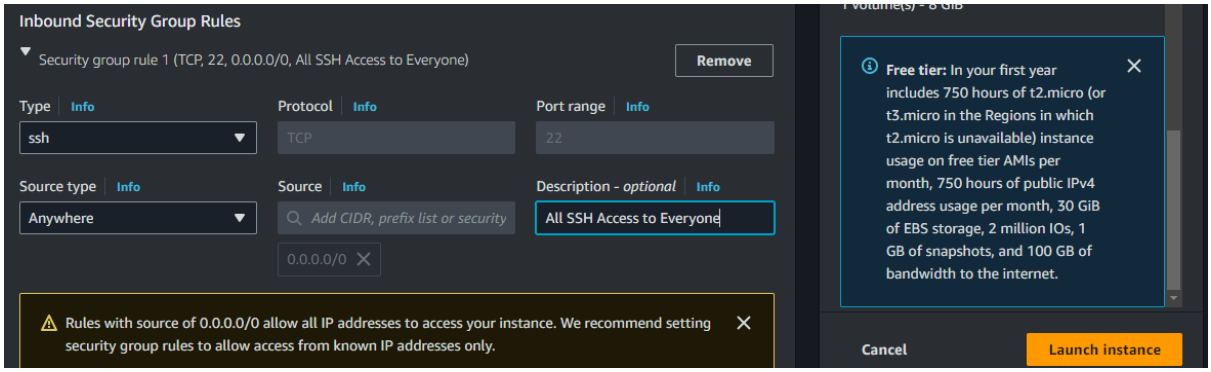
2. Create Key Pair, If u have Previously then Not Required go with the old one



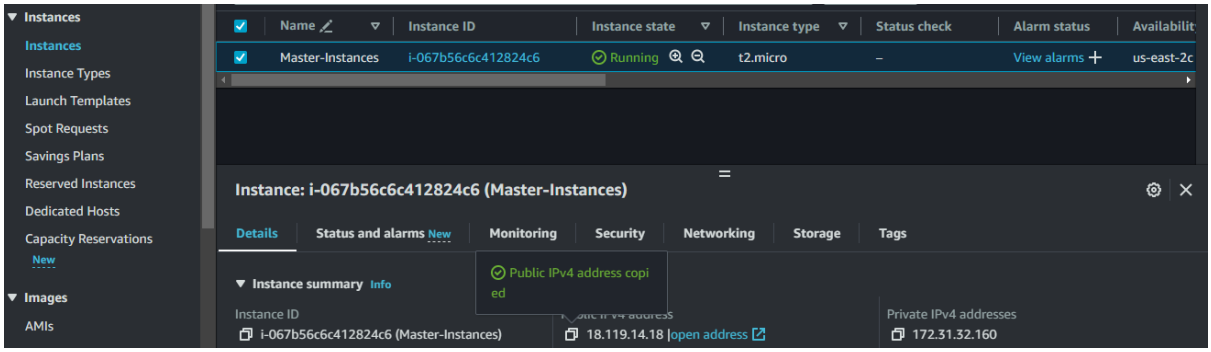
3. Leave Instance type as free tier and Configure Network Settings and Create SG



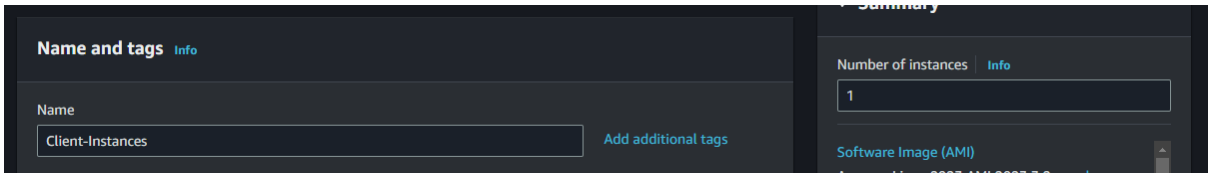
4. Inbound SG Allow Everyone for ssh access in Master Instances and the Launch



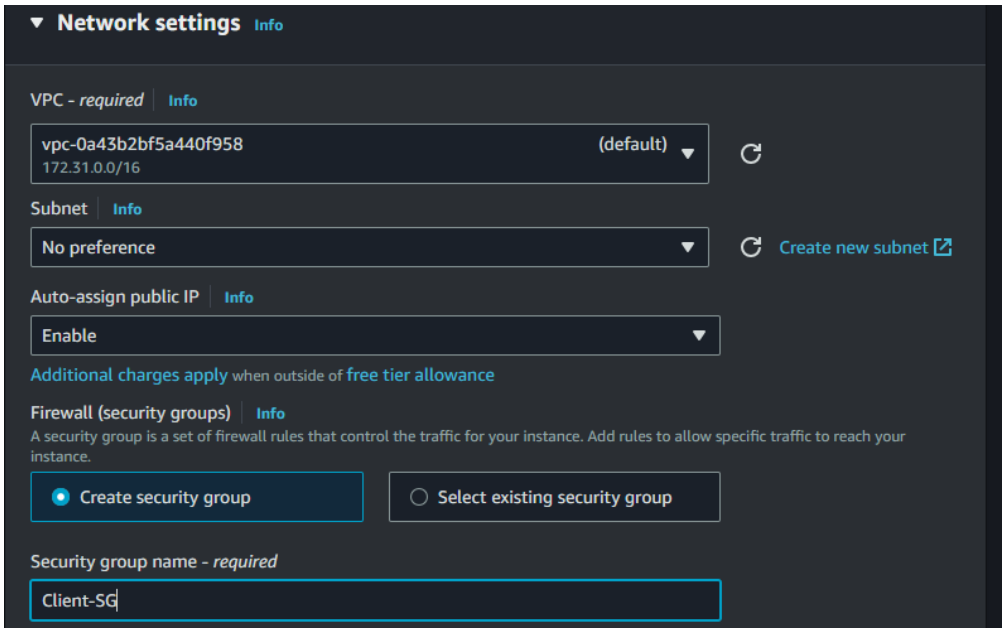
5. Remember Master Instances Public IP Because we have Allow MI Server only to Client Instances



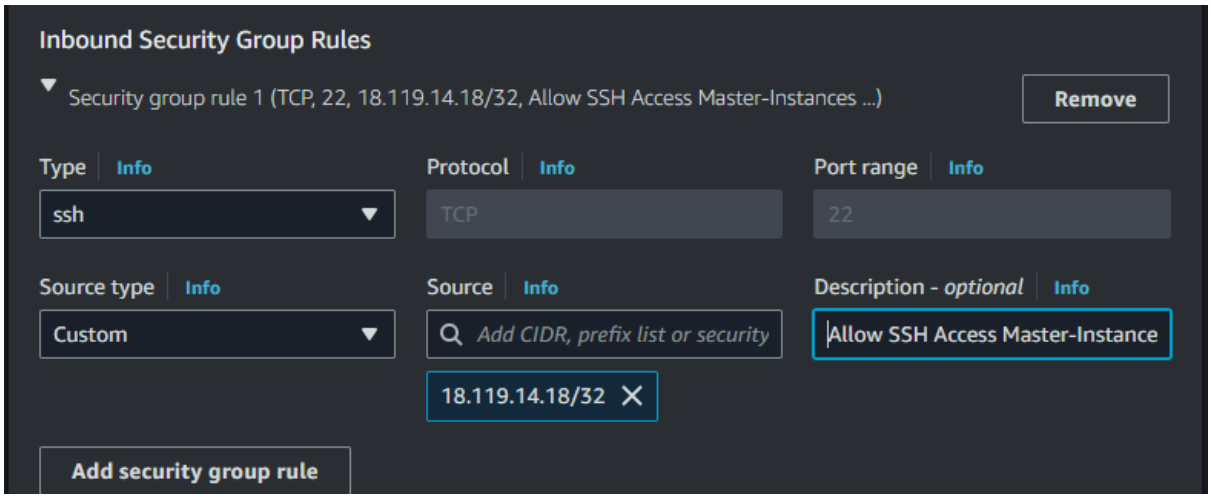
6. Create Client Instances Same as Master Instances but only Changes in Networking Part



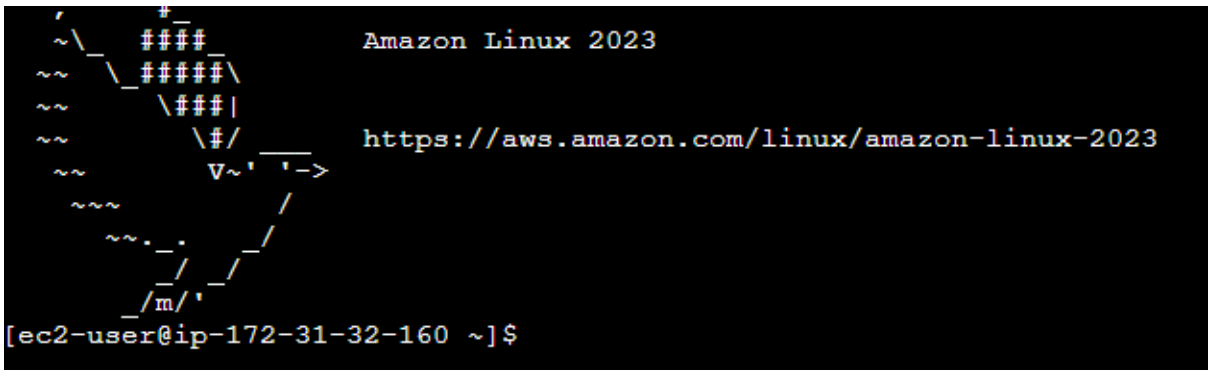
7. Create SG as a Client-SG



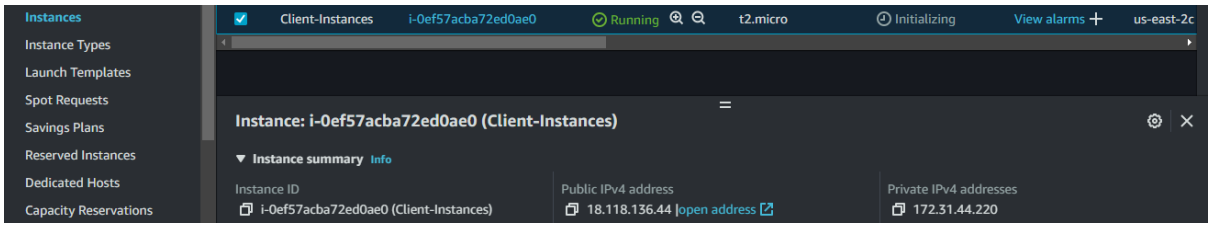
8. Allow SSh access for Master Instances only So Choose Custom and Type Public IP of MI and Launch Instances



9. Connect Master-Instances



10. This is the Client Private and Public Ip and Next step we are connecting Client Instances



*Follow the Commands:

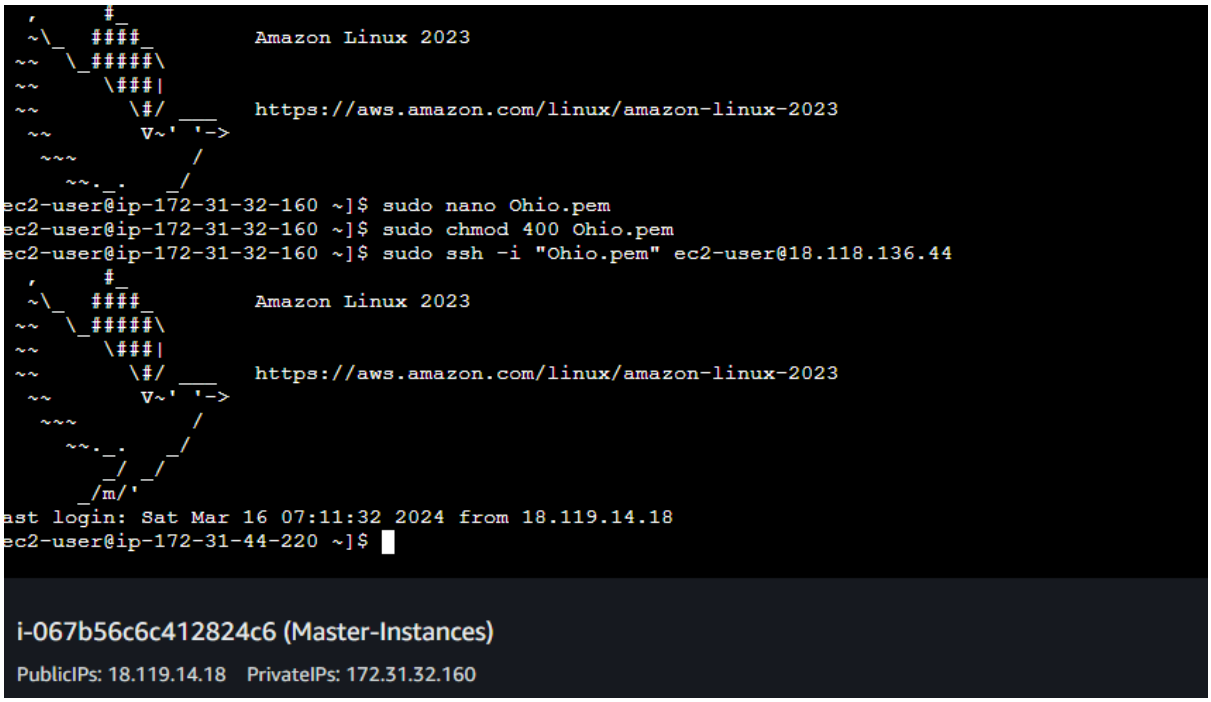
sudo yum update

sudo nano Name.pem

sudo chmod 400 Name.pem FOR sudo ssh -i Name.pem ec2-user@Public-IP(Login as a Super User)

sudo chmod 404 Name.pem FOR ssh -i Name.pem ec2-user@Public-IP(Because here U are not Login as Super User, U are Login as a Other/Everyone so U need Permsion to Read this file)

11. Successfully Connected to Client Instances



12. And We Confirm Client Instances Private and Public Ip