

Module 5: VPC Security Groups Assignment

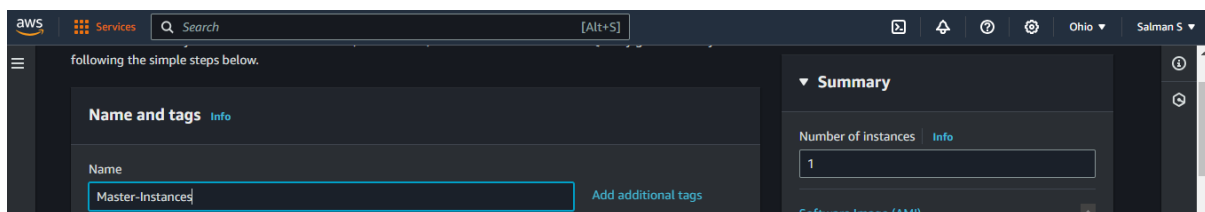
Problem Statement:

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



following the simple steps below.

Name and tags Info

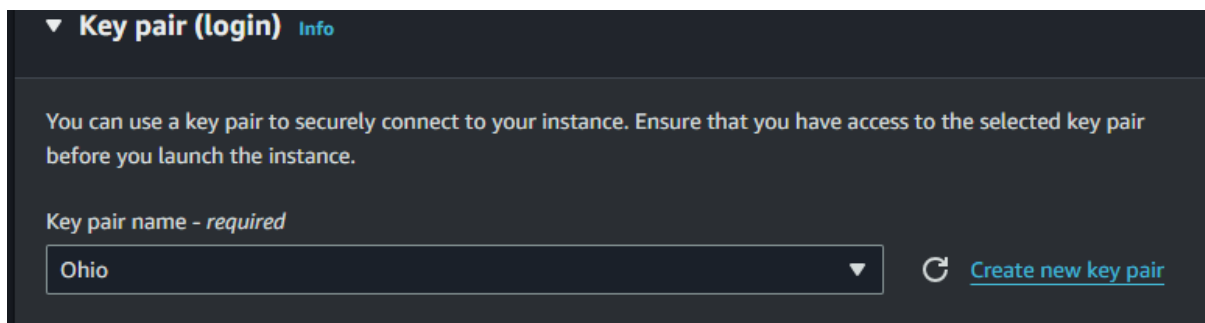
Name
Master-Instances Add additional tags

Summary

Number of instances Info
1

Software Image (AMI)

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



Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Ohio Create new key pair

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

The screenshot shows the 'Network settings' section in the AWS console. It includes fields for VPC (vpc-0a43b2bf5a440f958), Subnet (No preference), and Auto-assign public IP (Enable). Below these, there's a section for Firewall (security groups) with options to 'Create security group' or 'Select existing security group'. A 'Security group name' field is also present, containing 'Master-SG'.

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

The screenshot shows the 'Inbound Security Group Rules' configuration page. It displays a rule for 'ssh' access from 'Anywhere' (0.0.0.0/0) to port 22. A warning message states: 'Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.' A 'Launch instance' button is visible on the right.

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

The screenshot shows the 'Instances' console page. It lists a single instance named 'Master-Instances' with ID 'i-067b56c6c412824c6', which is in a 'Running' state. Below the instance list, the 'Instance summary' section shows the public IPv4 address '18.119.14.18' and the private IPv4 address '172.31.32.160'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
Master-Instances	i-067b56c6c412824c6	Running	t2.micro	-	View alarms	us-east-2c

Instance: i-067b56c6c412824c6 (Master-Instances)

Instance summary

Instance ID	Public IPv4 address	Private IPv4 addresses
i-067b56c6c412824c6 (Master-Instances)	18.119.14.18	172.31.32.160

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

The screenshot shows the 'Name and tags' section in the AWS console. It includes a 'Name' field containing 'Client-Instances' and an 'Add additional tags' button. The 'Summary' section on the right shows 'Number of instances' as 1 and 'Software Image (AMI)' as 'Amazon Linux 2 AMI'.

Client-SG

VPC - required Info

VPC - *required* | Info


```
vpc-0a43b2bf5a440f958
172.31.0.0/16
```

(default) ▼



Subnet Info

No preference

[Create new subnet](#) Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

- Create security group

- ☐ Select existing security group

Security group name - *required*

Client-SG

Master Instances only So Choose Custom and Type Public IP of MI and

Inbound Security Group Rules

Security group rule 1 (TCP, 22, 18.119.14.18/32, Allow SSH Access Master-Instances ...)

Remove

Type | Info

ssh

Protocol Info

Port range Info

Source type | Info

Custom

Source | Info

Q Add CIDR, prefix list or security

Description - optional Info

Allow SSH Access Master-Instance

18.119.14.18/32 X

Add security group rule

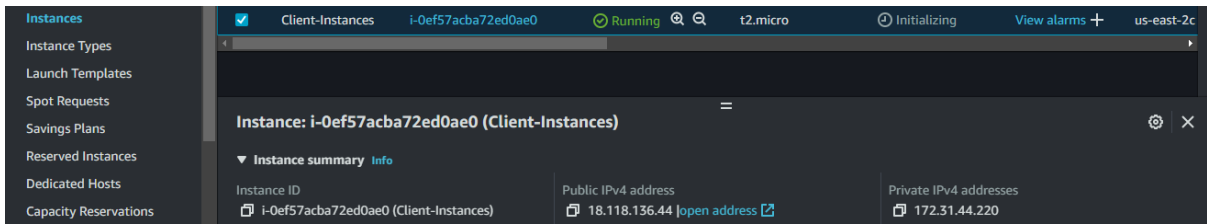
Master-Instances

Amazon Linux 2023

<https://aws.amazon.com/linux/amazon-linux-2023>

```
[ec2-user@ip-172-31-32-160 ~]$
```

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



***Follow the Commands:**

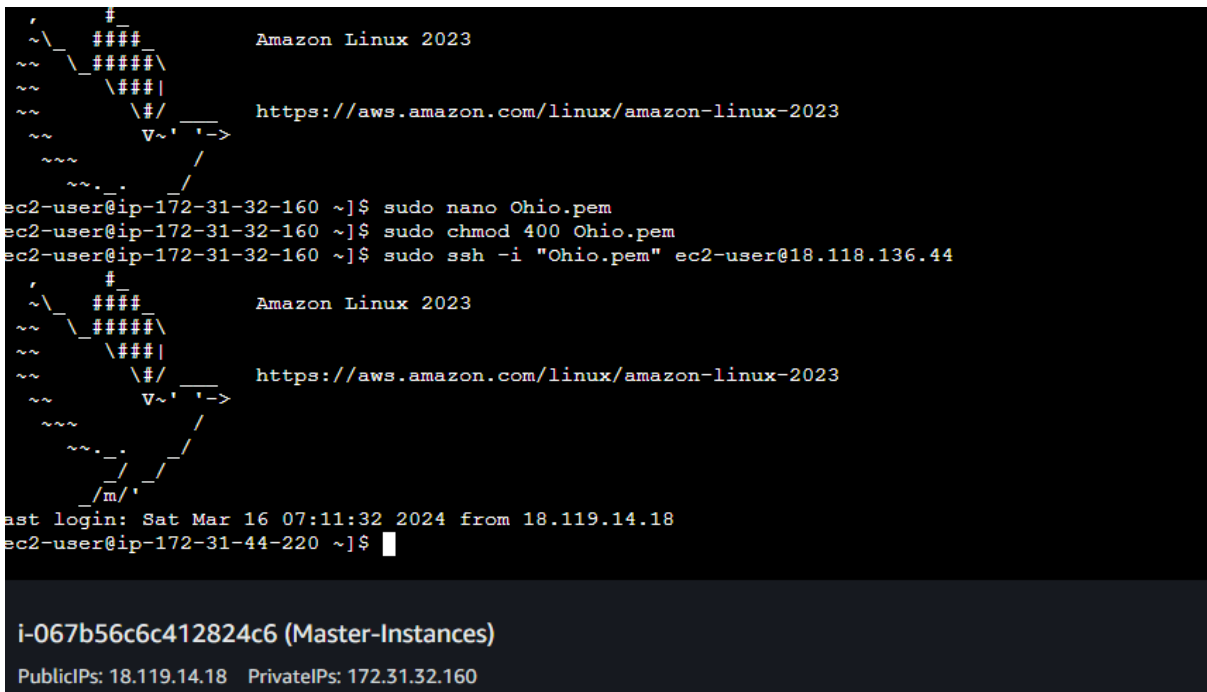
```
sudo yum update
```

```
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 Permission to Read this file)
```

11. Successfully Connected to **Client Instances**



12. And We Confirm Client Instances **Private and Public Ip**

