Implementing a Team Communication Solution using Mattermost and AWS (VPC| IGW | NAT instance | EC2 | Bastion host)

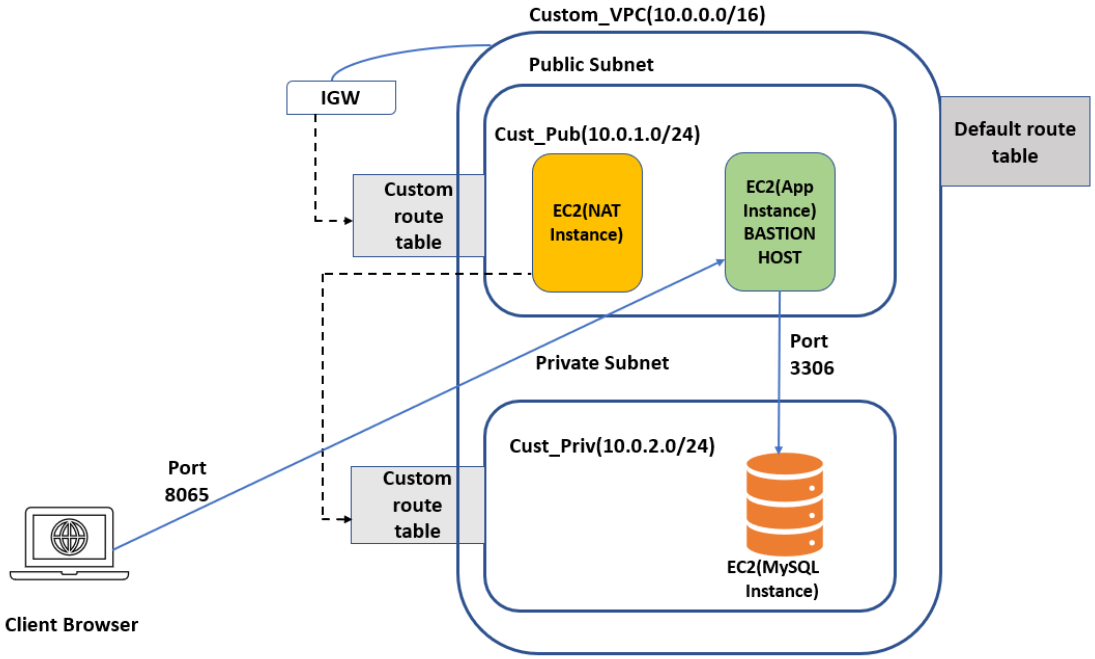
SCENARIO

Team communication and instant messaging solutions are an integral part of any business environment today. As of 2020, the total number of users of Slack and Microsoft Teams exceeded 20 million. Some organizations might have compliance policies in place which do not allow them to use services managed by third parties. We will design a communication solution that can be managed and hosted on servers controlled by the organization.

SOLUTION

Mattermost is an open-source, self-hostable online chat service. It is designed as an in-house chat platform for organizations and companies, and is mostly marketing itself as an open-source alternative to Slack. It uses a 3-tier architecture that can be hosted using an IaaS provider or on-premise servers. The purpose of this project is to deploy the trial version of the application on the public cloud i.e. AWS.

ARCHITECTURE



IMPLEMENTATION

- Implement 2 different subnets (one public and the other private) in a custom VPC
- Install and configure MySQL on an Ubuntu 18.04 instance on the private subnet
- Install and configure Mattermost Application on an Ubuntu 18.04 instance on the public subnet (This will be used as a bastion host to connect to the MySQL private instance)
- Provision a NAT instance on the public subnet
- Configure the security groups to allow the ports as shown in the architecture.

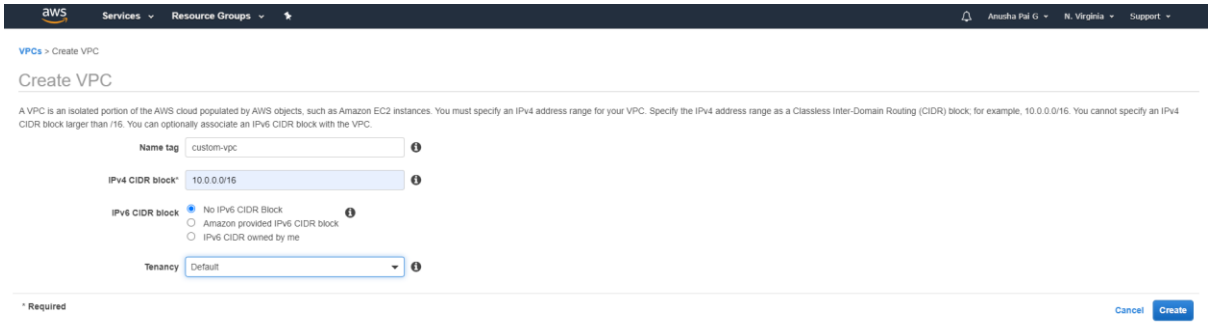
Client(web browser) – port 8065 –> Mattermost instance
Mattermost instance – port 3306 – >MySQL instance

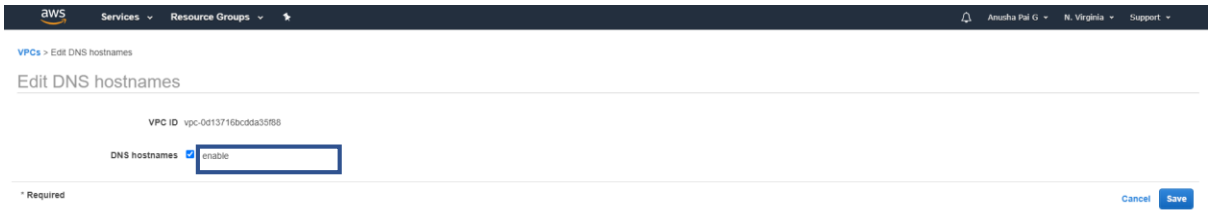
- Test the installation by accessing the IP of the public instance(Mattermost) in a browser against the port 8065.

STEPS

REGION : North Virginia

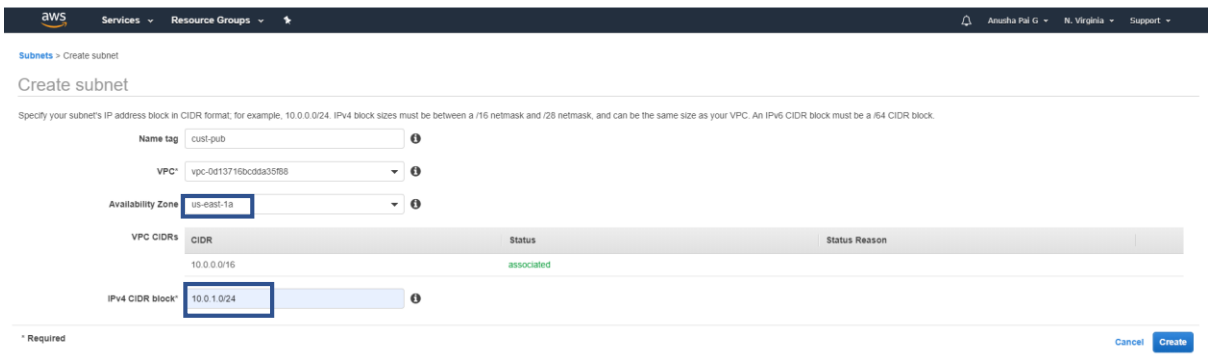
- Create a custom VPC (10.0.0.0/16) and enable DNS hostname option for the created VPC



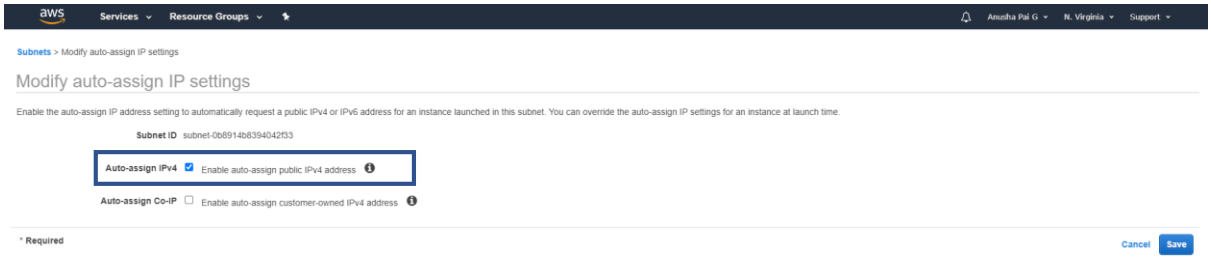


- Create 2 subnets in the Custom VPC

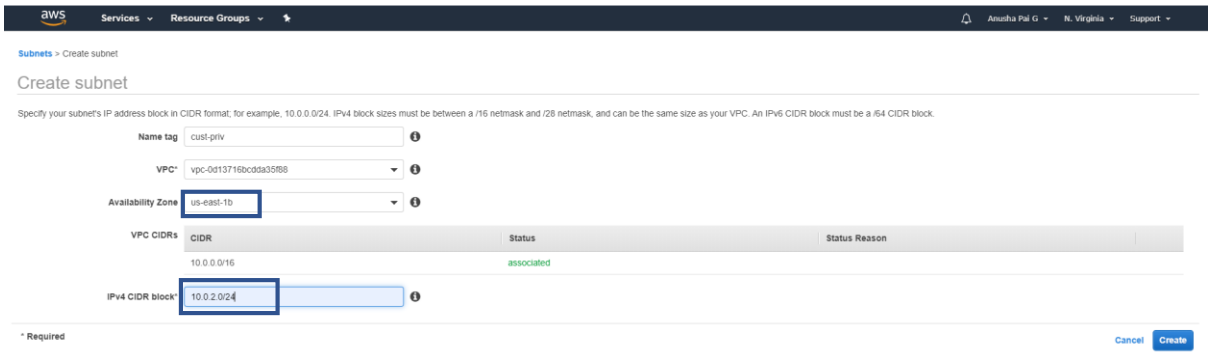
a) Public subnet (cust-pub : 10.0.1.0/24 : us-east-1a AZ)



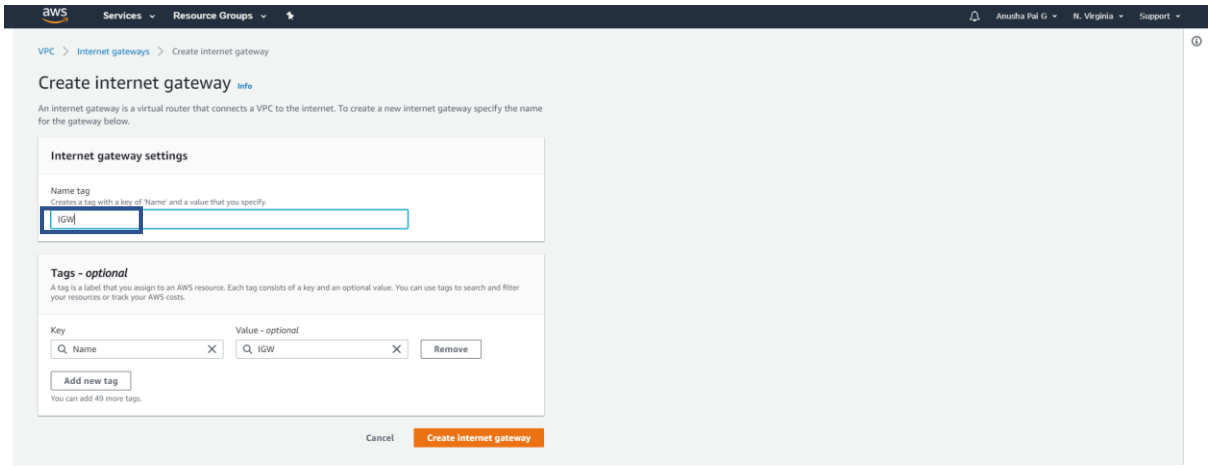
Enable auto assign public IPv4 address for cust-pub subnet only as we need a public IP to connect to the Bastion Host



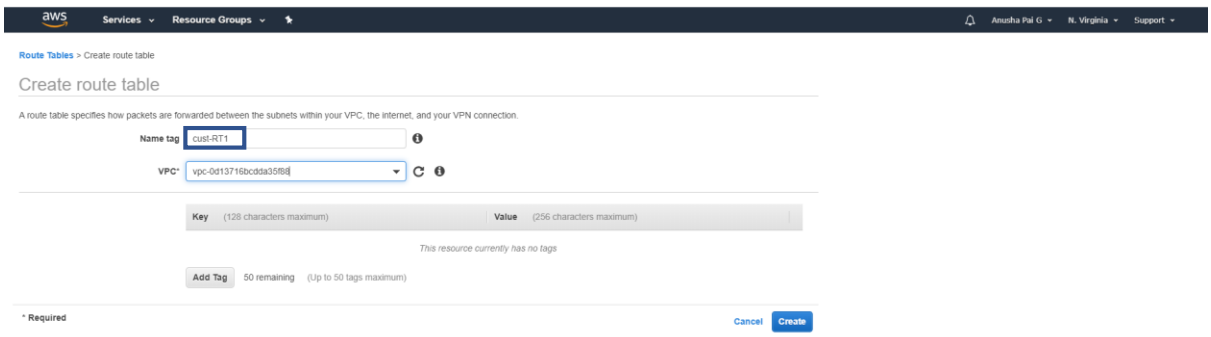
b) Private subnet (cust-priv : 10.0.2.0/16 : us-east-1b AZ)



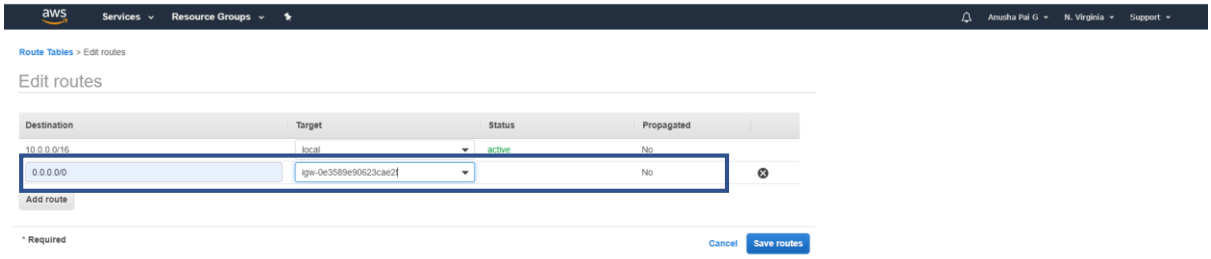
- Create Internet Gateway and attach it to the custom VPC



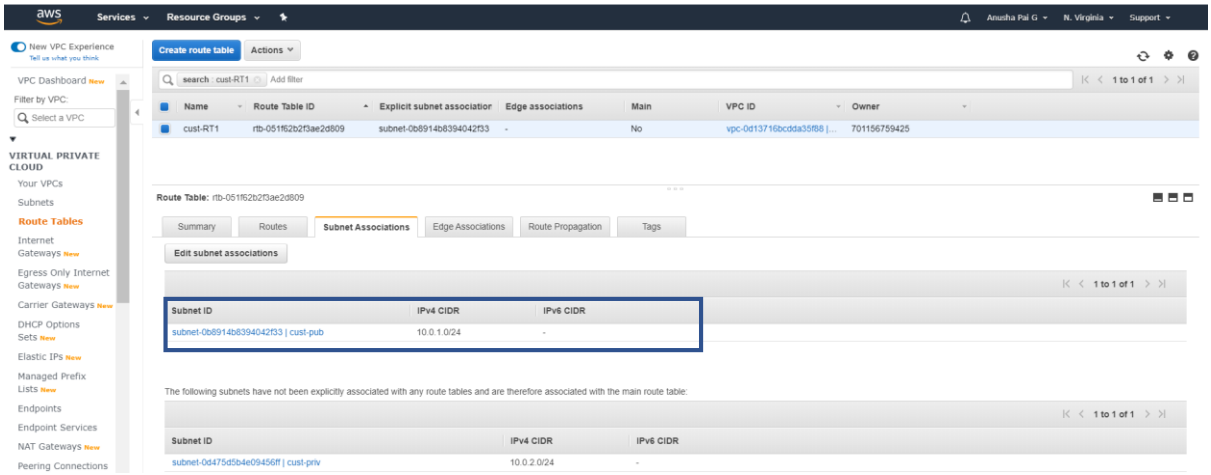
- Create a custom Route Table and associate it with the public subnet only so that it becomes internet facing and the private subnet is inaccessible to the internet



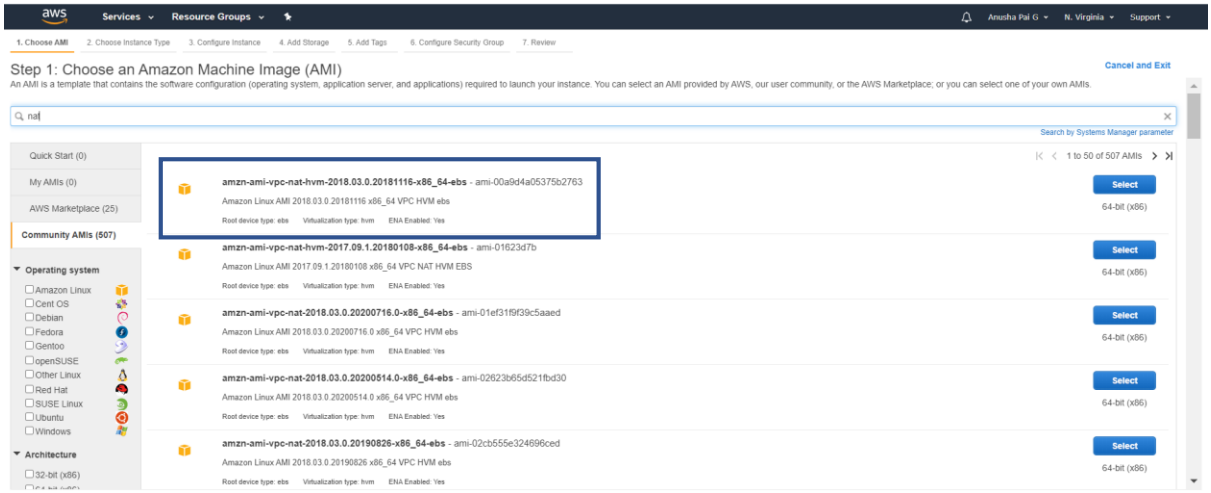
Add a route to reach internet via the IGW

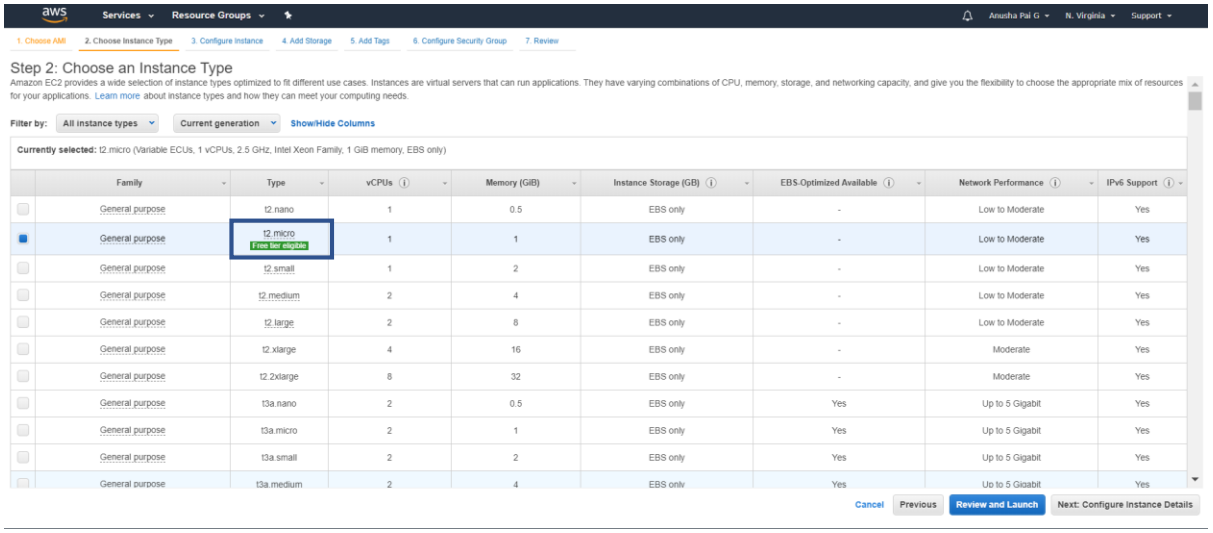


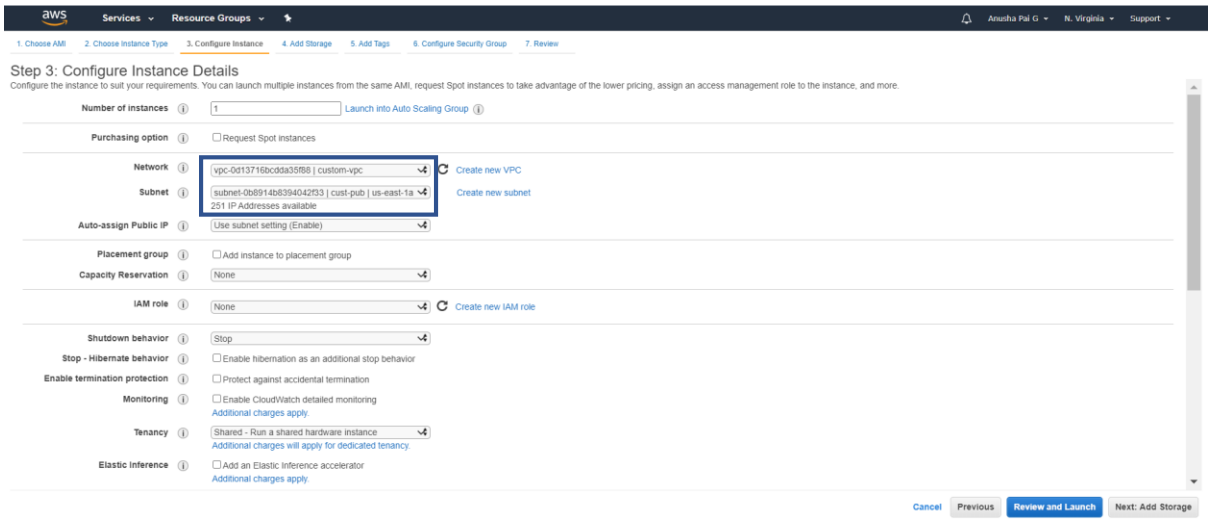
Associate the public subnet with the custom route table created

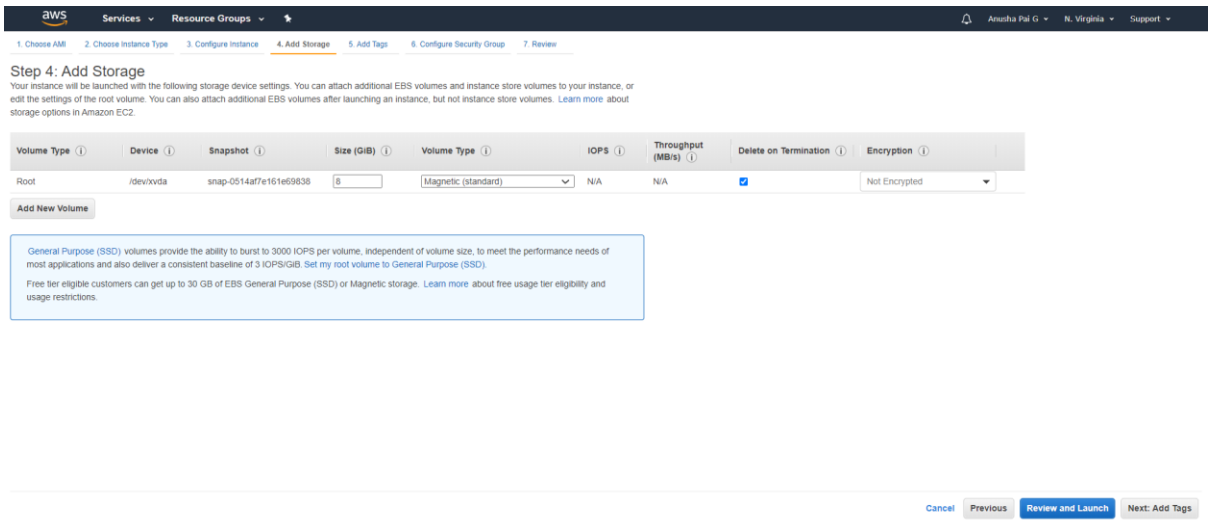


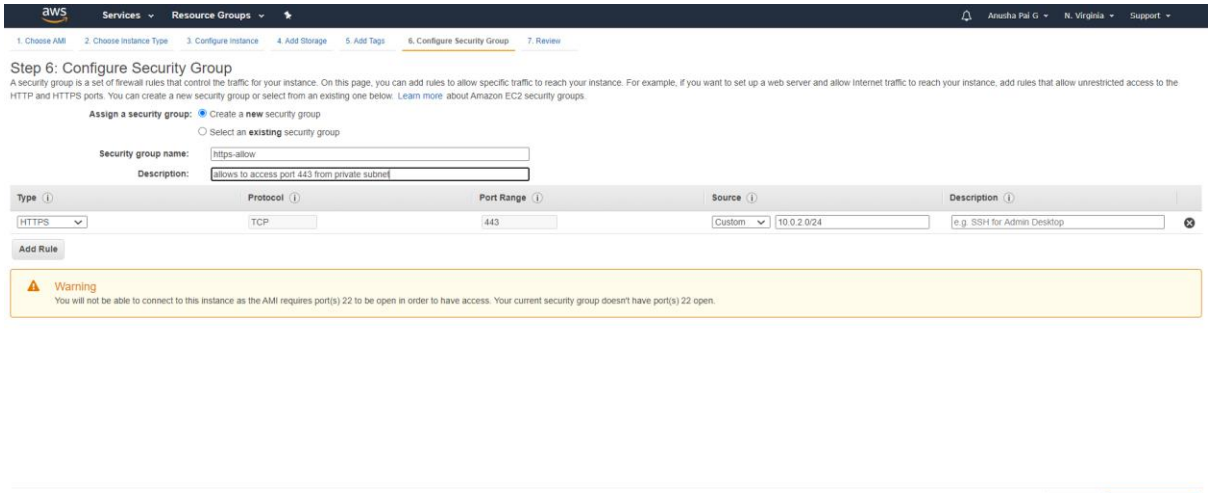
- Navigate to EC2 and Create a NAT instance in the public subnet

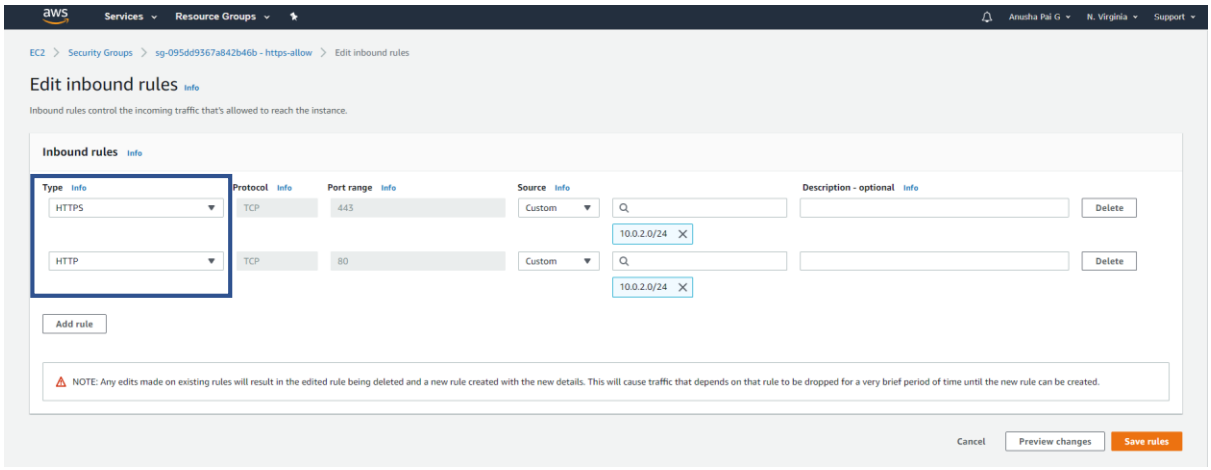



Services
Resource Groups
Anusha Pai G
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
Filter by:
All instance types
Current generation
Show/Hide Columns
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)
Family
Type
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
IPv6 Support
General purpose
t2.nano
1
0.5
EBS only
-
Low to Moderate
Yes
t2.micro
Free tier eligible
t2.small
t2.medium
t2.large
t2.xlarge
Moderate
t2.2xlarge
8
32
t3a.nano
Yes
Up to 5 Gigabit
t3a.micro
t3a.small
t3a.medium
Cancel
Previous
Review and Launch
Next: Configure Instance Details


Services
Resource Groups
Anusha Pai G
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-0d13716bcdda35f88 | custom-vpc
Create new VPC
Subnet
subnet-0b8914b8394042f33 | cust-pub | us-east-1a
251 IP Addresses available
Create new subnet
Auto-assign Public IP
Use subnet setting (Enable)
Placement group
Add instance to placement group
Capacity Reservation
None
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Stop - Hibernate behavior
Enable hibernation as an additional stop behavior
Enable termination protection
Protect against accidental termination
Monitoring
Enable CloudWatch detailed monitoring
Additional charges apply.
Tenancy
Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.
Elastic Inference
Add an Elastic Inference accelerator
Additional charges apply.
Cancel
Previous
Review and Launch
Next: Add Storage


Services
Resource Groups
Anusha Pai G
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.
Volume Type
Device
Snapshot
Size (GiB)
Volume Type
IOPS
Throughput (MB/s)
Delete on Termination
Encryption
Root
/dev/xvda
snap-0514af7e161e69838
8
Magnetic (standard)
N/A
N/A
Not Encrypted
Add New Volume
General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB. Set my root volume to General Purpose (SSD).
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.
Cancel
Previous
Review and Launch
Next: Add Tags

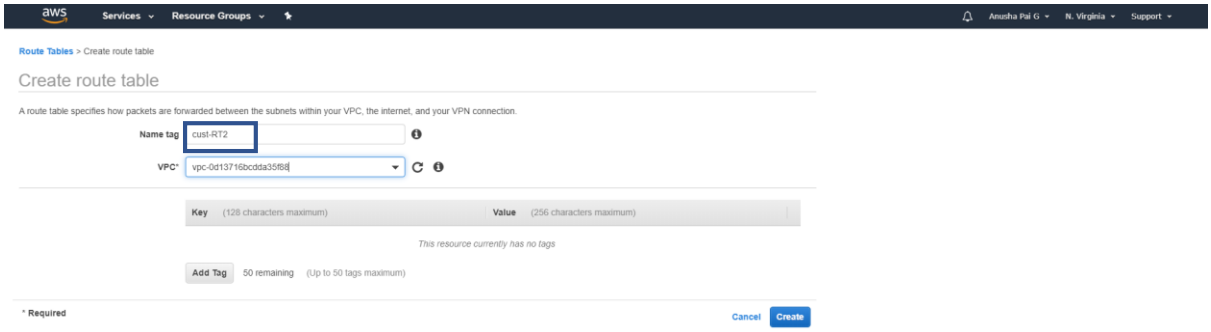




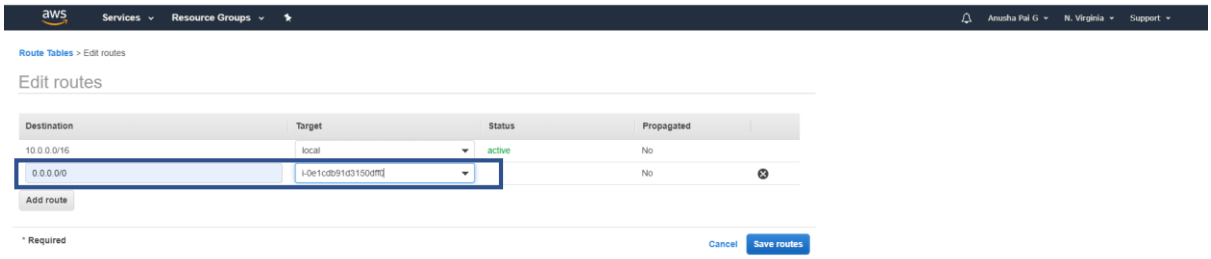
NOTE : Disable Source/Destination check in the NAT instance by selecting the instance and navigating to Actions->Networking->Change Source/Dest. Check

Why is this done ? All EC2 instances by default do source and destination checks i.e. the instance must either be a source or destination for any traffic it sends or receives. NAT instance acts as a GW and should be able to send or receive traffic i.e. NAT instance is not a source/destination.

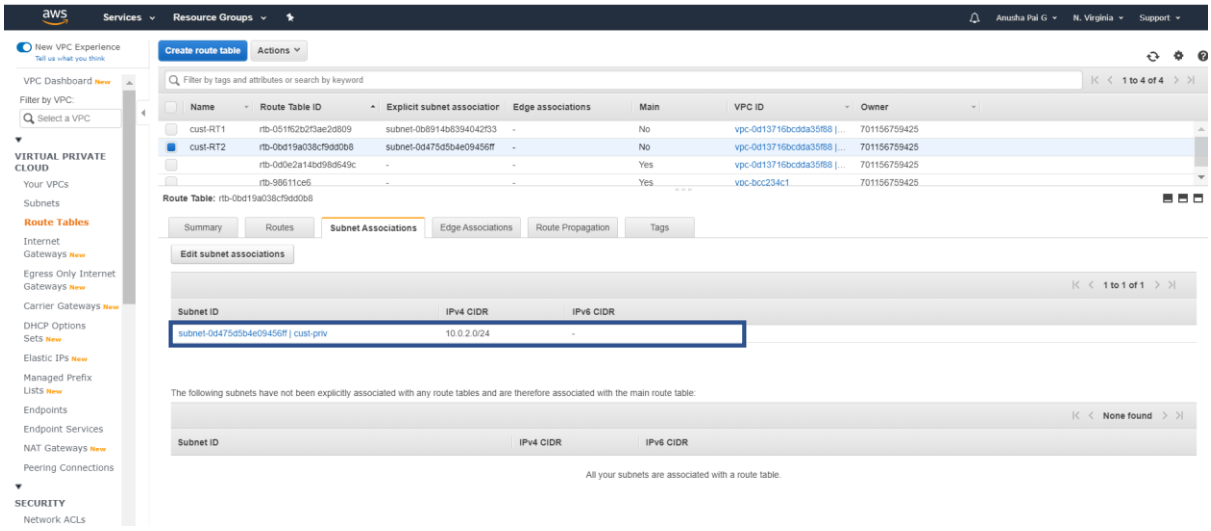
- Create the custom route table and associate it with the private subnet



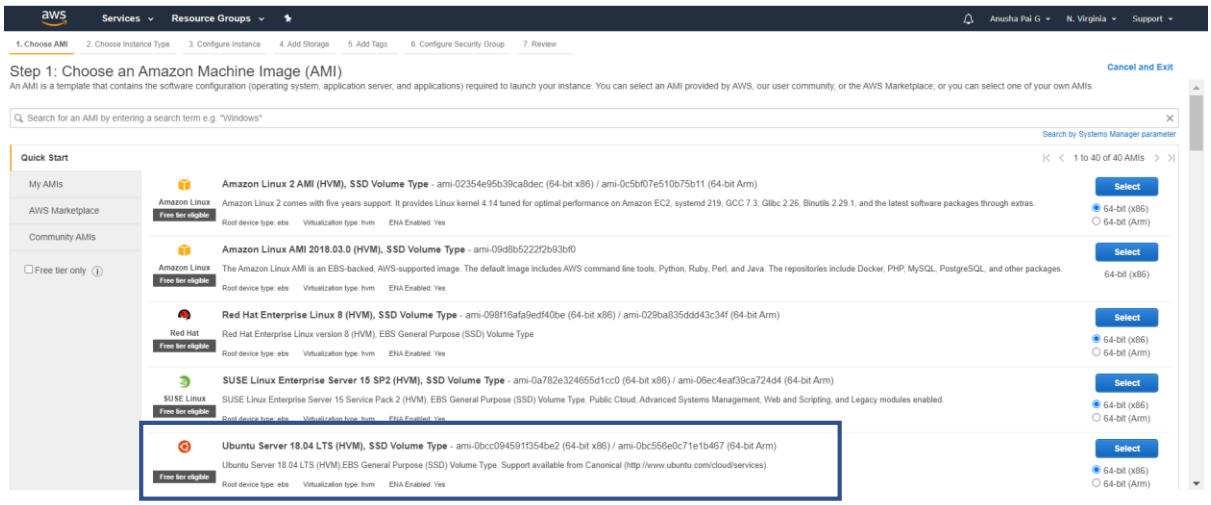
Add a route to reach internet via NAT instance

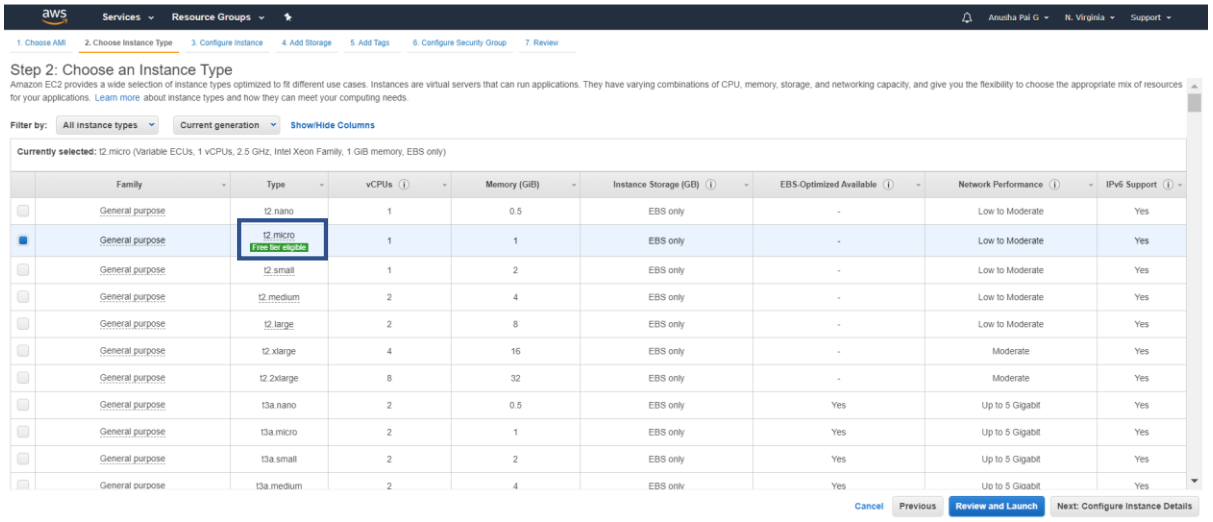


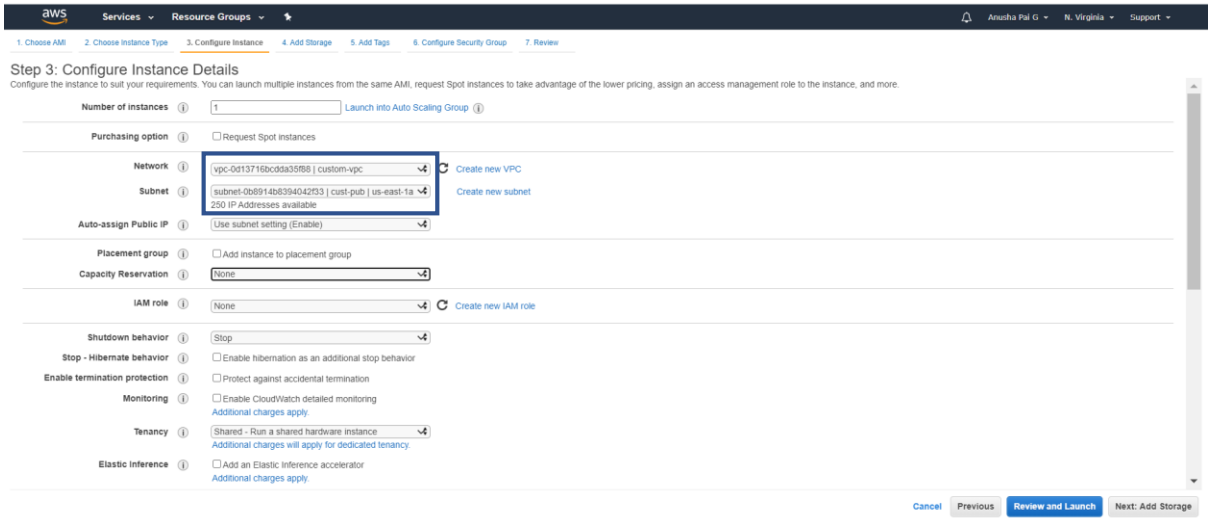
Associate the private subnet with the custom route table created

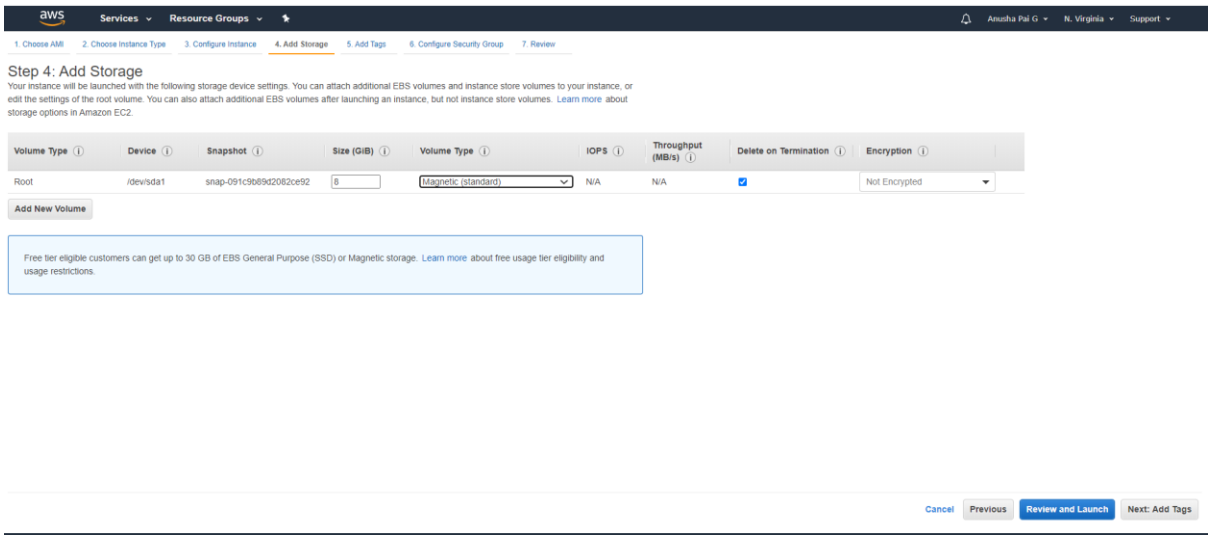


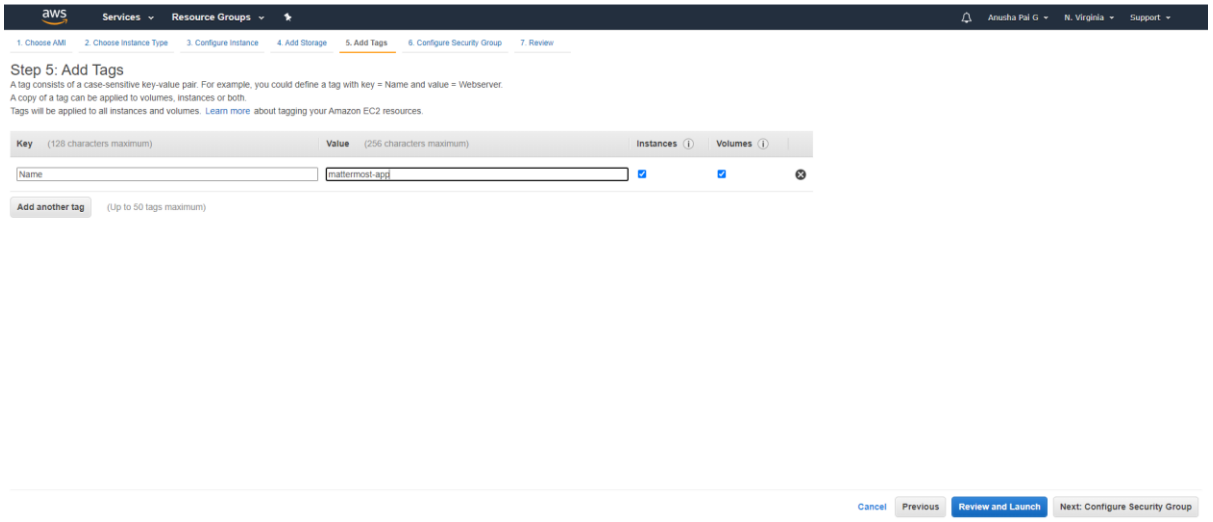
- Create the application server in public subnet

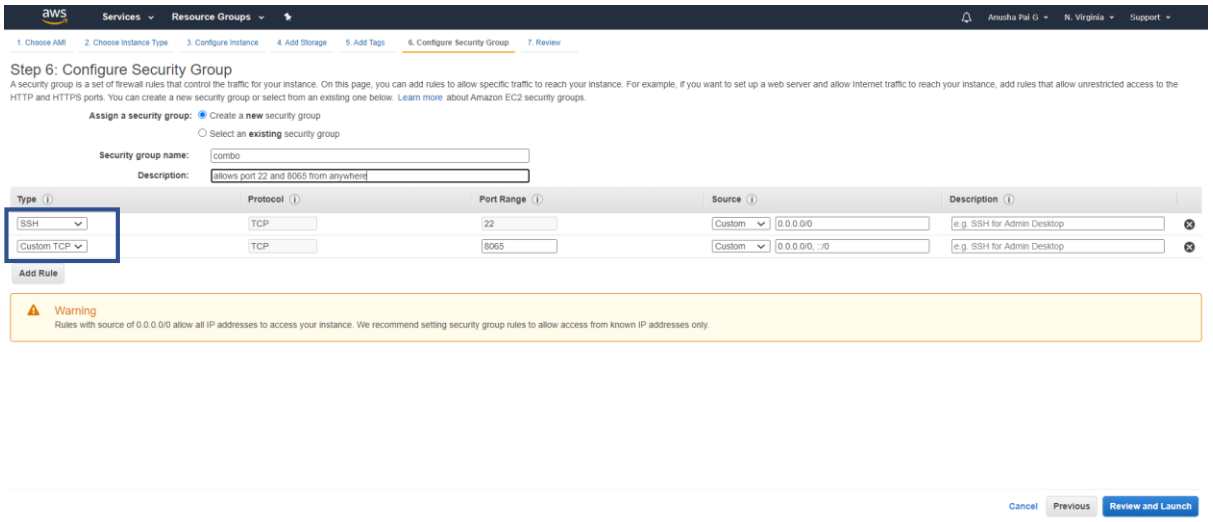



Services
Resource Groups
Anusha Pal G
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
Filter by:
All instance types
Current generation
Show/Hide Columns
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)
Family
Type
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
IPv6 Support
General purpose
t2.nano
1
0.5
EBS only
-
Low to Moderate
Yes
General purpose
t2.micro
Free tier eligible
1
1
EBS only
-
Low to Moderate
Yes
General purpose
t2.small
1
2
EBS only
-
Low to Moderate
Yes
General purpose
t2.medium
2
4
EBS only
-
Low to Moderate
Yes
General purpose
t2.large
2
8
EBS only
-
Low to Moderate
Yes
General purpose
t2.xlarge
4
16
EBS only
-
Moderate
Yes
General purpose
t2.2xlarge
8
32
EBS only
-
Moderate
Yes
General purpose
t3a.nano
2
0.5
EBS only
Yes
Up to 5 Gigabit
Yes
General purpose
t3a.micro
2
1
EBS only
Yes
Up to 5 Gigabit
Yes
General purpose
t3a.small
2
2
EBS only
Yes
Up to 5 Gigabit
Yes
General purpose
t3a.medium
2
4
EBS only
Yes
Up to 5 Gigabit
Yes
Cancel
Previous
Review and Launch
Next: Configure Instance Details

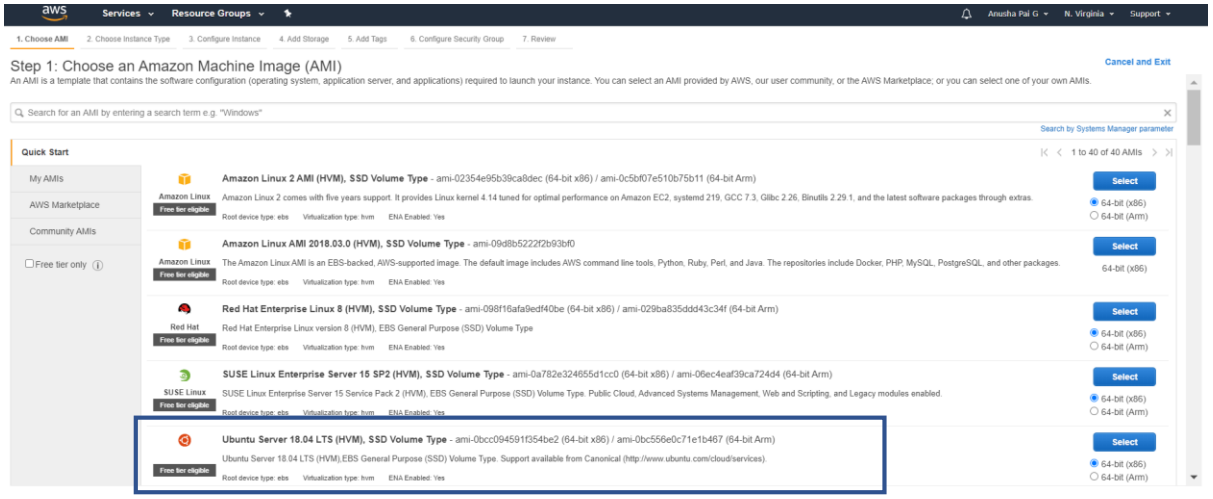

Services
Resource Groups
Anusha Pal G
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-0d13716bcdda35f88 | custom-vpc
Create new VPC
Subnet
subnet-0b8914b8394042f33 | cust-pub | us-east-1a
250 IP Addresses available
Create new subnet
Auto-assign Public IP
Use subnet setting (Enable)
Placement group
Add instance to placement group
Capacity Reservation
None
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Stop - Hibernate behavior
Enable hibernation as an additional stop behavior
Enable termination protection
Protect against accidental termination
Monitoring
Enable CloudWatch detailed monitoring
Additional charges apply.
Tenancy
Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.
Elastic Inference
Add an Elastic Inference accelerator
Additional charges apply.
Cancel
Previous
Review and Launch
Next: Add Storage

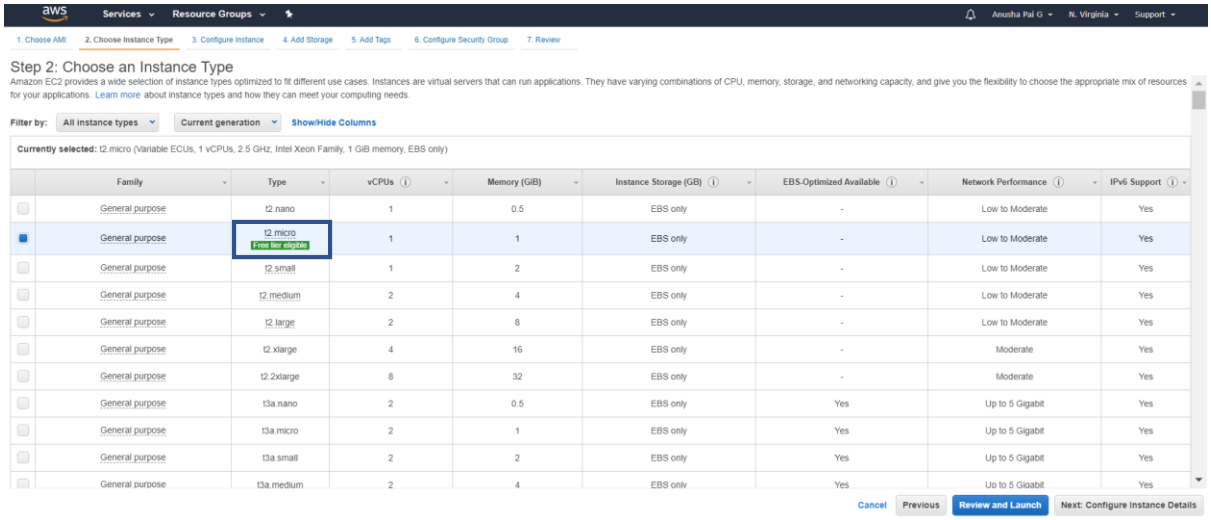

Services
Resource Groups
Anusha Pal G
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.
Volume Type
Device
Snapshot
Size (GiB)
Volume Type
IOPS
Throughput (MB/s)
Delete on Termination
Encryption
Root
/dev/sda1
snap-091c9b89d2082ce92
8
Magnetic (standard)
N/A
N/A
Not Encrypted
Add New Volume
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.
Cancel
Previous
Review and Launch
Next: Add Tags

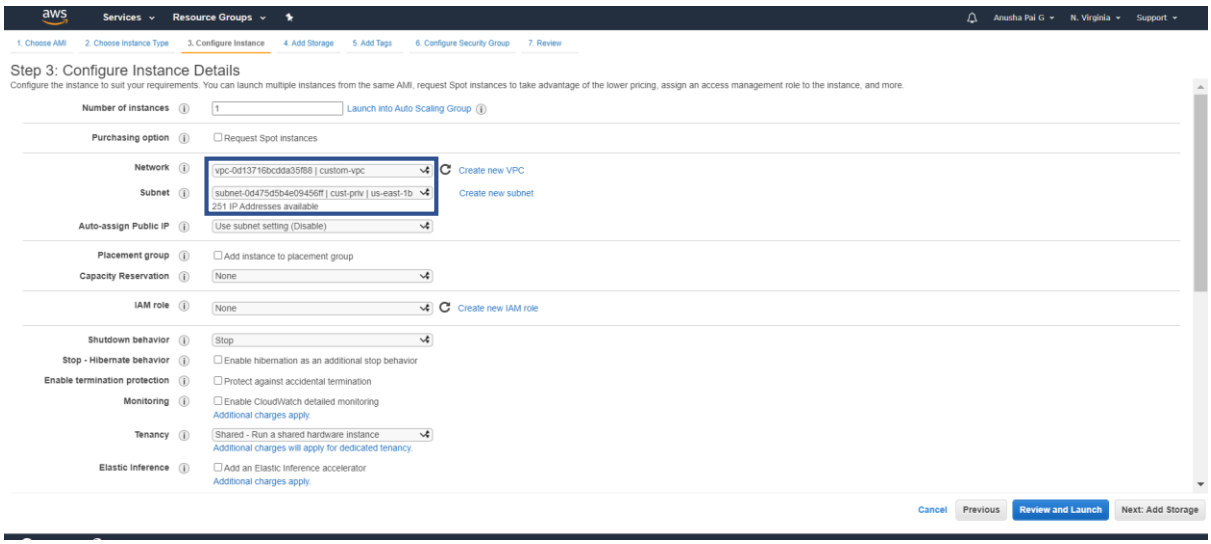


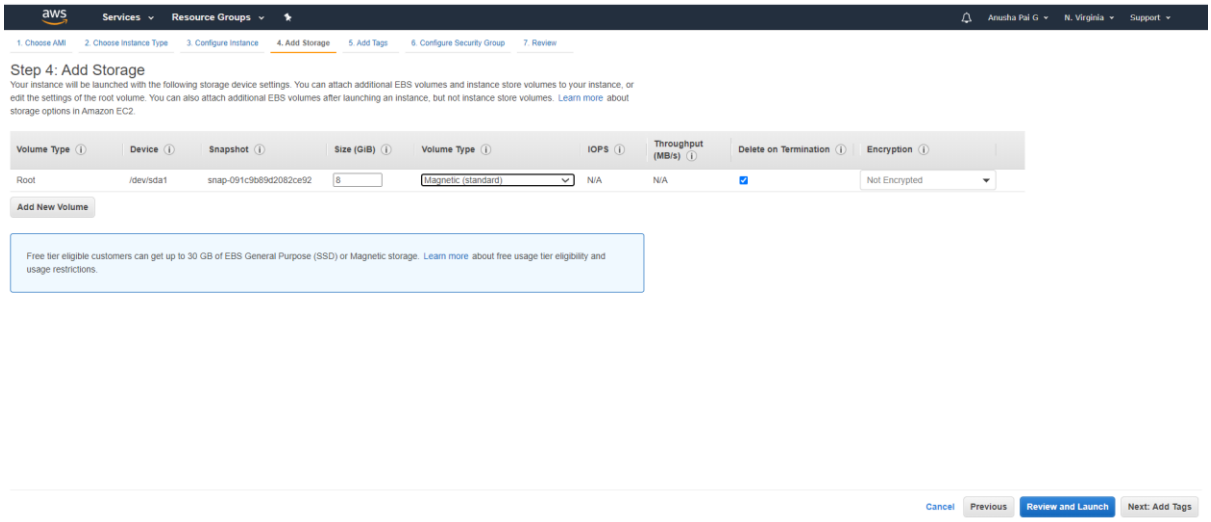


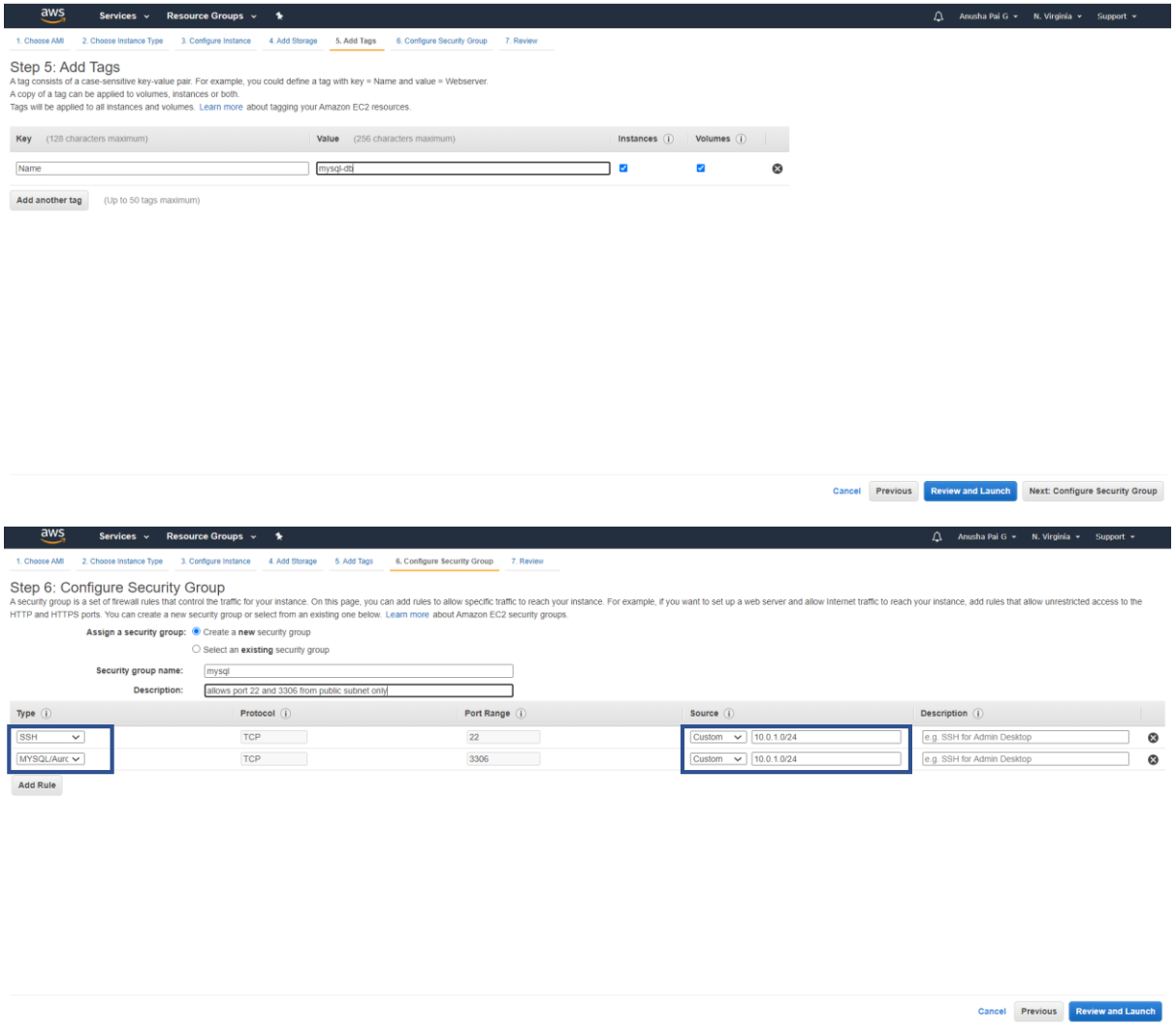
- Create DB server in the private subnet




Services
Resource Groups
Anusha Pai G
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
Filter by:
All instance types
Current generation
Show/Hide Columns
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)
Family
Type
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
IPv6 Support
General purpose
t2.nano
1
0.5
EBS only
-
Low to Moderate
Yes
t2.micro
Free tier eligible
1
1
EBS only
-
Low to Moderate
Yes
t2.small
2
EBS only
t2.medium
4
t2.large
8
t2.xlarge
16
Moderate
t2.2xlarge
32
t3a.nano
0.5
Yes
Up to 5 Gigabit
t3a.micro
t3a.small
t3a.medium
Cancel
Previous
Review and Launch
Next: Configure Instance Details


Services
Resource Groups
Anusha Pai G
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-0d13716bcdda35f88 | custom-vpc
Create new VPC
Subnet
subnet-0d475d5b4e09456ff | cust-priv | us-east-1b
Create new subnet
251 IP Addresses available
Auto-assign Public IP
Use subnet setting (Disable)
Placement group
Add instance to placement group
Capacity Reservation
None
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Stop - Hibernate behavior
Enable hibernation as an additional stop behavior
Enable termination protection
Protect against accidental termination
Monitoring
Enable CloudWatch detailed monitoring
Additional charges apply.
Tenancy
Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.
Elastic Inference
Add an Elastic Inference accelerator
Additional charges apply.
Cancel
Previous
Review and Launch
Next: Add Storage


Services
Resource Groups
Anusha Pai G
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.
Volume Type
Device
Snapshot
Size (GiB)
Volume Type
IOPS
Throughput (MB/s)
Delete on Termination
Encryption
Root
/dev/sda1
snap-091c9b89d2082ce92
8
Magnetic (standard)
N/A
N/A
Not Encrypted
Add New Volume
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.
Cancel
Previous
Review and Launch
Next: Add Tags



- Copy the pem file for the Database Server to the Application Server to use it as a Bastion Host
  The command is as follows scp -i <pem file of the application server> <path to pem file of the DB server> ubuntu@<public IP address of the application server>:/home/ubuntu

  NOTE : For the purposes of this demonstration, we have used the same pem file for the application and database server.

```
PS C:\Users\Anusha> Copy-Item 'D:\PGP CC GL\project solution\trial.pem'
PS C:\Users\Anusha> attrib.exe -a .\trial.pem
PS C:\Users\Anusha> attrib.exe +r .\trial.pem
PS C:\Users\Anusha> scp -i .\trial.pem trial.pem ubuntu@52.206.252.226:/home/ubuntu
The authenticity of host '52.206.252.226 (52.206.252.226)' can't be established.
ECDSA key fingerprint is SHA256:vxpk84iuxTrDiEVDAQvyxvSYayuzdqFemVaDJ3eK110.
Are you sure you want to continue connecting (yes/no)?
Please type 'yes' or 'no':
Warning: Permanently added '52.206.252.226' (ECDSA) to the list of known hosts.
trial.pem                                                     100% 1696     1.7KB/s   00:01
PS C:\Users\Anusha>
```

- Log into the application server and use it as a Bastion Host to log into the database server

  ssh -i .\trial.pem ubuntu@52.206.252.226

cd /home/ubuntu/
chmod 400 trial.pem
ssh -i trial.pem ubuntu@10.0.2.19

NOTE : we are using the private IP of the database server to log into it since it does not have a public IP/DNS address.

- Install and configure DB server as below
  1. Download the script
     cd /opt
     sudo wget https://storage.googleapis.com/skl-training/aws-codelabs/mattermost/install_mysql.sh

```
ubuntu@ip-10-0-2-90:/opt$ cat install_mysql.sh
#!/bin/bash
apt update -y
apt install mysql-server -y
echo "Installed MySQL"
echo "Configuring MySQL now"


mysql -u root <<-EOF
UPDATE mysql.user SET authentication_string=PASSWORD('password') WHERE User='root';
DELETE FROM mysql.user WHERE User='root' AND Host NOT IN ('localhost', '127.0.0.1', '::1');
DELETE FROM mysql.user WHERE User='';
DELETE FROM mysql.db WHERE Db='test' OR Db='test_%';
FLUSH PRIVILEGES;
CREATE USER 'mmuser'@'%' IDENTIFIED BY 'mostest';
CREATE DATABASE mattermost_test;
GRANT ALL PRIVILEGES ON mattermost_test.* TO 'mmuser'@'%';
EOF

echo "MySQL Congiguration complete"
sed "s/bind-address/#bind-address/" /etc/mysql/mysql.conf.d/mysqld.cnf > mysqld.cnf
mv mysqld.cnf /etc/mysql/mysql.conf.d/mysqld.cnf

/etc/init.d/mysql restart
ubuntu@ip-10-0-2-90:/opt$
```

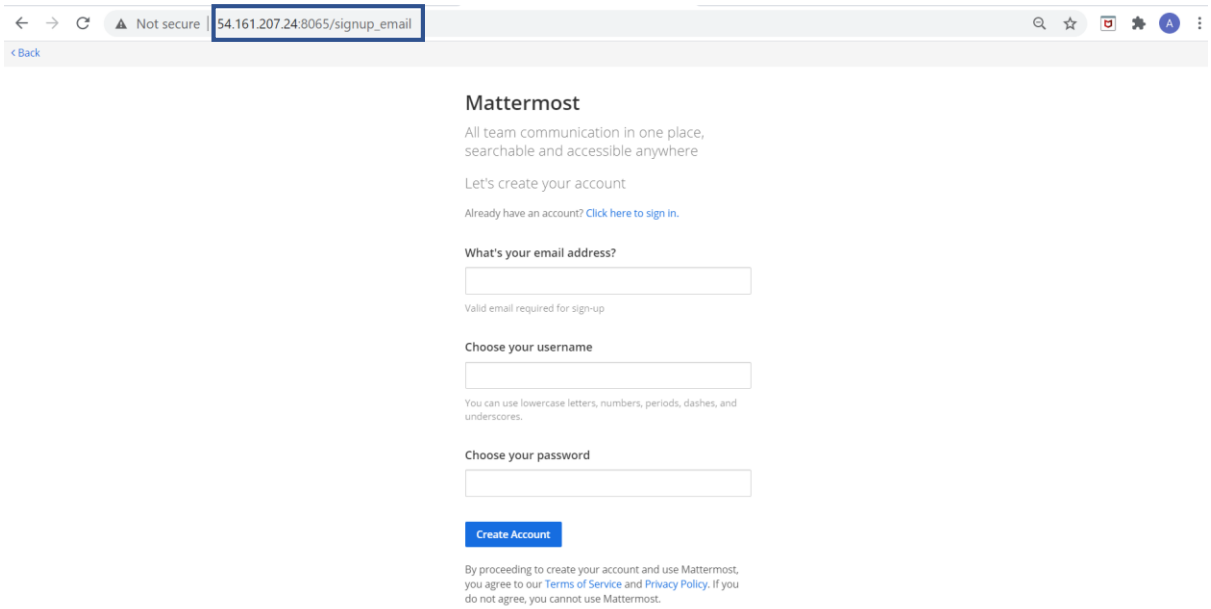
  2. Run the script
     sudo chmod 700 install_mysql.sh
     sudo ./install_mysql.sh
  3. Log out of the database server to go back into the application server

- Install the Mattermost application and configure the app server
  1. Download the script using the following command
     cd /opt
     sudo wget https://storage.googleapis.com/skl-training/aws-codelabs/mattermost/mattermost_install.sh

```
ubuntu@ip-10-0-1-6:/opt$ cat mattermost_install.sh
#!/bin/bash
wget https://releases.mattermost.com/5.19.0/mattermost-5.19.0-linux-amd64.tar.gz
echo "Downloaded Mattermost"
tar -xvzf mattermost*.gz
echo "Extracted Mattermost"
mv mattermost /opt
mkdir /opt/mattermost/data
useradd --system --user-group mattermost
echo "Created user"
sed "s/localhost:3306/$1:3306/" /opt/mattermost/config/config.json > config.json
mv config.json /opt/mattermost/config/config.json
ubuntu@ip-10-0-1-6:/opt$
```

2. Run the script :
   sudo chmod 700 mattermost_install.sh
   sudo ./mattermost_install.sh <private_IP_of_mysql_server>
   sudo chown -R mattermost:mattermost /opt/mattermost
   sudo chmod -R g+w /opt/mattermost
3. Run the Mattermost server:
   cd /opt/mattermost
   sudo -u mattermost ./bin/mattermost

- Test the success of the implementation by visiting the public IP of the application server in your browser with the port 8065


Not secure
54.161.207.24:8065/signup_email
Back
Mattermost
All team communication in one place, searchable and accessible anywhere
Let's create your account
Already have an account? Click here to sign in.
What's your email address?
Valid email required for sign-up
Choose your username
You can use lowercase letters, numbers, periods, dashes, and underscores.
Choose your password
Create Account
By proceeding to create your account and use Mattermost, you agree to our Terms of Service and Privacy Policy. If you do not agree, you cannot use Mattermost.