Declaration	
Questions in this exercise are intentionally complex and could be convoluted or confusing. This is by design and to simulate real life situations where customers seldom give crystal clear requirements and ask unambiguous questions.	
I have read the above statement and agree to these conditions	
I AGREE	Alka Sinha
	<Enter your name above this line to indicate that you are in agreement>

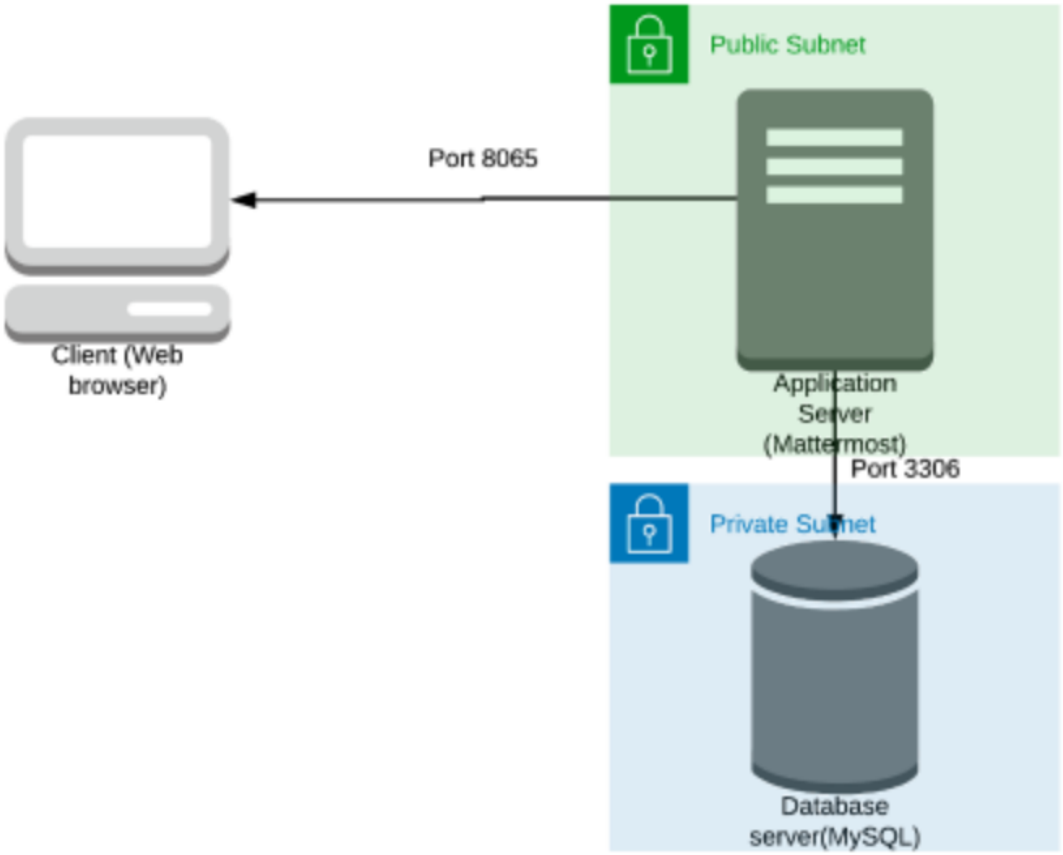
Instructions
Every screenshot requested in this workbook is compulsory and carries 0.5 marks
Your AWS account ID must be clearly visible in every screenshot using the AWS console; missing id or using someone else's id is not permitted. Such cases will be considered as plagiarism and severe penalty will be imposed.
All screenshots must be in the order mentioned under "Expected Screenshots" for every step
DO NOT WAIT UNTIL THE LAST MINUTE. The program office will not extend the project submission deadline under any circumstances.
The file should be renamed in the format BATCH_FIRSTNAME_LASTNAME_PROJECT1. For example: PGPCCMAY18_VIJAY_DWIVEDI_PROJECT1.pdf

Resource Clean Up
Cloud is always pay per use model and all resources/services that we consume are chargeable. Cleaning up when you've completed your lab or project is always necessary. This is true whether you're doing a lab or implementing a project at your workplace.
After completing the lab, make sure to delete each resource created in reverse chronological order.

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. They will prefer solutions that can be managed and hosted on servers controlled by them. The same will extend to communication solutions as well.

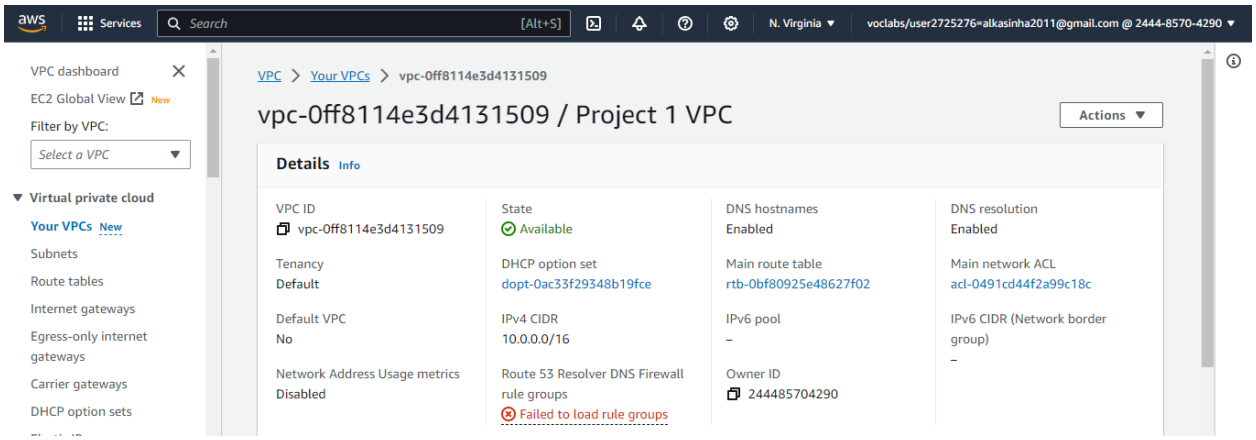
Architecture diagram



Architecture Implementation	
1	Implement 2 different subnets (one public and the other private) in a custom VPC
2	Install and configure MySQL on an Amazon Linux 2 instance on the private subnet using the instructions provided. (Hint: Use a bastion host and a NAT gateway)
3	Install and configure Mattermost on an Amazon Linux 2 instance on the public subnet using the provided instructions.
4	Configure the security groups to allow the ports as shown in the architecture.
5	Test the installation by accessing the IP of the public instance in a browser via the port 8065.

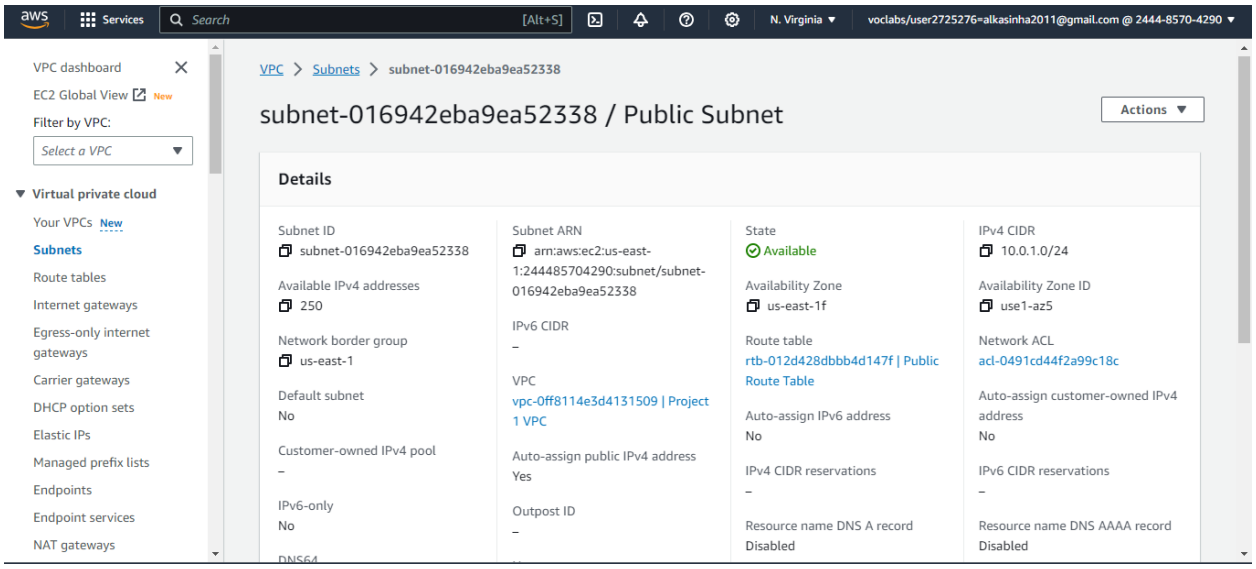
Step 1: VPC and Subnet Creation

Step number	a
Step name	Creation of VPC
Instructions	1) Navigate to VPC using the Services button at the top of the screen 2) Select "Your VPCs" on the left side of the screen 3) Click on "Create VPC" 4) Enter the following fields : Name: Project 1 VPC IPv4 CIDR Block : 10.0.0.0/16 The rest of the options can be ignored 5) Select "Create VPC" 6) Select the VPC and click on Actions->Edit DNS hostnames 7) Enable DNS hostnames and click on Save
Expected screenshots	1) Created VPC with properties visible

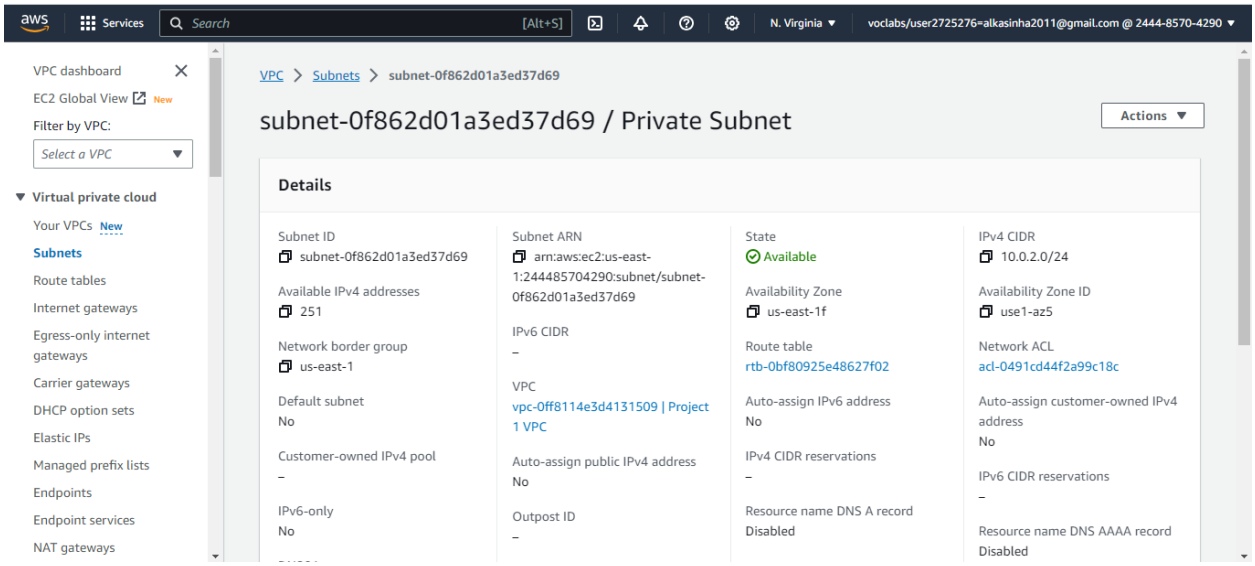


Step number	b
Step name	Creation of public subnet
Instructions	1) Navigate to VPC->Subnets 2) Click on "Create Subnet" 3) Enter the following fields Name tag : Public Subnet VPC : Select the Project 1 VPC IPv4 CIDR block : 10.0.1.0/24 The other options can be ignored 4) Click on Create 5) Once the subnet has been created, select the subnet and click on Actions->Modify Auto-assign IP settings 6) Enable the option "Auto assign IPv4" and select Save

Expected screenshots	1) Subnet Creation screen

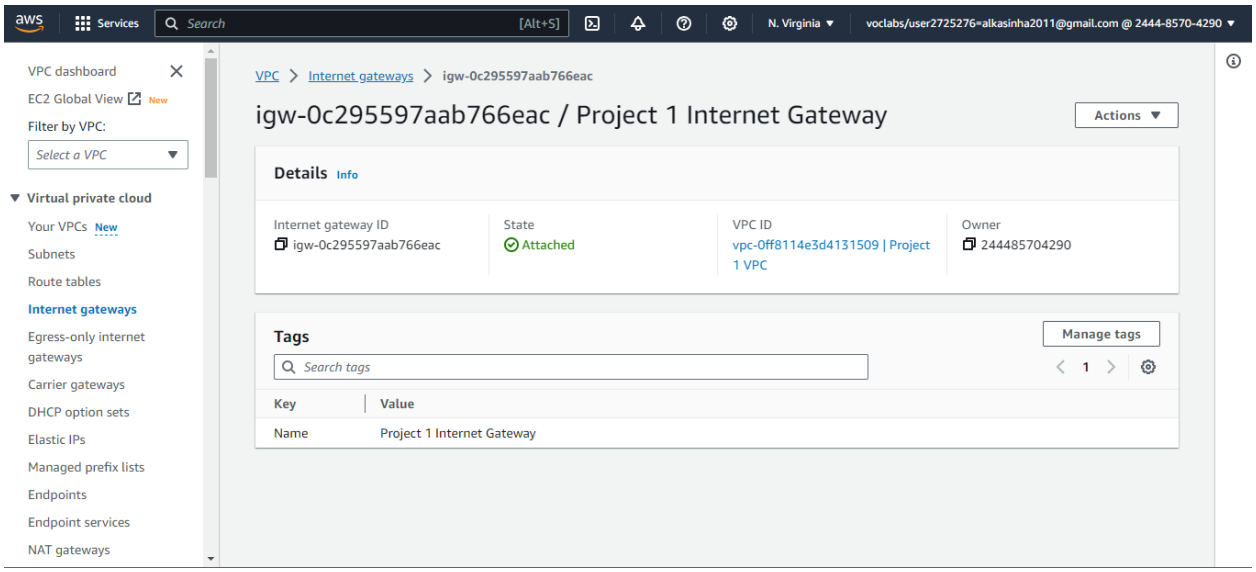


Step number	c
Step name	Creation of private subnet
Instructions	1) Navigate to VPC->Subnets 2) Click on "Create Subnet" 3) Enter the following fields Name tag : Private Subnet VPC : Select the Project 1 VPC IPv4 CIDR block : 10.0.2.0/24 The other options can be ignored 4) Click on Create
Expected screenshots	1) Subnet Creation screen



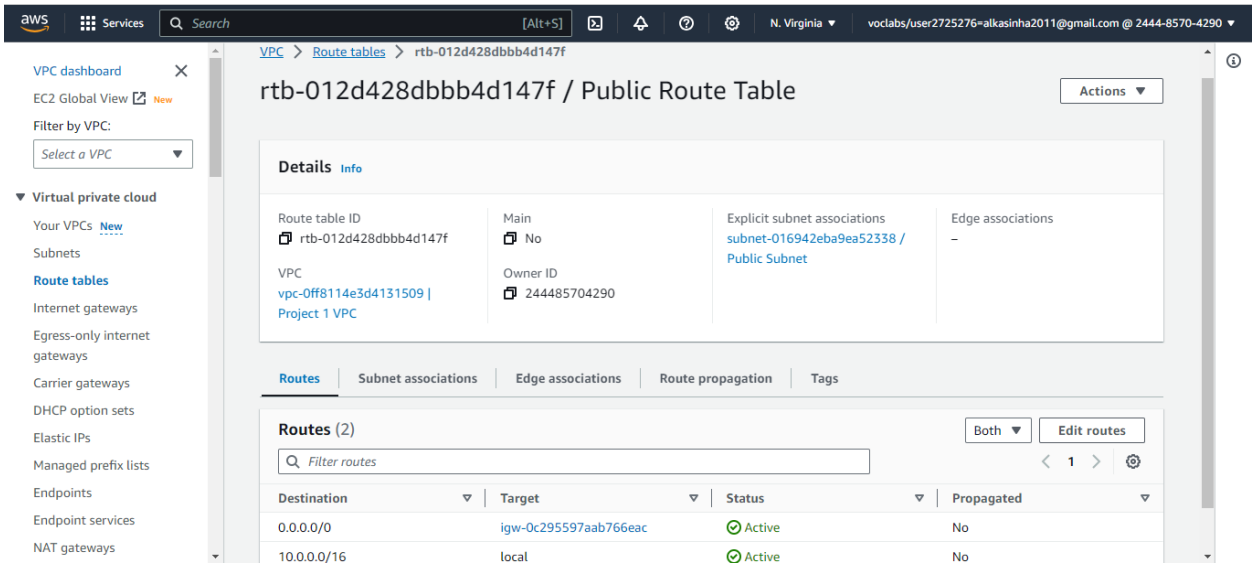
Step 2 : Internet Gateway and VPC

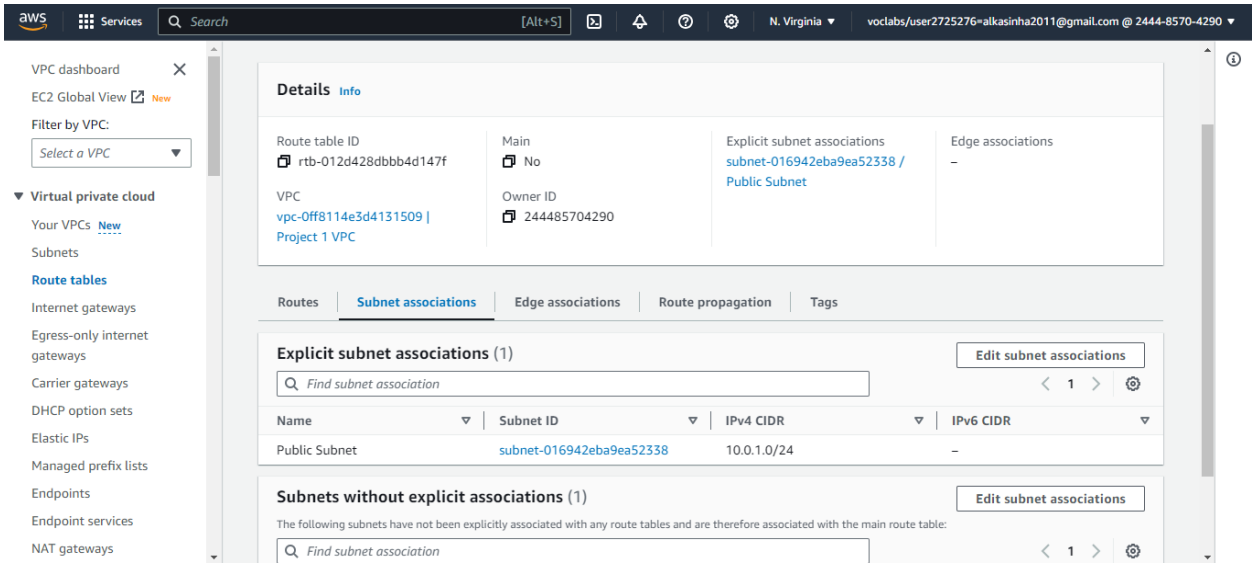
Step number	a
Step name	Creation and Configuration of Internet Gateway
Instructions	1) Navigate to VPCs->Internet Gateway 2) Click on "Create Internet Gateway" 3) Enter the name tag "Project 1 Internet Gateway" and click on "Create Internet Gateway" 4) After the gateway is created, select it and click on Actions->Attach to VPC 5) Select the Project 1 VPC and click on "Attach Internet Gateway"
Expected screenshots	1) Creation of Internet Gateway



Step number	b
Step name	Creation of public route table
Instructions	1) Navigate to VPC -> Route Tables and click on Create Route table 2) Enter the name tag "Public Route Table", select the Project 1 VPC from the dropdown and click on Create 3) Once the route table is created, select it and select the Routes tab below the list of route tables 4) Click in Edit Routes and add the following route (Don't edit the existing one) - Destination : 0.0.0.0/0 - Target : Select Internet Gateway and the select the Project 1 Internet Gateway Click on Save Routes

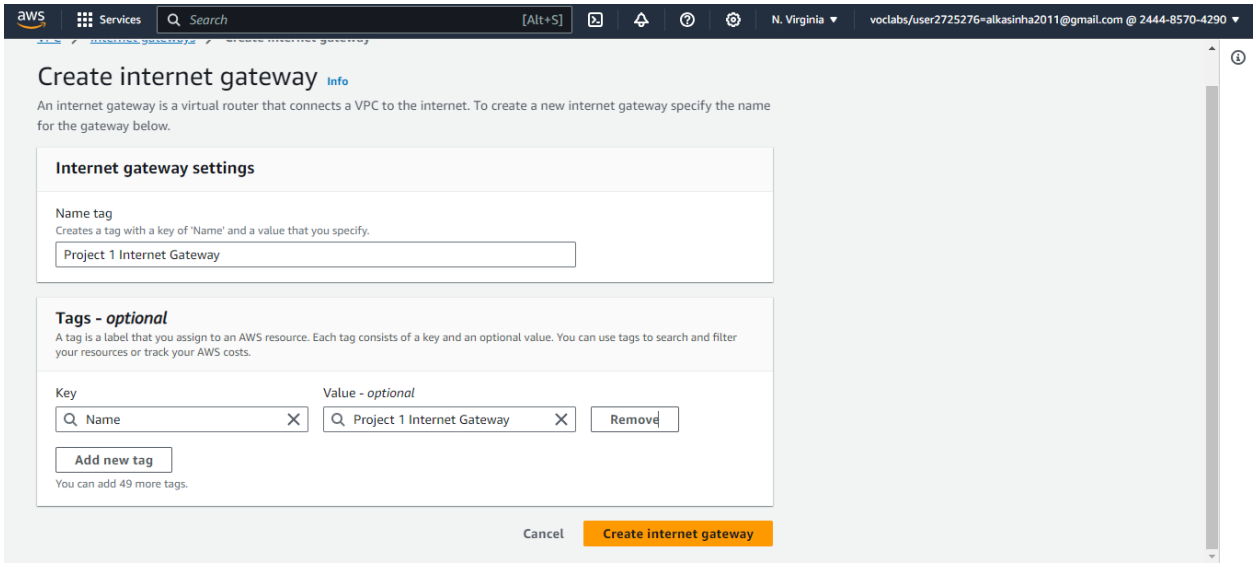
	5) Select the Subnet Associations tab and click on Edit Subnet Associations 6) Select the Public Subnet from the list and click on Save
Expected screenshots	1) Route list of the route table 2) Subnet Associations of the route table

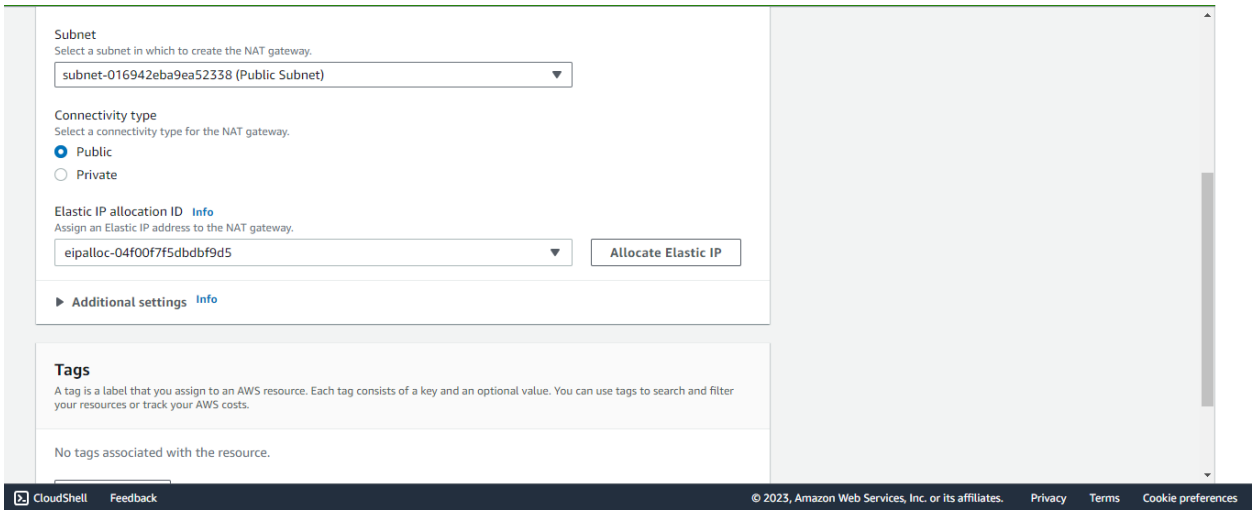


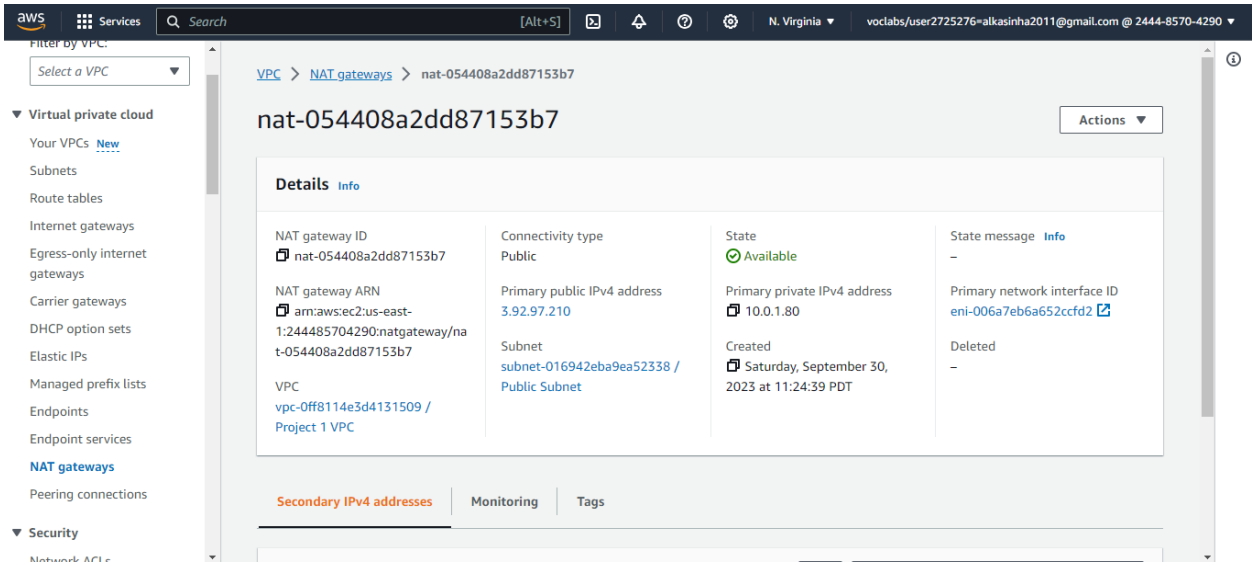


Step number	c
Step name	Creation of NAT gateway

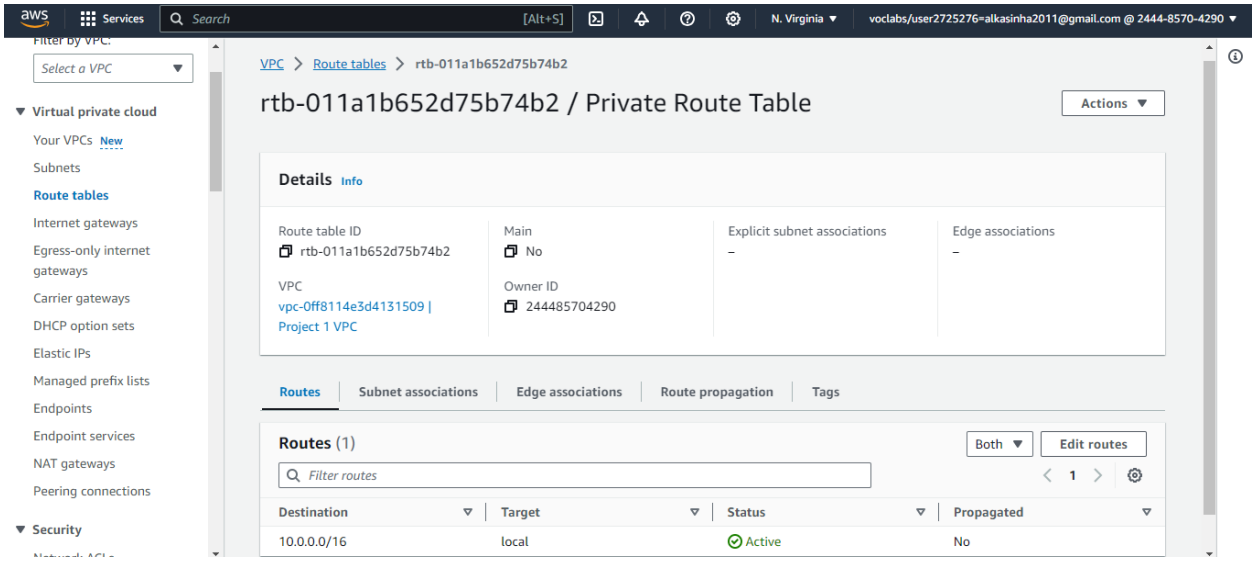
Instructions	1) Navigate to VPC using the Services button at the top of the screen 2) Select NAT Gateway at the left side of the screen 3) Click on Create NAT Gateway - Deploy it in the public subnet - Connectivity type : Public - Allocate an elastic IP by clicking on “Allocate Elastic IP” 4) Click on “Create NAT Gateway” to create the gateway
Expected screenshots	1) NAT gateway creation details 2) Gateway after creation

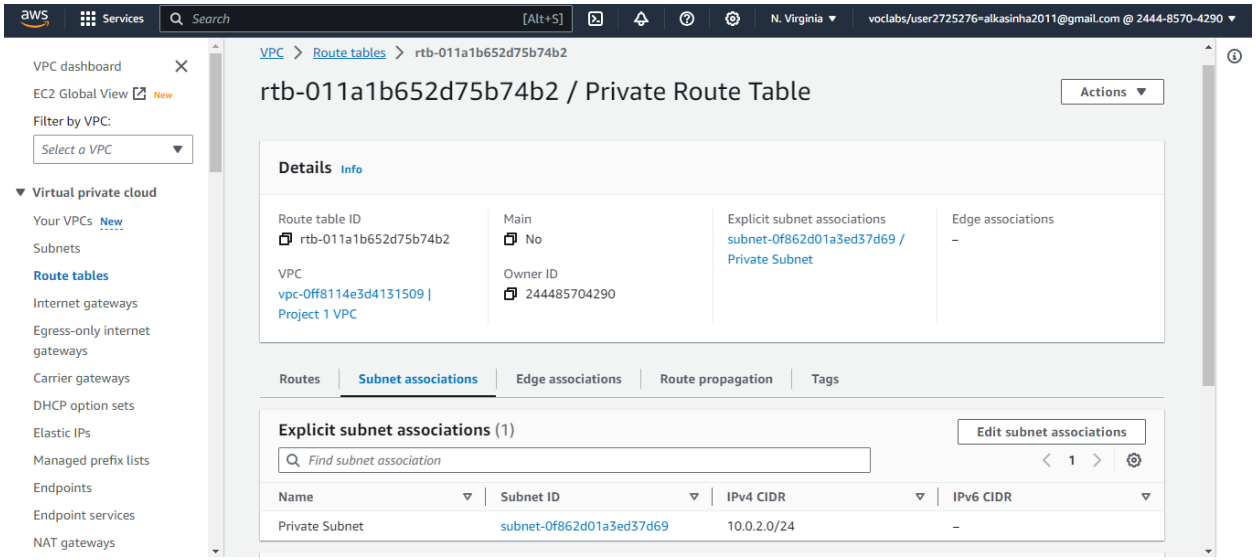






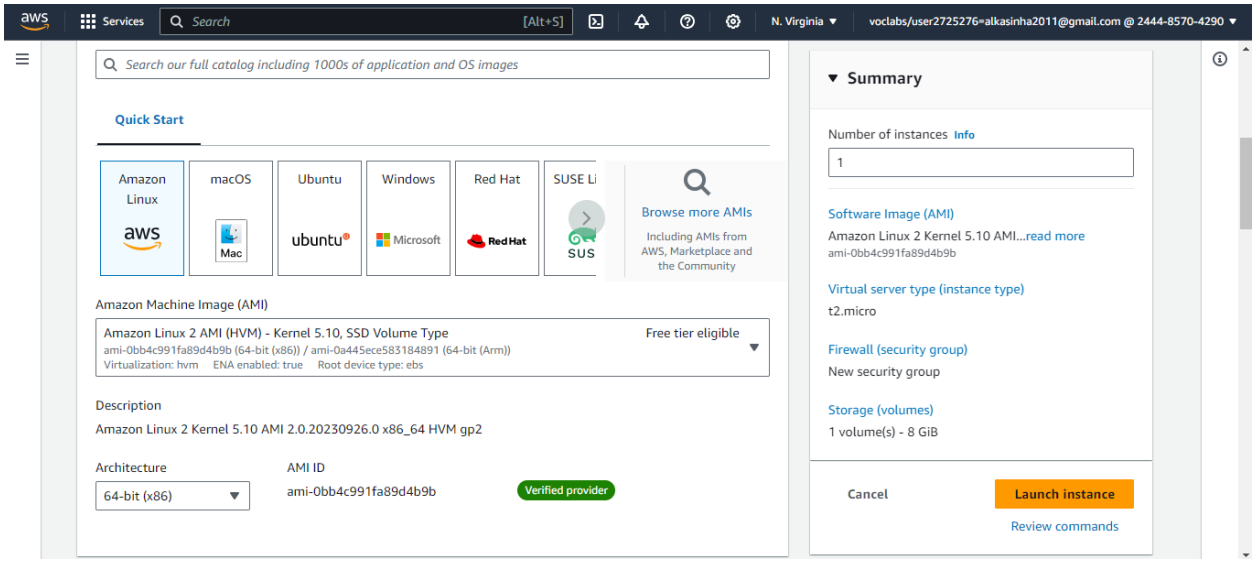
Step number	d
Step name	Creation of private route tables
Instructions	1) Navigate to VPC -> Route Tables and click on Create Route table 2) Enter the name tag "Private Route Table", select the Project 1 VPC from the dropdown and click on Create 3) Once the route table is created, select it and select the Routes tab below the list of route tables 4) Click in Edit Routes and add the following route (Don't edit the existing one) - Destination : 0.0.0.0/0 - Target: Select NAT Gateway and select the NAT Gateway created in the previous step Click on Save Routes 5) Select the Subnet Associations tab and click on Edit Subnet Associations 6) Select the private Subnet from the list and click on Save
Expected screenshots	1) Route list of the route table 2) Subnet association of the route table

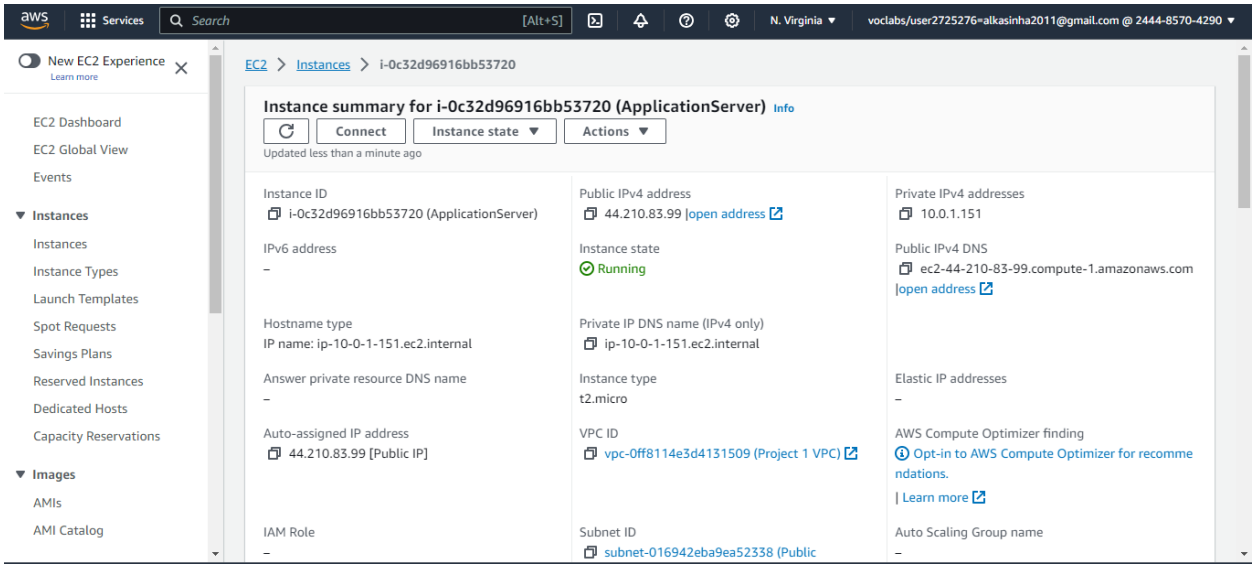

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2725276=alkasinha2011@gmail.com @ 2444-8570-4290
Select a VPC
Virtual private cloud
Your VPCs New
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
VPC > Route tables > rtb-011a1b652d75b74b2
rtb-011a1b652d75b74b2 / Private Route Table
Actions
Details Info
Route table ID
rtb-011a1b652d75b74b2
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-0ff8114e3d4131509 | Project 1 VPC
Owner ID
244485704290
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (1)
Both
Edit routes
Filter routes
1
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No

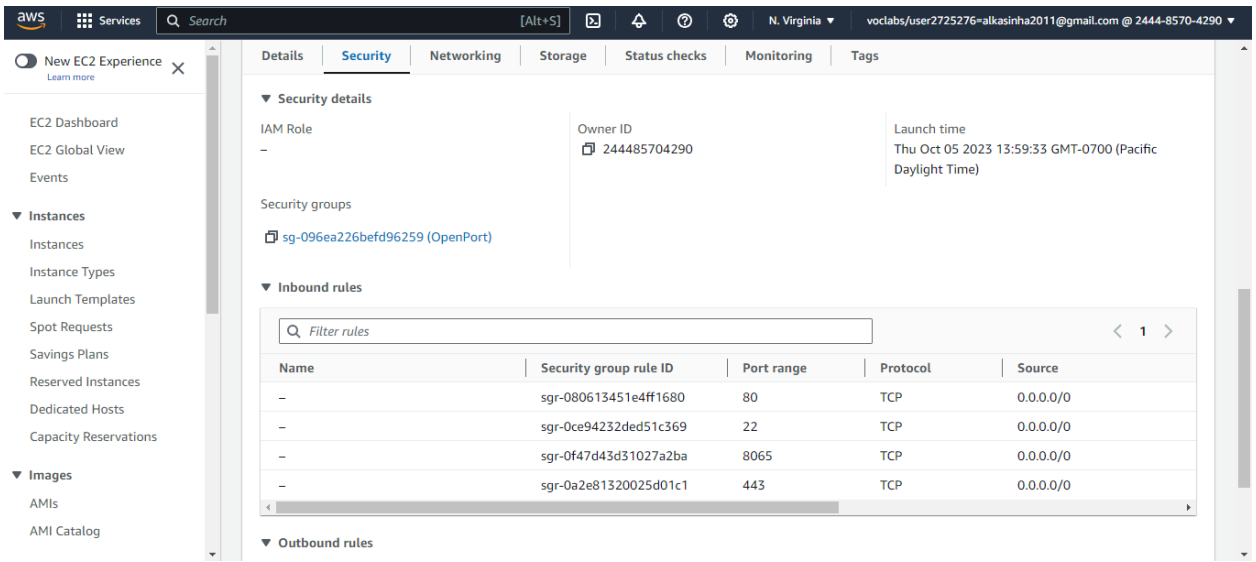

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2725276=alkasinha2011@gmail.com @ 2444-8570-4290
VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs New
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
VPC > Route tables > rtb-011a1b652d75b74b2
rtb-011a1b652d75b74b2 / Private Route Table
Actions
Details Info
Route table ID
rtb-011a1b652d75b74b2
Main
No
Explicit subnet associations
subnet-0f862d01a3ed37d69 / Private Subnet
Edge associations
–
VPC
vpc-0ff8114e3d4131509 | Project 1 VPC
Owner ID
244485704290
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (1)
Edit subnet associations
Find subnet association
1
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Private Subnet
subnet-0f862d01a3ed37d69
10.0.2.0/24
–

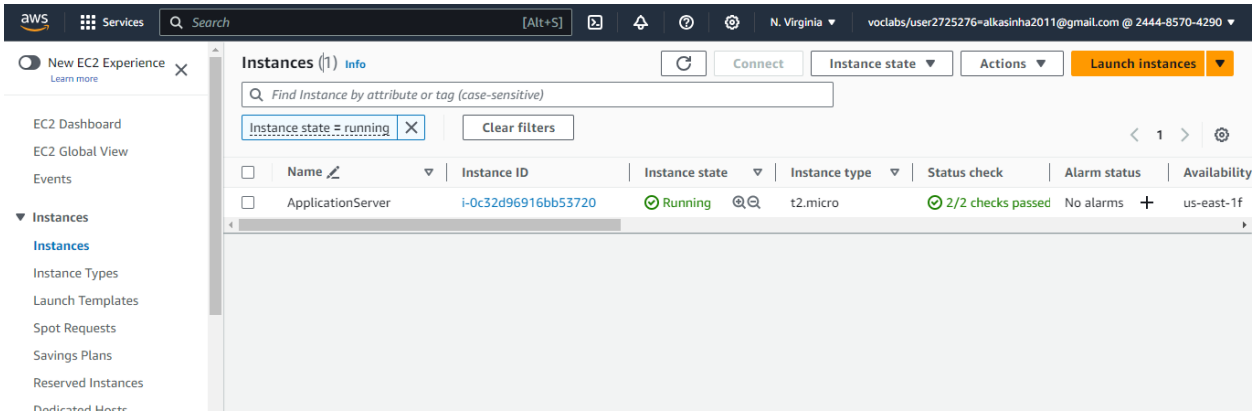
Step 3 : Creation of database and application servers

Step number	a
Step name	Creation of application server
Instructions	1) Navigate to EC2 using the Services button at the top of the screen 2) Select Instances at the left side of the screen 3) Click on Launch Instance - Select the AMI Amazon 2 Linux - Select the instance type t2.micro - Select Network as "Project 1 VPC" and subnet as "Public Subnet" - For the security group, open the ports 80,443, 22 and 8065 for source set to "Anywhere" 4) Launch the instance after creating a new pem file and downloading it
Expected screenshots	1) AMI used 2) Instance configuration screen 3) Security group rules 4) Instance after creation

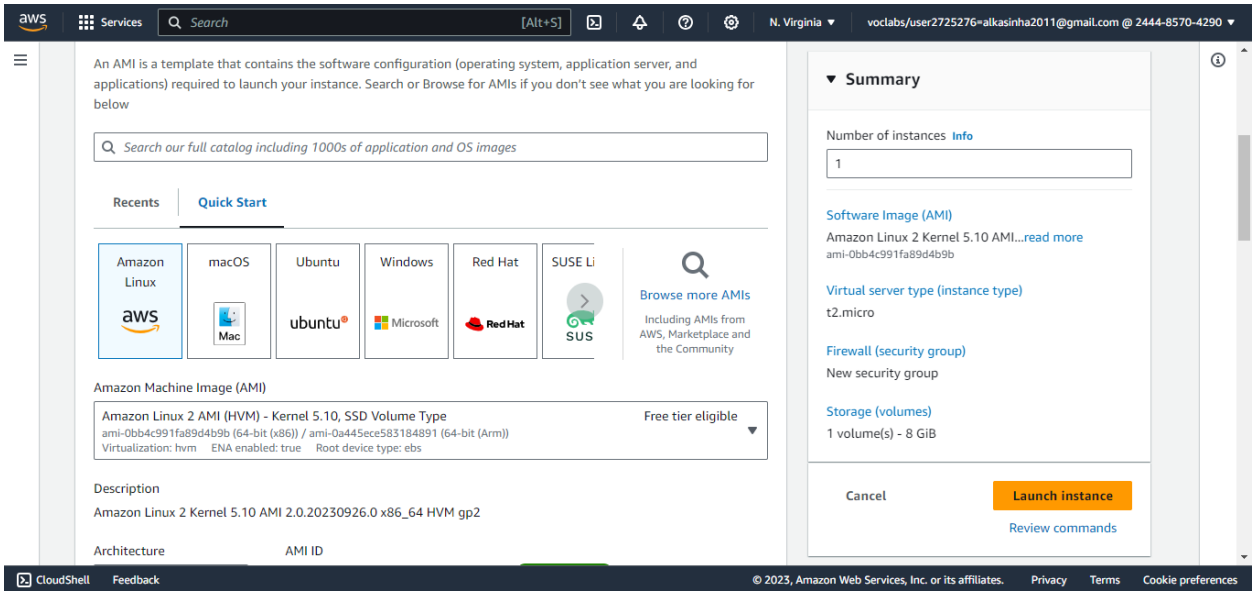


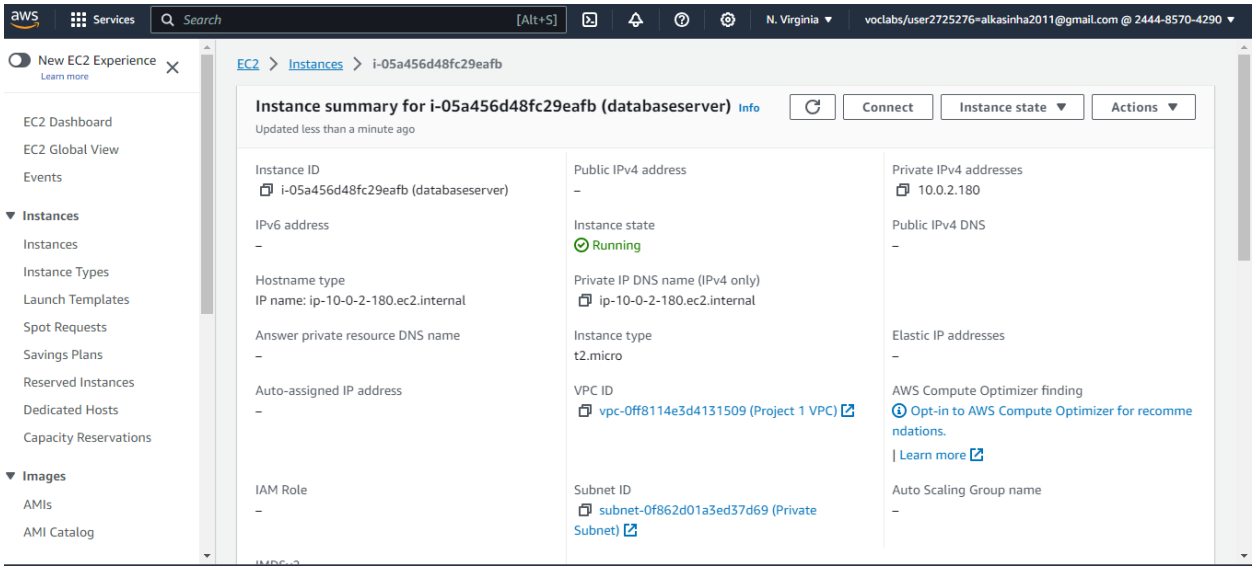

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2725276=alkasinha2011@gmail.com @ 2444-8570-4290
New EC2 Experience
Learn more
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
EC2 > Instances > i-0c32d96916bb53720
Instance summary for i-0c32d96916bb53720 (ApplicationServer) Info
Connect
Instance state
Actions
Updated less than a minute ago
Instance ID
i-0c32d96916bb53720 (ApplicationServer)
Public IPv4 address
44.210.83.99 |open address
Private IPv4 addresses
10.0.1.151
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-44-210-83-99.compute-1.amazonaws.com |open address
Hostname type
IP name: ip-10-0-1-151.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-0-1-151.ec2.internal
Answer private resource DNS name
–
Instance type
t2.micro
Elastic IP addresses
–
Auto-assigned IP address
44.210.83.99 [Public IP]
VPC ID
vpc-0ff8114e3d4131509 (Project 1 VPC)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
| Learn more
IAM Role
–
Subnet ID
subnet-016942eba9ea52338 (Public
Auto Scaling Group name
–

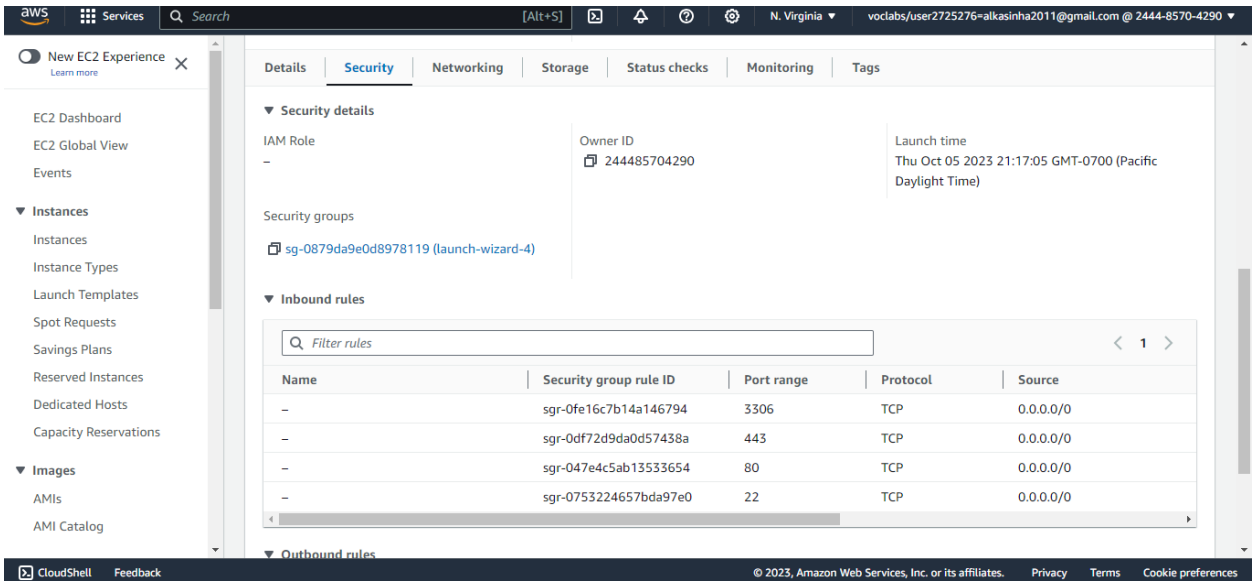

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2725276=alkasinha2011@gmail.com @ 2444-8570-4290
New EC2 Experience
Learn more
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Security details
IAM Role
–
Owner ID
244485704290
Launch time
Thu Oct 05 2023 13:59:33 GMT-0700 (Pacific Daylight Time)
Security groups
sg-096ea226befd96259 (OpenPort)
Inbound rules
Filter rules
1
Name
Security group rule ID
Port range
Protocol
Source
–
sgr-080613451e4ff1680
80
TCP
0.0.0.0/0
–
sgr-0ce94232ded51c369
22
TCP
0.0.0.0/0
–
sgr-0f47d43d31027a2ba
8065
TCP
0.0.0.0/0
–
sgr-0a2e81320025d01c1
443
TCP
0.0.0.0/0
Outbound rules

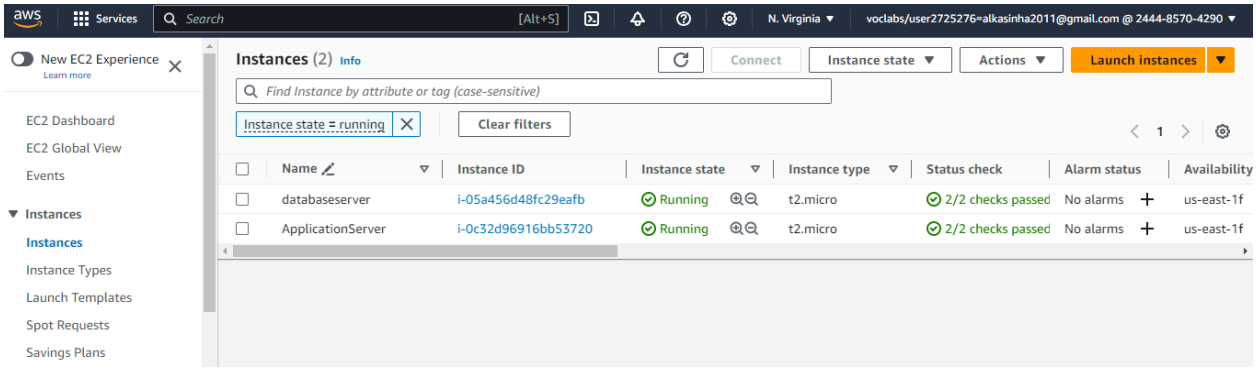

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2725276=alkasinha2011@gmail.com @ 2444-8570-4290
New EC2 Experience
Learn more
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Instances (1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Instance state = running
Clear filters
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability
ApplicationServer
i-0c32d96916bb53720
Running
t2.micro
2/2 checks passed
No alarms
us-east-1f

Step number	b
Step name	Creation of database server
Instructions	1) Navigate to EC2 using the Services button at the top of the screen 2) Select Instances at the left side of the screen 3) Click on Launch Instance - Select the AMI Amazon 2 Linux - Select the instance type t2.micro - Select Network as "Project 1 VPC" and subnet as "Private Subnet" - For the security group, open the ports 80, 443,22 and 3306 for source set to "Anywhere" 4) Launch the instance by selecting the same pem file created in the previous step
Expected screenshots	1) AMI used 2) Instance configuration screen 3) Security group rules 4) Instance after creation




Services
Search
[Alt+S]
N. Virginia
voclabs/user2725276=alkasinha2011@gmail.com @ 2444-8570-4290
New EC2 Experience
Learn more
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
EC2 > Instances > i-05a456d48fc29eafb
Instance summary for i-05a456d48fc29eafb (databaseserver) Info
Updated less than a minute ago
Connect
Instance state
Actions
Instance ID
i-05a456d48fc29eafb (databaseserver)
Public IPv4 address
–
Private IPv4 addresses
10.0.2.180
IPv6 address
–
Instance state
Running
Public IPv4 DNS
–
Hostname type
IP name: ip-10-0-2-180.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-0-2-180.ec2.internal
Answer private resource DNS name
–
Instance type
t2.micro
Elastic IP addresses
–
Auto-assigned IP address
–
VPC ID
vpc-0ff8114e3d4131509 (Project 1 VPC)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
Learn more
IAM Role
–
Subnet ID
subnet-0f862d01a3ed37d69 (Private Subnet)
Auto Scaling Group name
–

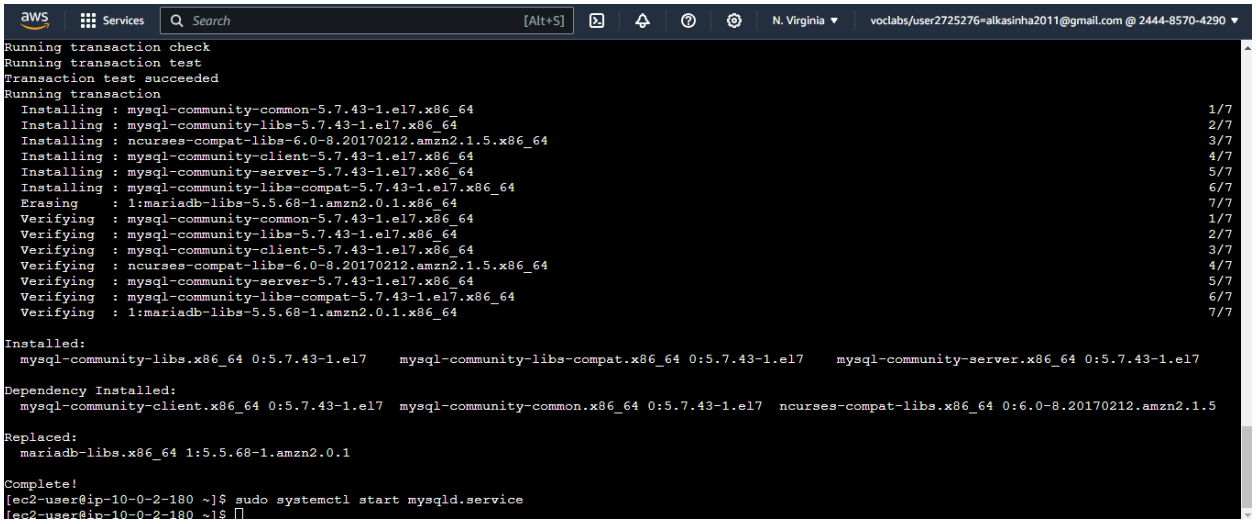

Services
Search
[Alt+S]
N. Virginia
voclabs/user2725276=alkasinha2011@gmail.com @ 2444-8570-4290
New EC2 Experience
Learn more
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Security details
IAM Role
–
Owner ID
244485704290
Launch time
Thu Oct 05 2023 21:17:05 GMT-0700 (Pacific Daylight Time)
Security groups
sg-0879da9e0d8978119 (launch-wizard-4)
Inbound rules
Filter rules
1
Name
Security group rule ID
Port range
Protocol
Source
–
sgr-0fe16c7b14a146794
3306
TCP
0.0.0.0/0
–
sgr-0df72d9da0d57438a
443
TCP
0.0.0.0/0
–
sgr-047e4c5ab13533654
80
TCP
0.0.0.0/0
–
sgr-0753224657bda97e0
22
TCP
0.0.0.0/0
Outbound rules
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
voclabs/user2725276=alkasinha2011@gmail.com @ 2444-8570-4290
New EC2 Experience
Learn more
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Instances (2) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Instance state = running
Clear filters
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability
databaseserver
i-05a456d48fc29eafb
Running
t2.micro
2/2 checks passed
No alarms
us-east-1f
ApplicationServer
i-0c32d96916bb53720
Running
t2.micro
2/2 checks passed
No alarms
us-east-1f

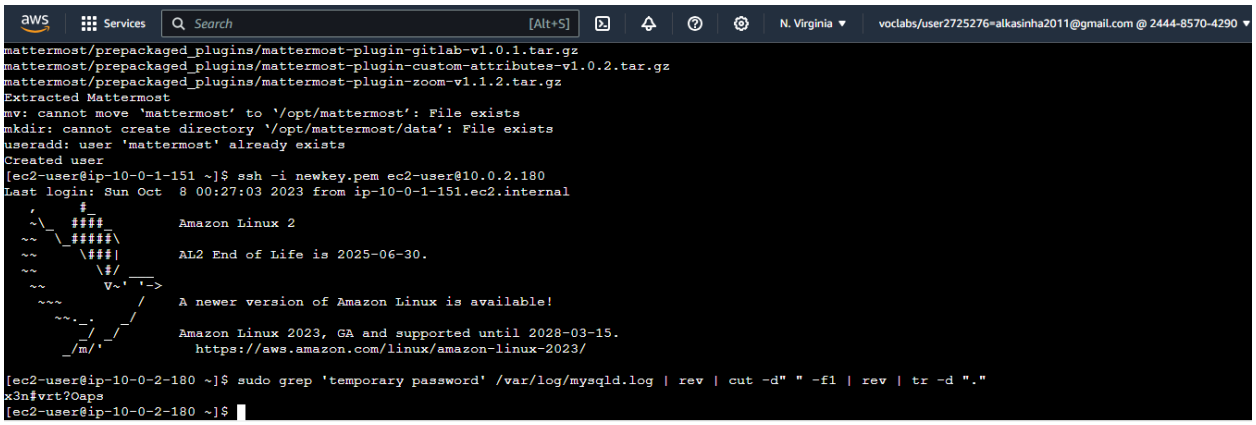
Step 4: Application and Database Installation and Testing

Step number	a
Step name	Installation and configuration of MySQL
Instructions	1) Navigate to the EC2 service console using the search box at the top 2) Select the database server created in the previous step 3) Click on the Connect button on the top right 4) In the tab “EC2 instance connect” , ensure that the value in the username field is **ec2-user** and click on Connect. 5) Enter the following commands one by one in the terminal which opens up to install and configure MySQL on the database server *sudo yum update* *wget http://dev.mysql.com/get/mysql57-community-release-el7-9.noarch.rpm* *sudo yum localinstall mysql57-community-release-el7-9.noarch.rpm -y* *sudo yum install mysql-community-server -y --nogpgcheck* *sudo systemctl start mysqld.service* Run the below command to retrieve a temporary password for MySQL *sudo grep 'temporary password' /var/log/mysqld.log | rev | cut -d" " -f1 | rev | tr -d "."* Login to MySQL with the below command and enter the above password when prompted *mysql -u root -p* Enter the below command after you login to MySQL *ALTER USER 'root'@'localhost' IDENTIFIED BY 'Password42!';* Type ‘exit’ into the MySQL prompt and press Enter to exit out of the MySQL environment. Enter the below commands to complete the setup. Ignore any warning messages you receive. *wget https://d6opu47qoi4ee.cloudfront.net/install_mysql_linux.sh* *chmod 777 install_mysql_linux.sh* *sudo ./install_mysql_linux.sh* 6) Type *exit* to exit the database server and go back to the application server
nbmji90	1) Installation of MySQL 2) Retrieving the temporary password 3) Executing the provided script

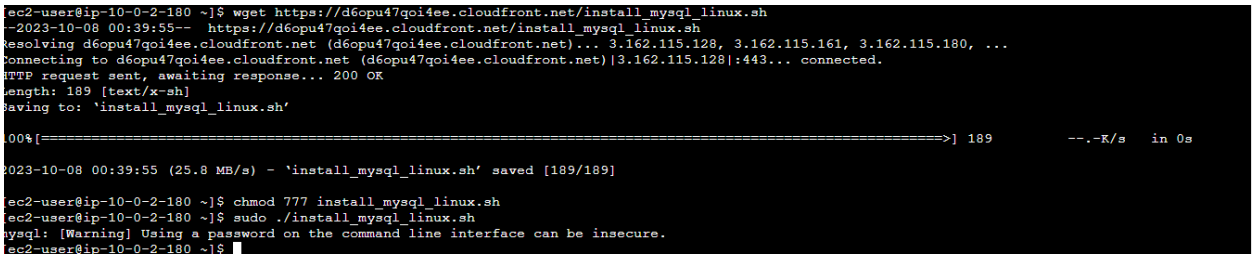
Installation of MySQL



Retrieving the temporary password



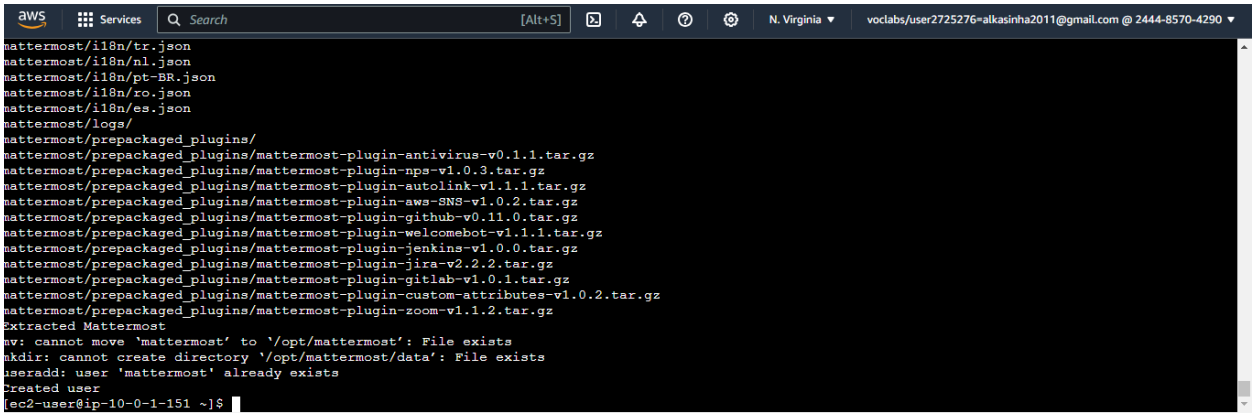
Executing provided script



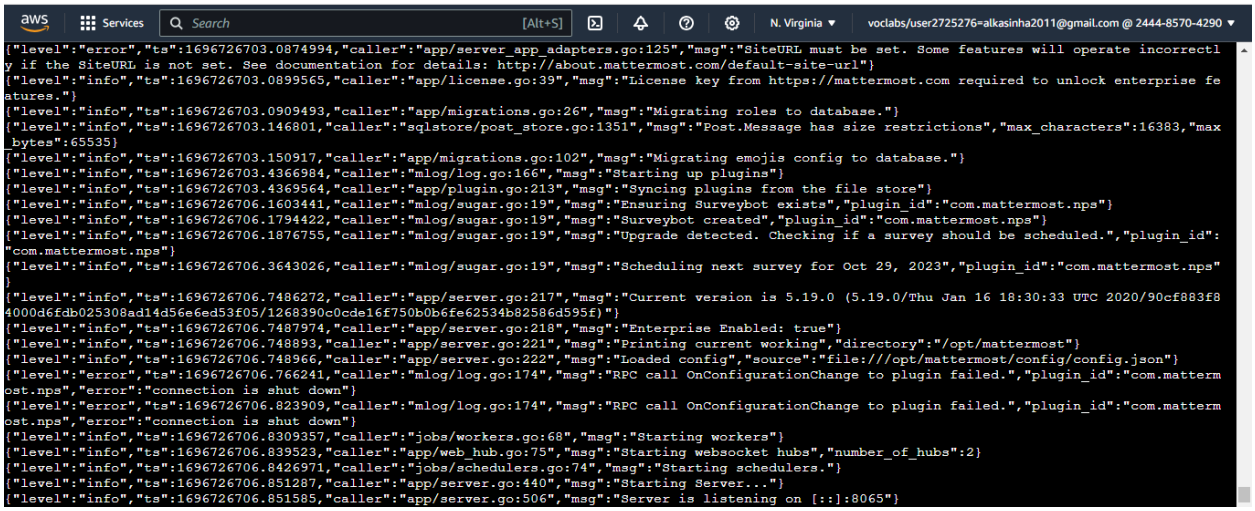
Step number	b
Step name	Installation and configuration of Mattermost

Instructions	1) Select the Application server in the EC2 console and connect to it using the same method as the database server in the previous step. 2) Enter the following commands in the terminal which opens up to install and configure Mattermost *wget https://d6opu47qoi4ee.cloudfront.net/install_mattermost_linux.sh* *sudo yum install dos2unix -y* *sudo dos2unix install_mattermost_linux.sh* *chmod 700 install_mattermost_linux.sh* *sudo ./install_mattermost_linux.sh <private IP of MySQL server>* Example : sudo *./install_mattermost_linux* 173.65.34.7 *sudo chown -R mattermost:mattermost /opt/mattermost* *sudo chmod -R g+w /opt/mattermost* *cd /opt/mattermost* *sudo -u mattermost ./bin/mattermost* 2) Check whether the server has been successfully deployed by navigating to the following URL in your web browser. The web page might take a couple of minutes to load. <public IP of the application server>:8065
Expected screenshots	1) Executing the script 2) Starting the Mattermost server 3) Accessing the application via web browser

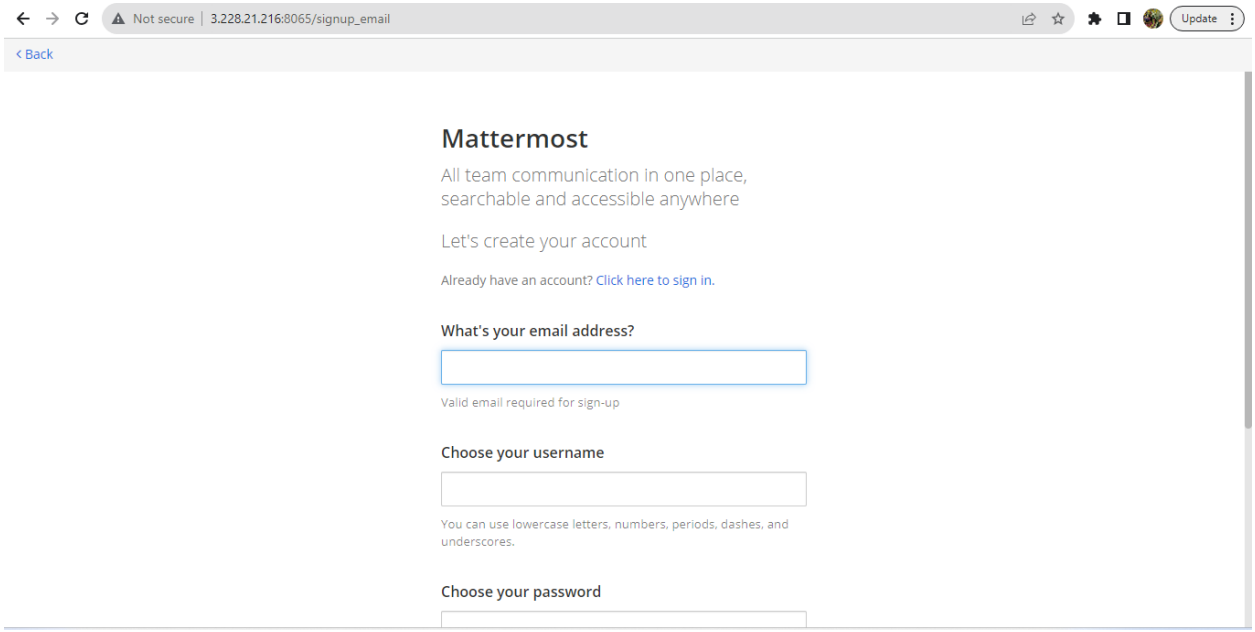
Executing the script-



Starting the Mattermost server



Accessing application via web browser



Step 5: Answer the following questions

Q1 What is the default setting for DNS hostnames when a new VPC is created?

a) Enabled

b) Disabled

c) Can be set during VPC creation

d) Depends on the region used

Enter your answer here B

Q2 What is the term used for the machine when we use it to log into the database server?

a) Bastion Host

b) NAT Gateway

c) Tunnel Interface

d) SSH Gateway

Enter your answer here A

Q3 The database server security group in this exercise has to keep port 3306 open. Which protocol uses this port to communicate?

a) HTTPS

b) RDP

c) TCP

d) SCP

Enter your answer here C

Q4 Which port is being used by Mattermost to communicate with the client application

a) 8080

b) 80

c) 443

d) 8065

Enter your answer here D

Q5 Which of the following is a reason why we cannot set the CIDR block for the public subnet to 10.0.2.0/16, assuming the values for the other CIDR blocks are the same as mentioned in the instructions?

a) CIDR block overlaps with existing block

b) CIDR block is not a valid CIDR

c) CIDR block does not fall within the VPC

d) There is no reason, this is a perfectly valid CIDR

Enter your answer here | A

Q6 Assume that you have been asked to create 3 EC2 instances - application server, the database server and NAT instance. Each of these instances have their own security groups with a set of ports to be kept open. One of those ports is entirely unnecessary for the given architecture to function. Which of the ports given in the option below could it be?

a) Port 22 on the NAT instances

b) Port 3306 on the database server

c) Port 443 on the NAT instance

d) Port 22 on the application server

Enter your answer here | D

Q7 How are we going to increase the security of the Mattermost server to ensure the users are from a specific organization and the traffic is originating from a known IP address?

Create security group which acts as a virtual firewall for Mattermost server to control incoming and outgoing traffic. Proper inbound rules control the incoming traffic to Mattermost server.

Q8 How do we achieve elasticity for the Mattermost server?

Configure Mattermost to use elasticsearch server. Set enable elasticsearch indexing to true in elasticsearch of system console. Set the Elasticsearch server connection details. Edit the config.json file. Enable elasticsearch by setting enable elasticsearch for search queries to true and setting enable elasticsearch for autocomplete to true.

Max points **15**

Grade distribution	
MCQs	6 (1 point each)
Subjective questions	10 (5 points each)
Implementation screenshots	24 points (1 point each)

Total	40 points

Appendix

This section contains optional details on how to SSH into an EC2 instance using the terminal and can be ignored by learners who are not from a technical background

Connecting to an EC2 instance using SSH

1) A terminal environment will be required to perform connect to an instance using SSH. Linux and macOS users can use the built-in terminal installed on their operating systems.
   Windows Users are advised to install a third-party terminal environment such as Gitbash https://git-scm.com/download/win
2) After opening the terminal environment, you will need to navigate to the folder containing the keypair file for the instance using the *cd* command. For example, if the keypair file is stored in the Downloads folder, you can use the below command

```
cd Downloads
```

3) Run the following command in the terminal to ensure that the keypair file is in read-only mode

```
chmod 400 <keypair file name>
```

4) Run the following command to SSH into the EC2 instance

```
ssh -i <keypair file name> ec2-user@<IP address of the instance>
```