

<b>Declaration</b>	
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	Dr. Shubhangi Kharche
	<Enter your name above this line to indicate that you are in agreement>

<b>Instructions</b>
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

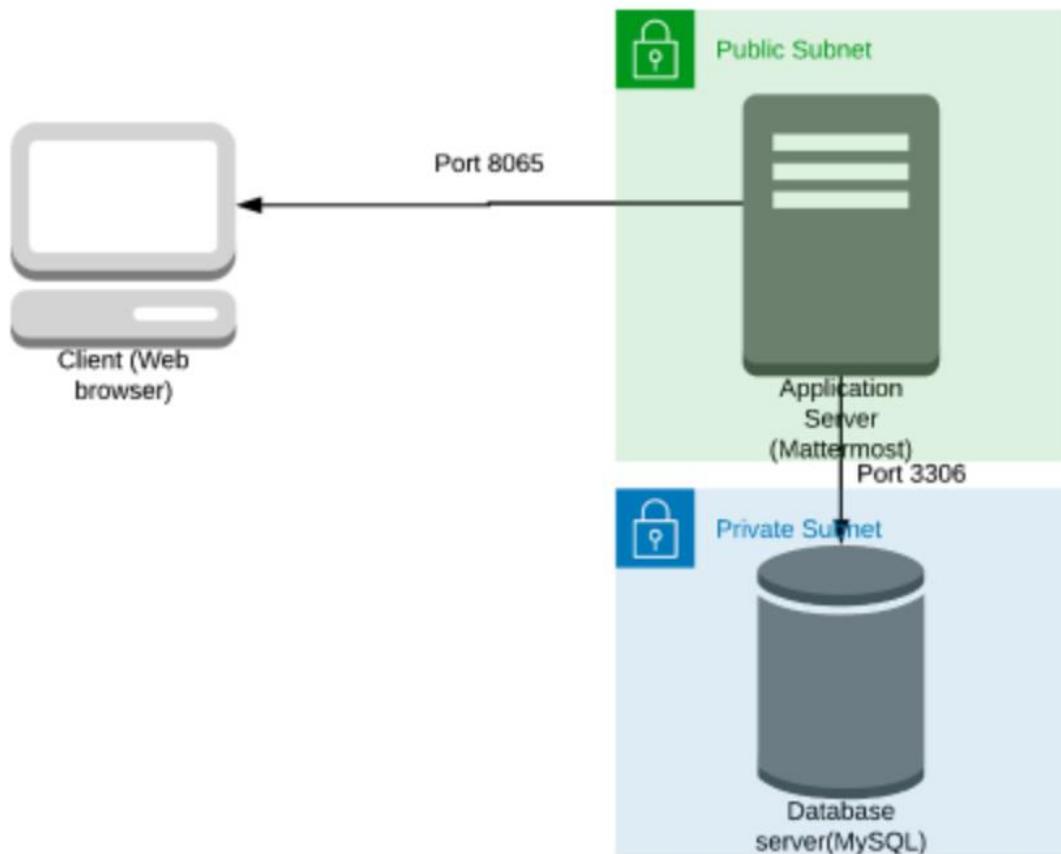
<b>Resource Clean Up</b>
Cloud is always pay per use model and all resources/services that we consume are chargeable. Cleaning up when you've completed your lab or project is always necessary. This is true whether you're doing a lab or implementing a project at your workplace.
After completing the lab, 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	<p>1) Navigate to VPC using the Services button at the top of the screen</p> <p>2) Select "Your VPCs" on the left side of the screen</p> <p>3) Click on "Create VPC"</p> <p>4) Enter the following fields :</p> <p>Name: Project 1 VPC</p> <p>IPv4 CIDR Block : 10.0.0.0/16</p> <p>The rest of the options can be ignored</p> <p>5) Select "Create VPC"</p> <p>6) Select the VPC and click on Actions-&gt;Edit DNS hostnames</p> <p>7) Enable DNS hostnames and click on Save</p>
Expected screenshots	1) Created VPC with properties visible

The screenshot shows the AWS VPC Management console. On the left, there's a sidebar with various navigation options like VPC Dashboard, EC2 Global View, Filter by VPC, and Select a VPC. The main area displays a table titled 'Your VPCs (1/2)'. A green banner at the top says 'DNS hostnames successfully updated.' The table has columns for Name, VPC ID, State, IPv4 CIDR, IPv6 CIDR, DHCP options set, Main route table, and Actions. One row is selected, showing 'project 1 VPC' with VPC ID 'vpc-0596d5852051c66fb'. Below the table, there's a 'Details' tab showing more VPC properties.

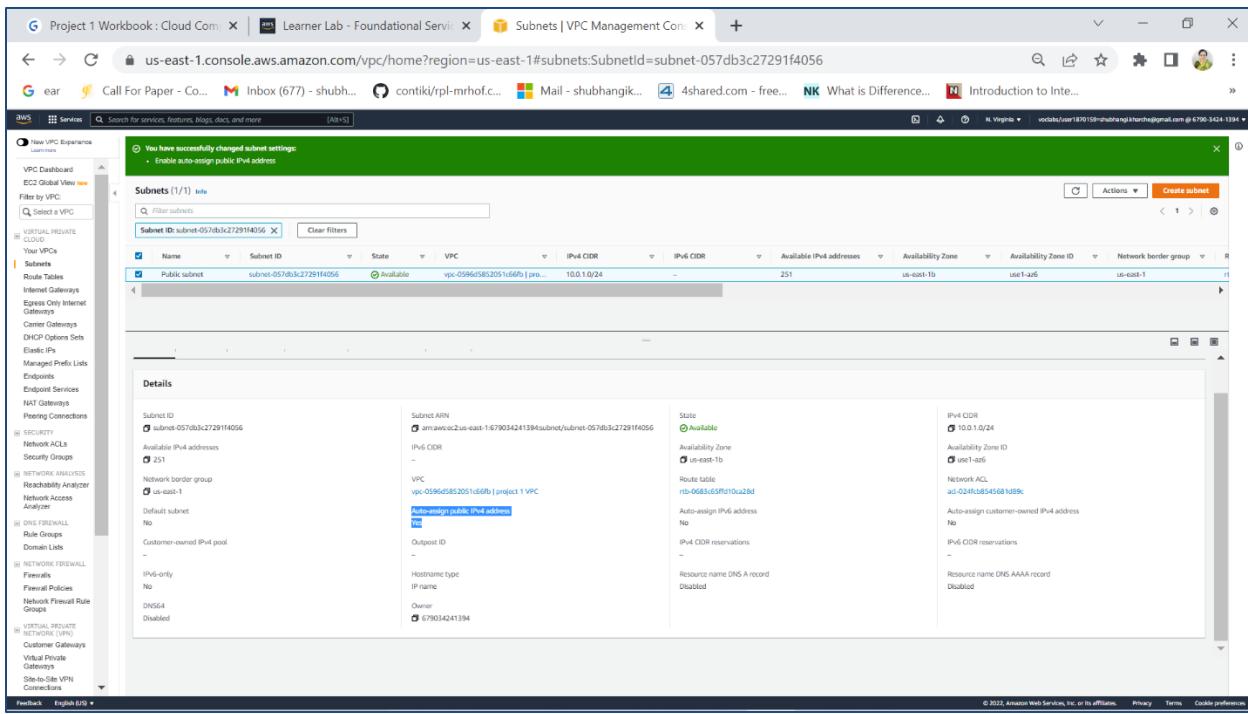
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Main route table
-	vpc-0836df73efcf874fd	Available	172.31.0.0/16	-	dopt-00a291a535a57...	rtb-03e5c8a13f946c431
<b>project 1 VPC</b>	<b>vpc-0596d5852051c66fb</b>	<b>Available</b>	<b>10.0.0.0/16</b>	<b>-</b>	<b>dopt-00a291a535a57...</b>	<b>rtb-0683c65ffd10ca28d</b>

**Details**

VPC ID	vpc-0596d5852051c66fb	State	Available	DNS hostnames	Enabled	DNS resolution	Enabled
Tenancy	Default	DHCP options set	dopt-00a291a535a579d2c	Main route table	rtb-0683c65ffd10ca28d	Main network ACL	ad-024fc8545681d89c
Default VPC	No	IPv4 CIDR	10.0.0.0/16	IPv6 pool	-	IPv6 CIDR (Network border group)	-
Route 53 Resolver DNS Firewall rule groups	<span style="color: red;">Failed to load rule groups</span>	Owner ID	679034241394				

**Fig 1: Created VPC with properties visible**

Step number	b
Step name	Creation of public subnet
Instructions	<ol style="list-style-type: none"> <li>1) Navigate to VPC-&gt;Subnets</li> <li>2) Click on "Create Subnet"</li> <li>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</li> <li>4) Click on Create</li> <li>5) Once the subnet has been created, select the subnet and click on Actions-&gt;Modify Auto-assign IP settings</li> <li>6) Enable the option "Auto assign IPv4" and select Save</li> </ol>
Expected screenshots	<ol style="list-style-type: none"> <li>1) Subnet Creation screen</li> </ol>



**Fig 2: Public Subnet Creation screen**

Step number	c
Step name	Creation of private subnet
Instructions	<ol style="list-style-type: none"> <li>1) Navigate to VPC-&gt;Subnets</li> <li>2) Click on "Create Subnet"</li> <li>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</li> <li>4) Click on Create</li> </ol>
Expected screenshots	1) Subnet Creation screen

The screenshot shows the AWS VPC Management Console with the URL <https://us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#subnets>. A green banner at the top says "You have successfully created 1 subnet: subnet-039eb8c670a658cd6". The left sidebar has sections for New VPC Experience, VPC Dashboard, EC2 Global View, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, Carrier Gateways, DHCP Options Sets, Elastic IPs, Managed Prefix Lists, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, SECURITY, Network ACLs, Security Groups, NETWORK ANALYSIS, Reachability Analyzer, Network Access Analyzer, and DNS FIREWALL. The main area shows a table of subnets with one row selected: "Private subnet" (subnet-039eb8c670a658cd6). The "Details" panel on the right shows the subnet's configuration, including Subnet ID (subnet-039eb8c670a658cd6), Subnet ARN (arn:aws:ec2:us-east-1:1679034241594:subnet/subnet-039eb8c670a658cd6), State (Available), IPv4 CIDR (10.0.2.0/24), Availability Zone (us-east-1b), Availability Zone ID (use1-az6), VPC (vpc-0596d5852051c66fb | project 1 VPC), Route table (rtb-0683c65fffd10ca28d), Default subnet (No), Auto-assign public IPv4 address (No), Customer-owned IPv4 pool (No), Auto-assign IPv6 address (No), IPv4 CIDR reservations (No), Outpost ID (No), and IPv6 CIDR reservations (No).

**Fig 3: Private Subnet Creation screen**

## Step 2 : Internet Gateway and VPC

Step number	a
Step name	Creation and Configuration of Internet Gateway
Instructions	<ol style="list-style-type: none"> <li>1) Navigate to VPCs-&gt;Internet Gateway</li> <li>2) Click on "Create Internet Gateway"</li> <li>3) Enter the name tag "Project 1 Internet Gateway" and click on "Create Internet Gateway"</li> <li>4) After the gateway is created, select it and click on Actions-&gt;Attach to VPC</li> <li>5) Select the Project 1 VPC and click on "Attach Internet Gateway"</li> </ol>
Expected screenshots	<ol style="list-style-type: none"> <li>1) Creation of Internet Gateway</li> </ol>

The screenshot shows the AWS VPC Internet Gateways page. On the left, there's a navigation sidebar with options like 'New VPC Experience', 'VPC Dashboard', 'EC2 Global View', 'Internet Gateways', 'Egress Only Internet Gateways', 'Carrier Gateways', 'DHCP Options Sets', 'Elastic IPs', 'Managed Prefix Lists', 'Endpoints', 'Endpoint Services', 'NAT Gateways', 'Peering Connections', 'SECURITY', 'Network ACLs', 'Security Groups', 'NETWORK ANALYSIS', 'Reachability Analyzer', 'Network Access Analyzer', and 'DNS FIREWALL'. The 'Internet Gateways' section is currently selected. The main content area displays a table titled 'Internet gateways (1/2) Info' with one row. The row contains the following information:

Name	Internet gateway ID	State	VPC ID	Owner
Project 1 Internet G...	igw-0b8729dd49637f487	Attached	vpc-0596d5852051c66fb   project 1 VPC	679034241394

Below the table, there's a detailed view for the selected gateway, showing its ID as 'igw-0b8729dd49637f487 / Project 1 Internet Gateway'. The 'Details' tab is selected, showing the following information:

Internet gateway ID igw-0b8729dd49637f487	State Attached	VPC ID vpc-0596d5852051c66fb   project 1 VPC	Owner 679034241394
--	-------------------	---	-----------------------

At the bottom right of the main content area, there are links for 'Feedback', 'English (US)', and 'Cookie preferences'. At the very bottom of the page, there are footer links for '© 2022, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

**Fig 4: Creation of Internet Gateway**

Step number	b
Step name	Creation of public route table
Instructions	<p>1) Navigate to VPC -&gt; Route Tables and click on Create Route table</p> <p>2) Enter the name tag "Public Route Table", select the Project 1 VPC from the dropdown and click on Create</p> <p>3) Once the route table is created, select it and select the Routes tab below the list of route tables</p> <p>4) Click in Edit Routes and add the following route (Don't edit the existing one)</p> <ul style="list-style-type: none"> <li>- Destination : 0.0.0.0/0</li> <li>- Target : Select Internet Gateway and the select the Project 1 Internet Gateway</li> </ul> <p>Click on Save Routes</p> <p>5) Select the Subnet Associations tab and click on Edit Subnet Associations</p> <p>6) Select the Public Subnet from the list and click on Save</p>
Expected screenshots	<ol style="list-style-type: none"> <li>1) Route list of the route table</li> <li>2) Subnet Associations of the route table</li> </ol>

You have successfully updated subnet associations for rtb-Oaa21f6c534ee5c71 / Public Route Table.

**rtb-Oaa21f6c534ee5c71 / Public Route Table**

Details Info

Route table ID rtb-Oaa21f6c534ee5c71	Main No	Explicit subnet associations subnet-057db3c27291f4056 / Public subnet	Edge associations -
VPC vpc-0596d5852051c66fb   project 1 VPC	Owner ID 679034241394		

Routes Subnet associations Edge associations Route propagation Tags

**Routes (2)**

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-0b8729dd49637f487	Active	No

Fig 5: Route list of the route table

You have successfully updated subnet associations for rtb-Oaa21f6c534ee5c71 / Public Route Table.

**rtb-Oaa21f6c534ee5c71 / Public Route Table**

Details Info

Route table ID rtb-Oaa21f6c534ee5c71	Main No	Explicit subnet associations subnet-057db3c27291f4056 / Public subnet	Edge associations -
VPC vpc-0596d5852051c66fb   project 1 VPC	Owner ID 679034241394		

Routes Subnet associations Edge associations Route propagation Tags

**Explicit subnet associations (1)**

Subnet ID	IPv4 CDR	IPv6 CDR
subnet-057db3c27291f4056 / Public subnet	10.0.1.0/24	-

**Subnets without explicit associations (1)**

Subnet ID	IPv4 CDR	IPv6 CDR
subnet-039ebc670a658cd6 / Private subnet	10.0.2.0/24	-

Fig 6: Subnet Associations of the route table

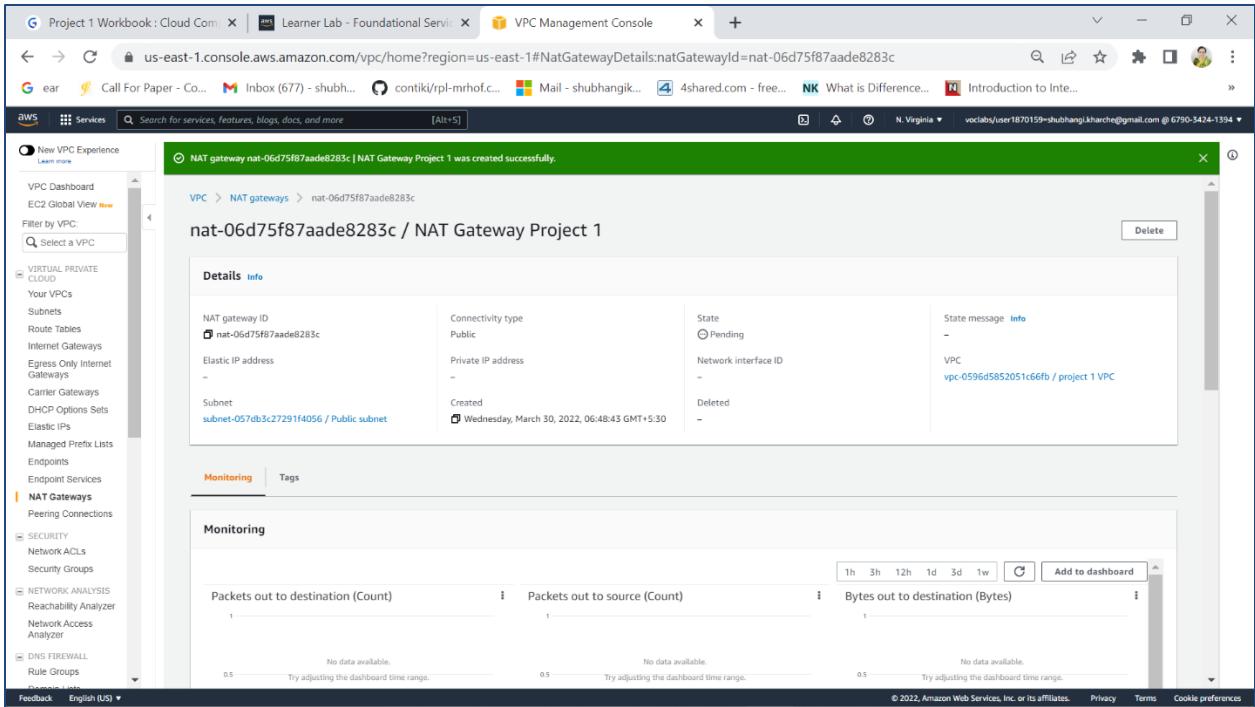
Step number	c
Step name	Creation of NAT gateway
Instructions	<p>1) Navigate to VPC using the Services button at the top of the screen</p> <p>2) Select NAT Gateway at the left side of the screen</p> <p>3) Click on Create NAT Gateway</p> <ul style="list-style-type: none"> <li>- Deploy it in the public subnet</li> <li>- Connectivity type : Public</li> <li>- Allocate an elastic IP by clicking on “Allocate Elastic IP”</li> </ul> <p>4) Click on “Create NAT Gateway” to create the gateway</p>
Expected screenshots	<p>1) NAT gateway creation details</p> <p>2) Gateway after creation</p>

The screenshot shows the AWS VPC Management Console with the 'NAT gateways' page open. A new NAT gateway named 'NAT Gateway Project 1' has been created. The 'Details' tab is selected, showing the following information:

NAT gateway ID	Connectivity type	State	State message
nat-06d75f87aaade8283c	Public	Available	-

Below the table, the 'Monitoring' and 'Tags' tabs are visible.

Fig 7: NAT gateway creation details



**Fig 8: Gateway after creation**

Step number	d
Step name	Creation of private route tables
Instruction	<p>1) Navigate to VPC -&gt; Route Tables and click on Create Route table</p> <p>2) Enter the name tag "Private Route Table", select the Project 1 VPC from the dropdown and click on Create</p> <p>3) Once the route table is created, select it and select the Routes tab below the list of route tables</p> <p>4) Click in Edit Routes and add the following route (Don't edit the existing one)</p> <ul style="list-style-type: none"> <li>- Destination : 0.0.0.0/0</li> <li>- Target: Select NAT Gateway and select the NAT Gateway created in the previous step</li> </ul> <p>Click on Save Routes</p> <p>5) Select the Subnet Associations tab and click on Edit Subnet Associations</p> <p>6) Select the private Subnet from the list and click on Save</p>
Expected screenshot	<p>1) Route list of the route table</p> <p>2) Subnet association of the route table</p>

You have successfully updated subnet associations for rtb-0b1d77b565ee8a07a / Private Route Table.

**rtb-0b1d77b565ee8a07a / Private Route Table**

Details Info

Route table ID: rtb-0b1d77b565ee8a07a Main: No Owner ID: vpc-0596d5852051c66fb | project 1 VPC

Explicit subnet associations: subnet-039eb8c670a658c06 / Private subnet Edge associations: -

**Routes (2)**

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	nat-06d75f87aae8283c	Active	No

Fig 9: Route list of the route table

You have successfully updated subnet associations for rtb-0b1d77b565ee8a07a / Private Route Table.

**rtb-0b1d77b565ee8a07a / Private Route Table**

Details Info

Route table ID: rtb-0b1d77b565ee8a07a Main: No Owner ID: vpc-0596d5852051c66fb | project 1 VPC

Explicit subnet associations: subnet-039eb8c670a658c06 / Private subnet Edge associations: -

**Subnet associations (1)**

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-039eb8c670a658c06 / Private subnet	10.0.2.0/24	-

**Subnets without explicit associations (0)**

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet ID	IPv4 CIDR	IPv6 CIDR
-	-	-

No subnets without explicit associations  
All your subnets are associated with a route table.

Fig 10: subnet association of the route table

### Step 3 : Creation of database and application servers

Step number	a
Step name	Creation of application server
Instructions	<ol style="list-style-type: none"><li>1) Navigate to EC2 using the Services button at the top of the screen</li><li>2) Select Instances at the left side of the screen</li><li>3) Click on Launch Instance</li><li>- Select the AMI Amazon 2 Linux</li><li>- Select the instance type t2.micro</li><li>- Select Network as "Project 1 VPC" and subnet as "Public Subnet"</li><li>- For the security group, open the ports 80,443, 22 and 8065 for source set to "Anywhere"</li><li>4) Launch the instance after creating a new pem file and downloading it</li></ol>
Expected screenshots	<ol style="list-style-type: none"><li>1) AMI used</li><li>2) Instance configuration screen</li><li>3) Security group rules</li><li>4) Instance after creation</li></ol>

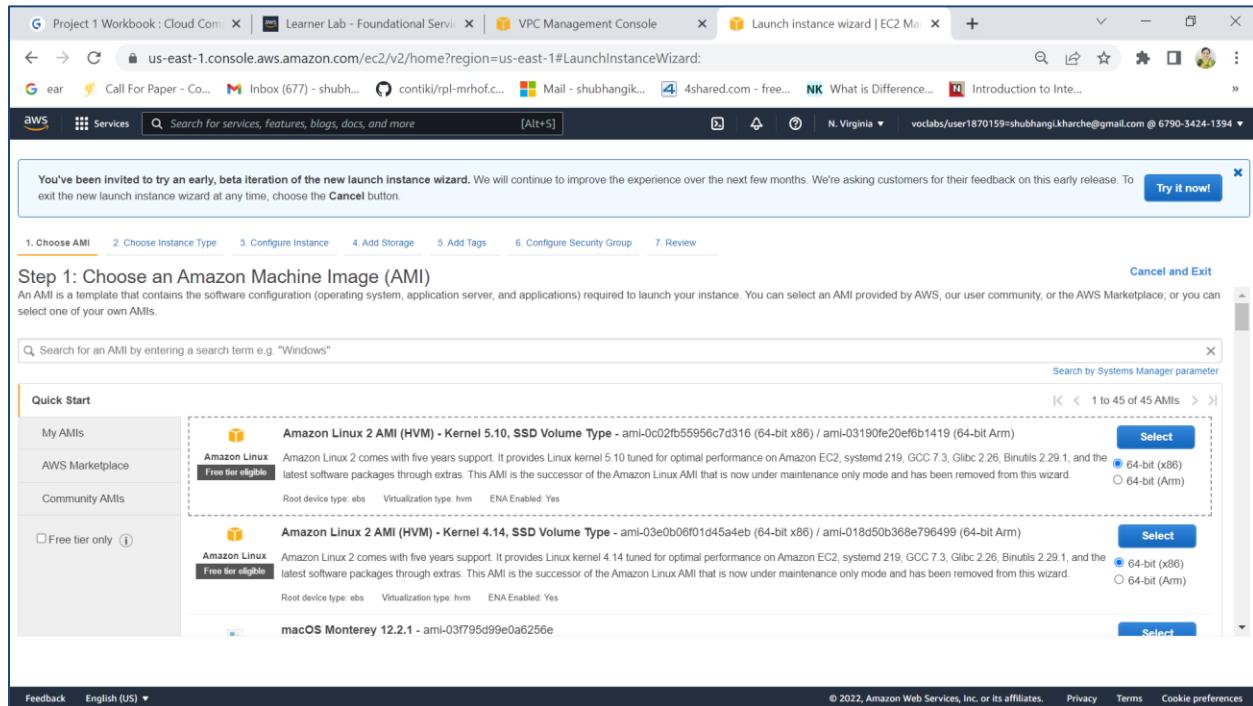


Fig 11: AMI used

**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 **Purchasing option:** Request Spot instances

**Network:** vpc-0596d5852051c66fb | project 1 VPC **Subnet:** subnet-057db3c27291f4056 | Public subnet | us-east-1

**Auto-assign Public IP:** Use subnet setting (Enable) **Hostname type:** Use subnet setting (IP name)

**DNS Hostname:**  Enable IP name IPv4 (A record) DNS requests  Enable resource-based IPv4 (A record) DNS requests  Enable resource-based IPv6 (AAAA record) DNS requests

**Placement group:**  Add instance to placement group **Capacity Reservation:** Open

**Domain join directory:** No directory **IAM role:** None

**Buttons:** Cancel, Previous, **Review and Launch**, Next: Add Storage

**Fig 12: Instance configuration screen**

**Step 6: Configure Security Group**

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

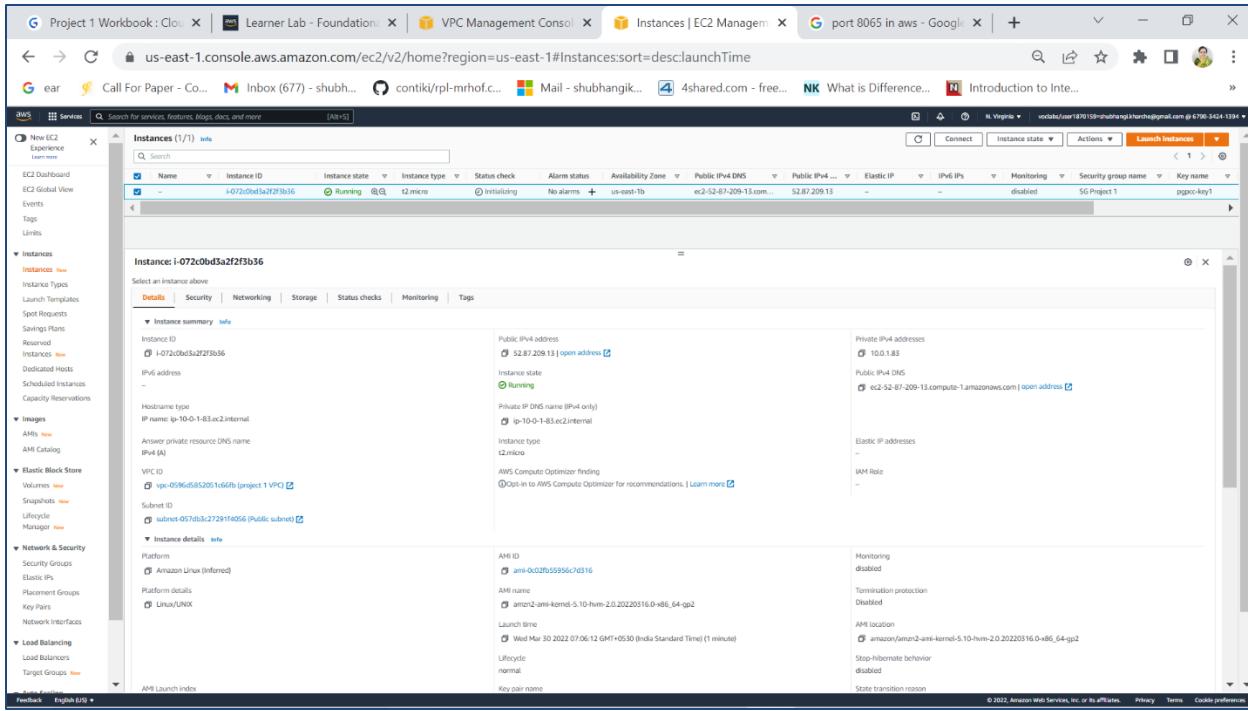
**Assign a security group:**  Create a new security group  Select an existing security group

**Security group name:** SG Project 1  
**Description:** launch-wizard-1 created 2022-03-30T06:58:05.566+05:30

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Anywhere	e.g. SSH for Admin Desktop
HTTP	TCP	80	Anywhere	e.g. SSH for Admin Desktop
Custom TCP	TCP	8065	Custom	mattermost

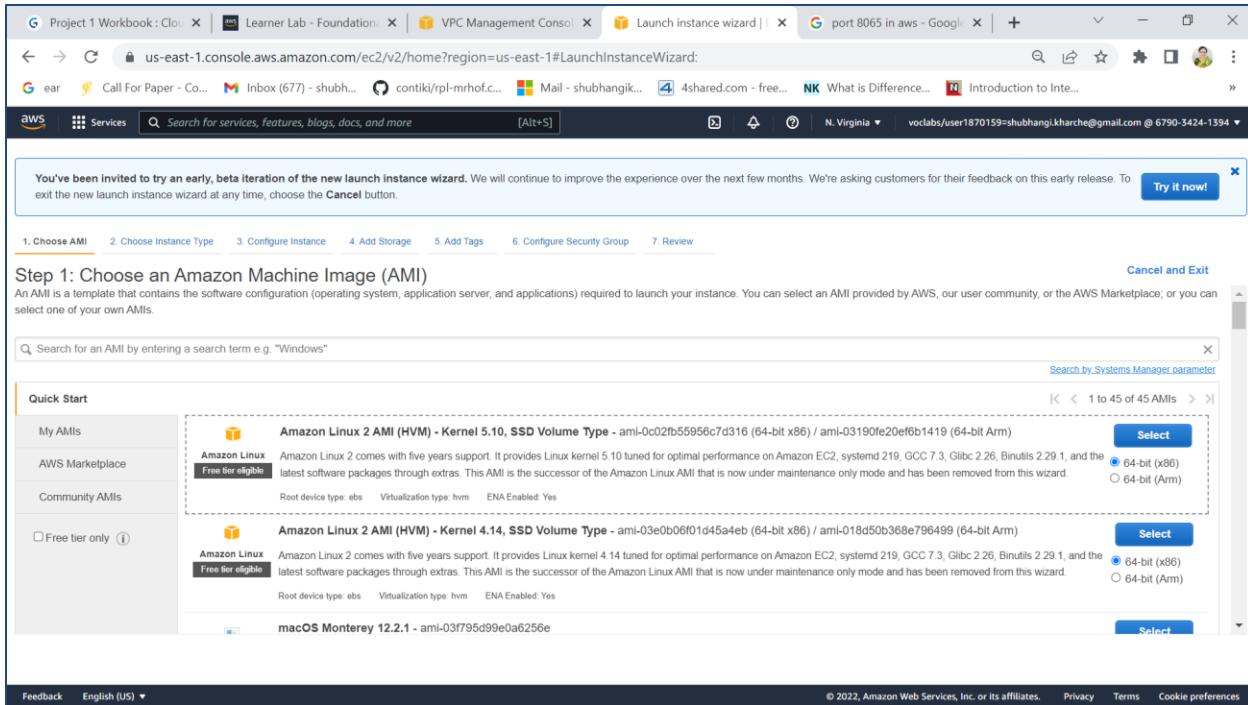
**Buttons:** Add Rule, Cancel, Previous, **Review and Launch**

**Fig 13: Security group rule**

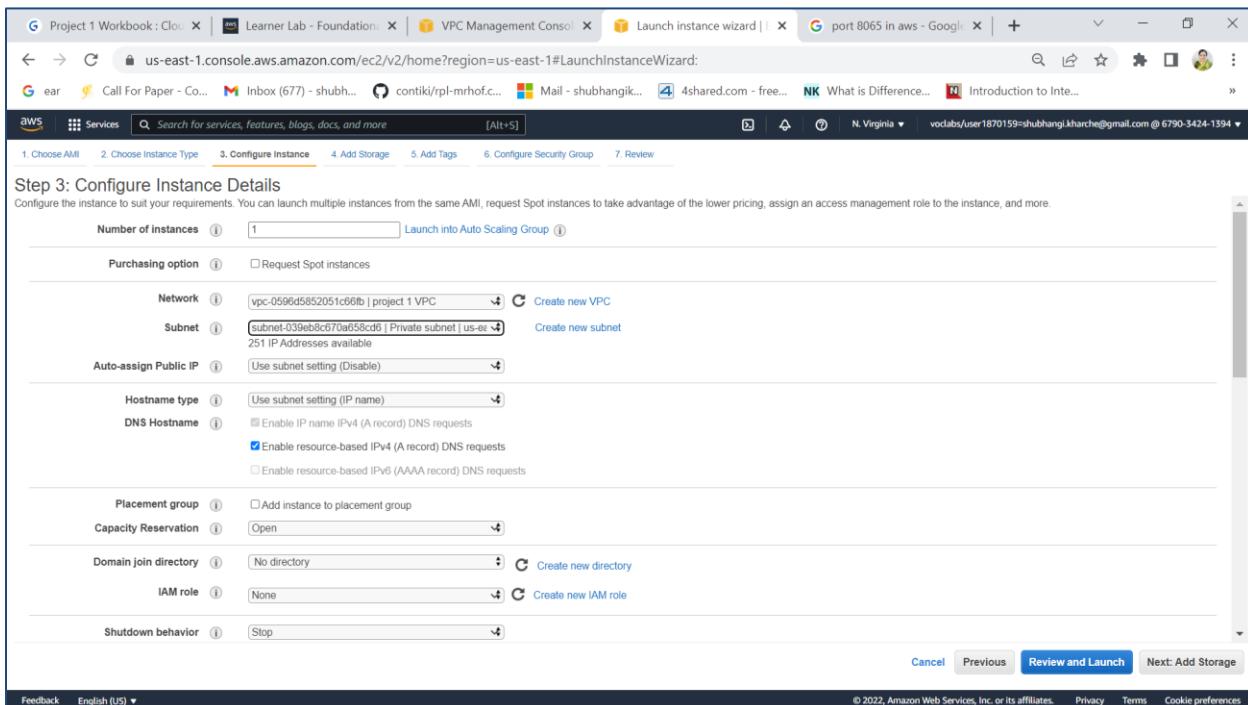


**Fig 14: Instance after creation**

Step number	b
Step name	Creation of database server
Instructions	<p>1) Navigate to EC2 using the Services button at the top of the screen</p> <p>2) Select Instances at the left side of the screen</p> <p>3) Click on Launch Instance</p> <ul style="list-style-type: none"> <li>- Select the AMI Amazon 2 Linux</li> <li>- Select the instance type t2.micro</li> <li>- Select Network as "Project 1 VPC" and subnet as "Private Subnet"</li> <li>- For the security group, open the ports 80, 443,22 and 3306 for source set to "Anywhere"</li> </ul> <p>4) Launch the instance by selecting the same pem file created in the previous step</p>
Expected screenshots	<ol style="list-style-type: none"> <li>1) AMI used</li> <li>2) Instance configuration screen</li> <li>3) Security group rules</li> <li>4) Instance after creation</li> </ol>



**Fig 15: AMI Used**



**Fig 16: Instance configuration screen**

**Step 6: Configure Security Group**

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

**Assign a security group:**  Create a new security group  Select an existing security group

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere	0.0.0.0/0, ::/0
HTTPS	TCP	443	Anywhere	0.0.0.0/0, ::/0
HTTP	TCP	80	Anywhere	0.0.0.0/0, ::/0
Custom TCP	TCP	3306	Anywhere	0.0.0.0/0, ::/0

**Add Rule**

**Warning**  
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.

**Review and Launch**

**Fig 17: security group rules**

**Instances (1/3) Info**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4	Elastic IP	IPv6 IPs	Monitoring	Security group name	Key name
-	i-0cd324b94f910be73	Running	t2.micro	Initializing	No alarms	us-east-1b	-	-	-	-	disabled	SG Project 1 DB	pgcc-key1
-	i-012eb696f74fcfb	Terminated	t2.micro	-	No alarms	us-east-1b	-	-	-	-	disabled	-	pgcc-key1
-	i-0720d5a2f2fb3b6	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	o-2-52-87-209-13.com...	52.87.209.13	-	-	disabled	SG Project 1	pgcc-key1

**Instance: i-0cd324b94f910be73**

**Details**

- Instance summary**
- Public IPv4 address**: 52.87.209.13
- Private IPv4 address**: 10.0.2.25
- Public IPv4 DNS**: o-2-52-87-209-13.com...
- Elastic IP addresses**: -
- IAM Role**: -

**Security**

- Amazon Linux (Inferred)**
- Platform details**: Linux/UNIX
- AMI ID**: ami-0x03fb55956c7ed316
- AMI name**: amazon2-amazon-kernel-5.10-hvm-2.0.20220316.0-x86\_64-gp2
- Launch time**: Wed Mar 30 2022 07:25:29 GMT+05:30 (India Standard Time) (1 minute)
- Lifecycle**: normal

**Fig 18: Instance after creation**

## Step 4: Application and Database Installation and Testing

Step number	a		
Step name	Installation and configuration of MySQL		
Instructions	<p>1) Copy the database pem file into the application server using the below command <code>scp -i &lt;application server pem file&gt; &lt;database server pem file&gt; ec2-user@&lt;application server public IP&gt;:/home/ec2-user</code></p> <p>2) Log into the application server using SSH/Putty</p> <p>3) From the application server, log into the database server using the pem file copied in step 1 and the private IP address of the database server with the following command <code>ssh -i &lt;database server pem file&gt; ec2-user@&lt;private IP of database server&gt;</code></p> <p>4) Enter the following commands to install and configure MySQL on the database server</p> <pre><code>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</code></pre> <p>Run the below command to retrieve a temporary password for MySQL</p> <pre><code>sudo grep 'temporary password' /var/log/mysqld.log   rev   cut -d" " -f1   rev   tr -d ":"</code></pre> <p>Log in to MySQL with the below command and enter the above password when prompted</p> <pre><code>mysql -u root -p</code></pre> <p>Enter the below command after you login to MySQL</p> <pre><code>ALTER USER 'root'@'localhost' IDENTIFIED BY 'Password42!';</code></pre> <p>Type 'exit' into the MySQL prompt and press Enter to exit out of the MySQL environment.</p> <p>Enter the below commands to complete the setup. Ignore any warning messages you receive.</p> <pre><code>wget https://d6opu47qoi4ee.cloudfront.net/install_mysql_linux.sh chmod 777 install_mysql_linux.sh sudo ./install_mysql_linux.sh</code></pre> <p>5) Type <code>exit</code> to exit the database server and go back to the application server</p> <tr><td>Expected screenshots</td><td><ul style="list-style-type: none"><li>1) Installation of MySQL</li><li>2) Retrieving the temporary password</li><li>3) Executing the provided script</li></ul></td></tr>	Expected screenshots	<ul style="list-style-type: none"><li>1) Installation of MySQL</li><li>2) Retrieving the temporary password</li><li>3) Executing the provided script</li></ul>
Expected screenshots	<ul style="list-style-type: none"><li>1) Installation of MySQL</li><li>2) Retrieving the temporary password</li><li>3) Executing the provided script</li></ul>		

```

Terminal File Edit View Search Terminal Help
mysql-community-common x86_64 5.7.37-1.el7
ncurses-compat-libs x86_64 6.0.8.20170212.amzn2.1.3
mysql57-community amzn2-core 311 k
308 k

Transaction Summary
=====
Install 3 Packages (+3 Dependent packages)

Total download size: 203 M
Downloaded packages:
(1/6): mysql-community-common-5.7.37-1.el7.x86_64.rpm | 311 kB 00:00:00
(2/6): mysql-community-client-5.7.37-1.el7.x86_64.rpm | 25 MB 00:00:00
(3/6): mysql-community-libs-compat-5.7.37-1.el7.x86_64.rpm | 1.2 MB 00:00:00
(4/6): mysql-community-libs-5.7.37-1.el7.x86_64.rpm | 2.4 MB 00:00:00
(5/6): ncurses-compat-libs-6.0.8.20170212.amzn2.1.3.x86_64.rpm | 308 kB 00:00:00
(6/6): mysql-community-server-5.7.37-1.el7.x86_64.rpm | 174 MB 00:00:02

Total
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : mysql-community-common-5.7.37-1.el7.x86_64
  Installing : mysql-community-libs-5.7.37-1.el7.x86_64
  Installing : ncurses-compat-libs-6.0.8.20170212.amzn2.1.3.x86_64
  Installing : mysql-community-client-5.7.37-1.el7.x86_64
  Installing : mysql-community-server-5.7.37-1.el7.x86_64
  Installing : mysql-community-libs-compat-5.7.37-1.el7.x86_64
  Erasing   : 1:mariadb-libs-5.5.68-1.amzn2.x86_64
  Verifying  : ncurses-compat-libs-6.0.8.20170212.amzn2.1.3.x86_64
  Verifying  : mysql-community-libs-5.7.37-1.el7.x86_64
  Verifying  : mysql-community-client-5.7.37-1.el7.x86_64
  Verifying  : mysql-community-common-5.7.37-1.el7.x86_64
  Verifying  : mysql-community-server-5.7.37-1.el7.x86_64
  Verifying  : mysql-community-client-5.7.37-1.el7.x86_64
  Verifying  : 1:mariadb-libs-5.5.68-1.amzn2.x86_64

Installed:
  mysql-community-libs.x86_64 0:5.7.37-1.el7          mysql-community-libs-compat.x86_64 0:5.7.37-1.el7          mysql-community-server.x86_64 0:5.7.37-1.el7

Dependency Installed:
  mysql-community-client.x86_64 0:5.7.37-1.el7      mysql-community-common.x86_64 0:5.7.37-1.el7      ncurses-compat-libs.x86_64 0:6.0.8.20170212.amzn2.1.3

Replaced:
  mariadb-libs.x86_64 1:5.5.68-1.amzn2

Completed!
[ec2-user@ip-10-0-2-25 ~]$ sudo systemctl start mysqld.service
[ec2-user@ip-10-0-2-25 ~]$ sudo grep 'temporary password' /var/log/mysqld.log |rev |cut -d"" -f1|rev|tr -d "."
cut: the delimiter must be a single character
Try 'cut --help' for more information.
[ec2-user@ip-10-0-2-25 ~]$ sudo grep 'temporary password' /var/log/mysqld.log |rev | cut -d"" -f1 | rev | tr -d "."
cut: the delimiter must be a single character
Try 'cut --help' for more information.

```

**Fig 19: Installation of MySql**

```

Terminal File Edit View Search Terminal Help
Installed:
  mysql-community-libs.x86_64 0:5.7.37-1.el7          mysql-community-libs-compat.x86_64 0:5.7.37-1.el7          mysql-community-server.x86_64 0:5.7.37-1.el7
Dependency Installed:
  mysql-community-client.x86_64 0:5.7.37-1.el7      mysql-community-common.x86_64 0:5.7.37-1.el7      ncurses-compat-libs.x86_64 0:6.0.8.20170212.amzn2.1.3
Replaced:
  mariadb-libs.x86_64 1:5.5.68-1.amzn2

Complete!
[ec2-user@ip-10-0-2-25 ~]$ sudo systemctl start mysqld.service
[ec2-user@ip-10-0-2-25 ~]$ sudo grep 'temporary password' /var/log/mysqld.log |rev |cut -d"" -f1|rev|tr -d "."
cut: the delimiter must be a single character
Try 'cut --help' for more information.
[ec2-user@ip-10-0-2-25 ~]$ sudo grep 'temporary password' /var/log/mysqld.log |rev | cut -d"" -f1 | rev | tr -d "."
cut: the delimiter must be a single character
Try 'cut --help' for more information.
[ec2-user@ip-10-0-2-25 ~]$ sudo grep 'temporary password' /var/log/mysqld.log |rev | cut -d"" -f1 | rev | tr -d "."
2022-03-30T03:13:15Z85284Z [Note] A temporary password is generated for root@localhost: /UwRnG7glUq=
[ec2-user@ip-10-0-2-25 ~]$ mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
[ec2-user@ip-10-0-2-25 ~]$ mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
[ec2-user@ip-10-0-2-25 ~]$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.37

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> ALTER USER 'root@localhost' IDENTIFIED BY 'Password42!';
ERROR 1820 (HY000): You must reset your password using ALTER USER statement before executing this statement.
mysql> ALTER USER 'root'@'localhost' IDENTIFIED BY 'Password42!';
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
[ec2-user@ip-10-0-2-25 ~]$ wget https://d0opu47qo14ee.cloudfront.net/install_mysql_linux.sh
https://d0opu47qo14ee.cloudfront.net/install_mysql_linux.sh: The requested URL was not found on this server.
[ec2-user@ip-10-0-2-25 ~]$ wget https://d0opu47qo14ee.cloudfront.net/install_mysql_linux.sh
2022-03-30 03:24:27-- https://d0opu47qo14ee.cloudfront.net/install_mysql_linux.sh
Resolving d0opu47qo14ee.cloudfront.net (d0opu47qo14ee.cloudfront.net)... 99.84.218.168, 99.84.218.37, 99.84.218.70, ...

```

**Fig 20: Retrieving the temporary password**

```

Terminal File Edit View Search Terminal Help
Server version: 5.7.37
Copyright (c) 2000, 2022, Oracle and/or its affiliates.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> ALTER USER 'root@localhost' IDENTIFIED BY 'Password42!';
ERROR 1820 (HY000): You must reset your password using ALTER USER statement before executing this statement.
mysql> ALTER USER 'root'@'localhost' IDENTIFIED BY 'Password42!';
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
[ec2-user@ip-10-0-2-25 ~]$ wget https://d6opu47qoi4ee.cloudfront.net/install_mysql_linux.sh
https://d6opu47qoi4ee.cloudfront.net/install_mysql_linux.sh: Unsupported scheme 'https'.
[ec2-user@ip-10-0-2-25 ~]$ wget https://d6opu47qoi4ee.cloudfront.net/install_mysql_linux.sh
--2022-03-30 03:24:27-- https://d6opu47qoi4ee.cloudfront.net/install_mysql_linux.sh
Resolving d6opu47qoi4ee.cloudfront.net (d6opu47qoi4ee.cloudfront.net)... 99.84.218.168, 99.84.218.37, 99.84.218.70, ...
Connecting to d6opu47qoi4ee.cloudfront.net (d6opu47qoi4ee.cloudfront.net)|99.84.218.168|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 189 [text/x-sh]
Saving to: 'install_mysql_linux.sh'

100%[=====] 189 --.-K/s in 0s

2022-03-30 03:24:27 (5.95 MB/s) - 'install_mysql_linux.sh' saved [189/189]

[ec2-user@ip-10-0-2-25 ~]$ chmod 777 install_mysql_linux.sh
[ec2-user@ip-10-0-2-25 ~]$ sudo ./install_mysql_linux.sh
mysql: [Warning] Using a password on the command line interface can be insecure.

[ec2-user@ip-10-0-2-25 ~]$ mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.7.37 MySQL Community Server (GPL)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

[ec2-user@ip-10-0-2-25 ~]$ Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>

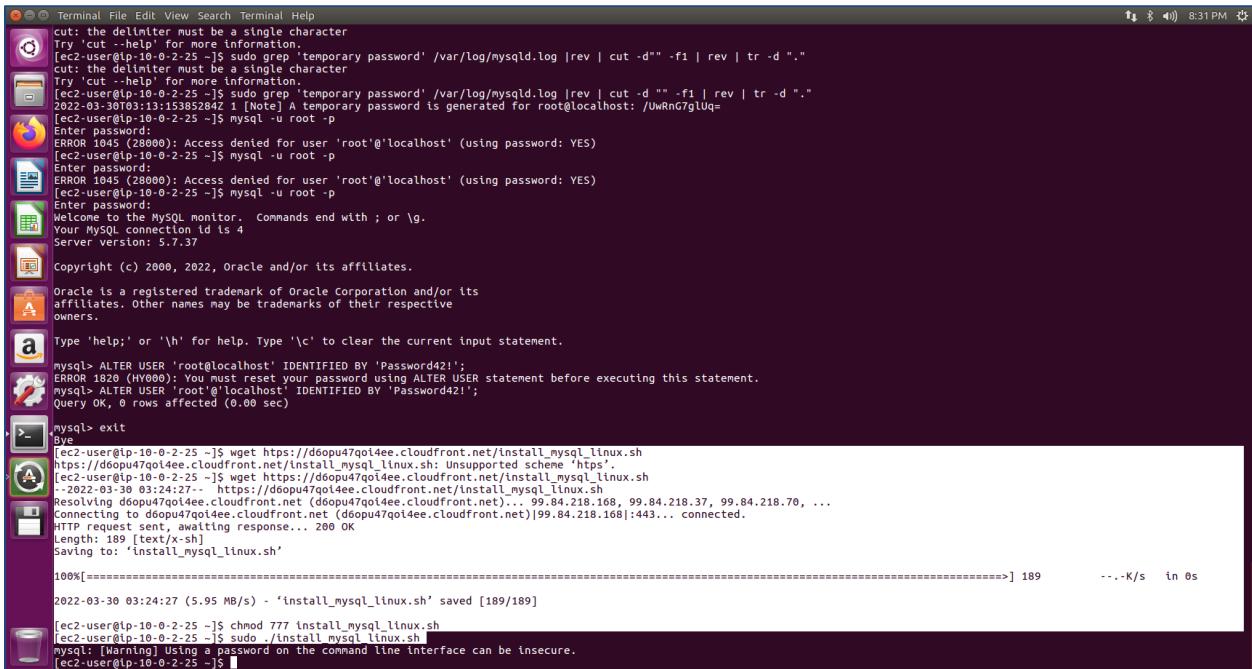
```

**Fig 21: Executing the provided script**

Step number	b
Step name	Installation and configuration of Mattermost
Instructions	<p>1) Enter the following commands after logging into the application server via SSH to install and configure Mattermost</p> <pre>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 &lt;private IP of MySQL server&gt; 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</pre> <p>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.</p> <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



```
Terminal File Edit View Search Terminal Help
[ec2-user@ip-10-0-2-25 ~]$ cut: the delimiter must be a single character
Try 'cut --help' for more information.
[ec2-user@ip-10-0-2-25 ~]$ sudo grep 'temporary password' /var/log/mysqld.log |rev | cut -d"\" -f1 | rev | tr -d "."
cut: the delimiter must be a single character
Try 'cut --help' for more information.
[ec2-user@ip-10-0-2-25 ~]$ sudo grep 'temporary password' /var/log/mysqld.log |rev | cut -d "" -f1 | rev | tr -d "."
[ec2-user@ip-10-0-2-25 ~]$ mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
[ec2-user@ip-10-0-2-25 ~]$ mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
[ec2-user@ip-10-0-2-25 ~]$ mysql -u root -p
Enter password:
Copyright (c) 2000, 2022, Oracle and/or its affiliates.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> ALTER USER 'root@localhost' IDENTIFIED BY 'Password42!';
ERROR 1820 (HY000): You must reset your password using ALTER USER statement before executing this statement.
mysql> ALTER USER 'root'@'localhost' IDENTIFIED BY 'Password42!';
Query OK, 0 rows affected (0.00 sec)

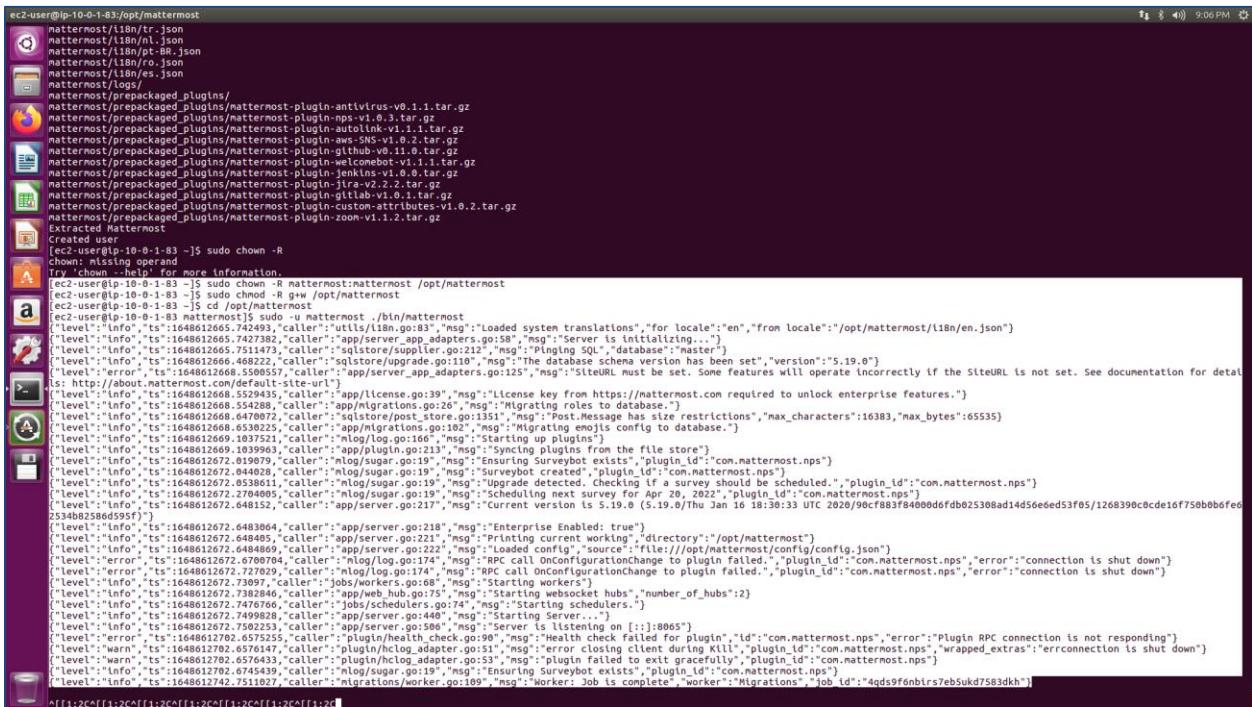
mysql> exit
Bye
[ec2-user@ip-10-0-2-25 ~]$ wget https://d0opu47qo4ee.cloudfront.net/install_mysql_linux.sh
https://d0opu47qo4ee.cloudfront.net/install_mysql_linux.sh: Unsupported scheme 'https'.
[ec2-user@ip-10-0-2-25 ~]$ wget https://d0opu47qo4ee.cloudfront.net/install_mysql_linux.sh
--2022-03-30 03:24:27-- https://d0opu47qo4ee.cloudfront.net/install_mysql_linux.sh
Resolving d0opu47qo4ee.cloudfront.net (d0opu47qo4ee.cloudfront.net)... 99.84.218.168, 99.84.218.70, ...
Connecting to d0opu47qo4ee.cloudfront.net (d0opu47qo4ee.cloudfront.net)|99.84.218.168|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 189 [text/x-sh]
Saving to: 'install_mysql_linux.sh'

100%[=====] 189 --.-K/s in 0s

2022-03-30 03:24:27 (5.95 MB/s) - 'install_mysql_linux.sh' saved [189/189]

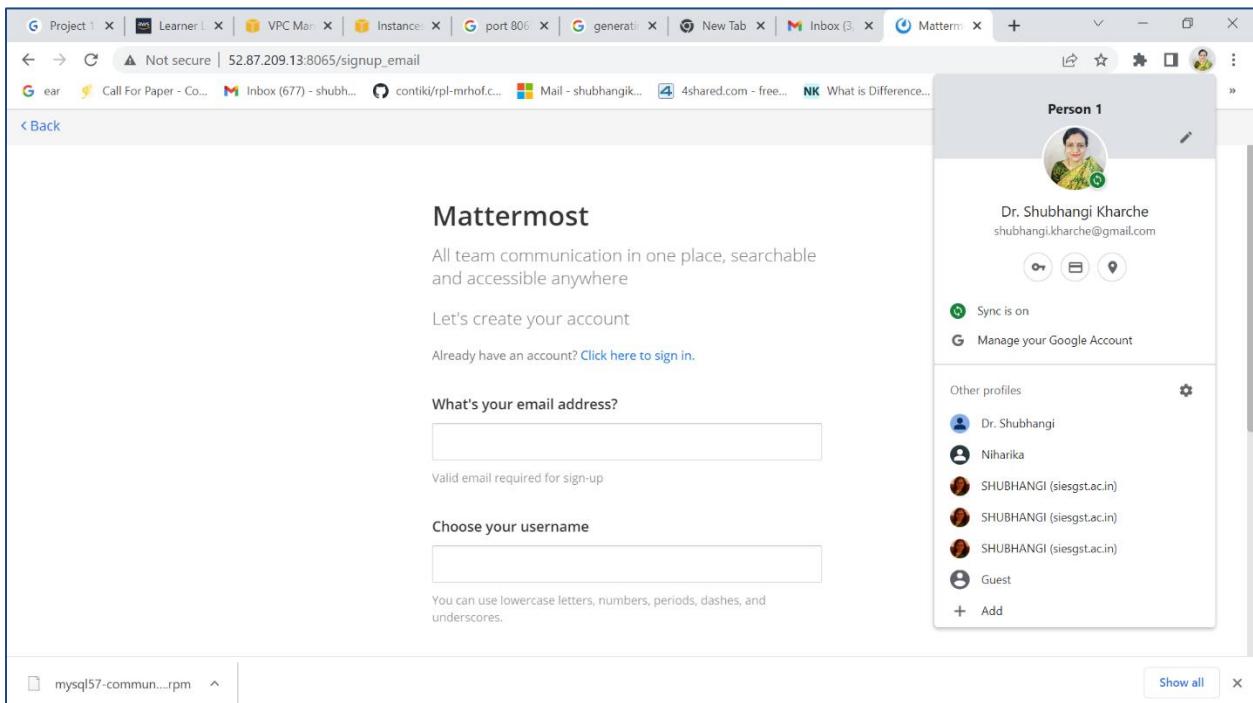
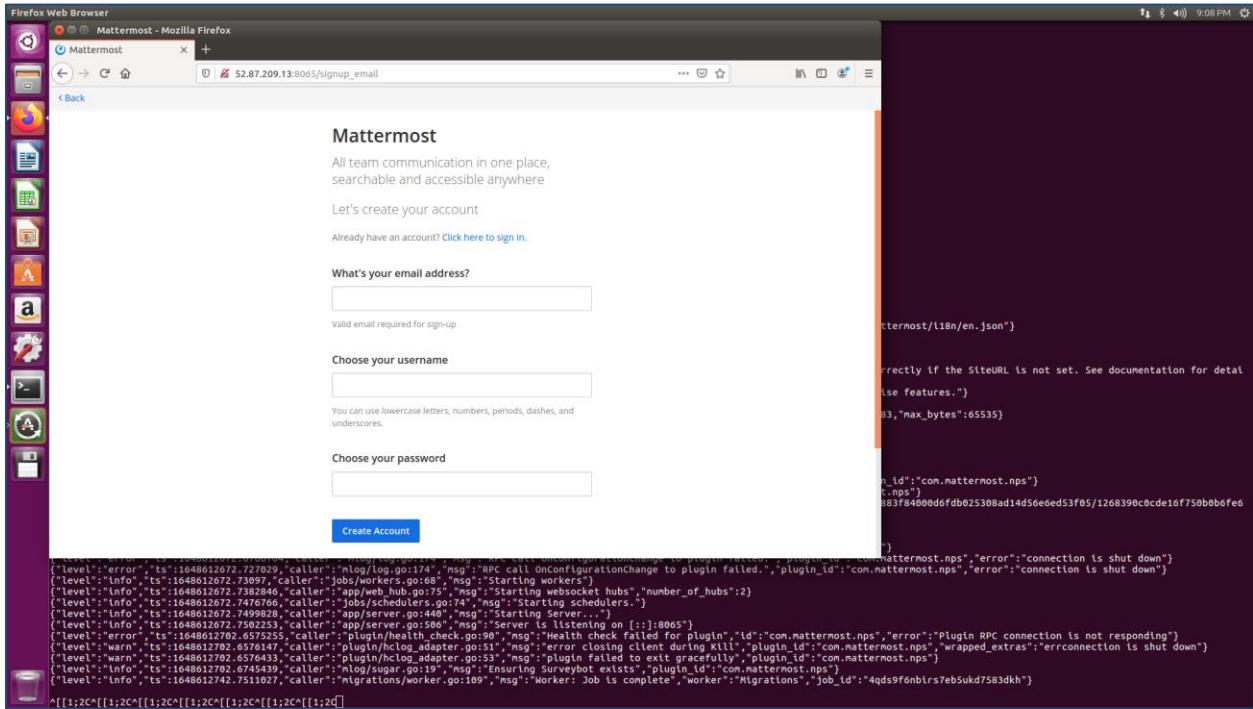
[ec2-user@ip-10-0-2-25 ~]$ chmod 777 install_mysql_linux.sh
[ec2-user@ip-10-0-2-25 ~]$ sudo ./install_mysql_linux.sh
[ec2-user@ip-10-0-2-25 ~]$
```

Fig 22: Executing the script



```
ec2-user@ip-10-0-1-83:/opt/mattermost
mattermost/l18n/zh.json
mattermost/l18n/zh_TW.json
mattermost/l18n/pt_BR.json
mattermost/l18n/ro.json
mattermost/l18n/es.json
mattermost/logs
mattermost/prepackaged_plugins/
mattermost/prepackaged_plugins/mattermost-plugin-antivirus-v0.1.1.tar.gz
mattermost/prepackaged_plugins/mattermost-plugin-nps-v1.0.3.tar.gz
mattermost/prepackaged_plugins/mattermost-plugin-autolink-v1.1.1.tar.gz
mattermost/prepackaged_plugins/mattermost-plugin-jenkins-v1.0.0.tar.gz
mattermost/prepackaged_plugins/mattermost-plugin-welcomebot-v1.1.0.tar.gz
mattermost/prepackaged_plugins/mattermost-plugin-jenkins-v1.0.0.tar.gz
mattermost/prepackaged_plugins/mattermost-plugin-jenkins-v1.0.1.2.tar.gz
mattermost/prepackaged_plugins/mattermost-plugin-jenkins-v1.0.1.2.tar.gz
mattermost/prepackaged_plugins/mattermost-plugin-custom-attributes-v1.0.2.tar.gz
mattermost/prepackaged_plugins/mattermost-plugin-zoom-v1.1.2.tar.gz
Extracted Mattermost
Created directory: /opt/mattermost
[ec2-user@ip-10-0-1-83 ~]$ sudo chown -R
chown: missing operand
Try 'chown --help' for more information.
[ec2-user@ip-10-0-1-83 ~]$ sudo chmod -R g+w /opt/mattermost
[ec2-user@ip-10-0-1-83 ~]$ cd /opt/mattermost
[ec2-user@ip-10-0-1-83 mattermost]$ sudo ./mattermost
("level": "info", "ts": "1648612665.742493", "caller": "utils/libn.go:83", "msg": "Loaded system translations", "for_locale": "en", "from_locale": "/opt/mattermost/l18n/en.json"}
("level": "info", "ts": "1648612665.742506", "caller": "utils/libn.go:83", "msg": "Server is initializing...")
("level": "info", "ts": "1648612665.751147", "caller": "sqlstore/sqlstore.go:217", "msg": "Pinging SQL", "database": "master")
("level": "info", "ts": "1648612666.468225", "caller": "sqlstore/upgrade.go:110", "msg": "The database schema version has been set", "version": "5.19.0"}
("level": "error", "ts": "1648612668.550657", "caller": "app/server/app_adapters.go:125", "msg": "SiteURL must be set. Some features will operate incorrectly if the SiteURL is not set. See documentation for details")
("ts": "http://about.mattermost.com/default-site-url")
("level": "info", "ts": "1648612668.554288", "caller": "app/licenses.go:39", "msg": "License key from https://mattermost.com required to unlock enterprise features."}
("level": "info", "ts": "1648612668.554288", "caller": "app/migrations.go:26", "msg": "Migrating roles to database."}
("level": "info", "ts": "1648612668.6470672", "caller": "sqlstore/post_store.go:135", "msg": "Post.Message has size restrictions", "max_characters": 16383, "max_bytes": 65535}
("level": "info", "ts": "1648612668.6530225", "caller": "app/migrations.go:166", "msg": "Starting up plugin migrations from file store"}
("level": "info", "ts": "1648612668.6530225", "caller": "app/migrations.go:166", "msg": "Starting up plugin migrations from file store"}
("level": "info", "ts": "1648612672.019879", "caller": "mlog/sugar.go:19", "msg": "Ensuring Surveybot exists", "plugin_id": "com.mattermost.nps"}
("level": "info", "ts": "1648612672.044028", "caller": "mlog/sugar.go:19", "msg": "Surveybot created", "plugin_id": "com.mattermost.nps"}
("level": "info", "ts": "1648612672.0538611", "caller": "mlog/sugar.go:19", "msg": "Backup detected. Checking if a survey should be scheduled", "plugin_id": "com.mattermost.nps"}
("level": "info", "ts": "1648612672.2704085", "caller": "mlog/sugar.go:19", "msg": "Scheduling next survey for Apr 20, 2022", "plugin_id": "com.mattermost.nps"}
("level": "info", "ts": "1648612672.648152", "caller": "app/server/go:217", "msg": "Current version is 5.19.0 (5.19.0) Thu Jan 18 18:38:33 UTC 2020/90cf883f4000d6fdb25308ad14d50eed53f05/1268390c0cde16f750b0b6fe253db82586d595f}
("level": "info", "ts": "1648612672.6483864", "caller": "app/server.go:218", "msg": "Enterprise Enabled: true"}
("level": "info", "ts": "1648612672.648405", "caller": "app/server.go:222", "msg": "Printing current working directory", "directory": "/opt/mattermost")
("level": "info", "ts": "1648612672.648405", "caller": "app/server.go:222", "msg": "Using configuration file", "file": "/opt/mattermost/config/config.json"}
("level": "error", "ts": "1648612672.6796704", "caller": "mlog/log.go:174", "msg": "RPC call OnConfigurationChange to plugin failed", "plugin_id": "com.mattermost.nps", "error": "connection is shut down"}
("level": "error", "ts": "1648612672.727029", "caller": "mlog/log.go:174", "msg": "RPC call OnConfigurationChange to plugin failed", "plugin_id": "com.mattermost.nps", "error": "connection is shut down"}
("level": "info", "ts": "1648612672.730977", "caller": "jobs/workers.go:68", "msg": "Starting workers"}
("level": "info", "ts": "1648612672.740982", "caller": "app/websocket.go:103", "msg": "Starting websocket hubs", "number_of_hubs": 2}
("level": "info", "ts": "1648612672.747676", "caller": "jobs/job_schedulers.go:77", "msg": "Starting job schedulers."}
("level": "info", "ts": "1648612672.7499828", "caller": "app/server.go:440", "msg": "Starting Server..."}
("level": "info", "ts": "1648612672.750233", "caller": "app/server.go:506", "msg": "Server is listening on [:8005]"}
("level": "error", "ts": "1648612702.6575255", "caller": "plugin/health_check.go:98", "msg": "Health check failed for plugin", "id": "com.mattermost.nps", "error": "Plugin RPC connection is not responding"}
("level": "error", "ts": "1648612702.6575255", "caller": "plugin/health_check.go:98", "msg": "Error connecting to plugin due to kill", "id": "com.mattermost.nps", "wrapped_extras": "errconnection is shut down"}
("level": "warn", "ts": "1648612702.6745432", "caller": "app/hlog_adapter.go:53", "msg": "Plugin failed to exit gracefully", "id": "com.mattermost.nps"}
("level": "info", "ts": "1648612702.6745439", "caller": "mlog/sugar.go:19", "msg": "Ensuring Surveybot exists", "plugin_id": "com.mattermost.nps"}
("level": "info", "ts": "1648612742.7511927", "caller": "migrations/worker.go:109", "msg": "Worker: Job is complete", "worker": "Migrations", "job_id": "4qds9fnbirs7eb5ukd7583kh"}]
```

Fig 23: starting the mattermost server



**Fig 24: Accessing the application via web browser.**

## **Step 5: Answer the following questions**

### **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

Disabled

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

Bastion Host

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

TCP

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

8065

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) CIDR block  
overlaps with  
existing block

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

c) Port 443 on  
the NAT  
instance

Q7 Describe the steps you would take to increase security of the servers you have deployed so that they are not reachable from external sources

Below are the options to increase the security of the deployed servers so that they are not reachable from external resources:

Option 1) In the Security Group for application server restrict the access to allow SSH only from admin laptop.

Option 2) Disable SSH to application server from anywhere.

Option 3) Install a Bastion host in DMZ to access the servers.

Option 4) Keep the pem file in a secure place so that it is only accessible to admin

Q8 Describe the steps required to deploy the given application in an autoscaling environment

Below are the steps required to deploy the given application in an autoscaling environment:

- 1) Create a target group (TG) with two mattermost EC2 instances.
- 2) Create an application load balancer (LB), define the mattermost URL in the ALB to use port 8065.
- 3) Associate a TG with the LB.
- 4) Create a launch template (LT) of mattermost EC2 instance.
- 5) Setup the autoscaling group (ASG).
- 6) Access the application via web browser using the URL of mattermost defined in LB to access the application.

**Max marks** 15

<b>Grades distribution</b>	
MCQs	6 (1 mark each)
Subjective questions	10 marks (5+5)
Implementation screenshots	24 marks (1 marks each)
Total	40 marks