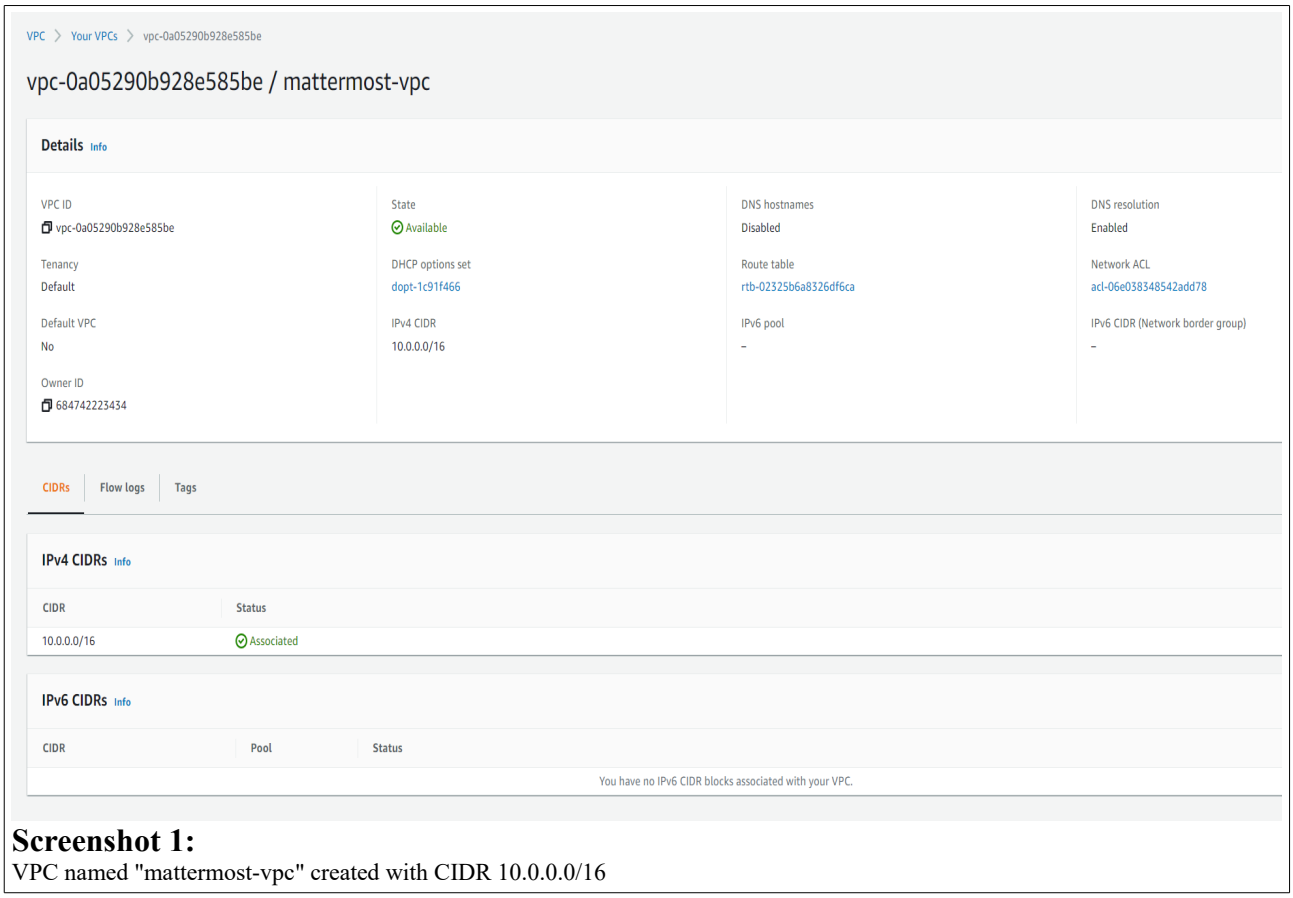
AWS Sysops Administrator Project

Name: Vlasis Pitsios
Email: vlasis.pitsios@vodafone.com
Company: Vodafone

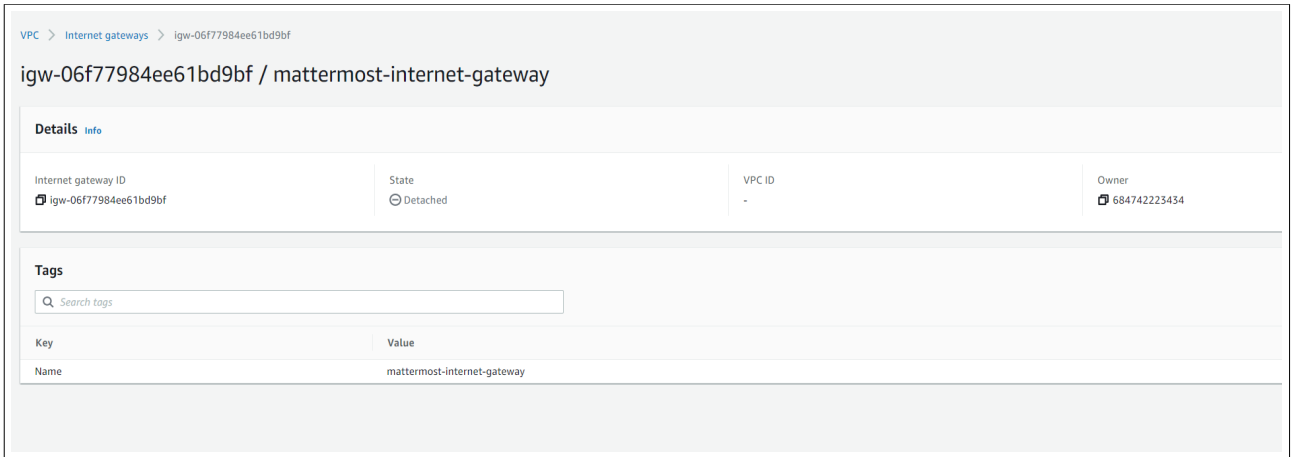
Main project (Description): You are a Cloud engineer working on a Team Communication Solution project for a big MNC. The client has compliance policies which do not allow them to use services managed by third parties. The client wants a team communication solution that can be managed and hosted on servers that are controlled by them.

Steps to perform

1) Implement two different subnets (one public and the other private) in a custom VPC
2) Install and configure MySQL on an Ubuntu 18.04 instance on the private subnet (Hint: Use a bastion host and a NAT instance)
3) Install and configure Mattermost on an Ubuntu 18.04 instance on the public subnet
4) Configure the security groups to allow the ports
5) Test the installation by accessing the IP of the public instance in a browser

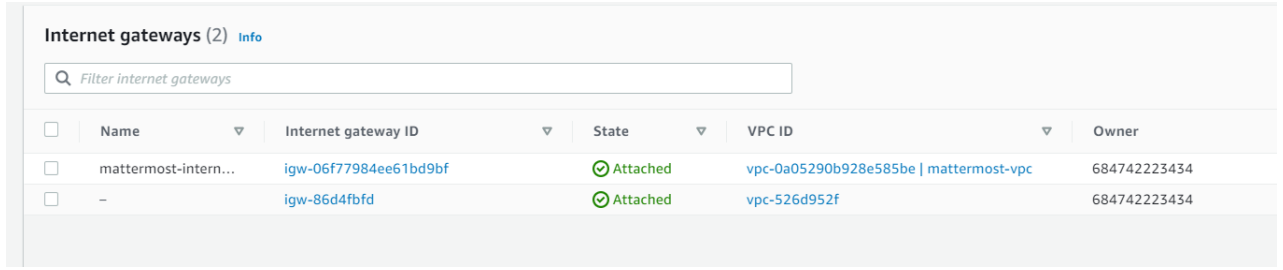


Screenshot 1:
VPC named "mattermost-vpc" created with CIDR 10.0.0.0/16



Screenshot 2:

Internet Gateway named as "mattermost-internet-gateway" created.

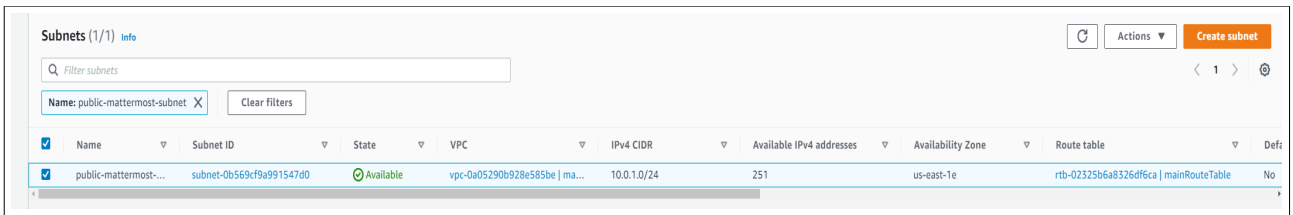


Screenshot 3:

Internet Gateway "mattermost-internet-gateway" is attached to "mattermost-vpc".

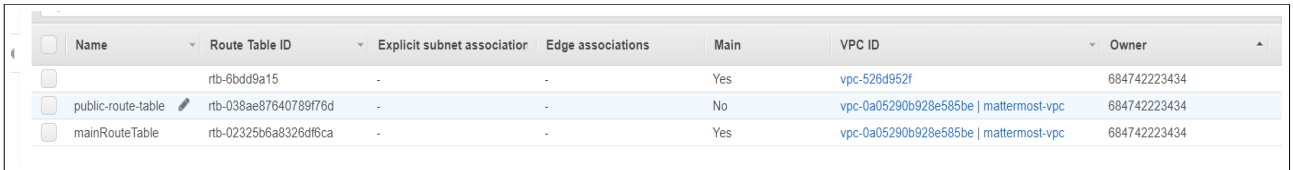
Screenshot 4:

Already existing route table is renamed to "mainRouteTable".



Screenshot 5:

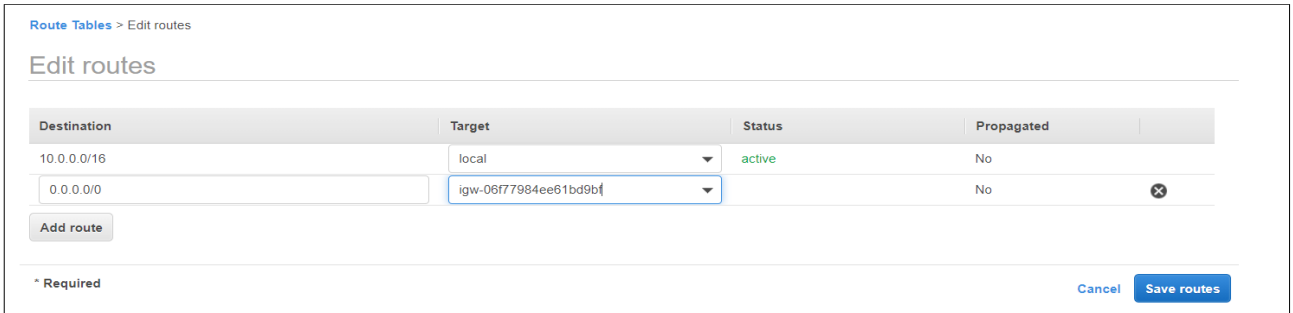
Public subnet named as "public-mattermost-subnet" created with CIDR 10.0.1.0/24. This subnet is attached to "mainRouteTable" route table.



Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
	rtb-6bdd9a15	-	-	Yes	vpc-526d952f	684742223434
public-route-table	rtb-038ae87640789f76d	-	-	No	vpc-0a05290b928e585be | mattermost-vpc	684742223434
mainRouteTable	rtb-02325b6a8326df6ca	-	-	Yes	vpc-0a05290b928e585be | mattermost-vpc	684742223434

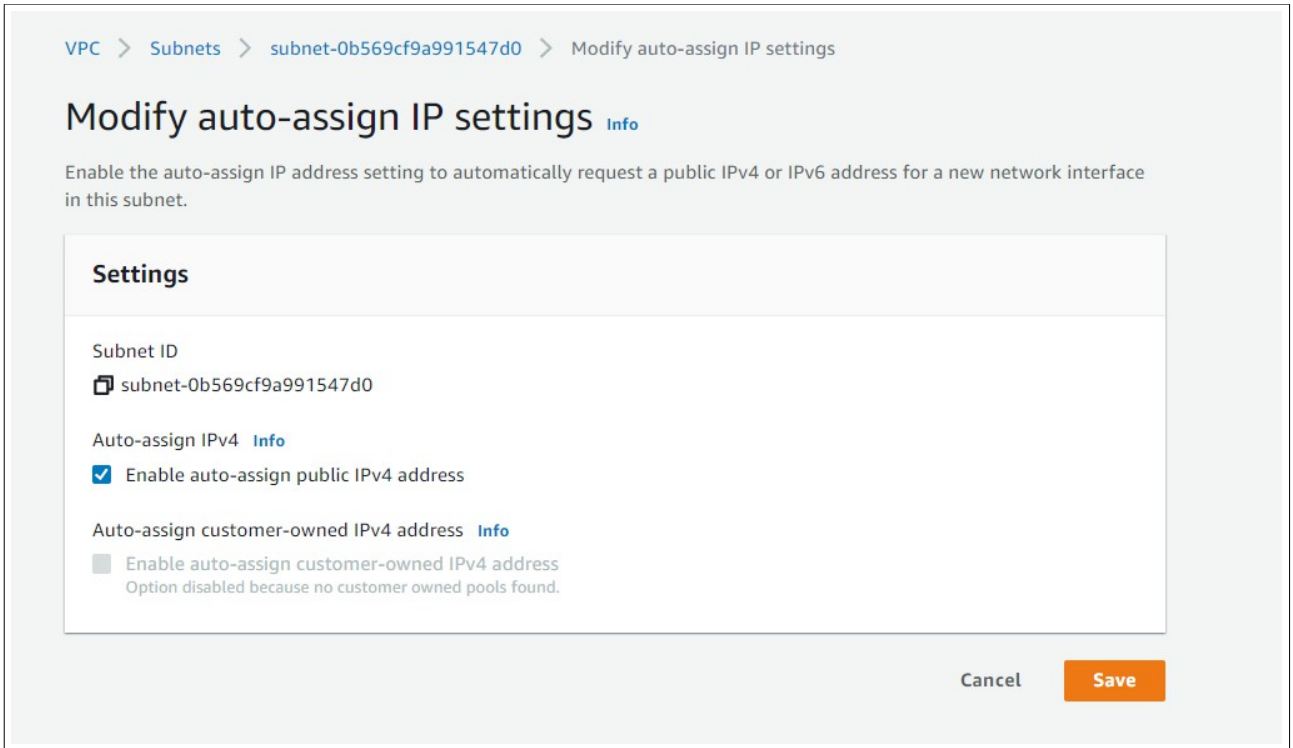
Screenshot 6:

Public route table named as "public route table" created. This public route table should be assigned to public subnet.



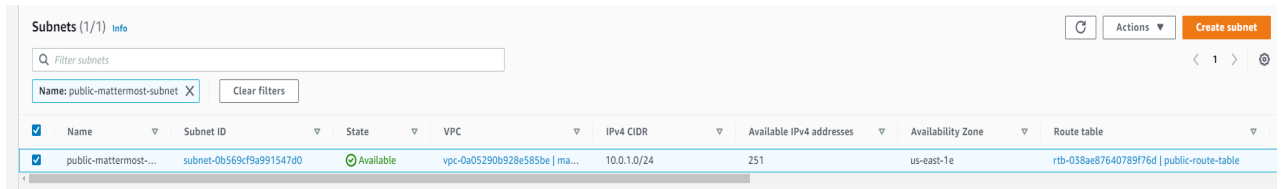
Screenshot 7:

Assign new route for destination "0.0.0.0/0" to the Internet Gateway on public route table.



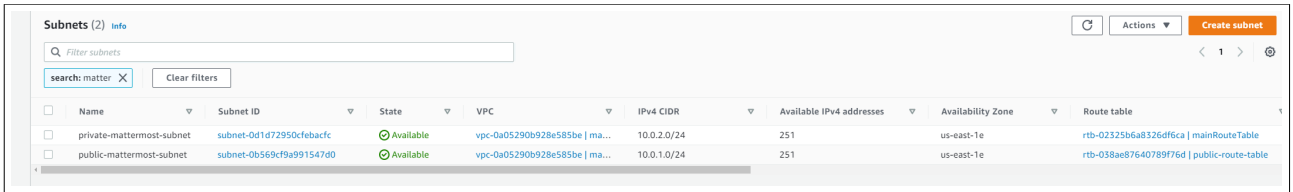
Screenshot 8:

Enable auto-assign public Ipv4 address to public subnet.



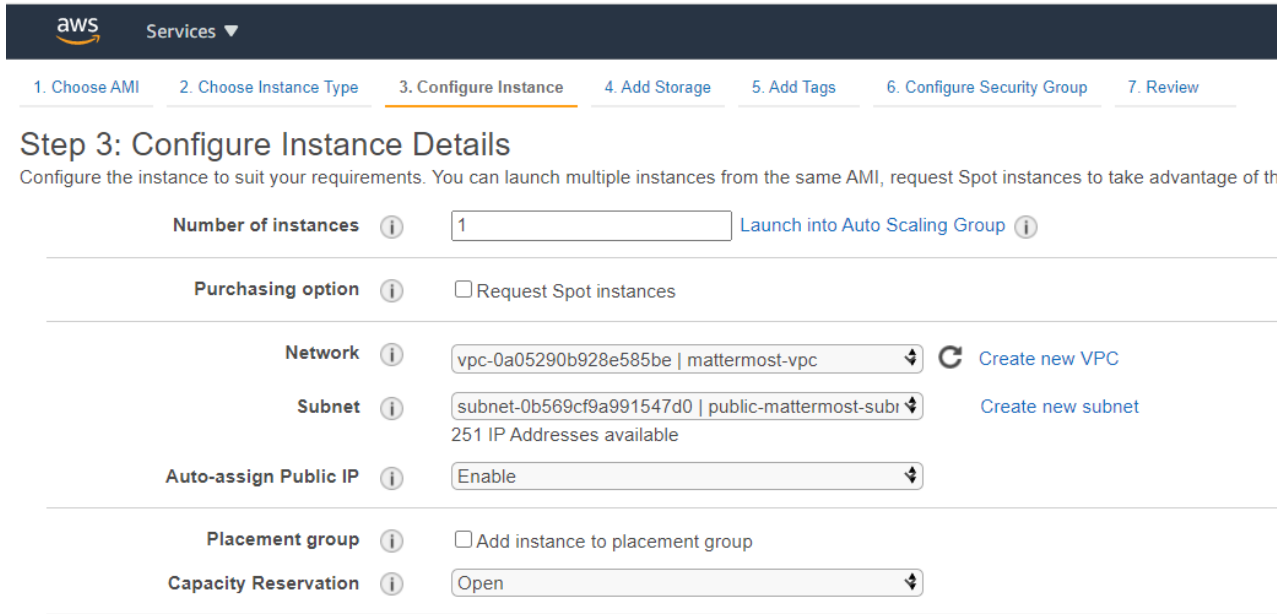
Screenshot 9:

Attach public route table to public subnet because we need the public subnet to be accessible from the internet.



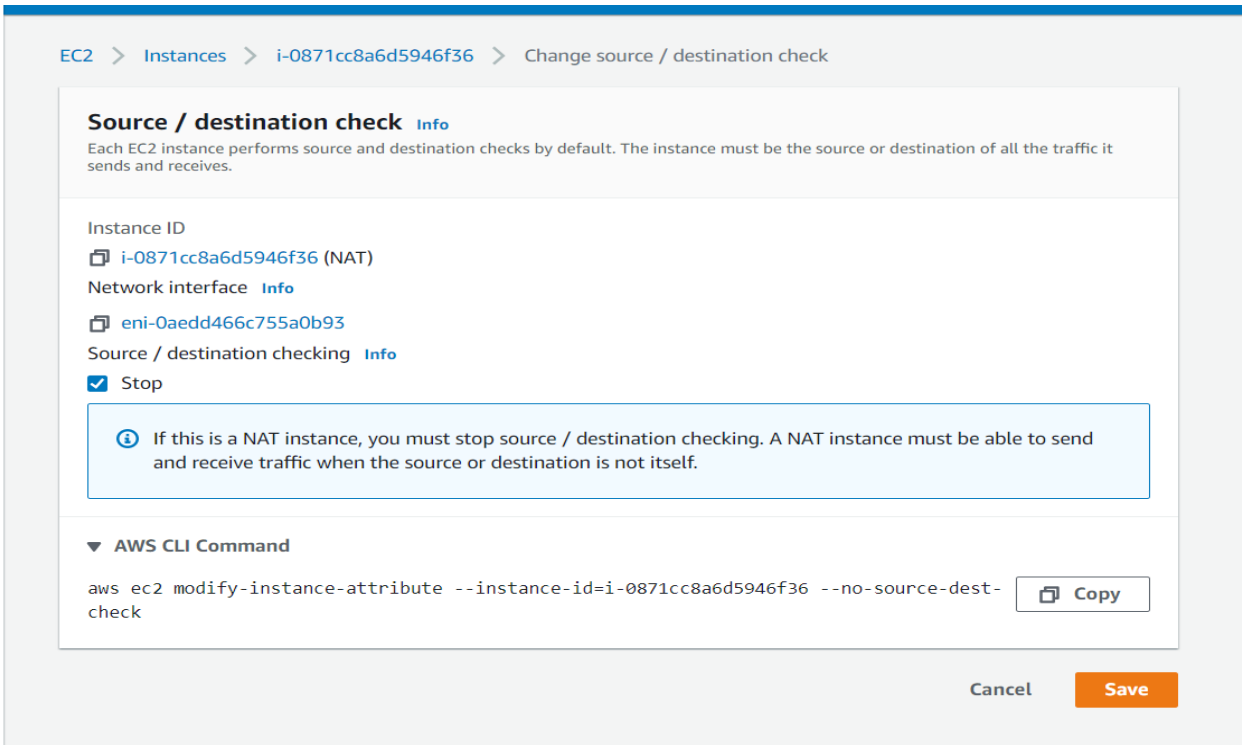
Screenshot 10:

Private subnet named as "private-mattermost-subnet" created with CIDR 10.0.2.0/24. This subnet is attached to "mainRouteTable" route table because this subnet should not be exposed to the internet.



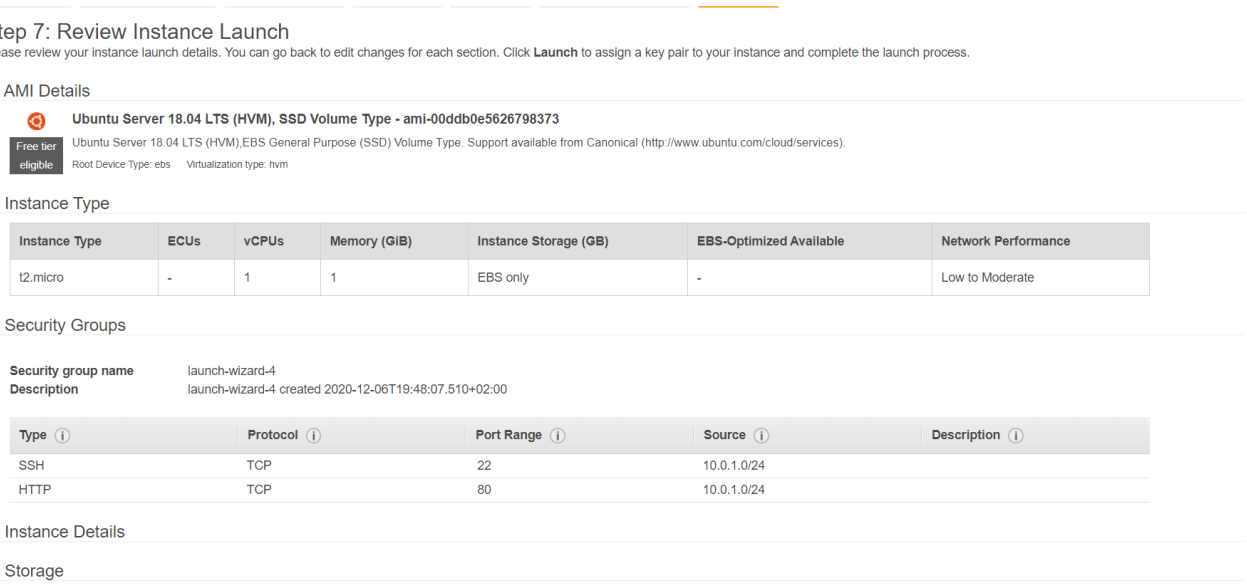
Screenshot 11:

Create a dedicated NAT EC2 instance on "mattermost-vpc" VPC and on public subnet. (The solution with EC2 as NAT instance did not work, that's why in a later step I use a VPC NAT Gateway instead)



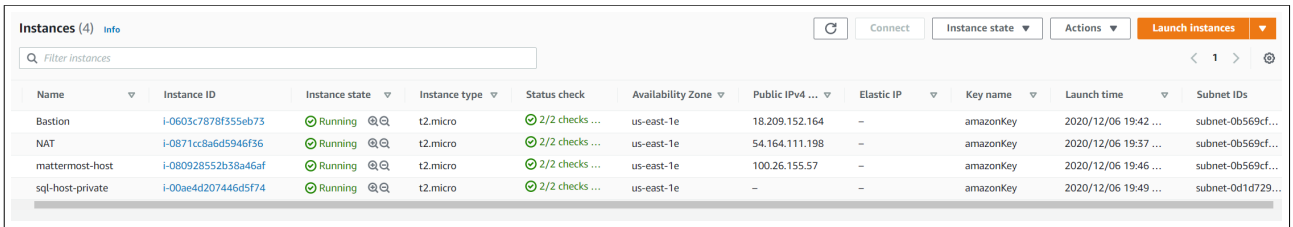
Screenshot 12:

Disable "Source / destination checking" on NAT EC2 instance. (The solution with EC2 as NAT instance did not work, that's why in a later step I use a VPC NAT Gateway instead)



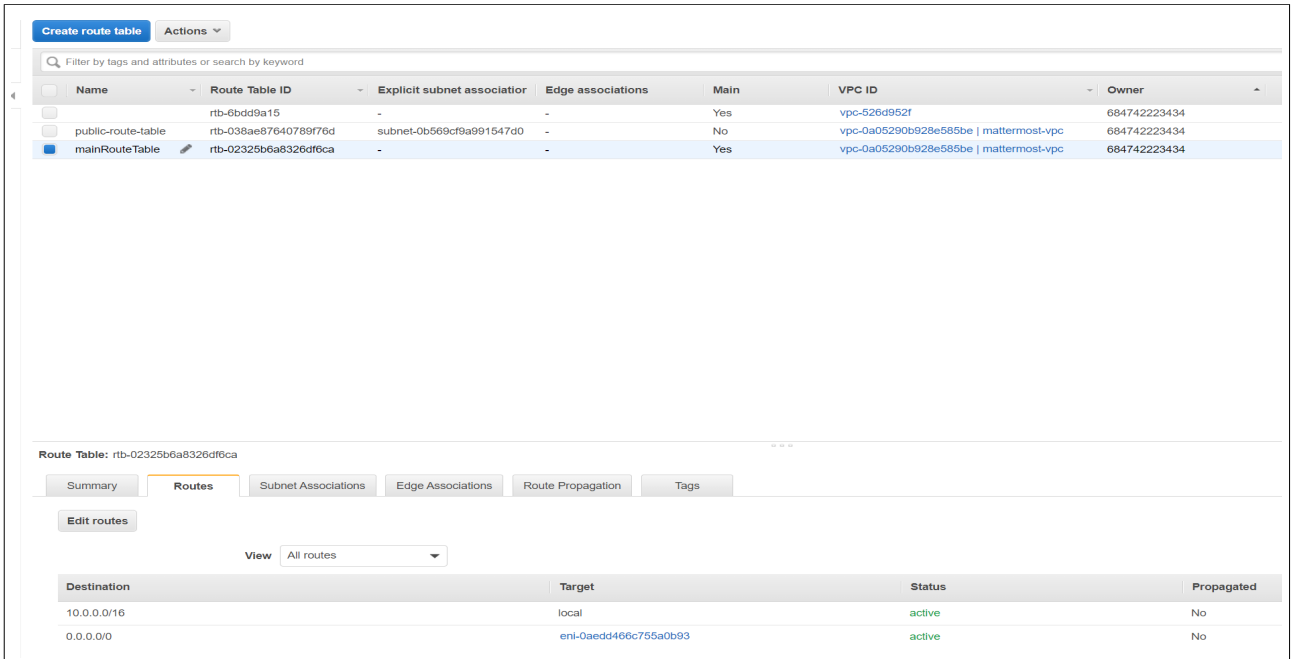
Screenshot 13:

Security group of the EC2 instance that will host the MySQL database and will exist on private subnet. This EC2 instance must accept traffic and SSH connection from the public subnet (10.0.1.0/24).



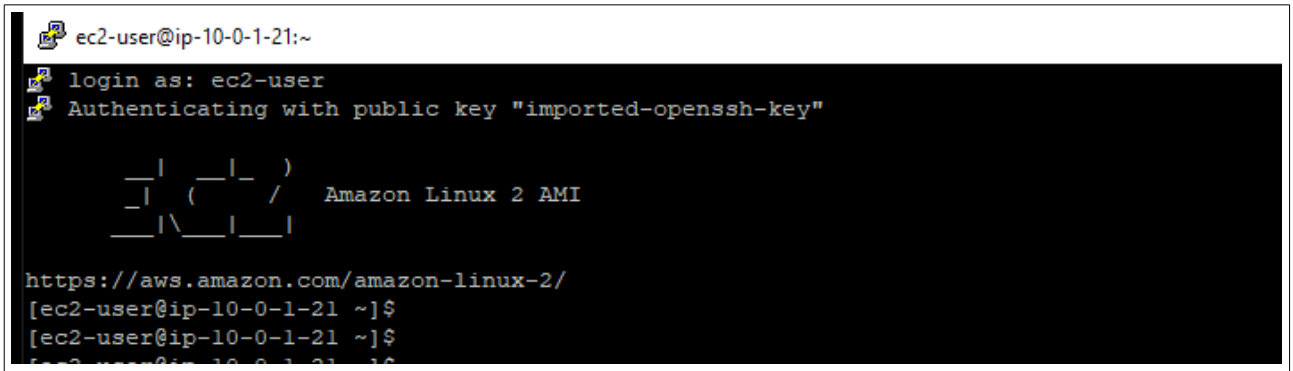
Screenshot 14:

All EC2 instances are ready. We need four (4) EC2 instances.
-A bastion EC2 on public subnet to connect to MySql instance on private subnet.
-A NAT EC2 on public subnet to redirect traffic from private subnet to the internet (The solution with EC2 as NAT instance did not work, that's why in a later step I use a VPC NAT Gateway instead).
-A mattermost-host instance on public subnet to install the mattermost application. This instance must have access to the MySql server on private subnet.
-A MySql EC2 instance on private subnet to install MySQL database.



Screenshot 15:

Add route with destination 0.0.0.0/0 and target the NAT EC2 server on main route table which is assigned to private subnet. This is necessary to install the MySql server on the EC2 instance on private subnet.



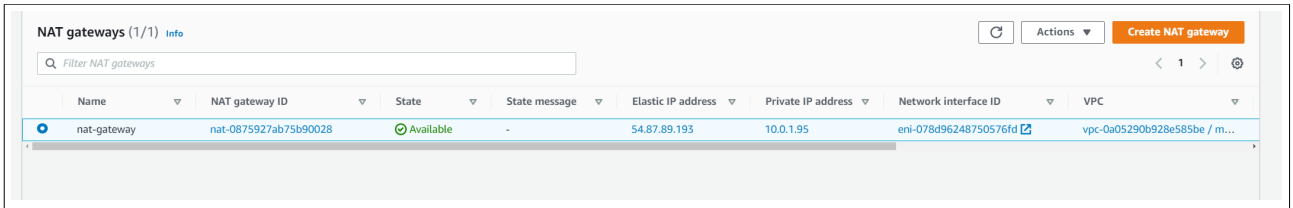
Screenshot 16:

Connect to Bastion EC2 server using Putty.

```
[root@ip-10-0-1-21 ec2-user]# cat private-key.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnsVblFoWIfAJ/Y2/oJLLpkFk4rbRmKxAM5t0ctwyJCpx55Nh
EtTl+qmsI7RY+jVlD/e4ef2ulgOVEbkvGlvK2cZ8iiLjDw42gD+Sb42HfnRikuml
yHpyNkTtJIATZfwy5r4ZOJfZD7qQYSSszzlYvqd7op8/tRJWIfkF2JeWPpJJQmnV
72crqrZv8SpgGeZMfStIWpggMF+drRRGGgf/qZi/HRu2fDc2gd40zoZBjbItpQ9T
ZJc3O7/vUHUqpiKYvSaUMExvLtFCIuPeeZKO07GJUGGaNhFc26AQFDwNvIGCrsXc
9UjMfQmcvMYRE4nU8N4ePTB3AlQdlfUNDzqOfwIDAQABAoIBAQCSvh3yc4DZRR42
tvhRlNtcgjxYPlhiH3IHQLrUHihJvOEiA9lIqnUUxBVRurIyL45Of8qFFa6uJwl0
JBAh3SkTNpyMn8n0dFJzHk6dw9VjTvZ8inllGZbOCc6UWbuUGxCAqlpsMAxyuSAQ
aPE/ZeVb8TgYCc+774KkS6DXmuNGWEEfwDl/520s2hQkf5+swQLnN8Wrh5gN0acW
fgWxIV8H35CoHZ/z5eel9jkNJ9CjN5Scpky+SOP7ZYQ+gKGCHlVt0PSkH65E7b0D
WveRFl+G5FsgiA0+hTL22bQb2gE6yybOBqlPSjpw7kFv/jTKBZIWB6Et60IG0IPn
ZCX5OYWhAoGBANS7meY5SKqYyGJfzQhX4+Z/7+EWDFYg5sDRf9MxlxshFaTrPSE4
bZKRSRv2tuC4FmJg52ql4IdDM6lsNiQLQGemcO8O+e0cXI7nRbInJBG6olVudVqv
4km9TlElYx9aAR4m3INujZKtDWOLuW56arslMFklQnlfcl5rur21E7SrAoGBAL8Q
HOsycDQzFbEzwoWApllxwBdGHOhqr96QiBtonlktCtnr41D6H16/AfBXDdp5PGnl
CvGj0c+mjMQdVRZiFOlUsSNGQmu8wwgx/6vlUhFiJHHAvaYp2kU54q2zINNiIMS3
3b0KaQYiyRMCbOzyk074YRKu5NRZ0YmGMYe+PAV9AoGBAMIJL5HnlBlO7A+WtEw0
5oG7FhCnbK8uqWsca8wlwk8TeUuI6aQgdQkoDZg9C4ejQX+QReR2aorVyBAZ0LRF
swQXs5DJhzs4EFCkMFUUEHk/U4w7CT2jifKagvtP776L+NMIvUAAmY882yZ+Lq/P
ZwTEugnFy4TRiEiKWLVqscOrAoGAZQCKmRcX07BxtjRrj5Gb3srQRjltSLwlbp2v
JfYfzs+N3ffiOkuPS9Hjn38VtrnCYy0D9Qup/YDJBl+OPH/rGi9cWQ5qTHQEEhAE
XY4ZLVFZfLzsRKv5VAEuwK5iGvzT38pnMOkQ7gpzilYL6RKvJt8MygiktVEqAO5s
vpqlNi0CgYBMqcUx2UONYbLC0P6K4Fk3Rzc9nCHN8yu2OzHC5lI2OOcl3jV9cc0Z
J+F3rN3Fl34RzlmihQ7noeens7bWGW72nBBHWlrV2mWd0RLIx2pTGFFhb6c7KTzV
Cv8zBlcUOcl8DOdCWECL996njolpSGG+l7NBkalaT+IajXU5+qHXmQ==
-----END RSA PRIVATE KEY-----
[root@ip-10-0-1-21 ec2-user]#
[root@ip-10-0-1-21 ec2-user]#
[root@ip-10-0-1-21 ec2-user]# ls
private-key.pem
[root@ip-10-0-1-21 ec2-user]#
[root@ip-10-0-1-21 ec2-user]# chmod 0600 private-key.pem
[root@ip-10-0-1-21 ec2-user]# ssh -i private-key.pem ec2-user@10.0.2.225
Authentication failed.
[root@ip-10-0-1-21 ec2-user]# ssh -i private-key.pem ubuntu@10.0.2.225
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Dec  6 18:25:43 UTC 2020

  System load:  0.0               Processes:           91
  Usage of /:   14.5% of 7.69GB   Users logged in:     0
  Memory usage: 17%               IP address for eth0: 10.0.2.225
  Swap usage:   0%

0 packages can be updated.
0 updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-2-225:~$
ubuntu@ip-10-0-2-225:~$
ubuntu@ip-10-0-2-225:~$
```

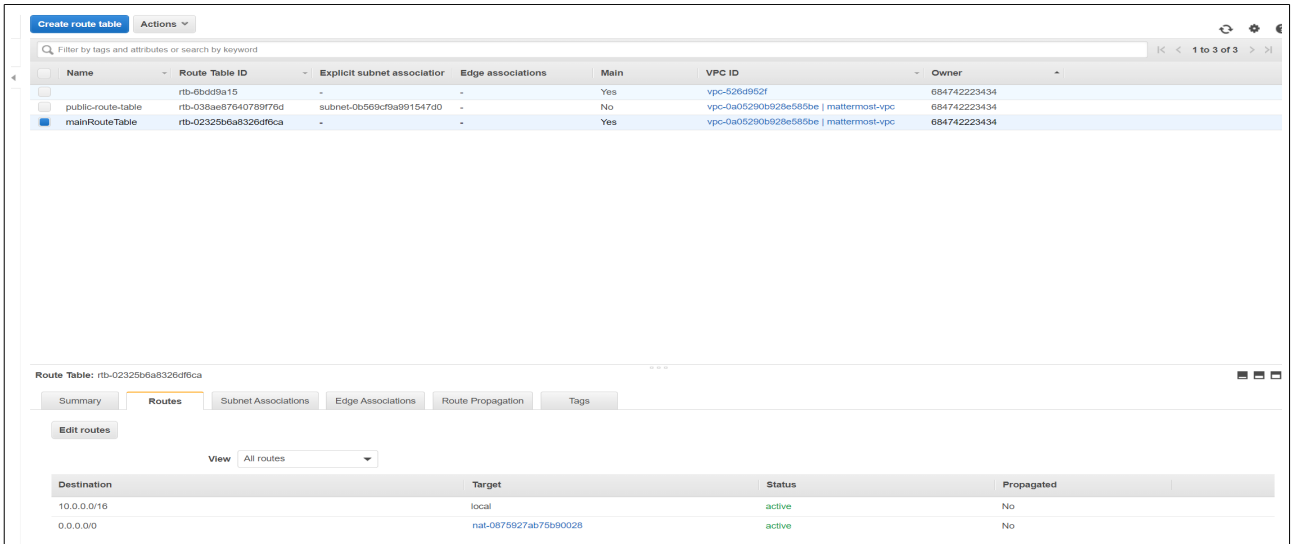
Screenshot 17:

Connect to MySql server with IP (10.0.2.225) on private subnet from Bastion EC2 server.



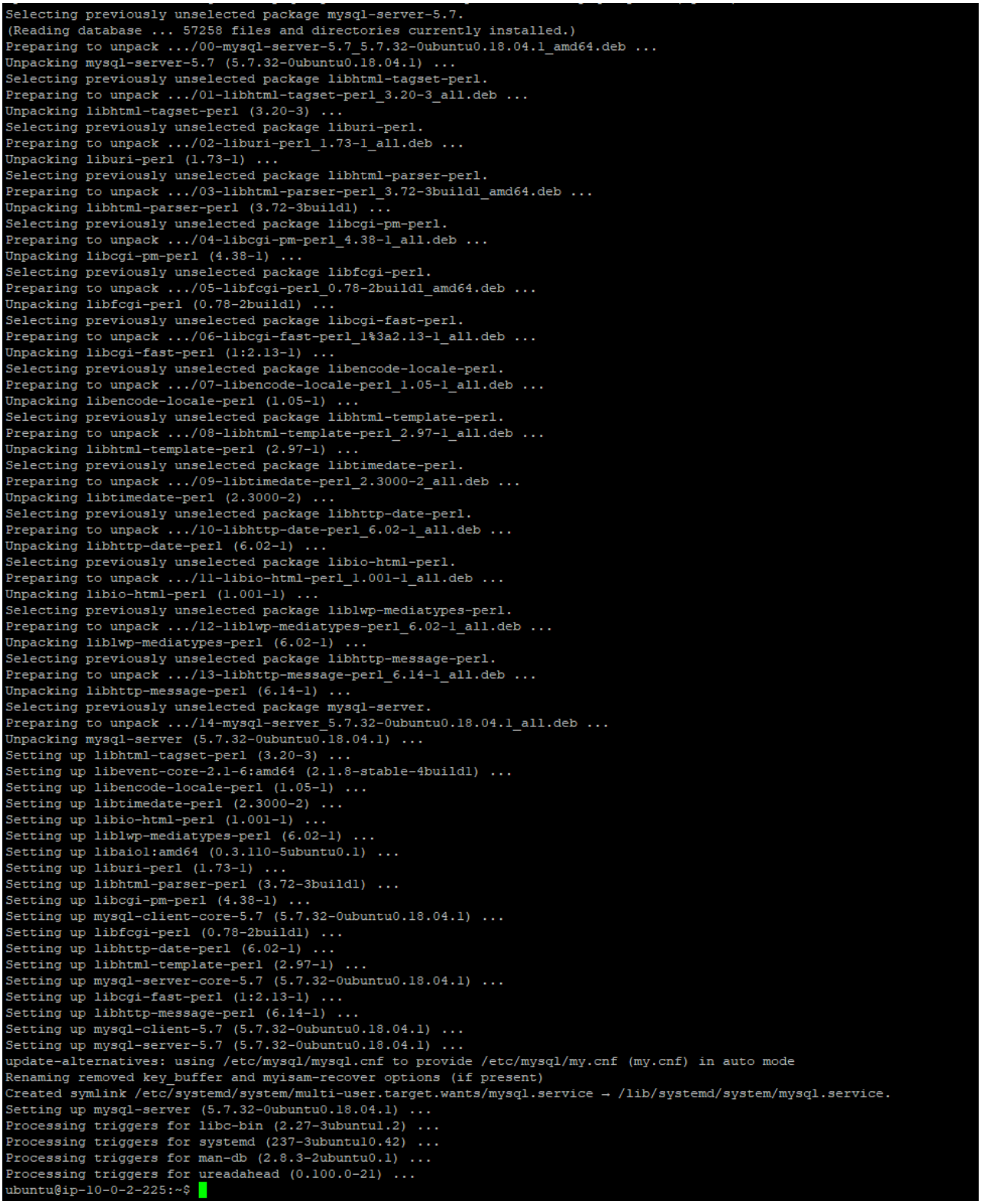
Screenshot 18:

Because the solution with the EC2 server as NAT instance did not work and I cannot install the MySQL server on the EC2 machine on private subnet (no connectivity to the internet), I create a NAT gateway instead and everything works fine.



Screenshot 19:

Update the entry on main route table which is assigned to private subnet in order to have the NAT gateway as target and not the NAT EC2 server instance.



Screenshot 20:

MySQL database installed on EC2 server with IP 10.0.2.225 on private subnet.

```
All done!
ubuntu@ip-10-0-2-225:~$
ubuntu@ip-10-0-2-225:~$
ubuntu@ip-10-0-2-225:~$ sudo mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.32-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

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> create user 'mmuser'@'%' identified by 'mmuser-password';
Query OK, 0 rows affected (0.00 sec)

mysql> create database mattermost;
Query OK, 1 row affected (0.00 sec)

mysql> grant all privileges on mattermost.* to 'mmuser'@'%';
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
ubuntu@ip-10-0-2-225:~$
```

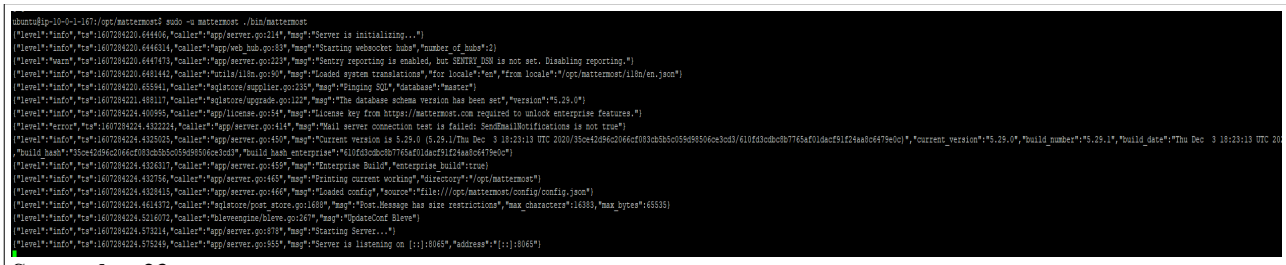
Screenshot 21:
Create user to MySql database on private subnet

```
ubuntu@ip-10-0-1-167: ~
login as: ubuntu
Authenticating with public key "imported-openssh-key"
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Dec  6 19:04:41 UTC 2020

  System load:  0.08              Processes:           90
  Usage of /:   14.6% of 7.69GB   Users logged in:     0
  Memory usage: 17%               IP address for eth0: 10.0.1.167
  Swap usage:   0%

0 packages can be updated.
0 updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-1-167:~$
ubuntu@ip-10-0-1-167:~$
ubuntu@ip-10-0-1-167:~$
```

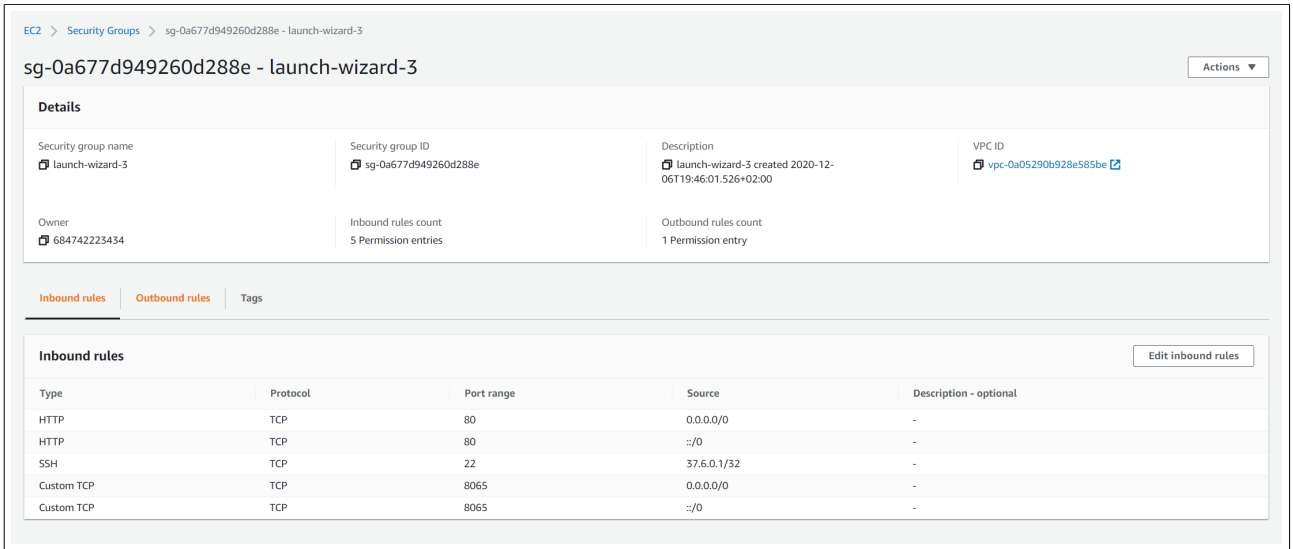
Screenshot 21:
Connect to Mattermost EC2 instance on public subnet (IP 10.0.1.167) using Putty.

```
},
"SqlSettings": {
    "DriverName": "mysql",
    "DataSource": "mmuser:mmuser-password@tcp(10.0.2.225:3306)/mattermost?charset=utf8mb4,utf8\u0026readTimeout=30s\u0026writeTimeout=30s",
    "DataSourceReplicas": [],
    "DataSourceSearchReplicas": [],
    "MaxIdleConns": 20,
    "ConnMaxLifetimeMilliseconds": 3600000,
    "MaxOpenConns": 300,
    "Trace": false,
    "AtRestEncryptKey": "krwi67tbqwgwg8jkfcj3d5hipt6w7jxf",
    "QueryTimeout": 30,
    "DisableDatabaseSearch": false
},
"LogSettings": {
    "EnableConsole": true,
    "ConsoleLevel": "INFO",
```

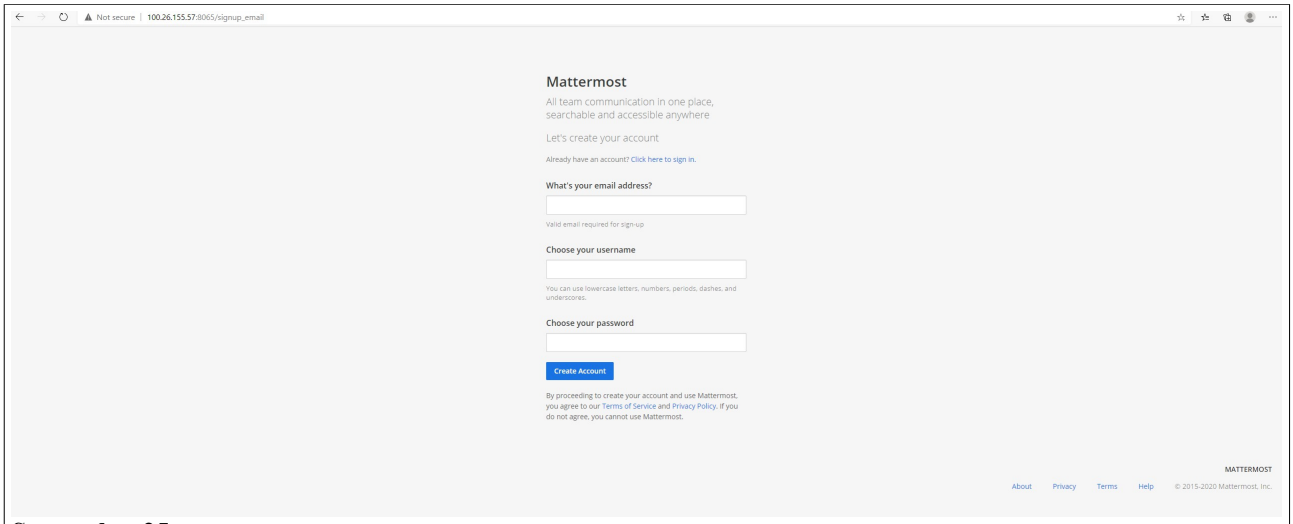

Screenshot 22:
Configure MySQL connection properties on "/opt/mattermost/config/config.json" file on Mattermost EC2 instance.



Screenshot 23:
By running "sudo -u mattermost ./bin/mattermost" command on Mattermost EC2 instance, Mattermost application runs without any problems and the server is listening on port 8065.



Screenshot 24:
Add an inbound roule on Mattermost EC2 instance in order to receive TCP traffic from the internet on port 8065.



Screenshot 25:
Use a broswer to run "100.26.155.57:8065". This is the public IP of Mattermost EC2 instance. Mattermost application works as expected.