

## Question 1

Step 1 :

Create an EC2 instance and choose AMazon Linux AML.

Step 2 :

Choose instance type t2 micro

Step 3 :

In the configure instance detail tab enable the auto assign public IP and add the following code in the Advance Detail user data body

```
#!/bin/bash
yum update -y
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
yum install -y httpd mariadb-server
systemctl start httpd
systemctl enable httpd
usermod -a -G apache ec2-user
chown -R ec2-user:apache /var/www
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} \;
find /var/www -type f -exec chmod 0664 {} \;
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

Step 4 :

Add storage and tags as per the need.

Step 5 :

Configure the security group for the instance by allowing HTTP port to the instance.

Step 6 :

Review and launch the instance.

Step 7 :

Connect to your instance with following command

ssh -i "ketavbhatt-PE.pem" [ec2-user@ec2-3-87-219-152.compute-1.amazonaws.com](https://ec2-user@ec2-3-87-219-152.compute-1.amazonaws.com)

Step 8 :

Command 'sudo service httpd start' is to start the apache server.

Step 9 :

Add index .html in html folder

```
cd /var/www/html
```

```
nano index.html
```

Hence we have added an index.html file in our EC2 instance.

Step 10 :

Attach Auto scaling group to the instance.

Create a new Auto Scaling Group by giving name to it.

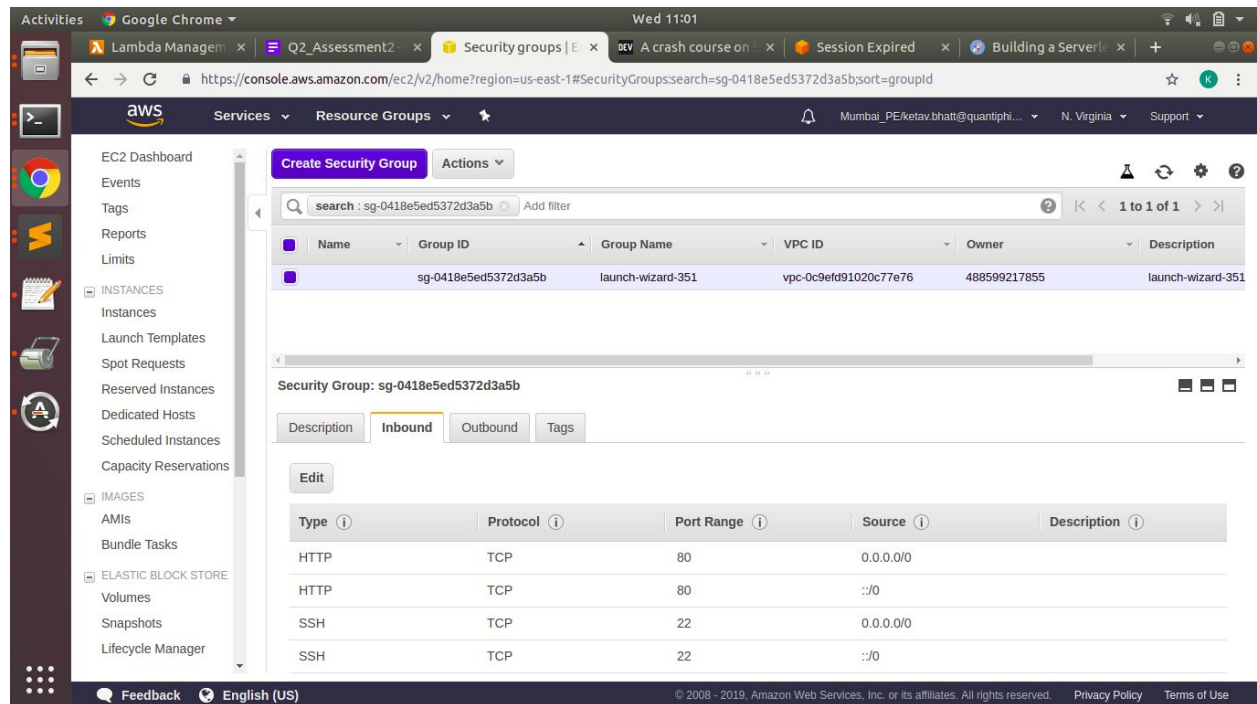
Step 11 :

Create a new Load Balancer and a new target group.

Step 12 :

Now add target to your Auto scaling group which is already connected to your instance.

## Security Group Rules:



The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for various AWS services. The main content area displays the 'Security Groups' page. A table lists the security groups, with 'sg-0418e5ed5372d3a5b' selected. Below the table, the 'Inbound' rules tab is active, showing a table of rules for HTTP and SSH traffic.

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	::/0	
SSH	TCP	22	0.0.0.0/0	
SSH	TCP	22	::/0	

## Listener Configuration :

The screenshot displays the AWS Management Console interface for configuring a Load Balancer. The left sidebar shows the navigation menu with categories like AMIs, ELASTIC BLOCK STORE, NETWORK & SECURITY, and LOAD BALANCING. The 'Load Balancers' option is selected under the 'LOAD BALANCING' category.

The main content area shows the 'ketav' Load Balancer details. The 'Listeners' tab is active, displaying a table of listener configurations. The table has columns for Listener ID, Security policy, SSL Certificate, and Rules. A single listener is listed with ID 'arn...e4065a4b1cec54c5', Security policy 'N/A', SSL Certificate 'N/A', and Rules 'Default: forwarding to ketav2'. A 'View/edit rules' link is provided for the listener.

Below the table, there is a section for 'Add listener' with buttons for 'Add listener', 'Edit', and 'Delete'. The 'Add listener' button is highlighted.

The bottom of the console shows the footer with 'Feedback', 'English (US)', and copyright information: '© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use'.

Listener ID	Security policy	SSL Certificate	Rules
arn...e4065a4b1cec54c5	N/A	N/A	Default: forwarding to ketav2 <a href="#">View/edit rules</a>