

Karthik Pradeep Hegadi

2KE20CS032

Assignment 41

Understood. To follow the provided instructions and create the files/directory using the same name and case as provided in the task steps, please provide me with the specific names and case instructions for the files/directory you want to create.

AWS

Assignment:8 Load_Configure Application Load Balancer

Create Application Load Balancer

1. Navigate to EC2 Load Balancer and click on Create Load Balancer
2. In the Load Balancer type choose Application Load Balancer and click on Create option
3. Provide the load balancer name, select Internet-facing, and IPv4 address type
4. In the network mapping select your VPC
5. In the subnet mapping select the availability zones and select public subnets that you have created from the dropdown

The screenshot shows the AWS EC2 Load Balancer creation process. In the 'Basic configuration' step, a new load balancer is being created with the name 'mattermost_LB-01'. It is set to 'Internet-facing' with 'IPv4' selected as the IP address type. In the 'Network mapping' step, a VPC named 'my-vpc-01' is selected, and two subnets are mapped: 'subnet-0f3a2030b8047392a' (my-public-subnet-1) and 'subnet-0cd9caa8bc0c4598b' (my-public-subnet-2), both assigned by AWS.

6. In the Security groups, click on create new security group and create as inbound and outbound rules as below

The screenshot shows the AWS Security Groups creation process. A new security group named 'SG_mattermost_LB-01' is being created. The 'VPC' dropdown is set to 'vpc-0e190ca43b317839f (my-vpc-01)'. The 'Inbound' tab shows a single rule allowing traffic from port 80 to 80 on the local host.

7. Once you create, select the security group and map it

INBOUND

Inbound rules [Info](#)

Type	Protocol	Port range	Source	Destination
All ICMP - IPv4	ICMP	All	Anywhere-IPv4	0.0.0.0/0
HTTP	TCP	80	Anywhere-IPv4	0.0.0.0/0
HTTPS	TCP	443	Anywhere-IPv4	0.0.0.0/0

Add rule

OUTBOUND

Outbound rules [Info](#)

Type	Protocol	Port range	Source	Destination
All traffic	All	All	Custom	0.0.0.0/0
All ICMP - IPv4	ICMP	All	Anywhere-IPv4	0.0.0.0/0
HTTP	TCP	80	Anywhere-IPv4	0.0.0.0/0
HTTPS	TCP	443	Anywhere-IPv4	0.0.0.0/0

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

Security groups

Select up to 5 security groups

SG_mattermost_LB-01 [X](#)
sg-0d9085f82835e6578 VPC: vpc-0e190ca43b317839f

Target group name

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

HTTP	80
------	----

1-65535

IP address type

8. In the Listeners and Routing, click on Create target group, select your VPC provide target group name from the list. Other options can be default.
9. In the Advanced health check settings you can give your custom values in the traffic port. (you can leave as default if you don't wish to change it)
10. Click on 'Next' option and in the List of Registered Instances select your public instances where your nginx server runs , click 'include as pending now' option and then Create the Target Group

Available instances (2/6)

<input type="checkbox"/>	Instance ID	Name	State	Security groups
<input checked="" type="checkbox"/>	i-05a4e1f88e7ed4668	public-inst(a)nginx-2	Running	launch-wizard-34
<input type="checkbox"/>	i-0afa5896198d39468	private-inst(a)appserver-2	Running	launch-wizard-41
<input type="checkbox"/>	i-0ec2b95123cb3bc84	openvpn-server-01	Running	OpenVPN Access Server
<input checked="" type="checkbox"/>	i-059f3bb15a76aad7d	public-inst(a)nginx-1	Running	launch-wizard-29
<input type="checkbox"/>	i-0e7568659b5b24589	private-inst(a)appserver-1	Running	launch-wizard-31
<input type="checkbox"/>	i-0a6d610ce310ab3bf	private-inst(a)dbserver	Running	launch-wizard-30

The screenshot shows the 'Targets' tab in the CloudWatch Metrics interface. It displays a table of registered targets with the following details:

Instance ID	Name	Port	Zone	Health status	Health status details	Anomaly detection
i-059f3bb15a76aad7d	public-instanc...	80	ap-south-1a	Unused	Target group is not co...	Normal
i-05a4e1f88e7ed4668	public-instanc...	80	ap-south-1b	Unused	Target group is not co...	Normal

At the top right, there are buttons for 'Anomaly mitigation: Not applicable' (with a help icon), 'Deregister', and 'Register targets'. Below the table is a footer with copyright information and links to 'Privacy', 'Terms', and 'Cookie preferences'.

The screenshot shows the 'Listeners and routing' section of the Load Balancer configuration. It displays a listener named 'HTTP:80' with the following settings:

- Protocol:** HTTP
- Port:** 80
- Default action:** Forward to target group 'tgLBmatter' (Target type: Instance, IPv4)
- Create target group** button

Below the listener configuration, there is a section for 'Listener tags - optional' with a 'Add listener tag' button and a note that you can add up to 50 more tags.

11. Map the Target group in the Load balancer configuration
12. Now click on Create Load Balancer and it should now be created successfully
13. Navigate to Listeners tab in the Load balancer click in the Target group, select your target
14. Navigate to target group and you can see the the details of the targets
15. You can launch the Load Balancer using the DNS name as marked below
16. Once you access the Load balancer DNS name the web server page should be displayed on the basis of round robin schedule which is been

Dashboard

▼ Details

Load balancer type Application	Status ⌚ Provisioning	VPC vpc-0e190ca43b317839f	IP address type IPv4
Scheme Internet-facing	Hosted zone ZP97RAFLXTNZK	Availability Zones subnet-0f3a2030b8047392a ap-south-1a (aps1-az1) subnet-0cd9caa8bc0c4598b ap-south-1b (aps1-az3)	Date created November 28, 2023, 23:06 (UTC+05:30)
Load balancer ARN arn:aws:elasticloadbalancing:ap-south-1:405819896469:loadbalancer/app/mattermostLB01/cabee551d6de1c7f	DNS name Info mattermostLB01-264641899.ap-south-1.elb.amazonaws.com (A Record)		

Listeners and rules [Listeners and rules \(1\) Info](#)

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

<input type="checkbox"/> Protocol:Port	<input type="checkbox"/> Default action	<input type="checkbox"/> Rules	<input type="checkbox"/> ARN	<input type="checkbox"/> Security policy	<input type="checkbox"/> Default SSL/TLS certificate
<input type="checkbox"/> HTTP:80	Forward to target group <ul style="list-style-type: none">tgLBmatter: 1 (100%)Group-level stickiness: Off	1 rule	ARN	Not applicable	Not applicable

© 2023, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Health checkup

[EC2](#) > Target groups

Target groups (1/1) [Info](#)

<input checked="" type="checkbox"/>	Name	ARN	Port	Protocol	Target type
<input checked="" type="checkbox"/>	tgLBmatter	arn:aws:elasticloadbalanci...	80	HTTP	Instance

Target group: tgLBmatter

Details

[arn:aws:elasticloadbalancing:ap-south-1:405819896469:targetgroup/tgLBmatter/7fb92735ced08489](#)

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1
IP address type IPv4	Load balancer None associated	
2 Total targets	健康的 2	不健康 0
		Unused

tgLBmatter

Details all are off

arn:aws:elasticloadbalancing:ap-south-1:405819896469:targetgroup/tgLBMatter/7fb92735ced08489

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-0e190ca43b317839f		
IP address type IPv4	Load balancer mattermostLB01				
2 Total targets	0 Healthy	0 Unhealthy	2 Unused		
			0 Initial		
			0 Draining		
0 Anomalous					

► **Distribution of targets by Availability Zone (AZ)**
Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets **Monitoring** **Health checks** **Attributes** **Tags**

tgLBmatter

Details

arn:aws:elasticloadbalancing:ap-south-1:405819896469:targetgroup/tgLBMatter/7fb92735ced08489

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-0e190ca43b317839f		
IP address type IPv4	Load balancer mattermostLB01				
2 Total targets	1 Healthy	0 Unhealthy	1 Unused		
			0 Initial		
			0 Draining		
0 Anomalous					

► **Distribution of targets by Availability Zone (AZ)**
Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets **Monitoring** **Health checks** **Attributes** **Tags**

tgLBmatter

Details

arn:aws:elasticloadbalancing:ap-south-1:405819896469:targetgroup/tgLBMatter/7fb92735ced08489

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-0e190ca43b317839f		
IP address type IPv4	Load balancer mattermostLB01				
2 Total targets	0 Healthy	1 Unhealthy	1 Unused		
			0 Initial		
			0 Draining		
0 Anomalous					

► **Distribution of targets by Availability Zone (AZ)**
Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets **Monitoring** **Health checks** **Attributes** **Tags**

Registered targets (2) [Info](#)

[Anomaly mitigation: Not applicable](#) [C](#) [Deregister](#) [Register targets](#)

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings.

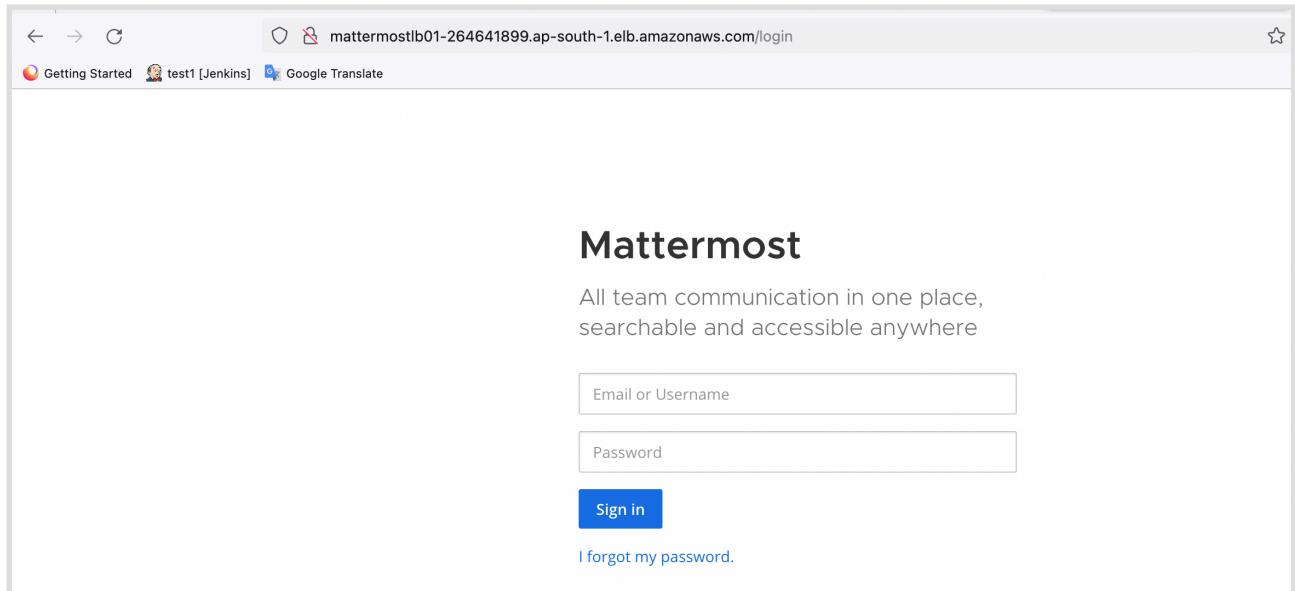
Results. All HTTP/HTTPS target groups now include anomaly detection by default. [Learn more](#)

tgLBMatter

Actions ▾

Details	
arn:aws:elasticloadbalancing:ap-south-1:405819896469:targetgroup/tgLBMatter/7fb92735ced08489	
Target type Instance	Protocol : Port HTTP: 80
IP address type IPv4	Protocol version HTTP1
VPC vpc-0e190ca43b317839f	
2 Total targets	○ 2 Healthy
	✖ 0 Unhealthy
	○ 0 Unused
	⌚ 0 Initial
	○ 0 Draining
Distribution of targets by Availability Zone (AZ) Select values in this table to see corresponding filters applied to the Registered targets table below.	

Verified: Yes it is coming in round-robin fashion



The screenshot shows a web browser window with the URL mattermostlb01-264641899.ap-south-1.elb.amazonaws.com/login. The page title is "Mattermost". The subtext reads "All team communication in one place, searchable and accessible anywhere". There are two input fields: "Email or Username" and "Password", followed by a blue "Sign in" button. Below the button is a link "I forgot my password."

Assignment:9 Load_Configure Network Load Balancer

Create Network Load Balancer and configure the DNS in your web server

1. Navigate to EC2 Load Balancer and click on Create Load Balancer
2. In the Load Balancer type choose Network Load Balancer and click on Create option
3. Provide the load balancer name, select Internal-facing, and IPv4 address type
4. In the network mapping select your VPC
5. In the subnet mapping select the availability zones and select the private subnets where you run the two mattermost instance

Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC
Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

my-vpc-01
vpc-0e190ca43b317839f
IPv4: 10.0.0.0/16

Mappings
Select at least one Availability Zone and one subnet for each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic only to targets in the selected Availability Zones. Zones that are not supported by the load balancer or VPC can't be selected. Subnets can be added, but not removed, once a load balancer is created.

ap-south-1a (aps1-az1)
Subnet
subnet-0691fa12817842c2d private_01

IPv4 address
Assigned by AWS

⚠ The selected subnet does not have a route to an internet gateway. This means that your load balancer will not receive internet traffic.
You can proceed with this selection; however, for internet traffic to reach your load balancer, you must update the subnet's route table in the [VPC console](#).

6. In the Listeners and Routing provide the TCP port 8065 , click on Create target group and select your VPC from the list, provide the target group name other options can be default.

Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener **TCP:8065** [Remove](#)

Protocol	Port	Default action
TCP	8065 1-65535	Forward to Select a target group ✖ Create target group

Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)
You can add up to 50 more tags.

[Add listener](#)

Target group name
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol : Port
Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

Protocol	Port
TCP	80 1-65535

IP address type
Only targets with the indicated IP address type can be registered to this target group.

7. In the Advanced health check settings you can give your custom values in the traffic port. (you can leave as default if you don't wish to change it)
8. Click on 'Next' option and in the List of Registered Instances select your private instances where you are running the mattermost

Available instances (2/5)				
	Instance ID	Name	State	Security g
<input type="checkbox"/>	i-05a4e1f88e7ed4668	public-inst(anginx)-2	Running	launch-wiz
<input checked="" type="checkbox"/>	i-0afa5896198d39468	private-inst(aappserver)-2	Running	launch-wiz
<input type="checkbox"/>	Instance private-inst(aappserver)-2	public-inst(anginx)-1	Running	launch-wiz
<input checked="" type="checkbox"/>	i-0e7568659b5b24589	private-inst(aappserver)-1	Running	launch-wiz
<input type="checkbox"/>	i-0a6d610ce310ab3bf	private-inst(dbserver)	Running	launch-wiz

9. Change the port number to 8065 and 'click include as pending below' and then create the target group.

public-inst(anginx)-1	Running	launch-wizard-29	ap-south-1
private-inst(aappserver)-1	Running	launch-wizard-31	ap-south-1
private-inst(dbserver)	Running	launch-wizard-30	ap-south-1

2 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.

G

1-65535 (separate multiple ports with commas)

Include as pending below

10. Map the Target group in the Load balancer configuration

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener **TCP:8065** Remove

Protocol	Port	Default action Info
TCP	: 8065	Forward to NBLmattermost Target type: Instance, IPv4
TCP Edit		

[Create target group](#)

Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)

You can add up to 50 more tags.

11. Click on Create Load Balancer and it should now be created successfully

12. Navigate to target group and you can see the the details of the targets

[EC2](#) > [Load balancers](#) > NLBsecuritygroup

NLBsecuritygroup [Edit](#) Actions ▾

Details	
Load balancer type Network	Status Active vpc-0e190ca43b317839f
Scheme Internet-facing	Hosted zone ZVDDRBQ08TROA Availability Zones subnet-0691fa12817842c2d ap-south-1a (aps1-a2) subnet-01e1b5812ebecfe9 ap-south-1b (aps1-az3)
Load balancer ARN arn:aws:elasticloadbalancing:ap-south-1:405819896469:loadbalancer/net/NLBsecuritygroup/f7d74fe03439000c	DNS name Info NLBsecuritygroup-f7d74fe03439000c.elb.ap-south-1.amazonaws.com (A Record)

[Listeners](#) [Network mapping](#) [Security](#) [Monitoring](#) [Integrations](#) [Attributes](#) [Tags](#)

Listeners (1) [Edit](#) Actions ▾ Add listener

A listener checks for connection requests using the protocol and port that you configure. Traffic received by a Network Load Balancer listener is forwarded to the selected target group.

<input type="checkbox"/> Protocol:Port	<input type="checkbox"/> Default action	<input type="checkbox"/> ARN	<input type="checkbox"/> Security policy	<input type="checkbox"/> Default SSL/TLS certificate	<input type="checkbox"/> ALPN policy	<input type="checkbox"/> Tags
<input type="checkbox"/> TCP:8065	Forward to target group • NLBtargetgroup	<input type="checkbox"/> ARN	Not applicable	Not applicable	None	0 tags

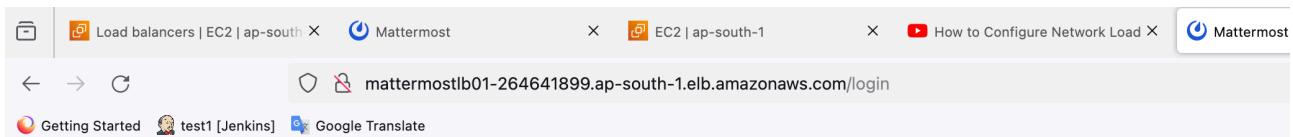
The screenshot shows the AWS CloudWatch Metrics Insights interface. A query is being run against CloudWatch Metrics data. The results are displayed in a table with columns for Metric Name, Metric Value, and Time. The table shows various metrics such as 'AWS/Lambda/FunctionStart' and 'AWS/Lambda/FunctionEnd' with their respective values and timestamp.

13.0 Open your web server Instance , navigate to /etc/nginx/conf.d/mattermost. Provide the DNS of your Network Load Balancer For both machine I have done

The screenshot shows the AWS Lambda function configuration interface. The 'Code' tab is selected, displaying the Lambda function's code in JSON format. The code defines a function named 'lambda_handler' that takes a 'event' parameter and returns a response. It uses the 'aws_lambda_powertools' library for logging and metrics. The function is triggered by an S3 event, specifically for new objects in a bucket named 'mattermost-backup'.

14. Now try to access your mattermost using the DNS of Application Load balancer

15. Now check the load balancing works by stopping the service / instance and also make a check on the Target health



After launching DNS

Mattermost

All team communication in one place,
searchable and accessible anywhere

[Sign in](#)

[I forgot my password.](#)