

# Practical 3

**Name:** Ishaan Bose

**Reg. no.:** 2147116

## **1. Describe Load Balancing and its significance in Cloud Environment.**

Cloud load balancing is defined as the method of splitting workloads and computing properties in a cloud computing. It enables enterprise to manage workload demands or application demands by distributing resources among numerous computers, networks or servers. Cloud load balancing includes holding the circulation of workload traffic and demands that exist over the Internet. Cloud load balancing helps enterprises achieve high performance levels for potentially lower costs than traditional on-premises load balancing technology. Cloud load balancing takes advantage of the cloud's scalability and agility to meet the demands of distributed workloads with high numbers of client connections. It also improves overall availability, increases throughput and reduces latency.

Cloud load balancing takes a software-based approach to distributing network traffic across resources, as opposed to hardware-based load balancing, which is more common in enterprise data centres. A load balancer receives incoming traffic and routes those requests to active targets based on a configured policy. A load balancing service also monitors the health of the individual targets to ensure that those resources are fully operational.

## **2. List the Load Balancing Service available in AWS, Azure and GCP.**

- Amazon Web Services (AWS) **Elastic Load Balancing** distributes incoming client traffic and routes it to registered targets such as EC2 instances. Elastic Load balancing supports four types of load balancers: Application, Network, Gateway and Classic. The load balancers differ in the features offered, the network layers at which they operate and supported communication protocols.
- **Google Cloud Load Balancer** (GCLB) service available on Google Cloud Platform is built on the same front-end server infrastructure that powers Google. The service offers a range of load balancers that vary depending on whether the customer needs external or internal load balancing, global or regional load balancing, Premium or Standard network service tiers, proxy or pass-through services, among other factors.
- Microsoft Azure offers four load balancing services. **Azure Traffic Manager** is a (OSI model) layer 7 DNS-based traffic load balancer for delivering services across global Azure regions. **Azure Load Balancer** is a layer 4 network load balancer for routing traffic between VMs. **Azure Application Gateway** is a layer 7 delivery controller for regional applications. **Azure Front Door** is a highly secure, layer 7 global load balancer for microservice.

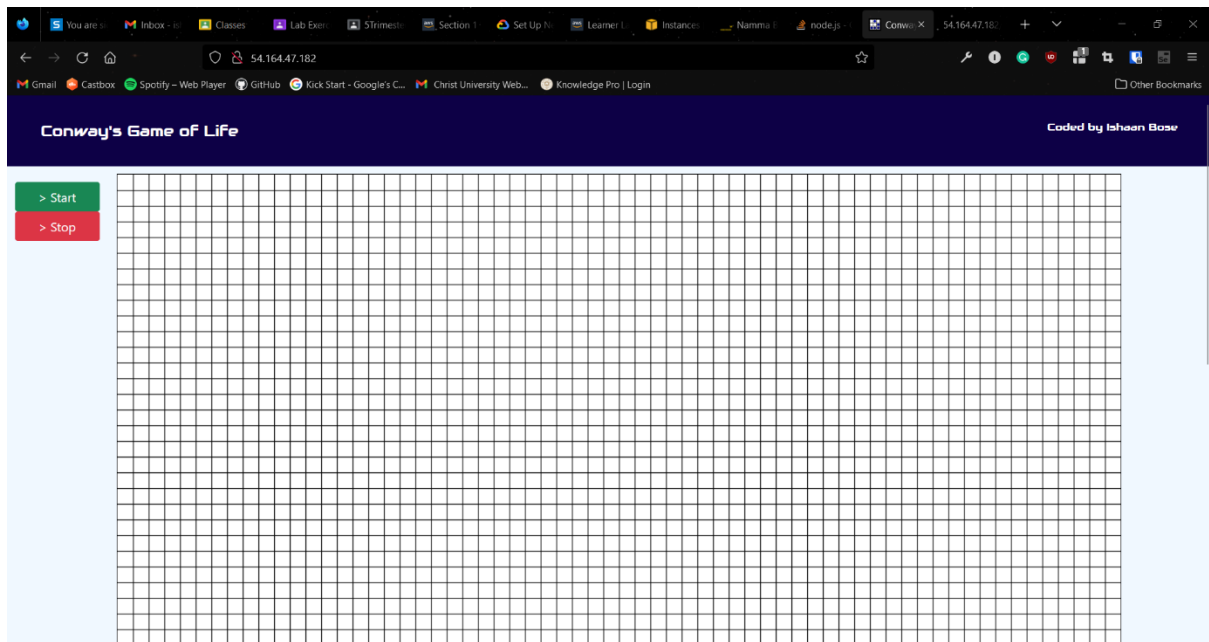
## **3. Create 2 Identical AWS EC2 / GCP VM Instances (Instance Name: Regno\_EC2\_VM1, Regno\_EC2\_VM2) and install a webserver of your choice in each of the instances to host web site of your organization globally.**

1. Create a second ec2 instance with the name 2147116\_EC2\_VM2.

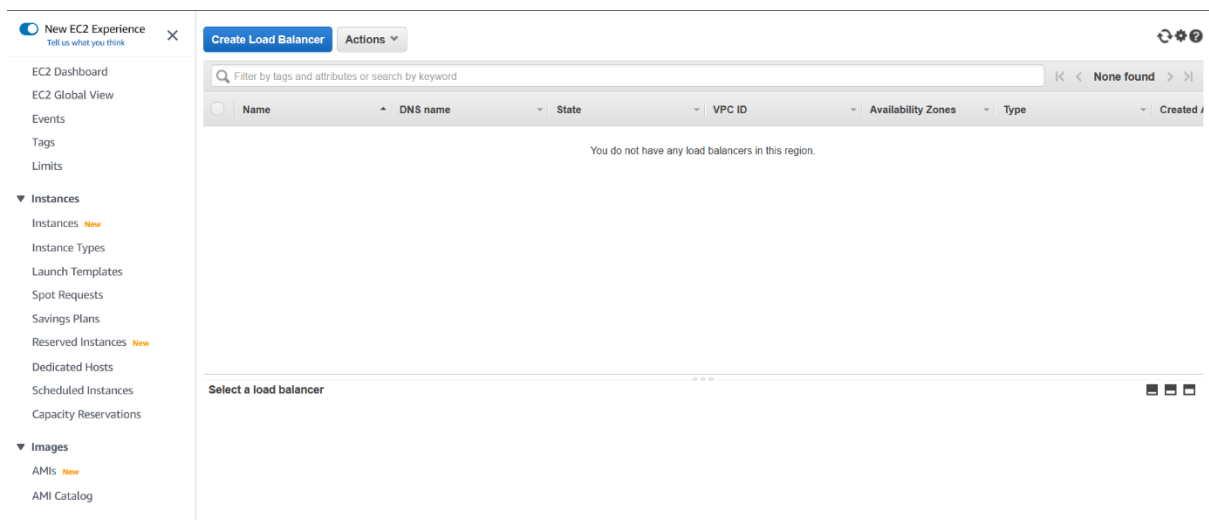
2. Select pre-existing key pair login and security group

3. Finally, click on Launch Instances.
4. Go to all instances and install a web server on new instance.

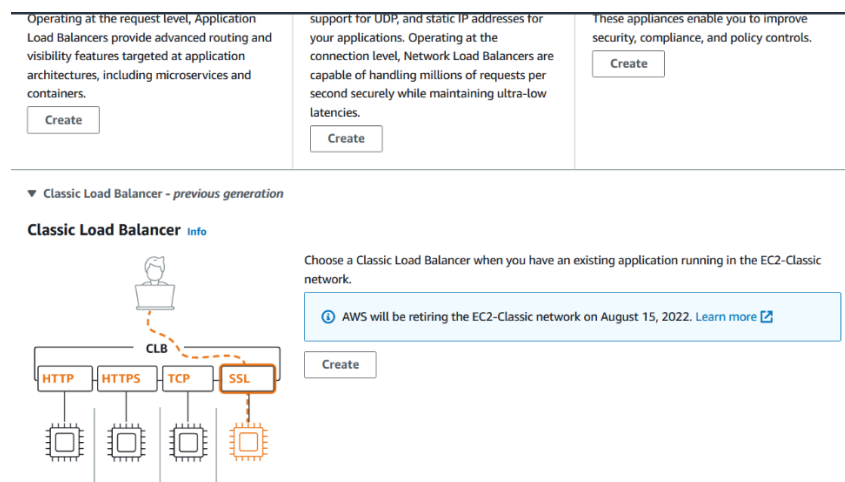
5. View website running on new instance.



6. Go to Load Balancer navigation menu and click on Create Load Balancer.



7. Scroll down to Classic Load Balancer and click create.



8. Fill in the details as follows:

1. Define Load Balancer2. Assign Security Groups3. Configure Security Settings4. Configure Health Check5. Add EC2 Instances6. Add Tags7. Review

Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name:

load-balancer

Create LB Inside:

My Default VPC (172.31.0.0/16)

Create an internal load balancer:

☐ (what's this?)

Enable advanced VPC configuration:

☒

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80

Add

Select Subnets

You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availability Zone, please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

VPC vpc-03f2ca44c63d7e7bf (172.31.0.0/16)

Available subnets

CancelNext: Assign Security Groups

9. Select subnets as per your instances.

1. Define Load Balancer2. Assign Security Groups3. Configure Security Settings4. Configure Health Check5. Add EC2 Instances6. Add Tags7. Review

Step 1: Define Load Balancer

HTTP80HTTP80

Add

Select Subnets

You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availability Zone, please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

VPC vpc-03f2ca44c63d7e7bf (172.31.0.0/16)

Available subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
	us-east-1b	subnet-01d7fd0ae9e0a6f8b	172.31.32.0/20	
	us-east-1c	subnet-076f96cbc02f3efa0	172.31.0.0/20	
	us-east-1e	subnet-0d5ad28e52b24e552	172.31.48.0/20	
	us-east-1f	subnet-0371c511e023a483	172.31.64.0/20	

Selected subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
	us-east-1a	subnet-0f22ad219727da9cc	172.31.16.0/20	
	us-east-1d	subnet-0deac311baadb9944	172.31.80.0/20	

CancelNext: Assign Security Groups

10. Click on Next: Assign Security Groups

11. Select the existing security group assigned to the instances.

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

### Step 2: Assign Security Groups

You have selected the option of having your Elastic Load Balancer inside of a VPC, which allows you to assign security groups to your load balancer. Please select the security groups to assign to this load balancer. This can be changed at any time.

Assign a security group: ☐ Create a new security group ☒ Select an existing security group

Filter: VPC security groups

Security Group ID	Name	Description	Actions
<input type="radio"/> sg-0324bc33e31a87aae	default	default VPC security group	<a href="#">Copy to new</a>
<input checked="" type="radio"/> sg-008f78ee736996475	launch-wizard-1	launch-wizard-1 created 2022-10-27T04:23:05.590Z	<a href="#">Copy to new</a>

[Cancel](#) [Previous](#) [Next: Configure Security Settings](#)

12. Click on Next: Configure Security Settings

13. For this practical, we are not using a secure listener. Choose Next: Configure Health Check to continue to the next step.

14. Change ping path to "/" and click on Next: Add EC2 Instances

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

### Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.

Ping Protocol: HTTP  
Ping Port: 80  
Ping Path: /

**Advanced Details**

Response Timeout: 5 seconds  
Interval: 30 seconds  
Unhealthy threshold: 2  
Healthy threshold: 10

[Cancel](#) [Previous](#) [Next: Add EC2 Instances](#)

15. Add the instances you wish to load balance.


16. Click Next: Add Tags. This page is optional and can be skipped.

17. Click on Review and Create

18. Verify all details and click on Create.

19. After load balancer is created, click on close.

### Load Balancer Creation Status

 **Successfully created load balancer**  
 Load balancer [load-balancer](#) was successfully created.  
 Note: It may take a few minutes for your instances to become active in the new load balancer.

[Close](#)

20. Wait for instances to be in service.

Create Load Balancer

Actions

Filter by tags and attributes or search by keyword

1 to 1 of 1

DNS name	State	VPC ID	Availability Zones	Type	Created At	Monitoring
load-balancer-1416238878.u...		vpc-03f2ca44c63d7e7bf	us-east-1d, us-east-1a	classic	November 3, 2022 at 11:03:...	

load-balancer-1416238878

23 03 2022

Description

Instances

Health check

Listeners

Monitoring

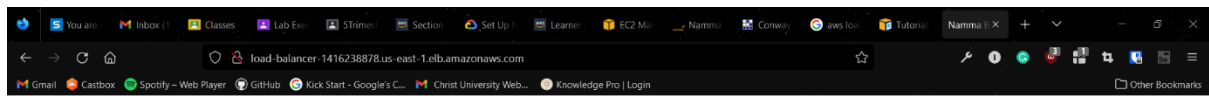
Tags

Migration

Basic Configuration

Name	load-balancer	Creation time	November 3, 2022 at 11:03:58 AM UTC+5:30
* DNS name	load-balancer-1416238878.us-east-1.elb.amazonaws.com (A Record)	Hosted zone	Z35SXDOTRQ7X7K
Type	Classic ( <a href="#">Migrate Now</a> )	Status	0 of 2 instances in service
Scheme	internet-facing	VPC	vpc-03f2ca44c63d7e7bf
Availability Zones	subnet-0deac311baadb9944 - us-east-1d, subnet-0f22ad219727da9cc - us-east-1a		

21. Once the instances are in service, copy the DNS name into address bar.
22. Refresh after a while to see both instances' websites being displayed.



# Namma Bengaluru

Explore the Silicon Valley of India

## Health-care

