

D Y Patil International University

School of Computer Science, Engineering, and Applications

Academic Year 2022-2023

Practical Assignment No. 1

Class: MCA-SEM III

Subject: Computer Forensics

Date 18 / 10 /2023

Name: - Udayan Mukund Pawar

PRN No.: - 20220804032

Experiments:

Aim:- Application Load Balancer

What is AWS?

AWS (Amazon Web Services) is a comprehensive, evolving cloud computing platform provided by Amazon that includes a mixture of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and packaged-software-as-a-service (SaaS) offerings. AWS services can offer an organization tools such as compute power, database storage and content delivery services.

Amazon.com Web Services launched its first web services in 2002 from the internal infrastructure that Amazon.com built to handle its online retail operations. In 2006, it began offering its defining IaaS services. AWS was one of the first companies to introduce a pay-as-you-go cloud computing model that scales to provide users with compute, storage or throughput as needed.

AWS offers many different tools and solutions for enterprises and software developers that can be used in data centers in up to 190 countries. Groups such as government agencies, education institutions, non-profits and private organizations can use AWS services.

What is Load Balancer:-

The elastic load balancer is a service provided by Amazon in which the incoming traffic is efficiently and automatically distributed across a group of backend servers in a manner that increases speed and performance. It helps to improve the scalability of your application and secures your applications. Load Balancer allows you to configure health checks for the registered targets. In case any of the registered targets (Autoscaling group) fails the health check, the load balancer will not route traffic to that unhealthy target. Thereby ensuring your application is highly

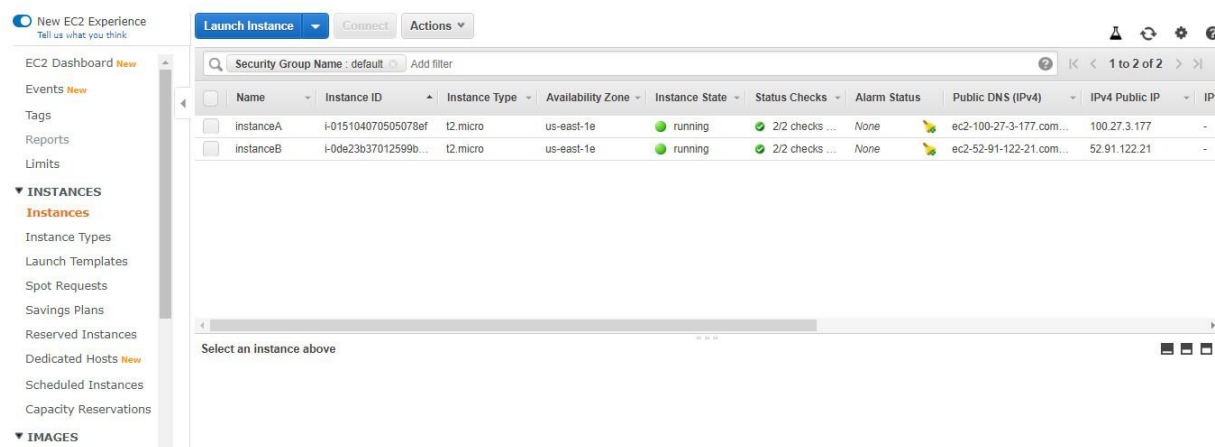
available and fault tolerant. To know more about load balancing refer to Load Balancing in Cloud Computing.

Types of Load Balancers

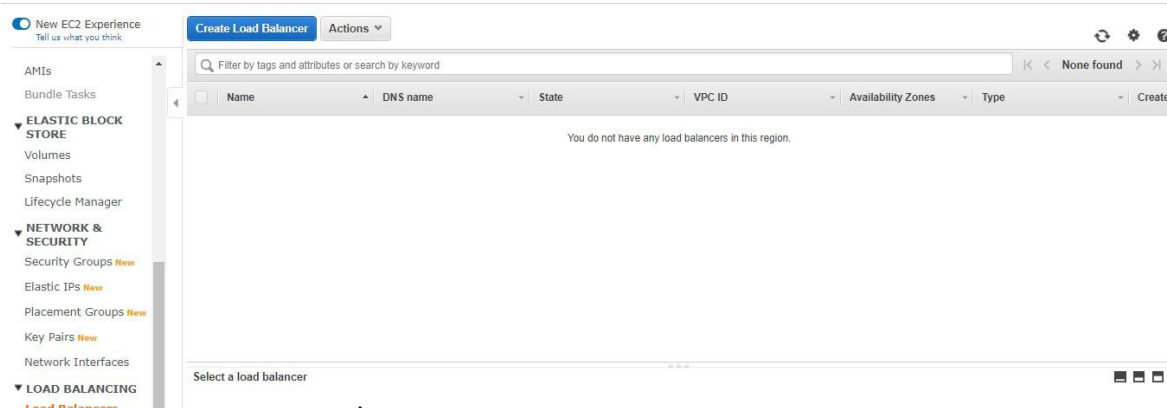
1. **Application Load Balancer:** This type of Load Balancer is used when decisions are to be made related to HTTP and HTTPS traffic routing. It supports path-based routing and host-based routing. This load balancer works at the Application layer of the OSI Model. The load balancer also supports dynamic host port mapping.
2. **Network Load Balancer:** This type of load balancer works at the transport layer(TCP/SSL) of the OSI model. It's capable of handling millions of requests per second. It is mainly used for load-balancing TCP traffic.
3. **Gateway Load Balancer:** Gateway Load Balancers provide you the facility to deploy, scale, and manage virtual appliances like firewalls. Gateway Load Balancers combine a transparent network gateway and then distribute the traffic.

Procedure:-

Step 1: Launch the two instances on the AWS management console named Instance A and Instance B. Go to services and select the load balancer. To create AWS free tier account refer to Amazon Web Services (AWS) – Free Tier Account Set up.



Step 2: Click on Create the load balancer.



Step 3: Select Application Load Balancer and click on Create.

Select load balancer type

Elastic Load Balancing supports three types of load balancers: Application Load Balancers, Network Load Balancers (new), and Classic Load Balancers. Choose the load balancer type that meets your needs. [Learn more about which load balancer is right for you](#)

Application Load Balancer

HTTP
HTTPS

Create

Choose an Application Load Balancer when you need a flexible feature set for your web applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

[Learn more >](#)

Network Load Balancer

TCP
TLS
UDP

Create

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your application. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

[Learn more >](#)

Classic Load Balancer

PREVIOUS GENERATION
for HTTP, HTTPS, and TCP

Create

Choose a Classic Load Balancer when you have an existing application running in the EC2-Classic network.

[Learn more >](#)

Step 4: Here you are required to configure the load balancer. Write the name of the load balancer. Choose the scheme as internet facing.

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives HTTP traffic on port 80.

Name ⓘ

Scheme ⓘ ☒ Internet-facing
☐ internal

IP address type ⓘ

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
<input type="text" value="HTTP"/>	<input type="text" value="80"/>
Add listener	

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

Step 5: Add at least 2 availability zones. Select us-east-1a and us-east-1b

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 1: Configure Load Balancer

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You must specify subnets from at least two Availability Zones to increase the availability of your load balancer.

VPC ⓘ

Availability Zones

☒ us-east-1a
IPv4 address ⓘ Assigned by AWS

☒ us-east-1b
IPv4 address ⓘ Assigned by AWS

☐ us-east-1c

☐ us-east-1d

☐ us-east-1e

☐ us-east-1f

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

Step 6: We don't need to do anything here. Click on Next: Configure Security Groups

1. Configure Load Balancer

2. Configure Security Settings

3. Configure Security Groups

4. Configure Routing

5. Register Targets

6. Review

Step 2: Configure Security Settings

⚠

Improve your load balancer's security. Your load balancer is not using any secure listener.
If your traffic to the load balancer needs to be secure, use the HTTPS protocol for your front-end connection. You can go back to the first step to add/configure secure listeners under [Basic Configuration](#) section. You can also continue with current settings.

Cancel

Previous

Next: Configure Security Groups

Step 7: Select the default security group. Click on Next: Configure Routing

1. Configure Load Balancer

2. Configure Security Settings

3. Configure Security Groups

4. Configure Routing

5. Register Targets

6. Review

Step 3: Configure Security Groups

A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one.

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="checkbox"/> sg-0bb0a9bc3e885adfb	AutoScaling-Security-Group-1	AutoScaling-Security-Group-1 (2020-06-15 12:00:39.275+05:30)	Copy to new
<input type="checkbox"/> sg-0b3772fb578b44ce	AutoScaling-Security-Group-2	AutoScaling-Security-Group-2 (2020-06-15 15:18:53.000+05:30)	Copy to new
<input checked="" type="checkbox"/> sg-103a4f3e	default	default VPC security group	Copy to new
<input type="checkbox"/> sg-0b13f451747da2fc2	launch-wizard-1	launch-wizard-1 created 2020-05-12T23:27:45.924+05:30	Copy to new
<input type="checkbox"/> sg-0458b504a37badf44	launch-wizard-10	launch-wizard-10 created 2020-06-13T14:15:46.319+05:30	Copy to new
<input type="checkbox"/> sg-0fd12e18e2b9c22d6	launch-wizard-11	launch-wizard-11 created 2020-06-15T11:38:34.722+05:30	Copy to new
<input type="checkbox"/> sg-04b735293b2ccb9a7	launch-wizard-12	launch-wizard-12 created 2020-06-15T15:10:02.695+05:30	Copy to new
<input type="checkbox"/> sg-0f3b470cd95160c71	launch-wizard-13	launch-wizard-13 created 2020-06-15T20:33:05.606+05:30	Copy to new
<input type="checkbox"/> sg-0d9a4600ea95453f	launch-wizard-2	launch-wizard-2 created 2020-05-13T05:34:24.807+05:30	Copy to new

Cancel

Previous

Next: Configure Routing

Step 8: Choose the name of the target group to be my target group. Click on Next: Register Targets.

1. Configure Load Balancer

2. Configure Security Settings

3. Configure Security Groups

4. Configure Routing

5. Register Targets

6. Review

Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.

Target group

Target group

ⓘ

New target group

Name

ⓘ

my-target-group

Target type

☒ Instance

☐ IP

☐ Lambda function

Protocol

ⓘ

HTTP

Port

ⓘ

80

Health checks

Protocol

ⓘ

HTTP

Path

ⓘ

/

Cancel

Previous

Next: Register Targets

Step 9: Choose instance A and instance B and click on Add to register. Click on Next: Review

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 5: Register Targets

Registered targets
To deregister instances, select one or more registered instances and then click Remove.

Remove

<input type="checkbox"/>	Instance	Name	Port	State	Security groups	Zone
<input type="checkbox"/>	i-015104070505078ef	instanceA	80	running	default	us-east-1e
<input type="checkbox"/>	i-0de23b37012599b85	instanceB	80	running	default	us-east-1e

Instances
To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered on port 80

Search Instances

<input type="checkbox"/>	Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-015104070505078ef	instanceA	running	default	us-east-1e	subnet-28f6cc16	172.31.48.0/20
<input checked="" type="checkbox"/>	i-0de23b37012599b85	instanceB	running	default	us-east-1e	subnet-28f6cc16	172.31.48.0/20

Cancel Previous Next: Review

Step 10: Review all the configurations and click on create

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 6: Review

Please review the load balancer details before continuing

▼ Load balancer Edit

Name my-loadbalancer
Scheme internet-facing
Listeners Port 80 - Protocol HTTP
IP address type ipv4
VPC vpc-c63330bc
Subnets subnet-07a25158, subnet-f6629590
Tags

▼ Security groups Edit

Security groups sg-103a4f3e

▼ Routing Edit

Target group New target group
Target group name my-target-group
Port 80
Target type instance
Protocol HTTP
Health check protocol HTTP
Path /
Health check port traffic port
Health threshold 5

Cancel Previous Create

Step 11: Congratulations!! You have successfully created a load balancer. Click on close.

Load Balancer Creation Status

✓ **Successfully created load balancer**
Load balancer my-loadbalancer was successfully created.
Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass the initial health checks.

Suggested next steps

- Discover other services that you can integrate with your load balancer. Visit the [Integrated services](#) tab within my-loadbalancer
- Consider using AWS Global Accelerator to further improve the availability and performance of your applications. [AWS Global Accelerator console](#)

Close

Result:- We have successfully created a load Balancer.