



Award of Completion

Kethireddy Yogesh

Has Successfully Completed

Star Cloud Computing

Star Authorized Delivery Partner

ADVANTAGE PRO

10th April 2023

Date

2023/ADV/12610

Certificate
Number



Authorized
Signatory

APPLICATION LOAD BALANCER IN LAWS

PROJECT SUPERVISOR : Ms.DHARANI

NAME OF THE STUDENT:KETHIREDDY YOGESH

REG NO: 40111510

Presentation Outline

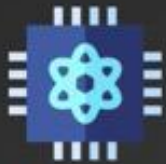
- Course Certificate
- Introduction
- Objectives
- System Architecture / Ideation Map
- Module Implementation
- Application Snapshots
- Results and Discussions
- Conclusion & Future work
- References

How to setup **Application Load Balancer** in **AWS**

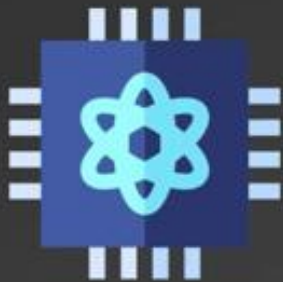


WHY LOAD BALANCER:

Vertical Scaling



t2.micro



C5.large



Horizontal Scaling



t2.micro



t2.micro

What is load balancer in aws:

- A load balancer serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability of your application.

Types of load balancers:

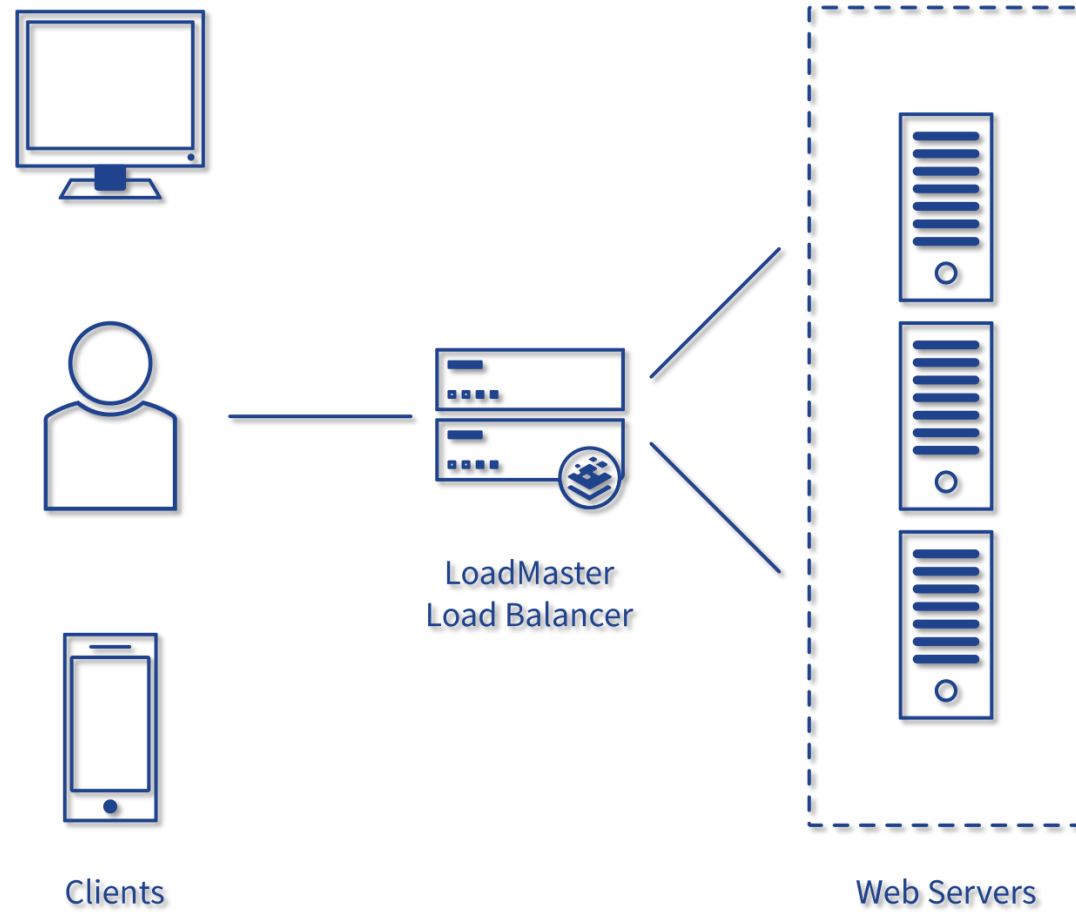
- Elastic Load Balancing supports the following types of load balancers: Application Load Balancers, and Network Load Balancers. Amazon ECS services can use these types of load balancer. Application Load Balancers are used to route HTTP/HTTPS (or Layer 7) traffic. Network Load Balancers and Classic Load Balancers are used to route TCP (or Layer 4) traffic.
- **Topics**
- APPLICATION LOAD BALANCER
- NETWORK LOAD BALANCER
- CLASSIC LOAD BALANCER

APPLICATION LOAD BALANCER:

- Application Load Balancer components
- A load balancer serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability of your application.

- An Layer 7 load balancer works at the application layer
- the highest layer in the OSI model
- makes its routing decisions based on more detailed information such as the characteristics of the HTTP/HTTPS header, message content, URL type, and cookie data.
- An application load balancer works at the request layer(Layer 7) of the OSI model.

DIAGRAMATIC REPRESSENTATION:



STEPS INVOLVED:

Step 1: Select a load balancer type.

Step 2: Define your load balancer.

Step 3: Assign security groups to your load balancer in a VPC.

Step 4: Configure health checks for your EC2 instances.

Step 5: Register EC2 instances with your load balancer.

Step 6: Tag your load balancer (optional)

Step 7:create any verify your load balancer

Step 8>Delete your load balancer

www.example.com



Amazon
Route 53



Application
Load Balancing

/ (default)

/stack-b



Stack A

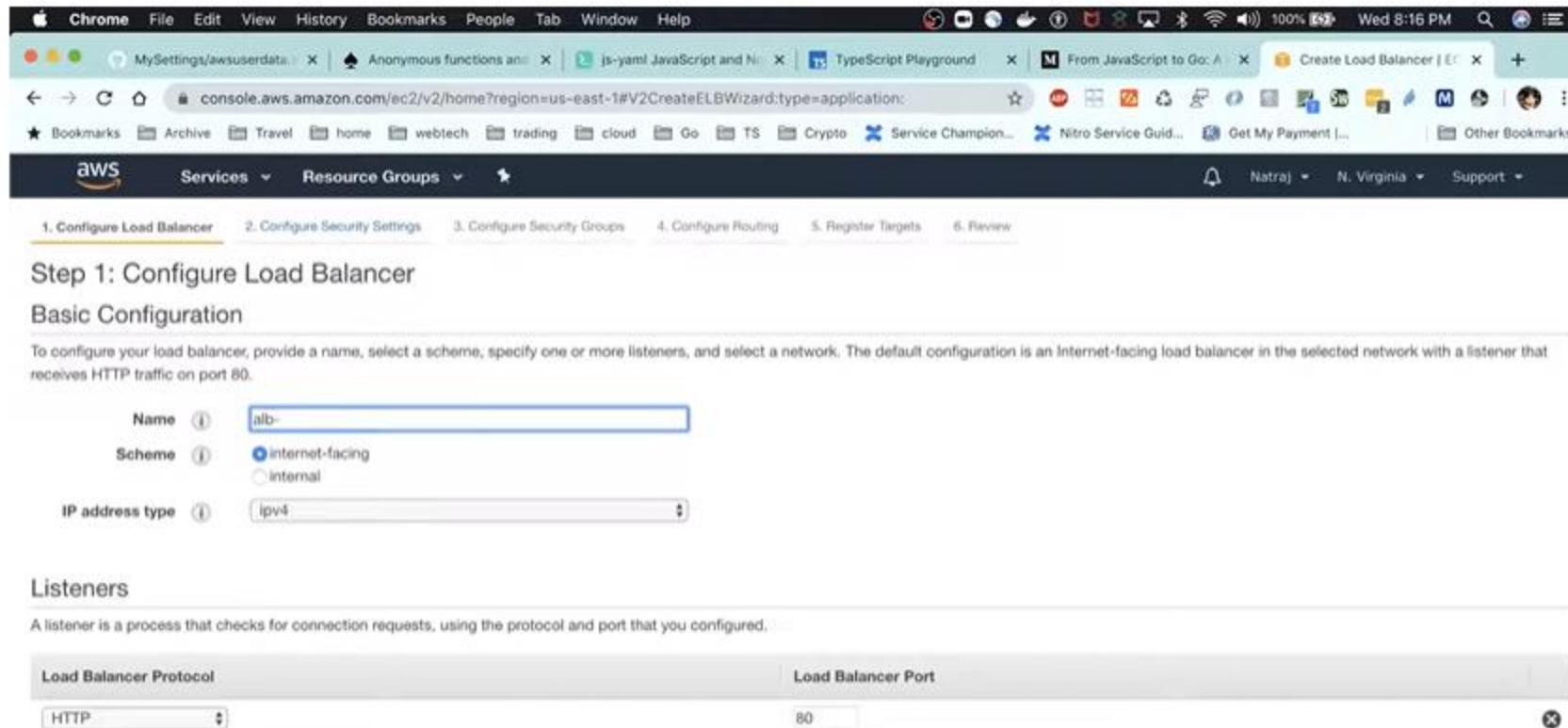


Stack B

APPLICATIONS OF APPLICATION LOAD BALANCER:

- **Improve Efficiency**
Load Balancers lessen the increased load on a server and maintain smooth operations and responses, providing a better experience for customers.
- **Predictive Analysis**
Traffic bottlenecks can be predicted by software load balancers before they occur in the real world.
- **Resilience**
With little or no downtime, the defective and under-performing components can be replaced promptly, providing information on which equipment needs service.
- **Security**
Load Balancer adds an extra layer of security to your website and applications without requiring any changes.
- **Scalability**
Load Balancers allow you to change the server infrastructure at any time without impacting services.

1.Configure load balancer:



Chrome File Edit View History Bookmarks People Tab Window Help

MySettings/awsuserdata... Anonymous functions and js-yaml JavaScript and No TypeScript Playground From JavaScript to Go: A Create Load Balancer | E

console.aws.amazon.com/ec2/v2/home?region=us-east-1#V2CreateELBWizard:type=application:

Bookmarks Archive Travel home webtech trading cloud Go TS Crypto Service Champion... Nitro Service Guid... Get My Payment |... Other Bookmarks

aws Services Resource Groups

Natraj N. Virginia Support

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

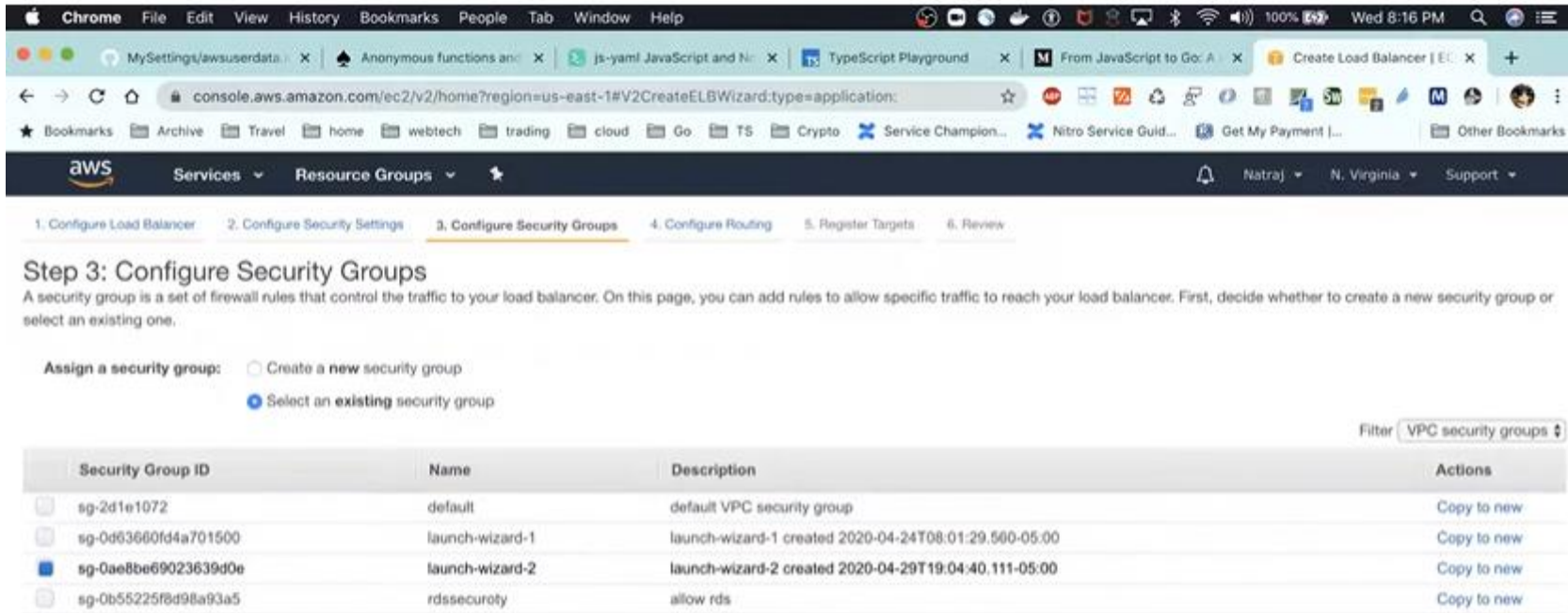
Listeners

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"/>

2.Configure security settings:

3.Configure Security Groups:



The screenshot shows the AWS Management Console interface for configuring a load balancer. The breadcrumb trail indicates the current step is '3. Configure Security Groups'. The page title is 'Step 3: Configure Security Groups'. Below the title, a paragraph explains that a security group is a set of firewall rules that control traffic to the load balancer. The 'Assign a security group' section has two radio buttons: 'Create a new security group' (unselected) and 'Select an existing security group' (selected). Below this, there is a table of existing VPC security groups. The table has four columns: 'Security Group ID', 'Name', 'Description', and 'Actions'. The table lists four security groups: 'sg-2d1e1072' (default), 'sg-0d63660fd4a701500' (launch-wizard-1), 'sg-0ae8be69023639d0e' (launch-wizard-2), and 'sg-0b55225f8d98af93a5' (rdssecurity). Each row has a 'Copy to new' link in the 'Actions' column.

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
sg-2d1e1072	default	default VPC security group	Copy to new
sg-0d63660fd4a701500	launch-wizard-1	launch-wizard-1 created 2020-04-24T08:01:29.560-05:00	Copy to new
sg-0ae8be69023639d0e	launch-wizard-2	launch-wizard-2 created 2020-04-29T19:04:40.111-05:00	Copy to new
sg-0b55225f8d98af93a5	rdssecurity	allow rds	Copy to new

4.Register settings:

The screenshot shows the AWS Management Console interface for the 'Create Load Balancer' wizard, specifically the 'Step 5: Register Targets' page. The browser is Chrome, and the URL is console.aws.amazon.com/ec2/v2/home?region=us-east-1#V2CreateELBWizard.type=application:. The page has a dark blue header with the AWS logo and navigation links. Below the header, a progress bar shows six steps: 1. Configure Load Balancer, 2. Configure Security Settings, 3. Configure Security Groups, 4. Configure Routing, 5. Register Targets (active), and 6. Review. The main content area is titled 'Step 5: Register Targets' and includes a brief description: 'Register targets with your target group. If you register a target in an Amazon Availability Zone, the load balancer directs routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.' Below this, there is a section for 'Registered targets' with a 'Remove' button and a table. The table has columns for Instance, Name, Port, State, Security groups, and Zone, but it is empty with the message 'No instances available.' Below the 'Registered targets' section is a section for 'Instances' with a description: '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.' This section includes an 'Add to registered' button and a text input field showing 'on port 80'. At the bottom, there is a search bar labeled 'Search Instances' and another table with columns for Instance, Name, State, Security groups, Zone, Subnet ID, and Subnet CIDR.

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

Step 5: Register Targets

Register targets with your target group. If you register a target in an Amazon Availability Zone, the load balancer directs routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets

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

Remove

Instance	Name	Port	State	Security groups	Zone
No instances available.					

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 X

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
----------	------	-------	-----------------	------	-----------	-------------

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

Step 5: Register Targets

Register targets with your target group. If you register a target in an Amazon Availability Zone, the Load Balancer automatically registers the target as soon as the registration process completes and the target passes the initial health checks.

Registered targets

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

Remove

Instance	Name	Port	State	Security groups	Zone
No instances available.					

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 X

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
----------	------	-------	-----------------	------	-----------	-------------

Review instances:

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, `launch-wizard-2`, is open to the world. Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

▼ AMI Details [Edit AMI](#)

amzn2-ami-hvm-2.0.20200406.0-x86_64-gp2 - ami-0323c3dd2da7fb37d
Amazon Linux 2 AMI 2.0.20200406.0 x86_64 HVM gp2
Root Device Type: ebs Virtualization type: hvm

▼ Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

▼ Security Groups [Edit security groups](#)

[Cancel](#) [Previous](#) [Launch](#)

Final output:

