

Assignment 4 – EC2 and ALB

Today's task:

1. Practice SGs using 2 public EC2 instances. There will be 2 SGs for each instance.
 - a. By enabling SSH rules in SG between them
 - b. Running applications
2. Run EC2 behind an ALB.

Bonus task: **NLB**

We will spin up NLBs only in 2 AZs. That means the load balancer can't distribute traffics to EC2s in other region. The reason is, the elastic IPs are precious and we can get up to 5 elastic IPs.

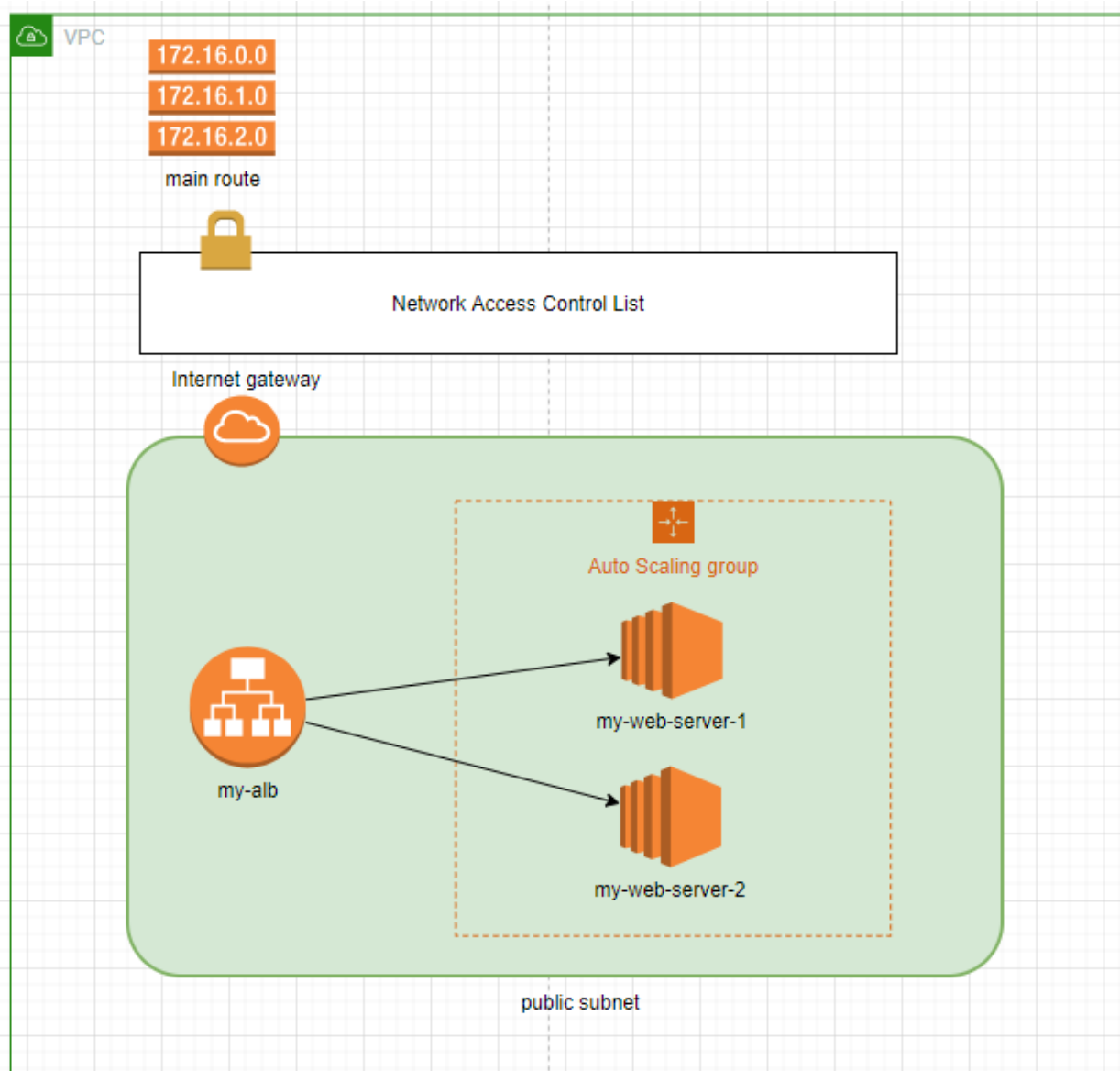
The logical component behind the elastic IP is that **Elastic Network Interface (ENI)**. We associate elastic IP with the ENI. All ENIs have the corresponding private IP associated with it. Network Load Balancer doesn't have any ENI that means there is no security group for Network Load Balancers. Basically, we are whitelisting the NLB using elastic ip with static private IPs.

1. Create 2 elastic IPs.
2. Create NLB and associate it with the elastic IPs.
3. Spin up 2 instances with different HTML content in us-east-1a, us-east-1b AZs.
4. Add the private instance in us-east-1a, us-east-1b to the target group of the NLB.
5. Update the target group and deselect **Preserve client IP addresses**

Grab private ip of the elastic ip in the AWS console, VPC, elastic ip section. Update the private instance's security group to allow **private IPs of the elastic IPs** that you created in the first step.

Submit items below in one pdf file:

1. Screenshot of app with your name
2. Submit ALB DNS
3. Screenshot of TG



Instruction 1. Create Security Groups

- Create a SG for the ALB which is open to the world.
- Create a SG for web servers that allows ALB's SG.

Create Application Load Balancer Security Group (Outbound Rule is Default - All Traffic)

Security group name my-lab-alb-sg	Security group ID sg-03e5e025e377518eb	Description Lab Application Load Balancer Security Group	VPC ID vpc-0b978358e22761686
Owner 409673912482	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules

Outbound rules

Tags

Inbound rules (1/1)						Manage tags	Edit inbound rules
Filter security group rules						< 1 >	
Type	Protocol	Port range	Source	Description			
HTTP	TCP	80	0.0.0.0/0	-			

Create EC2 Web Server Security Group (Outbound Rule is Default - All Traffic)

Security group name my-lab-EC2-Server-sg	Security group ID sg-0a370c15c5b405b61	Description Web Server Security Group	VPC ID vpc-0b978358e22761686
Owner 409673912482	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules

Outbound rules

Tags

Inbound rules (1/1)						Manage tags	Edit inbound rules
Filter security group rules						< 1 >	
Type	Protocol	Port range	Source	Description			
HTTP	TCP	80	sg-03e5e025e377518eb	-			

my-lab-alb-sg
Security Group

Instruction 2. Create 2 instances in public subnets

- Instance 1 prints instance 1 and Instance2 prints instance 2 so we can differentiate them.

EC2 Instance Startup Commands

```
#!/bin/bash
```

```

yum install httpd -y
cd /var/www/html
echo '<p>Instance 1</p>' > index.html
sudo service httpd start

```

#!/bin/bash --> tells the OS to invoke the specified shell to execute the script commands

Instruction 3. Create an ALB and attach instances

- Create the default http:80 listener.
- Select VPC and public subnets.
- Select the ALB's SG that you created in Task 1.
- Create a target group, type as Instance. Don't register targets for now.

Go to the Load Balancers Display from the EC2 Dashboard

The screenshot shows the AWS Management Console interface. On the left, the navigation menu is visible with categories like Snapshots, Lifecycle Manager, Network & Security, Load Balancing, and Auto Scaling. The 'Load Balancing' section is expanded, showing 'Load Balancers' and 'Target Groups'. A red arrow points from the 'Load Balancers' link to the 'Resources' section of the console. The 'Resources' section displays a table of EC2 resources in the US East (N. Virginia) Region. A red arrow points from the 'Load balancers' entry in the table to the 'Create Load Balancer' button on the 'Load Balancers' page. Below the table, a message states 'You do not have any load balancers in this region.'

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0
Key pairs	4	Load balancers	0
Placement groups	0	Security groups	7
Snapshots	0	Volumes	0

1) Click on Load Balancers

2) Click on Create Load Balancer

... **Create Load Balancer** Actions

Filter by tags and attributes or search by keyword

Name	DNS name	State	VPC ID	Availability Zones
You do not have any load balancers in this region.				

... **None found**

Select load balancer type

Elastic Load Balancing supports four types of load balancers: Application Load Balancers, Network Load Balancers, Gateway Load Balancers, 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.

Network Load Balancer

TCP
TLS
UDP

Create

Choose a Network Load Balancer when you need ultra-high performance, low latency, and support for connection-level load balancing. Network Load Balancers are capable of handling millions of requests per second securely.

Gateway Load Balancer

IP

Create

Choose a Gateway Load Balancer when you need to manage a fleet of third-party virtual appliances that support GENEVE. These appliances improve security, compliance, and policy controls.

3) Click on Create Application Load Balancer

...

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 ⓘ

4) Name Load Balancer

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"/>

[Cancel](#)

[Next: Configure Security Settings](#)

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

5) Select VPC

6) Select At Least 2 AZ Zones and Subnets

Additional AWS services can be integrated with this load balancer at launch when you enable them below. You can also add these and other services after your load balancer is created by reviewing the "Integrated Services" tab for the selected load balancer.

AWS Global Accelerator

☐ Create an accelerator to get static IP addresses and improve the performance and availability of your application. [Learn more](#)
[Additional charges apply](#)

Your Accelerator will be created with the following name that you can customize. Once your Accelerator is created you can manage it from the Global Accelerator console.

Accelerator name

Maximum 64 characters. Letters and numbers only.

► Tags

7) Click Next

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

...

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.

8) Click Next

[Cancel](#) [Previous](#) [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 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-002d4b487ca1292d2	default	default VPC security group	Copy to new
<input type="checkbox"/> sg-0d09b0bf676ce516f	launch-wizard-2	launch-wizard-2 created 2021-07-08T19:37:07.572-05:00	Copy to new
<input type="checkbox"/> sg-0fc356187933ae278	launch-wizard-3	launch-wizard-3 created 2021-07-08T20:58:44.588-05:00	Copy to new
<input checked="" type="checkbox"/> sg-03e5e025e377518eb	my-lab-alb-sg	Lab Application Load Balancer Security Group	Copy to new
<input type="checkbox"/> sg-0a370c15c5b405b61	my-lab-EC2-Server-sg	Web Server Security Group	Copy to new

7) Select the ALB Security Group you Created

9) Click Next

[Cancel](#) [Previous](#) [Next: Configure Routing](#)

...

Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify here. It also performs health checks on the targets using these settings. The target group you specify in this step will apply to all of the listeners configured on this load balancer. You can edit or add listeners after the load balancer is created.

Target group

Target group ⓘ New target group

Name ⓘ my-lab-target

Target type
☒ Instance
☐ IP
☐ Lambda function

Protocol ⓘ HTTP

Port ⓘ 80

Protocol version ⓘ ☒ HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

10) Name Target Group

11) Select Instance

Health checks

Protocol ⓘ HTTP

Path ⓘ /

12) Click Next

Advanced health check settings

Cancel Previous Next: Register Targets

...

Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts 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

<input type="checkbox"/>	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

13) Register the 2 EC2 instances here

Cancel Previous Next: Review

...

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-lab-alb
Scheme internet-facing
Listeners Port:80 - Protocol:HTTP
IP address type ipv4
VPC vpc-0b978358e22761686 (my-lab-vpc)
Subnets subnet-0ef43ef1cfcb561a0 (lab-sn-public-1A), subnet-03b7f8298553c4646 (lab-sn-public-1B)
Tags

▼ Security groups

Edit

Security groups sg-03e5e025e377518eb

▼ Routing

Edit

Target group New target group
Target group name my-lab-target

14) Click Create

Cancel

Previous

Create

Instruction 4. Verify and Test the ALB

View the Health Check on your the Target Group Details. Both Instances Should be Healthy

my-lab-target

Delete

arn:aws:elasticloadbalancing:us-east-1:409673912482:targetgroup/my-lab-target/785ca90756d47acd

Details

Target type	Protocol : Port	Protocol version	VPC		
Instance	HTTP: 80	HTTP1	vpc-0b978358e22761686		
Load balancer	my-lab-alb				
Total targets	Healthy	Unhealthy	Unused	Initial	Draining
2	2	0	0	0	0

Targets

Monitoring

Health checks

Attributes

Tags

Registered targets (2)

☐

Instance ID

▼

☐

Name

▼

☐

Port

▼

☐

Zone

▼

☐

Health status

▼

☐

Health status details

DNS on Load Balancer Display. Each EC2 will have a public address but you cannot access due to security group settings.

Create Load Balancer Actions

Filter by tags and attributes or search by keyword

DNS

Name	DNS name	State	VPC ID
my-lab-alb	my-lab-alb-613824474.us-east-1.elb.amazonaws.com	Active	vpc-0b978358e22761686

Test DNS with Web Browser

