

## Module 7: High Availability, Fault Tolerance And Disaster Recovery

---

### Demo Document 3

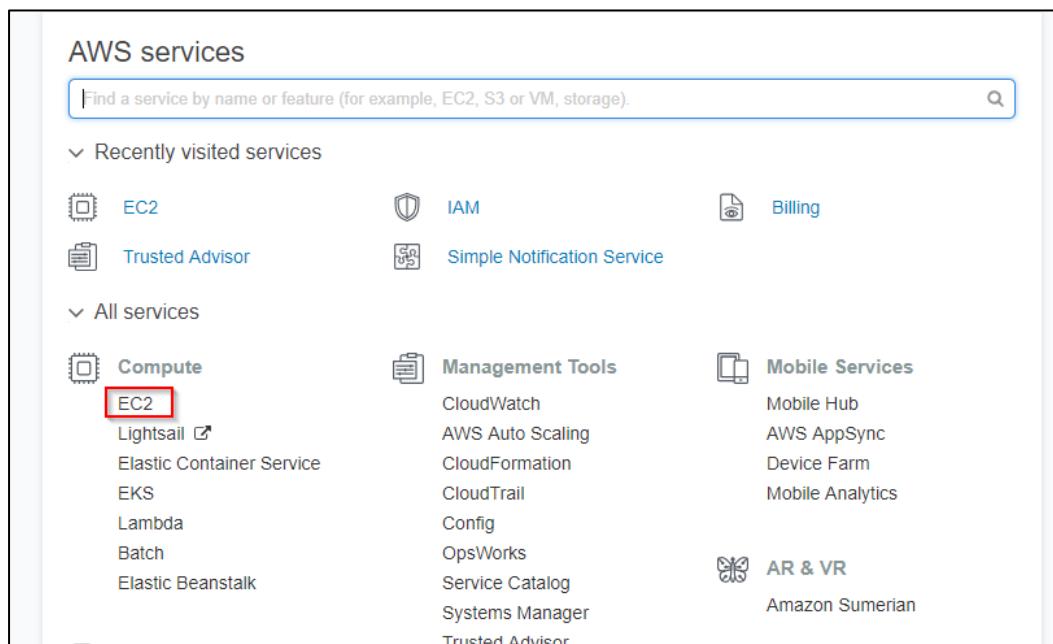
edureka!

**edureka!**

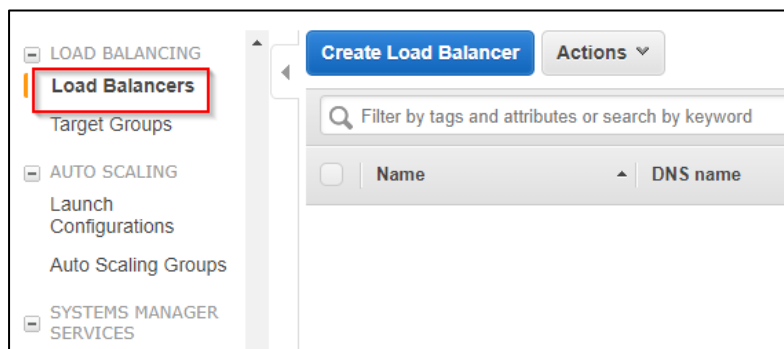
© Brain4ce Education Solutions Pvt. Ltd.

## Working of Load Balancer and Auto-Scaling to ensure Elasticity

**Step 1:** Go to AWS Management Console, select **EC2** instance and launch 2 instances



**Step 2:** After launching the instances in left navigation panel search for Load Balancing, click on “Load Balancer” which is below it



**Step 3:** Click on “Create Load Balancer” and select the “Application Load Balancer”

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, TLS termination and visibility features targeted at application architectures, including microservices and containers.

[Learn more >](#)

### Network Load Balancer

TCP

Create

Choose a Network Load Balancer when you need ultra-high performance and static IP addresses for your application. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second 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:** Give unique **name** to your Load Balancer, select the **availability zone** and click on “configure routing”

### Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default config 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"/>

### 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 Zone	Subnet ID	Subnet IPv4 CIDR	Name
<input checked="" type="checkbox"/> us-west-1a	subnet-300ba058	172.31.16.0/20	
<input checked="" type="checkbox"/> us-west-1c	subnet-310ba059	172.31.0.0/20	

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

**Step 5:** Create a new security group and click on “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 group or select an existing one.

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

**Security group name:**

**Description:**

Type <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>	Source <small>i</small>
HTTP <small>v</small>	TCP	80	Anywhere <small>v</small> 0.0.0.0/0, ::/0

**Step 6:** Create the target group for Apache instance and click on “Register targets”

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. 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. A target group can be associated with only one load balancer.

#### Target group

**Target group** i

**Name** i

**Protocol** i

**Port** i

**Target type** i

#### Health checks

**Protocol** i

**Path** i

**Step 7:** Add the Apache instance to target group click on “Add to register” and later 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

[Remove](#)

Instance	Name	Port	State	Security groups	Zone
<input checked="" type="checkbox"/> i-073ed0128a3fa35f4	apache26	80	running	launch-wizard-48	us-west-1c

**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

Search Instances

	Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input type="checkbox"/>	i-0ccbe47c23c011e...	Nagios_BSM	running	launch-wizard-23	us-west-1c	subnet-310ba059	172.31.0.0/20
<input type="checkbox"/>	i-0ee279e30dafa3...	apache-AC	running	AutoScaling-Securi...	us-west-1a	subnet-300ba058	172.31.16.0/20
<input type="checkbox"/>	i-06040cd3149c07...	Tomcat-AC	running	AutoScaling-Securi...	us-west-1c	subnet-310ba059	172.31.0.0/20

**Step 8:** Review all the added details 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** Application-LB  
**Scheme** internet-facing  
**Listeners** Port:80 - Protocol:HTTP  
**IP address type** ipv4  
**VPC** vpc-3f0ba057  
**Subnets** subnet-300ba058, subnet-310ba059  
**Tags**

▼ Security groups [Edit](#)

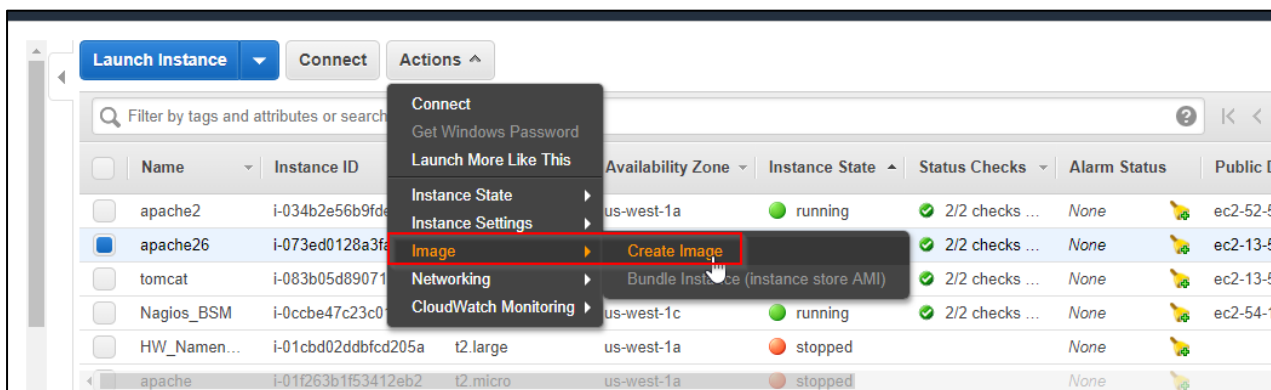
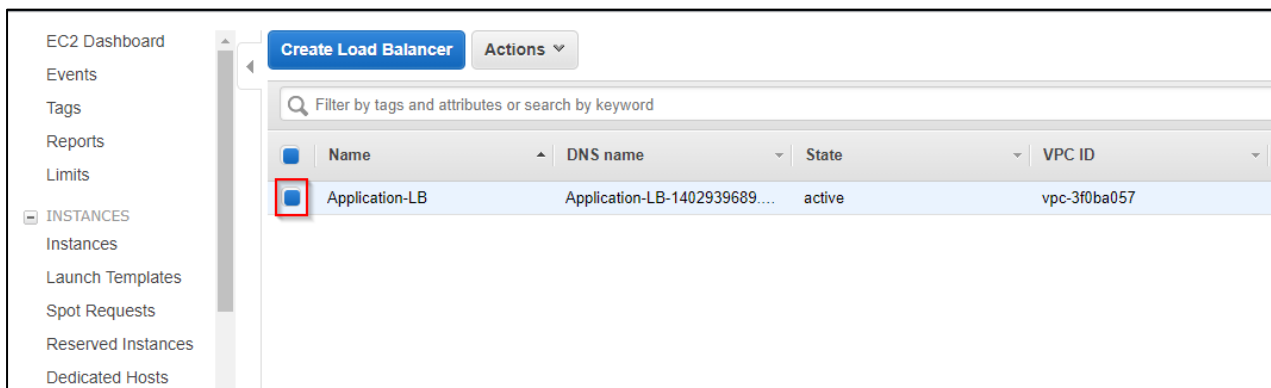
**Security groups** APP-LB

▼ Routing [Edit](#)

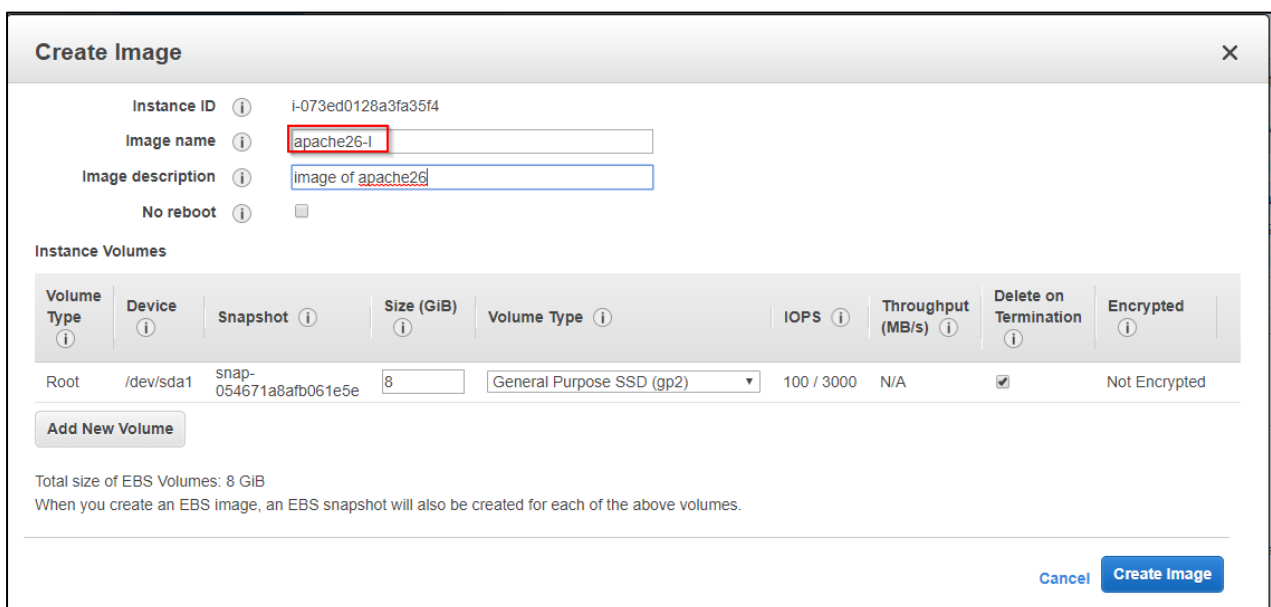
**Target group** New target group  
**Target group name** APACHE-TG  
**Port** 80  
**Target type** instance

[Cancel](#) [Previous](#) [Create](#)

**Step 9:** Once the Load Balancer is created go back to **EC2 instance dashboard** and create image of the instance



**Step 10:** Give the **image name** and click on “Create Image”



**Step 11:** Go to “Launch Configurations” and click on “Create launch configuration”

Placement Groups  
Key Pairs  
Network Interfaces

LOAD BALANCING  
Load Balancers  
Target Groups

AUTO SCALING  
**Launch Configurations**  
Auto Scaling Groups

SYSTEMS MANAGER  
SERVICES

**Launch Templates have arrived!**  
The EC2 Auto Scaling console now has full support for launch templates. Launch templates can be updated and versions of Amazon EC2. Create an Auto Scaling group to get started or [Learn more](#).

**Create launch configuration** Create Auto Scaling group Copy to launch template Actions

Filter:

<input type="checkbox"/>	Name	AMI ID	Instance Type	Spot Price	Creation Time
<input type="checkbox"/>	auto-scale	ami-0b81dc4e...	t2.micro		September 26, 2018 at 10:21:24...

**Step 12:** Select **My AMI** and choose the created image

**apache26-l** - ami-0da04c1f663611ac4  
Image of apache26  
Root device type: ebs Virtualization type: hvm Owner: 245376966395

**Select**  
64-bit

**Step 13:** Select the **t2.micro** and click on “Next”

**Create Launch Configuration**  
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of vCPUs, memory, networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your needs.

Filter by: **All instance types** Current generation Show/Hide Columns

**Currently selected:** t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-
<input checked="" type="checkbox"/>	General purpose	<b>t2.micro</b> Free tier eligible	1	1	EBS only	-
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-

**Step 14:** Give a unique name to create launch configuration

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

### Create Launch Configuration

**Name** ⓘ

**Purchasing option** ⓘ ☐ Request Spot Instances

**IAM role** ⓘ

**Monitoring** ⓘ ☐ Enable CloudWatch detailed monitoring  
[Learn more](#)

► Advanced Details

Later, if you want to use a different launch configuration, you can create a new one and apply it to any Auto Scaling group. Existing launch configurations can be edited.

**Step 15:** Configure the details and click on “Next”

### Create Launch Configuration

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes.  
<https://docs.aws.amazon.com/console/ec2/launchinstance/storage> about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput ⓘ	Delete on Termination ⓘ	Encrypted ⓘ
Root	/dev/sda1	snap-087842b1ea6574b59	<input type="text" value="8"/>	General Purpose (SSD)	100 / 3000	N/A	<input checked="" type="checkbox"/>	No

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Skip to review](#) [Next: Configure Security](#)



**Step 16:** Create a new security group and add the following rules

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

### Create Launch Configuration

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below.

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

**Security group name:**

**Description:**

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere 0.0.0.0/0
HTTP	TCP	80	Anywhere 0.0.0.0/0

**Step 17:** Check the details and click on “Create launch configurations”

### Create Launch Configuration

Review the details of your launch configuration. You can go back to edit the details of each section before you finish.

**Improve security of instances launched using your launch configuration, apache26-C. Your security group, AutoScaling-Security-Group-6, 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](#)

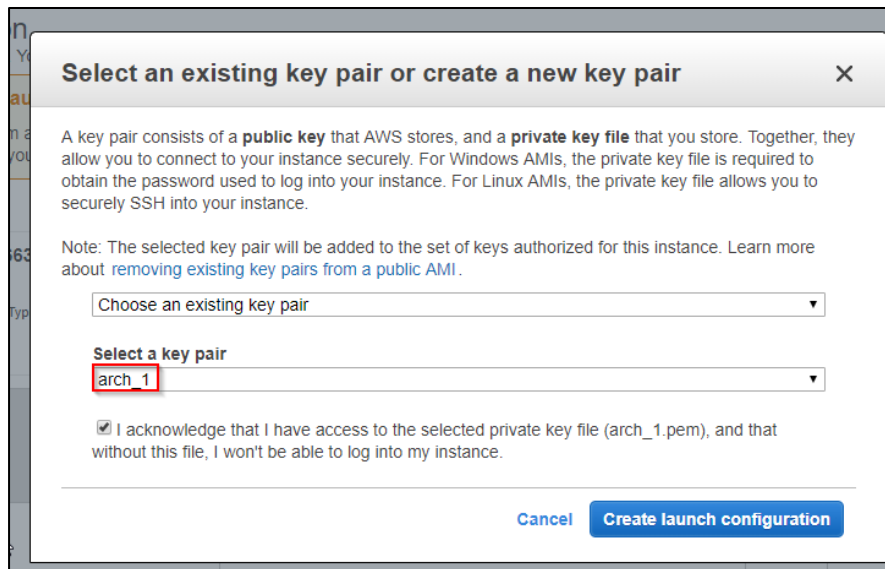
▼ AMI Details Edit AMI

**apache26-l - ami-0da04c1f663611ac4**  
 Image of apache26  
 Root device type: ebs Virtualization Type: hvm

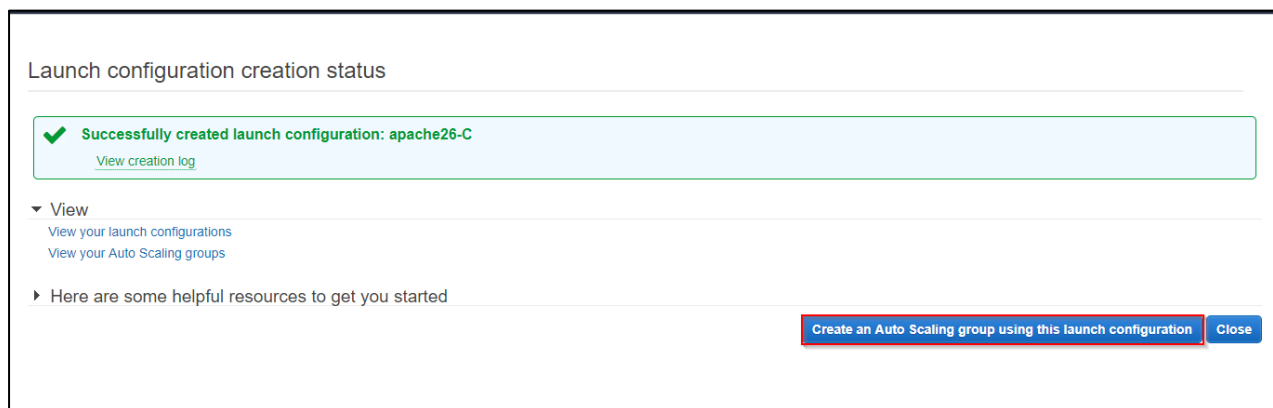
▼ Instance Type Edit instance type

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

**Step 18:** Choose an existing key pair and click on “Create launch configurations”



**Step 19:** On getting this notification click on “Create an Auto Scaling group using this launch configuration”



**Step 20:** Now create an **Auto Scaling Group** and name it

1. Configure Auto Scaling group details

2. Configure scaling policies

3. Configure Notifications

4. Configure Tags

5. Review

### Create Auto Scaling Group

Launch Configuration ⓘ

apache26-C

Group name ⓘ

apache-grp

Group size ⓘ

Start with 1 instances

Network ⓘ

vpc-3f0ba057 (172.31.0.0/16) (default)

Create new VPC

Subnet ⓘ

subnet-300ba058(172.31.16.0/20) | Default in us-west-1a x

subnet-310ba059(172.31.0.0/20) | Default in us-west-1c x

Create new subnet

Each instance in this Auto Scaling group will be assigned a public IP address. ⓘ

► Advanced Details

**Step 21:** For now select “Keep this group at its initial size”

1. Configure Auto Scaling group details

2. Configure scaling policies

3. Configure Notifications

4. Configure Tags

5. Review

### Create Auto Scaling Group

You can optionally add scaling policies if you want to adjust the size (number of instances) of your group automatically. A scaling policy uses a CloudWatch alarm that you assign to it. In each policy, you can choose to add or remove a specific number of instances or a percent of instances. When an alarm triggers, it will execute the policy and adjust the size of your group accordingly. [Learn more](#) about scaling policies.

☒

Keep this group at its initial size

☐

Use scaling policies to adjust the capacity of this group

**Step 22:** Click on “Next: Configure”

1. Configure Auto Scaling group details2. Configure scaling policies3. Configure Notifications4. Configure Tags5. Review

### Create Auto Scaling Group

Configure your Auto Scaling group to send notifications to a specified endpoint, such as an email address, whenever a specified event takes place, including: successful launch of an instance, failed instance launch, instance termination, and failed instance termination.

If you created a new topic, check your email for a confirmation message and click the included link to confirm your subscription. Notifications can only be sent to confirmed addresses.

Add notification

CancelPreviousReviewNext: Configure

**Step 23:** Check the details and click on “Create Auto Scaling group”

1. Configure Auto Scaling group details2. Configure scaling policies3. Configure Notifications4. Configure Tags5. Review

### Create Auto Scaling Group

Please review your Auto Scaling group details. You can go back to edit changes for each section. Click **Create Auto Scaling group** to complete the creation of an Auto Scaling group.

▼ Auto Scaling Group DetailsEdit details

Group name

apache-grp

Group size

1

Minimum Group Size

1

Maximum Group Size

1

Subnet(s)

subnet-300ba058,subnet-310ba059

Health Check Grace Period

300

Detailed Monitoring

No

Instance Protection

None

Service-Linked Role

AWSServiceRoleForAutoScaling

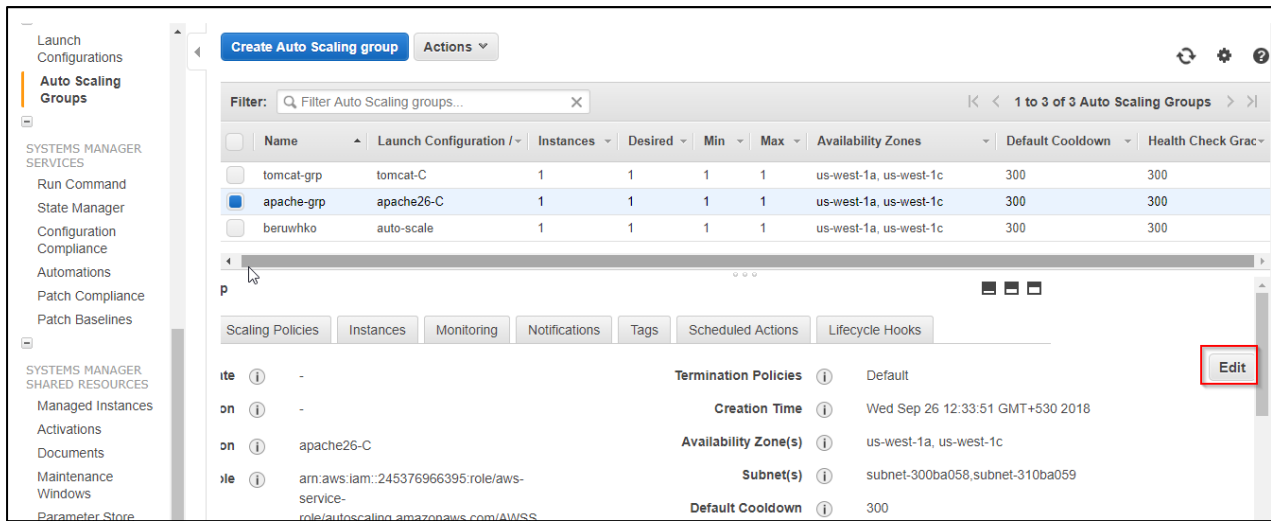
▼ Scaling PoliciesEdit scaling policies

▼ NotificationsEdit notifications

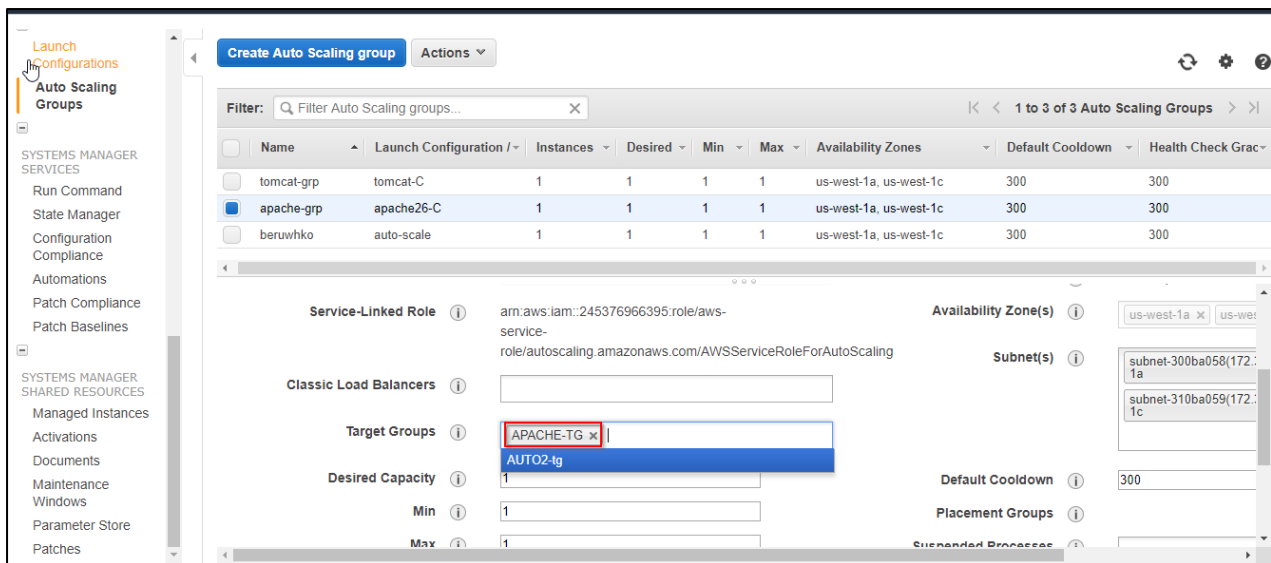
▼ TagsEdit tags

CancelPreviousCreate Auto Scaling group

**Step 24:** Click on *edit* to add the Auto Scaling Group to the Load Balancer



**Step 25:** Enter the created Target Groups



**Step 26:** Go back to **EC2 dashboard** you will see a new instance launched by the Auto – Scaling group which contains the same configuration as your launched instance

EC2 Dashboard

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
apache2	i-034b2e56b9fdeaeae	t2.micro	us-west-1a	running	2/2 checks ...	None	ec2-52-53-220-185.us-...
Tomcat-AC	i-06040cd3149c0740f	t2.micro	us-west-1c	running	2/2 checks ...	None	ec2-13-57-39-30.us-we...
tomcat	i-083b05d890710d6...	t2.micro	us-west-1a	running	2/2 checks ...	None	ec2-13-57-16-151.us-w...
Nagios_BSM	i-0ccbe47c23c011eeb	t2.micro	us-west-1c	running	2/2 checks ...	None	ec2-54-153-68-158.us-...
<b>apache-AC</b>	<b>i-0ee279e30dafa3bb1</b>	t2.micro	us-west-1a	running	2/2 checks ...	None	ec2-54-67-90-149.us-w...
HW_Namen...	i-01cbd02ddbfc205a	t2.large	us-west-1a	stopped		None	

Instance: **i-0ee279e30dafa3bb1 (apache-AC)** Public DNS: ec2-54-67-90-149.us-west-1.compute.amazonaws.com

Description Status Checks Monitoring Tags

Instance ID i-0ee279e30dafa3bb1 Public DNS (IPv4) ec2-54-67-90-149.us-west-1.compute.amazonaws.com

**Step 27:** Go back to **Load Balancer** and select the "Listeners"

Key Pairs Network Interfaces

LOAD BALANCING

**Load Balancers**

Target Groups

AUTO SCALING

Launch Configurations

Auto Scaling Groups

SYSTEMS MANAGER SERVICES

Run Command

State Manager

Configuration Compliance

Automations

Patch Compliance

Patch Baselines

SYSTEMS MANAGER SHARED RESOURCES

Managed Instances

Activations

Create Load Balancer Actions

Filter by tags and attributes or search by keyword

Name	DNS name	State	VPC ID	Availability Zones
Application-LB	Application-LB-1402939689....	active	vpc-3f0ba057	us-west-1a, us-west-1c

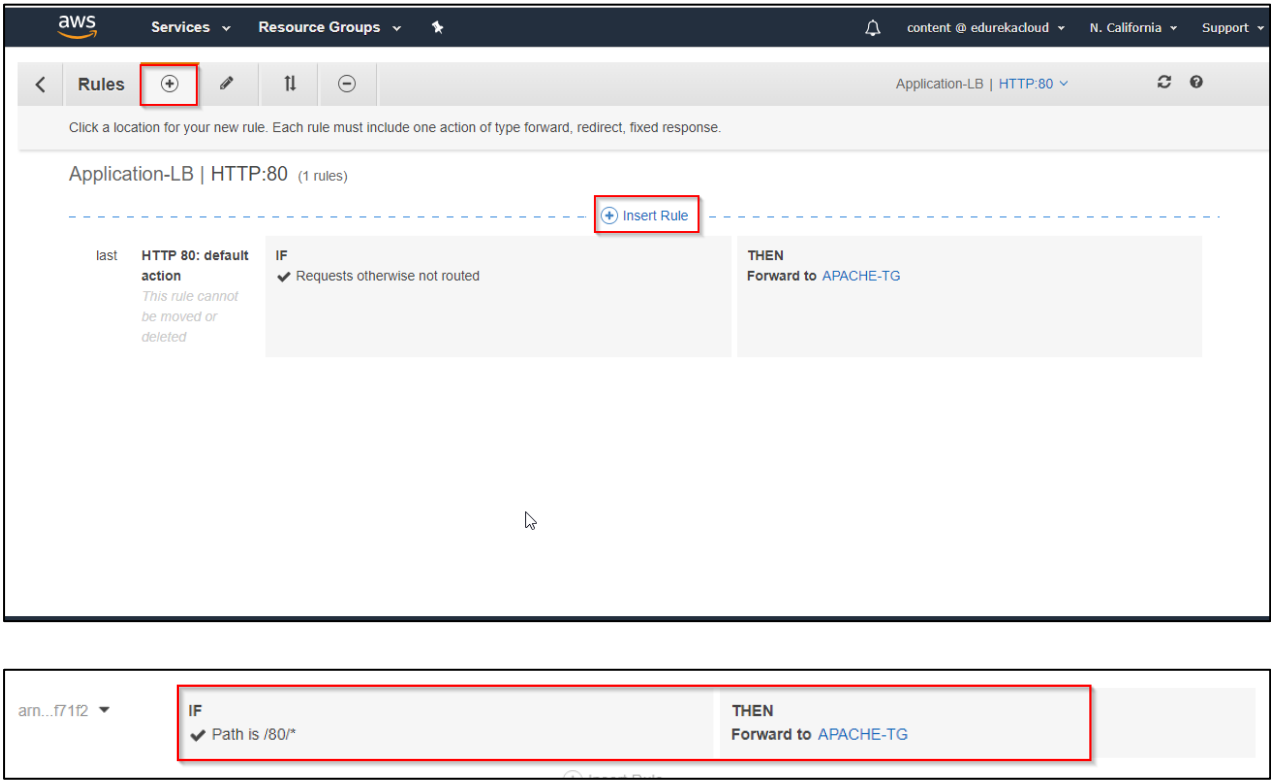
Description **Listeners** Monitoring Tags

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can remove, or update listeners and listener rules.

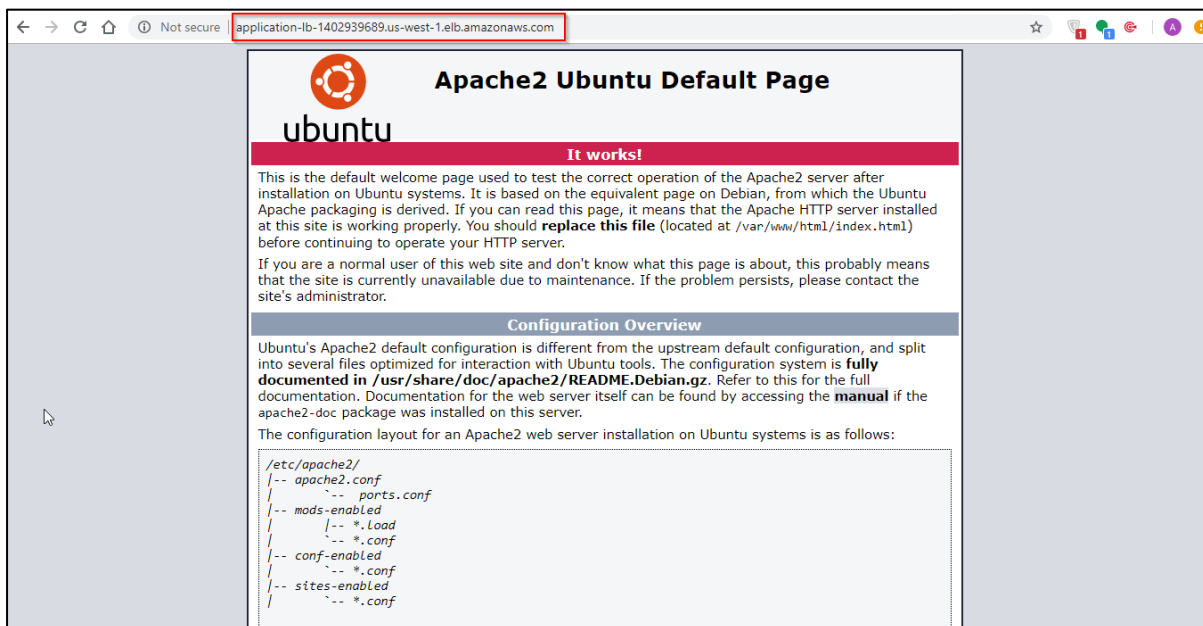
Add listener Edit Delete

Listener ID	Security policy	SSL Certificate	Rules
HTTP : 80 arn...14962e447a51eb29	N/A	N/A	Default: forwarding to APACHE-TG <a href="#">View/edit rules</a>

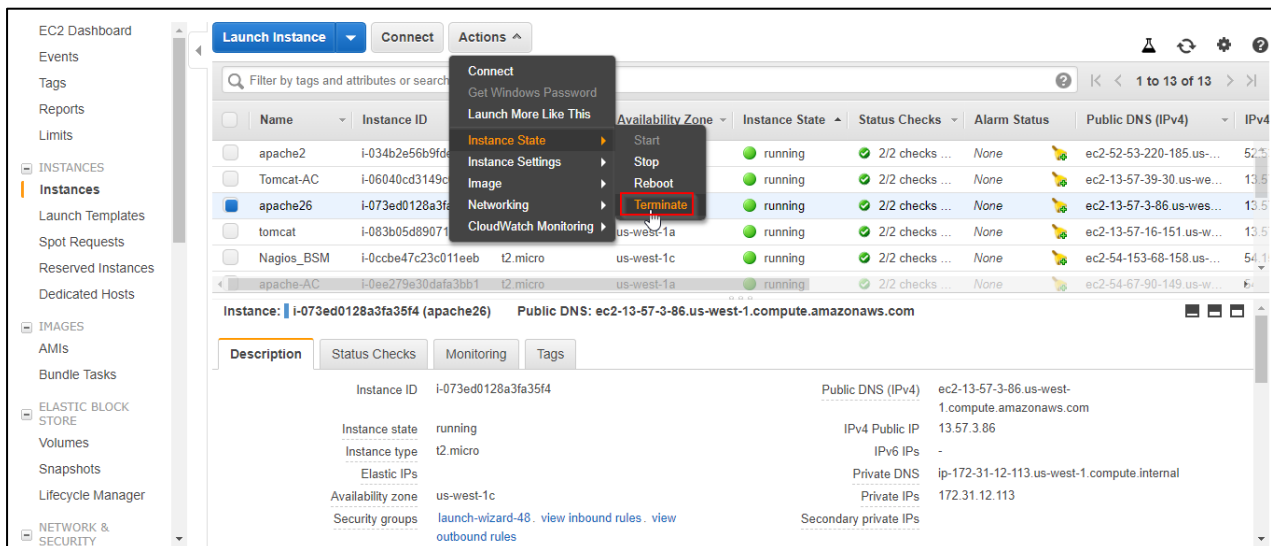
**Step 28:** Here we can add rules to check the path request ( This is mainly used if you want to attach two different servers types to same Load Balancer)



**Step 29:** To check the working of load balancer you can copy the **DNS** of Load Balancer and paste it in the browser, it will connect to you server

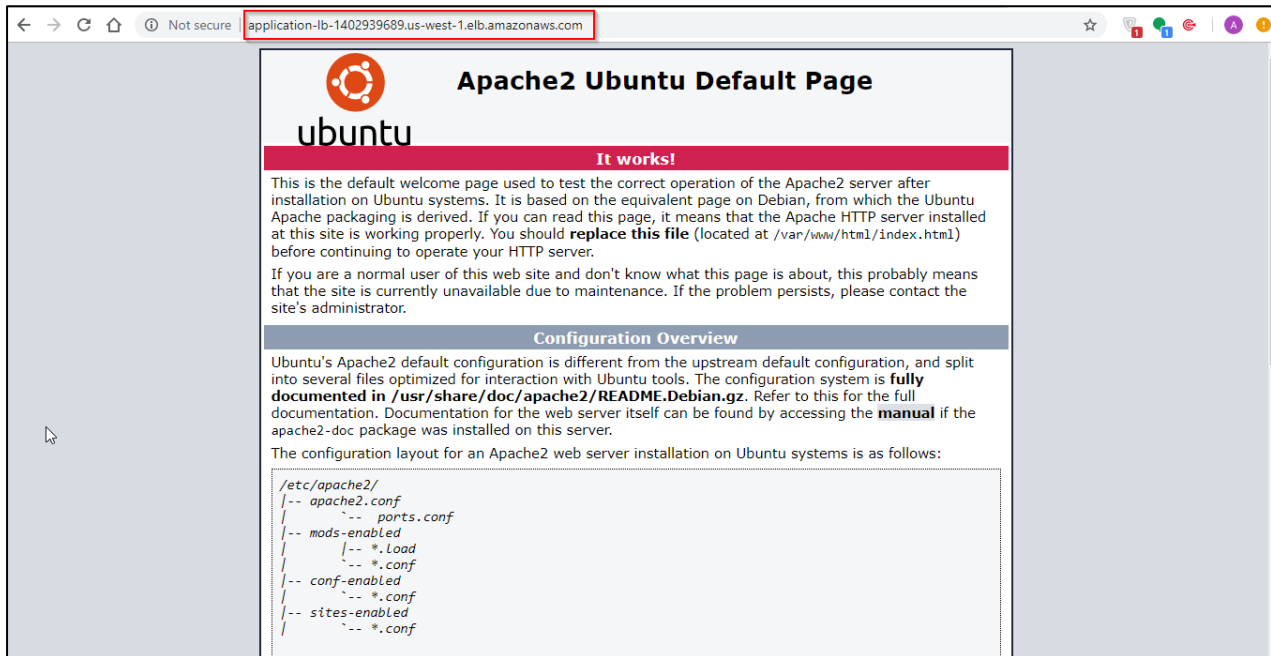


**Step 30:** Go back to EC2 dashboard and **delete** the root instance





**Step 31:** As you have attached the **Auto scaling group**, as per its function it will connect you to another **available instance** and still you can see your server when you paste the **Load Balancer DNS**



### Conclusion:

We have successfully created **Application Load Balancer, Auto Scaling Group** and learnt their functions