



CLOUD TRAIN
ACCELERATE YOUR GROWTH

MODULE 3

AUTO SCALING, LOAD BALANCING & ROUTE 53

AWS Workshop

Contact us

TO ACCELERATE YOUR CAREER GROWTH

For questions and more details:

please call @ [+91 98712 72900](tel:+919871272900), or

visit <https://www.thecloudtrain.com/>, or

email at support@thecloudtrain.com, or

WhatsApp us @ [+91 98712 72900](tel:+919871272900)

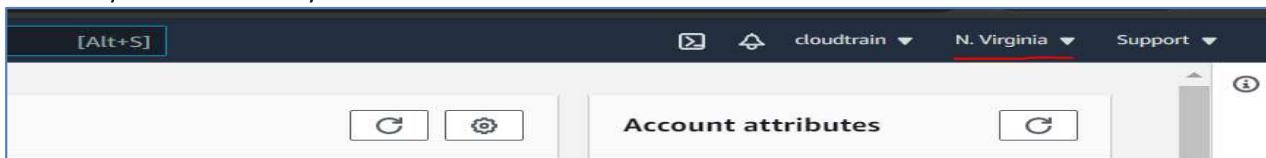
Create an Elastic Load Balancer (ELB)

Classic and Application

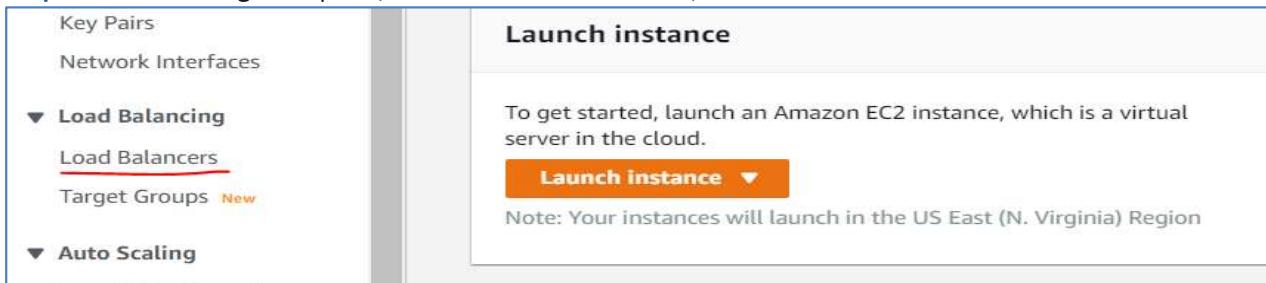
To create a Classic Load Balancer

Step 1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.

Step 2. On the navigation bar, choose a Region for your load balancer. Be sure to select the same Region that you selected for your EC2 instances.

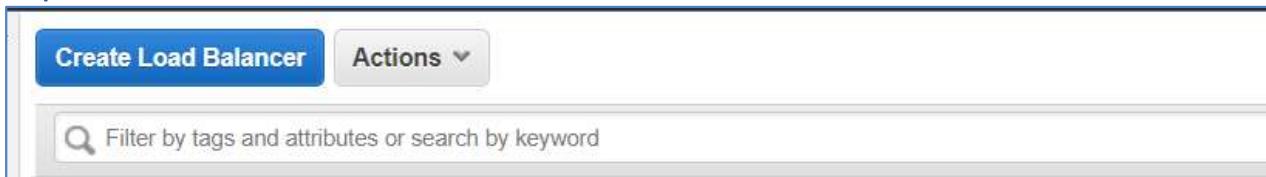


Step 3. On the navigation pane, under **LOAD BALANCING**, choose **Load Balancers**.



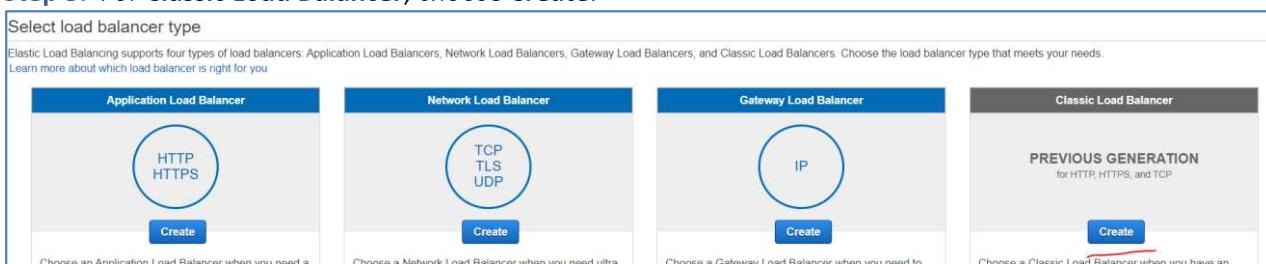
The screenshot shows the AWS Lambda service page. On the left, there's a navigation pane with 'Key Pairs', 'Network Interfaces', and a collapsed 'Load Balancing' section containing 'Load Balancers' (which is underlined in red) and 'Target Groups' (with a 'New' button). Below that is another collapsed 'Auto Scaling' section. On the right, there's a large 'Launch instance' card with the sub-headline 'To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.' It features a prominent orange 'Launch instance' button and a note below it stating 'Note: Your instances will launch in the US East (N. Virginia) Region'.

Step 4. Choose **Create Load Balancer**.



The screenshot shows the 'Create Load Balancer' page. At the top, there's a blue 'Create Load Balancer' button and a 'Actions' dropdown menu. Below that is a search bar with a magnifying glass icon and the placeholder text 'Filter by tags and attributes or search by keyword'.

Step 5. For Classic Load Balancer, choose **Create**.



The screenshot shows the 'Select load balancer type' page. It starts with a note: '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.' Below this, there are four cards: 'Application Load Balancer' (HTTP, HTTPS), 'Network Load Balancer' (TCP, TLS, UDP), 'Gateway Load Balancer' (IP), and 'Classic Load Balancer' (PREVIOUS GENERATION for HTTP, HTTPS, and TCP). Each card has a 'Create' button. A red arrow points to the 'Create' button for the 'Classic Load Balancer' card.

To define your load balancer and listener

Step 1. For Load Balancer name, type a name for your load balancer.

Step 2. For Create LB inside, select the same network that you selected for your instances: EC2-Classic or a specific VPC, say Default VPC.

Step 3. [Default VPC] If you selected a default VPC and would like to choose the subnets for your load balancer, select **Enable advanced VPC configuration**.

Step 4. Leave the default listener configuration.

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 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:	classic-lb		
Create LB Inside:	My Default VPC (172.31.0.0/16)		
Create an internal load balancer:	<input type="checkbox"/> (what's this?)		
Enable advanced VPC configuration:	<input checked="" type="checkbox"/>		
Listener Configuration:			
Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80
Add			

Step 5. For Available subnets, select at least one available public subnet using its add icon. The subnet is moved under **Selected subnets**. To improve the availability of your load balancer, select more than one public subnet. I have added 3 here: us-east-1a, us-east-1b and us-east-1c:

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 load balancer.

VPC vpc-0edb0533666a47053 (172.31.0.0/16)

Available subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR
	us-east-1d	subnet-0bf5799a192914da5	172.31.80.0/20
	us-east-1e	subnet-0eff7868d23073e81	172.31.48.0/20
	us-east-1f	subnet-0dd06ffa3a4e188cec	172.31.64.0/20

Selected subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR
	us-east-1a	subnet-0957b2b12373d8c15	172.31.16.0/20
	us-east-1b	subnet-03e8c6eadbe8383ae	172.31.32.0/20
	us-east-1c	subnet-05d14f97ad57460b4	172.31.0.0/20

Step 6. Choose **Next: Assign Security Groups**.

Assign security groups to your load balancer in a VPC

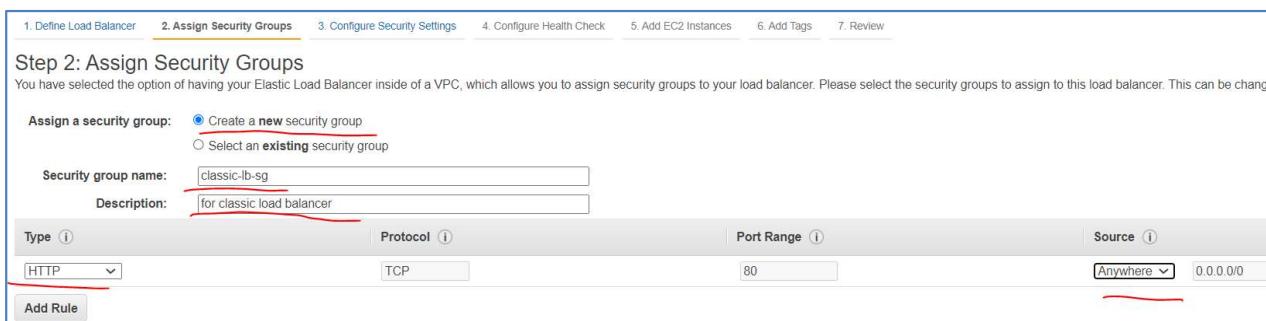
If you selected a VPC as your network, you must assign your load balancer a security group that allows inbound traffic to the ports that you specified for your load balancer and the health checks for your load balancer.

To assign security group to your load balancer

Step 1. On the **Assign Security Groups** page, select **Create a new security group**.

Step 2. Type a name and description for your security group, or leave the default name and description.

This new security group contains a rule that allows traffic to the port that you configured your load balancer to use.



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.

Assign a security group:

- Create a new security group
- Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source
HTTP	TCP	80	Anywhere (0.0.0.0/0)

Add Rule

Step 3. Choose **Next: Configure Security Settings**.

Step 4. For this tutorial, you are not using a secure listener. Choose **Next: Configure Health Check** to continue to the next step.

Configure health checks for your EC2 instances

Elastic Load Balancing automatically checks the health of the EC2 instances for your load balancer. If Elastic Load Balancing finds an unhealthy instance, it stops sending traffic to the instance and reroutes traffic to healthy instances. In this step, you customize the health checks for your load balancer.

To configure health checks for your instances

Step 1. On the **Configure Health Check** page, leave **Ping Protocol** set to HTTP and **Ping Port** set to 80.

Step 2. For **Ping Path**, replace the default value with a single forward slash ("/"). This tells Elastic Load Balancing to send health check queries to the default home page for your web server, such as index.html.

Step 3. For **Advanced Details**, leave the default values.

1. Define Load Balancer	2. Assign Security Groups	3. Configure Security Settings	4. Configure Health Check	5. Add EC2 Instances
-------------------------	---------------------------	--------------------------------	----------------------------------	----------------------

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 checks. You can customize the health check settings to fit 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	

Step 4. Choose **Next: Add EC2 Instances**.

Register EC2 instances with your load balancer

Your load balancer distributes traffic between the instances that are registered to it.

To register EC2 instances with your load balancer

Step 1. On the **Add EC2 Instances** page, select the instances to register with your load balancer. You will be able to see running instances in that region. Select the ones you want to balance load between:

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 5: Add EC2 Instances

The table below lists all your running EC2 instances. Check the boxes in the Select column to add those instances to this load balancer.

VPC vpc-0edb0533664a47053 (172.31.0.0/16)

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
i-03a96824be539fc9d		running	launch-wizard-1	us-east-1c	subnet-05d14f9...	172.31.0.0/20
i-0cf9c1fbdb651435e		running	launch-wizard-6	us-east-1a	subnet-0957b2b...	172.31.16.0/20

Step 2. Leave cross-zone load balancing and connection draining enabled.**Availability Zone Distribution**

1 instance in us-east-1a
1 instance in us-east-1c

- Enable Cross-Zone Load Balancing 
- Enable Connection Draining  300 seconds

Step 3. Choose **Next: Add Tags**.**Tag your load balancer (optional)**

You can tag your load balancer or continue to the next step.

To add tags to your load balancer**Step 1.** On the **Add Tags** page, specify a key and a value for the tag.**Step 2.** To add another tag, choose **Create Tag** and specify a key and a value for the tag.

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 6: Add Tags
Apply tags to your resources to help organize and identify them.

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key	Value
name	classic-lb

Create Tag

Step 3. After you are finished adding tags, choose **Review and Create** and then click **Create**.**Load Balancer Creation Status**

-  Successfully created load balancer

Load balancer classic-lb was successfully created.

Note: It may take a few minutes for your instances to become active in the new load balancer.

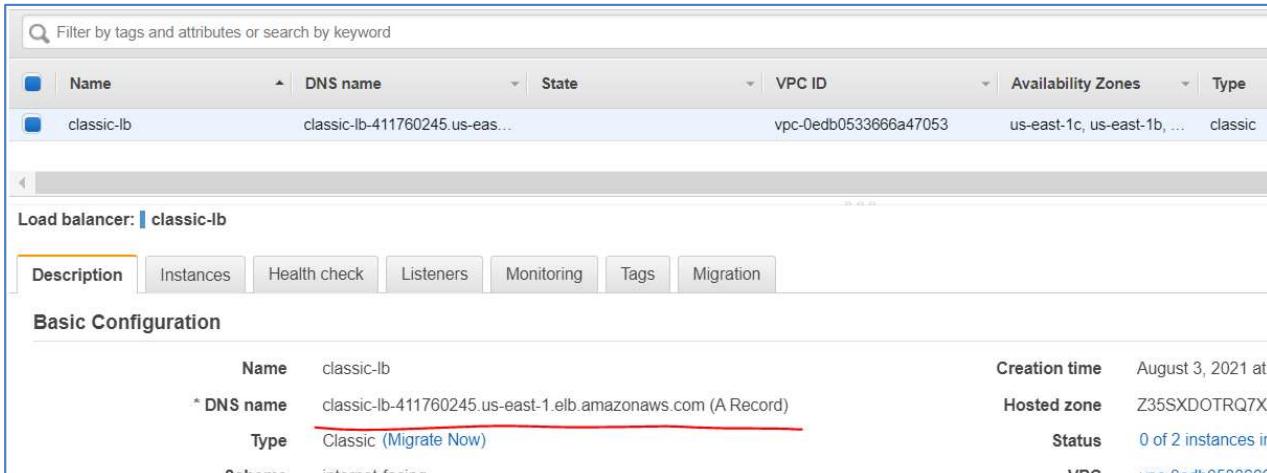
Create and verify your load balancer

Before you create the load balancer, review the settings that you selected. After creating the load balancer, you can verify that it's sending traffic to your EC2 instances.

To create and test your load balancer

1. On the **Review** page, choose **Create**.
2. After you are notified that your load balancer was created, choose **Close**.
3. Select your new load balancer.
4. On the **Description** tab, check the **Status** row. If it indicates that some of your instances are not in service, its probably because they are still in the registration process.
5. After at least one of your EC2 instances is in service, you can test your load balancer. Copy the string from **DNS name** (for example, my-load-balancer-1234567890.us-west-2.elb.amazonaws.com) and paste it into the address field of an internet-connected web browser.

If your load balancer is working, you see the default page of your server.

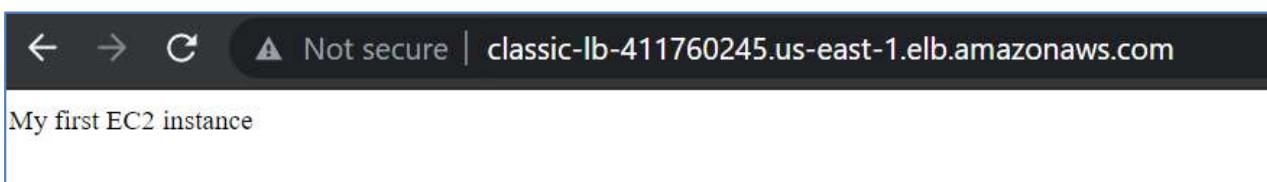


The screenshot shows the AWS CloudFormation console with the search bar set to "classic-lb". A table lists the load balancer details:

Name	DNS name	State	VPC ID	Availability Zones	Type
classic-lb	classic-lb-411760245.us-east-1.elb.amazonaws.com	Creating	vpc-0edb0533666a47053	us-east-1c, us-east-1b, us-east-1a	classic

Below the table, the "classic-lb" load balancer is selected. The "Description" tab is active. The "Basic Configuration" section displays the following details:

Name	classic-lb	Creation time	August 3, 2021 at 10:45 AM
* DNS name	classic-lb-411760245.us-east-1.elb.amazonaws.com (A Record)	Hosted zone	Z35SXDOTRQ7X7
Type	Classic (Migrate Now)	Status	0 of 2 instances in service
Schema	internet-facing	VPC	vpc-0edb0533666a47053



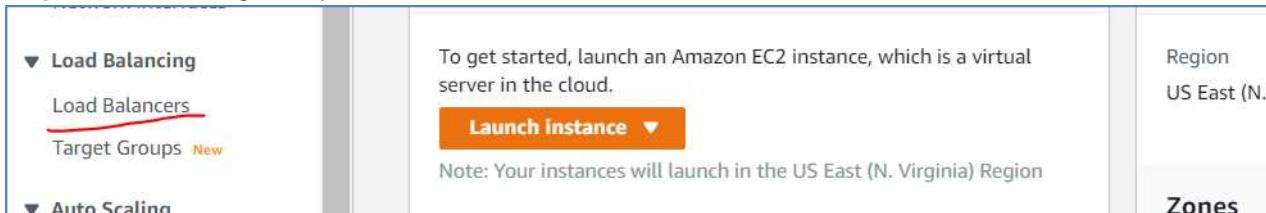
The screenshot shows a web browser window with the URL "classic-lb-411760245.us-east-1.elb.amazonaws.com". The address bar also shows "Not secure". The page content is "My first EC2 instance".

Configure an Application load balancer

To configure your load balancer and listener

Step 1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.

Step 2. On the navigation pane, under **LOAD BALANCING**, choose **Load Balancers**.



To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

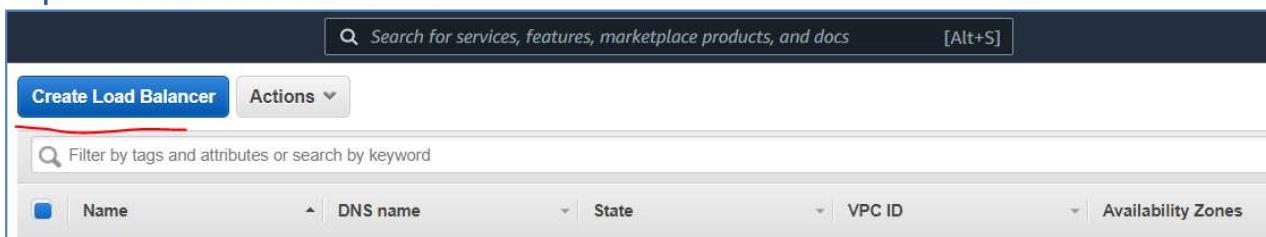
Launch instance ▾

Note: Your instances will launch in the US East (N. Virginia) Region

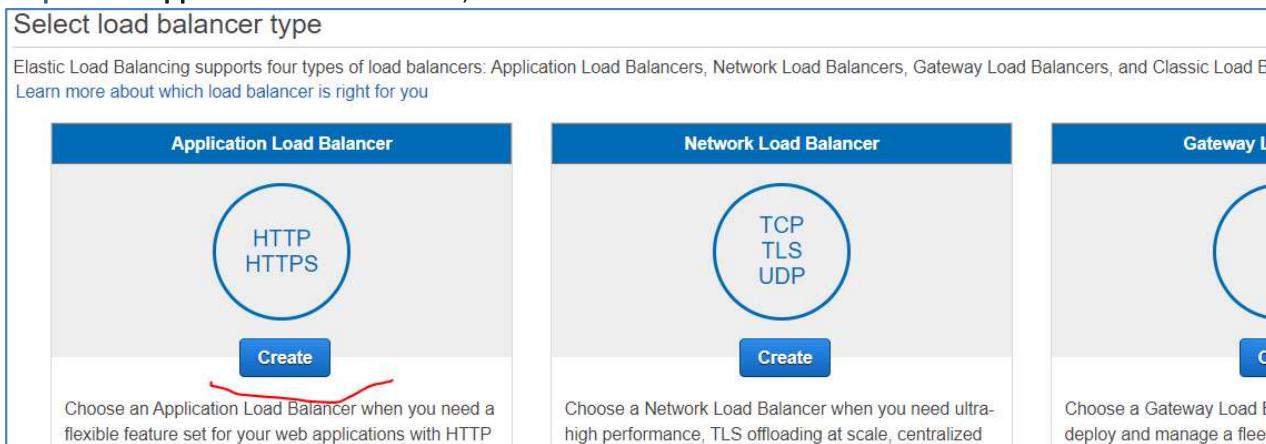
Region
US East (N. Virginia)

Zones

Step 3. Choose **Create Load Balancer**.



Step 4. For Application Load Balancer, choose **Create**.



Select load balancer type

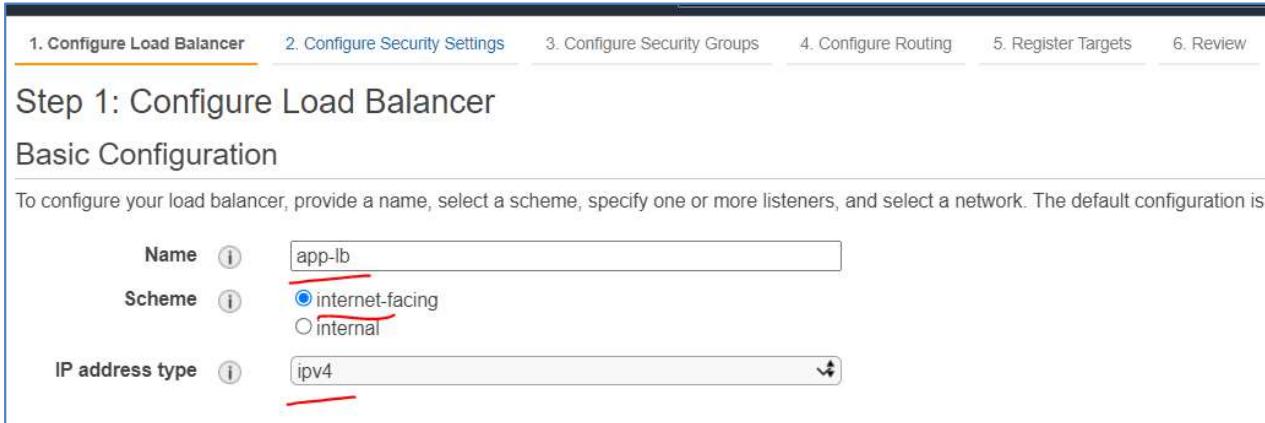
Elastic Load Balancing supports four types of load balancers: Application Load Balancers, Network Load Balancers, Gateway Load Balancers, and Classic Load Balancers. Learn more about which load balancer is right for you.

Application Load Balancer  Create Choose an Application Load Balancer when you need a flexible feature set for your web applications with HTTP	Network Load Balancer  Create Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized monitoring, and more	Gateway L...  Create Choose a Gateway Load Balancer when you need to deploy and manage a fleet of devices or virtual machines
--	---	---

Step 5. For **Name**, enter a name for your load balancer. For example, **app-lb**

Step 6. For **Scheme**, an internet-facing load balancer routes requests from clients over the internet to targets. An internal load balancer routes requests to targets using private IP addresses.

Step 7. For IP address type, choose **ipv4** if your clients use IPv4 addresses to communicate with the load balancer, or choose **dualstack** if your clients use both IPv4 and IPv6 addresses to communicate with the load balancer. If the load balancer is an internal load balancer, you must choose **ipv4**.



The screenshot shows the 'Step 1: Configure Load Balancer' page. At the top, there are six tabs: 1. Configure Load Balancer (selected), 2. Configure Security Settings, 3. Configure Security Groups, 4. Configure Routing, 5. Register Targets, and 6. Review. Below the tabs, the section title 'Step 1: Configure Load Balancer' is displayed. Under 'Basic Configuration', there are three fields: 'Name' with value 'app-lb', 'Scheme' with 'internet-facing' selected (radio button highlighted with a red box), and 'IP address type' with 'ipv4' selected (dropdown menu highlighted with a red box). A note below the fields states: 'To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is selected.'

Step 8. For **Listeners**, the default is a listener that accepts HTTP traffic on port 80. You can keep the default listener settings, modify the protocol, or modify the port. Choose **Add** to add another listener (for example, an HTTPS listener).



The screenshot shows the 'Listeners' configuration page. The title 'Listeners' is at the top. A note below it says: 'A listener is a process that checks for connection requests, using the protocol and port that you configured.' There is a table with two columns: 'Load Balancer Protocol' and 'Load Balancer Port'. The first row shows 'HTTP' in the protocol column and '80' in the port column. A 'Add listener' button is located at the bottom left of the table area.

Step 9. Select one subnet per zone to enable. If you enabled dual-stack mode for the load balancer, select subnets with associated IPv6 CIDR blocks. You can specify one of the following:

- Subnets from at least two Availability Zones
- Subnets from one or more Local Zones
- One Outpost subnet

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 the availability of your load balancer.

VPC	vpc-0edb0533666a47053 (172.31.0.0/16) (default)
Availability Zones	<input checked="" type="checkbox"/> us-east-1a subnet-0957b2b12373d8c15 <input checked="" type="checkbox"/> us-east-1b subnet-03e8c6eadbe8383ae <input checked="" type="checkbox"/> us-east-1c subnet-05d14f97ad57460b4
	IPv4 address Assigned by AWS
	IPv4 address Assigned by AWS
	IPv4 address Assigned by AWS

Step 10. Leave other thing default and Choose **Next: Configure Security Settings**.

Configure a security group

To configure a security group for your load balancer

Step 1. Choose **Create a new security group**.

Step 2. Enter a name and description for the security group, or keep the default name and description.

This new security group contains a rule that allows traffic to the port that you selected for your load balancer on the **Configure Load Balancer** page.

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	<input checked="" type="radio"/> Create a new security group <input type="radio"/> Select an existing security group		
Security group name	app-lb-sg		
Description	Load balancer for app LB		
Type	Protocol	Port Range	Source
HTTP	TCP	80	Anywhere
<input type="button" value="Add Rule"/>			

Step 3. Choose **Next: Configure Routing**.

Configure a target group

You register targets with a target group. The target group that you configure in this step is used as the target group in the default listener rule, which forwards requests to the target group.

To configure your target group

Step 1. For **Target group**, keep the default, **New target group**.

Step 2. For **Name**, enter a name for the target group.

Step 3. For **Target type**, select **Instance** to register targets by instance ID.

Step 4: Configure Routing

Target group 	<input type="text" value="New target group"/> 
Name 	<input type="text" value="app-lb-target"/>
Target type	<input checked="" type="radio"/> Instance <input type="radio"/> IP <input type="radio"/> Lambda function
Protocol 	<input type="text" value="HTTP"/> 
Port 	<input type="text" value="80"/>
Protocol version 	<input checked="" type="radio"/> HTTP1 <small>Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.</small> <input type="radio"/> HTTP2 <small>Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.</small> <input type="radio"/> gRPC <small>Send requests to targets using gRPC. Supported when the request protocol is gRPC.</small>

Health checks

Protocol 	<input type="text" value="HTTP"/> 
Path 	<input type="text" value="/"/>

► Advanced health check settings

Step 4. Choose **Next: Register Targets**.

Configure targets for the target group

With an Application Load Balancer, the target type of your target group determines how you register targets with the target group.

To register targets by instance ID

Step 1. For **Instances**, select one or more instances.

Step 2. Enter the instance listener port, and then choose **Add to registered**.

Step 3. When you have finished registering instances, choose **Next: Review** and then **Click Create**.

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	Instance	Name	Port	State	Security groups	Zone
<input type="checkbox"/>	i-03a6824be539fcf9d		80	running	launch-wizard-1	us-east-1c
<input type="checkbox"/>	i-0cf9c1fbdd651435e		80	running	launch-wizard-6	us-east-1a

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
<input type="checkbox"/>	i-03a6824be539fcf9d
<input type="checkbox"/>	i-0cf9c1fbdd651435e

Load Balancer Creation Status

Successfully created load balancer

Load balancer **app-lb** was successfully created.

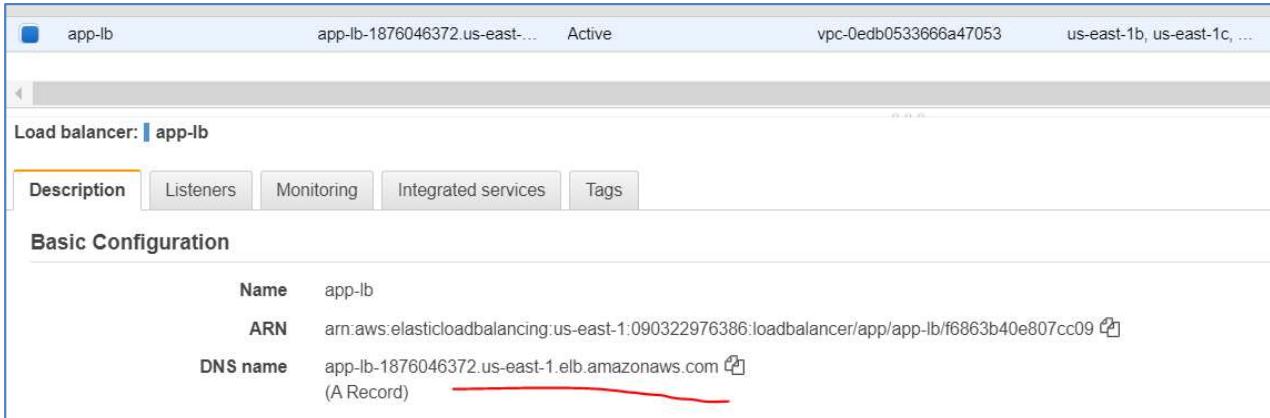
Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass the initial health checks.

Suggested next steps

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

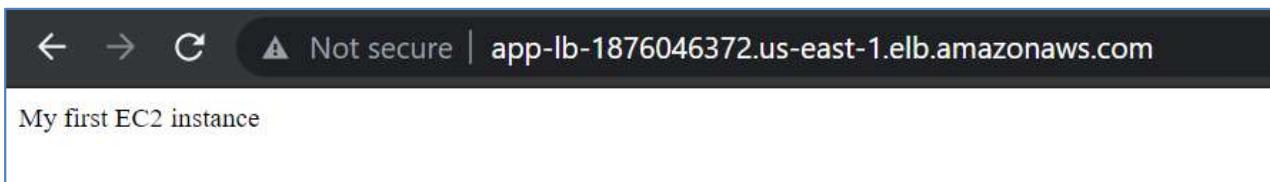
Test the load balancer

After creating your load balancer, you can verify that your targets have passed the initial health check and then test that the load balancer is sending traffic to your targets



The screenshot shows the AWS Elastic Load Balancing console. A single load balancer named "app-lb" is listed. The details shown are:

Name	app-lb
ARN	arn:aws:elasticloadbalancing:us-east-1:090322976386:loadbalancer/app/app-lb/f6863b40e807cc09
DNS name	app-lb-1876046372.us-east-1.elb.amazonaws.com (A Record)



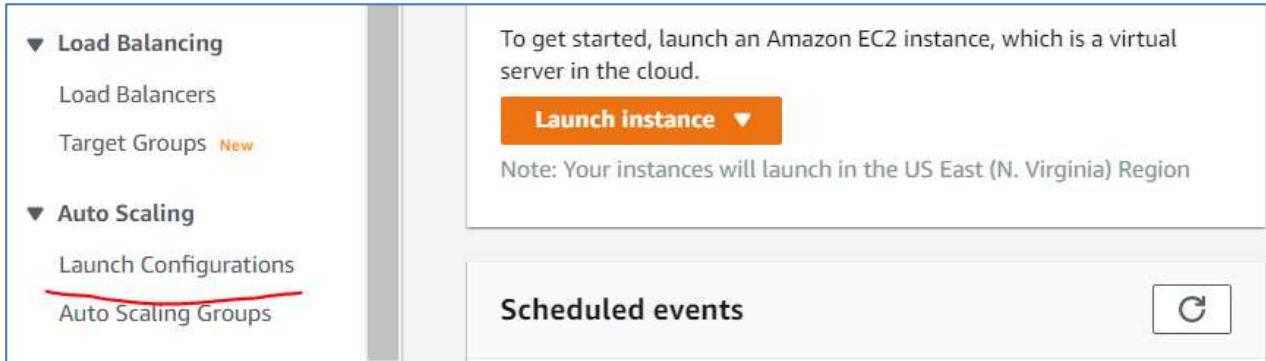
The screenshot shows a web browser window. The address bar displays the URL "Not secure | app-lb-1876046372.us-east-1.elb.amazonaws.com". The main content area of the browser shows the text "My first EC2 instance".

Configuration of an auto-scaling group

To create a launch configuration (console)

Step 1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.

Step 2. On the navigation pane, under **AUTO SCALING**, choose **Launch Configurations**.



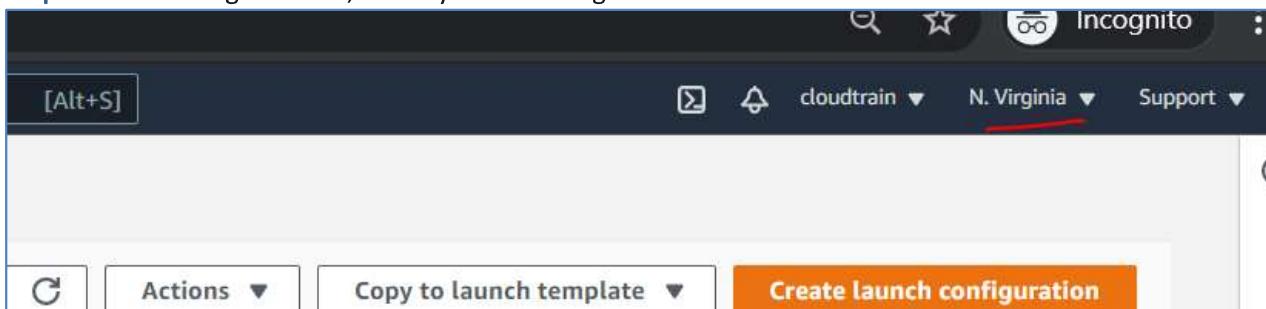
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▾

Note: Your instances will launch in the US East (N. Virginia) Region

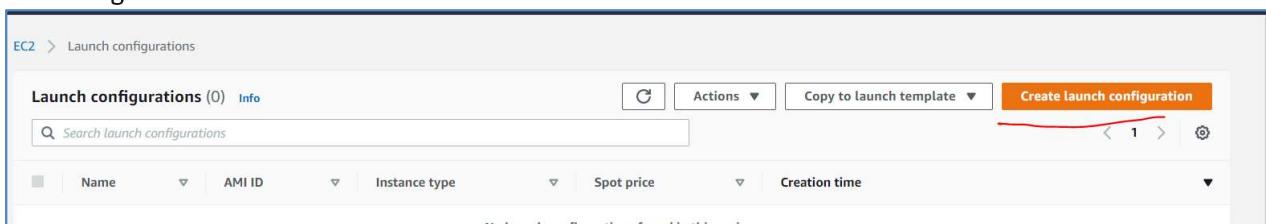
Scheduled events

Step 3. In the navigation bar, select your AWS Region.



[Alt+S] [Σ] [Bell] cloudtrain N. Virginia Support

Step 4. Choose **Create launch configuration**, and enter a name for your launch configuration, say **launch-config1**.



EC2 > Launch configurations

Launch configurations (0) Info

Actions ▾ Copy to launch template ▾ Create launch configuration

No launch configurations found in this region

Step 5. For **Amazon machine image (AMI)**, choose an AMI. Let's use the same AMI that we created for webserver instance, so that we can test our website on auto scaling.

Step 6. For **Instance type**, select a hardware configuration for your instances.

Launch configuration name

Name

Amazon machine image (AMI) [Info](#)

AMI

Instance type [Info](#)

Instance type
 [Choose instance type](#)

Step 7. Leave other values default and for **Security groups**, create or select the security group to associate with the group's instances. If you leave the **Create a new security group** option selected, a default SSH rule is configured for Amazon EC2 instances running Linux. Add HTTP rule also to access your website on port 80:

Security groups [Info](#)

Assign a security group
 Create a new security group
 Select an existing security group

Security group name

Description

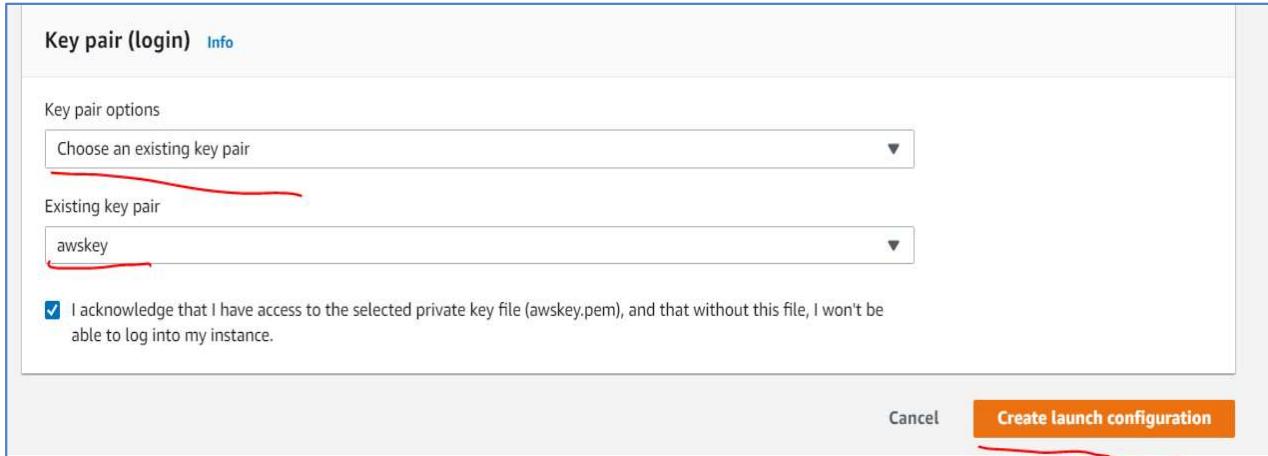
Rules

Type	Protocol	Port range	Source type	Source
<input type="checkbox"/> SSH	TCP	22	Anywhere	0.0.0.0/0
<input type="checkbox"/> HTTP	TCP	80	Anywhere	0.0.0.0/0

Step 8. For Key pair (login), choose an option under Key pair options.

If you've already configured an Amazon EC2 instance key pair, you can choose it here.

If you don't already have an Amazon EC2 instance key pair, choose **Create a new key pair** and give it a recognizable name. Choose **Download key pair** to download the key pair to your computer. We use existing one here:



Key pair (login) [Info](#)

Key pair options

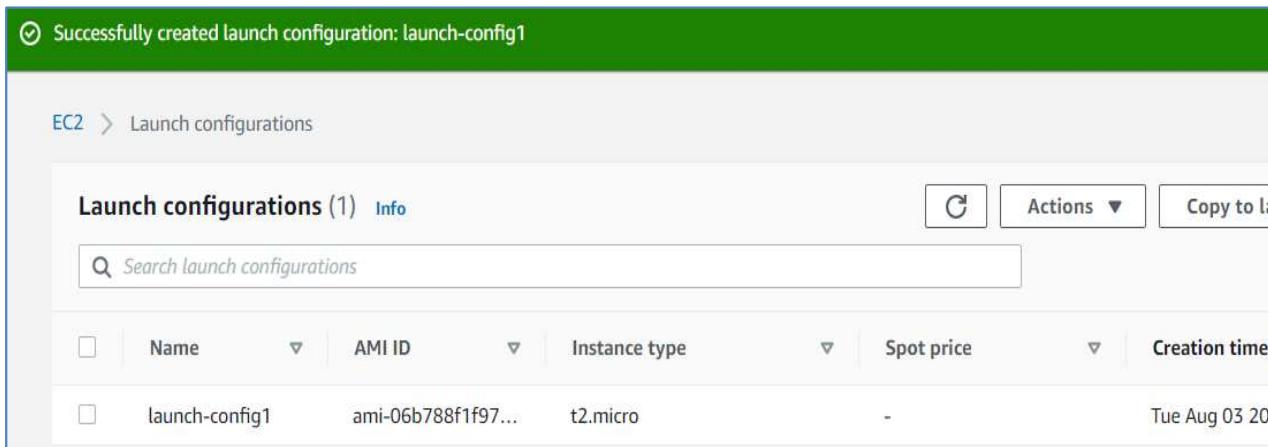
Choose an existing key pair

Existing key pair

awskey

I acknowledge that I have access to the selected private key file (awskey.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#) [Create launch configuration](#)



EC2 > Launch configurations

Launch configurations (1) [Info](#)

Search launch configurations

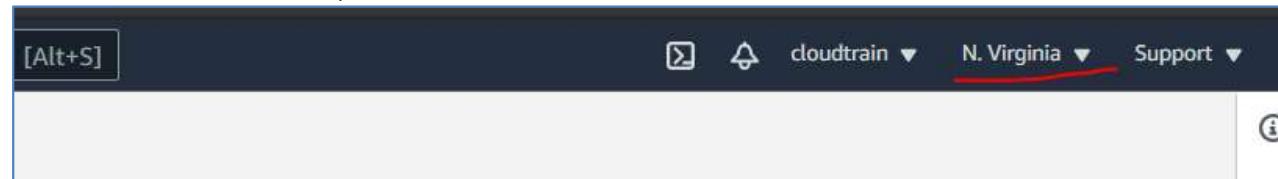
<input type="checkbox"/>	Name	AMI ID	Instance type	Spot price	Creation time
<input type="checkbox"/>	launch-config1	ami-06b788f1f97...	t2.micro	-	Tue Aug 03 2021

To create an Auto Scaling group using a launch configuration (console)

Step 1. Open the Amazon EC2 Auto Scaling console at <https://console.aws.amazon.com/ec2autoscaling/> and click on **Create Auto Scaling Group**



Step 2. On the navigation bar at the top of the screen, choose the same Region that you used when you created the launch template.

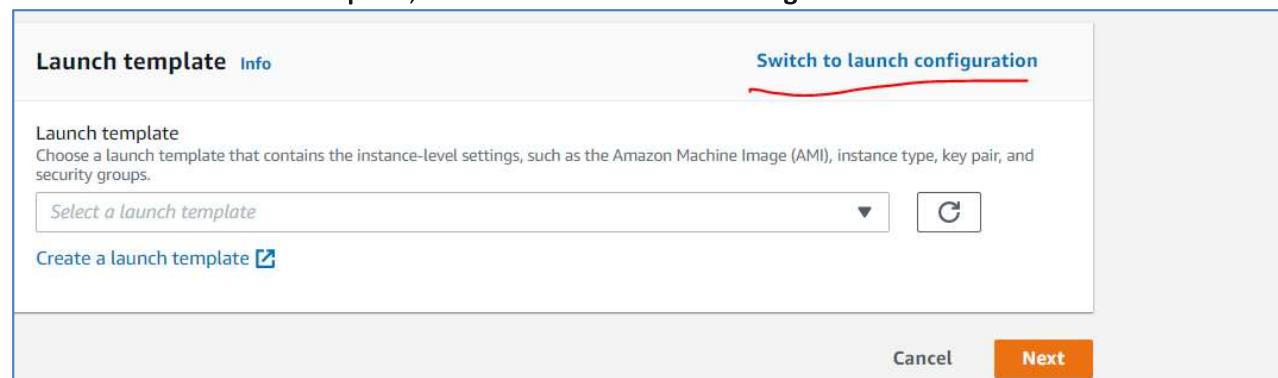


Step 3. Choose **Create an Auto Scaling group**.

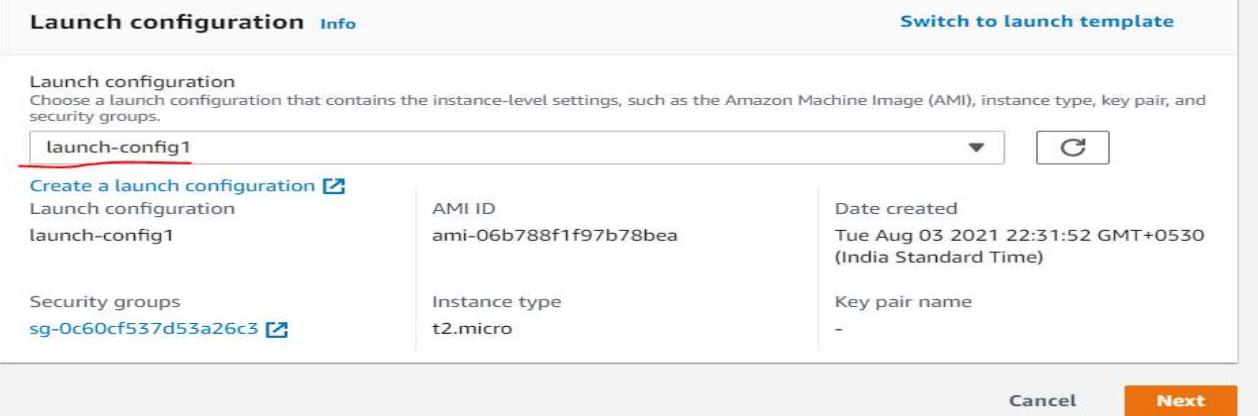
Step 4. On the **Choose launch template or configuration** page, for **Auto Scaling group name**, enter a name for your Auto Scaling group, say **Auto Scaling Grp1**

Step 5. To choose a launch configuration, do the following:

- For **Launch Template**, choose **Switch to launch configuration**.



- b. For **Launch configuration**, choose an existing launch configuration.



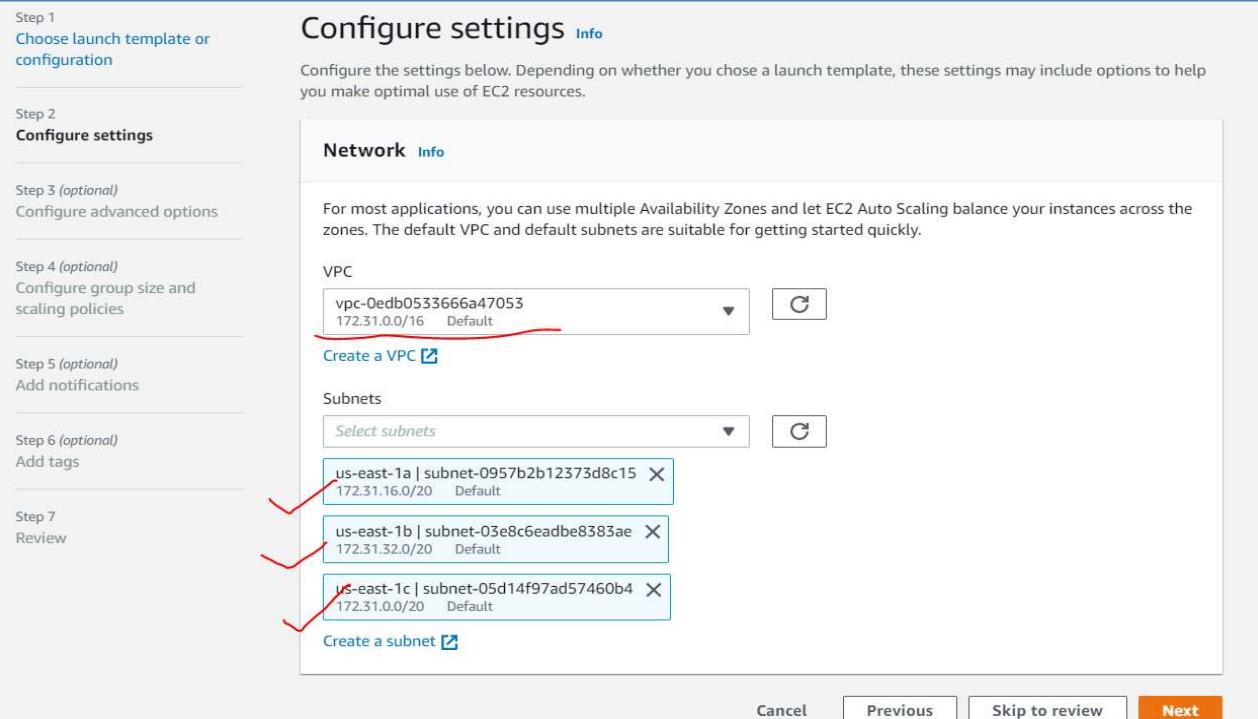
The screenshot shows the 'Launch configuration' page. At the top, there's a search bar with 'launch-config1' and a 'Create a launch configuration' button. Below the search bar, it lists a single launch configuration named 'launch-config1'. To its right, details are shown: AMI ID 'ami-06b788f1f97b78bea', Instance type 't2.micro', and Date created 'Tue Aug 03 2021 22:31:52 GMT+0530 (India Standard Time)'. There's also a 'Key pair name' field which is empty. At the bottom right are 'Cancel' and 'Next' buttons.

- c. Verify that your launch configuration supports all of the options that you are planning to use, and then choose **Next**.

Step 6. On the **Configure settings** page, under **Network**, for **VPC**, choose the VPC for the security groups that you specified in your launch configuration.

Step 7. For **Subnet**, choose one or more subnets in the specified VPC. Use subnets in multiple Availability Zones for high availability.

Step 8. Accept the rest of the defaults and choose **Skip to review**.



The screenshot shows the 'Configure settings' page for Step 8. On the left, a sidebar lists steps from 1 to 7. Step 8 is currently active. The main area is titled 'Network' and shows a VPC dropdown set to 'vpc-0edb0533666a47053 172.31.0.0/16 Default'. Below it is a 'Create a VPC' button. A 'Subnets' section shows three subnets listed: 'us-east-1a | subnet-0957b2b12373d8c15 172.31.16.0/20 Default', 'us-east-1b | subnet-03e8c6eadbe8383ae 172.31.32.0/20 Default', and 'us-east-1c | subnet-05d14f97ad57460b4 172.31.0.0/20 Default'. Each subnet has a red checkmark next to it. At the bottom are 'Create a subnet' and 'Skip to review' buttons.

Step 9. On the Review page, lets edit the **Configure group size and scaling policies** -> minimum 1 and maximum 2. Then choose **Create Auto Scaling group**

Configure group size and scaling policies Info

Set the desired, minimum, and maximum capacity of your Auto Scaling group. You can optionally add a scaling policy to dynamically scale the number of instances in the group.

Group size - optional Info

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

Desired capacity

Minimum capacity

Maximum capacity



Step 4: Configure group size and scaling policies

[Edit](#)

Group size

Desired capacity

Minimum capacity

Maximum capacity

⌚ Auto Scaling Grp1 created successfully

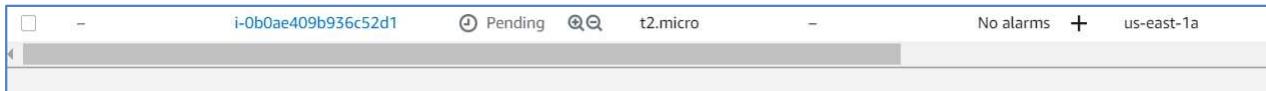
[EC2](#) > Auto Scaling groups

Auto Scaling groups (1)

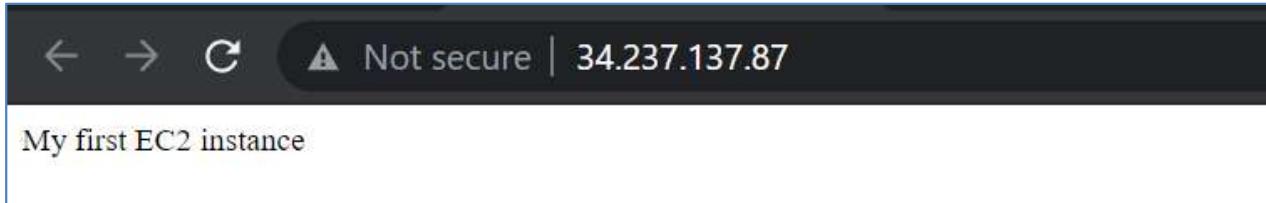
 Search your Auto Scaling groups

<input type="checkbox"/>	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max
<input type="checkbox"/>	Auto Scaling Grp1	launch-config1	0	⌚ Updating capacity	1	1	2

Step 10. After some time, you can see a new instance has been created using Auto scaling as per minimum count specified:



Step 11. We have successfully configured the Auto scaling for EC2 instances. If you try to access the website, you should be able to access it using public IP of EC2 instance:



Integrating ELB with Auto Scaling

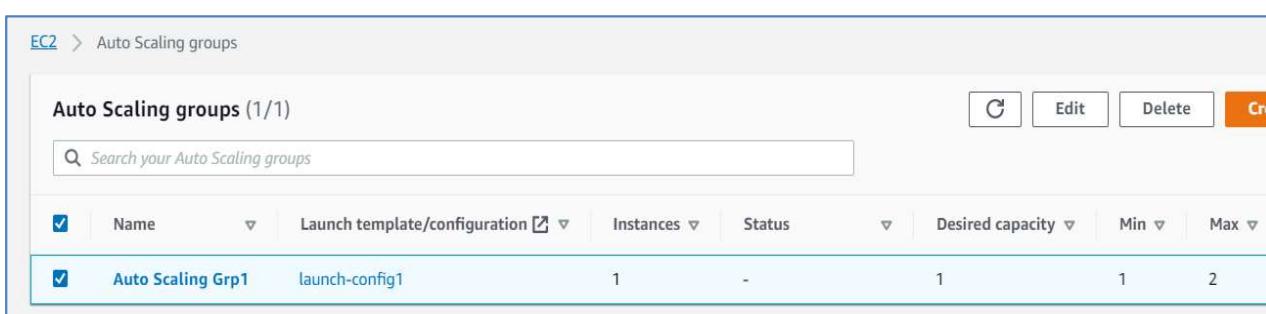
To attach an existing load balancer to an existing Auto Scaling group

Use the following procedure to attach a load balancer to an existing Auto Scaling group.

Step 1. Open the Amazon EC2 Auto Scaling console at <https://console.aws.amazon.com/ec2autoscaling/>.

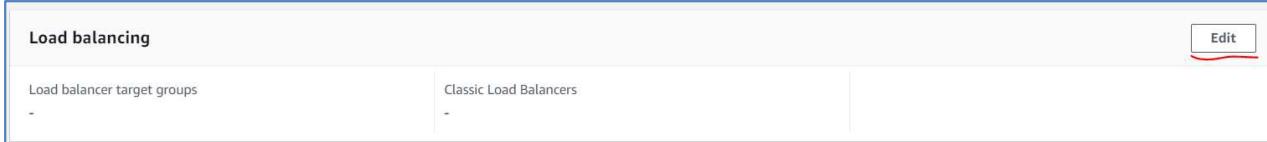
Step 2. Select the check box next to an existing group.

A split pane opens up in the bottom part of the **Auto Scaling groups** page, showing information about the group that's selected.



A screenshot of the AWS Auto Scaling Groups page. The top navigation bar shows "EC2 > Auto Scaling groups". The main table header includes columns for "Name", "Launch template/configuration", "Instances", "Status", "Desired capacity", "Min", and "Max". A single row is selected, showing "Auto Scaling Grp1" with "launch-config1", 1 instance, and a status of "-". The "Desired capacity" is set to 1, and the "Min" and "Max" values are both 2. Action buttons for "Create", "Edit", and "Delete" are visible in the top right of the table area.

Step 3. On the Details tab, choose **Load balancing**, **Edit**.

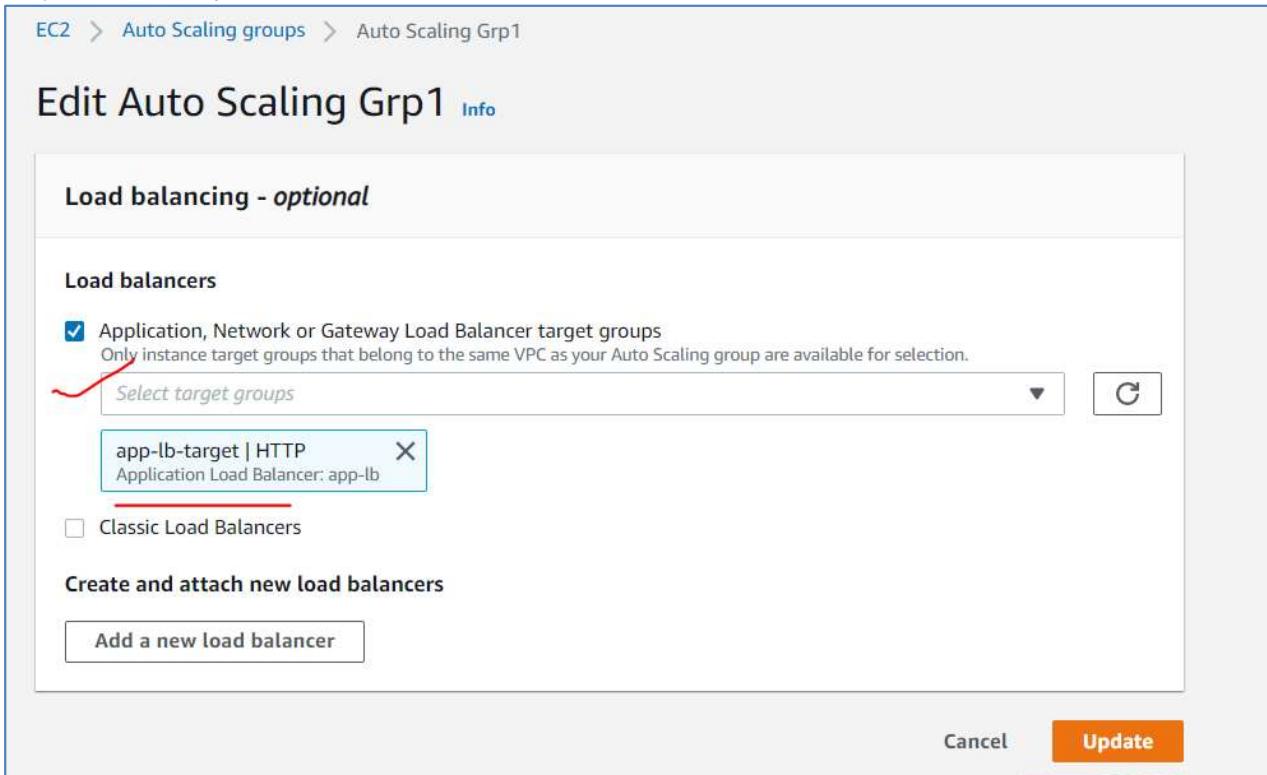


The screenshot shows the 'Load balancing' section of the AWS CloudFormation Details tab. It includes two columns: 'Load balancer target groups' and 'Classic Load Balancers'. Both columns currently show a single entry with a minus sign. In the top right corner of the section, there is an 'Edit' button, which is highlighted with a red underline.

Step 4. Under **Load balancing**, do one of the following:

- For **Application, Network or Gateway Load Balancer target groups**, select its check box and choose a target group. This is what we use here. Select the application load balancer that we created earlier.
- For **Classic Load Balancers**, select its check box and choose your load balancer.

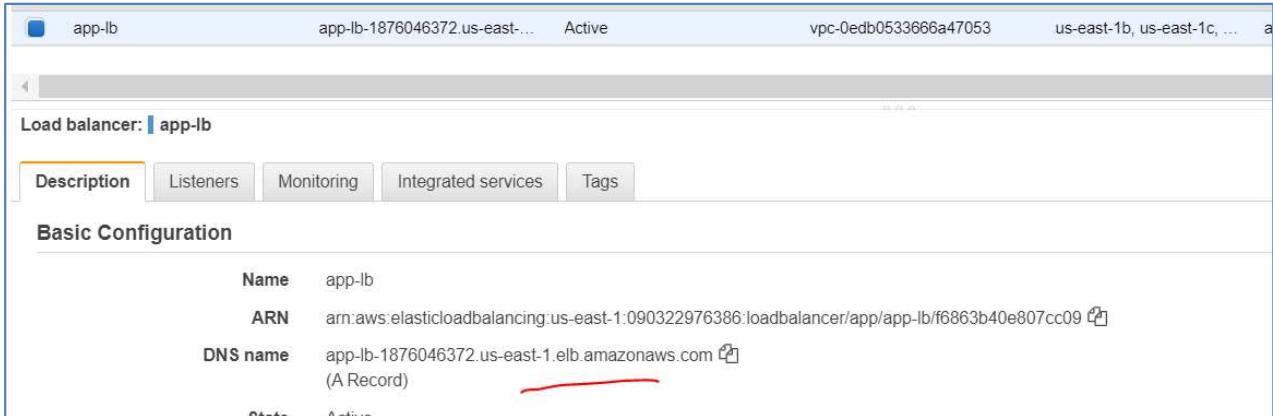
Step 5. Choose **Update**.



The screenshot shows the 'Edit Auto Scaling Grp1' page in the AWS Auto Scaling Groups section. The 'Load balancing - optional' section is expanded. Under 'Load balancers', the 'Application, Network or Gateway Load Balancer target groups' checkbox is checked and highlighted with a red underline. A dropdown menu labeled 'Select target groups' contains a single item: 'app-lb-target | HTTP' (Application Load Balancer: app-lb), which is also highlighted with a red underline. Below this, the 'Classic Load Balancers' checkbox is unchecked. At the bottom of the 'Create and attach new load balancers' section is a 'Add a new load balancer' button. At the very bottom of the page are 'Cancel' and 'Update' buttons, with the 'Update' button being highlighted with a red underline.

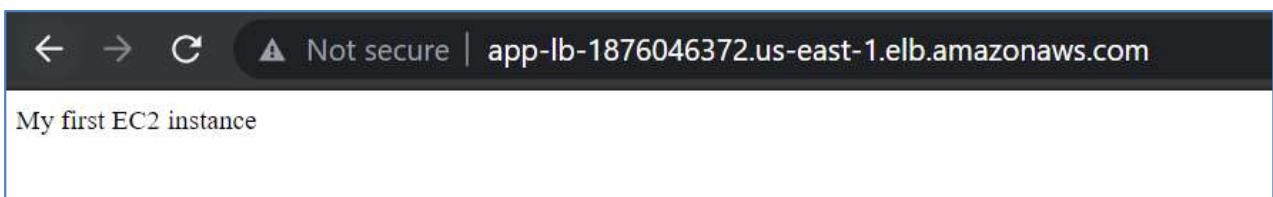
Step 6. You should be able to access your website deployed on Auto scaling group using Load Balancer

DNS as well now:



The screenshot shows the AWS Elastic Load Balancing console for a load balancer named "app-lb". The "Basic Configuration" section displays the following details:

Name	app-lb
ARN	arn:aws:elasticloadbalancing:us-east-1:090322976386:loadbalancer/app/app-lb/f6863b40e807cc09
DNS name	app-lb-1876046372.us-east-1.elb.amazonaws.com (A Record)
State	Active



The screenshot shows a web browser window with the following details:

- Address bar: Not secure | app-lb-1876046372.us-east-1.elb.amazonaws.com
- Content area: My first EC2 instance