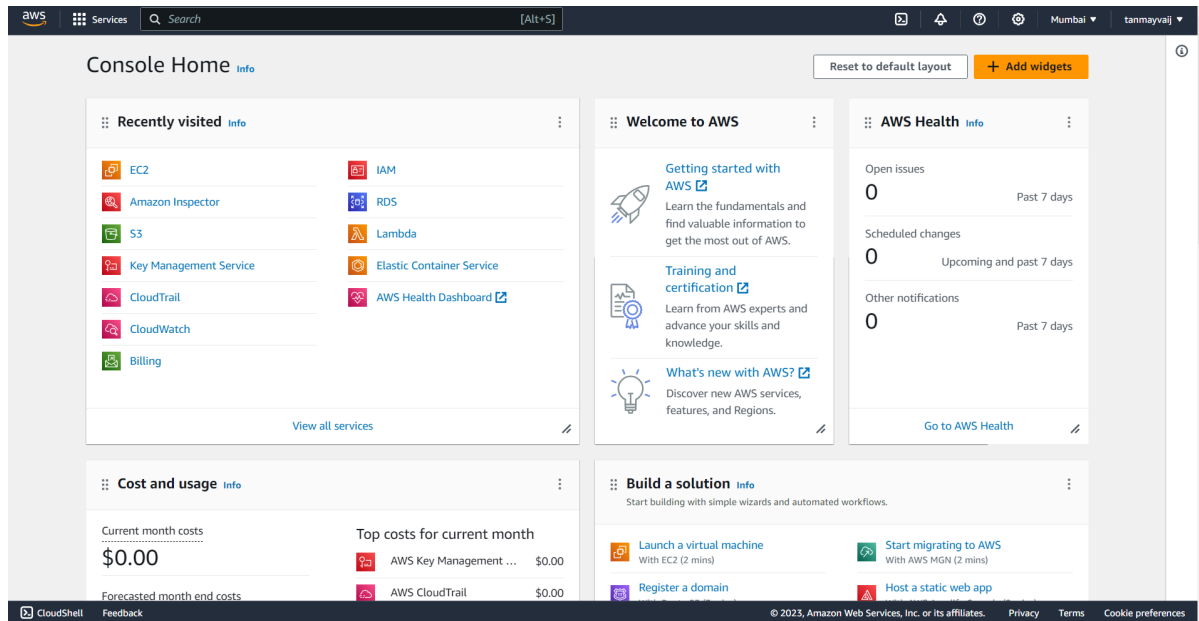
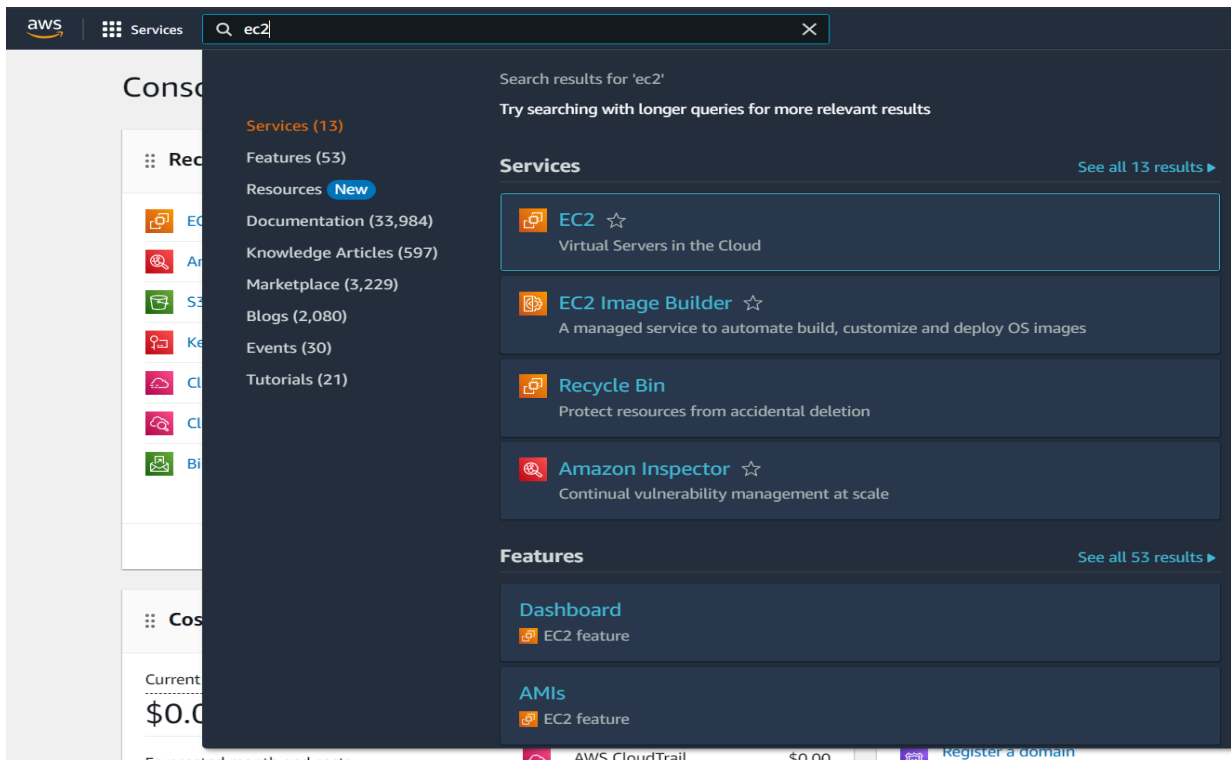


Application Load Balancer with Auto Scaling Group

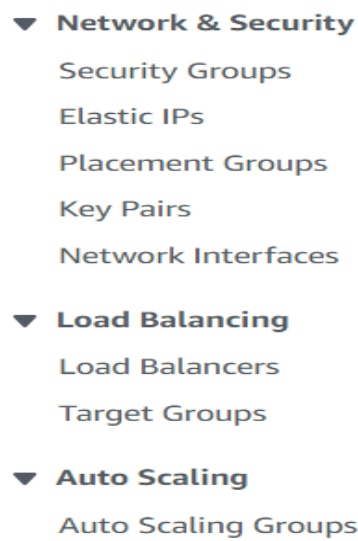
1. Sign in to the AWS Console.



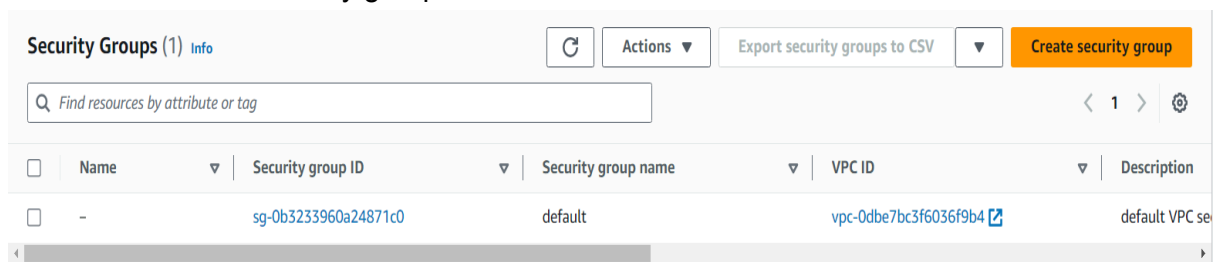
2. Search and select EC2.



3. In the side menu select “Security Groups”.



4. Click on “Create security group”.



5. Give a name and description for the load balancer security group.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

6. In the “Inbound rules” add two rules, “HTTP” and “HTTPS” and give their sources as “Anywhere”.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info
HTTP ▼	TCP	80	Anyw... ▼ Q 0.0.0.0/0 0.0.0.0/0 ✕
HTTPS ▼	TCP	443	Anyw... ▼ Q 0.0.0.0/0 0.0.0.0/0 ✕
<button>Add rule</button>			

7. Now create a security group for the launch template.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

8. Add SSH and set its source as “Anywhere”, then add HTTP and HTTPS and set their source as the security group of the load balancer.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info
SSH ▼	TCP	22	Anyw... ▼ <div><div>0.0.0.0/0</div><div>0.0.0.0/0 ✕</div></div>
HTTP ▼	TCP	80	Custom ▼ <div><div>sg-0485b6e21070796: ✕</div><div>sg-0485b6e2107079698 ✕</div></div>
HTTPS ▼	TCP	443	Custom ▼ <div><div>sg-0485b6e21070796: ✕</div><div>sg-0485b6e2107079698 ✕</div></div>

Add rule

9. Now, from the side menu click on “Launch Templates”

- ▼ **Instances**
- Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

[New](#)

10. Give a name and description to the launch template.

Launch template name and description

Launch template name - *required*

my-lt

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description

a launch template

Max 255 chars

11. Select “Ubuntu” as the OS Image.

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Don't include in launch template

Amazon Linux

macOS

Ubuntu

Windows

Red H

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

ami-0287a05f0ef0e9d9a (64-bit (x86)) / ami-0b6581fde9e6e7779 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-09-19

Architecture

AMI ID

Verified provider

64-bit (x86) ▼

ami-0287a05f0ef0e9d9a

Verified provider

12. Select “t2.micro” as the instance type.

▼ Instance type [Info](#)

Advanced

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0724 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour

☒ All generations
[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

13. Select a key pair name or create if it doesn't exist.

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name

root

[Create new key pair](#)

14. Select the security group created for the launch template.

▼ Network settings [Info](#)

Subnet [Info](#)

Don't include in launch template

[Create new subnet](#)

When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Select existing security group

☐ Create security group

Security groups [Info](#)

Select security groups

my-lt-grp sg-0193aa1357ffc9995 ✕
VPC: vpc-0dbe7bc3f6036f9b4

[Compare security group rules](#)

► Advanced network configuration

15. Now click on advance settings, and scroll down till end, and add the following code. Then click on “Create launch template”.

```
#!/bin/bash
sudo apt update -y
sudo apt install apache2 -y
sudo echo "<h1>Instance $(hostname -f)</h1>" | sudo tee
/var/www/html/index.html
```

16. Inside the menu, click on the target group and then click on “Create target group”.

Target groups [Info](#)

Actions ▾

Create target group

Q Filter target groups

< 1 > ⚙

	Name ▾	ARN ▾	Port ▾	Protocol ▾	Target type ▾	Load balancer ▾
<div>No target groups</div> <div>You don't have any target groups in ap-south-1</div> <div>Create target group</div>						

17. Choose “Instances” as the target type and give a name to the target group. Then click next and click on “Create target group”.

Basic configuration

Settings in this section can't be changed after the target group is created.

Choose a target type

☒ Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

☐ IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

☐ Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

☐ Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

my-tg

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

18. Now in the side menu click on load balancers, and then click on “Create load balancer”.

Load balancers

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Actions

Create load balancer

< 1 >

	Name	DNS name	State	VPC ID	Availability Zones	Type	Date
No load balancers							
You don't have any load balancers in ap-south-1							
<div>Create load balancer</div>							

19. Give a name to the load balancer.

Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

my-lb

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

20. Select at least 2 zones.

Mappings Info

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones or the VPC are not available for selection.

☒ ap-south-1a (aps1-az1)

Subnet

subnet-0e7d41dc412c388cd

IPv4 address

Assigned by AWS

☒ ap-south-1b (aps1-az3)

Subnet

subnet-040e0fac65e6a4617

IPv4 address

Assigned by AWS

☒ ap-south-1c (aps1-az2)

Subnet

subnet-018c2b387a7b91b47

IPv4 address

Assigned by AWS

21. Select the security group created for load balancer.

Security groups Info

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

Security groups

Select up to 5 security groups

default
sg-0b3233960a24871c0 VPC: vpc-0dbe7bc3f6036f9b4

my-lb-grp
sg-0485b6e2107079698 VPC: vpc-0dbe7bc3f6036f9b4

22. Here select the target group which we created already and at the end click on “Create load balancer”.

Default action [Info](#)

Forward to	my-tg Target type: Instance, IPv4	HTTP ▼	
------------	--------------------------------------	--------	---

[Create target group](#) 

23. Then in the side menu click on Auto Scaling Group, give a name and select the launch template which we created previously.


Name


Auto Scaling group name
Enter a name to identify the group.

Must be unique to this account in the current Region and no more than 255 characters.

Launch template [Info](#) [Switch to launch configuration](#)

Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

 ▼ 

[Create a launch template](#) 

24. Select all the 3 zones and then click on “Next”.

Network [Info](#)

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC
Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-0dbe7bc3f6036f9b4
172.31.0.0/16 Default

↻

[Create a VPC](#)

Availability Zones and subnets
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

↻

ap-south-1c | subnet-018c2b387a7b91b47 ✕
172.31.16.0/20 Default

ap-south-1b | subnet-040e0fac65e6a4617 ✕
172.31.0.0/20 Default

ap-south-1a | subnet-0e7d41dc412c388cd ✕
172.31.32.0/20 Default

[Create a subnet](#)

25. Select “Attach to an existing load balancer” and select the load balancer.

Load balancing [Info](#)

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

☐ **No load balancer**
Traffic to your Auto Scaling group will not be fronted by a load balancer.

☒ **Attach to an existing load balancer**
Choose from your existing load balancers.

☐ **Attach to a new load balancer**
Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to an existing load balancer
Select the load balancers that you want to attach to your Auto Scaling group.

☒ **Choose from your load balancer target groups**
This option allows you to attach Application, Network, or Gateway Load Balancers.

☐ **Choose from Classic Load Balancers**

Existing load balancer target groups
Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups

↻

my-tg | HTTP ✕
Application Load Balancer: my-lb

26. Turn on Elastic Load Balancing health checks, and set the Health check grace period to 60 seconds.

Health checks

Health checks increase availability by replacing unhealthy instances. When you use multiple health checks, all are evaluated, and if at least one fails, instance replacement occurs.

EC2 health checks

[Always enabled](#)

Additional health check types - *optional* [Info](#)

☒ Turn on Elastic Load Balancing health checks **Recommended**

Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto Scaling can replace it on its next periodic check.

[EC2 Auto Scaling will start to detect and act on health checks performed by Elastic Load Balancing. To avoid unexpected terminations, first verify the settings of these health checks in the \[Load Balancer console\]\(#\)](#)

Health check grace period [Info](#)

This time period delays the first health check until your instances finish initializing. It doesn't prevent an instance from terminating when placed into a non-running state.

seconds

27. Set the “Max desired capacity” to 4. Select a target tracking scaling policy with the metric type: Average CPU utilisation. Set target value to 30 and instance warmup to 60 seconds. Then click on “Create auto scaling group”.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity	Max desired capacity
<input type="text" value="1"/>	<input type="text" value="4"/>
Equal or less than desired capacity	Equal or greater than desired capacity

Automatic scaling - *optional*

Choose whether to use a target tracking policy [Info](#)

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

☐ No scaling policies

Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

☒ Target tracking scaling policy

Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

Scaling policy name

Metric type [Info](#)

Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Target value

Instance warmup [Info](#)

seconds

28. An instance will start running after creating auto scaling group, connect to the instance and fire the command “sudo apt update -y && sudo apt install stress -y && sudo stress --cpu 8 --timeout 200”.

```

aws | Services | Search | [Alt+S]
* Support: https://ubuntu.com/advantage

System information as of Thu Nov 23 09:24:46 UTC 2023

System load: 0.0          Processes:           102
Usage of /: 23.3% of 7.57GB Users logged in:      0
Memory usage: 23%        IPv4 address for eth0: 172.31.8.132
Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

63 updates can be applied immediately.
39 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

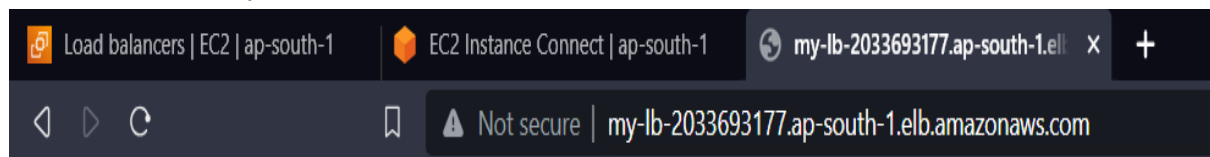
ubuntu@ip-172-31-8-132:~$ sudo apt update -y && sudo apt install stress -y && sudo stress --cpu 8 --timeout 200

```

29. After a few minutes all the 4 instances will start running due to stress.

Instances (4) Info								
Find Instance by attribute or tag (case-sensitive)								
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input type="checkbox"/>		i-000bafaa10741d28f	Running	t2.micro	Initializing	No alarms	ap-south-1b	ec2-3-110-54-25
<input type="checkbox"/>		i-0e4e83294449ec98f	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1b	ec2-65-2-3-243.z
<input type="checkbox"/>		i-010776f00ba18a21c	Running	t2.micro	Initializing	No alarms	ap-south-1a	ec2-13-233-18-2
<input type="checkbox"/>		i-0c631edea8d3b5fb0	Running	t2.micro	Initializing	No alarms	ap-south-1a	ec2-15-206-28-1

30. Then put the load balancer dns name in the browser and it will start showing different ip addresses on every reload.



Instance ip-172-31-44-244.ap-south-1.compute.internal