Little bit advanced labs - part 1

Part 1: EC2 with ELB and ASG

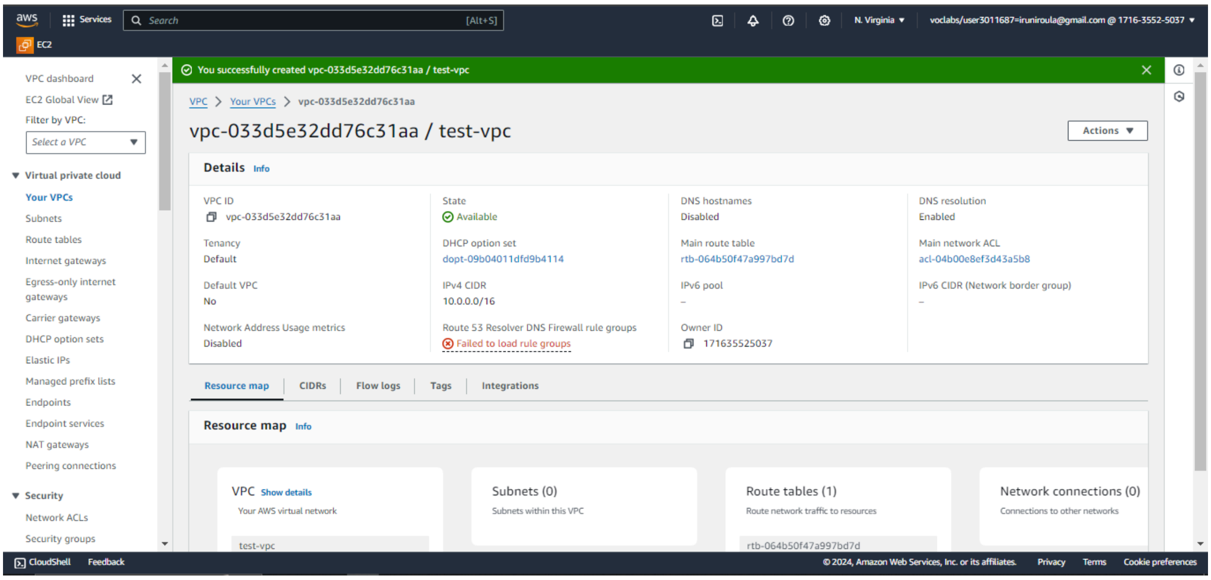
Objective: Learn how to create a scalable and highly available web application environment using Amazon EC2 instances, ELB, and ASG.

Approach:

1. **Launch EC2 Instances**: Start by launching two or more EC2 instances. These instances will run a simple web application (e.g., a "Hello World" page or any basic web service).
2. **Configure Load Balancer**: Set up an Elastic Load Balancer (ELB) to distribute incoming web traffic across your EC2 instances. This step ensures high availability and fault tolerance.
3. **Set Up Auto Scaling Group (ASG)**: Create an ASG that uses the launched EC2 instances. Configure ASG policies to automatically scale the number of instances up or down based on criteria like CPU usage or network traffic.
4. **Test Your Setup**: Simulate traffic to test the scaling policies and the load balancer. Observe how ASG adds or removes instances and how ELB distributes traffic.
5. **Verify Website Functionality**: Ensure that the website hosted on EC2 instances remains accessible and functional during scaling operations.

Goal: By the end of this lab, students will have a hands-on understanding of setting up a load-balanced and auto-scaled web application using AWS services.

Created a VPC



You successfully created vpc-033d5e32dd76c31aa / test-vpc

VPC > Your VPCs > vpc-033d5e32dd76c31aa

vpc-033d5e32dd76c31aa / test-vpc

Details Info

VPC ID: vpc-033d5e32dd76c31aa

State: Available

DNS hostnames: Disabled

DNS resolution: Enabled

Tenancy: Default

DHCP option set: dopt-09b04011dfd9b4114

Main route table: rtb-064b50f47a997bd7d

Main network ACL: acl-04b00e8ef3d43a5b8

Default VPC: No

IPv4 CIDR: 10.0.0.0/16

IPv6 pool: –

IPv6 CIDR (Network border group): –

Network Address Usage metrics: Disabled

Route 53 Resolver DNS Firewall rule groups: Failed to load rule groups

Owner ID: 171635525037

Resource map Info

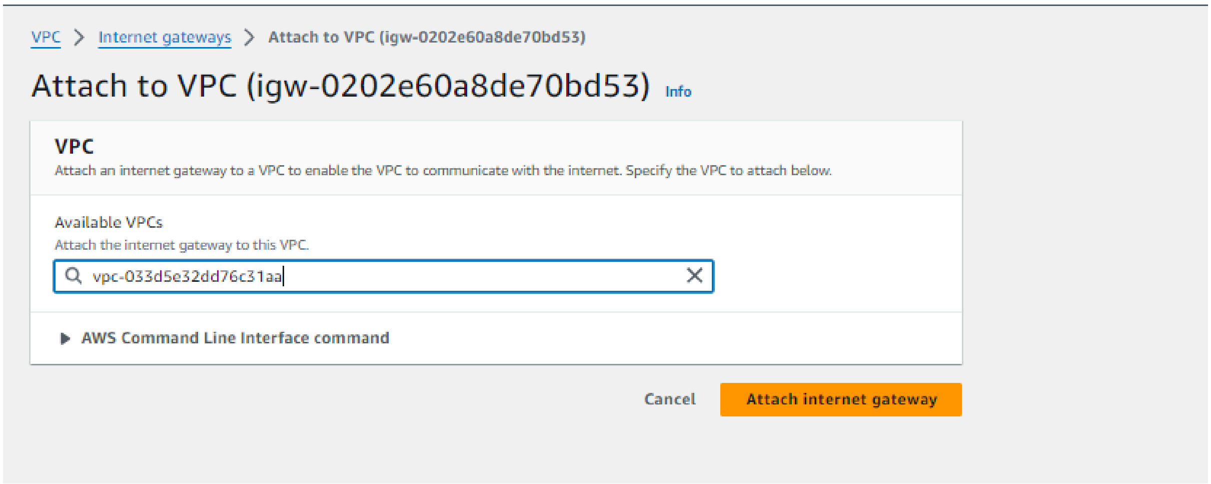
VPC Show details — Your AWS virtual network: test-vpc

Subnets (0) — Subnets within this VPC

Route tables (1) — Route network traffic to resources: rtb-064b50f47a997bd7d

Network connections (0) — Connections to other networks

Created an internet gateway and attached to the VPC created earlier



VPC > Internet gateways > Attach to VPC (igw-0202e60a8de70bd53)

Attach to VPC (igw-0202e60a8de70bd53) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

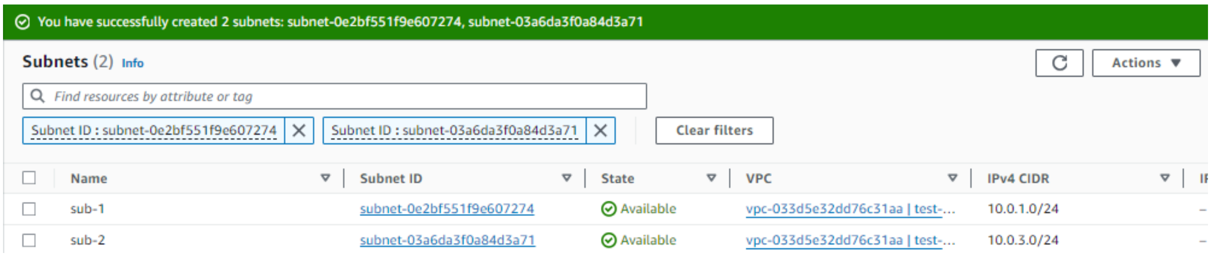
Available VPCs

Attach the internet gateway to this VPC.

vpc-033d5e32dd76c31aa

▶ AWS Command Line Interface command
Cancel
Attach internet gateway

Two subnets created



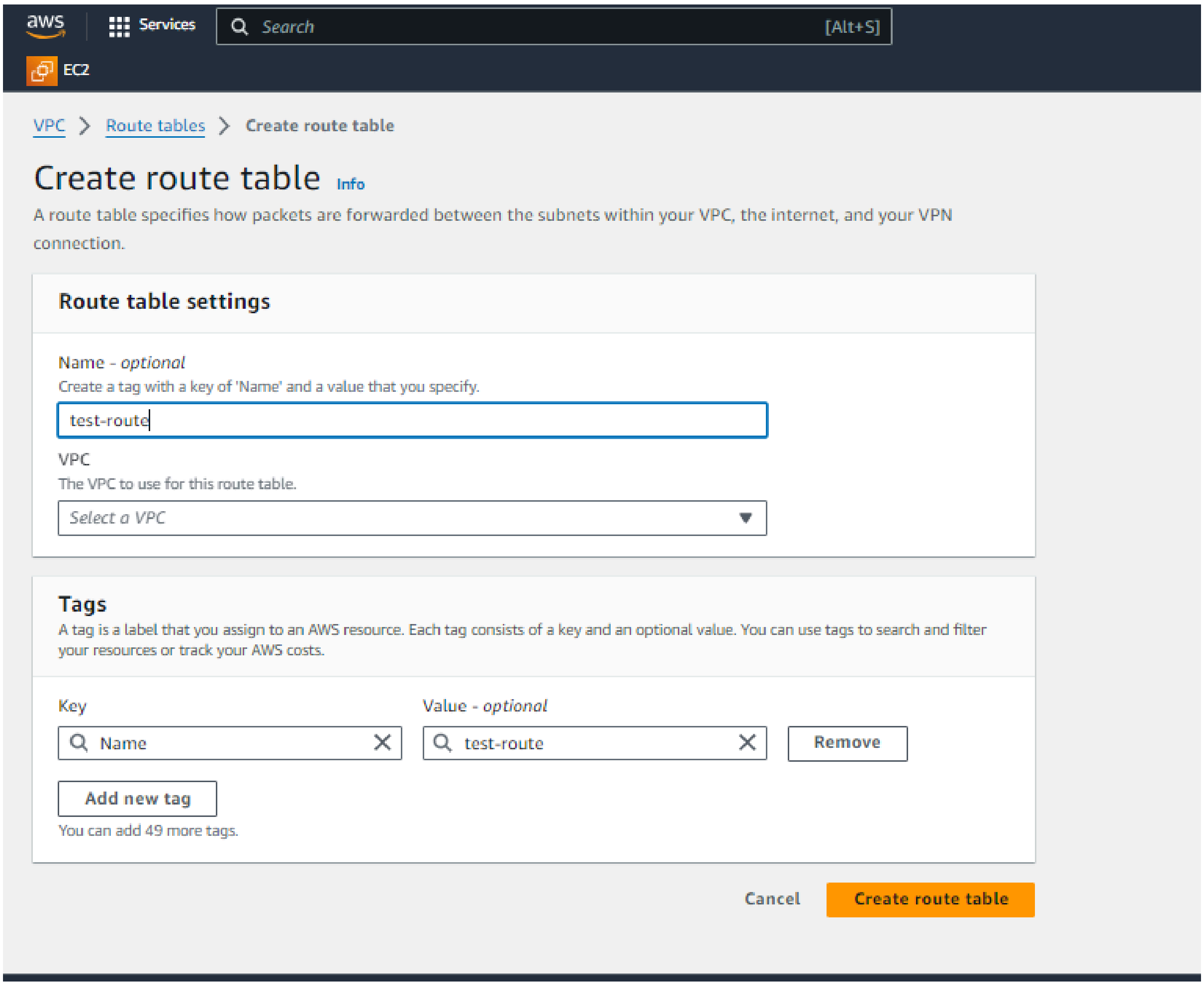
You have successfully created 2 subnets: subnet-0e2bf551f9e607274, subnet-03a6da3f0a84d3a71

Subnets (2) Info

Subnet ID : subnet-0e2bf551f9e607274 ✕ Subnet ID : subnet-03a6da3f0a84d3a71 ✕ Clear filters

□	Name	Subnet ID	State	VPC	IPv4 CIDR	IF
□	sub-1	subnet-0e2bf551f9e607274	✓ Available	vpc-033d5e32dd76c31aa | test-...	10.0.1.0/24	–
□	sub-2	subnet-03a6da3f0a84d3a71	✓ Available	vpc-033d5e32dd76c31aa | test-...	10.0.3.0/24	–

Create Route Table



VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
test-route

VPC
The VPC to use for this route table.
Select a VPC

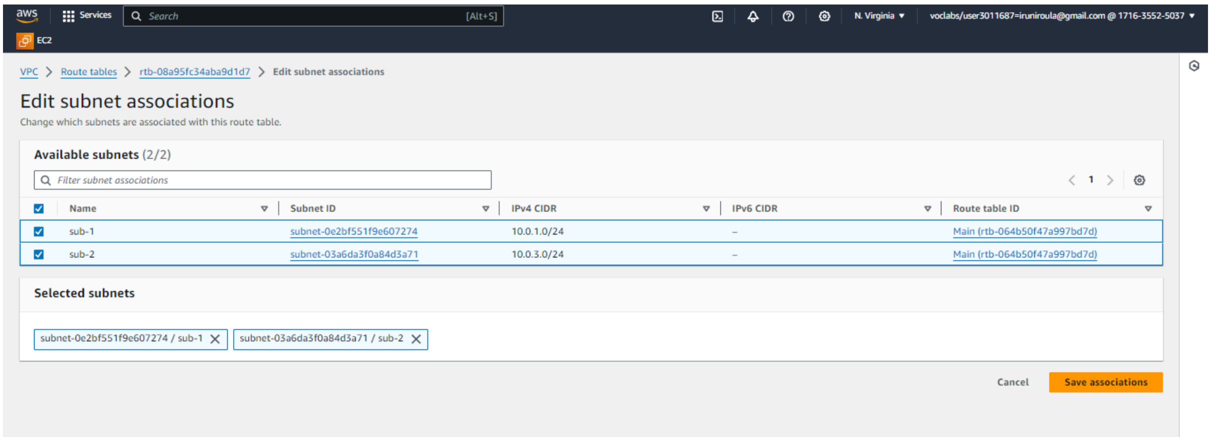
Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	test-route	Remove

Add new tag
You can add 49 more tags.

Edit subnet associations for the route table



VPC > Route tables > rtb-08a95fc34aba9d1d7 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/2)

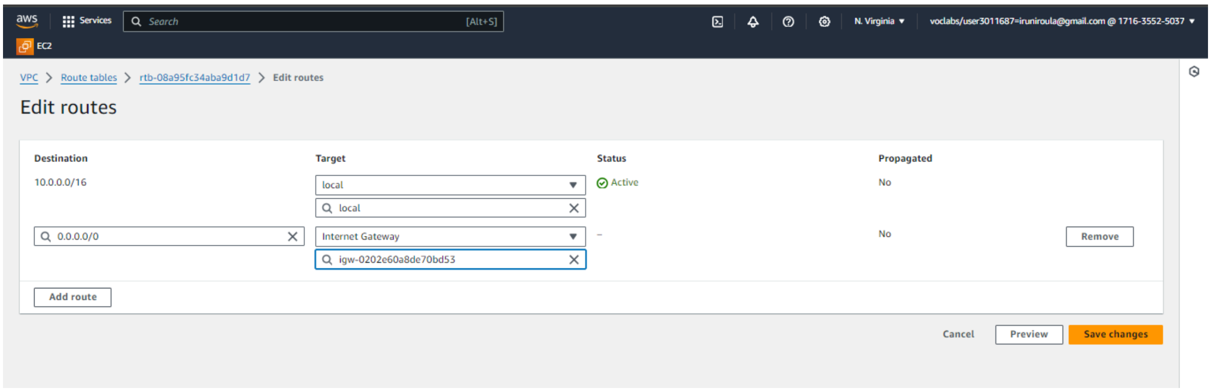
Filter subnet associations

☑	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	sub-1	subnet-0e2bf551f9e607274	10.0.1.0/24	–	Main (rtb-064b50f47a997bd7d)
☑	sub-2	subnet-03a6da3f0a84d3a71	10.0.3.0/24	–	Main (rtb-064b50f47a997bd7d)

Selected subnets

subnet-0e2bf551f9e607274 / sub-1 ✕ subnet-03a6da3f0a84d3a71 / sub-2 ✕

Edit routes

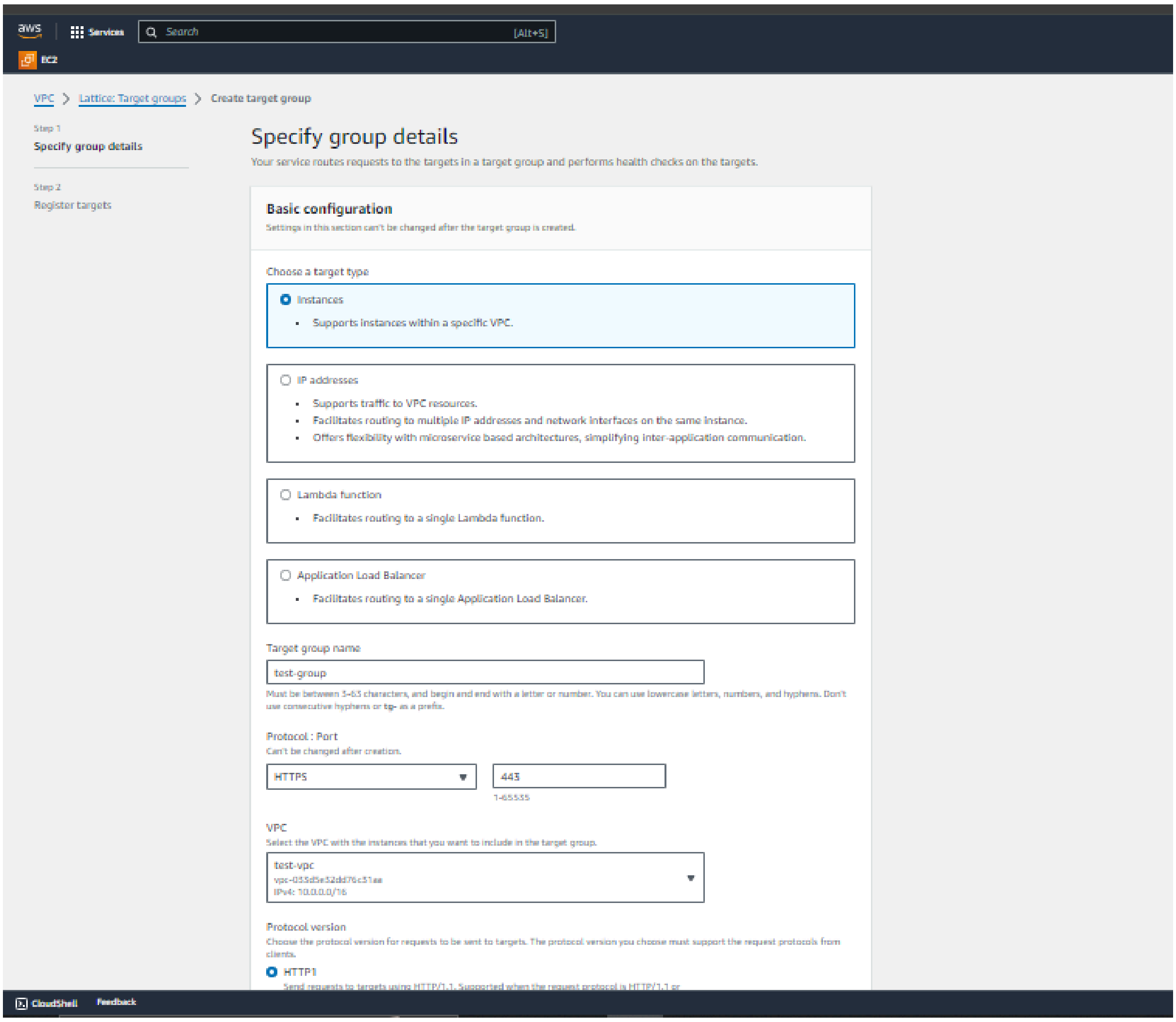

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3011687=iruniroula@gmail.com @ 1716-3552-5037
EC2
VPC > Route tables > rtb-08a95fc34aba9d1d7 > Edit routes

Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/16	local local	Active	No	
0.0.0.0/0	Internet Gateway igw-0202e60a8de70bd53	-	No	Remove

Add route
Cancel
Preview
Save changes

Create target group



Specify group details

Your service routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

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

Choose a target type

● Instances
- Supports instances within a specific VPC.

○ IP addresses
- Supports traffic to VPC resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.

○ Lambda function
- Facilitates routing to a single Lambda function.

○ Application Load Balancer
- Facilitates routing to a single Application Load Balancer.

Target group name

test-group

Must be between 3-63 characters, and begin and end with a letter or number. You can use lowercase letters, numbers, and hyphens. Don't use consecutive hyphens or tg- as a prefix.

Protocol : Port

Can't be changed after creation.

HTTPS ▼ 443

1-65535

VPC

Select the VPC with the instances that you want to include in the target group.

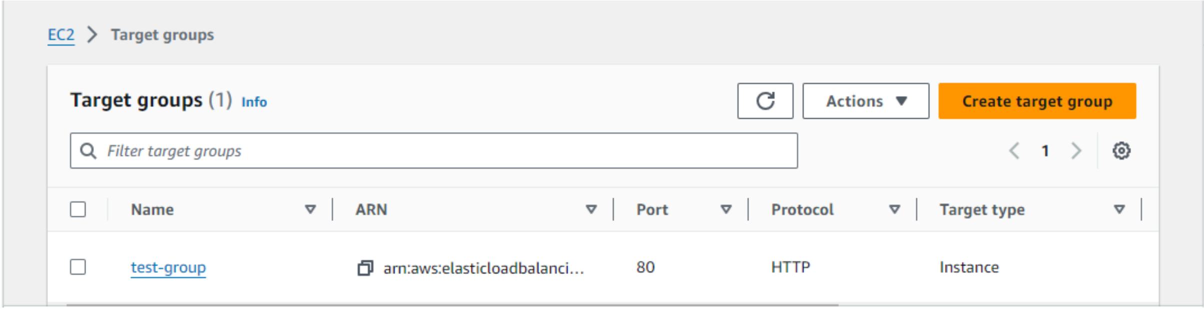
test-vpc
vpc-033d5e32dd76c31ae
IPv4: 10.0.0.0/16

Protocol version

Choose the protocol version for requests to be sent to targets. The protocol version you choose must support the request protocols from clients.

● HTTP1

Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or



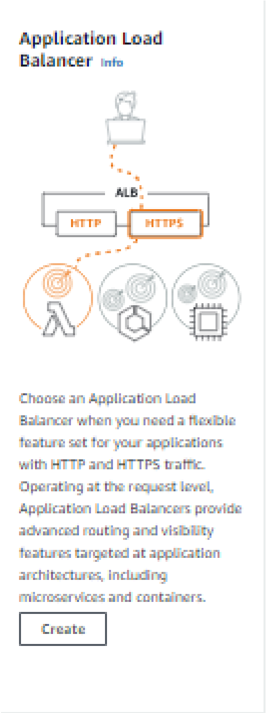
EC2 > Target groups

Target groups (1) Info

Filter target groups

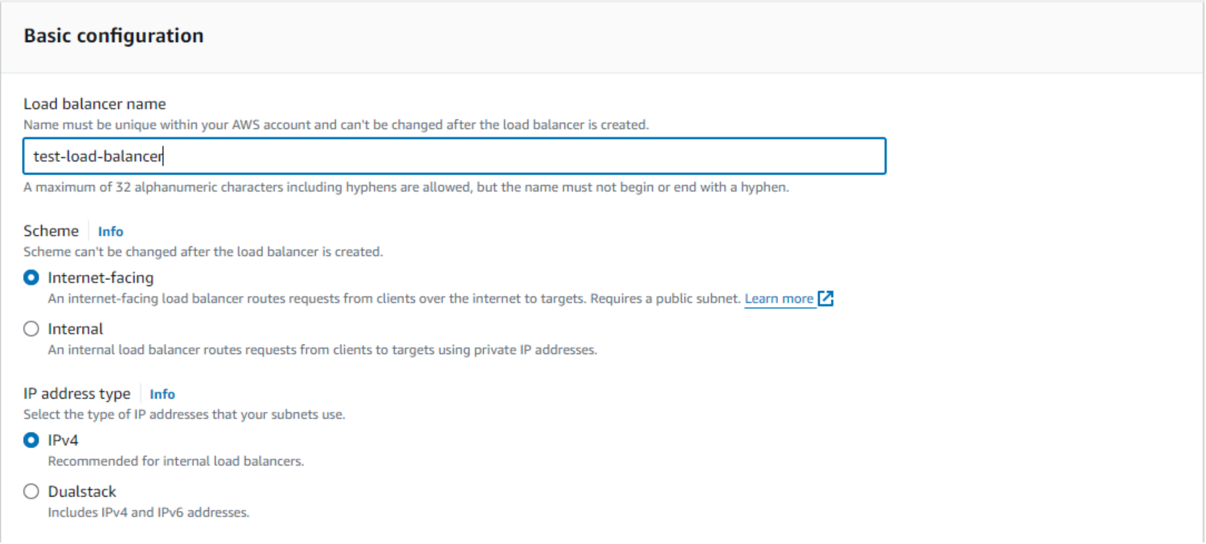
☐	Name	ARN	Port	Protocol	Target type
☐	test-group	arn:aws:elasticloadbalanci...	80	HTTP	Instance

Create Application Load Balancer



Application Load Balancer Info

Choose an Application Load Balancer when you need a flexible feature set for your 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.



Basic configuration

Load balancer name

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

test-load-balancer

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

Scheme | Info

Scheme can't be changed after the load balancer is created.

● Internet-facing

An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more

○ Internal

An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type | Info

Select the type of IP addresses that your subnets use.

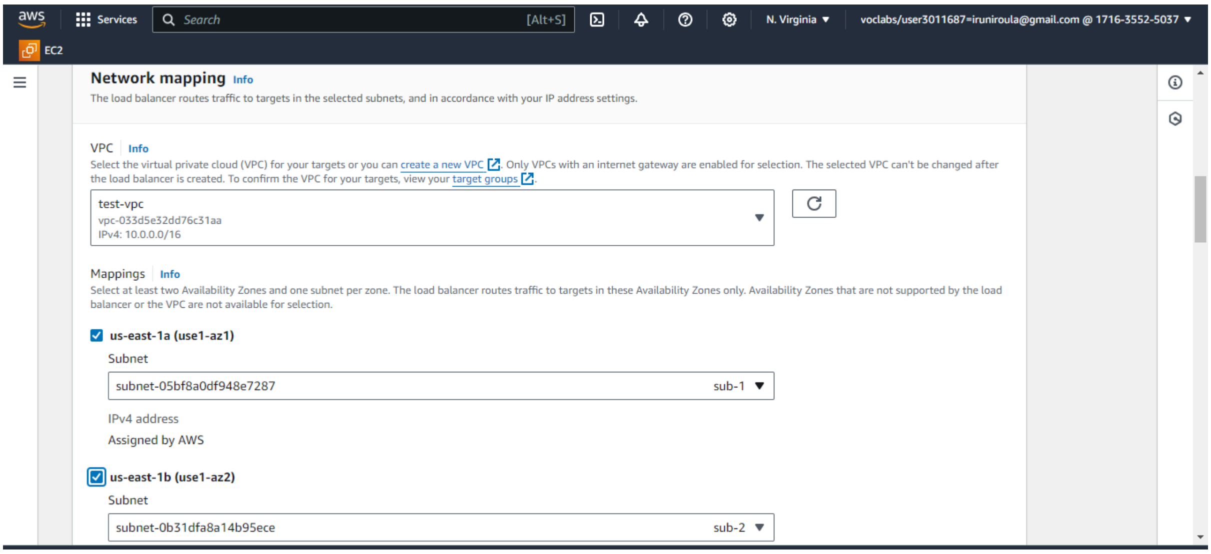
● IPv4

Recommended for internal load balancers.

○ Dualstack

Includes IPv4 and IPv6 addresses.

Configure Application Load Balancer as follows:



Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC | Info

Select the virtual private cloud (VPC) for your targets or you can create a new VPC. Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups.

test-vpc
vpc-033d5e32dd76c31aa
IPv4: 10.0.0.0/16

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 that are not supported by the load balancer or the VPC are not available for selection.

☑ us-east-1a (use1-az1)

Subnet

subnet-05bf8a0df948e7287 sub-1 ▼

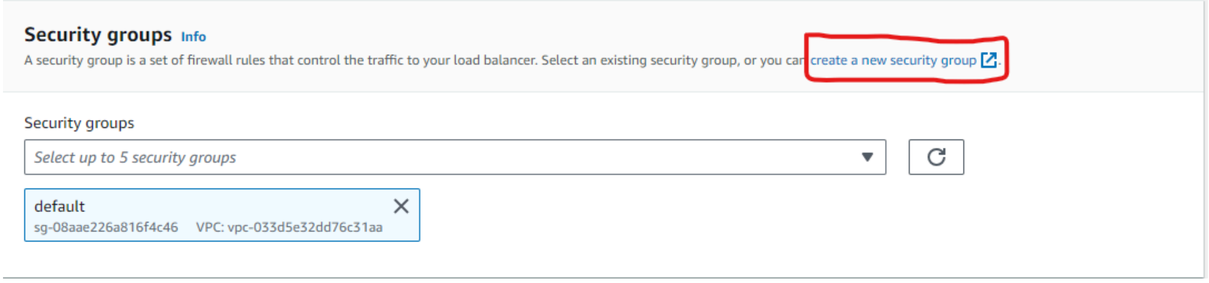
IPv4 address

Assigned by AWS

☑ us-east-1b (use1-az2)

Subnet

subnet-0b31dfa8a14b95ece sub-2 ▼



Security groups Info

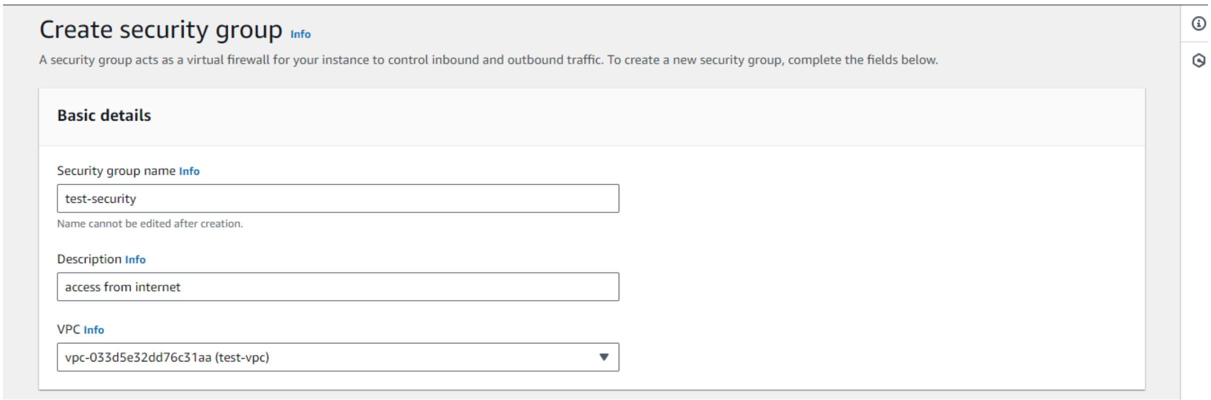
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups

Select up to 5 security groups ▼

default ✕
sg-08aae226a816f4c46 VPC: vpc-033d5e32dd76c31aa

Create security group to enable http access



Create security group Info

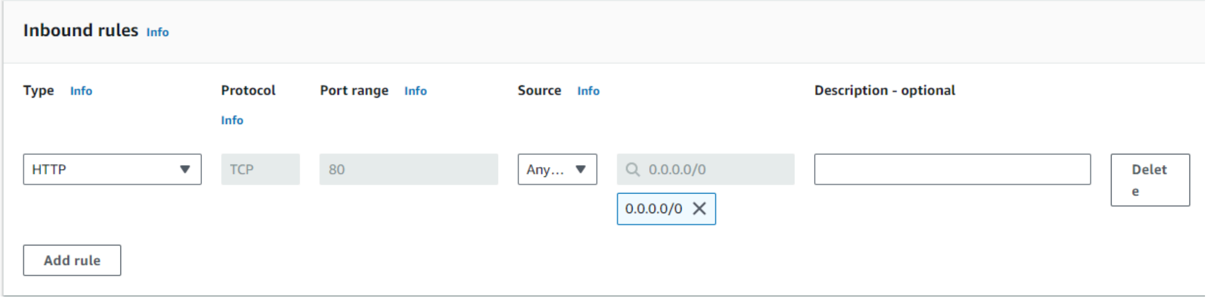
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info
test-security
Name cannot be edited after creation.

Description Info
access from internet

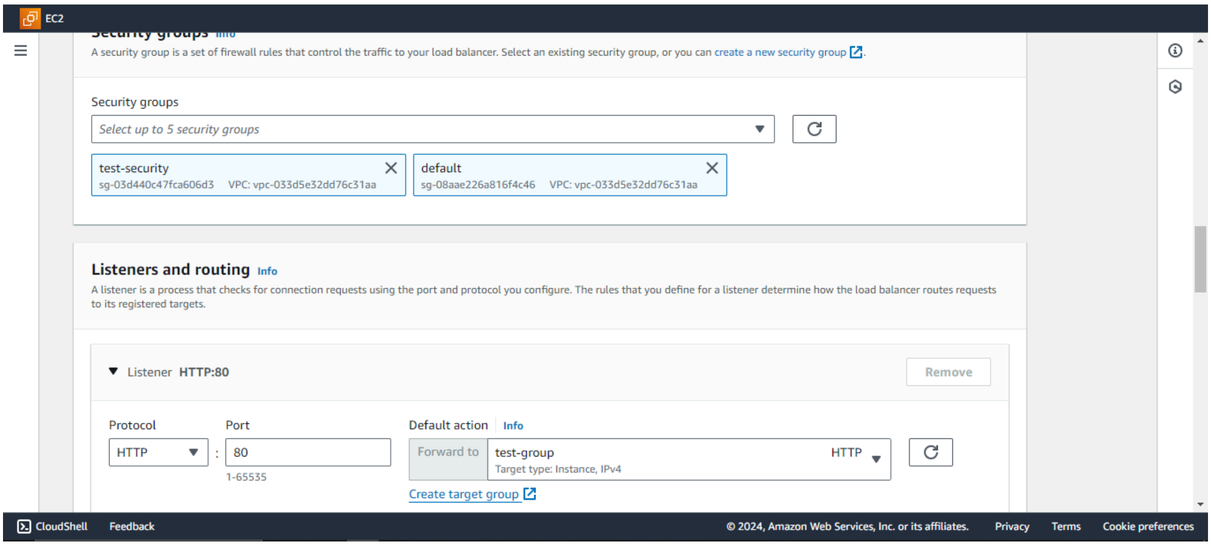
VPC Info
vpc-033d5e32dd76c31aa (test-vpc)



Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional
HTTP	TCP	80	Any…	0.0.0.0/0 0.0.0.0/0	

Select target group created



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

test-security
sg-03d440c47fca606d3 VPC: vpc-033d5e32dd76c31aa

default
sg-08aae226a816f4c46 VPC: vpc-033d5e32dd76c31aa

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

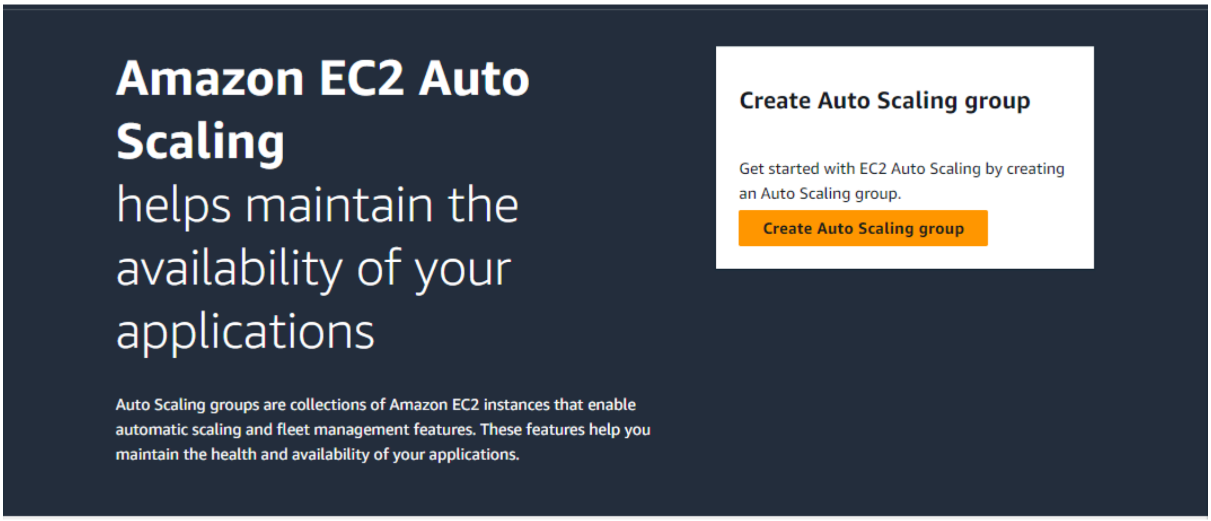
▼ Listener HTTP:80

Protocol: HTTP
Port: 80
1-65535

Default action Info
Forward to test-group HTTP
Target type: Instance, IPv4

Create target group

Click on Create Auto scaling group by navigating to EC2 dashboard and selecting ASG



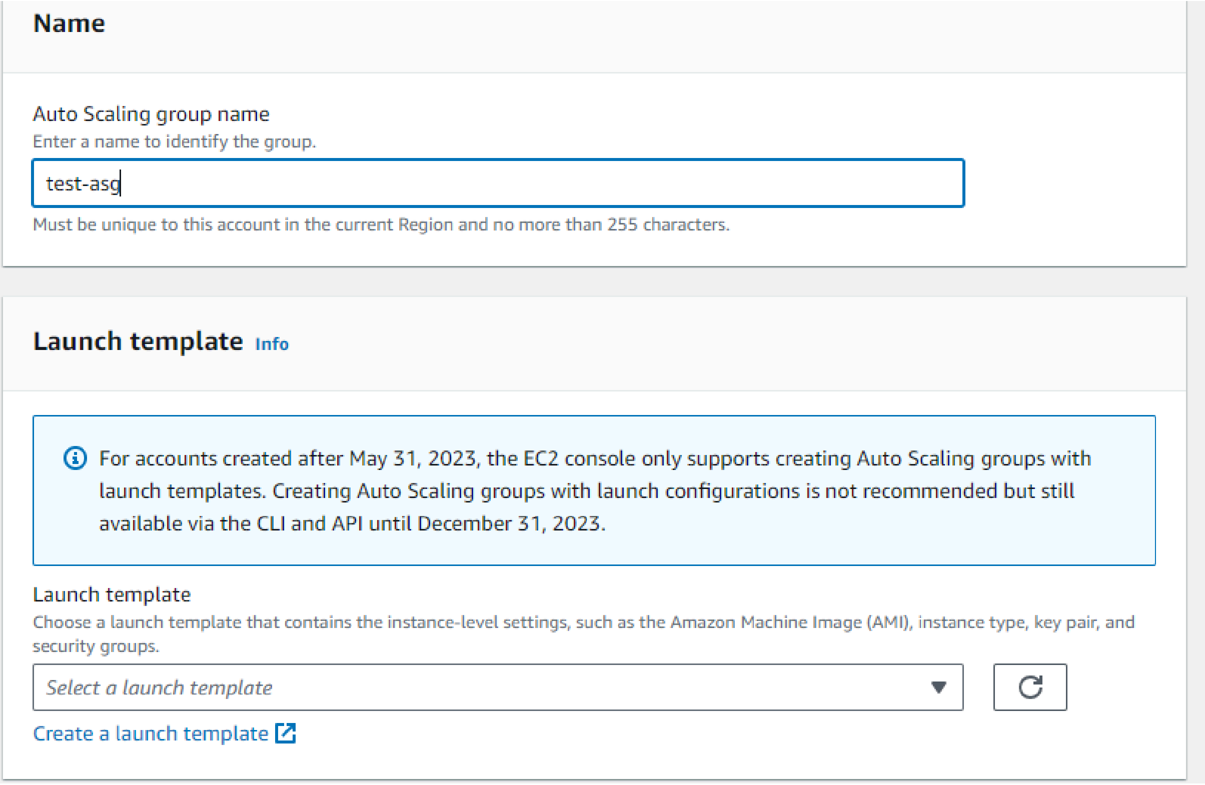
Amazon EC2 Auto Scaling helps maintain the availability of your applications

Auto Scaling groups are collections of Amazon EC2 instances that enable automatic scaling and fleet management features. These features help you maintain the health and availability of your applications.

Create Auto Scaling group

Get started with EC2 Auto Scaling by creating an Auto Scaling group.

Configure Auto Scaling Group



Name

Auto Scaling group name

Enter a name to identify the group.

test-asg

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

Launch template Info

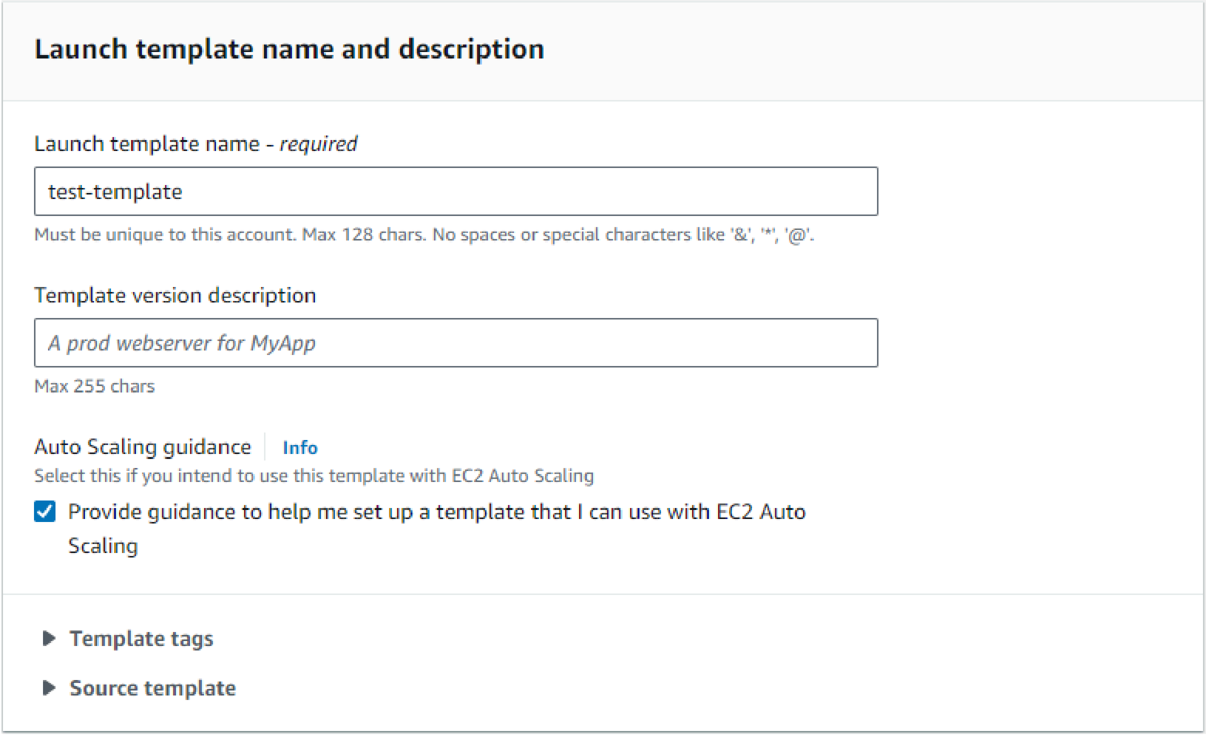
For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

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.

Select a launch template

Create Launch Template



Launch template name and description

Launch template name - *required*

test-template

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

Template version description

A prod webserver for MyApp

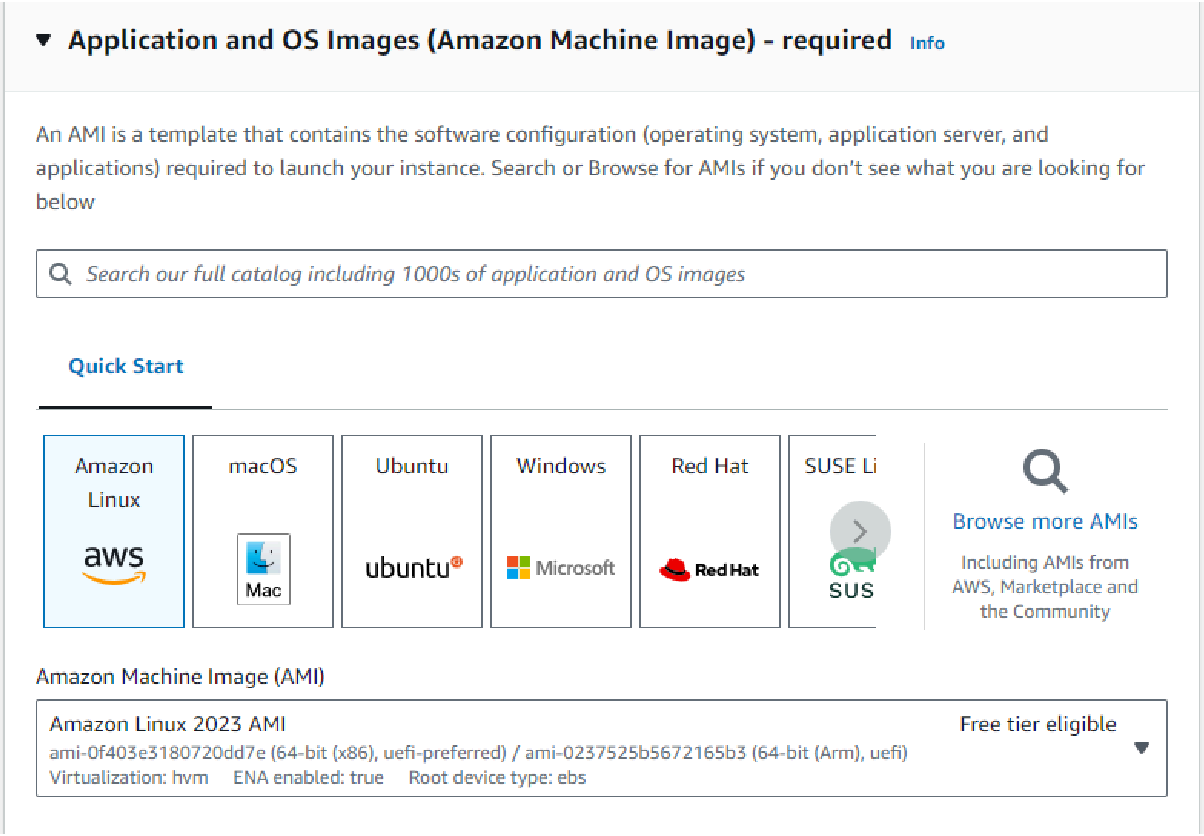
Max 255 chars

Auto Scaling guidance | Info

Select this if you intend to use this template with EC2 Auto Scaling

☑ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

Configure launch template by selecting appropriate settings

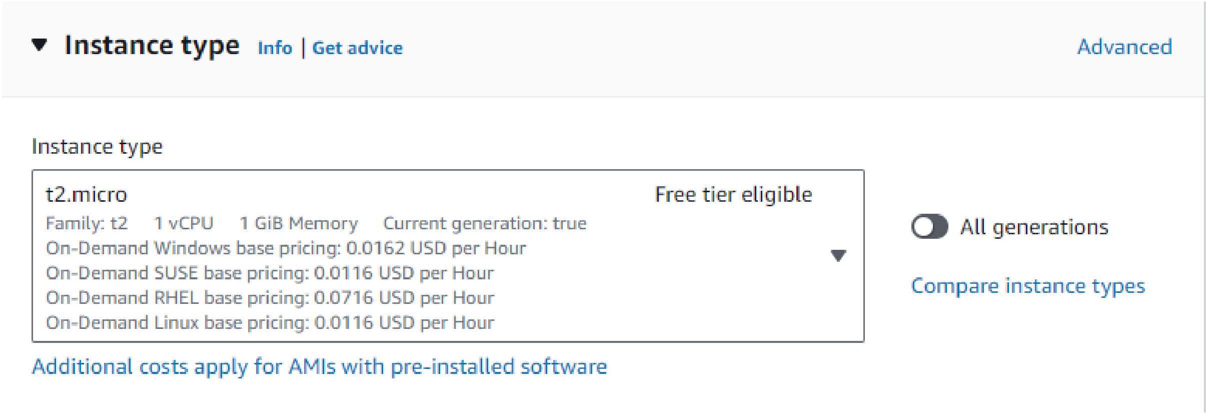

▼ Application and OS Images (Amazon Machine Image) - required
Info

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

Search our full catalog including 1000s of application and OS images
Quick Start
Amazon Linux
aws
macOS
Mac
Ubuntu
ubuntu
Windows
Microsoft
Red Hat
Red Hat
SUSE Li
SUS
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

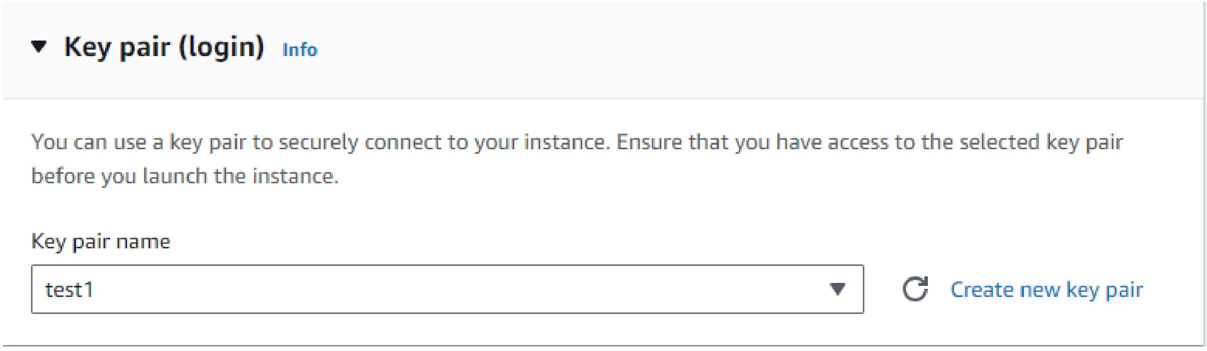
Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-0f403e3180720dd7e (64-bit (x86), uefi-preferred) / ami-0237525b5672165b3 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs



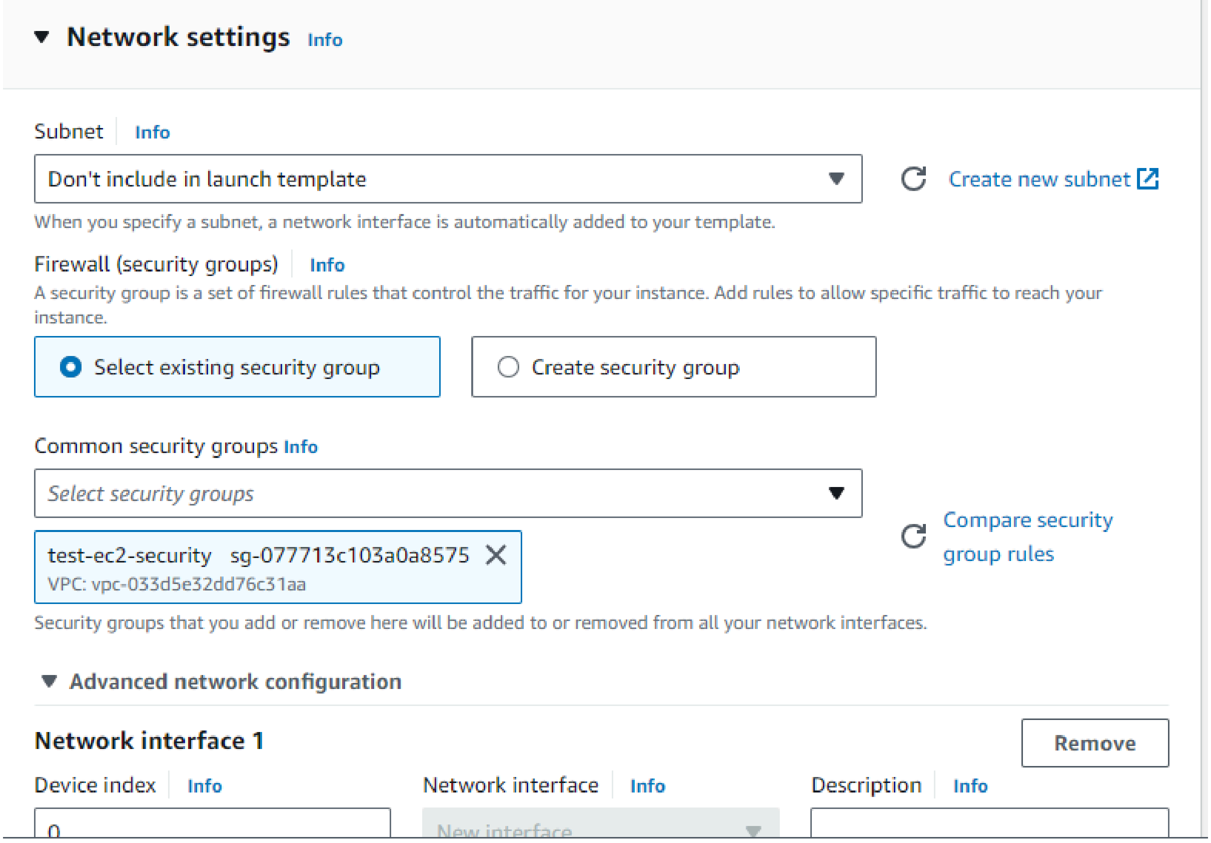
Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour



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: test1



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

Common security groups Info

Select security groups

test-ec2-security sg-077713c103a0a8575
VPC: vpc-033d5e32dd76c31aa

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Advanced network configuration

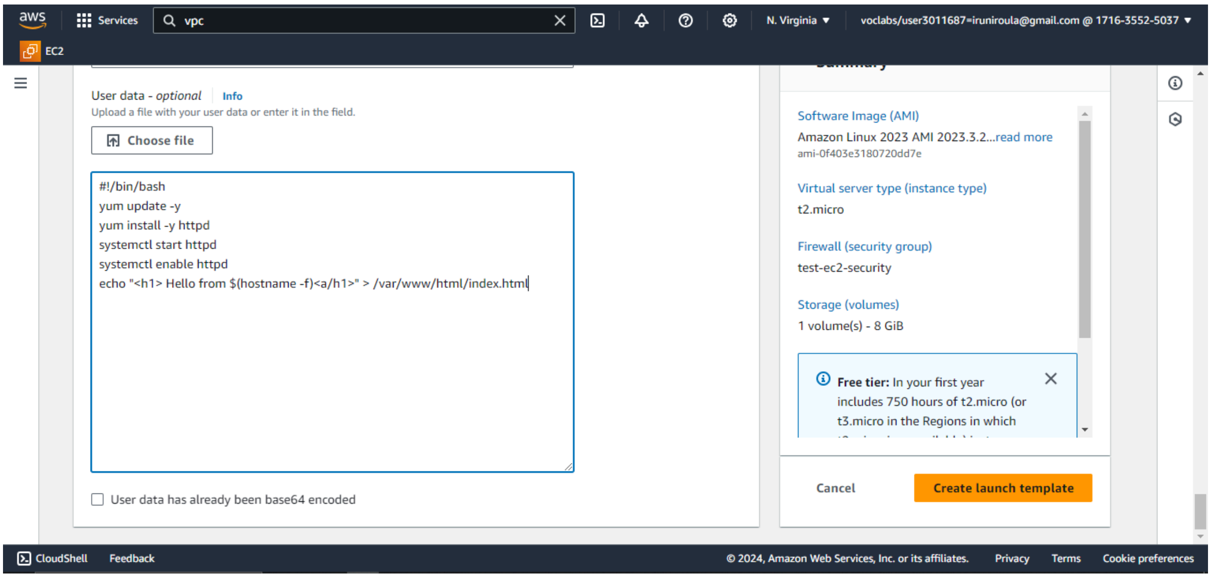
Network interface 1

Remove

Device index | Info: 0

Network interface | Info: New interface

Description | Info



User data - *optional* | Info

Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "<h1> Hello from $(hostname -f)<a/h1>" > /var/www/html/index.html
```

□ User data has already been base64 encoded

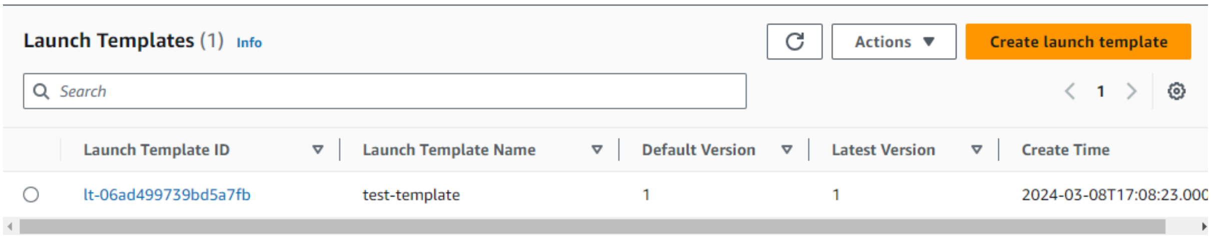
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0f403e3180720dd7e

Virtual server type (instance type)
t2.micro

Firewall (security group)
test-ec2-security

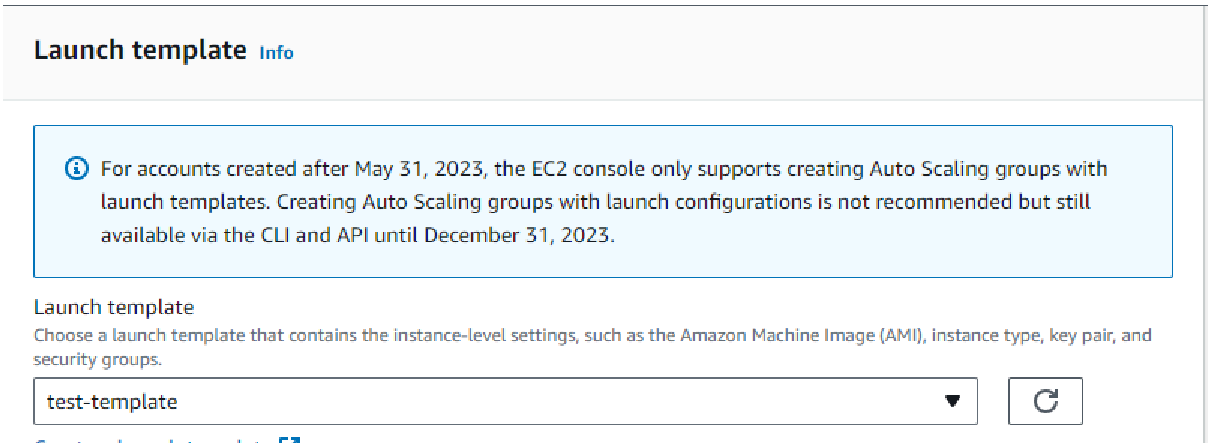
Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which



Launch Templates (1) Info

	Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time
○	lt-06ad499739bd5a7fb	test-template	1	1	2024-03-08T17:08:23.000



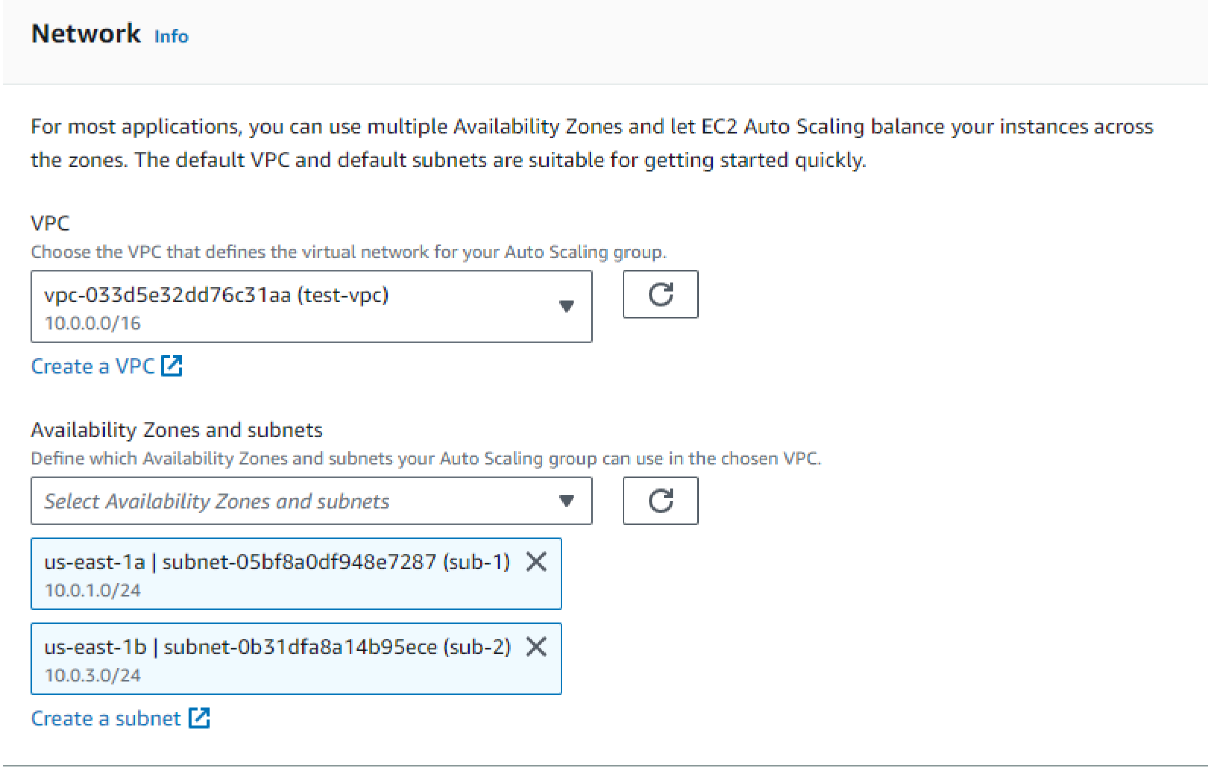
Launch template Info

For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

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.

test-template



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-033d5e32dd76c31aa (test-vpc)
10.0.0.0/16

Create a VPC

Availability Zones and subnets

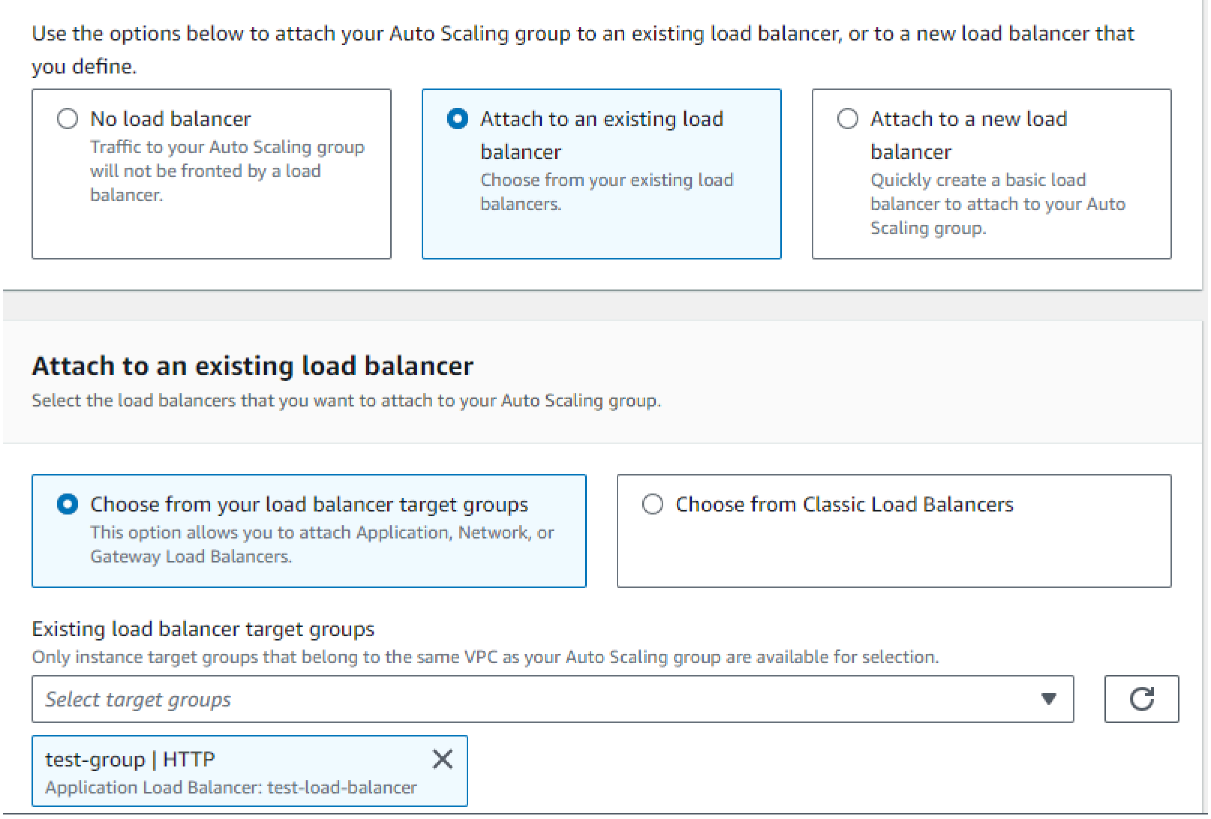
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

us-east-1a | subnet-05bf8a0df948e7287 (sub-1)
10.0.1.0/24

us-east-1b | subnet-0b31dfa8a14b95ece (sub-2)
10.0.3.0/24

Create a subnet



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.

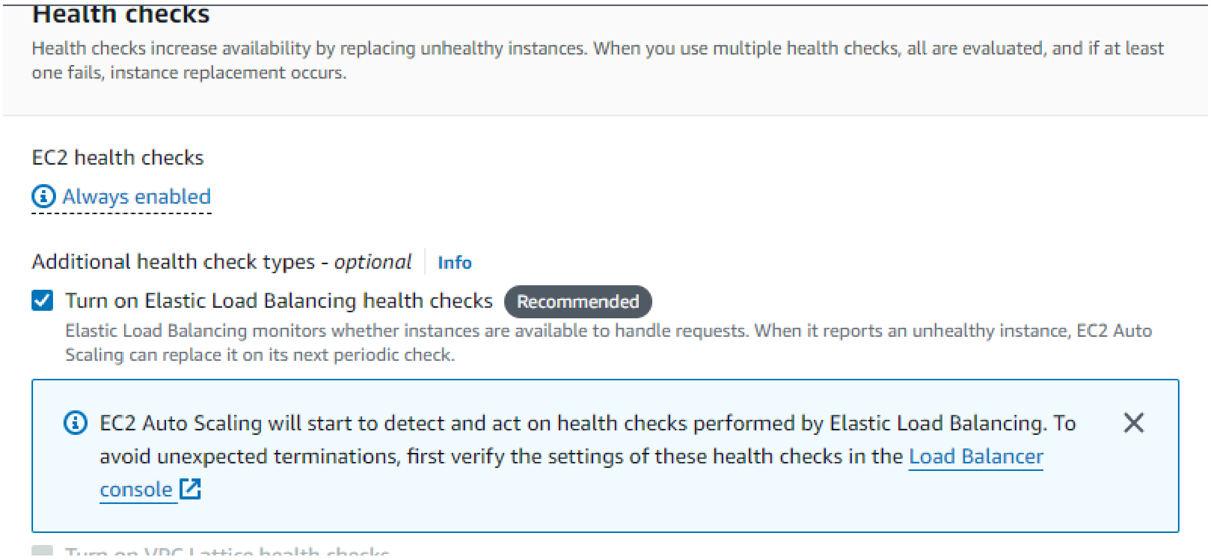
● Choose from your load balancer target groups
This option allows you to attach Application, Network, or Gateway Load Balancers.

○ 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 ▼

test-group | HTTP ✕
Application Load Balancer: test-load-balancer



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.

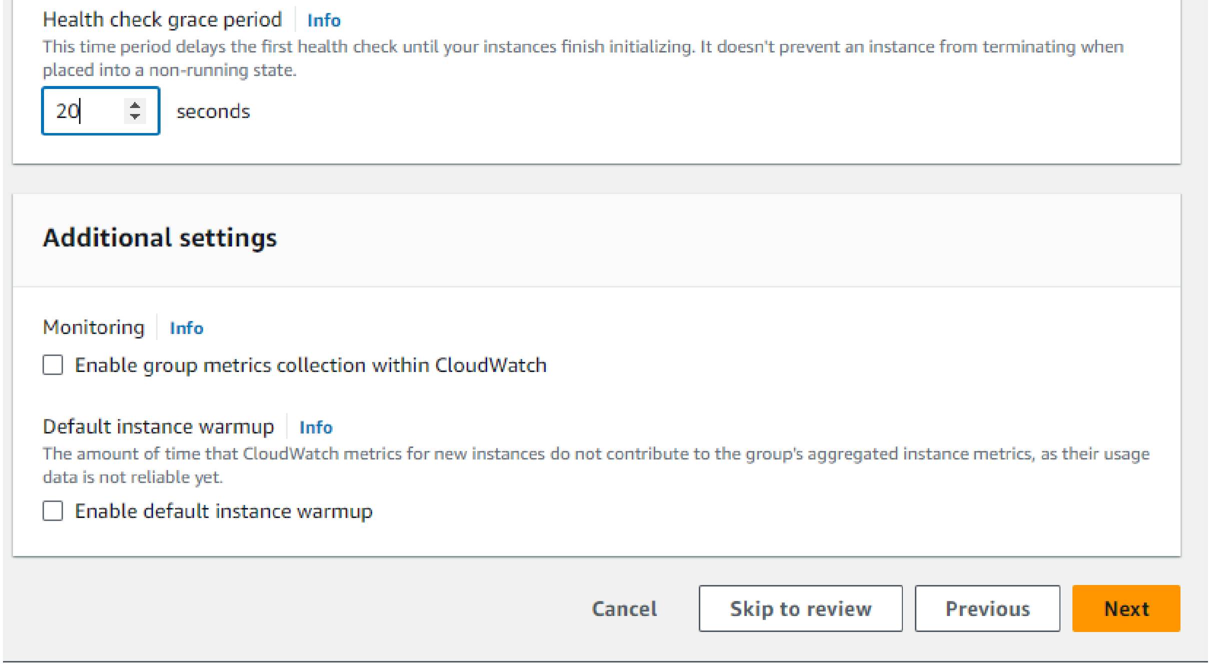
EC2 health checks
ⓘ Always enabled

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 ✕

□ Turn on VPC Lattice health checks



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.

20 seconds

Additional settings

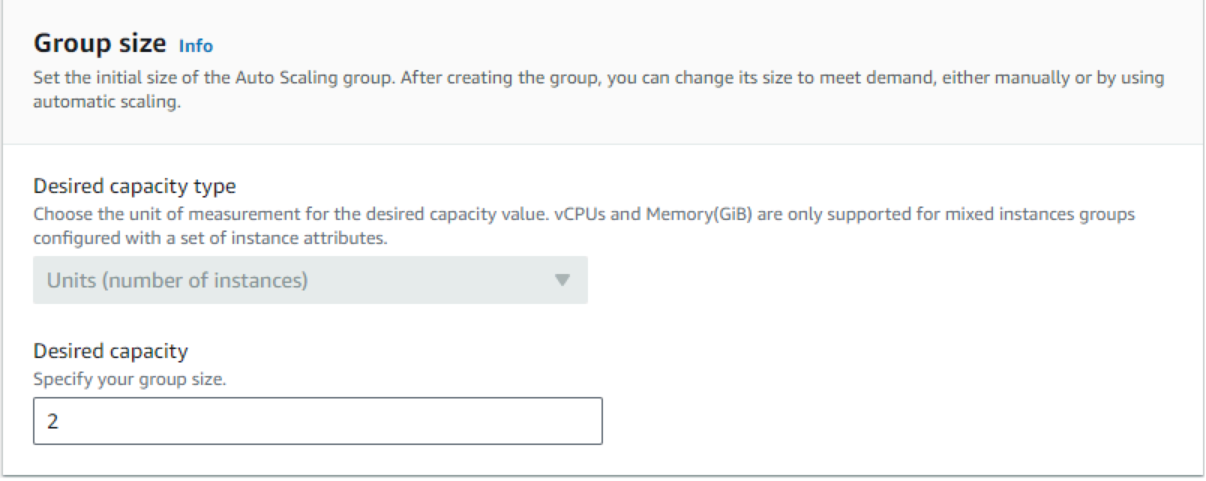
Monitoring Info

□ Enable group metrics collection within CloudWatch

Default instance warmup Info

The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.

□ Enable default instance warmup



Group size Info

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

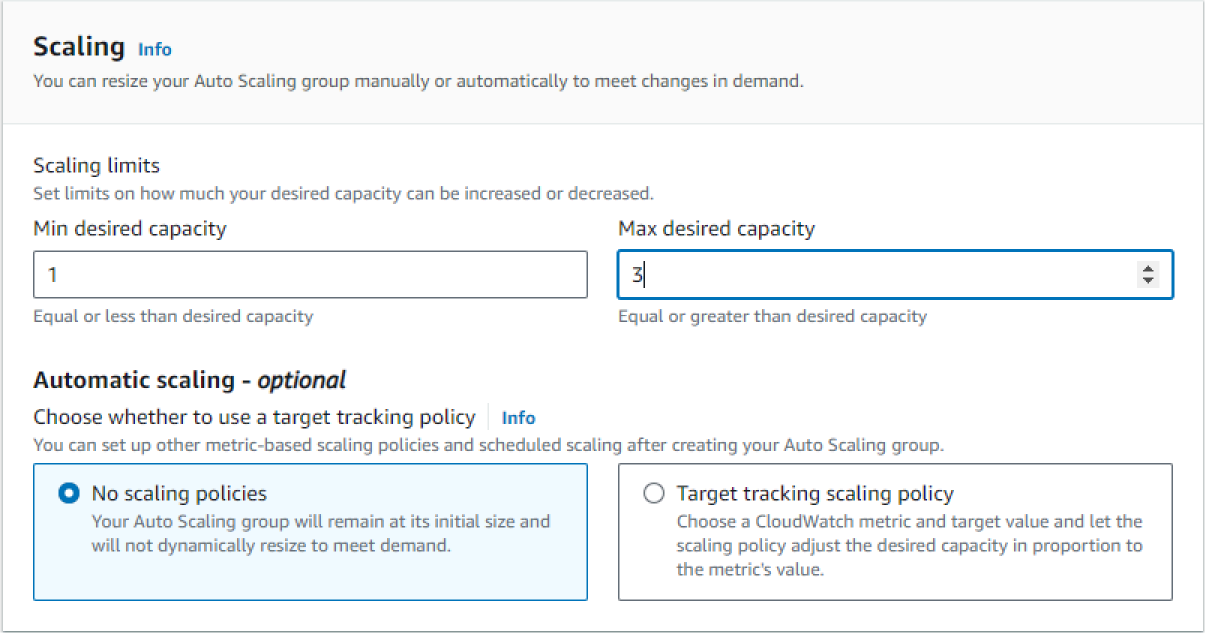
Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances)

Desired capacity

Specify your group size.

2



Scaling Info

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

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

Min desired capacity	Max desired capacity
1	3
Equal or less than desired capacity	Equal or greater than desired capacity

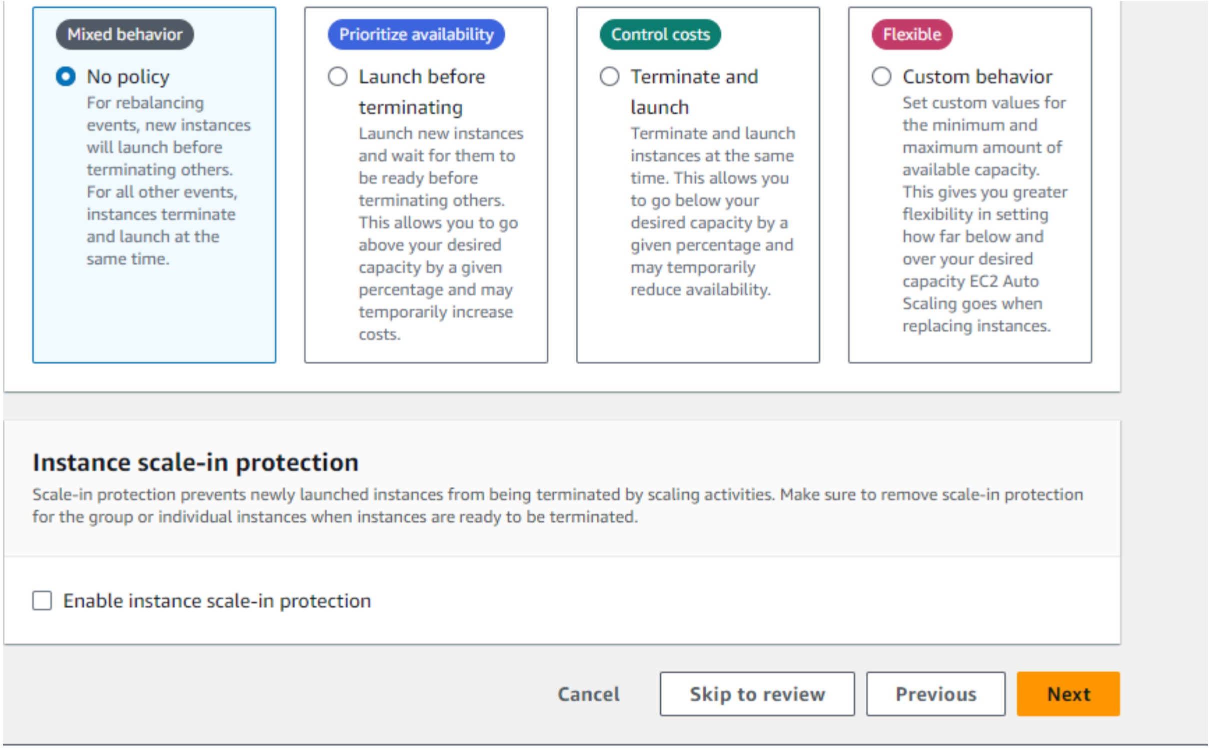
Automatic scaling - *optional*

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.



Mixed behavior
● No policy
For rebalancing events, new instances will launch before terminating others. For all other events, instances terminate and launch at the same time.

Prioritize availability
○ Launch before terminating
Launch new instances and wait for them to be ready before terminating others. This allows you to go above your desired capacity by a given percentage and may temporarily increase costs.

Control costs
○ Terminate and launch
Terminate and launch instances at the same time. This allows you to go below your desired capacity by a given percentage and may temporarily reduce availability.

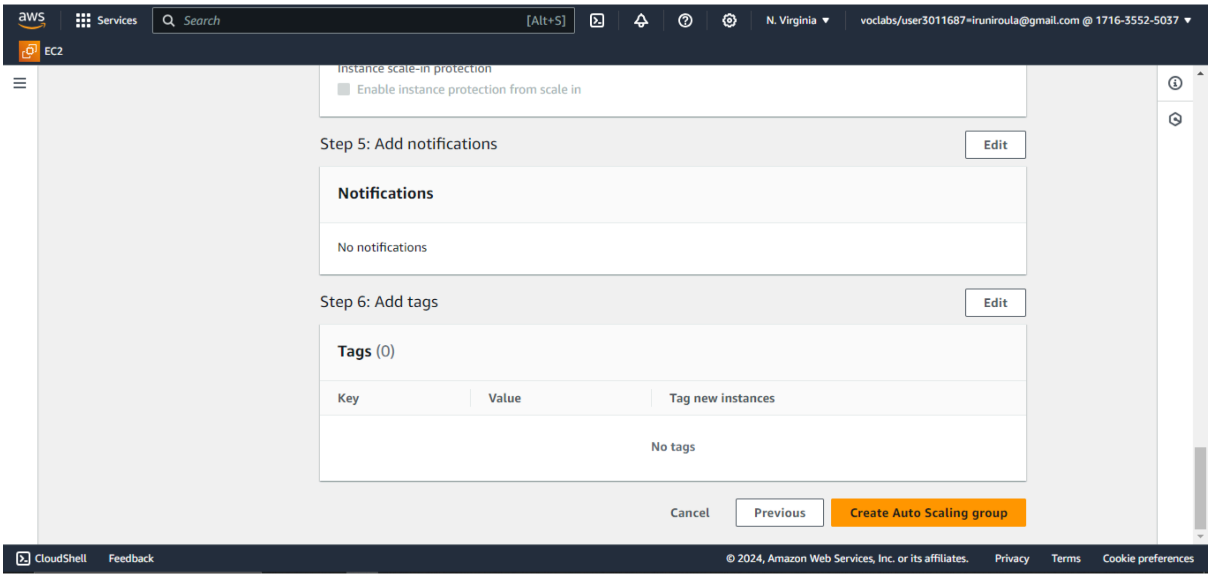
Flexible
○ Custom behavior
Set custom values for the minimum and maximum amount of available capacity. This gives you greater flexibility in setting how far below and over your desired capacity EC2 Auto Scaling goes when replacing instances.

Instance scale-in protection

Scale-in protection prevents newly launched instances from being terminated by scaling activities. Make sure to remove scale-in protection for the group or individual instances when instances are ready to be terminated.

□ Enable instance scale-in protection

After configuring all the required settings. Click on Create Auto Scaling Group



Instance scale-in protection

□ Enable instance protection from scale in

Step 5: Add notifications

Notifications

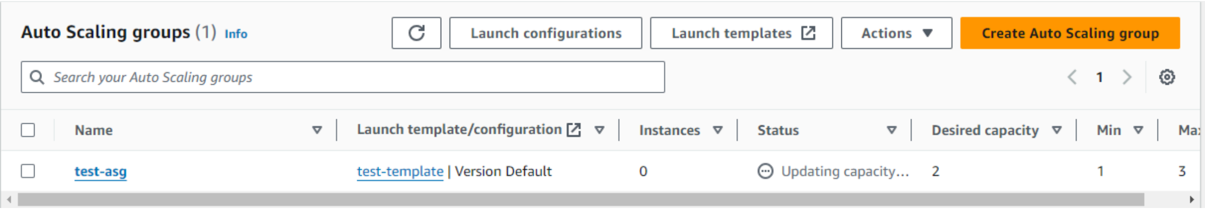
No notifications

Step 6: Add tags

Tags (0)

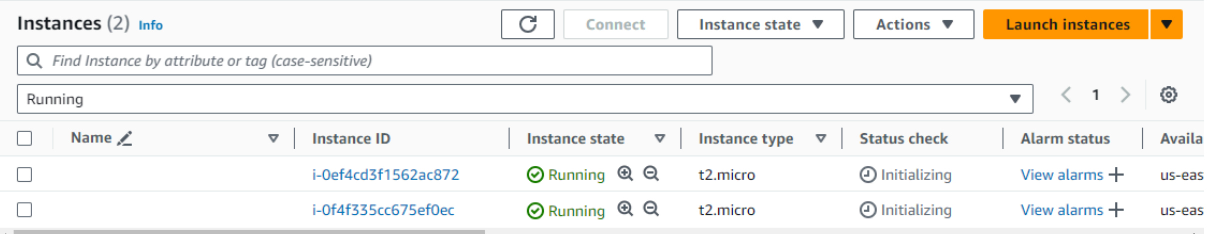
Key	Value	Tag new instances
	No tags	

© 2024, Amazon Web Services, Inc. or its affiliates.


Auto Scaling groups (1) Info

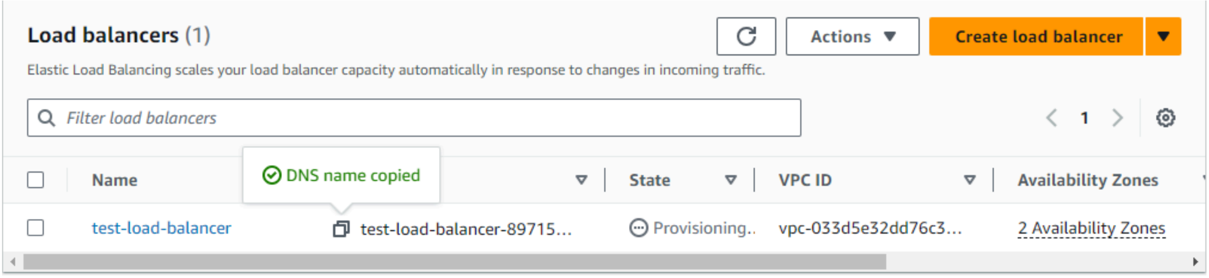
□	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Ma:
□	test-asg	test-template | Version Default	0	Updating capacity...	2	1	3

These are the two instances created through Auto Scaling


Instances (2) Info

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availa
□		i-0ef4cd3f1562ac872	Running	t2.micro	Initializing	View alarms +	us-eas
□		i-0f4f335cc675ef0ec	Running	t2.micro	Initializing	View alarms +	us-eas

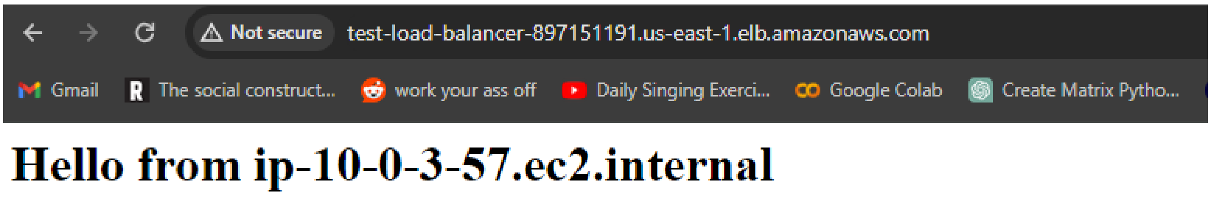
Copy the DNS from load balancer attached to the ASG and paste on the browser


Load balancers (1)

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

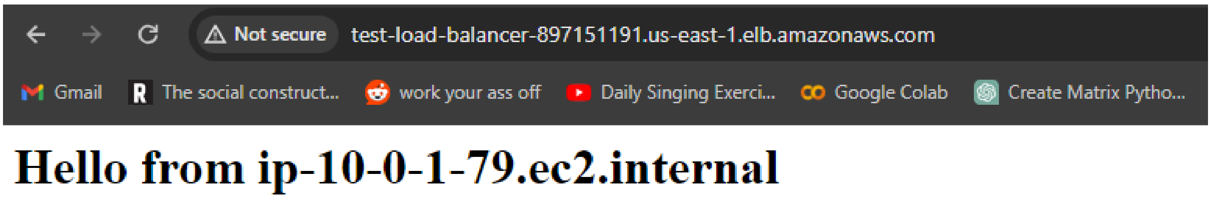
□	Name		State	VPC ID	Availability Zones
□	test-load-balancer	test-load-balancer-89715...	Provisioning..	vpc-033d5e32dd76c3...	2 Availability Zones

Each refresh will give a new IP address



test-load-balancer-897151191.us-east-1.elb.amazonaws.com

Hello from ip-10-0-3-57.ec2.internal



test-load-balancer-897151191.us-east-1.elb.amazonaws.com

Hello from ip-10-0-1-79.ec2.internal