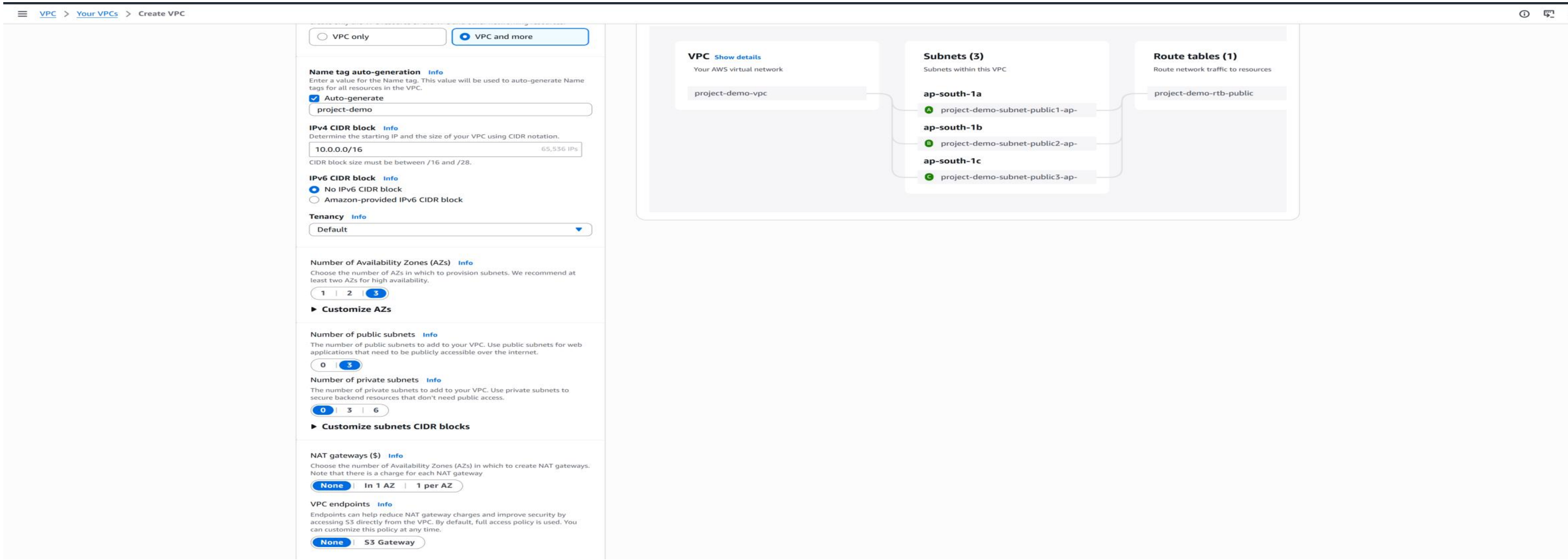
HOW TO CREATE AUTO SCALLING GROUP

Step1: Create a VPC (virtual private cloud)

- Go to vpc console -----> create vpc
- Name tag auto-generation : add name ex → project-demo
- Number of Availability Zones : 3
- Number of public subnets :3
- Number of private subnets : 0
- Nat gateway : None
- Vpc endpoints : None

---click create vpc ---



≡ VPC > Your VPCs > Create VPC

○ VPC only ● VPC and more

Name tag auto-generation Info

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☑ Auto-generate

project-demo

IPv4 CIDR block Info

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

● No IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

Tenancy Info

Default

Number of Availability Zones (AZs) Info

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 | 2 | [✓ 3]

▶ Customize AZs

Number of public subnets Info

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 | [✓ 3]

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

[✓ 0] | 3 | 6

▶ Customize subnets CIDR blocks

NAT gateways ($) Info

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

[✓ None] | In 1 AZ | 1 per AZ

VPC endpoints Info

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

[✓ None] | S3 Gateway

VPC Show details

Your AWS virtual network

project-demo-vpc

Subnets (3)

Subnets within this VPC

ap-south-1a

A project-demo-subnet-public1-ap-

ap-south-1b

B project-demo-subnet-public2-ap-

ap-south-1c

C project-demo-subnet-public3-ap-

Route tables (1)

Route network traffic to resources

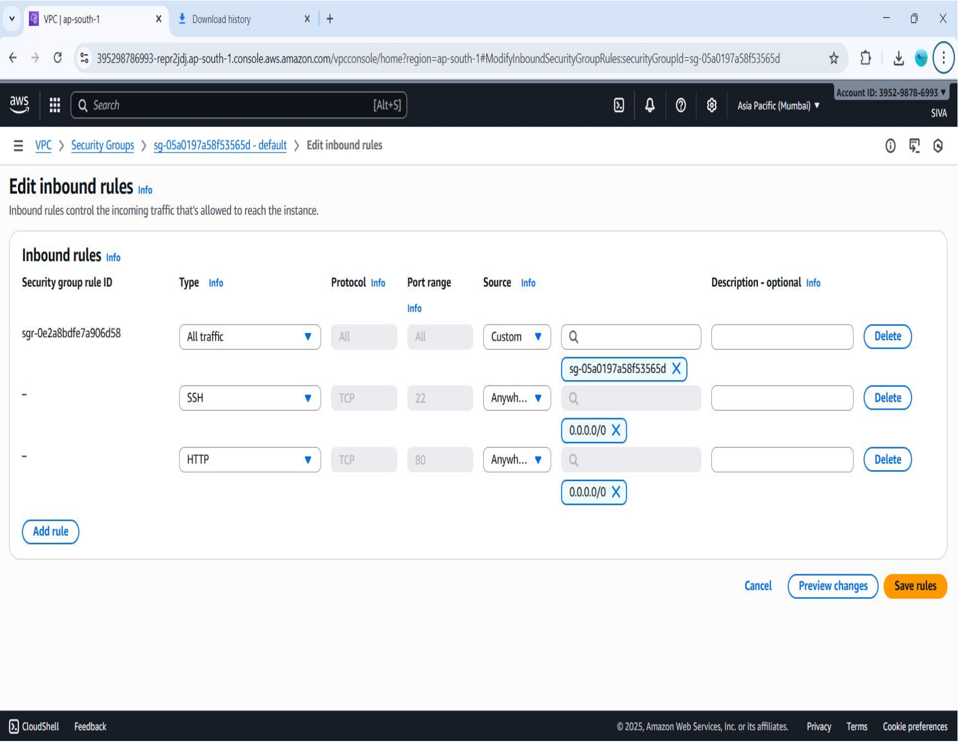
project-demo-rtb-public

Step 2: set up the security groups:

Steps :

- Go to security groups -------> first choose the vpcid
- then -----> set the inbounded and outbounded rules and save it

INBOUNDED RULES OUT BOUNDED RULES



VPC | ap-south-1 · Download history

395298786993-repr2jdj.ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-05a0197a58f53565d

Account ID: 3952-9878-6993 · Asia Pacific (Mumbai) · SIVA

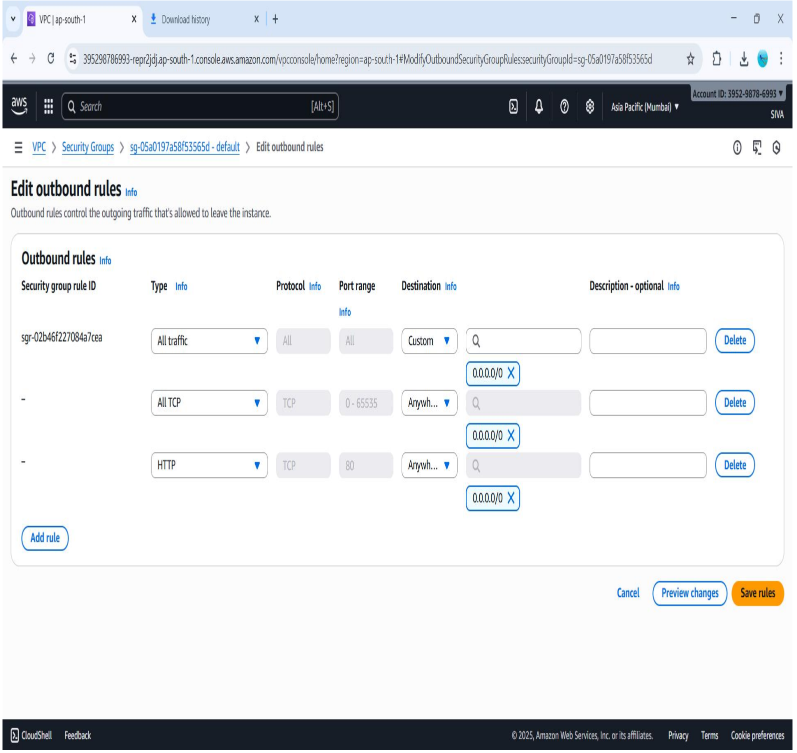
VPC > Security Groups > sg-05a0197a58f53565d - default > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional
sgr-0e2a8bdfe7a906d58	All traffic	All	All	Custom	sg-05a0197a58f53565d	
-	SSH	TCP	22	Anywh...	0.0.0.0/0	
-	HTTP	TCP	80	Anywh...	0.0.0.0/0	



VPC | ap-south-1 · Download history

395298786993-repr2jdj.ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#ModifyOutboundSecurityGroupRules:securityGroupId=sg-05a0197a58f53565d

Account ID: 3952-9878-6993 · Asia Pacific (Mumbai) · SIVA

VPC > Security Groups > sg-05a0197a58f53565d - default > Edit outbound rules

Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules Info

Security group rule ID	Type	Protocol	Port range	Destination		Description - optional
sgr-02b46f227084a7cea	All traffic	All	All	Custom	0.0.0.0/0	
-	All TCP	TCP	0 - 65535	Anywh...	0.0.0.0/0	
-	HTTP	TCP	80	Anywh...	0.0.0.0/0	

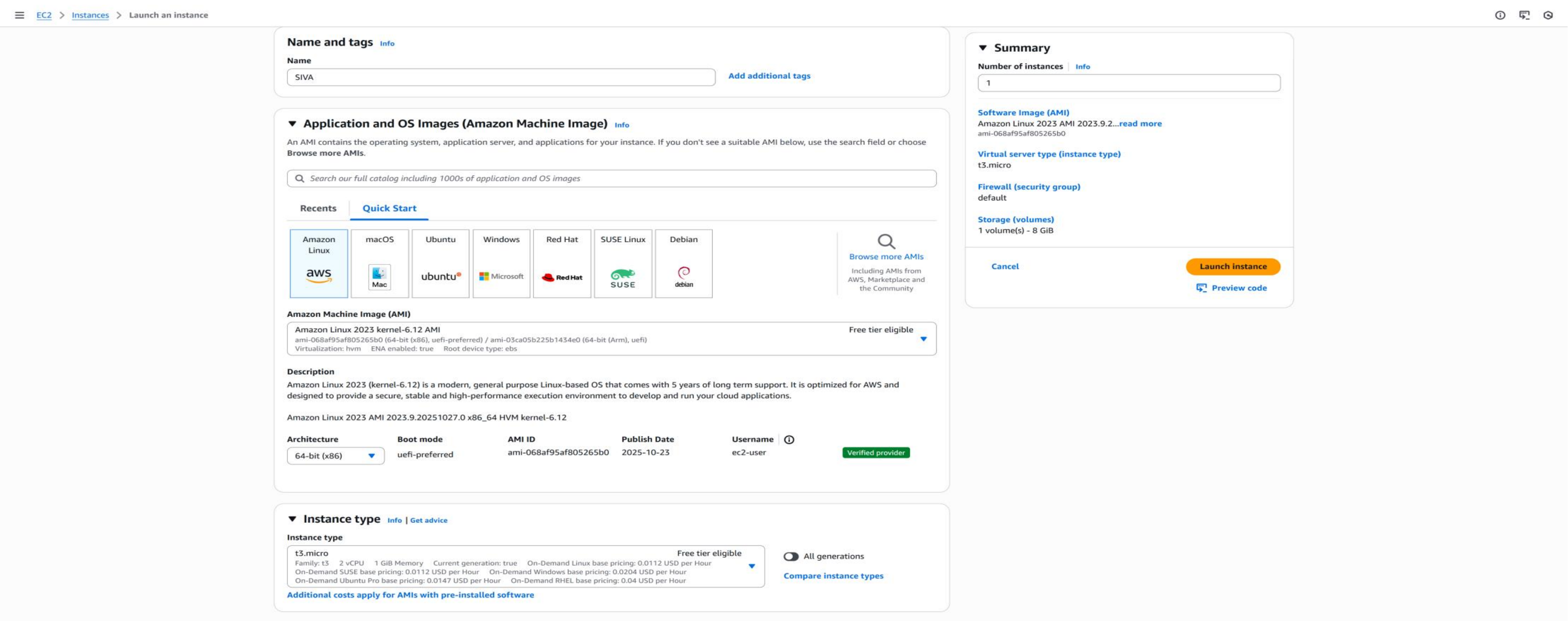
step3: create an one instance and attach image and template

1. Create a instance

- Go to EC2 ----> launch instance
- Give Name ----> EX:siva
- Choose Amazon Machine Image (AMI) :amazon linux 2023 kernal-6.12AMI
- Instance type :type3.micro
- Select you keypair : linuxxx
- Select your vpc : project-demo

❖ Auto-assign public IP : enable
❖ Attach the security group : default
❖ advanced detail ----->user data , paste

Now we create one instance and go to chrome browser then paste ip address



EC2 > Instances > Launch an instance

Name and tags Info

Name: SIVA

Application and OS Images (Amazon Machine Image) Info

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.

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

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.12 AMI — Free tier eligible
ami-068af95af805265b0 (64-bit (x86), uefi-preferred) / ami-03ca05b225b1434e0 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 (kernel-6.12) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.9.20251027.0 x86_64 HVM kernel-6.12

Architecture	Boot mode	AMI ID	Publish Date	Username	
64-bit (x86)	uefi-preferred	ami-068af95af805265b0	2025-10-23	ec2-user	Verified provider

Instance type Info | Get advice

Instance type

t3.micro — Free tier eligible
Family: t3 2 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0112 USD per Hour
On-Demand SUSE base pricing: 0.0112 USD per Hour On-Demand Windows base pricing: 0.0204 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0147 USD per Hour On-Demand RHEL base pricing: 0.04 USD per Hour

Summary

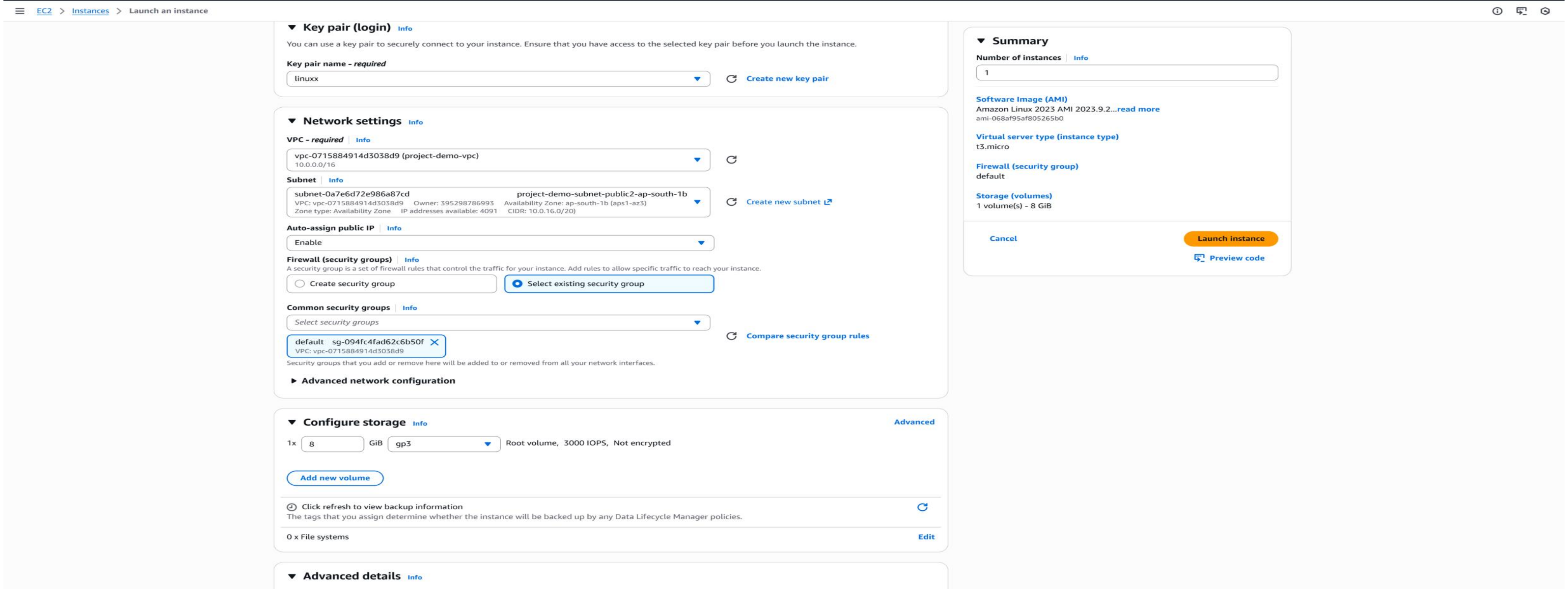
Number of instances Info: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more
ami-068af95af805265b0

Virtual server type (instance type)
t3.micro

Firewall (security group)
default

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



EC2 > Instances > Launch an instance

▼ **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 - *required*

linuxx ▼ | Create new key pair

▼ **Network settings** Info

VPC - *required* | Info

vpc-0715884914d3038d9 (project-demo-vpc)
10.0.0.0/16

Subnet | Info

subnet-0a7e6d72e986a87cd   project-demo-subnet-public2-ap-south-1b
VPC: vpc-0715884914d3038d9   Owner: 395298786993   Availability Zone: ap-south-1b (aps1-az3)
Zone type: Availability Zone   IP addresses available: 4091   CIDR: 10.0.16.0/20)

Create new subnet

Auto-assign public IP | Info

Enable

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.

○ Create security group   ● Select existing security group

Common security groups | Info

Select security groups | Compare security group rules

default sg-094fc4fad62c6b50f ✕
VPC: vpc-0715884914d3038d9

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

▶ **Advanced network configuration**

▼ **Configure storage** Info   Advanced

1x 8 GiB gp3 ▼ Root volume, 3000 IOPS, Not encrypted

Add new volume

Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems   Edit

▼ **Advanced details** Info

▼ **Summary**

Number of instances | Info

1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more
ami-068af95af805265b0

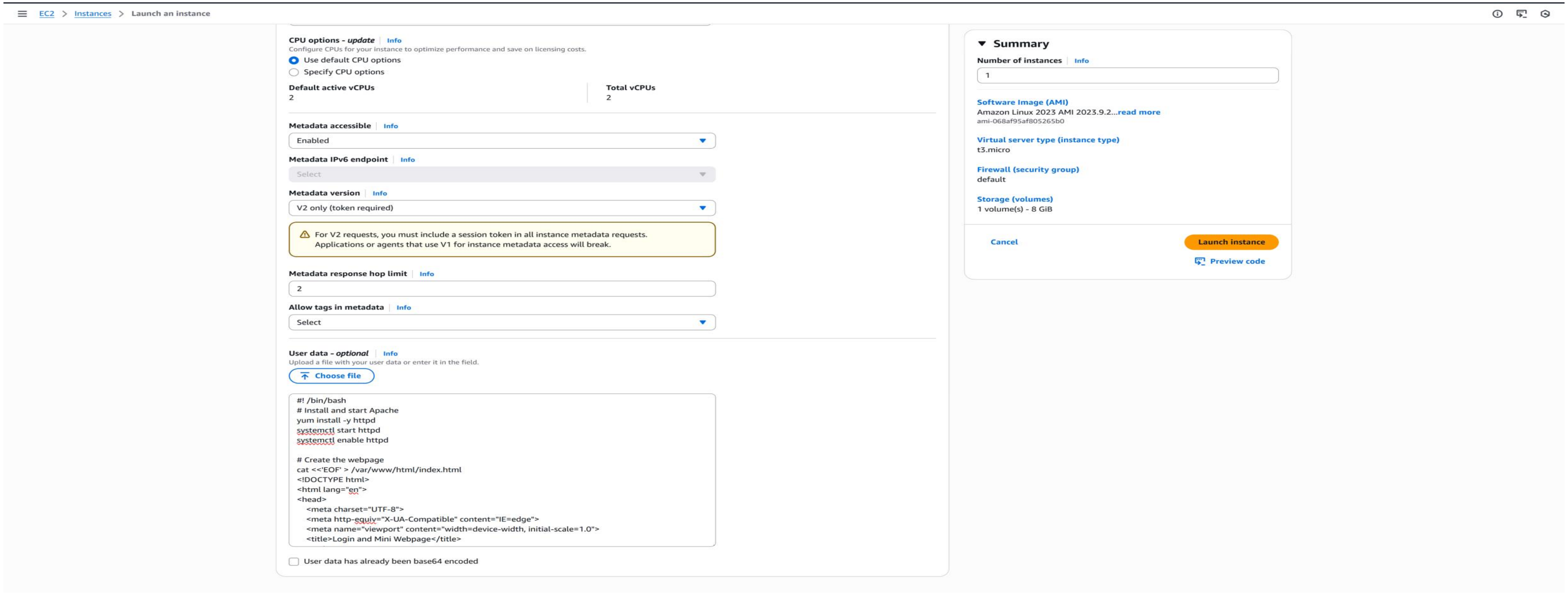
Virtual server type (instance type)
t3.micro

Firewall (security group)
default

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

Cancel   Launch instance

Preview code



EC2 > Instances > Launch an instance

CPU options - *update* | Info

Configure CPUs for your instance to optimize performance and save on licensing costs.

● Use default CPU options
○ Specify CPU options

Default active vCPUs	Total vCPUs
2	2

Metadata accessible | Info

Enabled

Metadata IPv6 endpoint | Info

Select

Metadata version | Info

V2 only (token required)

⚠ For V2 requests, you must include a session token in all instance metadata requests.
Applications or agents that use V1 for instance metadata access will break.

Metadata response hop limit | Info

2

Allow tags in metadata | Info

Select

User data - *optional* | Info

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

Choose file

```
#! /bin/bash
# Install and start Apache
yum install -y httpd
systemctl start httpd
systemctl enable httpd

# Create the webpage
cat <<'EOF' > /var/www/html/index.html
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta http-equiv="X-UA-Compatible" content="IE=edge">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <title>Login and Mini Webpage</title>
```

□ User data has already been base64 encoded

▼ **Summary**

Number of instances | Info

1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more
ami-068af95af805265b0

Virtual server type (instance type)
t3.micro

Firewall (security group)
default

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

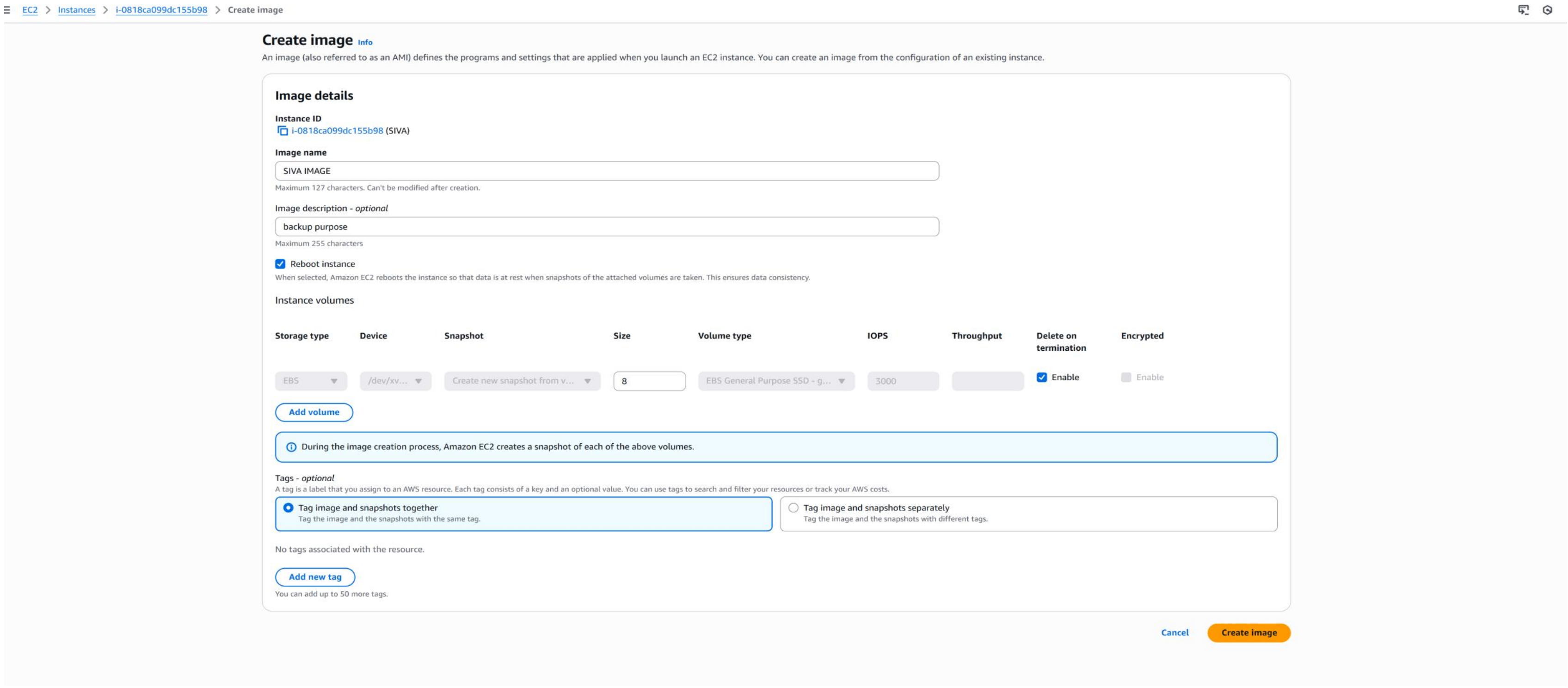
Cancel   Launch instance

Preview code

Step 4: create an AMI from the instance:

Go to EC2 instance ----> actions ----> image ---->create image

- Image name : siva image
- Image description : backup purpose
- Click : create image



EC2 > Instances > i-0818ca099dc155b98 > Create image

Create image Info

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.

Image details

Instance ID
i-0818ca099dc155b98 (SIVA)

Image name
SIVA IMAGE
Maximum 127 characters. Can't be modified after creation.

Image description - *optional*
backup purpose
Maximum 255 characters

☑ Reboot instance
When selected, Amazon EC2 reboots the instance so that data is at rest when snapshots of the attached volumes are taken. This ensures data consistency.

Instance volumes

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/xv...	Create new snapshot from v...	8	EBS General Purpose SSD - g...	3000		☑ Enable	□ Enable

Add volume

ⓘ During the image creation process, Amazon EC2 creates a snapshot of each of the above volumes.

Tags - *optional*
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.

● Tag image and snapshots together
Tag the image and the snapshots with the same tag.

○ Tag image and snapshots separately
Tag the image and the snapshots with different tags.

No tags associated with the resource.

Add new tag
You can add up to 50 more tags.

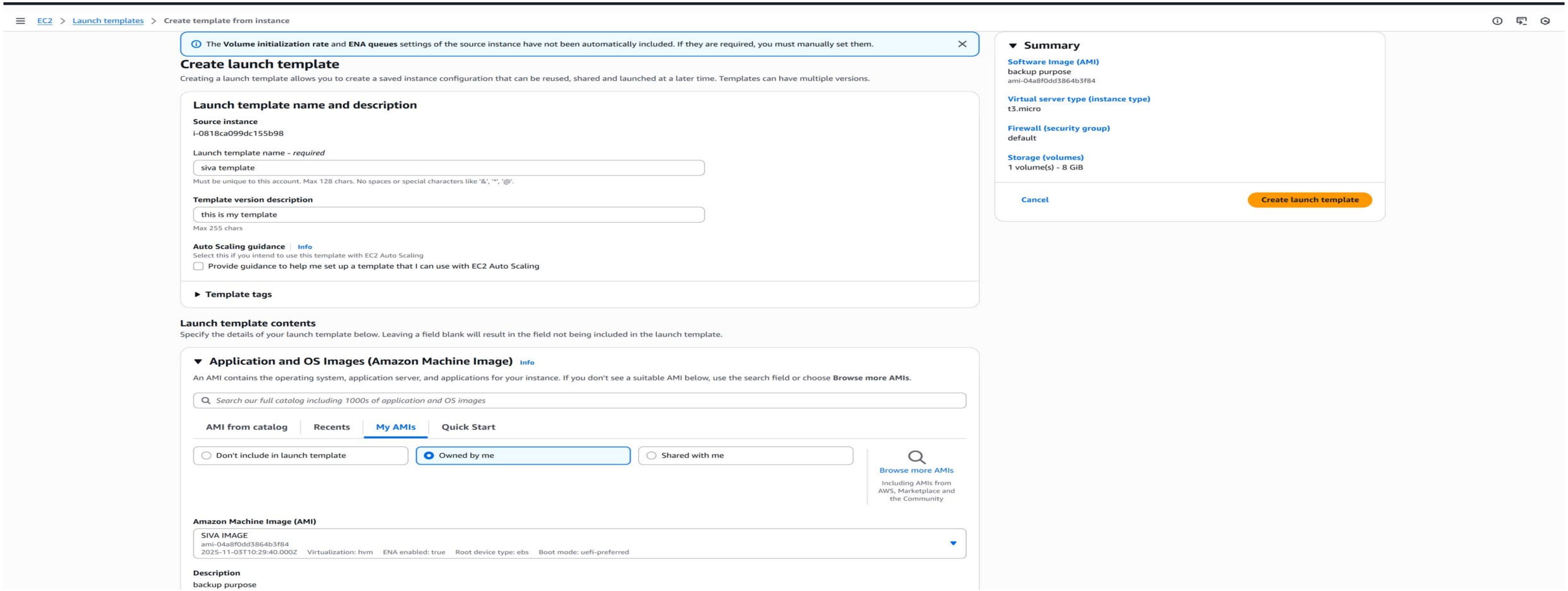
Cancel | Create image

Step 5: create a launch template

Go to EC2 ----> launch template ---> create launch template

1. Launch template name : ex : siva template
2. Template version description : this my template
3. Choose your AMI :siva image
4. Select Instance type :t3micro
5. Select your Key pair name : linuxx
6. Select Network settings

Click template create



The **Volume initialization rate** and **ENA queues** settings of the source instance have not been automatically included. If they are required, you must manually set them.

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

Launch template name and description

Source instance
i-0818ca099dc155b98

Launch template name - *required*
siva template
Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description
this is my template
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

▸ Template tags

Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

▾ Application and OS Images (Amazon Machine Image) Info

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose **Browse more AMIs**.

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

○ Don't include in launch template ● Owned by me ○ Shared with me

Amazon Machine Image (AMI)
SIVA IMAGE
ami-04a8f0dd3864b3f84
2025-11-03T10:29:40.000Z Virtualization: hvm ENA enabled: true Root device type: ebs Boot mode: uefi-preferred

Description
backup purpose

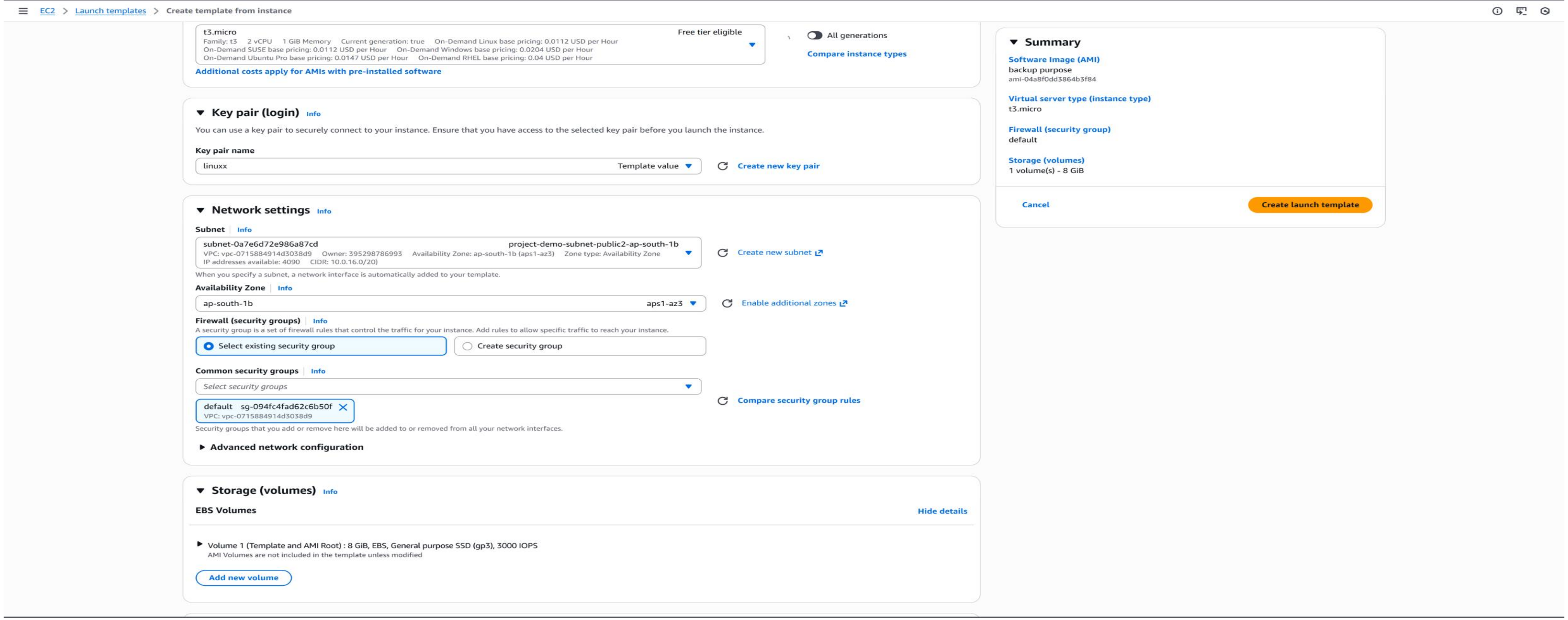
▾ Summary

Software Image (AMI)
backup purpose
ami-04a8f0dd3864b3f84

Virtual server type (instance type)
t3.micro

Firewall (security group)
default

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



t3.micro Free tier eligible
Family: t3 2 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0112 USD per Hour
On-Demand SUSE base pricing: 0.0112 USD per Hour On-Demand Windows base pricing: 0.0204 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0147 USD per Hour On-Demand RHEL base pricing: 0.04 USD per Hour

Additional costs apply for AMIs with pre-installed software

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: linuxx — Template value

Network settings Info

Subnet | Info
subnet-0a7e6d72e986a87cd project-demo-subnet-public2-ap-south-1b
VPC: vpc-0715884914d3038d9 Owner: 395298786993 Availability Zone: ap-south-1b (aps1-az3) Zone type: Availability Zone
IP addresses available: 4090 CIDR: 10.0.16.0/20)

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

Availability Zone | Info: ap-south-1b aps1-az3

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
default sg-094fc4fad62c6b50f
VPC: vpc-0715884914d3038d9

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

▸ Advanced network configuration

Storage (volumes) Info

EBS Volumes

▸ Volume 1 (Template and AMI Root) : 8 GiB, EBS, General purpose SSD (gp3), 3000 IOPS
AMI Volumes are not included in the template unless modified

Summary

Software Image (AMI)
backup purpose
ami-04a8f0dd3864b3f84

Virtual server type (instance type)
t3.micro

Firewall (security group)
default

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

Step 6 : create a load balancer :

Steps :

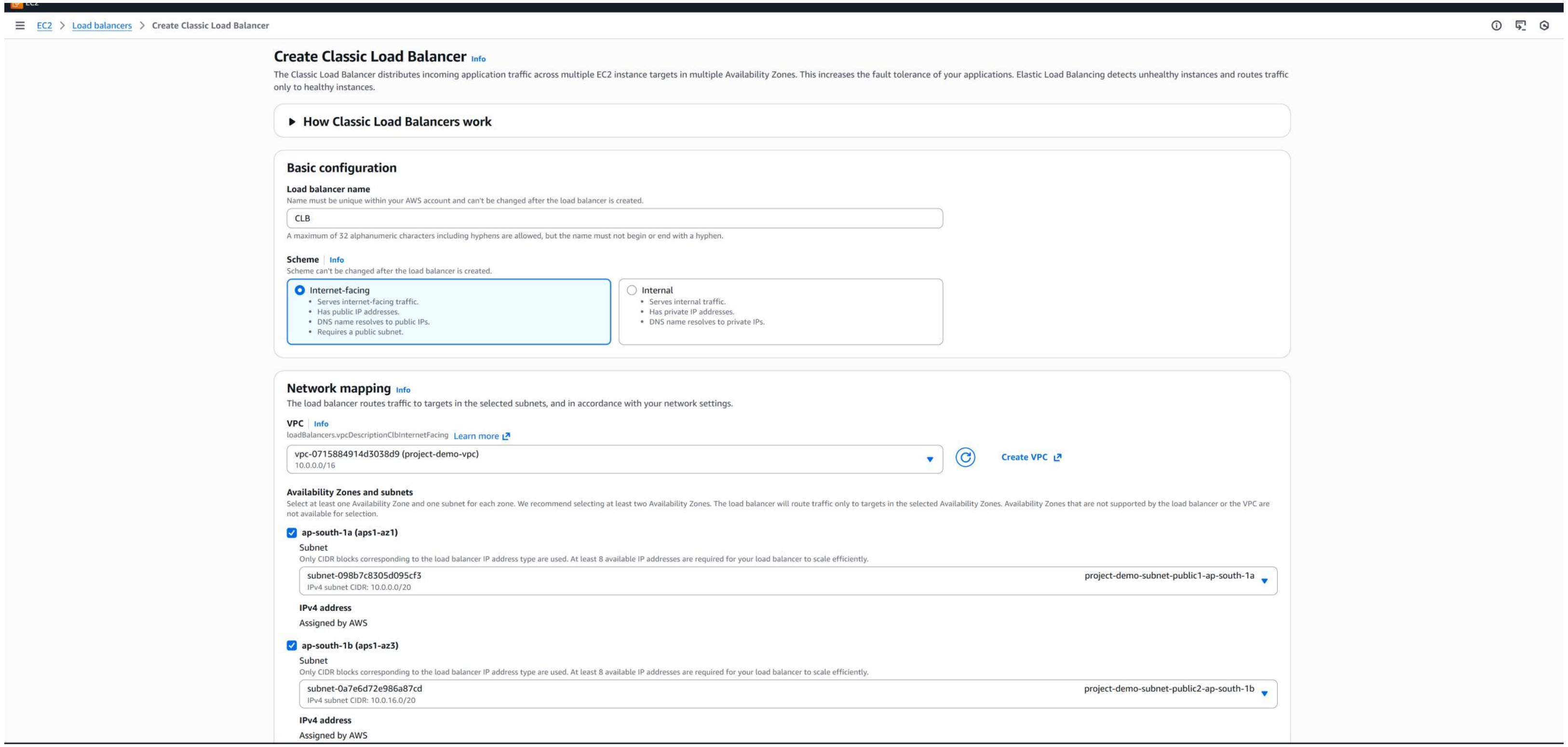
Go to EC2 ----> load balancer -----> create a load balancer

A. Create a classic load balancer ---> load balancer name ---> CLB
B. Edit network mapping :

Select your vpc

Availability zones and subnets : ap-south-1a (aps1-az1) ap-south-1b (aps1-az3) , ap-south-1c (aps1-az2)

Select security groups



EC2 > Load balancers > Create Classic Load Balancer

Create Classic Load Balancer Info

The Classic Load Balancer distributes incoming application traffic across multiple EC2 instance targets in multiple Availability Zones. This increases the fault tolerance of your applications. Elastic Load Balancing detects unhealthy instances and routes traffic only to healthy instances.

▶ How Classic Load Balancers work

Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.
CLB
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
- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name resolves to public IPs.
- Requires a public subnet.

○ Internal
- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.

Network mapping Info

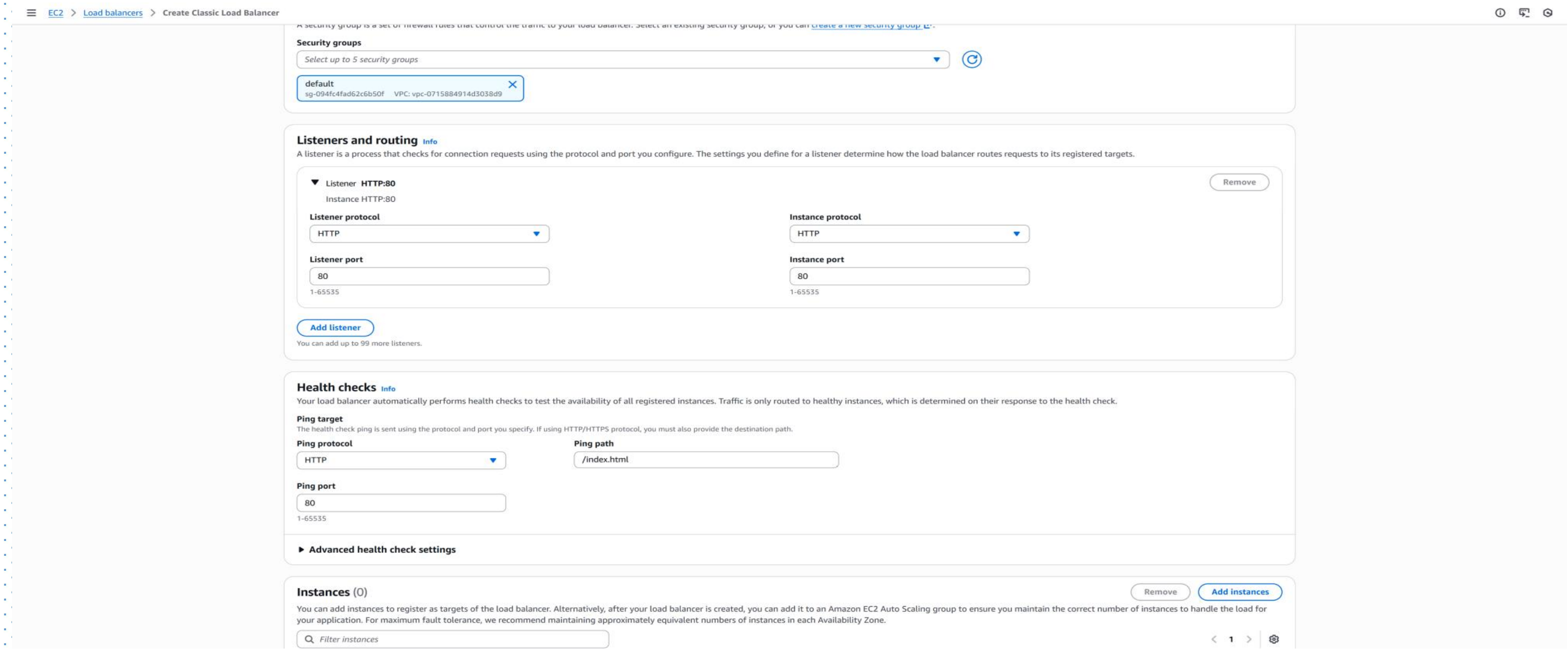
The load balancer routes traffic to targets in the selected subnets, and in accordance with your network settings.

VPC | Info
loadBalancers.vpcDescriptionClbInternetFacing Learn more
vpc-0715884914d3038d9 (project-demo-vpc)
10.0.0.0/16
Create VPC

Availability Zones and subnets
Select at least one Availability Zone and one subnet for each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic only to targets in the selected Availability Zones. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

☑ ap-south-1a (aps1-az1)
Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.
subnet-098b7c8305d095cf3 project-demo-subnet-public1-ap-south-1a
IPv4 subnet CIDR: 10.0.0.0/20
IPv4 address
Assigned by AWS

☑ ap-south-1b (aps1-az3)
Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.
subnet-0a7e6d72e986a87cd project-demo-subnet-public2-ap-south-1b
IPv4 subnet CIDR: 10.0.16.0/20
IPv4 address
Assigned by AWS



EC2 > Load balancers > Create Classic Load Balancer

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-094fc4fad62c6b50f VPC: vpc-0715884914d3038d9

Listeners and routing Info

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

▼ Listener **HTTP:80**
Instance HTTP:80
Remove

Listener protocol HTTP	**Instance protocol** HTTP
Listener port 80 1-65535	**Instance port** 80 1-65535

Add listener
You can add up to 99 more listeners.

Health checks Info

Your load balancer automatically performs health checks to test the availability of all registered instances. Traffic is only routed to healthy instances, which is determined on their response to the health check.

Ping target
The health check ping is sent using the protocol and port you specify. If using HTTP/HTTPS protocol, you must also provide the destination path.

Ping protocol
HTTP

Ping path
/index.html

Ping port
80
1-65535

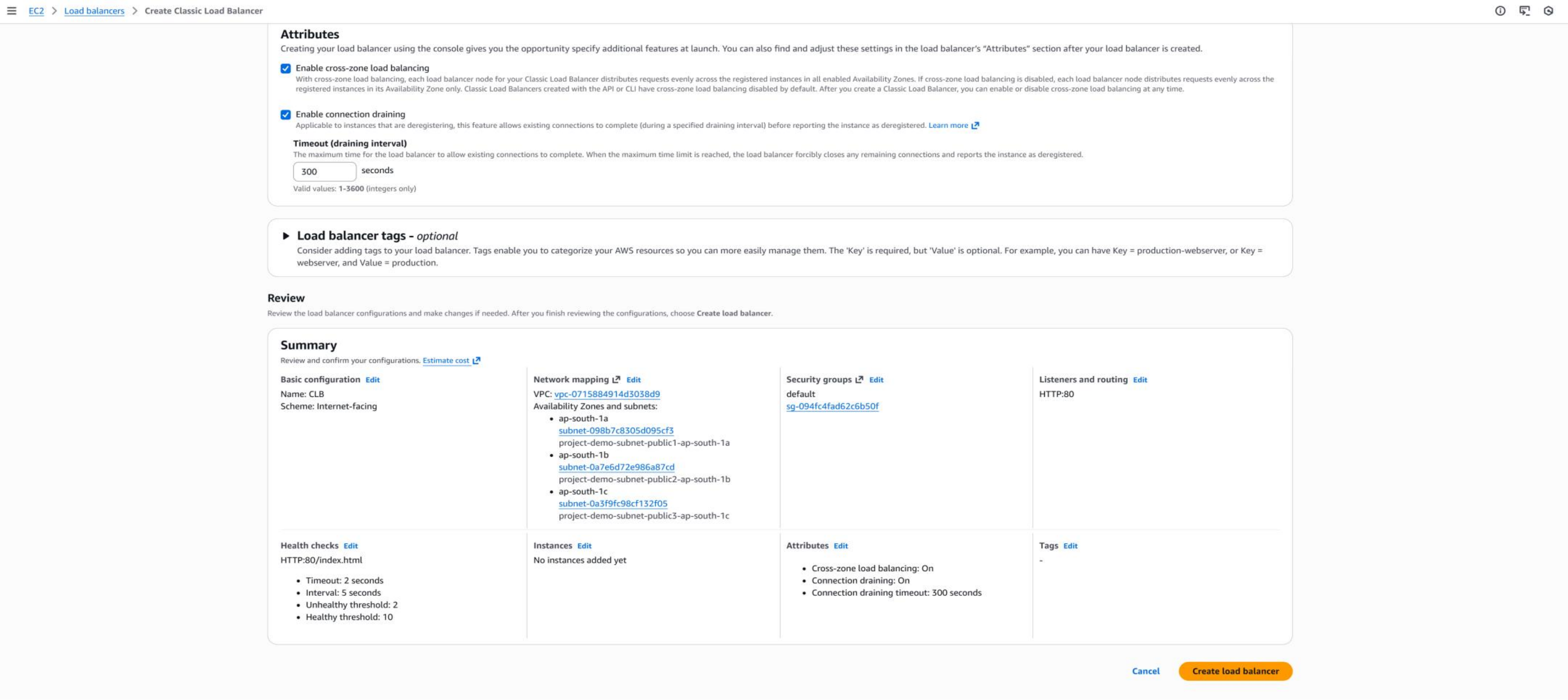
▶ Advanced health check settings

Instances (0)

Remove Add instances

You can add instances to register as targets of the load balancer. Alternatively, after your load balancer is created, you can add it to an Amazon EC2 Auto Scaling group to ensure you maintain the correct number of instances to handle the load for your application. For maximum fault tolerance, we recommend maintaining approximately equivalent numbers of instances in each Availability Zone.

Filter instances
< 1 >



Attributes

Creating your load balancer using the console gives you the opportunity specify additional features at launch. You can also find and adjust these settings in the load balancer's "Attributes" section after your load balancer is created.

☑ Enable cross-zone load balancing

With cross-zone load balancing, each load balancer node for your Classic Load Balancer distributes requests evenly across the registered instances in all enabled Availability Zones. If cross-zone load balancing is disabled, each load balancer node distributes requests evenly across the registered instances in its Availability Zone only. Classic Load Balancers created with the API or CLI have cross-zone load balancing disabled by default. After you create a Classic Load Balancer, you can enable or disable cross-zone load balancing at any time.

☑ Enable connection draining

Applicable to instances that are deregistering, this feature allows existing connections to complete (during a specified draining interval) before reporting the instance as deregistered. Learn more

Timeout (draining interval)

The maximum time for the load balancer to allow existing connections to complete. When the maximum time limit is reached, the load balancer forcibly closes any remaining connections and reports the instance as deregistered.

300 seconds

Valid values: **1-3600** (integers only)

▶ **Load balancer tags** - *optional*

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

Review

Review the load balancer configurations and make changes if needed. After you finish reviewing the configurations, choose **Create load balancer**.

Summary

Review and confirm your configurations. Estimate cost

Basic configuration Edit	Network mapping Edit	Security groups Edit	Listeners and routing Edit
Name: CLB Scheme: Internet-facing	VPC: vpc-0715884914d3038d9 Availability Zones and subnets: • ap-south-1a subnet-098b7c8305d095cf3 project-demo-subnet-public1-ap-south-1a • ap-south-1b subnet-0a7e6d72e986a87cd project-demo-subnet-public2-ap-south-1b • ap-south-1c subnet-0a3f9fc98cf132f05 project-demo-subnet-public3-ap-south-1c	default sg-094fc4fad62c6b50f	HTTP:80
Health checks Edit	**Instances** Edit	**Attributes** Edit	**Tags** Edit
HTTP:80/index.html • Timeout: 2 seconds • Interval: 5 seconds • Unhealthy threshold: 2 • Healthy threshold: 10	No instances added yet	• Cross-zone load balancing: On • Connection draining: On • Connection draining timeout: 300 seconds	-

After creater a classic load balancer check DNS name :CLB-923948916.ap-south-1.elb.amazonaws.com

Step 7 : create an auto scaling group:

<u>Steps</u> :

Go to EC2 ---> auto scalling groups ---> create an auto scalling group

1) Auto scalling groups name : alg
2) Select your template : siva-template

NEXT PAGE

3) Network : select your vpc
4) Select availability zones : 3 1a.1b.1c

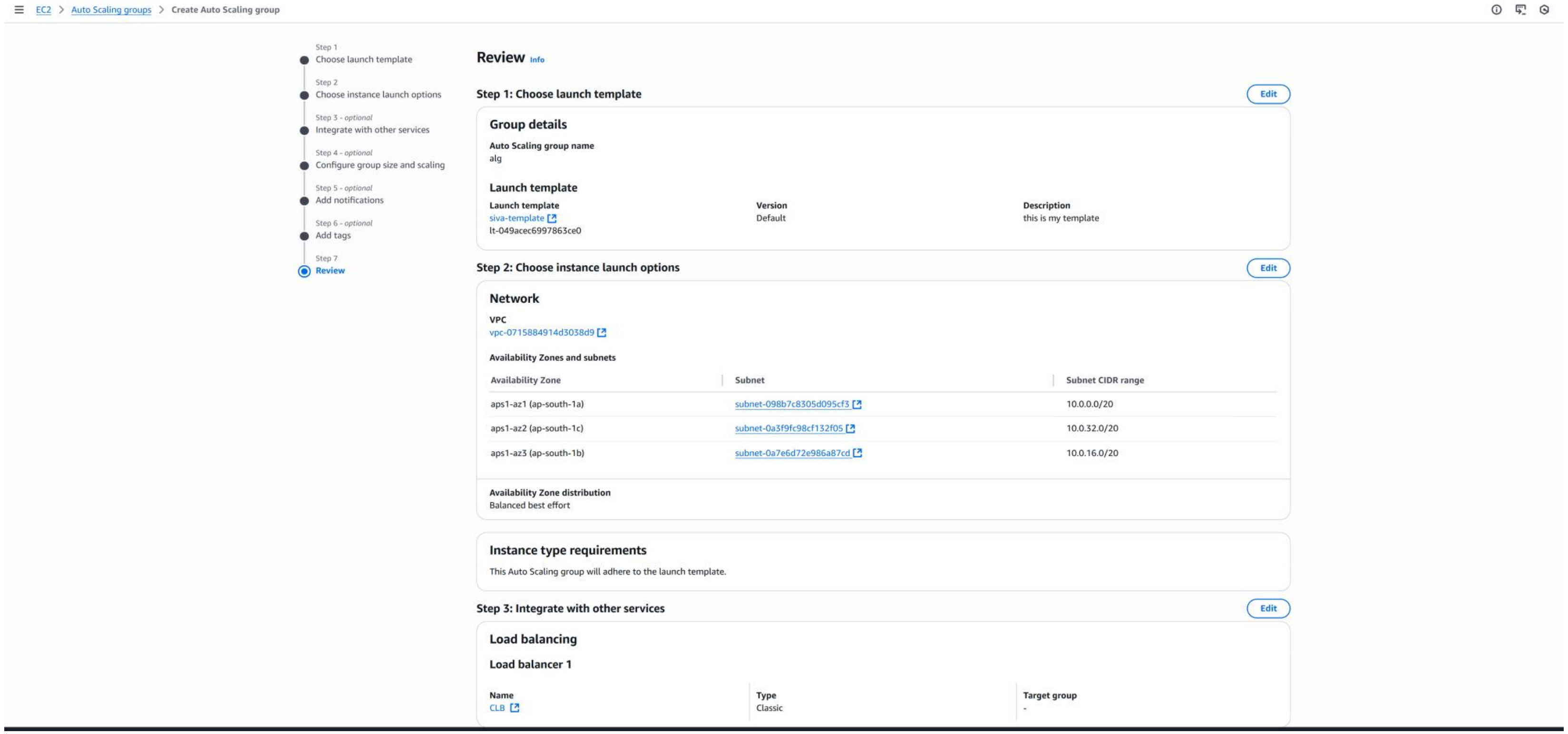
NEXT PAGE

5) Attach to an existing load balancer ---->choose from classic load balancer -----> select your classic load balancer

NEXT PAGE

6) Desired capacity :3
7) Scaling limits---> min desired capacity : 3---->max desired capacity--->5
8) Select monitoring : enable (it is optional)
9) Simple notification service (sns) ---> create topic -->name : siva-->

Create subscription ---> select protocol---> Email -->end point enter email address



Review Info

Step 1: Choose launch template

Group details

Auto Scaling group name
alg

Launch template

Launch template	Version	Description
siva-template lt-049acec6997863ce0	Default	this is my template

Step 2: Choose instance launch options

Network

VPC
vpc-0715884914d3038d9

Availability Zones and subnets

Availability Zone	Subnet	Subnet CIDR range
aps1-az1 (ap-south-1a)	subnet-098b7c8305d095cf3	10.0.0.0/20
aps1-az2 (ap-south-1c)	subnet-0a3f9fc98cf132f05	10.0.32.0/20
aps1-az3 (ap-south-1b)	subnet-0a7e6d72e986a87cd	10.0.16.0/20

Availability Zone distribution
Balanced best effort

Instance type requirements

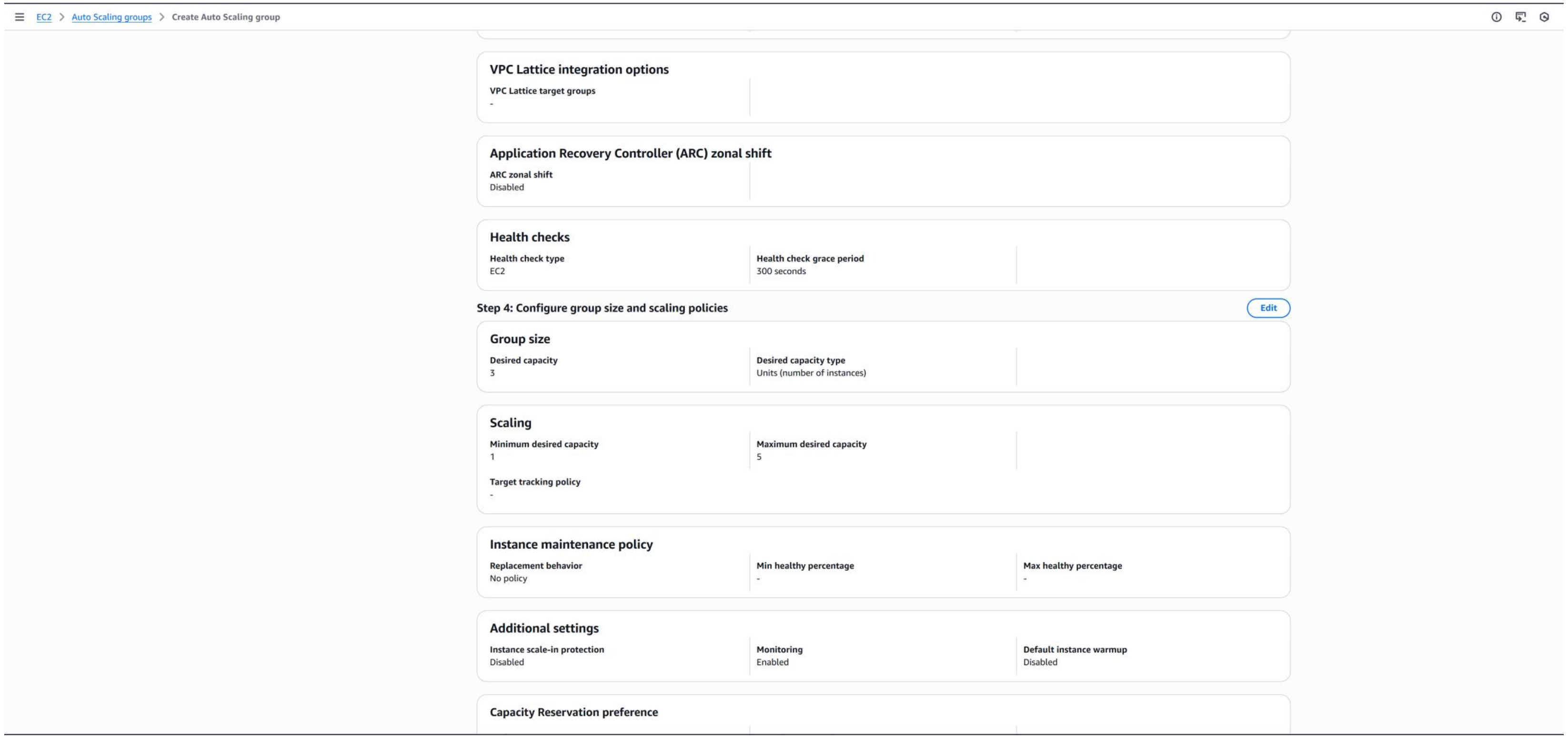
This Auto Scaling group will adhere to the launch template.

Step 3: Integrate with other services

Load balancing

Load balancer 1

Name	Type	Target group
CLB	Classic	-



VPC Lattice integration options

VPC Lattice target groups
-

Application Recovery Controller (ARC) zonal shift

ARC zonal shift
Disabled

Health checks

Health check type	Health check grace period
EC2	300 seconds

Step 4: Configure group size and scaling policies

Group size

Desired capacity	Desired capacity type
3	Units (number of instances)

Scaling

Minimum desired capacity	Maximum desired capacity
1	5

Target tracking policy
-

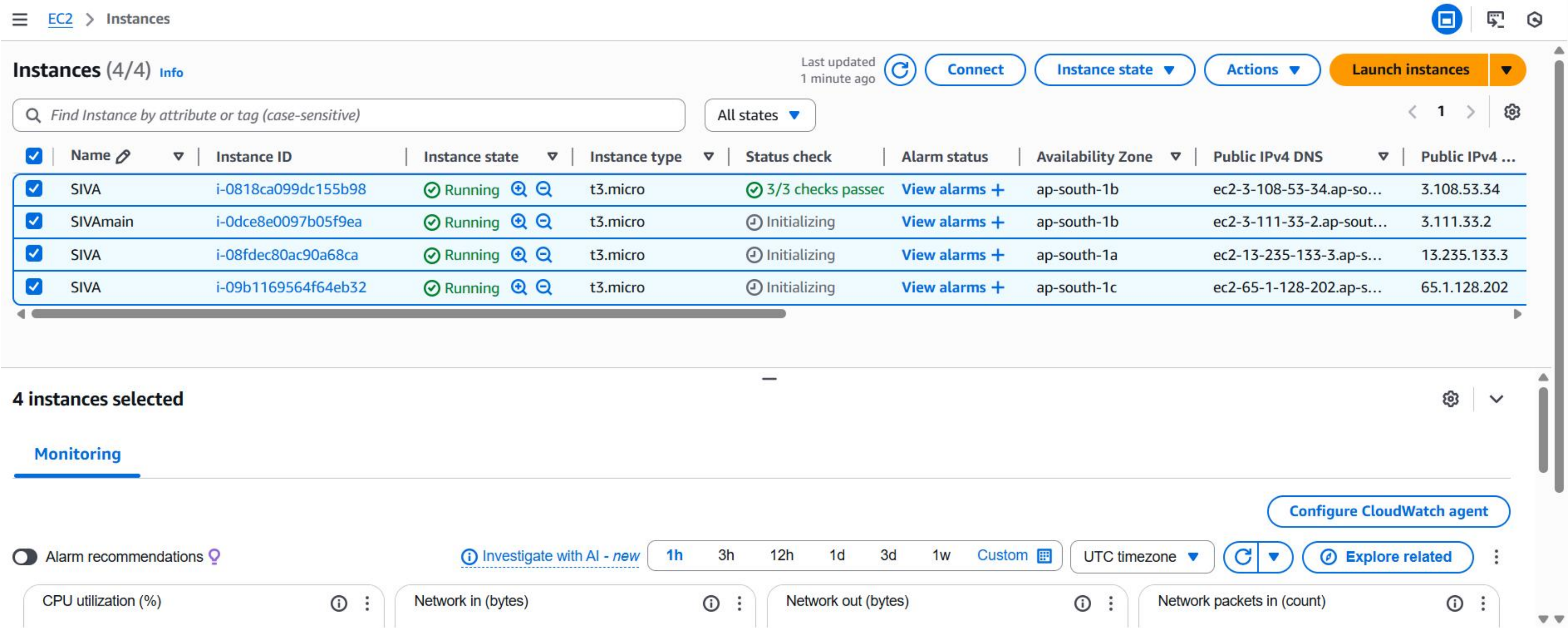
Instance maintenance policy

Replacement behavior	Min healthy percentage	Max healthy percentage
No policy	-	-

Additional settings

Instance scale-in protection	Monitoring	Default instance warmup
Disabled	Enabled	Disabled

Capacity Reservation preference



EC2 > Instances

Instances (4/4) Info

Last updated 1 minute ago

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
☑	SIVA	i-0818ca099dc155b98	✓ Running	t3.micro	✓ 3/3 checks passec	View alarms +	ap-south-1b	ec2-3-108-53-34.ap-so...	3.108.53.34
☑	SIVAmain	i-0dce8e0097b05f9ea	✓ Running	t3.micro	Initializing	View alarms +	ap-south-1b	ec2-3-111-33-2.ap-sout...	3.111.33.2
☑	SIVA	i-08fdec80ac90a68ca	✓ Running	t3.micro	Initializing	View alarms +	ap-south-1a	ec2-13-235-133-3.ap-s...	13.235.133.3
☑	SIVA	i-09b1169564f64eb32	✓ Running	t3.micro	Initializing	View alarms +	ap-south-1c	ec2-65-1-128-202.ap-s...	65.1.128.202

4 instances selected

Monitoring

Step 8 create an another application load balancer :

First we create an target group

Target group---> t.g name : ssa --->select your vpc ---> health checks path: index.html

Go to load balancer ----> create application load balancer

→Create application load balance name ---> select your vpc
→Select availability zones
→Attach target group
→Create application load balancer

→ Attach to auto scalling groups