

## Preeti.3tier-architecture-AWS

### Pre-requisites

1. Download Code from Github to local

git clone <https://github.com/aws-samples/aws-three-tier-web-architecture-workshop.git>

2. S3 Bucket Creation → **3tier-webapp-preeti**
3. IAM EC2 Instance Role Creation → [EC2-SSM-S3-3tier](#)
  - a. AmazonSSMManagedInstanceCore
  - b. AmazonS3ReadOnlyAccess

### Network and security

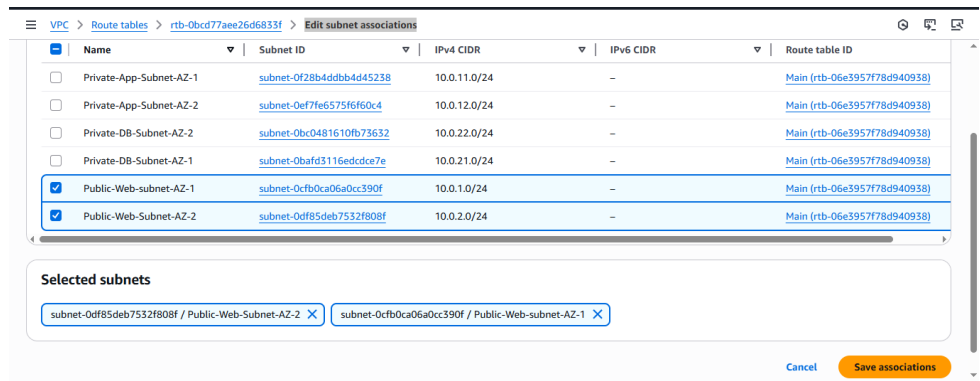
1. Foundation network (VPC)
  - c. **VPC**: 10.0.0.0/16 → 3tier-vpc
  - d. Private-App-Subnet-AZ-1 → 10.0.11.0/24
  - e. Private-App-Subnet-AZ-2 → 10.0.12.0/24
  - f. Private-DB-Subnet-AZ-1 → 10.0.21.0/24
  - g. Private-DB-Subnet-AZ-2 → 10.0.22.0/24
  - h. Public-Web-Subnet-AZ-1 → 10.0.1.0/24
  - i. Public-Web-Subnet-AZ-2 → 10.0.2.0/24
2. **IGW** attached to VPC. → 3-tier-igw attach to 3tier-vpc
3. **1 NAT Gateway** in **one** public subnet.
  - a. 3tier-NAT-AZ1 → Public-Web-subnet-AZ-1 → connectivity-type:Public → allocate-elastic-ip
  - b. 3tier-NAT-AZ2 → Public-Web-subnet-AZ-2 → connectivity-type:Public → allocate-elastic-ip
4. **Route tables**:
  - a. **PublicRouteTable** →

#### i. Edit routes → add route

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
0.0.0.0/0	Internet Gateway	-	No	CreateRoute

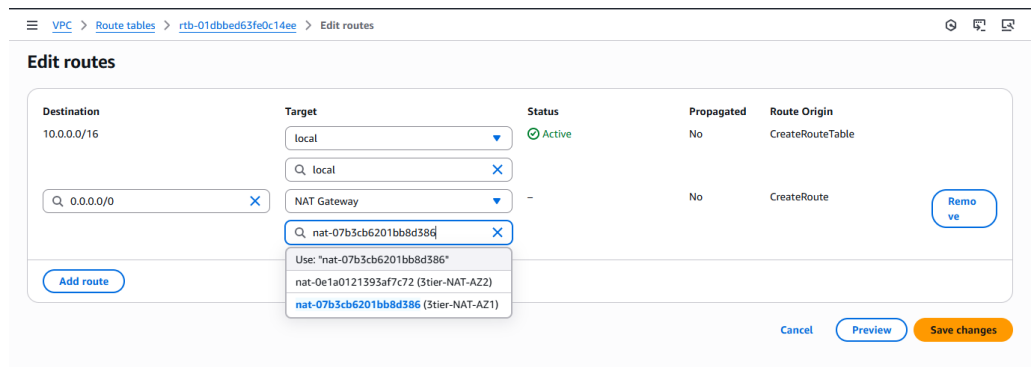
Buttons: Add route, Remove, Cancel, Preview, Save changes

#### ii. Edit subnet associations

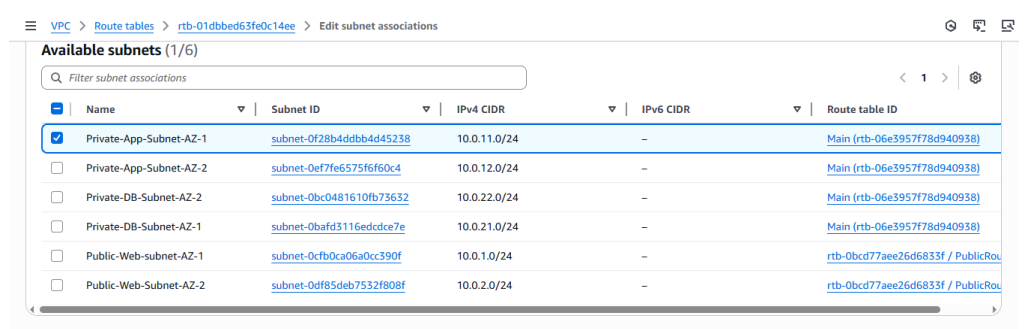


## b. PrivateRouteTable-AZ1→

### i. Edit routes→add route(use target natgateway pf AZ1)



### ii. Edit subnet associations



## c. PrivateRouteTable-AZ2→

### i. Edit routes→add route

### ii. Edit subnet associations

## 5. Security Groups

### a. InternetFacing-Ig-sg

VPC > Security Groups > Create security group

Name cannot be edited after creation.

**Description** [Info](#)

InternetFacing-lg-sg

**VPC** [Info](#)

vpc-01ad458320395fc2b (3tier-vpc)

**Inbound rules** [Info](#)

Type	Protocol	Port range	Source	Description - optional	
HTTP	TCP	80	Any...	0.0.0.0/0	Delete
Custom TCP	TCP	0	Any...	::/0	Delete

## b. WebTier-sg

VPC > Security Groups > Create security group

Name cannot be edited after creation.

**Description** [Info](#)

WebTier

**VPC** [Info](#)

vpc-01ad458320395fc2b (3tier-vpc)

**Inbound rules** [Info](#)

Type	Protocol	Port range	Source	Description - optional	
HTTP	TCP	80	Cus... sg-0a85efd9ff69e47c0		Delete
HTTP	TCP	80	My IP 106.51.46.129/32		Delete

## c. Internal-lg-sg

VPC > Security Groups > Create security group

**Basic details**

**Security group name** [Info](#)

Internal-lb-sg

Name cannot be edited after creation.

**Description** [Info](#)

Internal-lb-sg

**VPC** [Info](#)

vpc-01ad458320395fc2b (3tier-vpc)

**Inbound rules** [Info](#)

Type	Protocol	Port range	Source	Description - optional	
HTTP	TCP	80	Cus... sg-034deaa974994df8c		Delete

Use: "sg-034deaa974994df8c"

CIDR blocks

Security Groups

WebTier-sg | sg-034deaa974994df8c

Prefix lists

## d. PrivateInstances-sg

VPC > Security Groups > Create security group

Name cannot be edited after creation.

**Description** Info

PrivateInstances-sg

**VPC** Info

vpc-01ad458320395fc2b (3tier-vpc)

**Inbound rules** Info

Type	Protocol	Port range	Source	Optional
Custom TCP	TCP	4000	Cus...	
Custom TCP	TCP	4000	My IP	

Use: "sg-03ae92a8df99c252a"

CIDR blocks

Security Groups

Internal-lb-sg | sg-03ae92a8df99c252a

Prefix lists

Q sg-03ae92a8df99c252a X

sg-03ae92a8df99c252a X

106.51.46.129/32 X

Delete

## e. DB-SG

VPC > Security Groups > Create security group

Name cannot be edited after creation.

**Description** Info

DB-sg

**VPC** Info

vpc-01ad458320395fc2b (3tier-vpc)

**Inbound rules** Info

Type	Protocol	Port range	Source	Optional
MYSQL/Aurora	TCP	3306	Cus...	

Add rule

Use: "sg-0dc1a61be1fbae7a"

CIDR blocks

Security Groups

PrivateInstances-sg | sg-0dc1a61be1fbae7a

Prefix lists

Q sg-0dc1a61be1fbae7a X

sg-0dc1a61be1fbae7a X

Delete

## DB-deployment(Aurora MySQL (DB tier))

- Go to RDS → subnet groups → create DB subnet group

Aurora and RDS > Subnet groups > Create DB subnet group

**VPC**

Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

3tier-vpc (vpc-01ad458320395fc2b)  
6 Subnets, 2 Availability Zones

**Add subnets**

**Availability Zones**

Choose the Availability Zones that include the subnets you want to add.

Choose an availability zone

ap-south-1a X ap-south-1b X

**Subnets**

Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

Select subnets

Private-DB-Subnet-AZ-1  
Subnet ID: subnet-0baf03116edc0e7e CIDR: 10.0.21.0/24 X

Private-DB-Subnet-AZ-2  
Subnet ID: subnet-0bc0481610fb73632 CIDR: 10.0.22.0/24 X

- Create DB

Aurora and RDS

>

Create database

Create database

Info

Choose a database creation method

☒ Standard create

You set all of the configuration options, including ones for availability, security, backups, and maintenance.

☐ Easy create


Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options


Engine type

Info


☒ Aurora (MySQL Compatible)



☐ Aurora (PostgreSQL Compatible)



☐ MySQL



☐ PostgreSQL

☐ MariaDB

☐ Oracle

Templates

Choose a sample template to meet your use case.

☐ Production

Use defaults for high availability and fast, consistent performance.

☒ Dev/Test

This instance is intended for development use outside of a production environment.

Settings

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

Account ID: 1952-7567-5477

Preeti B

Aurora and RDS

>

Create database

Master username

Info

Type a login ID for the master user of your DB instance.

admin

1 to 32 alphanumeric characters. The first character must be a letter.

Credentials management

You can use AWS Secrets Manager or manage your master user credentials.

☐ Managed in AWS Secrets Manager - *most secure*

RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

☒ Self managed

Create your own password or have RDS create a password that you manage.

☐ Auto generate password

Amazon RDS can generate a password for you, or you can specify your own password.

Master password

Info

\*\*\*\*\*

Password strength

Weak

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' \* @

Confirm master password

Info

\*\*\*\*\*

Availability & durability

Multi-AZ deployment

Info

☒ Create an Aurora Replica or Reader node in a different AZ (recommended for scaled availability)

Creates an Aurora Replica for fast failover and high availability.

☐ Don't create an Aurora Replica

**DB subnet group** [Info](#)

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB cluster can use in the VPC that you selected.

**three-tier-db-sg**  
2 Subnets, 2 Availability Zones

**Public access** [Info](#)

☐ Yes  
RDS assigns a public IP address to the cluster. Amazon EC2 instances and other resources outside of the VPC can connect to your cluster. Resources inside the VPC can also connect to the cluster. Choose one or more VPC security groups that specify which resources can connect to the cluster.

☒ No  
RDS doesn't assign a public IP address to the cluster. Only Amazon EC2 instances and other resources inside the VPC can connect to your cluster. Choose one or more VPC security groups that specify which resources can connect to the cluster.

**VPC security group (firewall)** [Info](#)

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

☒ Choose existing  
Choose existing VPC security groups

☐ Create new  
Create new VPC security group

**Existing VPC security groups**

Choose one or more options

DB-sg [X](#)

**three-tier-db-sg**

**Subnet group details**

VPC ID  
vpc-01ad458320395fc2b

ARN  
arn:aws:rds:ap-south-1:195275675477:subgrp:three-tier-db-sg

**Supported network types**  
IPv4

**Description**  
three-tier-DB-sg

**Subnets (2)**

Availability zone	Subnet name	Subnet ID	CIDR block
ap-south-1b	Private-DB-Subnet-AZ-2	subnet-0bc0481610fb73652	10.0.22.0/24
ap-south-1a	Private-DB-Subnet-AZ-1	subnet-0bafd3116edcdce7e	10.0.21.0/24

**Tags (0)**

[Manage tags](#)

**database-1**

[Modify](#) [Actions](#)

**Related**

Filter by databases

DB identifier	Status	Role	Engine	Region	Size	Recom...	CPU	Curren...	Mainte...
database-1	Available	Regional c...	Aurora My...	ap-south-1	2 instances	-	-	-	none
database-1-instance-1	Available	Writer ins...	Aurora My...	ap-south-1a	db.r7g.large	8.18%	2 Sele...	none	
database-1-instance-1-ap-south-1b	Available	Reader ins...	Aurora My...	ap-south-1b	db.r7g.large	8.07%	2 Sele...	none	

[Connectivity & security](#) [Monitoring](#) [Logs & events](#) [Configuration](#) [Zero-ETL integrations](#) [Maintenance & backups](#) [Data migrations - new](#) [Tags](#) [Re...](#)

**Endpoints (2)**

Find resources

Endpoint name	Status	Type	Port
database-1.cluster-cbuk8ak4hzf.ap-south-1.rds.amazonaws.com	Available	Writer	3306
database-1.cluster-ro-cbuk8ak4hzf.ap-south-1.rds.amazonaws.com	Available	Reader	3306

## App Tier Instance Deployment:

### 1. Create EC2-instance → AppServer

EC2 > Instances > Launch an instance

Launch the instance.

**Key pair name - required**

Proceed without a key pair (Not recommended) Default value [Create new key pair](#)

**▼ Network settings** [Info](#)

**VPC - required** [Info](#)

vpc-01ad458320395fc2b (3tier-vpc) 10.0.0.0/16 [Create new VPC](#)

**Subnet** [Info](#)

subnet-0f28b4ddb4d45238 Private-App-Subnet-AZ-1  
VPC: vpc-01ad458320395fc2b Owner: 195275675477  
Availability Zone: ap-south-1a (aps1-az1) Zone type: Availability Zone  
IP addresses available: 251 CIDR: 10.0.11.0/24 [Create new subnet](#)

**Auto-assign public IP** [Info](#)

Disable

**▼ Summary**

**Number of instances** [Info](#)

1

**Software Image (AMI)**  
Amazon Linux 2023 AMI 2023.8.2...[read more](#)  
ami-0144277607031eca2

**Virtual server type (instance type)**  
t2.micro

**Firewall (security group)**  
New security group

**Storage (volumes)**

[Cancel](#) [Launch instance](#) [Preview code](#)

---

EC2 > Instances > Launch an instance

☐ Create security group ☒ Select existing security group

**Common security groups** [Info](#)

Select security groups

PrivateInstances-sg sg-0dcb1a61be1fbae7a [Compare security group rules](#)  
VPC: vpc-01ad458320395fc2b

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

► **Advanced network configuration**

**▼ Advanced details** [Info](#)

**Domain join directory** [Info](#)

Select [Create new directory](#)

**IAM instance profile** [Info](#)

EC2-SSM-S3-3tier  
arn:aws:iam::195275675477:instance-profile/EC2-SSM-S3-3tier [Create new IAM profile](#)

**Hostname type** [Info](#)

IP name

**DNS Hostname** [Info](#)

**▼ Summary**

**Number of instances** [Info](#)

1

**Software Image (AMI)**  
Amazon Linux 2023 AMI 2023.8.2...[read more](#)  
ami-0144277607031eca2

**Virtual server type (instance type)**  
t2.micro

**Firewall (security group)**  
PrivateInstances-sg

**Storage (volumes)**

[Cancel](#) [Launch instance](#)

## 2. Connect to SSM

- sudo -su ec2-user
- ping 8.8.8.8
- sudo dnf install -y <https://dev.mysql.com/get/mysql84-community-release-el9-1.noarch.rpm>
- sudo rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql
- sudo dnf install -y mysql
- connect to DB → copy RDS writer endpoint
  - mysql -h database-1-instance-1.cbukc8ak4hzf.ap-south-1.rds.amazonaws.com -u admin -p
  - CREATE DATABASE webappdb;
  - SHOW DATABASES;
  - USE webappdb;
  - CREATE TABLE IF NOT EXISTS transactions(id INT NOT NULL AUTO\_INCREMENT, amount DECIMAL(10,2), description VARCHAR(100), PRIMARY KEY(id));
  - SHOW TABLES;

- g. INSERT INTO transactions (amount,description) VALUES ('400','groceries');
- h. SELECT \* FROM transactions;
- i. Exit
- g. Go to s3 and upload files of app-tier by updating DbConfig.js with your values

```
module.exports = Object.freeze({
  DB_HOST : 'database-1-instance-1.cbukc8ak4hzf.ap-south-1.rds.amazonaws.com',
  DB_USER : 'admin',
  DB_PWD : '123456',
  DB_DATABASE : 'webappdb'
});
```

- h. Go to session manager
  - a. curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.38.0/install.sh | bash
  - b. source ~/.bashrc
  - c. nvm install 16
  - d. nvm use 16
  - e. npm install -g pm2
  - f. cd ~/
  - g. aws s3 cp s3://3tier-webapp-preeti/app-tier/ app-tier --recursive
  - h. cd ~/app-tier
  - i. npm install
  - j. pm2 start index.js
  - k. pm2 list
  - l. pm2 logs
  - m. pm2 startup
  - n. sudo env PATH=\$PATH:/home/ec2-user/.nvm/versions/node/v16.20.2/bin  
/home/ec2-user/.nvm/versions/node/v16.20.2/lib/node\_modules/pm2/bin/pm2  
startup systemd -u ec2-user --hp /home/ec2-user
  - o. pm2 save
  - p. curl <http://localhost:4000/health>
  - q. curl <http://localhost:4000/transaction>

### Internal Load Balancing and Auto Scaling

1. Navigate to EC2 dashboard. Select the app tier instance we created and under Actions select Image and templates. Create AMI of it.
2. Goto target group and create one



aws Search [Alt+S] Asia Pacific (Mumbai) Account ID: 1952-7567-5477 Preeti B

EC2 > Target groups > AppTier-tg

aws:elasticloadbalancing:ap-south-1:195275675477:targetgroup/AppTier-tg/ee2ab9ecaa4553c3

Target type Instance	Protocol : Port HTTP: 4000	Protocol version HTTP1	VPC vpc-01ad458320395fc2b
IP address type IPv4	Load balancer None associated		

0 Total targets	0 Healthy	0 Unhealthy	0 Unused	0 Initial	0 Draining
--------------------	--------------	----------------	-------------	--------------	---------------

0 Anomalous

Targets Monitoring Health checks Attributes Tags

Health check settings

Protocol HTTP	Path /health	Port Traffic port	Healthy threshold 2 consecutive health check successes
------------------	-----------------	----------------------	---

Edit

### 3. Internal Load Balancer

EC2 > Load balancers > Create Application Load Balancer

Load balancer name

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

App-tier-internal-lb

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.
- Compatible with the IPv4 and Dualstack IP address types.

Load balancer IP address type | Info

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

☒ IPv4

Includes only IPv4 addresses.

☐ Dualstack

Includes IPv4 and IPv6 addresses.

EC2 > Load balancers > Create Application Load Balancer

vpc-01ad458320395fc2b (3tier-vpc)  
10.0.0.0/16

Create VPC

IP pools - new | Info

You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view Pools in the [Amazon VPC IP Address Manager console](#).

☐ Use IPAM pool for public IPv4 addresses

Compatible with Internet-facing scheme, IPv4 and Dualstack IP address types.

Availability Zones and subnets | Info

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

☒ 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-0f28b4ddb4d45238  
IPv4 subnet CIDR: 10.0.11.0/24

Private-App-Subnet-AZ-1

☒ 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-0ef7fe6575f6f60c4  
IPv4 subnet CIDR: 10.0.12.0/24

Private-App-Subnet-AZ-2

EC2 > Load balancers > Create Application Load Balancer

Security groups

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

Internal-lb-sg

sg-03ae92a8df99c252a VPC: vpc-01ad458320395fc2b

Listeners and routing

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

Forward to AppTier-tg

Target type: Instance, IPv4

HTTP

Remove

Create target group

## Create load balancer

### 4. Create launch template

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

Launch template name - required

App-tier-launch-template

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

Template version description

A nnnnd wehserver for MuAnn

Summary

Software Image (AMI)

-

Virtual server type (instance type)

-

Firewall (security group)

-

Storage (volumes)

-

EC2 > Launch templates > Create launch template

Recents My AMIs Quick Start

Don't include in launch template

Owned by me

Shared with me

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

AppServerImage

ami-02f8d6292e2c948b9

2025-08-15T15:57:03.000Z Virtualization: hvm ENA enabled: true Root device type: ebs Boot mode: uefi-preferred

Description

Appserverimage

Architecture x86\_64

AMI ID ami-02f8d6292e2c948b9

Summary

Software Image (AMI)

Appserverimage

ami-02f8d6292e2c948b9

Virtual server type (instance type)

-

Firewall (security group)

-

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours

Cancel

Create launch template

Instance type

Advanced

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Windows base pricing: 0.017 USD per Hour

On-Demand RHEL base pricing: 0.0268 USD per Hour

On-Demand Linux base pricing: 0.0124 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour

On-Demand SUSE base pricing: 0.0124 USD per Hour

Free tier eligible

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

Appserverimage

ami-02f8d6292e2c948b9

Virtual server type (instance type)

t2.micro

Firewall (security group)

PrivateInstances-sg

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours

▼ 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.

Availability Zone

Info

Don't include in launch template

▼

↻ Enable additional zones

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

▼

PrivateInstances-sg sg-Qdcb1a61be1fbae7a

×

VPC: vpc-01ad458320395fc2b

↻ Compare security group rules

Appserverimage

ami-02f8d6292e2c948b9

Virtual server type (instance type)

t2.micro

Firewall (security group)

PrivateInstances-sg

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours

×

Cancel

Create launch template

▼ Advanced details

Info

IAM instance profile

Info

EC2-SSM-S3-3tier

▼

arn:aws:iam::195275675477:instance-profile/EC2-SSM-S3-3tier

↻ Create new IAM profile

Hostname type

Info

Don't include in launch template

▼

## Create auto-scaling-groups

### 5. Create ASG

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

Account ID: 1952-7567-5477

Preeti B

EC2 > Auto Scaling groups > Create Auto Scaling group

Choose launch template

Step 2

Choose instance launch options

Step 3 - optional

Integrate with other services

Step 4 - optional

Configure group size and scaling

Step 5 - optional

Add notifications

Step 6 - optional

Add tags

Step 7

Review

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name

Enter a name to identify the group.

AppTierASG

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.

App-tier-launch-template

↻

Create a launch template

EC2 > Auto Scaling groups > Create Auto Scaling group

Choose VPC

Step 3

Choose instance launch options

Step 4 - optional

Integrate with other services

Step 5 - optional

Configure group size and scaling

Step 6 - optional

Add notifications

Step 7

Review

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

vpc-01ad458320395fc2b (3tier-vpc)

▼

↻

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

▼

↻

aps1-az1 (ap-south-1a) | subnet-0f28b4ddb4d45238 (Private-App-Subnet-AZ-1)

×

10.0.11.0/24

aps1-az3 (ap-south-1b) | subnet-0ef7fe6575f6f60c4 (Private-App-Subnet-AZ-2)

×

10.0.12.0/24

Create a subnet

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 4 - optional  
 Step 5 - optional  
 Step 6 - optional  
 Step 7  
 Review

☐ 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

AppTier-tg | HTTP  
 Application Load Balancer: App-tier-internal-lb

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 6 - optional  
 Add tags  
 Step 7  
 Review

**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**  
 2  
 Equal or less than desired capacity

**Max desired capacity**  
 2  
 Equal or greater than desired capacity

**Automatic scaling - optional**  
 Choose whether to use a target tracking policy | Info

☒ 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.

aws Search [Alt+S] Asia Pacific (Mumbai) Account ID: 1952-7567-5477 Preeti B

EC2 > Target groups > AppTier-tg

**AppTier-tg** Actions

**Details**  
 arn:aws:elasticloadbalancing:ap-south-1:195275675477:targetgroup/AppTier-tg/ee2ab9ecaa4553c3

<b>Target type</b> Instance	<b>Protocol : Port</b> HTTP: 4000	<b>Protocol version</b> HTTP1	<b>VPC</b> <a href="#">vpc-01ad458320395fc2b</a>
<b>IP address type</b> IPv4	<b>Load balancer</b> <a href="#">App-tier-internal-lb</a>		

2 Total targets	2 Healthy 0 Anomalous	0 Unhealthy	0 Unused	0 Initial	0 Draining
--------------------	-----------------------------	----------------	-------------	--------------	---------------

**Distribution of targets by Availability Zone (AZ)**  
 Select values in this table to see corresponding filters applied to the Registered targets table below.

## Web Tier Instance Deployment

1. Update Config File → **application-code/nginx.conf**
2. Upload **webtier** and **nginx.conf** to s3 bucket.
3. Create ec2-instance → WebServer

Search

[Alt+S]

Asia Pacific (Mumbai)Account ID: 1952-7567-5477Preeti R

Amazon S3> Buckets> 3tier-webapp-preeti

3tier-webapp-preeti

Objects (3)

Copy S3 URICopy URLDownloadOpenDeleteActionsCreate folderUpload

Find objects by prefix

	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	app-tier/	Folder	-	-	-
<input type="checkbox"/>	nginx.conf	conf	August 16, 2025, 02:31:10 (UTC+05:30)	2.6 KB	Standard
<input type="checkbox"/>	web-tier/	Folder	-	-	-

EC2> Instances> Launch an instance

Name and tags

Name

WebServer

Add additional tags

Application and OS Images (Amazon Machine Image)

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

RecentsMy AMIsQuick Start

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Del

Browse more AMIs

Summary

Number of instances

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.8.2...[read more](#)

ami-0144277607031eca2

Virtual server type (instance type)

t2.micro

Firewall (security group)

WebTier-sg

Storage (volumes)

Cancel

Launch instance

Preview code

Instance type

Info | Get advice

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Windows base pricing: 0.017 USD per Hour

On-Demand RHEL base pricing: 0.0268 USD per Hour On-Demand Linux base pricing: 0.0124 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour

On-Demand SUSE base pricing: 0.0124 USD per Hour

Free tier eligible

All generations

Compare instance types

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 - required

Proceed without a key pair (Not recommended)

Default value

Create new key pair

**VPC - required** | [Info](#)

vpc-01ad458320395fc2b (3tier-vpc)  
10.0.0.0/16

**Subnet** | [Info](#)

subnet-0cfb0ca06a0cc390f **Public-Web-subnet-AZ-1**  
VPC: vpc-01ad458320395fc2b Owner: 195275675477  
Availability Zone: ap-south-1a (aps1-az1) Zone type: Availability Zone  
IP addresses available: 250 CIDR: 10.0.1.0/24

**Auto-assign public IP** | [Info](#)

Enable

Additional charges apply when outside of free tier allowance

**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

WebTier-sg sg-034deaa974994df8c X  
VPC: vpc-01ad458320395fc2b

Compare security group rules

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

---

**Advanced details** | [Info](#)

**Domain join directory** | [Info](#)

Select

Create new directory

**IAM instance profile** | [Info](#)

EC2-SSM-S3-3tier  
arn:aws:iam::195275675477:instance-profile/EC2-SSM-S3-3tier

Create new IAM profile

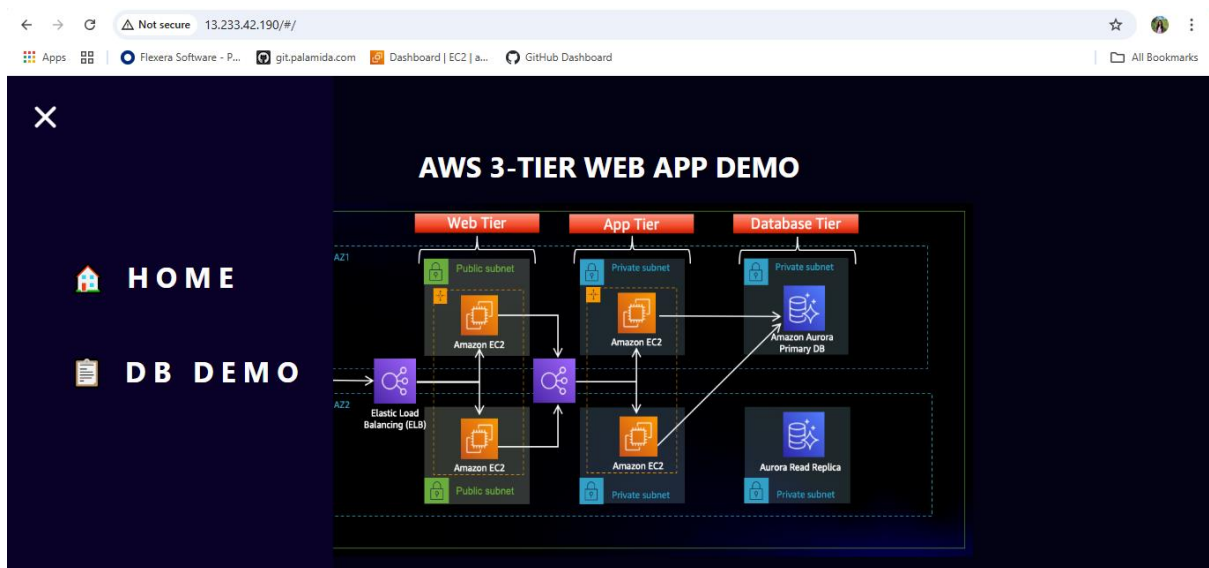
**Hostname type** | [Info](#)

IP name

#### 4. Connect to session manager

- a. `sudo -su ec2-user`
- b. `ping 8.8.8.8`
- c. `curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.38.0/install.sh | bash`
- d. `source ~/.bashrc`
- e. `nvm install 16`
- f. `nvm use 16`
- g. `cd ~/`
- h. `aws s3 cp s3://3tier-webapp-preeti/web-tier/ web-tier --recursive`
- i. `cd ~/web-tier`
- j. `npm install`
- k. `npm run build`
- l. `sudo dnf install -y nginx`
- m. `cd /etc/nginx`
- n. `ls`
- o. `sudo cp nginx.conf nginx.conf_backup`

- p. `sudo rm nginx.conf`
- q. `sudo aws s3 cp s3://3tier-webapp-preeti/nginx.conf`
- .
- r. `sudo service nginx restart`
- s. `chmod -R 755 /home/ec2-user`
- t. `sudo chkconfig nginx on`



ID	AMOUNT	DESC
1	400	groceries

- 5. create image of webserver → WebServerImage
- 6. create target group → WebTier-tg

EC2 > Target groups > Create target group

**Target group name**  
 WebTier-tg  
 A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

**Protocol**  
 Protocol for load balancer-to-target communication. Can't be modified after creation.  
 HTTP

**Port**  
 Port number where targets receive traffic. Can be overridden for individual targets during registration.  
 80  
 1-65535

**IP address type**  
 Only targets with the indicated IP address type can be registered to this target group.  
☒ **IPv4**  
 Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.  
☐ **IPv6**  
 Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

**VPC**  
 Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.  
 vpc-01ad458320395fc2b (3tier-vpc)  
 10.0.0.0/16

Create VPC

EC2 > Target groups > Create target group

☐ **gRPC**  
 Send requests to targets using gRPC. Supported when the request protocol is gRPC.

**Health checks**  
 The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

**Health check protocol**  
 HTTP

**Health check path**  
 Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.  
 /health  
 Up to 1024 characters allowed.

► **Advanced health check settings**

## 7. create external-load-balancer → Web-tier-external-lb

EC2 > Load balancers > Create Application 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.  
 Web-tier-external-lb  
 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.
- Compatible with the **IPv4** and **Dualstack** IP address types.

**Load balancer IP address type** | Info  
 Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

☒ **IPv4**  
 Includes only IPv4 addresses.

☐ **Dualstack**  
 Includes IPv4 and IPv6 addresses.

☐ **Dualstack without public IPv4**  
 Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.



**EC2** > **Load balancers** > Create Application Load Balancer

**Network mapping** [Info](#)

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

**VPC** | [Info](#)

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#).

**vpc-01ad458320395fc2b (stier-vpc)** [Create VPC](#)

**IP pools** - [new](#) | [Info](#)

You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view Pools in the [Amazon VPC IP Address Manager console](#).

☐ Use IPAM pool for public IPv4 addresses

The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

**Availability Zones and subnets** | [Info](#)

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

☒ **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-0cfb0ca06a0cc390f** [Public-Web-subnet-AZ-1](#)

IPv4 subnet CIDR: 10.0.0.0/16

☒ **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-0df85deb7532f808f** [Public-Web-Subnet-AZ-2](#)

IPv4 subnet CIDR: 10.0.2.0/24

**EC2** > **Load balancers** > Create Application 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

**internetFacing-ig-sg** [X](#)

sg-0a85ef97f67e47c0 VPC: vpc-01ad458320395fc2b

**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 **Default action** | [Info](#)

Forward to **WebTier-tg** HTTP [Create target group](#)

Target type: Instance, IPv4

**Listener tags - optional**

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

## 8. Create launch template → Web-tier-launch-template

**EC2** > **Launch templates** > Create launch template

**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](#).

**Recents** **My AMIs** **Quick Start**

☐ Don't include in launch template ☒ Owned by me ☐ Shared with me

[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

**Amazon Machine Image (AMI)**

**WebServerImage**

ami-02d2cbaff1ccad117

2025-08-15T21:34:00.000Z Virtualization: hvm ENA enabled: true Root device type: ebs Boot mode: uefi-preferred

**Description**

WebServerImage

▼ Instance type

Info | [Get advice](#)

Advanced

Instance type

t2.micro

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

Free tier eligible

On-Demand RHEL base pricing: 0.0268 USD per Hour On-Demand Linux base pricing: 0.0124 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0142 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

▼ 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

Don't include in launch template

▼

↻

Create new key pair

☰

[EC2](#) > [Launch templates](#) > Create 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.

Availability Zone

Info

Don't include in launch template

▼

↻

Enable additional zones

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

▼

WebTier-sg sg-034deaa974994df8c

×

VPC: vpc-01ad458320395fc2b

↻

Compare security group rules

▶ Advanced network configuration

▼ Advanced details

Info

IAM instance profile

Info

EC2-SSM-S3-3tier

am:aws:iam:195275675477:instance-profile/EC2-SSM-S3-3tier

▼

↻

Create new IAM profile

Hostname type

Info

Don't include in launch template

▼

DNS Hostname

Info

☐ Enable resource-based IPv4 (A record) DNS requests

☐ Enable resource-based IPv6 (AAAA record) DNS requests

## 9. Create autoscalinggroup→WebTierASG

Step 1

Choose launch template

Step 2

Choose instance launch options

Step 3 - optional

Integrate with other services

Step 4 - optional

Configure group size and scaling

Step 5 - optional

Add notifications

Step 6 - optional

Add tags

Step 7

Review

## Choose launch template Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

**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**  

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.  
  
[Create a launch template](#)

**Version**  
  
[Create a launch template version](#)

Step 6 - optional

Add tags

Step 7

Review

**Instance type**  
t2.micro

**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.  
  
[Create a VPC](#)  
**Availability Zones and subnets**  
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.  
  

aps1-az1 (ap-south-1a) | subnet-0cfb0ca06a0cc390f (Public-Web-subnet-AZ-1)

aps1-az3 (ap-south-1b) | subnet-0df85deb7532f808f (Public-Web-Subnet-AZ-2)

  
[Create a subnet](#)  
**Availability Zone distribution - new**  
Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone, select a strategy:  

☒ **Balanced best effort**  
If launches fail in one Availability Zone, Auto Scaling will attempt to launch in another healthy Availability Zone.

☐ **Balanced only**  
If launches fail in one Availability Zone, Auto Scaling will continue to attempt to launch in the unhealthy Availability Zone to preserve balanced distribution.

Step 3 - optional

Integrate with other services

Step 4 - optional

Configure group size and scaling

Step 5 - optional

Add notifications

Step 6 - optional

Add tags

Step 7

Review

**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.  
  

WebTier-tg | HTTP

**VPC Lattice integration options Info**  
To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.  
**Select VPC Lattice service to attach**

**EC2 > Auto Scaling groups > Create Auto Scaling group**

Step 3 - optional: Integrate with other services  
 Step 4 - optional: **Configure group size and scaling**  
 Step 5 - optional: Add notifications  
 Step 6 - optional: Add tags  
 Step 7: Review

**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.

**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**   
 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.

**EC2 > Instances**

EC2 Dashboard  
 EC2 Global View  
 Events

**Instances**  
 Instances  
 Instance Types  
 Launch Templates  
 Spot Requests  
 Savings Plans  
 Reserved Instances  
 Dedicated Hosts  
 Capacity Reservations

**Images**  
 AMIs  
 AMI Catalog

**Elastic Block Store**  
 Volumes  
 Snapshots  
 Lifecycle Manager

**Instances (9)** Info  
 Last updated less than a minute ago  
 Connect Instance state Actions Launch instances

Find instance by attribute or tag (case-sensitive)  All states

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public
<input type="checkbox"/>	server2	i-0310244081d7b3a67	Stopped	t2.medium	–	<a href="#">View alarms +</a>	ap-south-1b	–	–
<input type="checkbox"/>	Agent	i-0ee28a2fbb8948a54	Stopped	t2.micro	–	<a href="#">View alarms +</a>	ap-south-1b	–	–
<input checked="" type="checkbox"/>		i-0e7904bc7d1ae79b8	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	ap-south-1b	–	–
<input checked="" type="checkbox"/>		i-0fdd8ea4960733d8f	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	ap-south-1b	–	–
<input type="checkbox"/>	ubuntu	i-06f060b10ebf0f569	Stopped	t2.micro	–	<a href="#">View alarms +</a>	ap-south-1a	–	–
<input checked="" type="checkbox"/>		i-090ad2f4c4aab730d	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	ap-south-1a	–	–
<input type="checkbox"/>	AppServer	i-0311ca293877aec57	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	ap-south-1a	–	–
<input type="checkbox"/>	WebServer	i-06ca67b6eb1497bf0	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	ap-south-1a	–	13.233
<input checked="" type="checkbox"/>		i-0a9125f87be260c34	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	ap-south-1a	–	–

Select an instance

**EC2 > Target groups > WebTier-tg**

**WebTier-tg** Actions

**Details**  
 arn:aws:elasticloadbalancing:ap-south-1:195275675477:targetgroup/WebTier-tg/s0becbfcfc7817e

<b>Target type</b> Instance	<b>Protocol : Port</b> HTTP: 80	<b>Protocol version</b> HTTP1	<b>VPC</b> <a href="#">vpc-01ad458320395fc2b</a>
<b>IP address type</b> IPv4	<b>Load balancer</b> <a href="#">Web-tier-external-lb</a>		

2 Total targets      2 Healthy      0 Unhealthy      0 Anomalous      0 Unused      0 Initial      0 Draining

**Distribution of targets by Availability Zone (AZ)**  
 Select values in this table to see corresponding filters applied to the Registered targets table below.

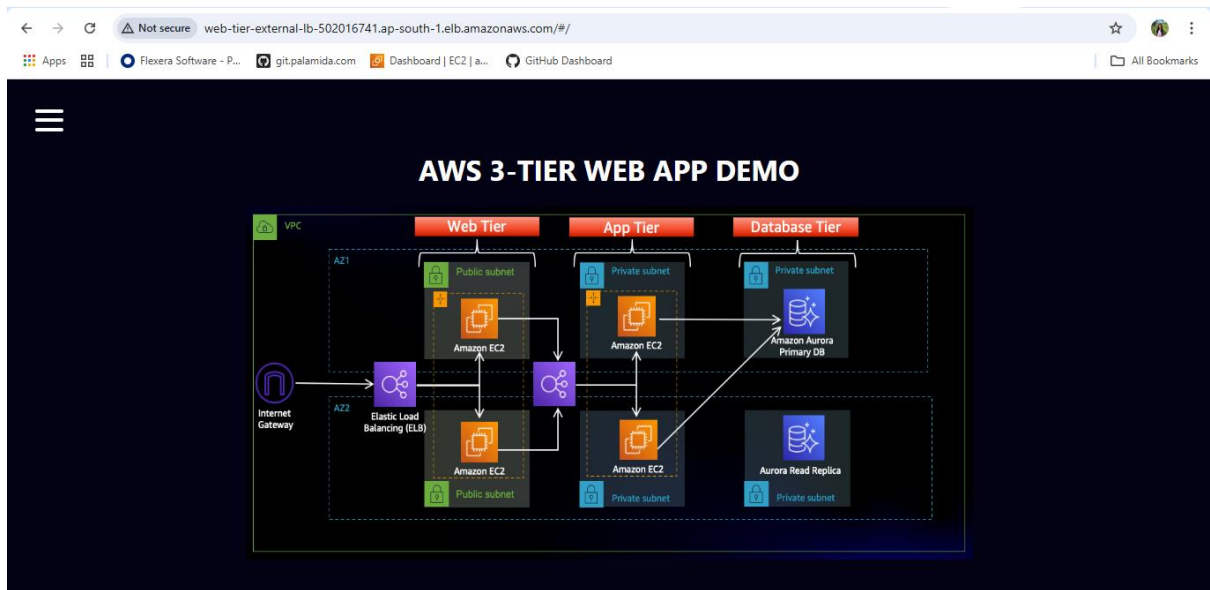
**Targets**   Monitoring   Health checks   Attributes   Tags

**Registered targets (2)** Info      Anomaly mitigation: **Not applicable**      Deregister      Register targets

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

10. Hit the DNS of external loadbalancer → **Web-tier-external-lb**

**Web-tier-external-lb-502016741.ap-south-1.elb.amazonaws.com**



← → ↻ Not secure web-tier-external-lb-502016741.ap-south-1.elb.amazonaws.com/#/db Apps Flexera Software - P... git.palamida.com Dashboard | EC2 | a... GitHub Dashboard All Bookmarks

×

HOME

DB DEMO

### AURORA DATABASE DEMO PAGE

DEL

ID	AMOUNT	DESC
ADD		
1	400	groceries
2	200	apple
3	100	orange
4	250	veggies