Designing a Highly Available 3-Tier Web Application Architecture on AWS

What is AWS?

Amazon Web Services (AWS) is a comprehensive and widely adopted cloud platform offering over 200 fully featured services from data centers globally. These services include computing power, storage options, and various tools for databases, machine learning, analytics, and more. AWS helps businesses scale and grow by providing flexible, reliable, scalable, easy-to-use, and cost-effective cloud computing solutions.

Why Use AWS?..

1. Scalability:

   - Automatic Scaling: AWS can automatically scale resources up or down based on demand, ensuring that applications run smoothly without overprovisioning or underutilizing resources.

   - Elastic Load Balancing: Distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses, improving availability and fault tolerance.

2. Cost Efficiency:

   - Pay-as-You-Go: AWS follows a pay-as-you-go pricing model, meaning you only pay for the services you use, reducing upfront capital expenditure.

   - Cost Management Tools: AWS provides tools like AWS Cost Explorer and AWS Budgets to monitor and optimize spending.

3. Security:

   - Data Protection: AWS offers robust security services and features, including encryption, threat detection, and identity management.

   - Compliance Certifications: AWS meets a wide range of compliance standards such as GDPR, HIPAA, and SOC.

4. Global Reach:

   - Global Infrastructure: AWS operates in multiple geographic regions worldwide, ensuring low latency and high availability.

   - Content Delivery Network (CDN): Amazon CloudFront delivers content globally with low latency and high transfer speeds.

Real-Time Use Cases

1. Web Hosting:

- Scalable Websites: Companies can host scalable websites using Amazon EC2, Amazon S3, and Amazon RDS.

- Static and Dynamic Content: AWS supports both static (via Amazon S3) and dynamic content (using Amazon EC2 and databases).

2. Data Backup and Storage:

- Reliable Storage: AWS offers reliable storage solutions such as Amazon S3 and Amazon Glacier for backups, data archiving, and disaster recovery.

- High Durability: Amazon S3 provides 99.999999999% (11 9's) of data durability.

3. Big Data and Analytics:

- Data Processing: AWS services like Amazon EMR, AWS Glue, and Amazon Redshift help process and analyze large datasets.

- Real-Time Analytics: Amazon Kinesis allows for real-time data streaming and analytics.

4. DevOps:

- Continuous Integration and Delivery (CI/CD): AWS offers tools like AWS CodePipeline, AWS CodeBuild, and AWS CodeDeploy for automating code deployments.

- Infrastructure as Code (IaC): Services like AWS CloudFormation and AWS CDK allow developers to define infrastructure using code.

What is 3 tier architecture?..

A 3-tier architecture is a well-established software architecture that separates applications into three logical and physical computing tiers. Each tier is responsible for specific tasks and can be developed, maintained, and scaled independently. The three tiers are:

1. Presentation Tier (Client Tier):

- This is the user interface layer, where the user interacts with the application. It can be a web browser, desktop application, or mobile app.
- It is responsible for displaying information to the user and collecting user input.
- Technologies commonly used: HTML, CSS, JavaScript, React, Angular, Vue.js.

2. Application Tier (Logic Tier or Middle Tier):

- This is the business logic layer, where data processing occurs. It acts as an intermediary between the presentation tier and the data tier.
- It handles business rules, computations, and data manipulation.
- Technologies commonly used: Java, .NET, Python, Node.js, Ruby on Rails.

3. Data Tier (Database Tier or Storage Tier):

- This is the database layer, where data is stored and managed. It includes databases and data storage systems.
- It handles data retrieval, storage, and management.
- Technologies commonly used: MySQL, PostgreSQL, MongoDB, Oracle, SQL Server.

Benefits of 3-Tier Architecture:

- Separation of Concerns: Each tier can be developed and maintained independently, making the application more modular and easier to manage.
- Scalability: Each tier can be scaled independently based on load and performance requirements.
- Maintainability: Changes in one tier do not necessarily impact the other tiers, making it easier to update and maintain.
- Reusability: Business logic and data access layers can be reused across different applications and projects.

- Flexibility: Different technologies can be used in each tier, allowing for the best tools to be chosen for specific tasks.

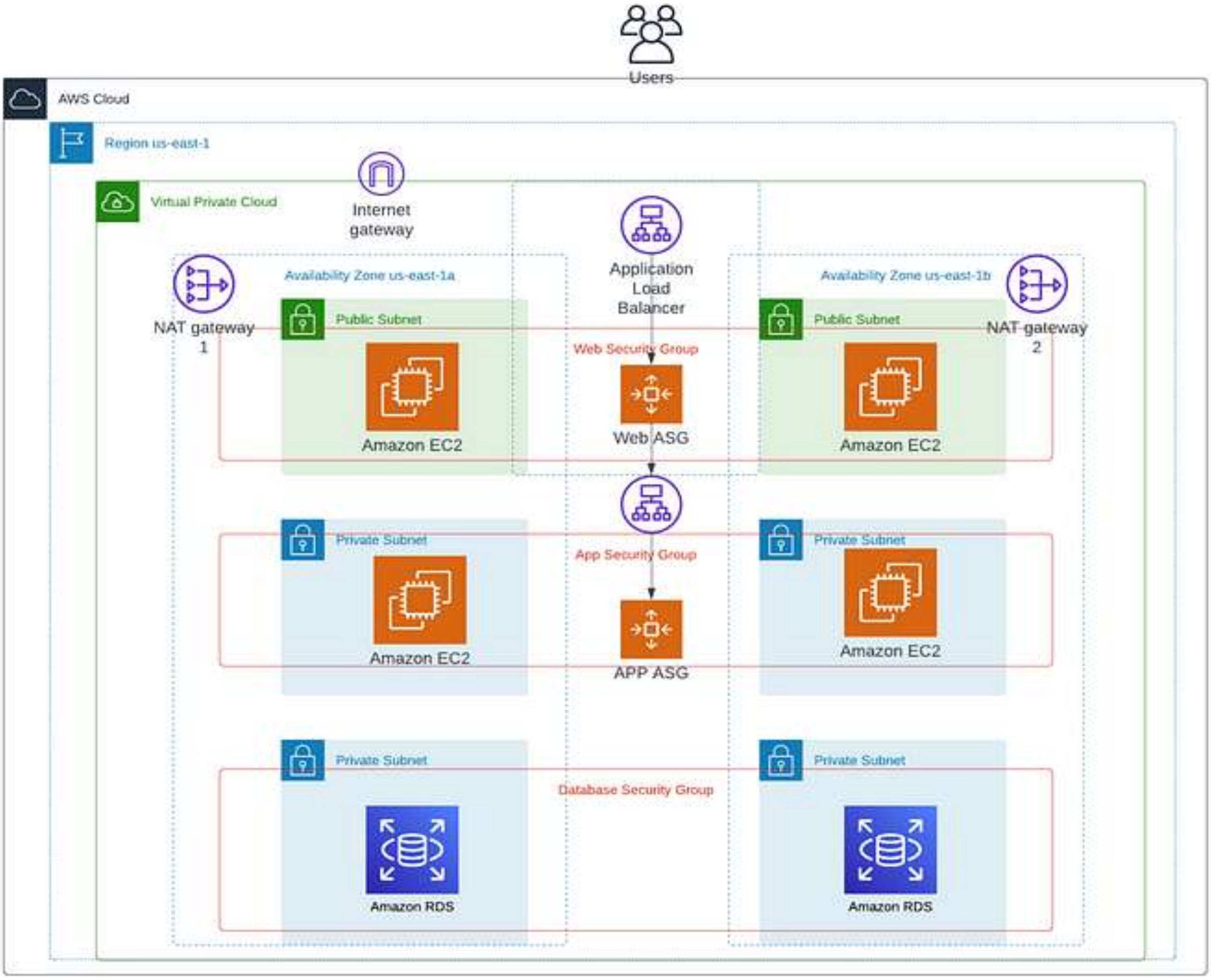
Example Scenario:

For a simple e-commerce application:

- Presentation Tier: The website or mobile app where users browse products and make purchases.

- Application Tier: The server that processes orders, manages user sessions, and handles business logic such as calculating totals and applying discounts.

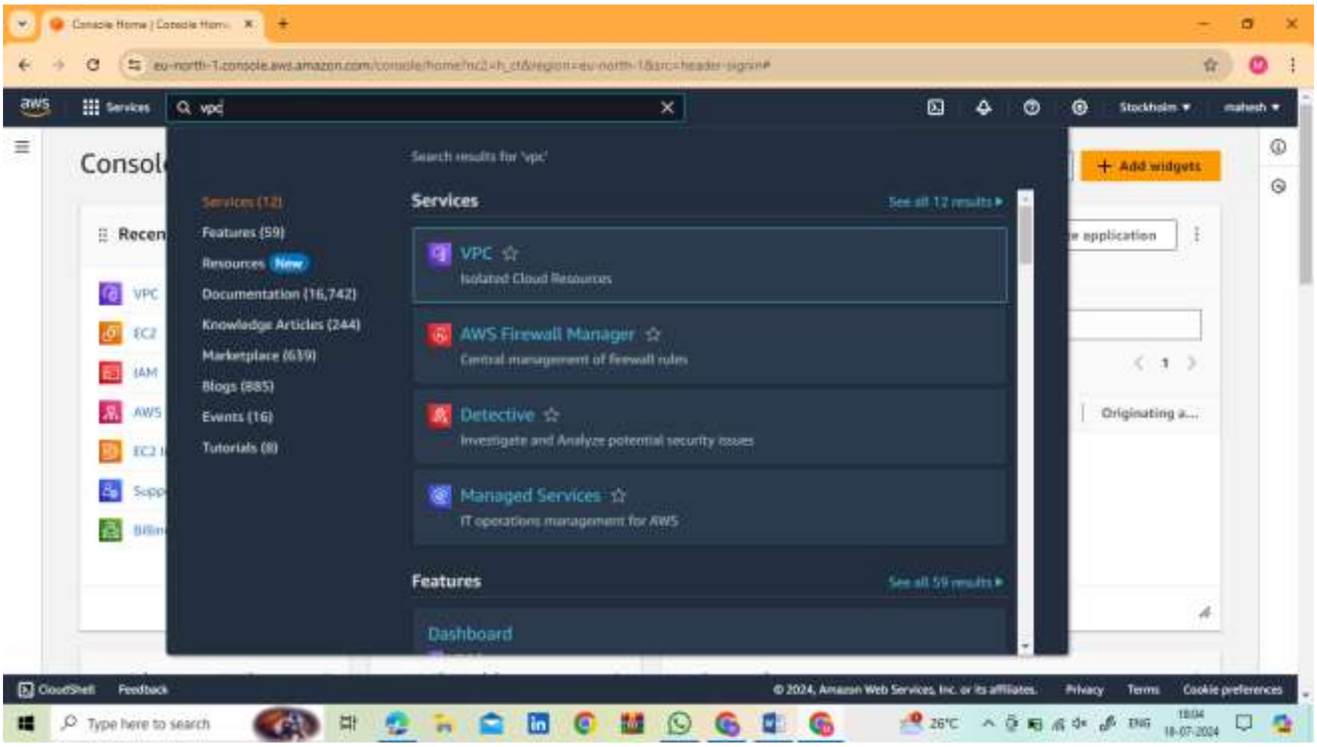
- Data Tier: The database that stores product information, user details, order history, and inventory levels.

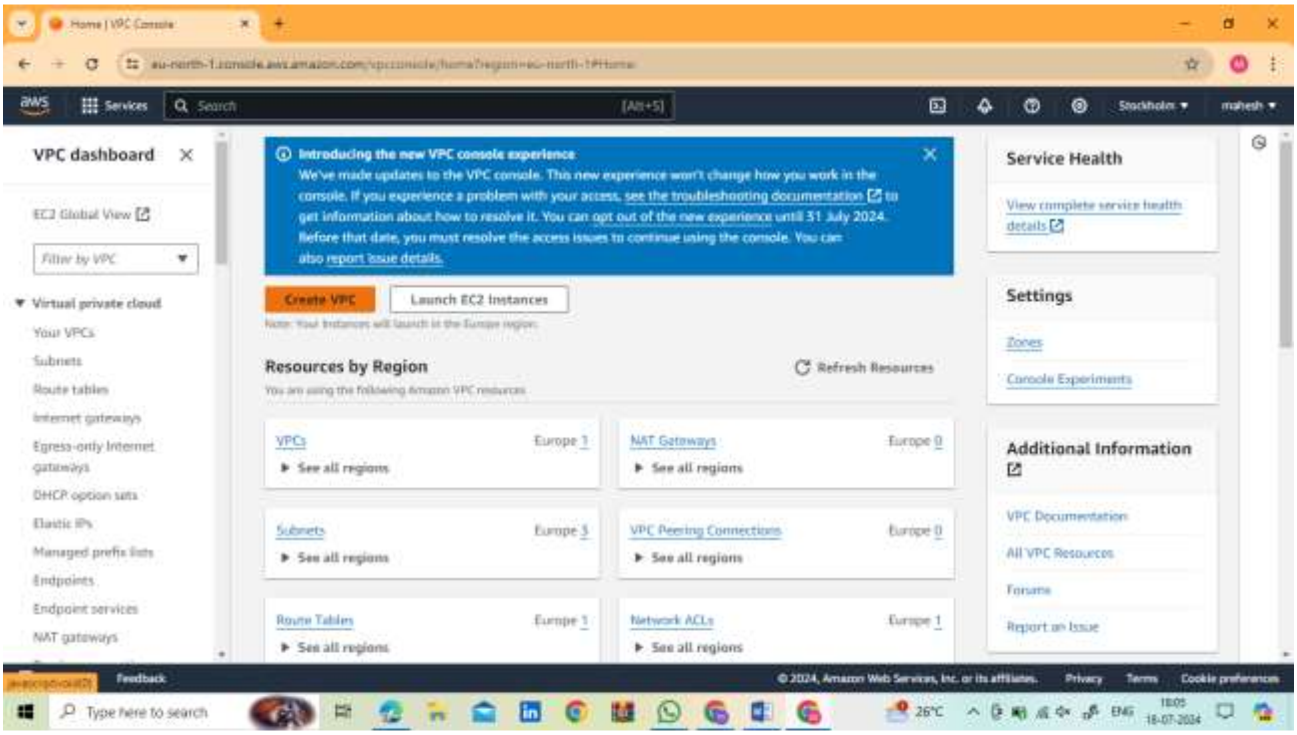


Step1----------------------creating Vpc

Based on the architecture diagram as a reference, our initial step involves creating a new VPC containing 2 public subnets and 4 private subnets.

To begin, please log into the AWS Management Console and click on the "Create VPC" button.





Introducing the new VPC console experience

We've made updates to the VPC console. This new experience won't change how you work in the console. If you experience a problem with your access, see the troubleshooting documentation to get information about how to resolve it. You can opt out of the new experience until 31 July 2024. Before that date, you must resolve the access issues to continue using the console. You can also report issue details.

Note: Your instances will launch in the Europe region.

You are using the following Amazon VPC resources

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

Let's proceed with creating a VPC that includes multiple public and private subnets across 2 Availability Zones. Ensure the following settings:

- Choose "VPC and more" option.

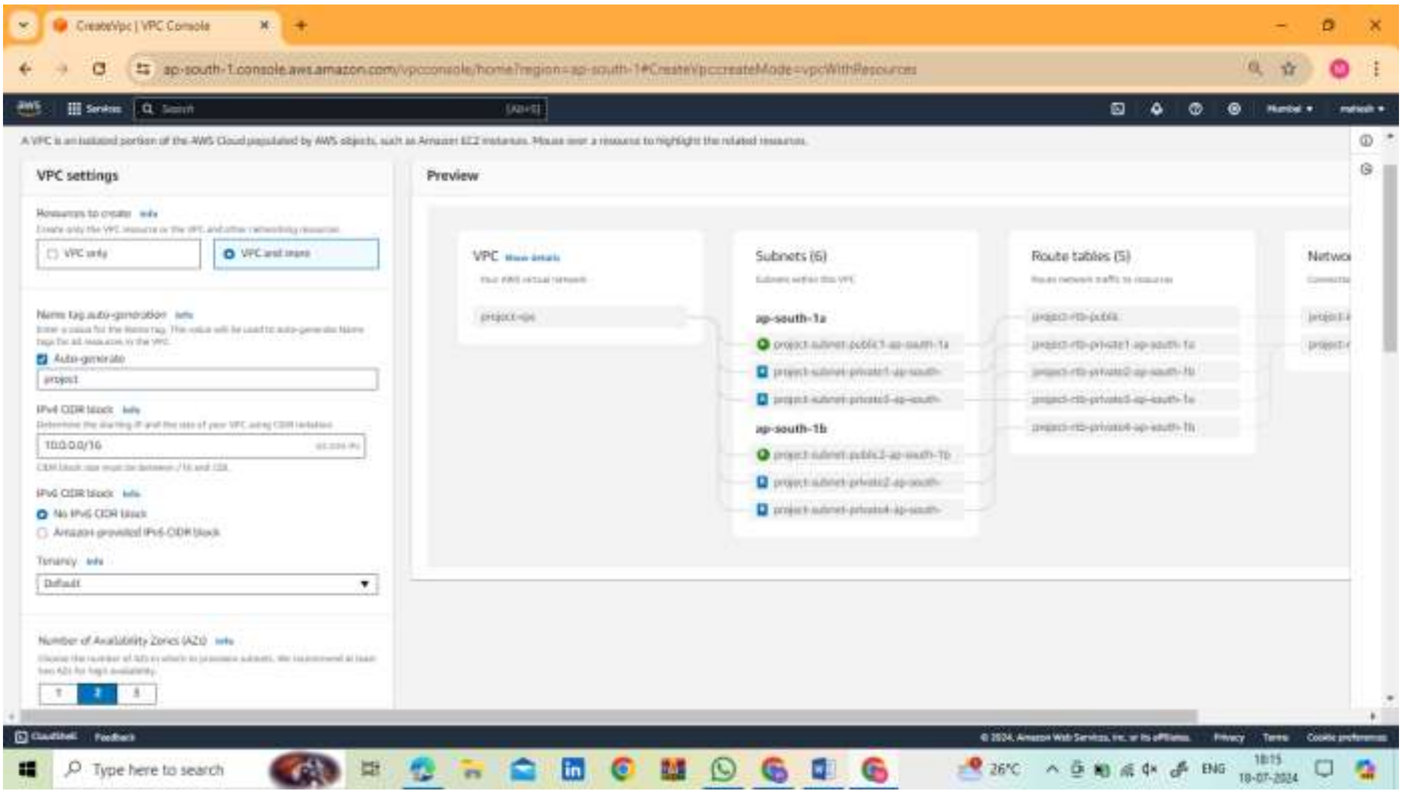
- Name your VPC.

- Use the auto-assigned IPv4 CIDR block of "10.0.0.0/16".

- Select no IPv6 support.

- Choose default Tenancy.

- Specify 2 public subnets and 4 private subnets.



CreateVpc | VPC Console
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateVpc:createMode=vpcWithResources
Services
Search

VPC settings

Resources to create Info

□ VPC only ● VPC and more

Name tag auto-generation Info

☑ Auto-generate

project

IPv4 CIDR block Info

10.0.0.0/16

IPv6 CIDR block Info

● No IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

Tenancy Info

Default

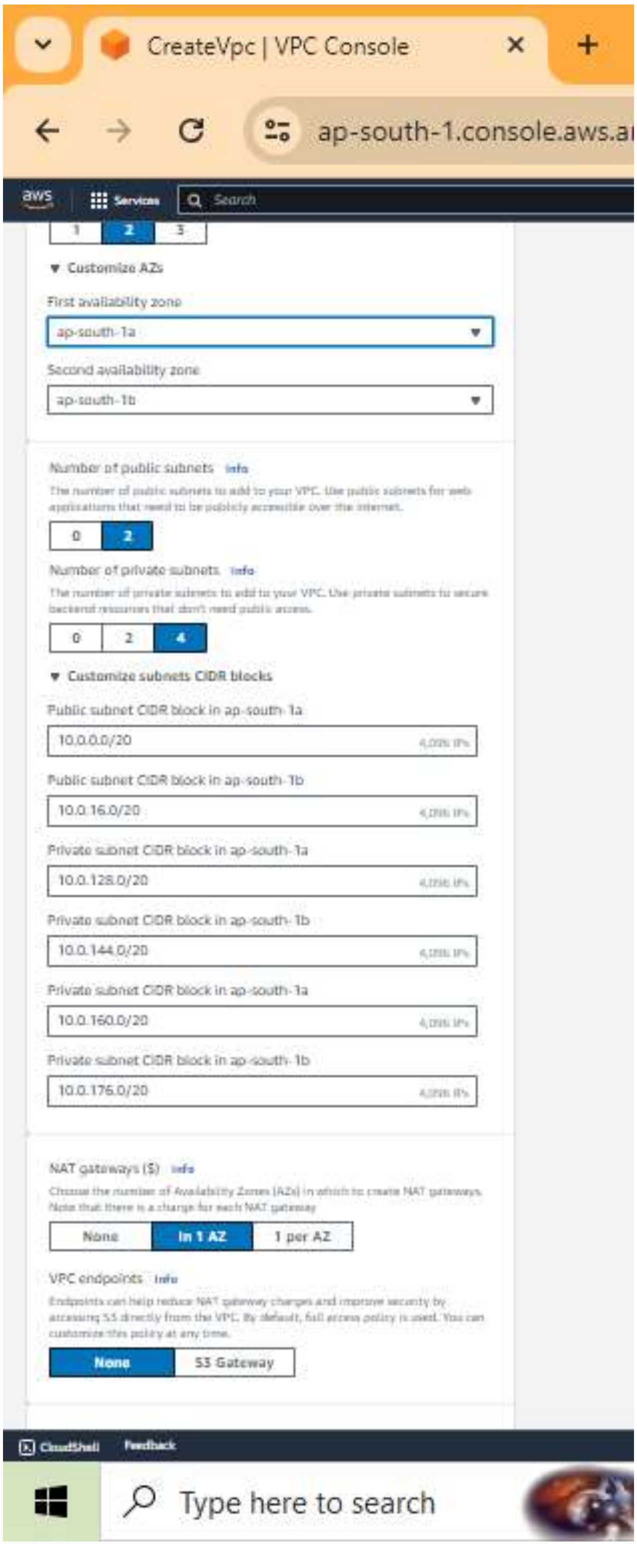
Number of Availability Zones (AZs) Info

1 **2** 3

Preview
VPC
project-vpc
Subnets (6)
ap-south-1a
project-subnet-public1-ap-south-1a
project-subnet-private1-ap-south-
project-subnet-private3-ap-south-
ap-south-1b
project-subnet-public2-ap-south-1b
project-subnet-private2-ap-south-
project-subnet-private4-ap-south-
Route tables (5)
project-rtb-public
project-rtb-private1-ap-south-1a
project-rtb-private2-ap-south-1b
project-rtb-private3-ap-south-1a
project-rtb-private4-ap-south-1b
Netwo
CloudShell
Feedback
Type here to search
26°C
ENG
18:15
18-07-2024

Before creating the VPC, let's expand and customize the Availability Zones (AZs) and the CIDR blocks for subnets.

For the NAT gateway, select "in 1 AZ". Do not configure VPC endpoints. Ensure that the options "Enable DNS hostnames" and "Enable DNS resolution" remain checked.



▼ Customize AZs

First availability zone

ap-south-1a

Second availability zone

ap-south-1b

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 | **2**

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 | 2 | **4**

▼ Customize subnets CIDR blocks

Public subnet CIDR block in ap-south-1a

10.0.0.0/20 4,096 IPs

Public subnet CIDR block in ap-south-1b

10.0.16.0/20 4,096 IPs

Private subnet CIDR block in ap-south-1a

10.0.128.0/20 4,096 IPs

Private subnet CIDR block in ap-south-1b

10.0.144.0/20 4,096 IPs

Private subnet CIDR block in ap-south-1a

10.0.160.0/20 4,096 IPs

Private subnet CIDR block in ap-south-1b

10.0.176.0/20 4,096 IPs

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

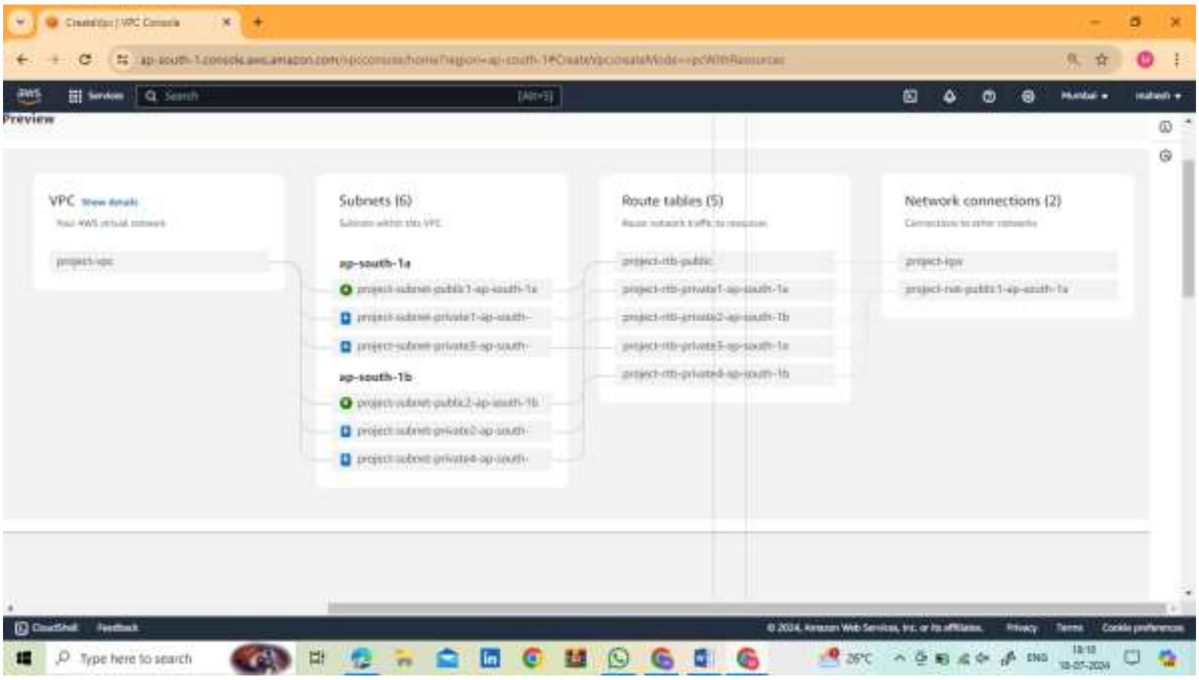
None | **In 1 AZ** | 1 per AZ

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

To proceed, click on the "Create VPC" button. The diagram below illustrates the route that your new VPC will follow.



Preview

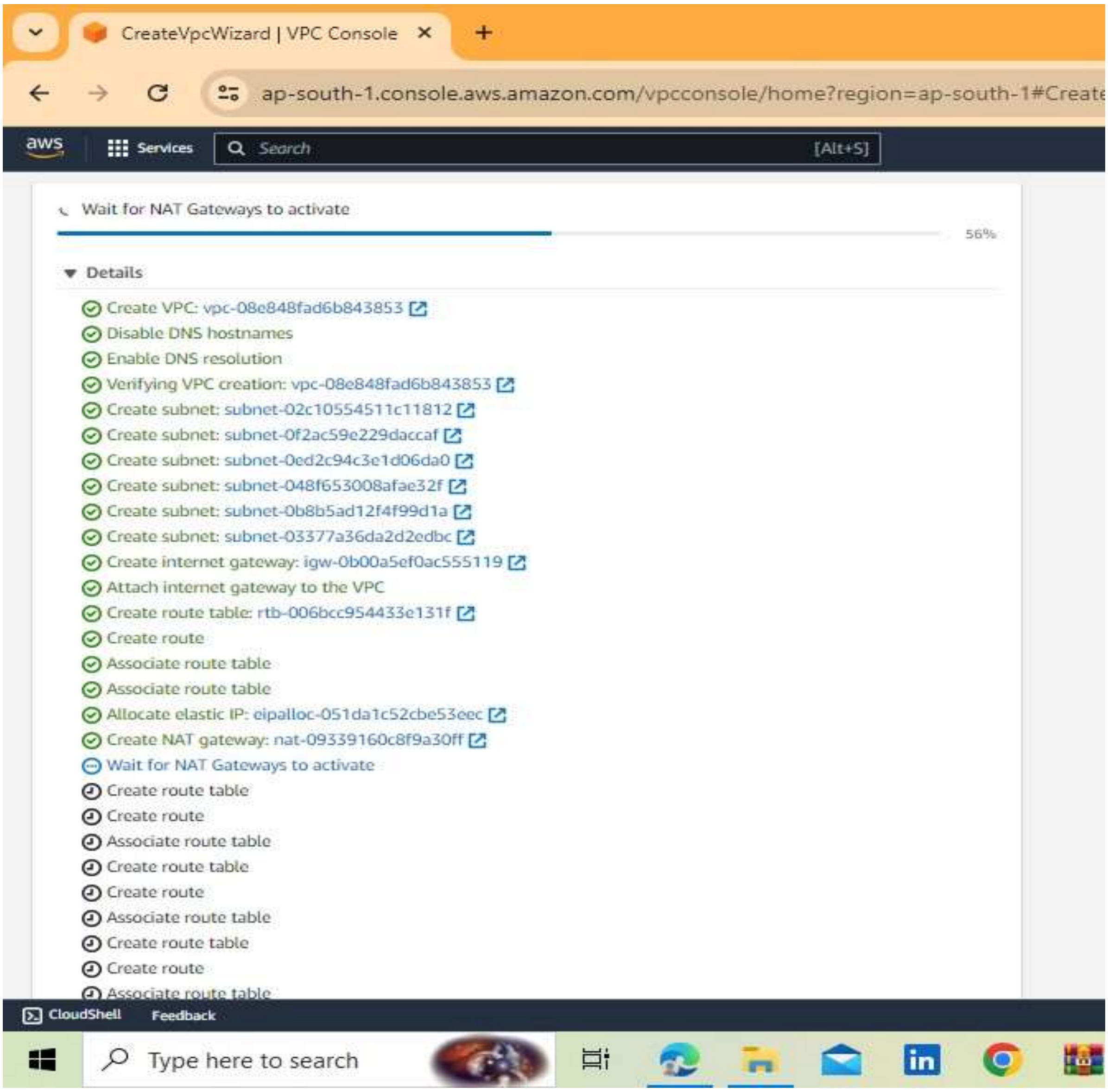
VPC Show details
Your AWS virtual network
project-vpc

Subnets (6)
Subnets within this VPC
ap-south-1a
project-subnet-public1-ap-south-1a
project-subnet-private1-ap-south-
project-subnet-private3-ap-south-
ap-south-1b
project-subnet-public2-ap-south-1b
project-subnet-private2-ap-south-
project-subnet-private4-ap-south-

Route tables (5)
Route network traffic to resources
project-rtb-public
project-rtb-private1-ap-south-1a
project-rtb-private2-ap-south-1b
project-rtb-private3-ap-south-1a
project-rtb-private4-ap-south-1b

Network connections (2)
Connections to other networks
project-igw
project-nat-public1-ap-south-1a

Once you click "Create VPC," you will be presented with a workflow chart that visually represents the creation process of your resources.


CreateVpcWizard | VPC Console
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#Create
aws
Services
Search
[Alt+S]
CloudShell
Feedback
Type here to search

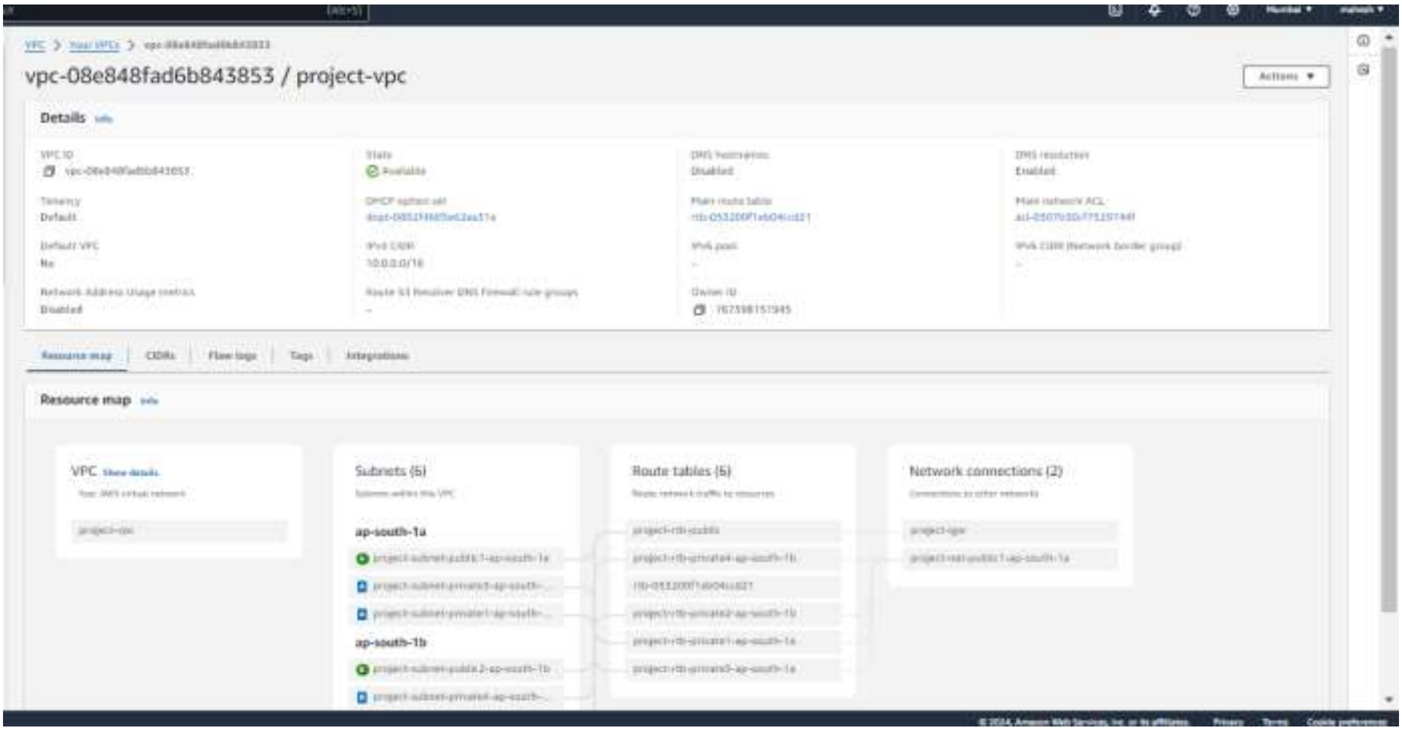
Wait for NAT Gateways to activate

56%

▼ Details

✓ Create VPC: vpc-08e848fad6b843853
✓ Disable DNS hostnames
✓ Enable DNS resolution
✓ Verifying VPC creation: vpc-08e848fad6b843853
✓ Create subnet: subnet-02c10554511c11812
✓ Create subnet: subnet-0f2ac59e229daccaf
✓ Create subnet: subnet-0ed2c94c3e1d06da0
✓ Create subnet: subnet-048f653008afae32f
✓ Create subnet: subnet-0b8b5ad12f4f99d1a
✓ Create subnet: subnet-03377a36da2d2edbc
✓ Create internet gateway: igw-0b00a5ef0ac555119
✓ Attach internet gateway to the VPC
✓ Create route table: rtb-006bcc954433e131f
✓ Create route
✓ Associate route table
✓ Associate route table
✓ Allocate elastic IP: eipalloc-051da1c52cbe53eec
✓ Create NAT gateway: nat-09339160c8f9a30ff
⋯ Wait for NAT Gateways to activate
◷ Create route table
◷ Create route
◷ Associate route table
◷ Create route table
◷ Create route
◷ Associate route table
◷ Create route table
◷ Create route
◷ Associate route table

After the creation process completes, you can view your new VPC in the AWS Management Console to ensure everything is set up correctly.

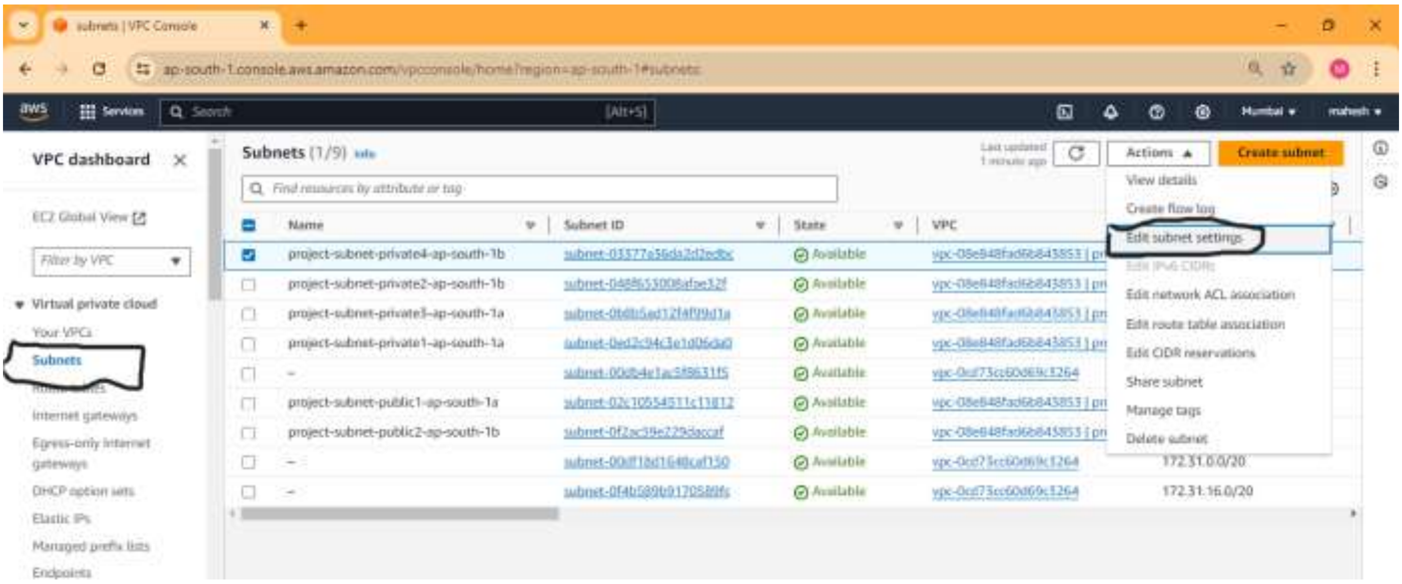


vpc-08e848fad6b843853 / project-vpc

Details

VPC ID vpc-08e848fad6b843853	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0852f46f5e62aa17a	Main route table rtb-053200f1eb04ccd21	Main network ACL acl-0507b5b7f7525744f
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 –	Owner ID 767398151945	

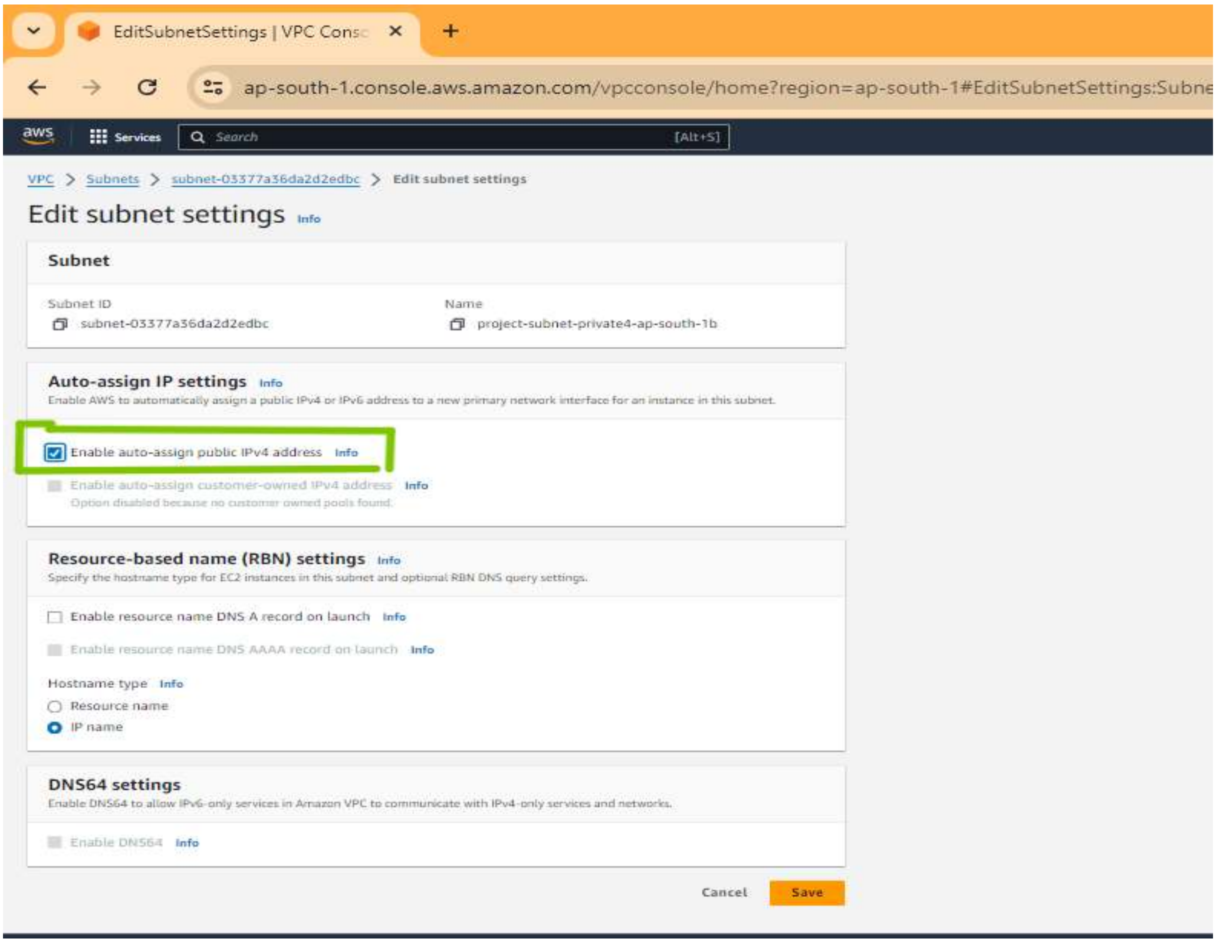
Next, navigate to the Subnets tab in the VPC console. Select one of the newly created subnets. Under the "Actions" tab, expand the dropdown menu and choose "Edit subnet settings."



ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#subnets

Subnets (1/9)

	Name	Subnet ID	State	VPC	
☑	project-subnet-private4-ap-south-1b	subnet-03377a56da2d2edbc	Available	vpc-08e848fad6b843853 | pr	
□	project-subnet-private2-ap-south-1b	subnet-0488653008dfae32f	Available	vpc-08e848fad6b843853 | pr	
□	project-subnet-private3-ap-south-1a	subnet-0b0b5ad12f4f99d1a	Available	vpc-08e848fad6b843853 | pr	
□	project-subnet-private1-ap-south-1a	subnet-0ed2c94c3e1d06da0	Available	vpc-08e848fad6b843853 | pr	
□	–	subnet-00db4e1ac5f86311f5	Available	vpc-0cd73cc60d69c3264	
□	project-subnet-public1-ap-south-1a	subnet-02c10554511c11812	Available	vpc-08e848fad6b843853 | pr	
□	project-subnet-public2-ap-south-1b	subnet-0f2ac39e229daccaf	Available	vpc-08e848fad6b843853 | pr	
□	–	subnet-00df18d1648caf150	Available	vpc-0cd73cc60d69c3264	172.31.0.0/20
□	–	subnet-0f4b589b91705888fc	Available	vpc-0cd73cc60d69c3264	172.31.16.0/20


EditSubnetSettings | VPC Consc
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#EditSubnetSettings:Subne
aws
Services
Search
[Alt+S]
VPC > Subnets > subnet-03377a36da2d2edbc > Edit subnet settings

Edit subnet settings Info

Subnet

Subnet ID
subnet-03377a36da2d2edbc

Name
project-subnet-private4-ap-south-1b

Auto-assign IP settings Info

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

☑ Enable auto-assign public IPv4 address Info

□ Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings Info

Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

□ Enable resource name DNS A record on launch Info

□ Enable resource name DNS AAAA record on launch Info

Hostname type Info
○ Resource name
● IP name

DNS64 settings

Enable DNS64 to allow IPv6-only services in Amazon VPC to communicate with IPv4-only services and networks.

□ Enable DNS64 Info

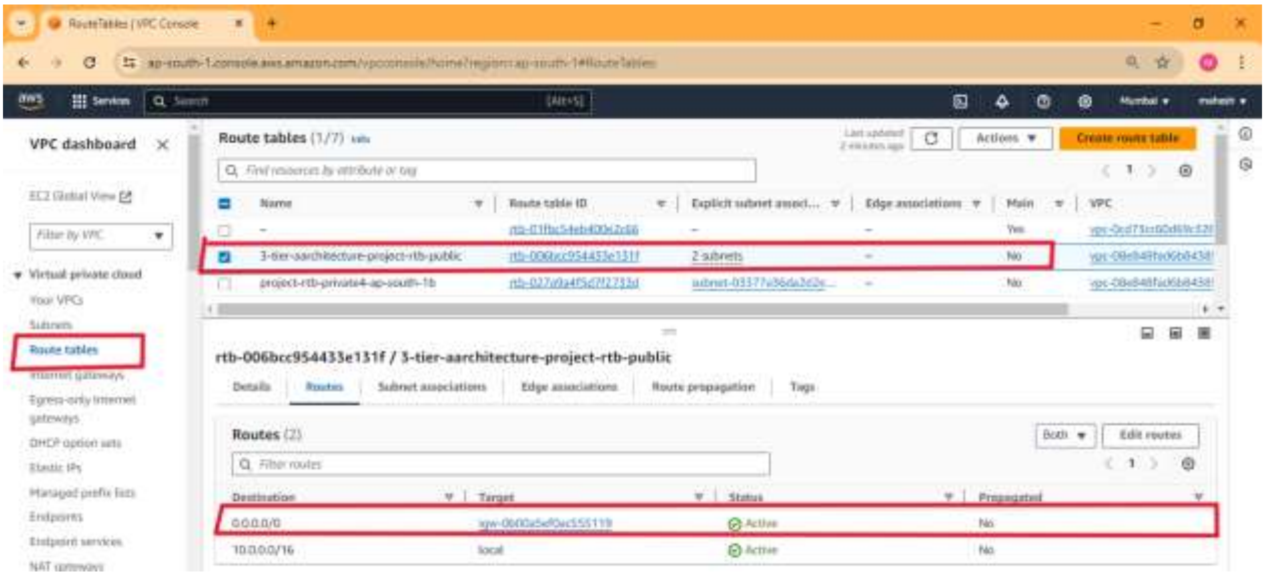
Check the box for "Enable auto-assign IPv4 address" and then click "Save." Repeat this step for all six of the newly created subnets.

Update Web Tier Public Route Table:

To ensure the correct subnets are associated with the appropriate route table:

1. Navigate to the Route Tables tab under the VPC dashboard.

2. Verify that the automatically created route table is correctly associated with the green-highlighted public subnets. If not, click "edit subnet associations" and select the required subnets.



Route tables (1/7)

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
-	rtb-01fbc54eb400e2c66	-	-	Yes	vpc-0cd71cc60d69c52
3-tier-aarchitecture-project-rtb-public	rtb-006bcc954433e131f	2 subnets	-	No	vpc-08e849fad6b8438
project-rtb-private4-ap-south-1b	rtb-027a9a4f5d7f2733d	subnet-03377a36da2d2e...	-	No	vpc-08e848fad6b8438

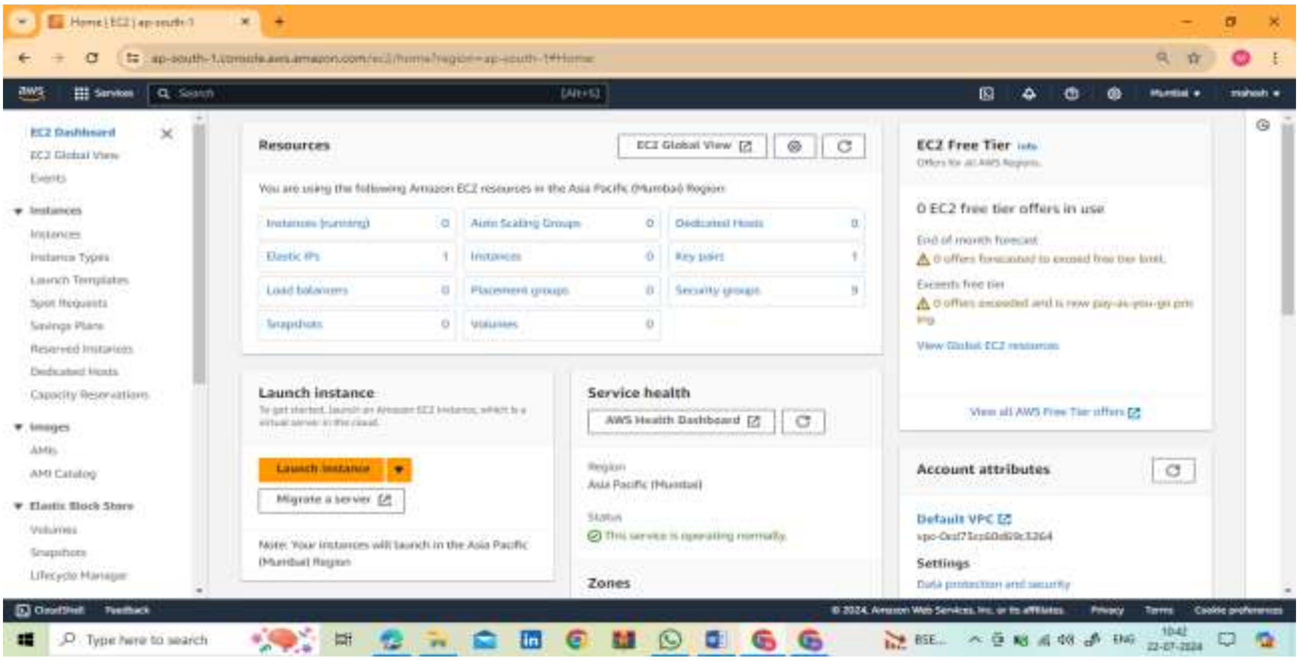
rtb-006bcc954433e131f / 3-tier-aarchitecture-project-rtb-public

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0b00a5ef0ac555119	Active	No
10.0.0.0/16	local	Active	No

Step-2: Creating a Web Server Layer

Next, we will create our first tier, representing our front-end user interface (web interface). We will create an auto-scaling group of EC2 instances that will host a custom webpage for us. Start by heading to launch an EC2 instance.



Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	1	Instances	0	Key pairs	1
Load balancers	0	Placement groups	0	Security groups	9
Snapshots	0	Volumes	0		

Launch instance

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

Note: Your instances will launch in the Asia Pacific (Mumbai) Region

Service health

Region
Asia Pacific (Mumbai)

Status
This service is operating normally.

Zones

EC2 Free Tier
Offers for all AWS Regions.

0 EC2 free tier offers in use

End of month forecast
⚠ 0 offers forecasted to exceed free tier limit.

Exceeds free tier
⚠ 0 offers exceeded and is now pay-as-you-go pricing

View Global EC2 resources

View all AWS Free Tier offers

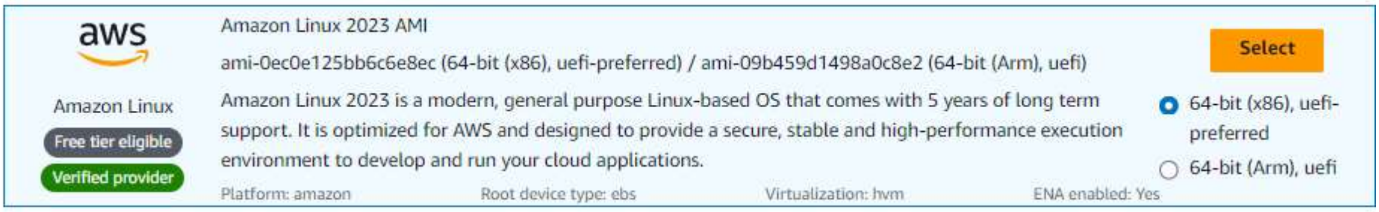
Account attributes

Default VPC
vpc-0cd71cc60d69c3264

Settings
Data protection and security

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

Give your instance a name and choose an AMI. I can use Amazon Linux 2023 AMI.



Amazon Linux 2023 AMI

ami-0ec0e125bb6c6e8ec (64-bit (x86), uefi-preferred) / ami-09b459d1498a0c8e2 (64-bit (Arm), uefi)

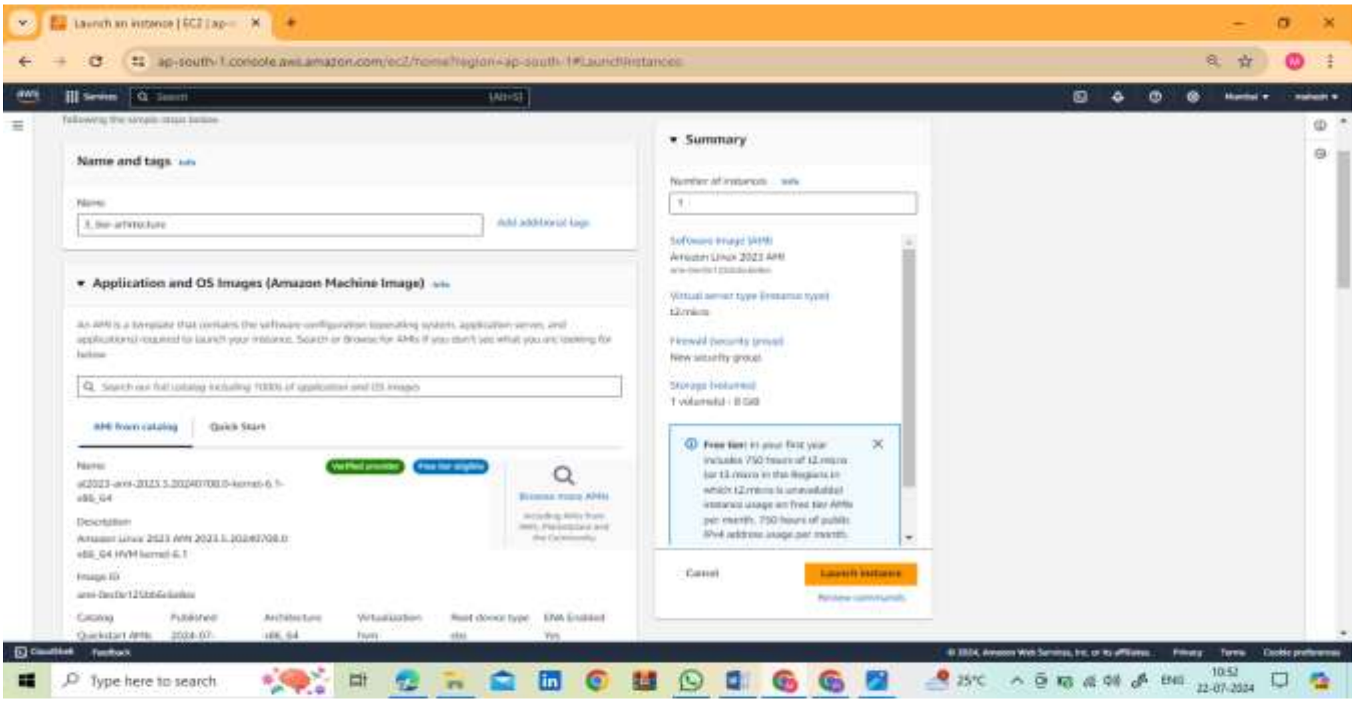
Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Platform: amazon Root device type: ebs Virtualization: hvm ENA enabled: Yes

● 64-bit (x86), uefi-preferred

○ 64-bit (Arm), uefi

Give some name for your instance, I will as 3_tier architecture



Name and tags

Name: 3_tier-architecture

Application and OS Images (Amazon Machine Image)

Name: al2023-ami-2023.5.20240708.0-kernel-6.1-x86_64

Description: Amazon Linux 2023 AMI 2023.5.20240708.0 x86_64 HVM kernel-6.1

Catalog: Quickstart AMIs; Published: 2024-07-; Architecture: x86_64; Virtualization: hvm; Root device type: ebs; ENA Enabled: Yes

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI

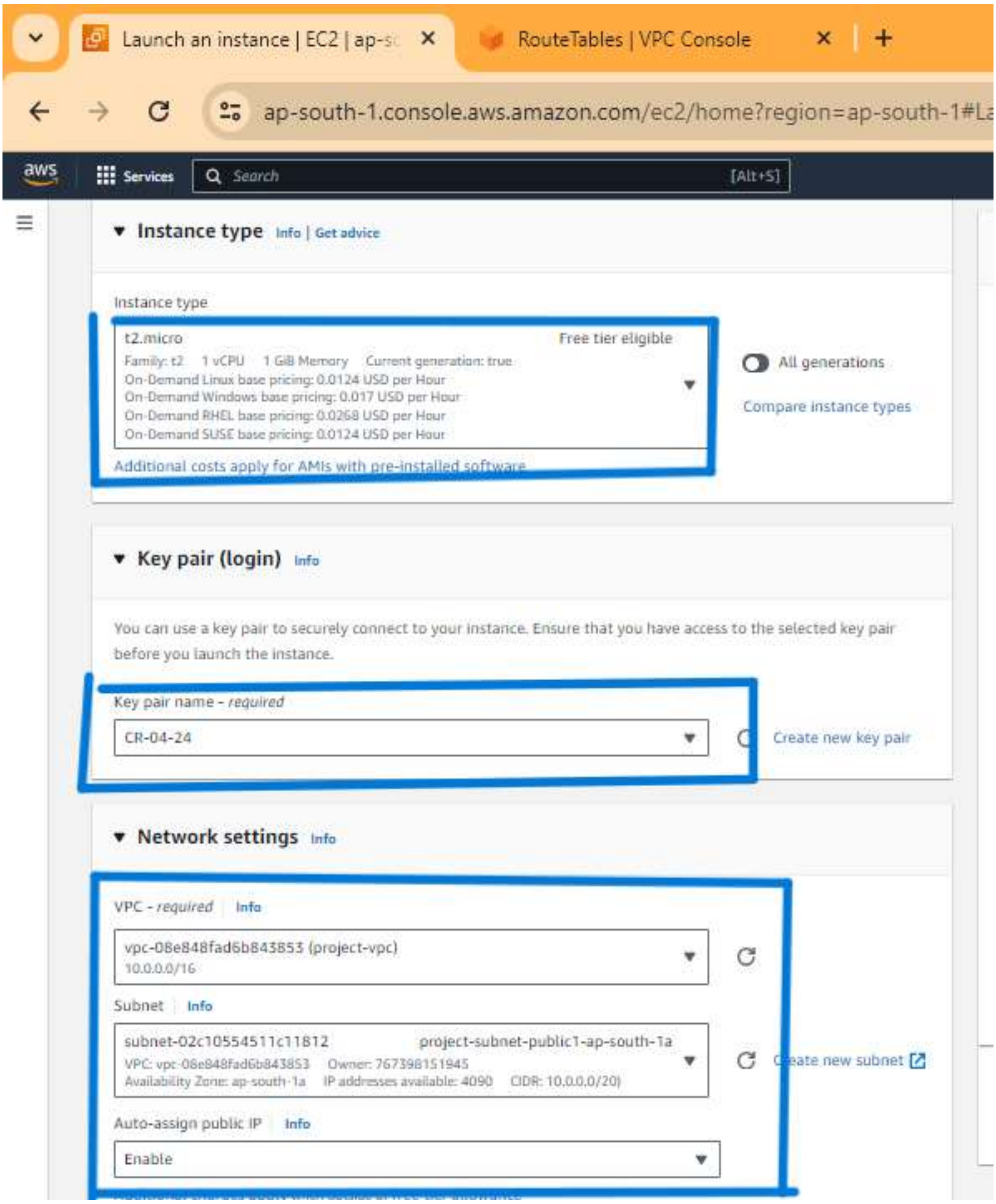
Virtual server type (instance type): t2.micro

Firewall (security group): New security group

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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month.

Choose the key pair you will use, and ensure that you select your new VPC and the appropriate subnet. Make sure Auto-assign IP is enabled.



Launch an instance | EC2 | ap-sc
RouteTables | VPC Console
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#La
aws
Services
Search
[Alt+S]

▼ Instance type Info | Get advice

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour

Additional costs apply for AMIs with pre-installed software

○ All generations

Compare instance types

▼ 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*

CR-04-24

Create new key pair

▼ Network settings Info

VPC - *required* Info

vpc-08e848fad6b843853 (project-vpc)
10.0.0.0/16

Subnet Info

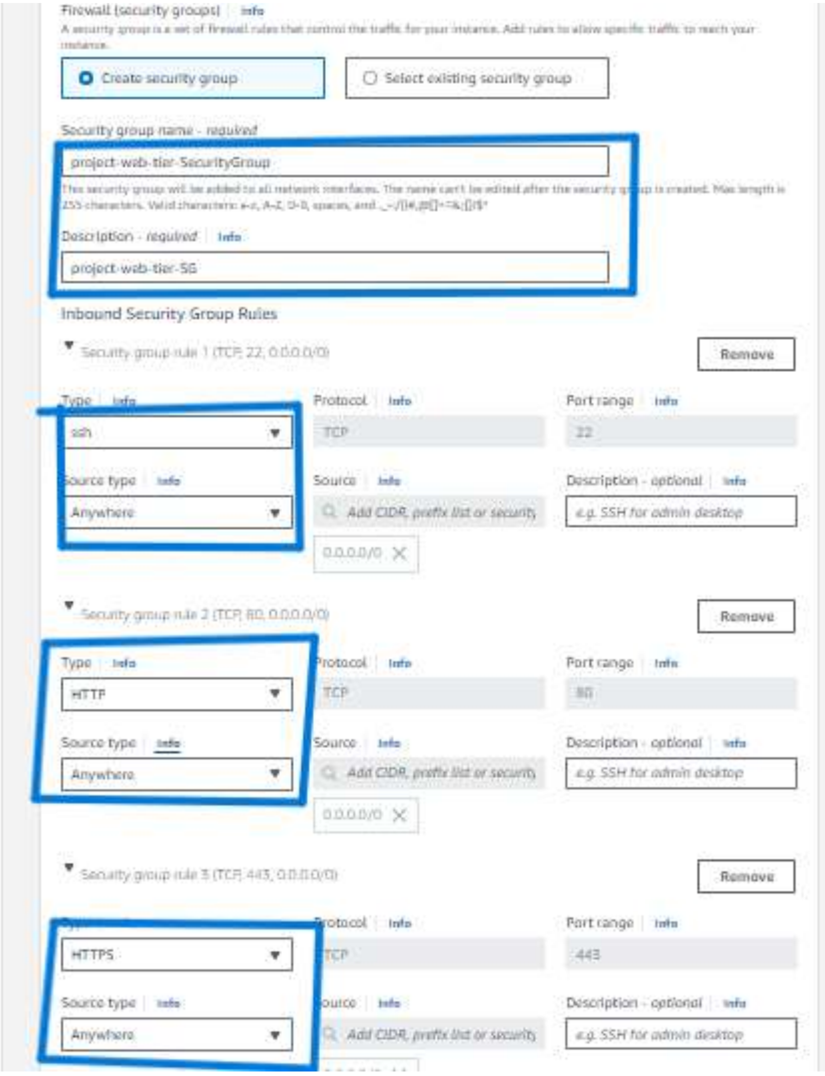
subnet-02c10554511c11812 project-subnet-public1-ap-south-1a
VPC: vpc-08e848fad6b843853 Owner: 767398151945
Availability Zone: ap-south-1a IP addresses available: 4090 CIDR: 10.0.0.0/20)

Create new subnet

Auto-assign public IP Info

Enable

Create a new security group. For inbound security group rules, add rules for SSH, HTTP, and HTTPS from any source. Although this configuration is not standard or secure, it is acceptable for the purposes of this demonstration.



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

Security group name - *required*

project-web-tier-SecurityGroup

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* | Info

project-web-tier-SG

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) Remove

Type	Protocol	Port range
ssh	TCP	22
Source type	**Source**	**Description - optional**
Anywhere	Add CIDR, prefix list or security 0.0.0.0/0	e.g. SSH for admin desktop

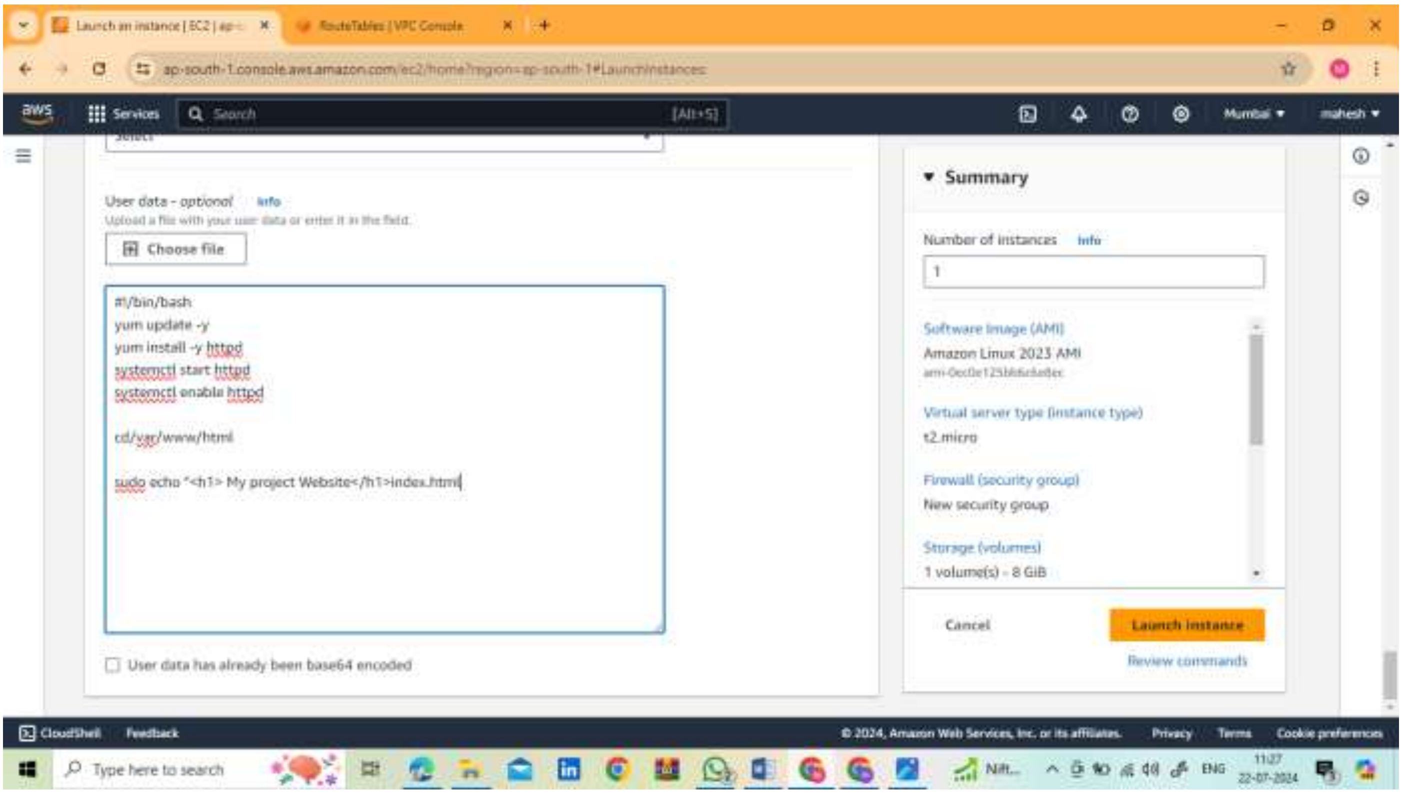
▼ Security group rule 2 (TCP, 80, 0.0.0.0/0) Remove

Type	Protocol	Port range
HTTP	TCP	80
Source type	**Source**	**Description - optional**
Anywhere	Add CIDR, prefix list or security 0.0.0.0/0	e.g. SSH for admin desktop

▼ Security group rule 3 (TCP, 443, 0.0.0.0/0) Remove

Type	Protocol	Port range
HTTPS	TCP	443
Source type	**Source**	**Description - optional**
Anywhere	Add CIDR, prefix list or security	e.g. SSH for admin desktop

Leave the configuration storage settings unchanged. In the Advanced details section, scroll all the way to the bottom. We will use a script to launch an Apache web server when the instance starts.



Launch an instance | EC2 | ap-
RouteTables | VPC Console
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Services
Search
[Alt+S]
Mumbai ▼
mahesh ▼

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

cd/var/www/html

sudo echo "<h1> My project Website</h1>index.html
```

□ User data has already been base64 encoded

▼ Summary

Number of instances Info: 1

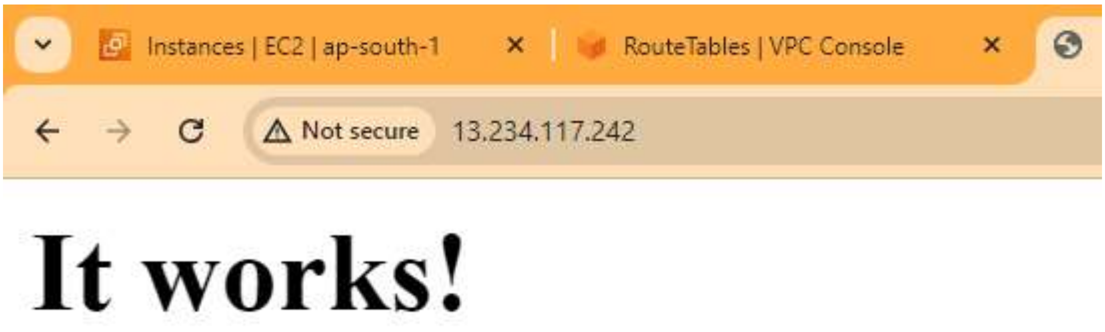
Software Image (AMI): Amazon Linux 2023 AMI, ami-0ec0e125bb6c4a6ec

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

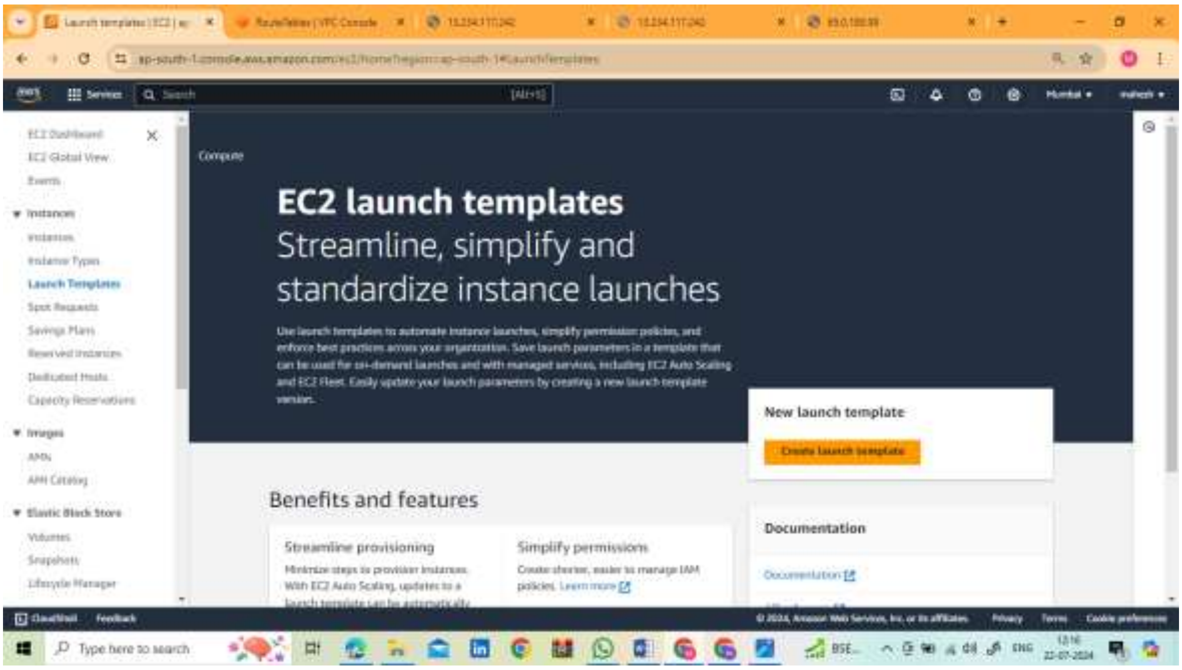
Storage (volumes): 1 volume(s) - 8 GiB

Launch your new instance! Once your instance is up and running, copy the public IP address and paste it into a web browser.



It works!

For this project to work, we need to create an auto-scaling group and attach it to our EC2 instance. This will enhance our reliability and availability. Next, we are going to create a launch template. Before proceeding, we need to define the launch template, which will specify the resources to be allocated when the auto-scaling group launches on-demand instances. Under the EC2 dashboard, select "Launch Templates" and click the “Create launch template” button.



EC2 launch templates

Streamline, simplify and standardize instance launches

Use launch templates to automate instance launches, simplify permission policies, and enforce best practices across your organization. Save launch parameters in a template that can be used for on-demand launches and with managed services, including EC2 Auto Scaling and EC2 Fleet. Easily update your launch parameters by creating a new launch template version.

Benefits and features

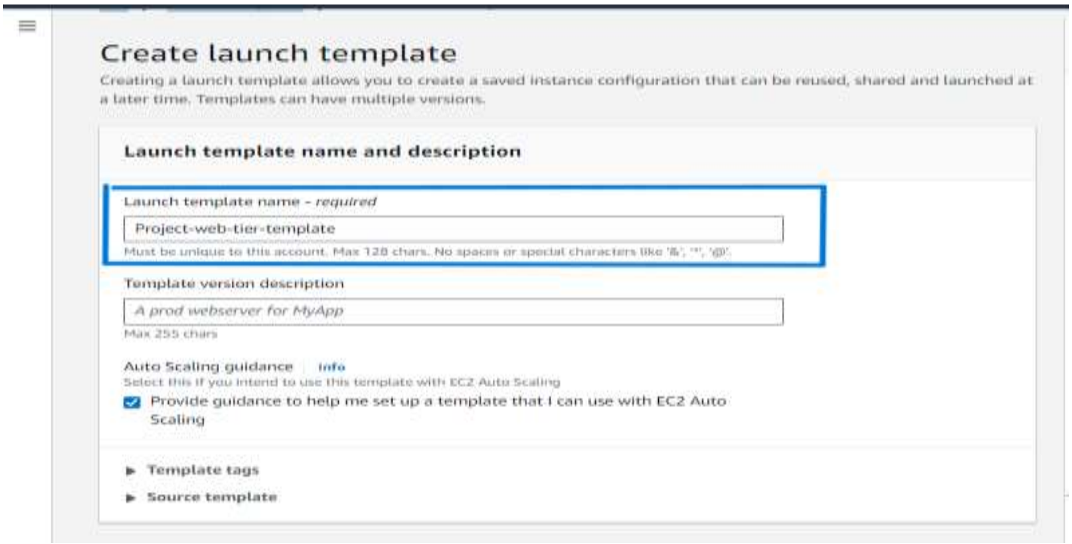
Streamline provisioning

Minimize steps to provision instances. With EC2 Auto Scaling, updates to a launch template can be automatically

Simplify permissions

Create shorter, easier to manage IAM policies. Learn more

Give your template a name and select the option to "provide guidance."



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*

Project-web-tier-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

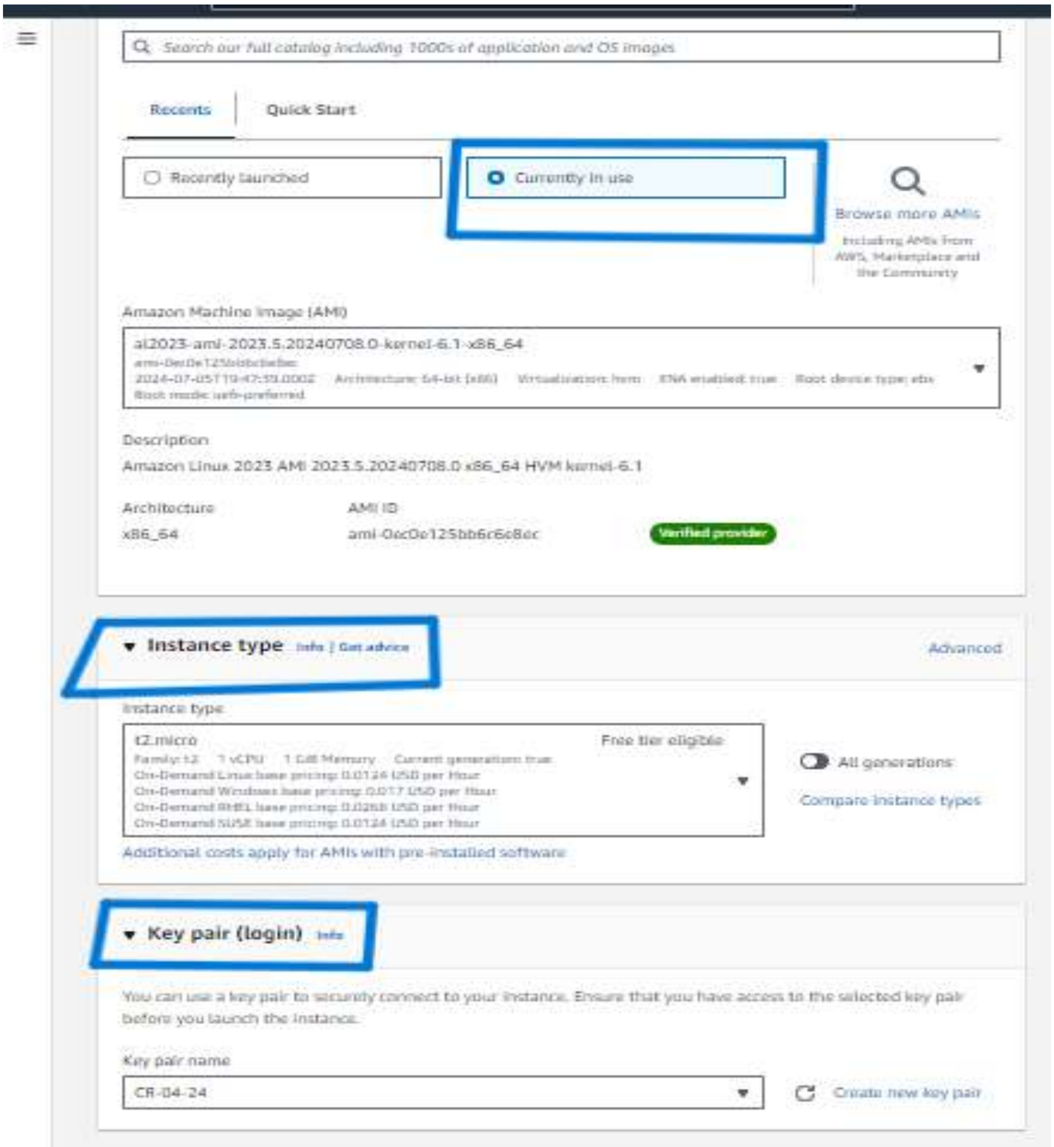
Select this if you intend to use this template with EC2 Auto Scaling

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

▸ Template tags

▸ Source template

Use our recently launched AMI, select the t2.micro instance type, and choose your key pair.



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

○ Recently launched

● Currently in use

Amazon Machine Image (AMI)

al2023-ami-2023.5.20240708.0-kernel-6.1-x86_64
ami-0ec0e125bb6c6c8ec
2024-07-05T19:47:33.000Z Architecture: 64-bit (x86) Virtualization: hvm ENA enabled: true Root device type: ebs
Boot mode: uefi-preferred

Description

Amazon Linux 2023 AMI 2023.5.20240708.0 x86_64 HVM kernel-6.1

Architecture	AMI ID	
x86_64	ami-0ec0e125bb6c6c8ec	Verified provider

▾ Instance type Info | Get advice

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour

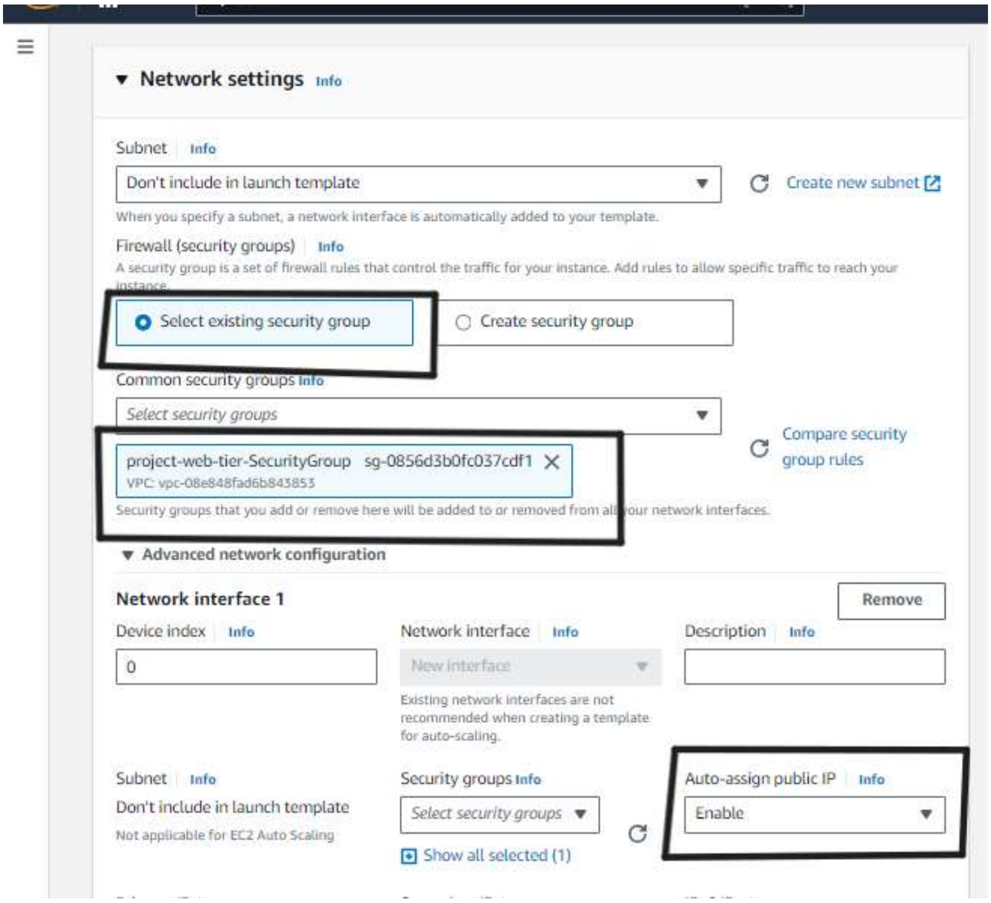
▾ Key pair (login) Info

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

CR-04-24

For the firewall settings, select "Choose an existing security group" and ensure the security group (SG) we created for the web tier is selected. In the Advanced network configuration section, enable Auto-assign public IP.



▾ 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 ▾

project-web-tier-SecurityGroup sg-0856d3b0fc037cdf1 ✕
VPC: vpc-08e848fad6b843853

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 ▾
Existing network interfaces are not recommended when creating a template for auto-scaling.

Description Info:

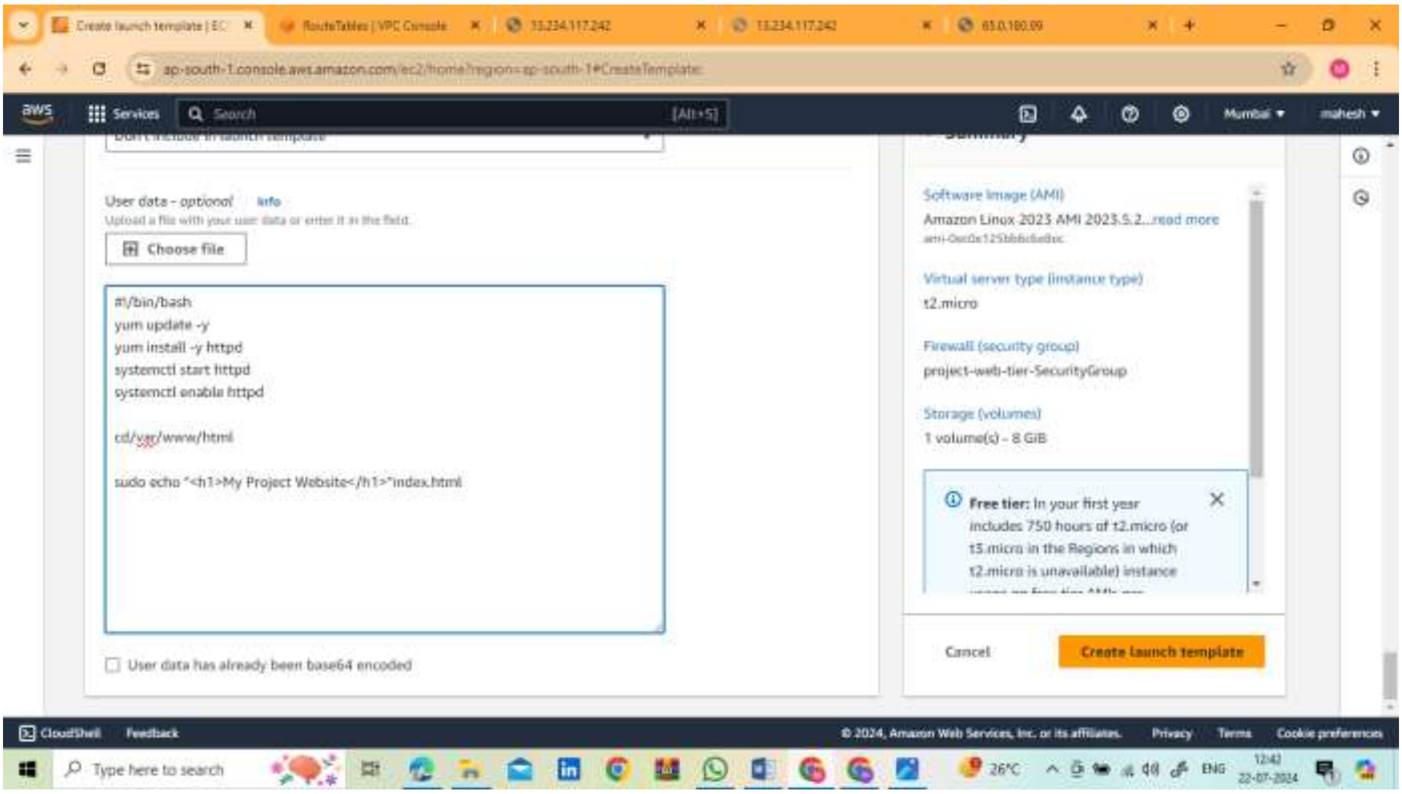
Subnet Info: Don't include in launch template
Not applicable for EC2 Auto Scaling

Security groups Info: Select security groups ▾
Show all selected (1)

Auto-assign public IP Info: Enable ▾

We will leave the storage options unchanged for now. Click on the Advanced details tab, scroll down, and enter the same script we used earlier for our EC2 instance.

Click the "Create launch template" button.



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#CreateTemplate:

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 enabla httpd

cd/var/www/html

sudo echo "<h1>My Project Website</h1>"index.html
```

□ User data has already been base64 encoded

Summary

Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-0ec0e125bbb6c6e8ec

Virtual server type (instance type)
t2.micro

Firewall (security group)
project-web-tier-SecurityGroup

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

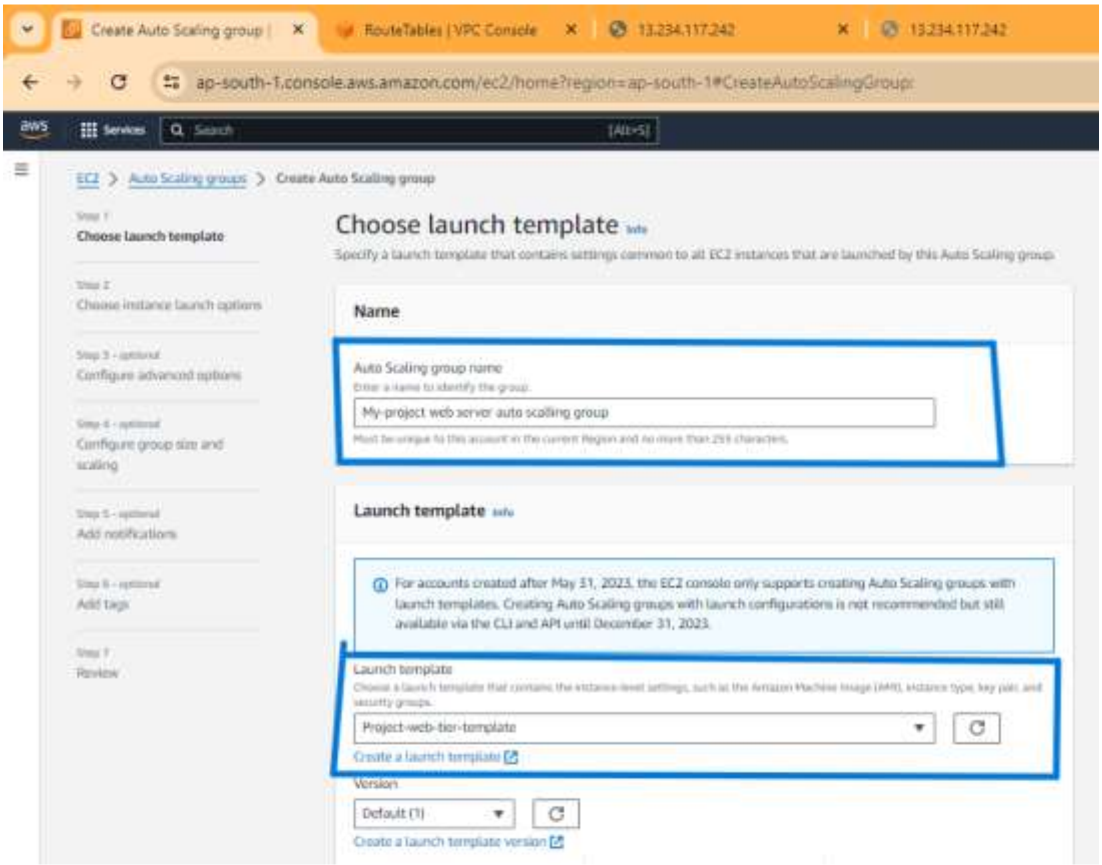
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance

Cancel — Create launch template

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Navigate to the Auto Scaling tab at the bottom of the EC2 dashboard. Click “Create auto scaling group.” The launch template we just created will be used by the auto-scaling group to launch new EC2 instances when scaling up.

Name your auto-scaling group (ASG), choose the launch template you created, and then click the Next button.


Create Auto Scaling group |
RouteTables | VPC Console
13.234.117.242
13.234.117.242
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#CreateAutoScalingGroup:
aws
Services
Search
[Alt+S]
EC2
Auto Scaling groups
Create Auto Scaling group
Step 1
Choose launch template
Step 2
Choose instance launch options
Step 3 - optional
Configure advanced options
Step 4 - optional
Configure group size and scaling
Step 5 - optional
Add notifications
Step 6 - optional
Add tags
Step 7
Review
Info
Info
Create a launch template
Create a launch template version

Choose launch template

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.

My-project web server auto scaling group

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

Launch template

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.

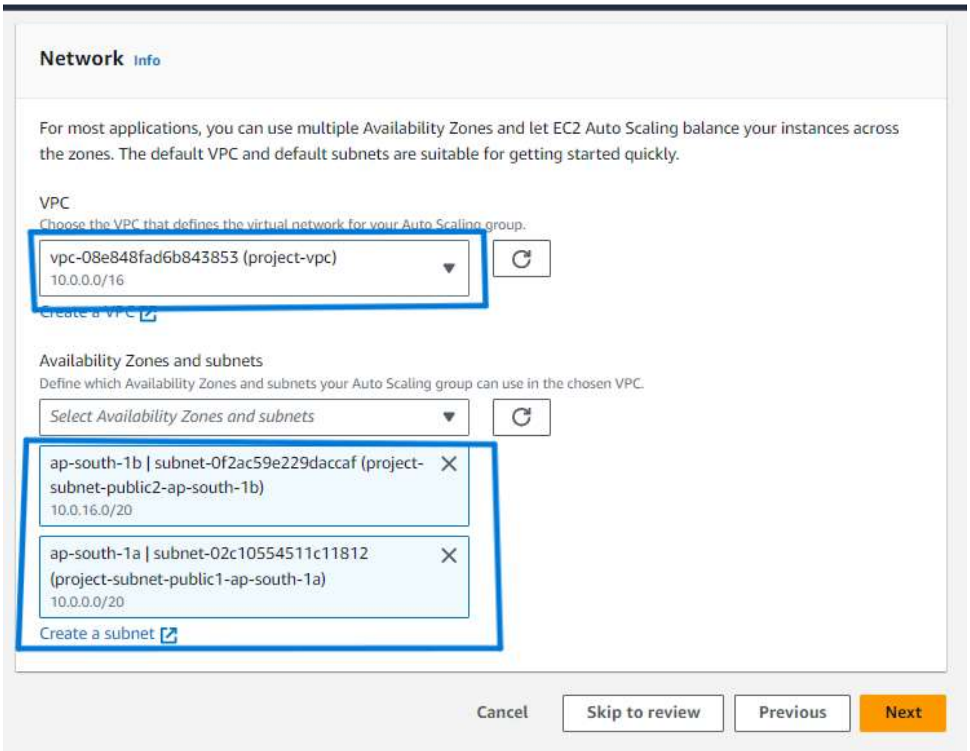
Project-web-tier-template

Version

Default (1)

Under Network, ensure you select the VPC you created earlier. Additionally, under Availability Zones and Subnets, select the public subnets that were created; your selections may vary.

Click the Next button.



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-08e848fad6b843853 (project-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

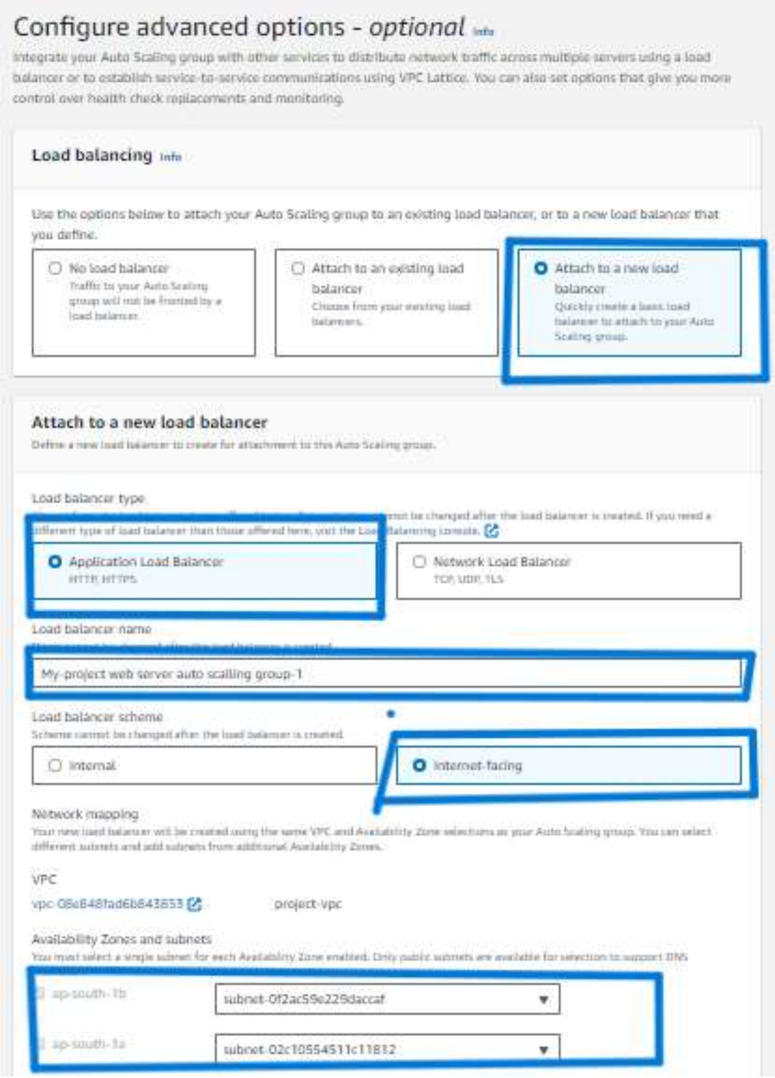
ap-south-1b | subnet-0f2ac59e229daccaf (project-subnet-public2-ap-south-1b)
10.0.16.0/20

ap-south-1a | subnet-02c10554511c11812 (project-subnet-public1-ap-south-1a)
10.0.0.0/20

Create a subnet

Now we have the option to allocate a load balancer for our ASG. A load balancer will distribute incoming traffic across multiple servers, which helps improve availability and performance.

Select "Attach to a new load balancer" and choose "Application Load Balancer." Assign a name to your load balancer, and specify it as "Internet facing" since it is intended for our web tier.



Configure advanced options - *optional* Info

Integrate your Auto Scaling group with other services to distribute network traffic across multiple servers using a load balancer or to establish service-to-service communications using VPC Lattice. You can also set options that give you more control over health check replacements and monitoring.

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 a new load balancer

Define a new load balancer to create for attachment to this Auto Scaling group.

Load balancer type

cannot be changed after the load balancer is created. If you need a different type of load balancer than those offered here, visit the Load Balancing console.

● Application Load Balancer
HTTP, HTTPS

○ Network Load Balancer
TCP, UDP, TLS

Load balancer name

My-project web server auto scalling group-1

Load balancer scheme

Scheme cannot be changed after the load balancer is created.

○ Internal

● Internet-facing

Network mapping

Your new load balancer will be created using the same VPC and Availability Zone selections as your Auto Scaling group. You can select different subnets and add subnets from additional Availability Zones.

VPC

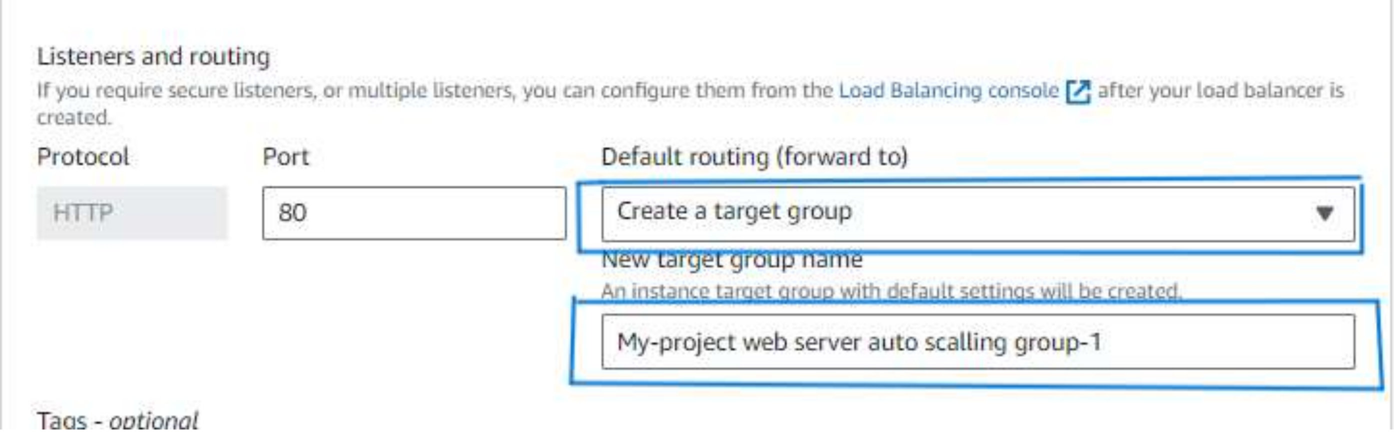
vpc-08e848fad6b843653 project-vpc

Availability Zones and subnets

You must select a single subnet for each Availability Zone enabled. Only public subnets are available for selection to support DNS

ap-south-1b	subnet-0f2ac59e229daccaf ▼
ap-south-1a	subnet-02c10554511c11812 ▼

Your VPC and the two public subnets should already be selected. In the "Listeners and routing" section, select "Create a target group," ensuring it is set to port 80 for HTTP traffic.



Listeners and routing

If you require secure listeners, or multiple listeners, you can configure them from the Load Balancing console after your load balancer is created.

Protocol	Port	Default routing (forward to)
HTTP	80	Create a target group ▼

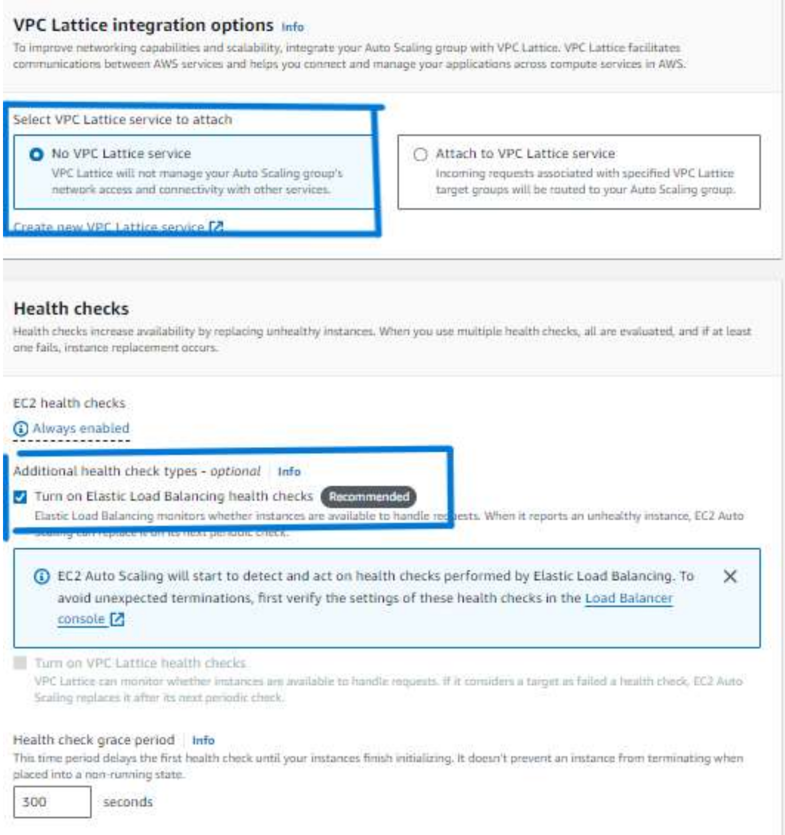
New target group name

An instance target group with default settings will be created.

My-project web server auto scalling group-1

Tags - *optional*

Ensure that the service for Leave No VPC Lattice is activated. Click to enable Elastic Load Balancing health checks.



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

● No VPC Lattice service
VPC Lattice will not manage your Auto Scaling group's network access and connectivity with other services.

○ Attach to VPC Lattice service
Incoming requests associated with specified VPC Lattice target groups will be routed to your Auto Scaling group.

Create new VPC Lattice service

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.

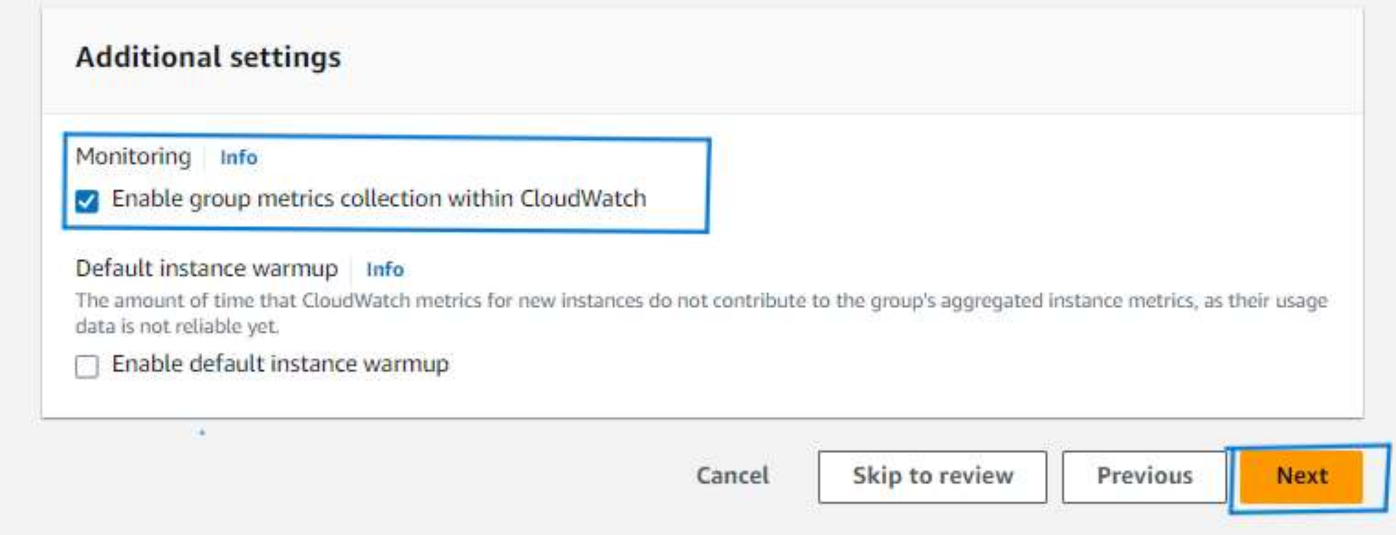
EC2 Auto Scaling will start to detect and act on health checks performed by Elastic Load Balancing. To avoid unexpected terminations, first verify the settings of these health checks in the Load Balancer console

□ Turn on VPC Lattice health checks
VPC Lattice can monitor whether instances are available to handle requests. If it considers a target as failed a health check, EC2 Auto Scaling replaces it after its next periodic check.

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.

300 seconds

Verify that "Enable Group Metrics Collection within Cloud Watch" is checked.

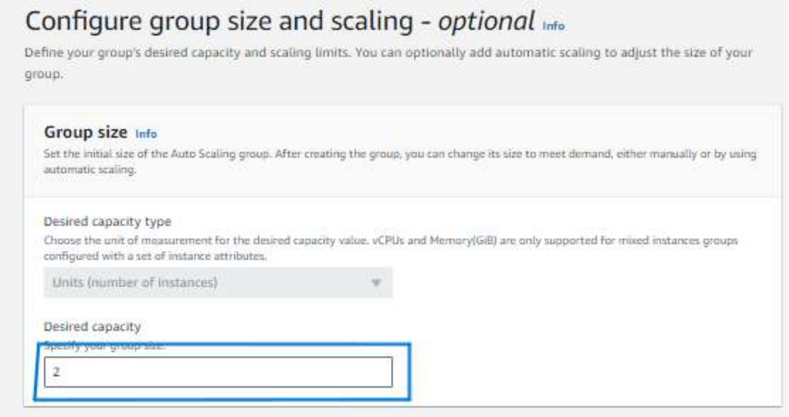


Additional settings

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

Next, we configure the group size and scaling policy for our Auto Scaling Group (ASG). To ensure reliability and performance, set the desired capacity and minimum capacity to 2, and the maximum capacity to 4.



Configure group size and scaling - *optional* Info

Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.

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

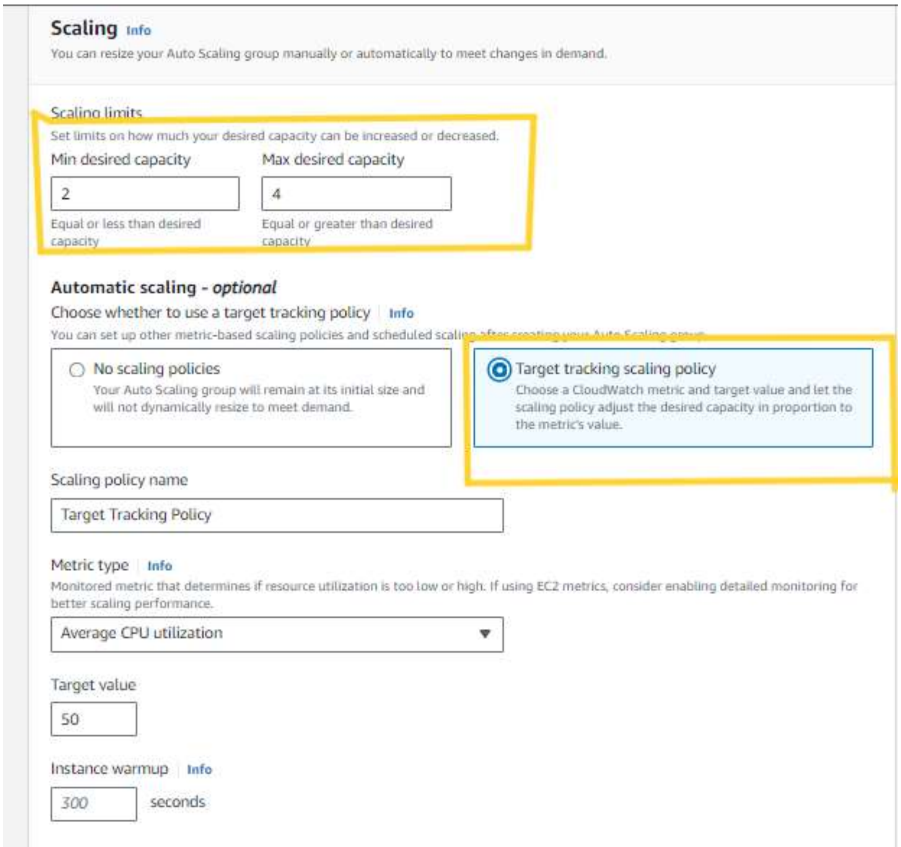
Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

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
2	4
Equal or less than desired capacity	Equal or greater than desired capacity

Automatic scaling - *optional*

Choose whether to use a target tracking policy Info

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

○ No scaling policies
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

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

Scaling policy name

Target Tracking Policy

Metric type Info

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

Average CPU utilization

Target value

50

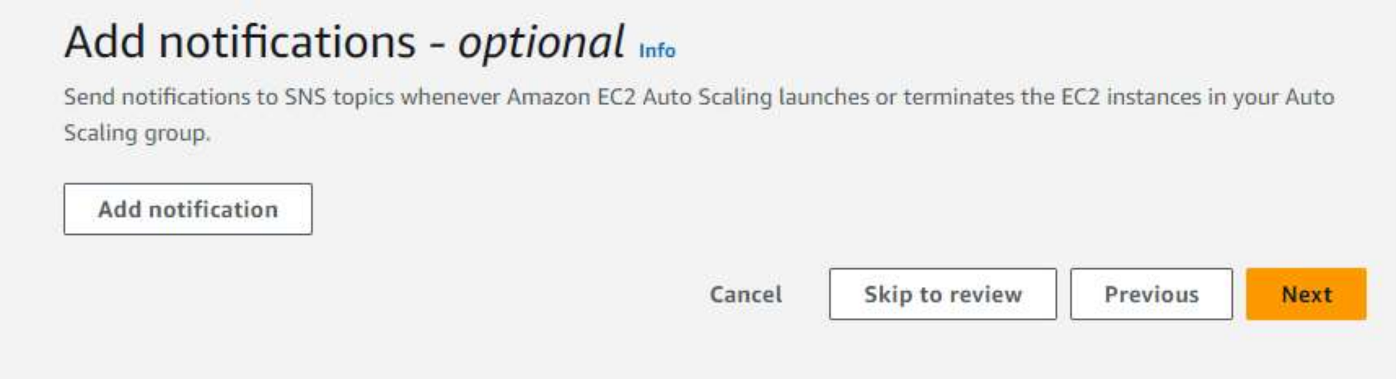
Instance warmup Info

300 seconds

In the scaling policies section, select "Target tracking scaling policy." Set the metric type to "Average CPU Utilization" with a target value of 50.

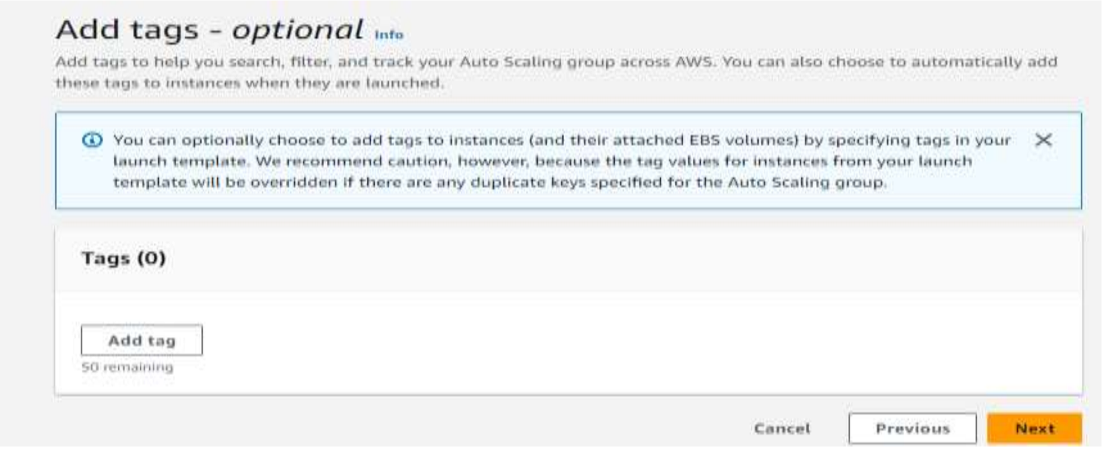
Then, click the "Next" button.

On the next screen, you have the option to add notifications through SNS topics. However, I have skipped this step for now. Click the "Next" button.



Add notifications - *optional* Info

Send notifications to SNS topics whenever Amazon EC2 Auto Scaling launches or terminates the EC2 instances in your Auto Scaling group.



Add tags - *optional* Info

Add tags to help you search, filter, and track your Auto Scaling group across AWS. You can also choose to automatically add these tags to instances when they are launched.

ⓘ You can optionally choose to add tags to instances (and their attached EBS volumes) by specifying tags in your launch template. We recommend caution, however, because the tag values for instances from your launch template will be overridden if there are any duplicate keys specified for the Auto Scaling group. ✕

Tags (0)

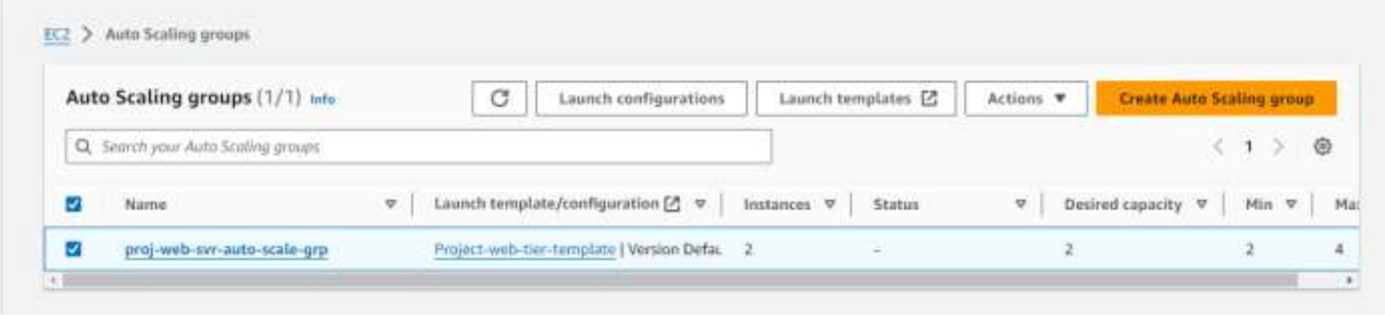
Add tag

50 remaining

Cancel | Previous | Next

Review your settings on the next page, and at the bottom, click the "Create Auto Scaling Group" button. You should see a green banner indicating your success. Once the ASG has finished updating capacity, navigate to your EC2 dashboard to verify that the new instance has been created.

Note: In my previous examples, my names were not accepted for the auto scaling group. Ensure that you follow the appropriate naming conventions.



EC2 > Auto Scaling groups

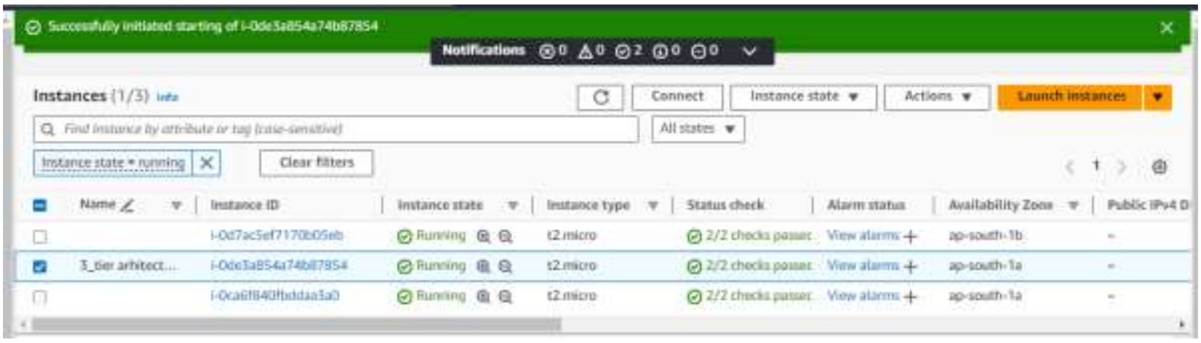
Auto Scaling groups (1/1) Info

Launch configurations | Launch templates | Actions ▼ | Create Auto Scaling group

Search your Auto Scaling groups

☑	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Ma
☑	proj-web-svr-auto-scale-grp	Project-web-tier-template | Version Defa	2	-	2	2	4

As you can see in the ec2 console it will show 2 more desired instanes, the Auto Scaling Group (ASG) is performing as expected.



Successfully initiated starting of i-0de3a854a74b87854

Notifications ⊗0 ⚠0 ⊘2 ⓘ0 ⊖0

Instances (1/3) Info

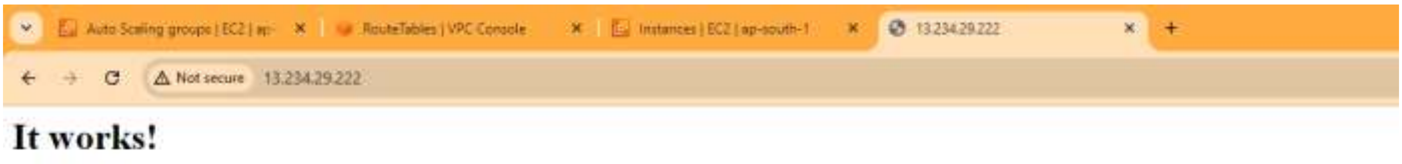
Connect | Instance state ▼ | Actions ▼ | Launch instances ▼

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

Instance state = running ✕ | Clear filters

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
☐		i-0d7ac5ef7170b05eb	✓ Running	t2.micro	✓ 2/2 checks passec	View alarms +	ap-south-1b	-
☑	3_tier arhitect...	i-0de3a854a74b87854	✓ Running	t2.micro	✓ 2/2 checks passec	View alarms +	ap-south-1a	-
☐		i-0ca6f840fbddaa3a0	✓ Running	t2.micro	✓ 2/2 checks passec	View alarms +	ap-south-1a	-

Before we proceed, it's a good idea to take a moment to connect to the instances that were created. As you can see, everything has been successful!



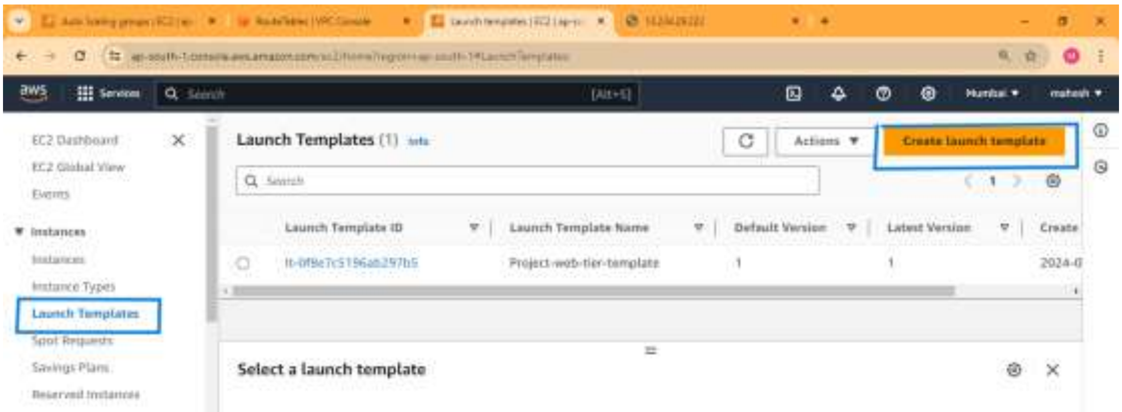
Auto Scaling groups | EC2 | ap- ✕ | RouteTables | VPC Console ✕ | Instances | EC2 | ap-south-1 ✕ | 13.234.29.222 ✕ +

⚠ Not secure 13.234.29.222

It works!

Step-3 : Creating an Application Tier

Next, we will create the back-end of our 3-tier architecture. Instead of starting with an EC2 instance, I'll begin by navigating to the Launch Templates tab under the EC2 dashboard.

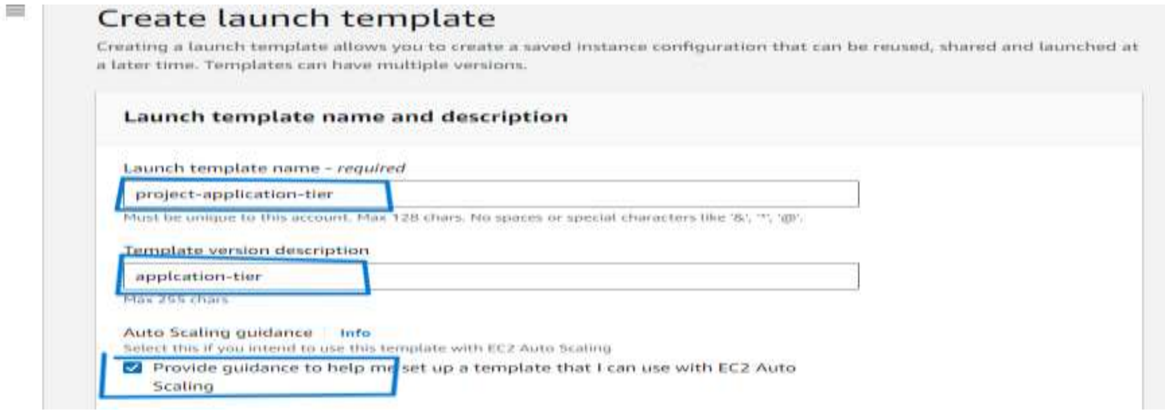


Launch Templates (1) Info

	Launch Template ID	Launch Template Name	Default Version	Latest Version	Create
○	lt-0f8e7c5196ab297b5	Project-web-tier-template	1	1	2024-0

Select a launch template

Name your new template and select the "Guidance" tab again.



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*

project-application-tier

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

Template version description

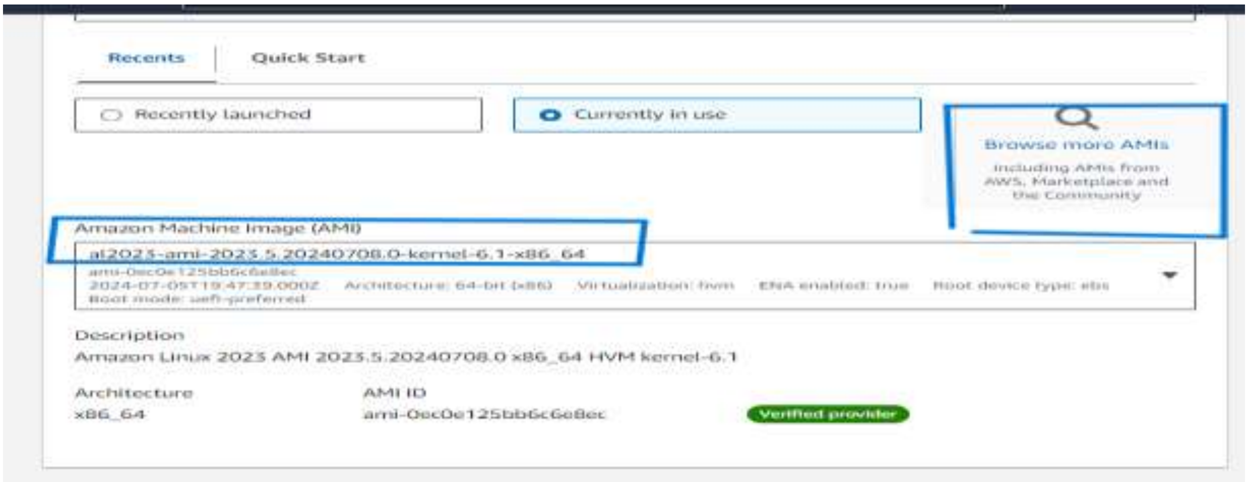
applcation-tier

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



Amazon Machine Image (AMI)

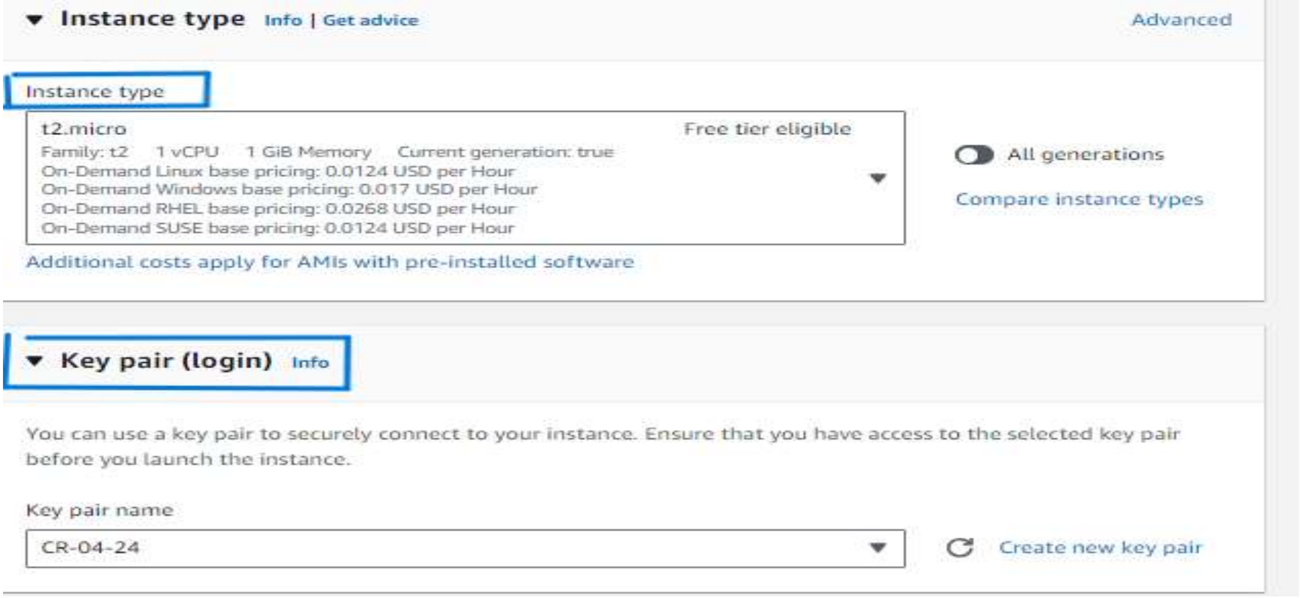
al2023-ami-2023.5.20240708.0-kernel-6.1-x86_64
ami-0ec0e125bb6c6e8ec
2024-07-05T19:47:39.000Z Architecture: 64-bit (x86) Virtualization: hvm ENA enabled: true Root device type: ebs
Boot mode: uefi-preferred

Description
Amazon Linux 2023 AMI 2023.5.20240708.0 x86_64 HVM kernel-6.1

Architecture
x86_64

AMI ID
ami-0ec0e125bb6c6e8ec

Select "Browse more AMIs," then choose Amazon Linux 2 for your AMI. Select the `t2.micro` instance type and also choose your key pair.



▼ Instance type Info | Get advice

Advanced

Instance type

t2.micro

Free tier eligible

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

On-Demand Linux base pricing: 0.0124 USD per Hour

On-Demand Windows base pricing: 0.017 USD per Hour

On-Demand RHEL base pricing: 0.0268 USD per Hour

On-Demand SUSE base pricing: 0.0124 USD per Hour

Additional costs apply for AMIs with pre-installed software

All generations

Compare instance types

▼ 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.

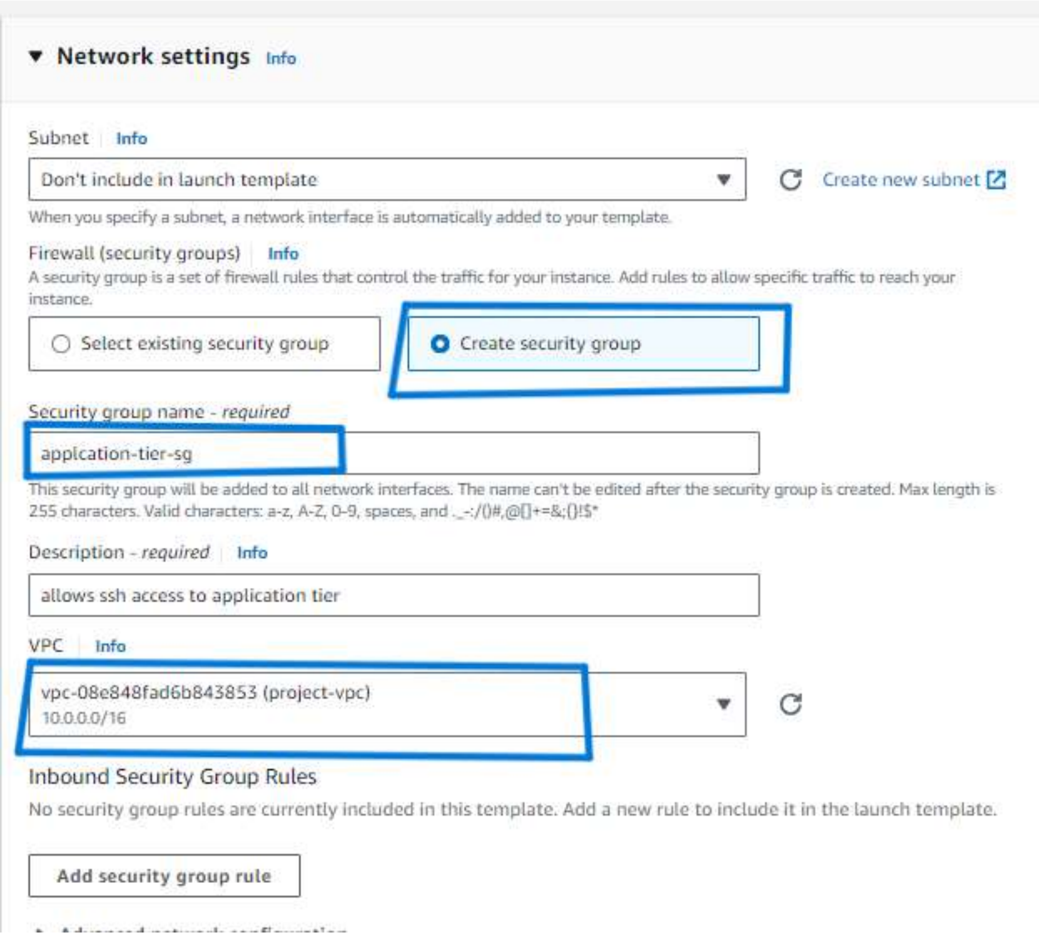
Key pair name

CR-04-24

Create new key pair

Under the network settings, we want to limit access to the application tier for security purposes. Ensure there is no public access to the application layer or the data tier. We will create a new security group. Select our VPC; I now realize that a better name could have been chosen for this part!

Name your new security group and select the VPC that we created at the beginning.



▼ Network settings Info

Subnet | Info

Don't include in launch template

Create new subnet

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

Firewall (security groups) | Info

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

○ Select existing security group

● Create security group

Security group name - *required*

applcation-tier-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* | Info

allows ssh access to application tier

VPC | Info

vpc-08e848fad6b843853 (project-vpc)
10.0.0.0/16

Inbound Security Group Rules

No security group rules are currently included in this template. Add a new rule to include it in the launch template.

Add security group rule

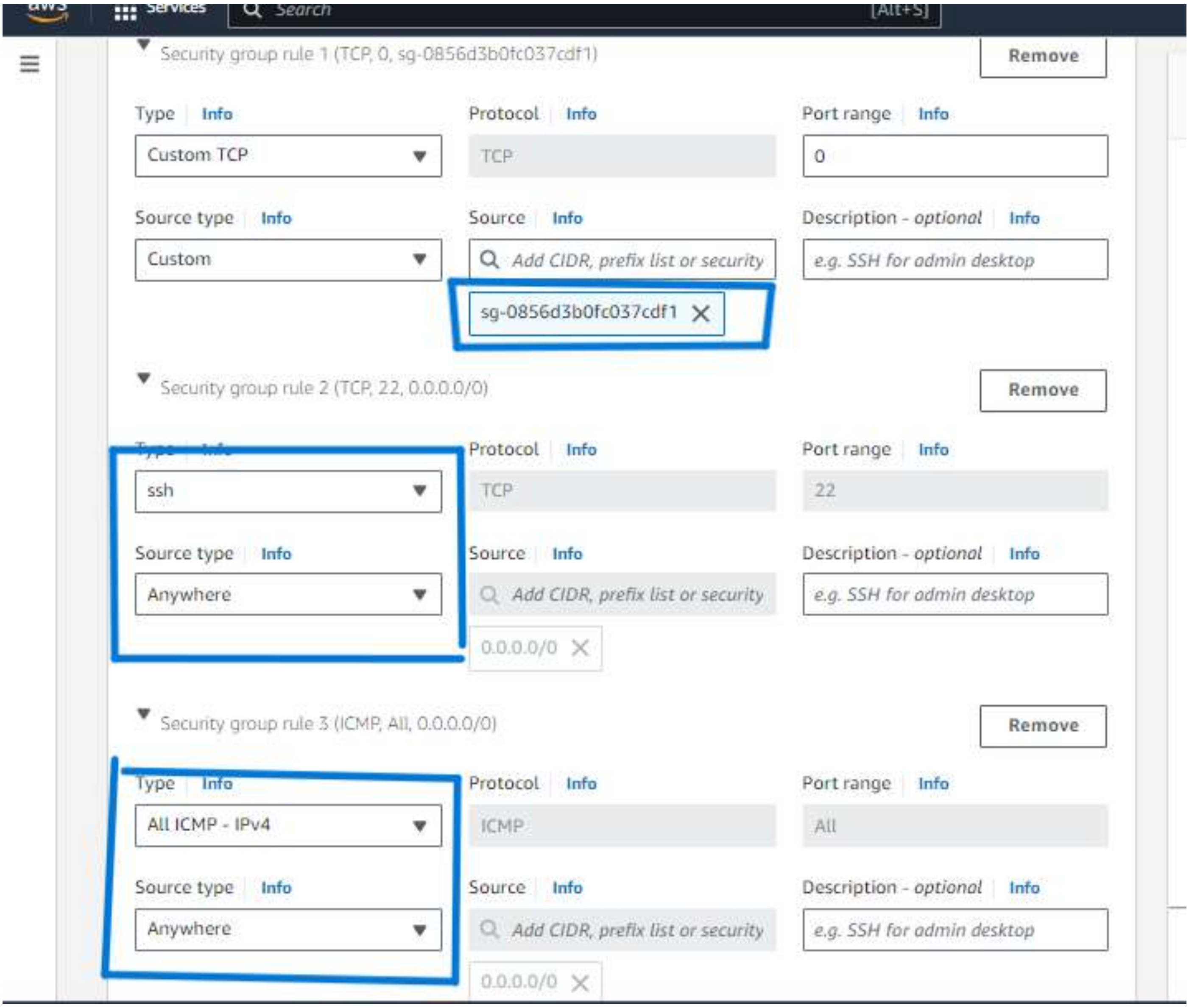
▸ Advanced network configuration

We will create three security group rules:

1. For SSH Access: Use "My IP" as the source.

2. For Custom TCP: Use the security group from our web tier (tier-1) as the source.

3. For ICMP (IPv4): Set the source type to "Anywhere" to allow ping requests from the public internet. This will help us test if traffic is routed properly to the application tier.



Security group rule 1 (TCP, 0, sg-0856d3b0fc037cdf1)

Type: Custom TCP
Protocol: TCP
Port range: 0
Source type: Custom
Source: Add CIDR, prefix list or security
sg-0856d3b0fc037cdf1 ✕
Description - *optional*: e.g. SSH for admin desktop

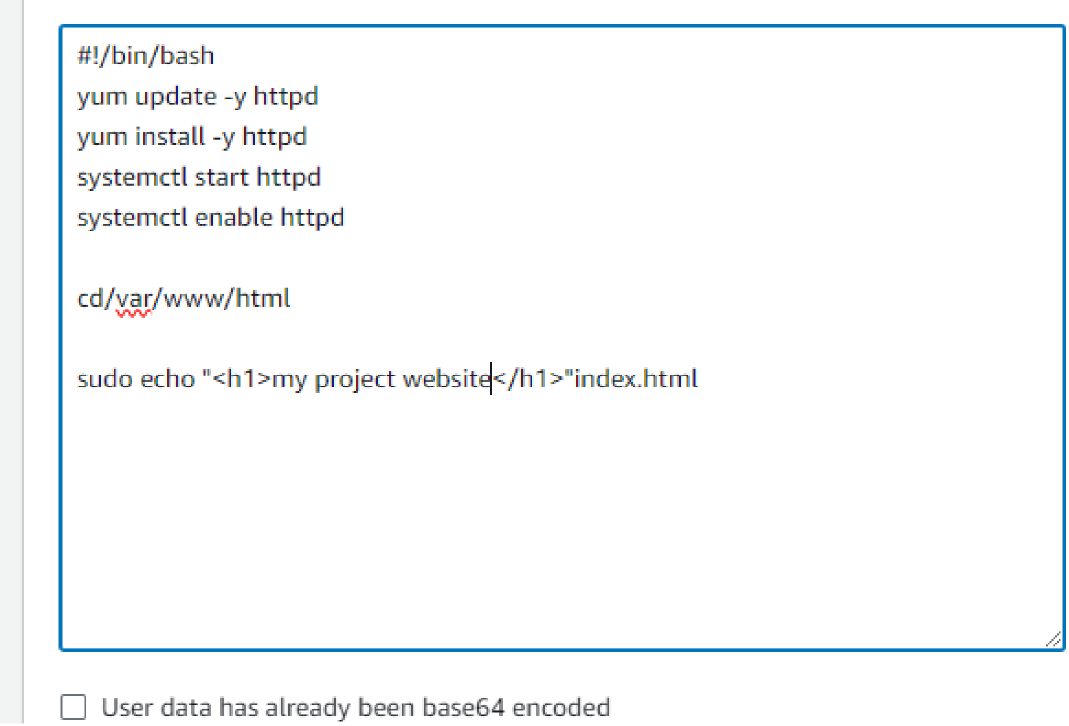
Security group rule 2 (TCP, 22, 0.0.0.0/0)

Type: ssh
Protocol: TCP
Port range: 22
Source type: Anywhere
Source: Add CIDR, prefix list or security
0.0.0.0/0 ✕
Description - *optional*: e.g. SSH for admin desktop

Security group rule 3 (ICMP, All, 0.0.0.0/0)

Type: All ICMP - IPv4
Protocol: ICMP
Port range: All
Source type: Anywhere
Source: Add CIDR, prefix list or security
0.0.0.0/0 ✕
Description - *optional*: e.g. SSH for admin desktop

We will leave the storage volumes as they are and proceed to the bottom of the "Advanced details" section to enter our script. After entering the script, click "Next."

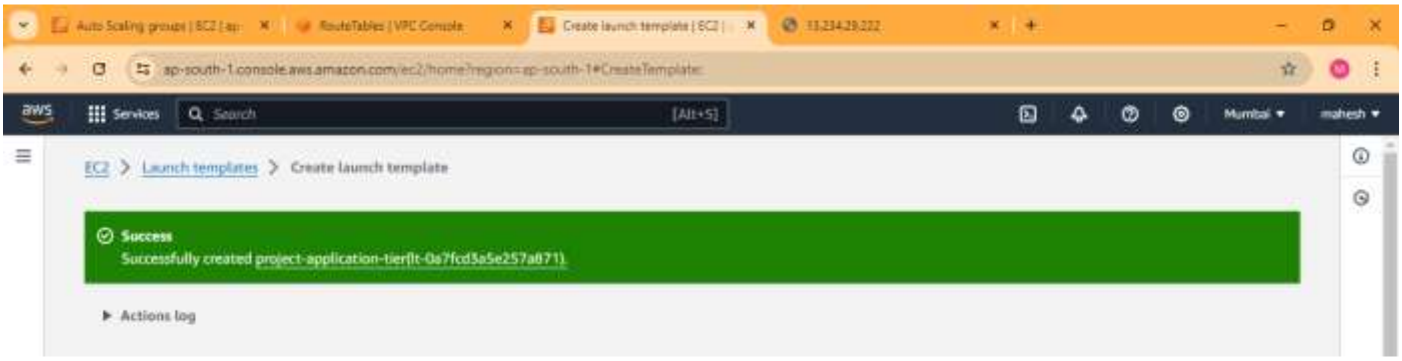


```
#!/bin/bash
yum update -y httpd
yum install -y httpd
systemctl start httpd
systemctl enable httpd

cd/var/www/html

sudo echo "<h1>my project website</h1>"index.html
```

□ User data has already been base64 encoded

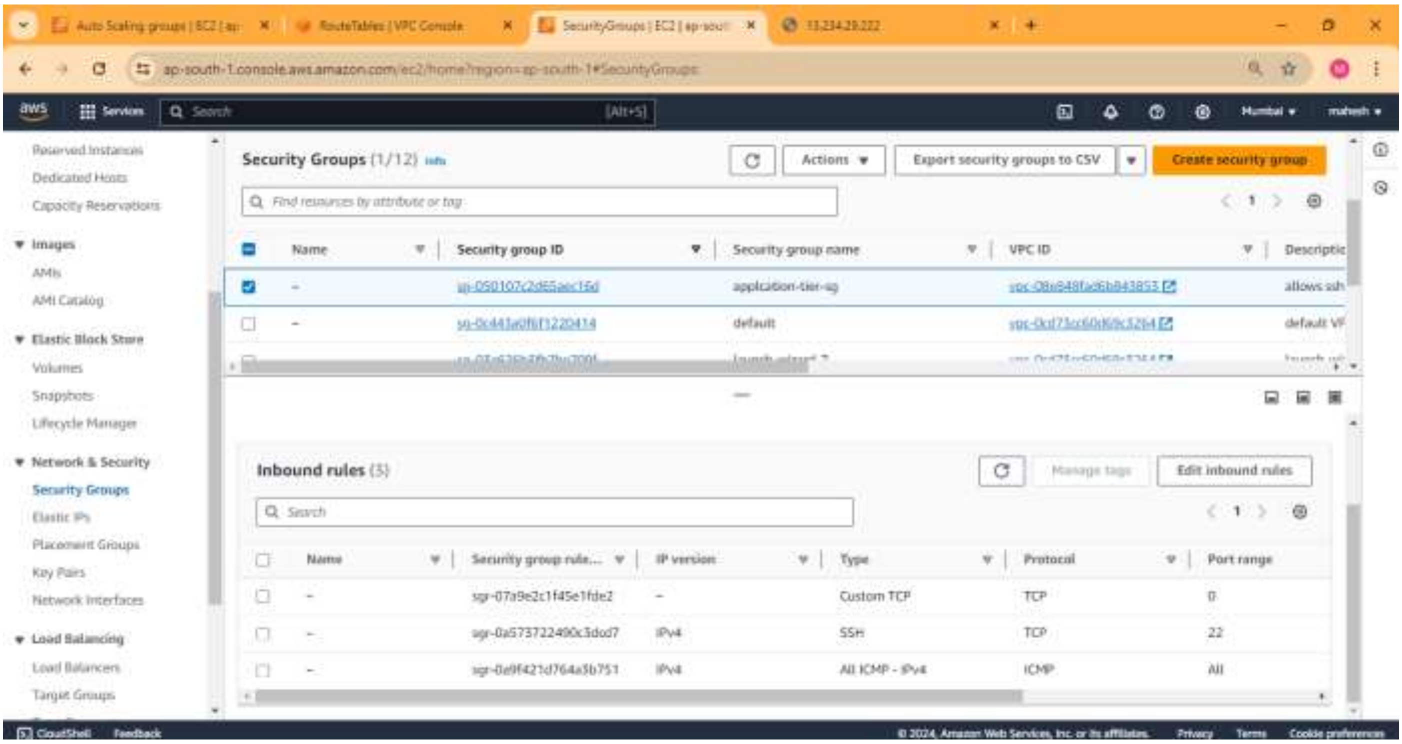


Auto Scaling groups | EC2 | ap
RouteTables | VPC Console
Create launch template | EC2 |
13.234.29.222
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#CreateTemplate:
aws
Services
Search
[Alt+S]
Mumbai ▾
mahesh ▾
EC2 > Launch templates > Create launch template
▸ Actions log

Success
Successfully created project-application-tier(lt-0a7fcd3a5e257a871).

Starting from scratch can be a learning experience, but modifying an existing template would indeed save time in the future. It’s all part of the learning process, and finding efficient ways to manage your resources is valuable!

I went back to the security group and updated my inbound rules.



Security Groups (1/12) Info

Actions ▾ | Export security groups to CSV | Create security group

Find resources by attribute or tag

	Name	Security group ID	Security group name	VPC ID	Descriptio
☑	–	sg-050107c2d65aec16d	application-tier-sg	vpc-08e848fad6b843853	allows ssh
□	–	sg-0c441a0f6f1220414	default	vpc-0cd73cc60d69c3264	default VP
□		sg-03a626b2fb7bc7001	launch-wizard-7	vpc-0cd73cc60d69c3264	launch-wiz

Inbound rules (3)

Manage tags | Edit inbound rules

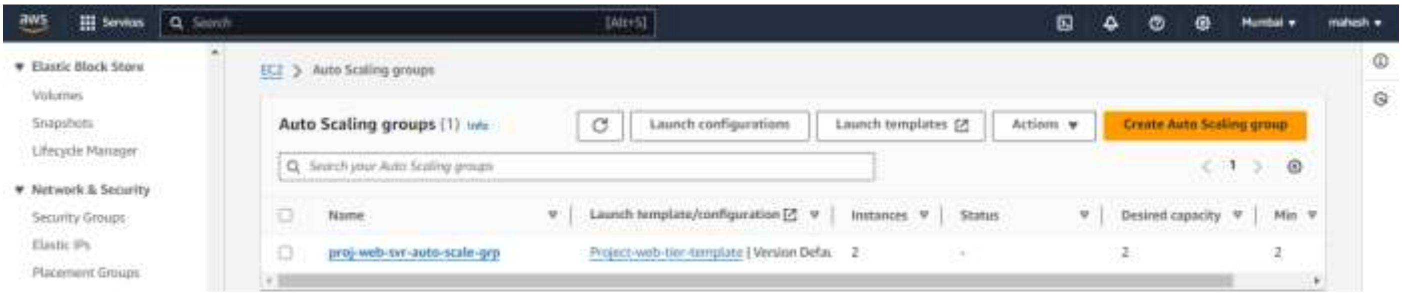
Search

	Name	Security group rule...	IP version	Type	Protocol	Port range
□	–	sgr-07a9e2c1f45e1fde2	–	Custom TCP	TCP	0
□	–	sgr-0a573722490c3dcd7	IPv4	SSH	TCP	22
□	–	sgr-0e9f421d764a3b751	IPv4	All ICMP - IPv4	ICMP	All

Once this was fixed, I went back and recreated the application layer template using the Application Tier SG1 that I just altered. I just double checked the security group rules and used the same settings for everything else above.

Application Tier Auto-Scaling Group:

Okay, now we're ready to create our Auto Scaling Group for the application layer. Under the EC2 dashboard, go to "Create an Auto Scaling Group."



Auto Scaling groups (1) Info

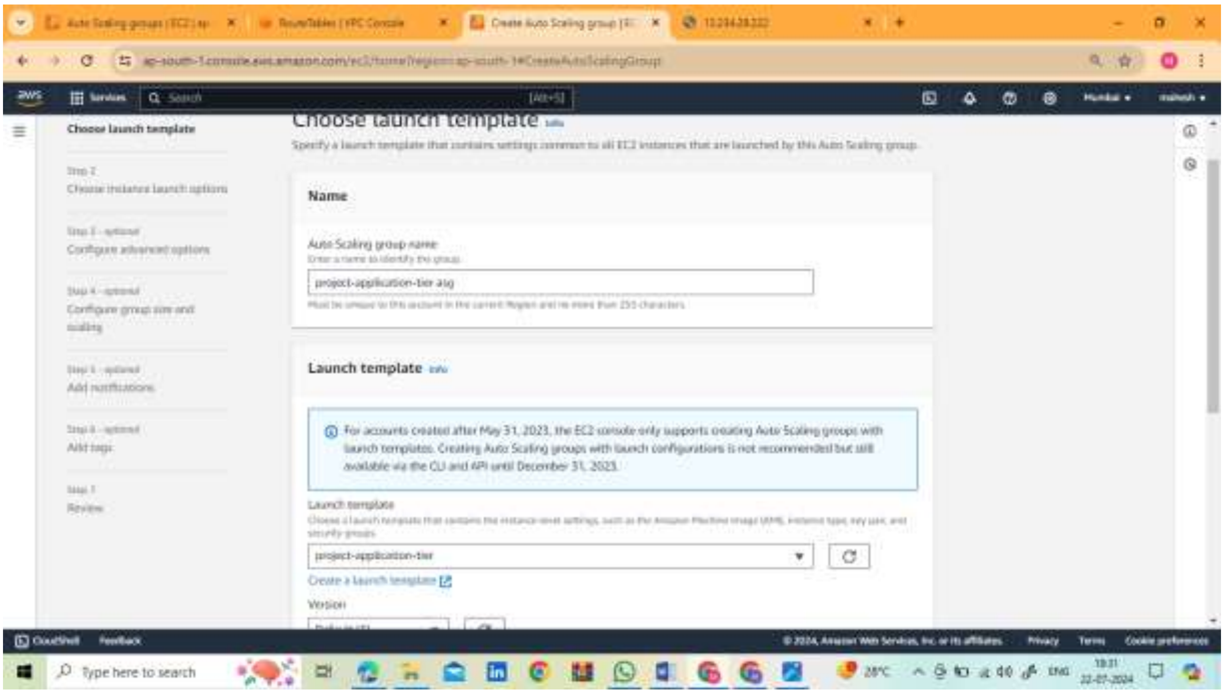
Launch configurations | Launch templates | Actions ▾ | Create Auto Scaling group

Search your Auto Scaling groups

□	Name	Launch template/configuration	Instances	Status	Desired capacity	Min
□	proj-web-svr-auto-scale-grp	Project-web-tier-template | Version Defa	2	-	2	2

Name your new Auto Scaling Group and select the appropriate launch template, then click the "Next" button.

Choose the correct VPC and select 2 private subnets, then click the "Next" button.



Choose launch template

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

Name

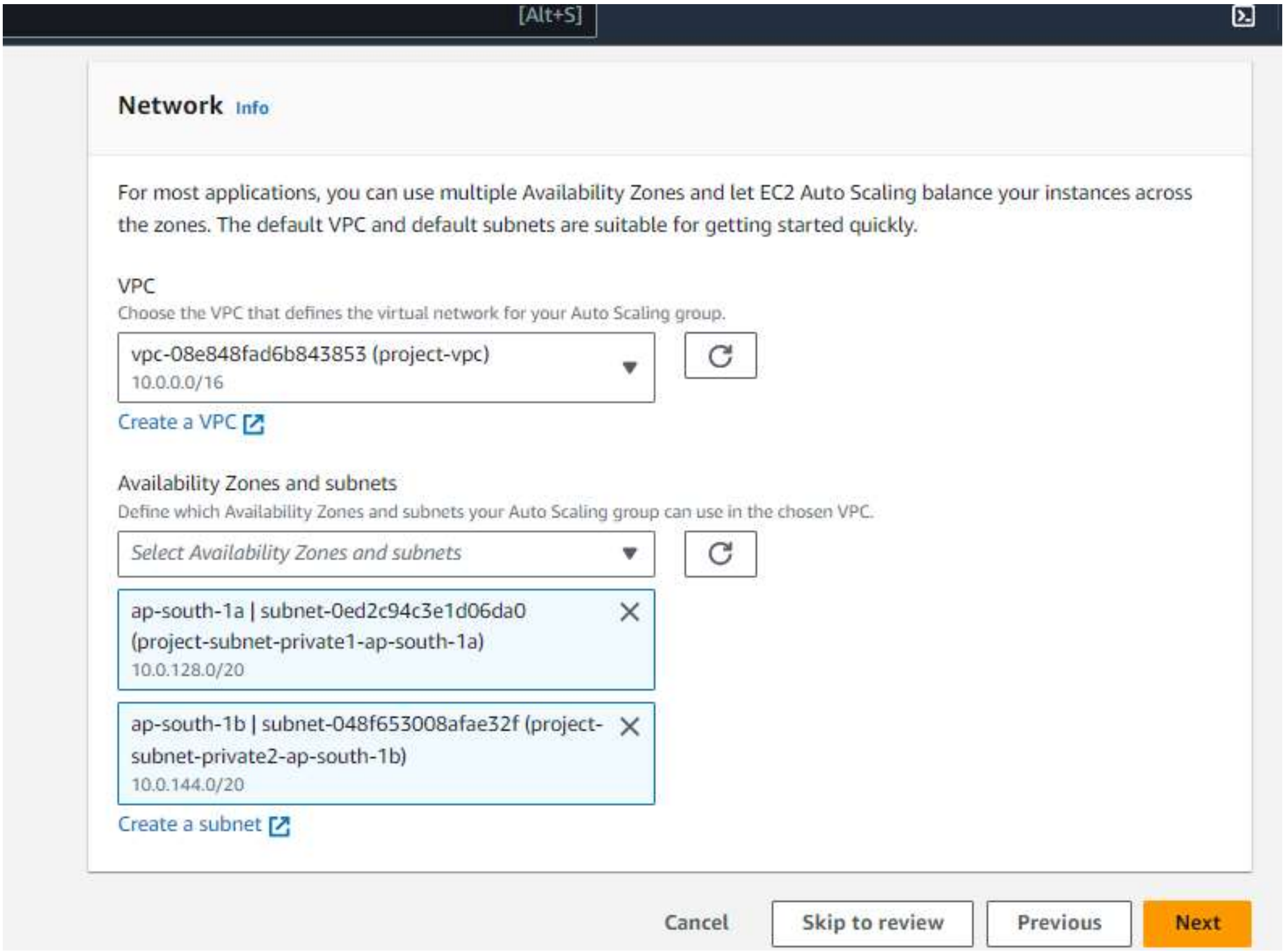
Auto Scaling group name: project-application-tier asg

Launch template

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: project-application-tier

We are given the option to attach a load balancer, and we want to do this. Select an application load balancer, name it, and configure it as an internal load balancer. Double-check that the VPC and subnets are correct. My settings are accurate.



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.

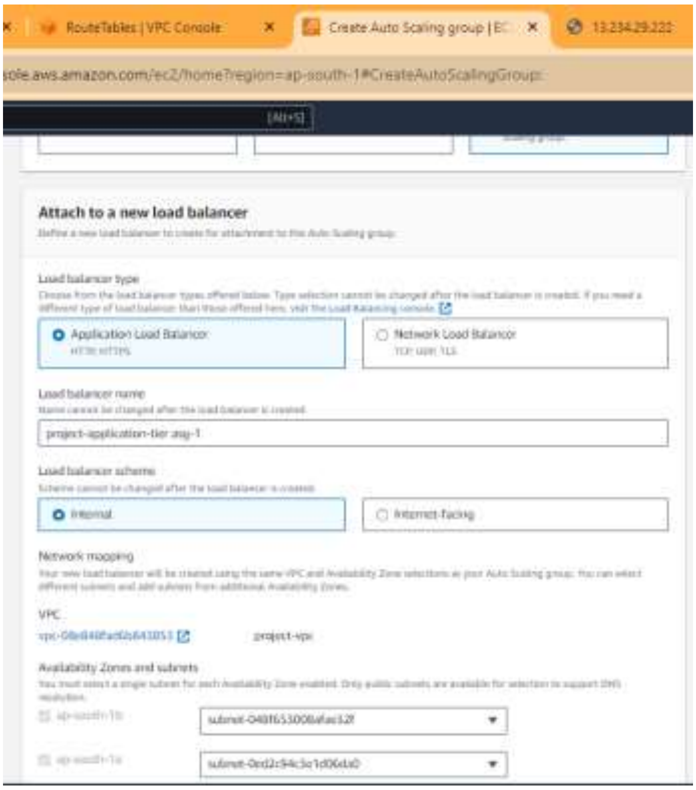
vpc-08e848fad6b843853 (project-vpc)
10.0.0.0/16

Availability Zones and subnets

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

ap-south-1a | subnet-0ed2c94c3e1d06da0 (project-subnet-private1-ap-south-1a)
10.0.128.0/20

ap-south-1b | subnet-048f653008afae32f (project-subnet-private2-ap-south-1b)
10.0.144.0/20



RouteTables | VPC Console

Create Auto Scaling group | EC

13.234.29.222

sole.aws.amazon.com/ec2/home?region=ap-south-1#CreateAutoScalingGroup:

[Alt+S]

Attach to a new load balancer

Define a new load balancer to create for attachment to this Auto Scaling group.

Load balancer type

Choose from the load balancer types offered below. Type selection cannot be changed after the load balancer is created. If you need a different type of load balancer than those offered here, visit the Load Balancing console

● Application Load Balancer
HTTP, HTTPS

○ Network Load Balancer
TCP, UDP, TLS

Load balancer name

Name cannot be changed after the load balancer is created.

project-application-tier asg-1

Load balancer scheme

Scheme cannot be changed after the load balancer is created.

● Internal

○ Internet-facing

Network mapping

Your new load balancer will be created using the same VPC and Availability Zone selections as your Auto Scaling group. You can select different subnets and add subnets from additional Availability Zones.

VPC

vpc-08e848fad2b643053 project-vpc

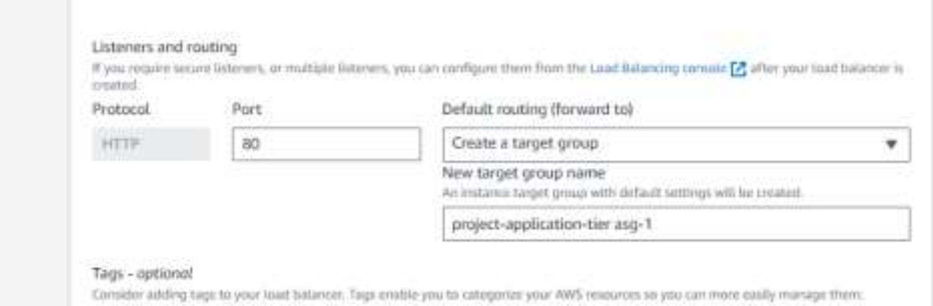
Availability Zones and subnets

You must select a single subnet for each Availability Zone enabled. Only public subnets are available for selection to support DNS resolution.

☑ ap-south-1b subnet-0481653008afac32f

☑ ap-south-1a subnet-0ed2c94c3c1d06da0

Under "Listeners and routing," create a new target group and set the port to 80 once again.



Listeners and routing

If you require secure listeners, or multiple listeners, you can configure them from the Load Balancing console after your load balancer is created.

Protocol	Port	Default routing (forward to)
HTTP	80	Create a target group

New target group name

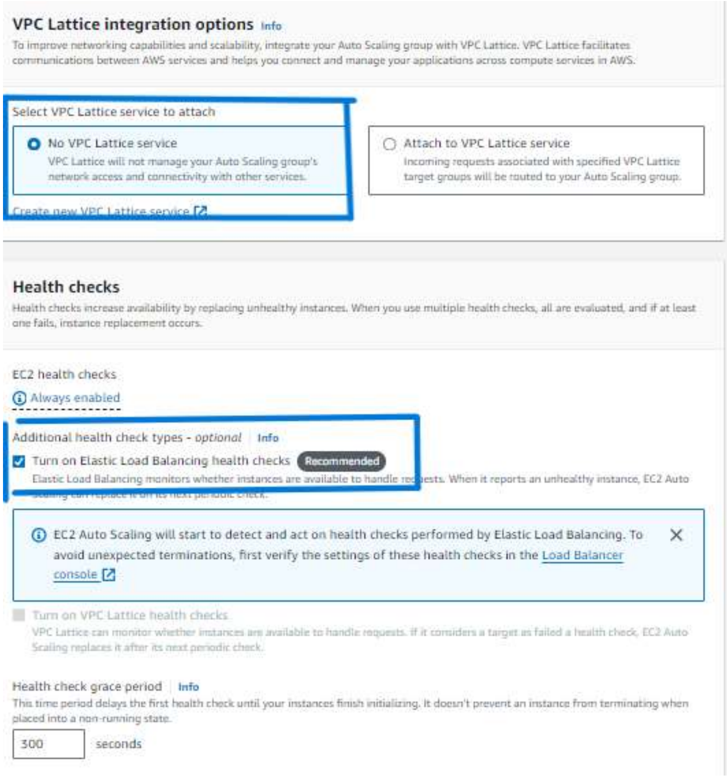
An instance target group with default settings will be created.

project-application-tier asg-1

Tags - optional

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

Below, I have chosen to turn on health checks and enable group metrics within Cloud-Watch.



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

● No VPC Lattice service
VPC Lattice will not manage your Auto Scaling group's network access and connectivity with other services.

○ Attach to VPC Lattice service
Incoming requests associated with specified VPC Lattice target groups will be routed to your Auto Scaling group.

Create new VPC Lattice service

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

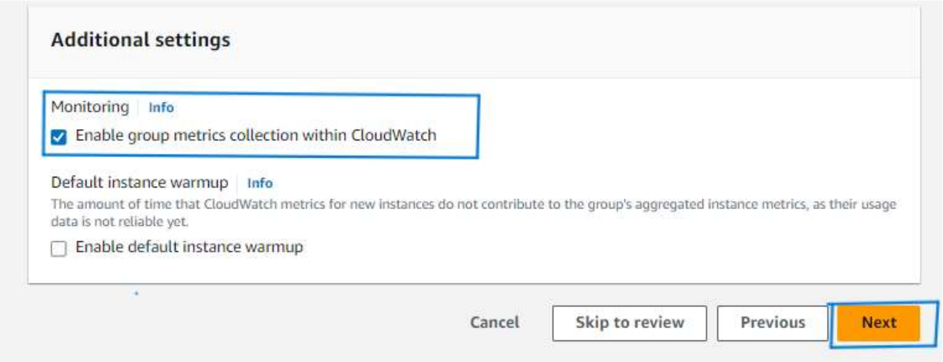
Additional health check types - *optional* Info

☑ 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
VPC Lattice can monitor whether instances are available to handle requests. If it considers a target as failed a health check, EC2 Auto Scaling replaces it after its next periodic check.

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.
300 seconds



Additional settings

Monitoring Info
☑ Enable group metrics collection within CloudWatch

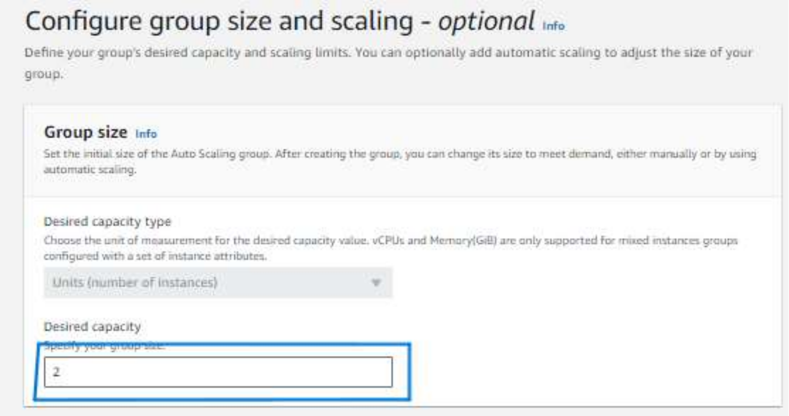
Default instance warmup Info
The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.
□ Enable default instance warmup

On the next screen, set your desired capacity, minimum capacity, and maximum capacity:

- Desired capacity: 2

- Minimum capacity: 2

- Maximum capacity: 4



Configure group size and scaling - *optional* Info

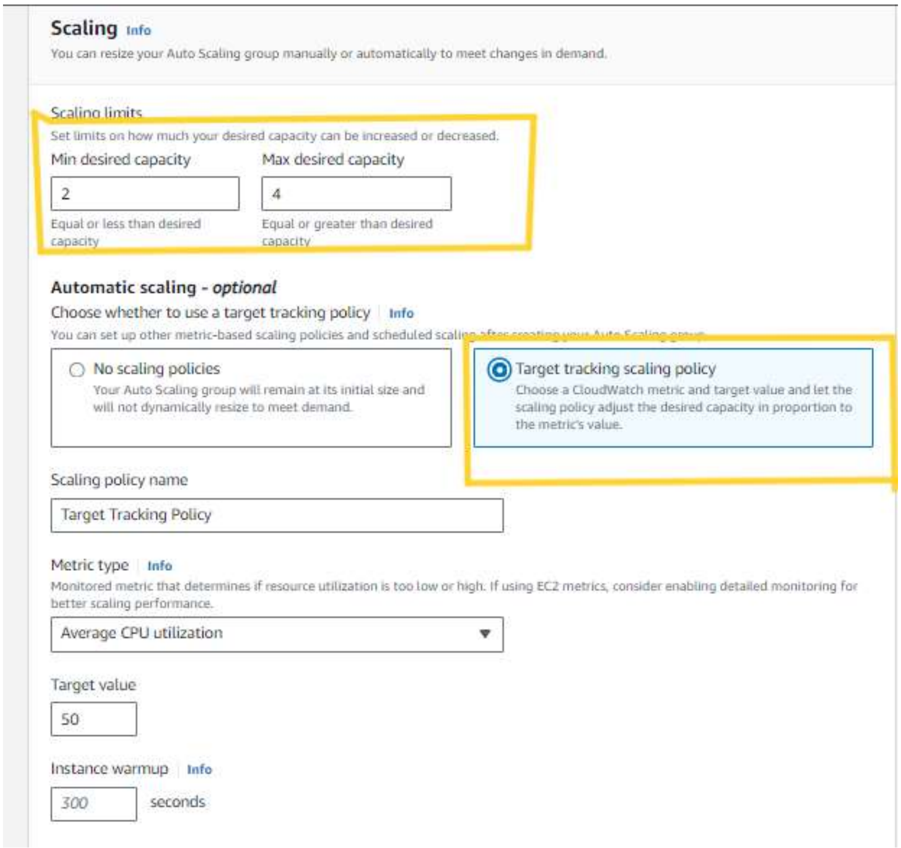
Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.

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: 2 (Equal or less than desired capacity)

Max desired capacity: 4 (Equal or greater than desired capacity)

Automatic scaling - *optional*

Choose whether to use a target tracking policy Info

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

○ No scaling policies
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

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

Scaling policy name: Target Tracking Policy

Metric type Info

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

Average CPU utilization

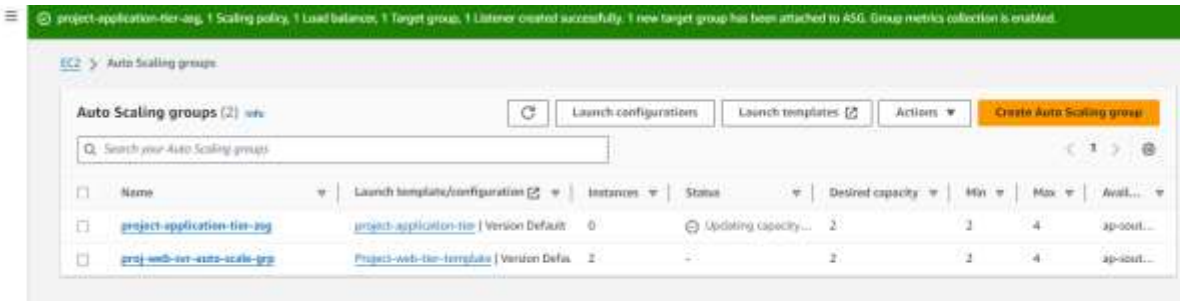
Target value: 50

Instance warmup Info: 300 seconds

Then, I selected target tracking with a CPU utilization target of 50%.

Click the "Next" button. Add notifications if desired, then add tags. Review your new Auto Scaling Group (ASG) settings and create it.

As you can see below, my new application layer ASG is updating the capacity.



project-application-tier-asg, 1 Scaling policy, 1 Load balancer, 1 Target group, 1 Listener created successfully. 1 new target group has been attached to ASG. Group metrics collection is enabled.

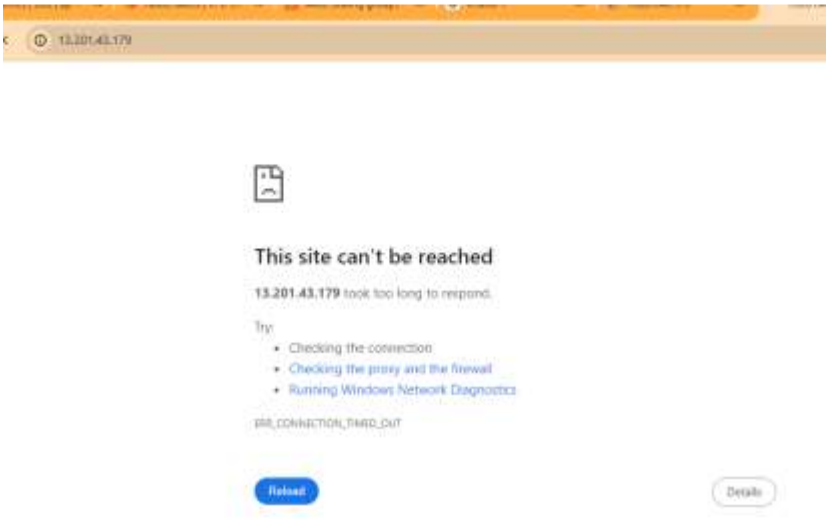
EC2 > Auto Scaling groups

Auto Scaling groups (2) Info

	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Avail...
□	project-application-tier-asg	project-application-tier | Version Default	0	Updating capacity...	2	2	4	ap-sout...
□	proj-web-tier-auto-scale-grp	Project-web-tier-template | Version Defa...	2	-	2	2	4	ap-sout...

Once the new EC2 instances are created and running, we will attempt to SSH into them. If we set it up correctly, we should not be able to establish a connection.

When I tried to SSH into the application tier EC2 instance, the connection timed out, which is exactly the expected outcome.



13.201.43.179

This site can't be reached

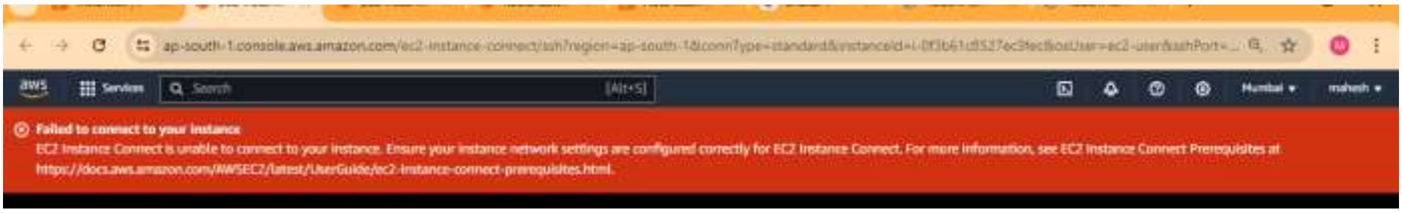
13.201.43.179 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

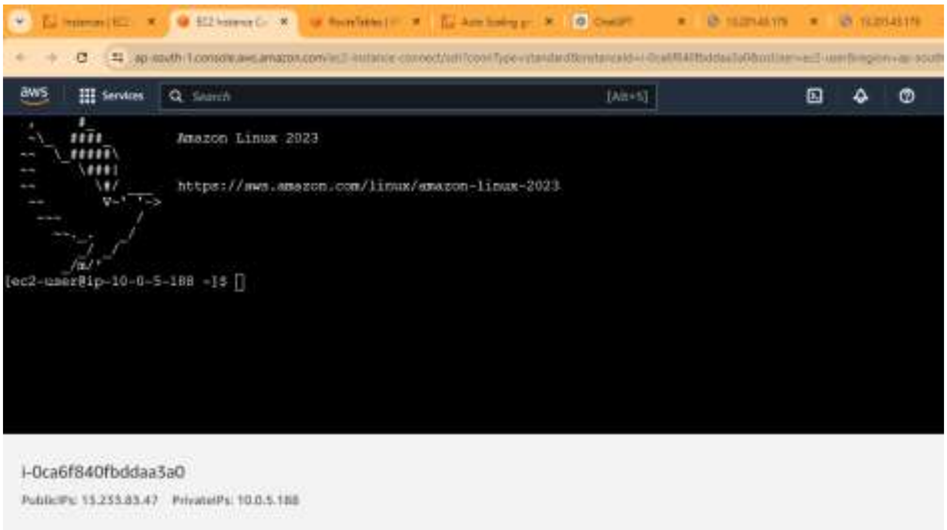
Try to connect your newly created instance using Git Bash or the AWS console. If it does not connect, it shows a timeout error.



Failed to connect to your instance
EC2 Instance Connect is unable to connect to your instance. Ensure your instance network settings are configured correctly for EC2 Instance Connect. For more information, see EC2 Instance Connect Prerequisites at https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-prerequisites.html.

I also tried to connect using EC2 Connect, and this failed as well.

Next, we need to check if our tier-1 servers interact with our tier-2 servers. To test this, log in to your tier-1 EC2 instances via SSH and run a ping command to the private IP address of our tier-2 servers. Below, you can see a successful ping.



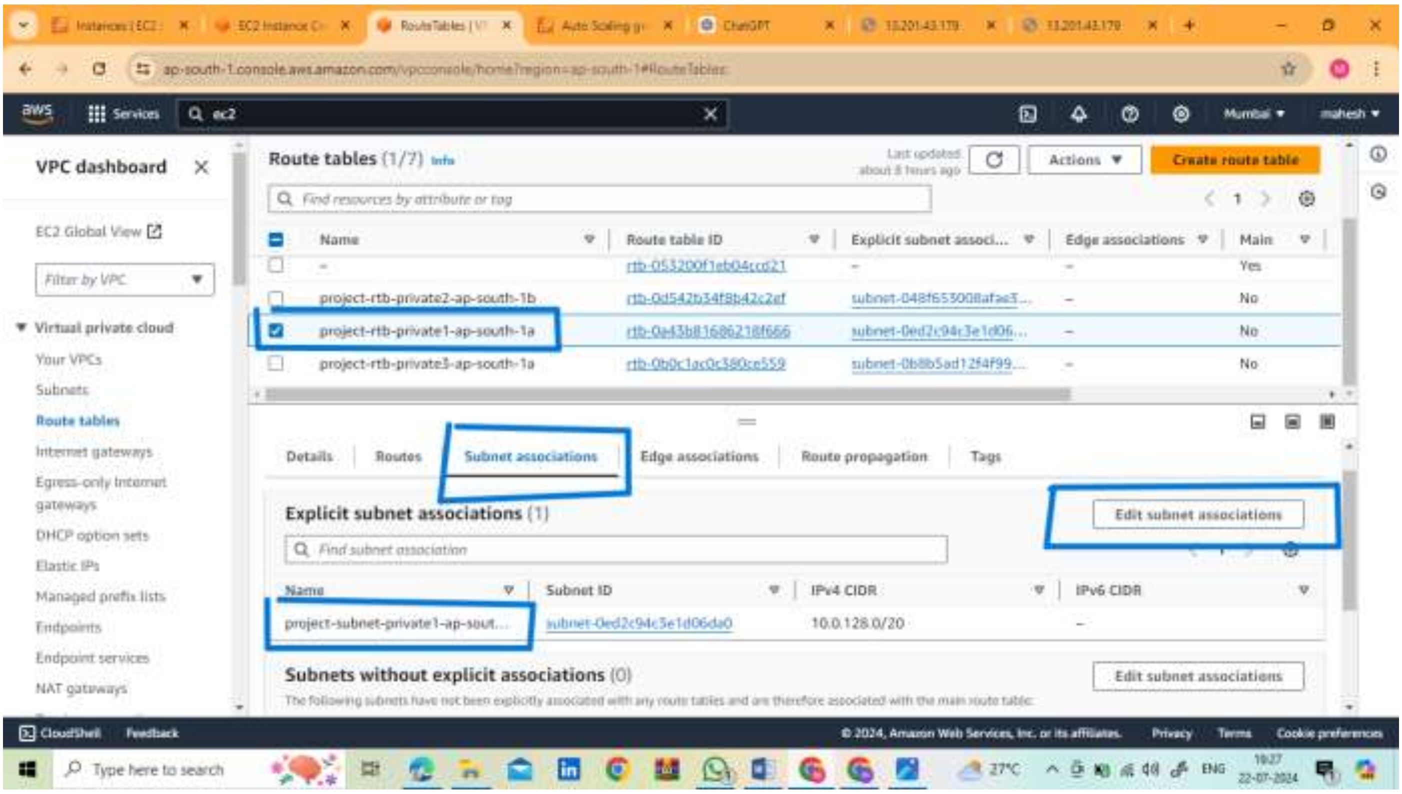
```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-5-188 ~]$ 
```

i-0ca6f840fbddaa3a0

PublicIPs: 13.233.83.47   PrivateIPs: 10.0.5.188

Update the application (Tier-2) Route table:

Head back to the VPC dashboard, select "Route Tables," and choose one of the route tables that was automatically created when we set up our VPC. I only have one subnet associated with this table, so click on "Edit Subnet Associations."



Route tables (1/7)

	Name	Route table ID	Explicit subnet associ...	Edge associations	Main
□	–	rtb-053200f1eb04ccd21	–	–	Yes
□	project-rtb-private2-ap-south-1b	rtb-0d542b34f8b42c2ef	subnet-048f653008afae3...	–	No
☑	project-rtb-private1-ap-south-1a	rtb-0a43b81686218f666	subnet-0ed2c94c3e1d06...	–	No
□	project-rtb-private3-ap-south-1a	rtb-0b0c1ac0c380ce559	subnet-0b8b5ad12f4f99...	–	No

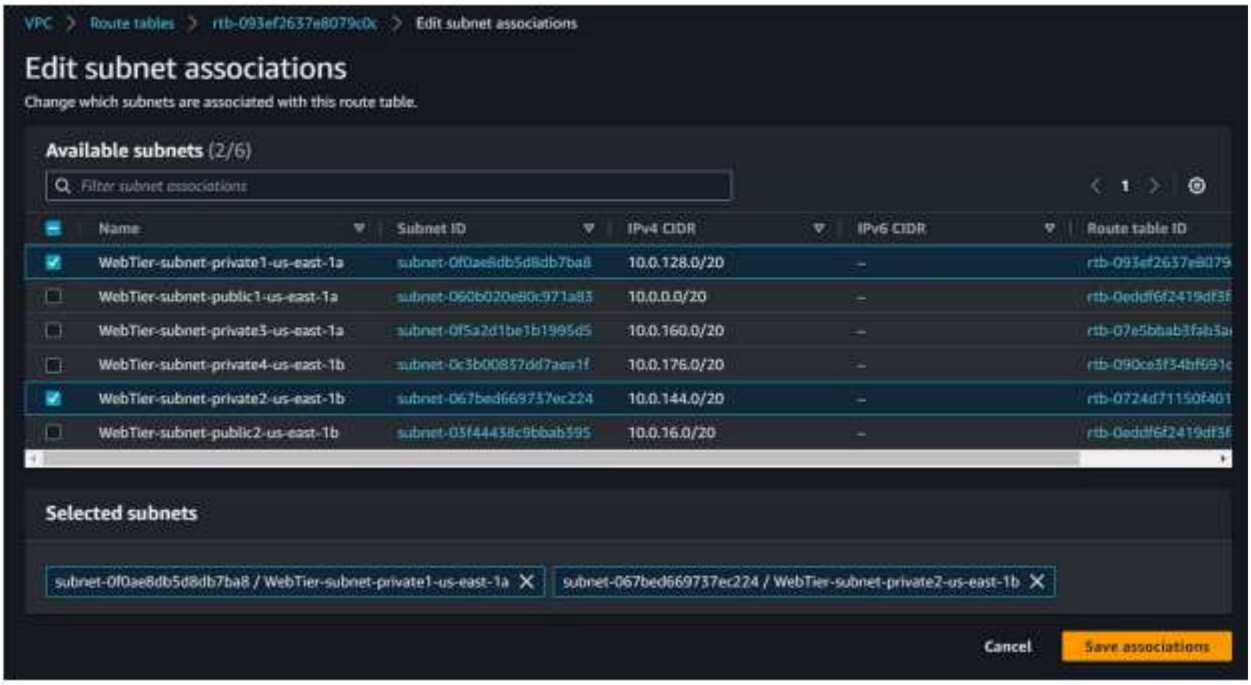
Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
project-subnet-private1-ap-sout...	subnet-0ed2c94c3e1d06da0	10.0.128.0/20	–

Subnets without explicit associations (0)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Addanothersubnetthatisprivate.



VPC > Route tables > rtb-093ef2637e8079c0c > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/6)

☐	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	WebTier-subnet-private1-us-east-1a	subnet-0f0ae8db5d8db7ba8	10.0.128.0/20	–	rtb-093ef2637e8079
☐	WebTier-subnet-public1-us-east-1a	subnet-060b020e80c971a83	10.0.0.0/20	–	rtb-0eddf6f2419df3f
☐	WebTier-subnet-private3-us-east-1a	subnet-0f5a2d1be1b1995d5	10.0.160.0/20	–	rtb-07e5bbab3fab3a
☐	WebTier-subnet-private4-us-east-1b	subnet-0c3b00837dd7aea1f	10.0.176.0/20	–	rtb-090ce3f34bf691c
☑	WebTier-subnet-private2-us-east-1b	subnet-067bed669737ec224	10.0.144.0/20	–	rtb-0724d71150f401
☐	WebTier-subnet-public2-us-east-1b	subnet-03f44438c9bbab395	10.0.16.0/20	–	rtb-0eddf6f2419df3f

Selected subnets

subnet-0f0ae8db5d8db7ba8 / WebTier-subnet-private1-us-east-1a ✕

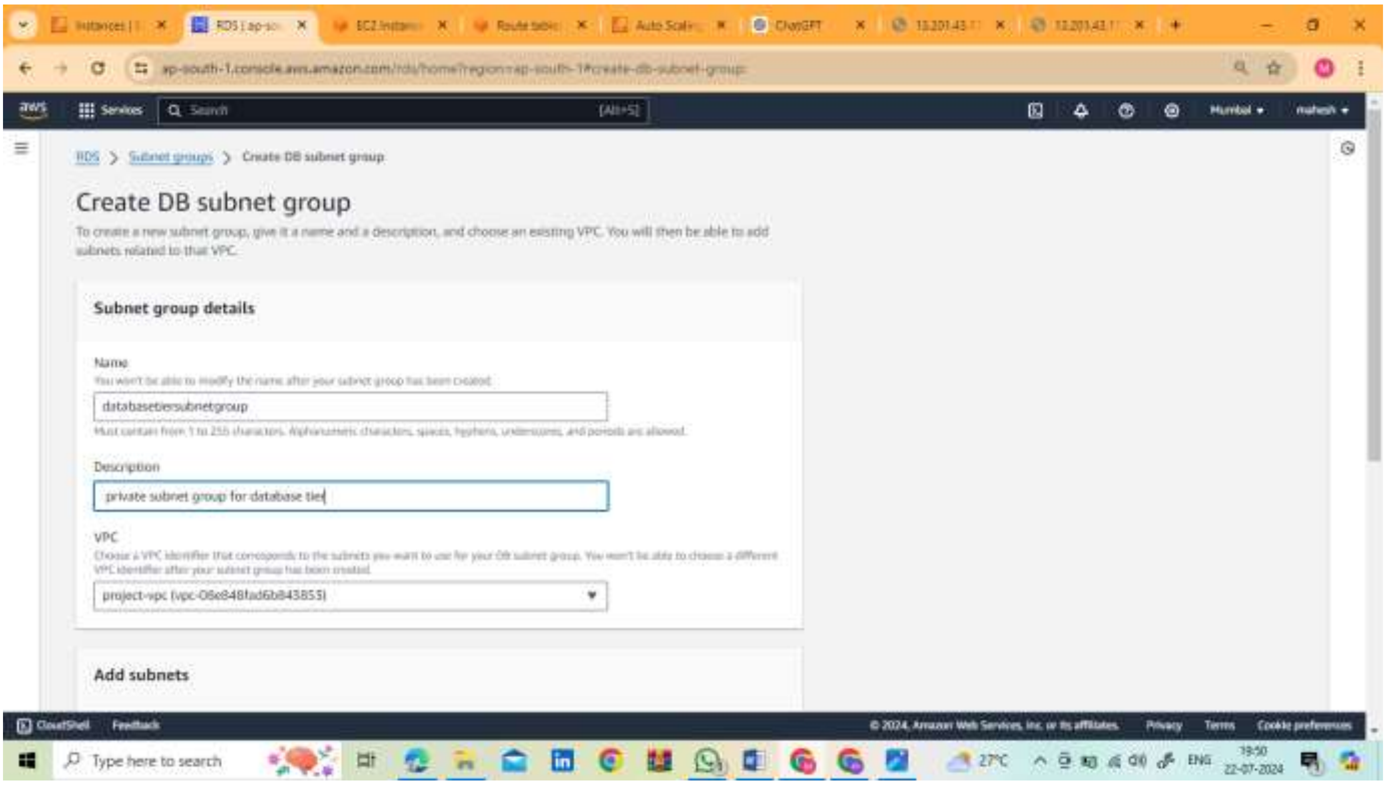
subnet-067bed669737ec224 / WebTier-subnet-private2-us-east-1b ✕

Part 4: Creating a Database Tier:

Almost there! We have created and tested 2 out of the 3 tiers successfully. We are now going to build our database tier. For this exercise, we will use a MySQL RDS database, though AWS offers several types of databases.

Create a DB Subnet Group:

We will begin by creating a subnet group. Navigate to the RDS console, click on "Subnet Groups" in the left-side menu, and then click the orange "Create DB Subnet Group" button.



RDS > Subnet groups > Create DB subnet group

Create DB subnet group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet group details

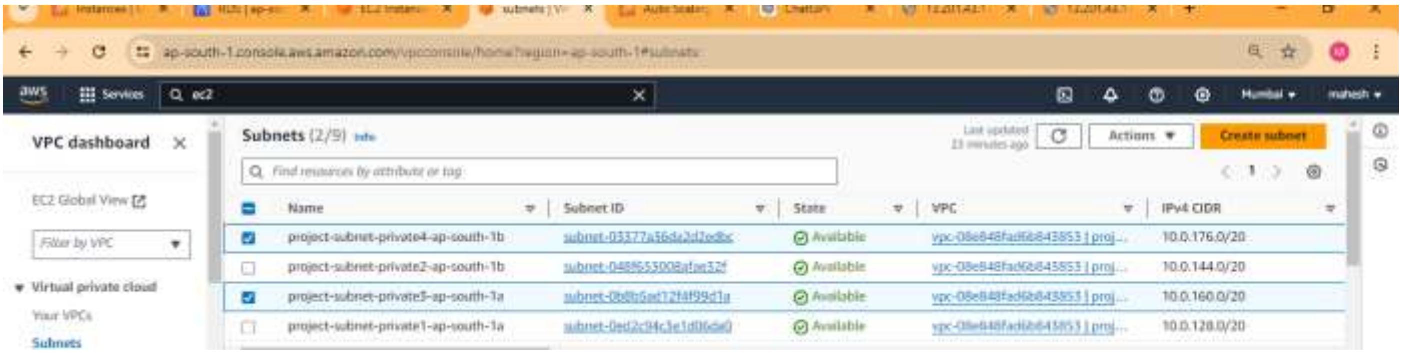
Name
You won't be able to modify the name after your subnet group has been created.
databasetiersubnetgroup
Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description
private subnet group for database tie

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.
project-vpc (vpc-08e848fad6b843853)

Add subnets

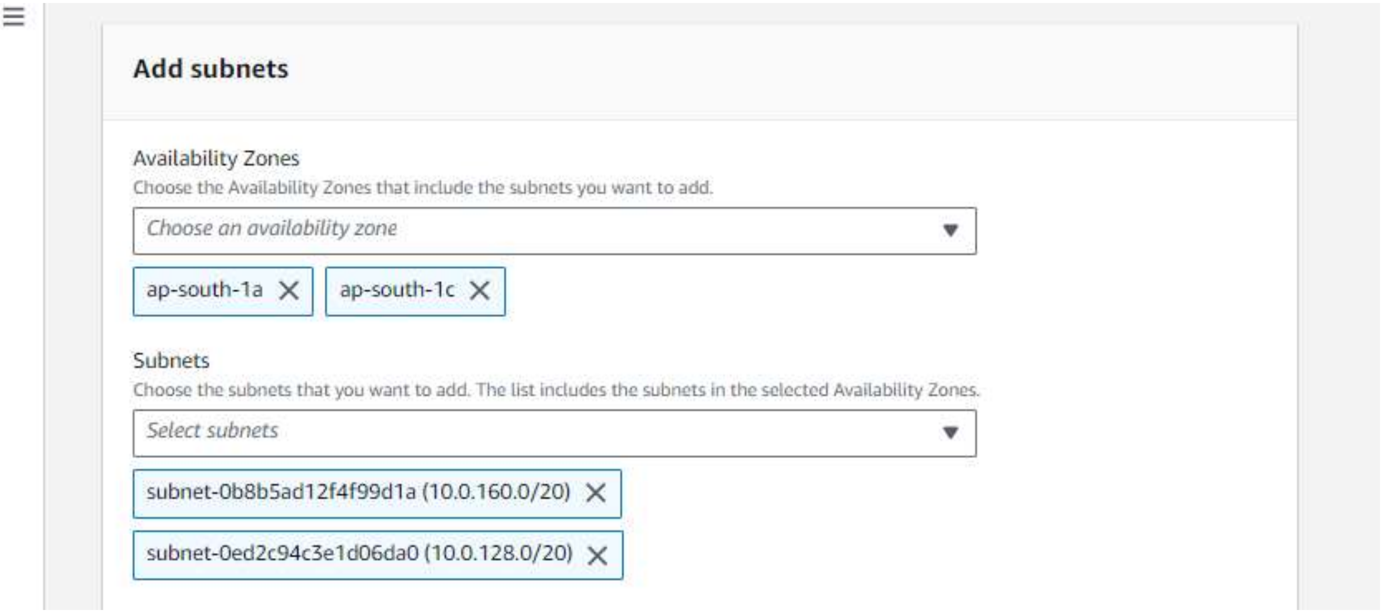
For the next part, we need to know the availability zones for the last two subnets that were automatically created. Head back to the VPC console. Under "Subnets," locate the last two subnets you have, ensuring you do not select the private subnets already used in tier 2.



Subnets (2/9)

	Name	Subnet ID	State	VPC	IPv4 CIDR
☑	project-subnet-private4-ap-south-1b	subnet-03377a56da2d2edbc	Available	vpc-08e848fad6b843853 | proj...	10.0.176.0/20
□	project-subnet-private2-ap-south-1b	subnet-0489553008afae32f	Available	vpc-08e848fad6b843853 | proj...	10.0.144.0/20
☑	project-subnet-private3-ap-south-1a	subnet-0b8b5ad12f4f99d1a	Available	vpc-08e848fad6b843853 | proj...	10.0.160.0/20
□	project-subnet-private1-ap-south-1a	subnet-0ed2c94c3e1d06da0	Available	vpc-08e848fad6b843853 | proj...	10.0.128.0/20

Back at the RDS console, select the availability zones that you are going to use.



Add subnets

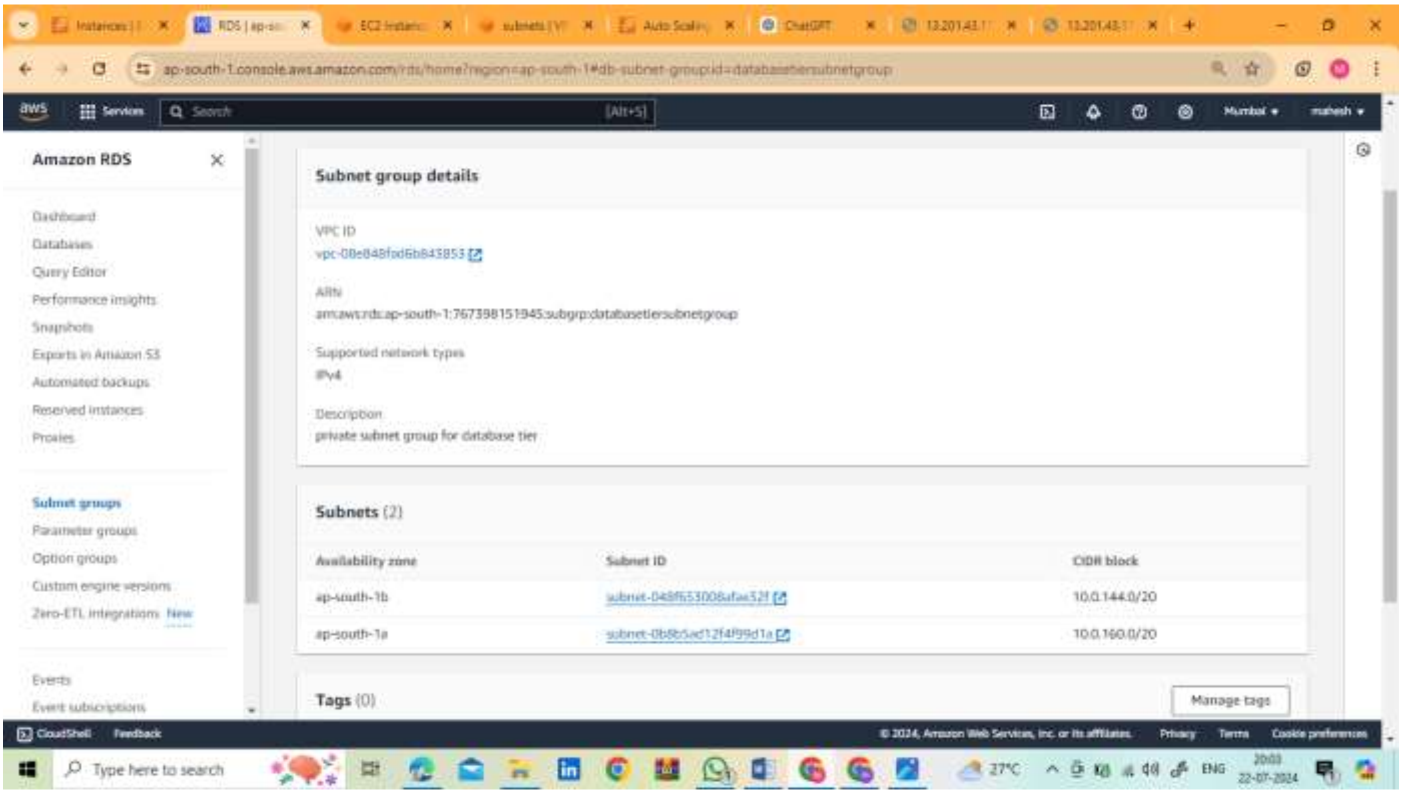
Availability Zones
Choose the Availability Zones that include the subnets you want to add.
Choose an availability zone

ap-south-1a ✕ ap-south-1c ✕

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

subnet-0b8b5ad12f4f99d1a (10.0.160.0/20) ✕

subnet-0ed2c94c3e1d06da0 (10.0.128.0/20) ✕



Subnet group details

VPC ID
vpc-08e848fad6b843853

ARN
arn:aws:rds:ap-south-1:767398151945:subgrp:databasetiersubnetgroup

Supported network types
IPv4

Description
private subnet group for database tier

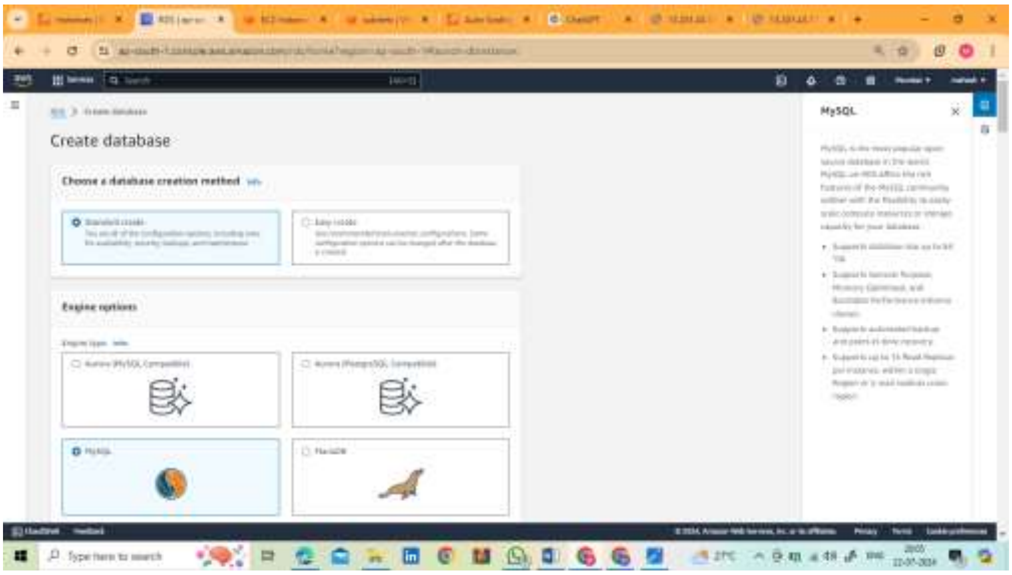
Subnets (2)

Availability zone	Subnet ID	CIDR block
ap-south-1b	subnet-048f653008afae32f	10.0.144.0/20
ap-south-1a	subnet-0b8b5ad12f4f99d1a	10.0.160.0/20

Tags (0)

Manage tags

Back in the RDS console, click 'Create database.' Select the MySQL DB option.



Create database

Choose a database creation method Info

● Standard create

○ Easy create

Engine options

Engine type Info

○ Aurora (MySQL Compatible)

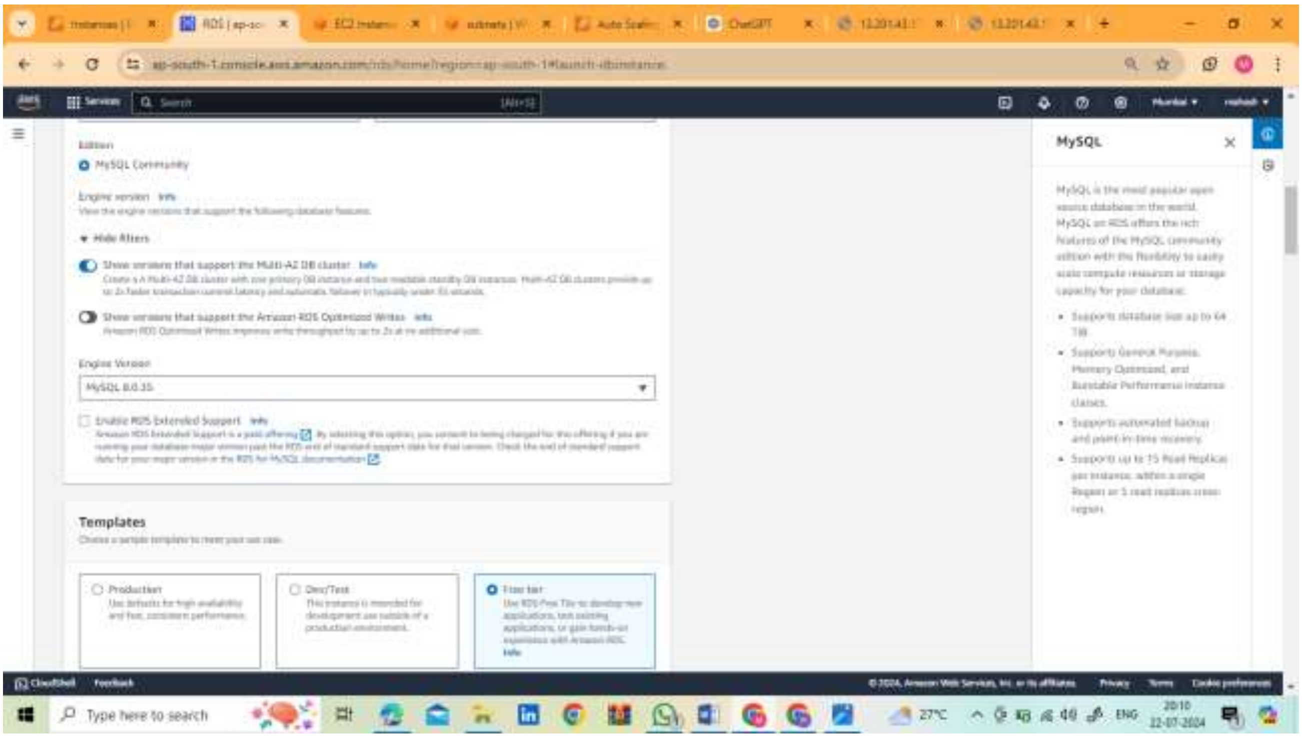
○ Aurora (PostgreSQL Compatible)

● MySQL

○ MariaDB

MySQL

Next, you can choose a Multi-AZ deployment with three database instances: one primary instance and two read-only standby instances. This setup provides a very reliable system, but we do not need this at the moment.



Edition

● MySQL Community

Engine version Info

View the engine versions that support the following database features.

▼ Hide filters

Show versions that support the Multi-AZ DB cluster Info

Create a A Multi-AZ DB cluster with one primary DB instance and two readable standby DB instances. Multi-AZ DB clusters provide up to 2x faster transaction commit latency and automatic failover in typically under 35 seconds.

Show versions that support the Amazon RDS Optimized Writes Info

Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

Engine Version

MySQL 8.0.35

□ Enable RDS Extended Support Info

Amazon RDS Extended Support is a paid offering. By selecting this option, you consent to being charged for this offering if you are running your database major version past the RDS end of standard support date for that version. Check the end of standard support date for your major version in the RDS for MySQL documentation.

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.

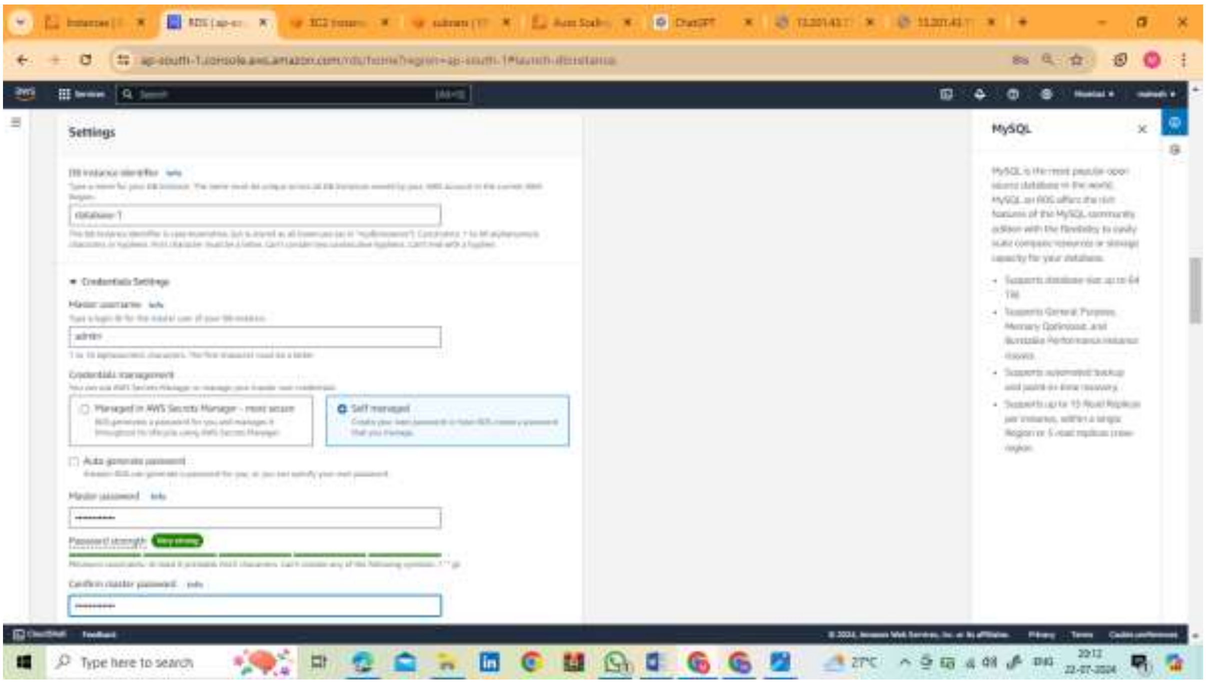
● Free tier
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. Info

MySQL

MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

There are also availability and durability options; however, none are available with the free tier. We do not need them either. Under 'Settings,' name your DB and create a master username and password. These credentials should be different from your AWS account login, as they are specific to the database you are creating.



Settings

DB instance identifier Info

database-1

▾ Credentials Settings

Master username Info

admin

Credentials management

○ Managed in AWS Secrets Manager - most secure

● Self managed

□ Auto generate password

Master password Info

Password strength Very strong

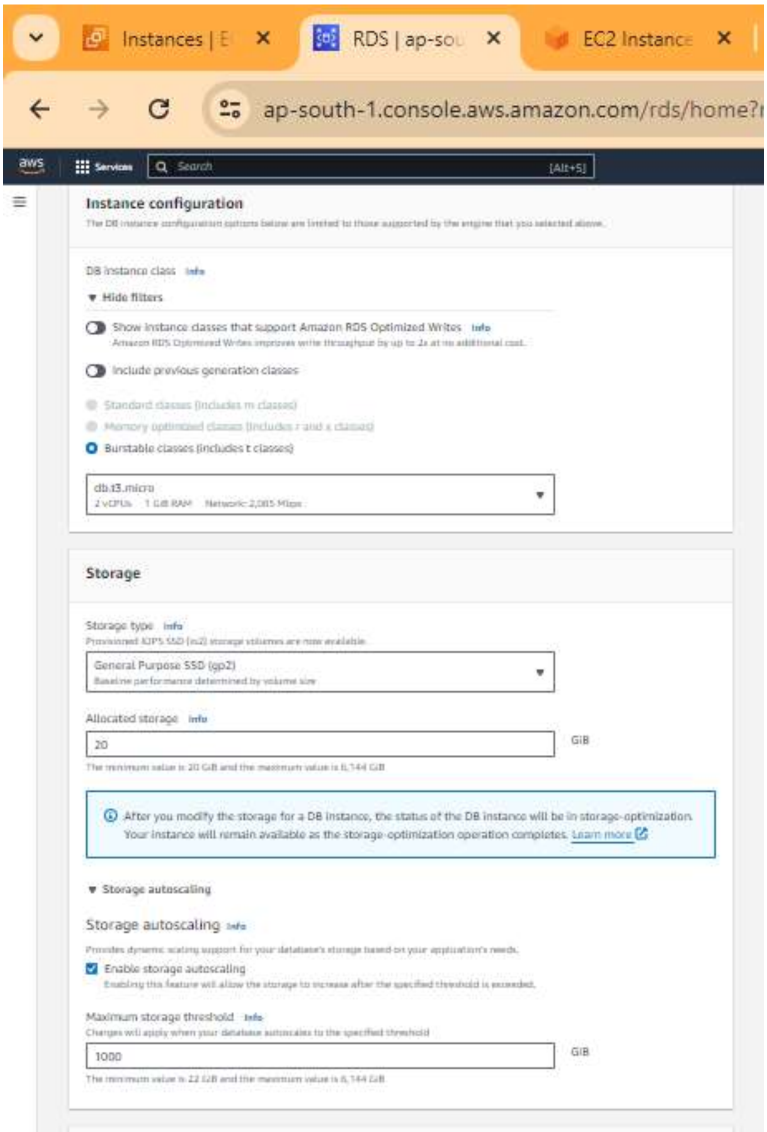
Confirm master password Info

MySQL

MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

You will need your username and password, so make sure to store them in a secure place! Under 'Instance configuration,' the burstable classes option is pre-selected because it’s the only one available for the free tier. I left my instance type as `db.t2.micro`. You can add storage as needed; I left mine at the default settings.



Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class Info

▼ Hide filters

○ Show instance classes that support Amazon RDS Optimized Writes Info
Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

○ Include previous generation classes

○ Standard classes (includes m classes)
○ Memory optimized classes (includes r and x classes)
● Burstable classes (includes t classes)

db.t3.micro
2 vCPUs 1 GiB RAM Network: 2,085 Mbps

Storage

Storage type Info
Provisioned IOPS SSD (io2) storage volumes are now available.

General Purpose SSD (gp2)
Baseline performance determined by volume size

Allocated storage Info
20 GiB
The minimum value is 20 GiB and the maximum value is 6,144 GiB

After you modify the storage for a DB instance, the status of the DB instance will be in storage-optimization. Your instance will remain available as the storage-optimization operation completes. Learn more

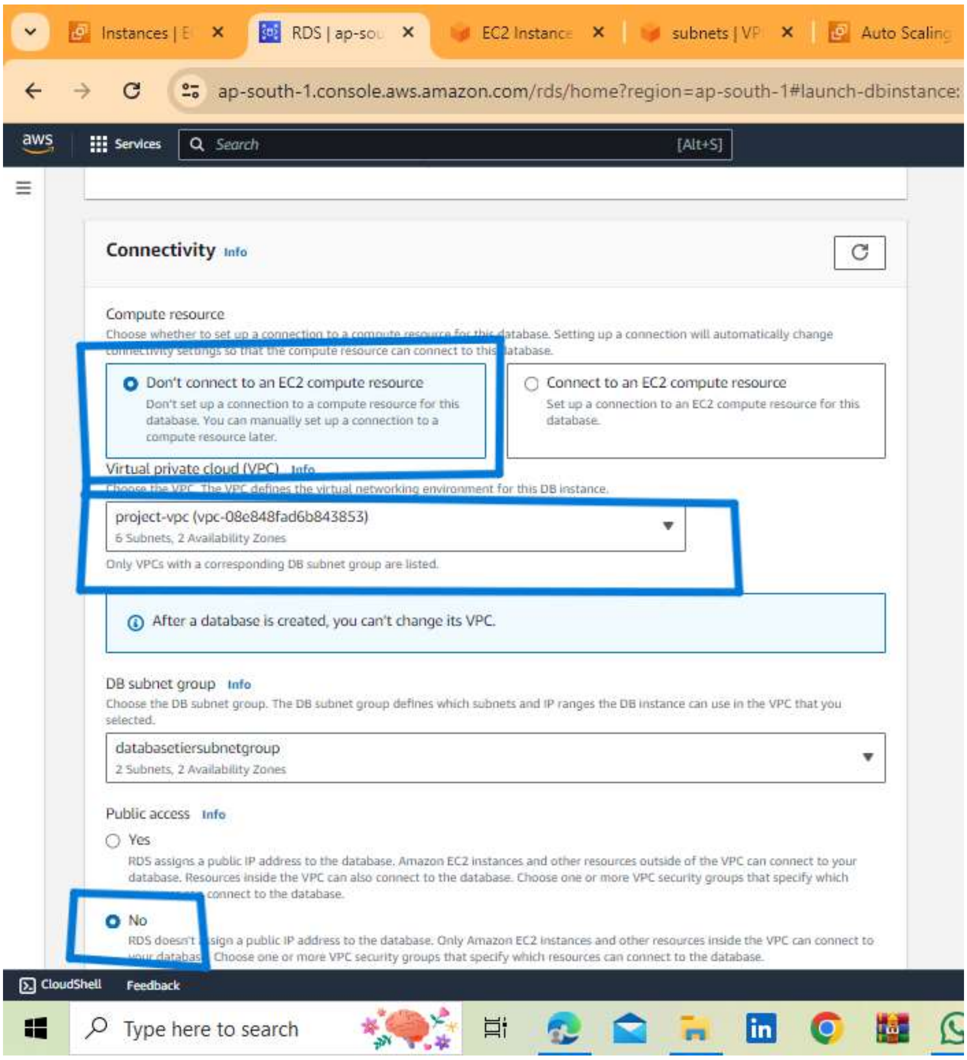
▼ Storage autoscaling

Storage autoscaling Info
Provides dynamic scaling support for your database's storage based on your application's needs.

☑ Enable storage autoscaling
Enabling this feature will allow the storage to increase after the specified threshold is exceeded.

Maximum storage threshold Info
Charges will apply when your database autoscales to the specified threshold
1000 GiB
The minimum value is 22 GiB and the maximum value is 6,144 GiB

We are going to set up our network manually, so choose not to connect to an EC2 resource. Select the appropriate VPC; the subnet group you created earlier should be listed as default. Choose 'Create new VPC security group (firewall).



ap-south-1.console.aws.amazon.com/rds/home?region=ap-south-1#launch-dbinstance:

Connectivity Info

Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

● Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

○ Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.

Virtual private cloud (VPC) Info

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

project-vpc (vpc-08e848fad6b843853)
6 Subnets, 2 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

DB subnet group Info

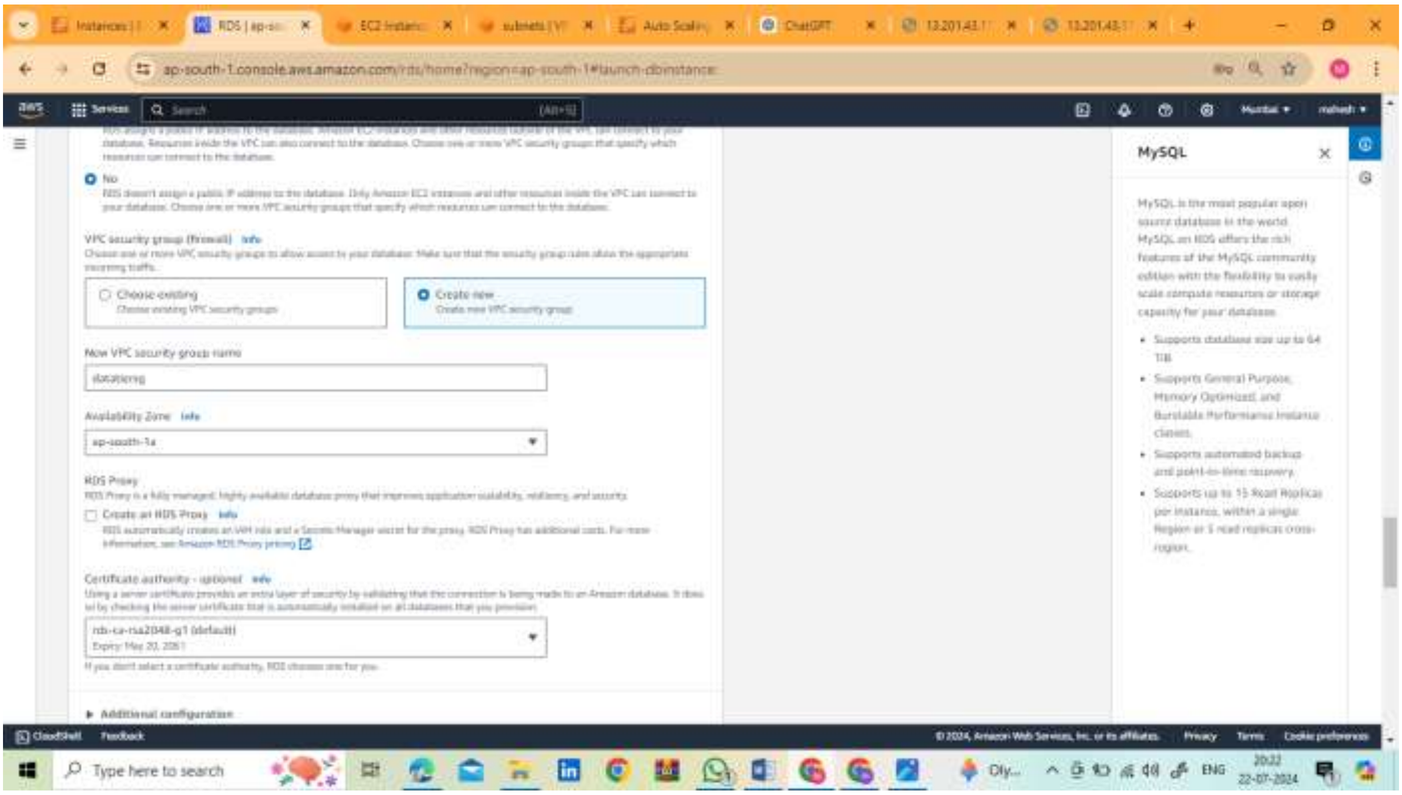
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

databasetiersubnetgroup
2 Subnets, 2 Availability Zones

Public access Info

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

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



ap-south-1.console.aws.amazon.com/rds/home?region=ap-south-1#launch-dbinstance:

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

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

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

New VPC security group name

datatiersg

Availability Zone Info

ap-south-1a

RDS Proxy

RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.

□ Create an RDS Proxy Info
RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see Amazon RDS Proxy pricing

Certificate authority - optional Info

Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-rsa2048-g1 (default)
Expiry: May 20, 2061

If you don't select a certificate authority, RDS chooses one for you.

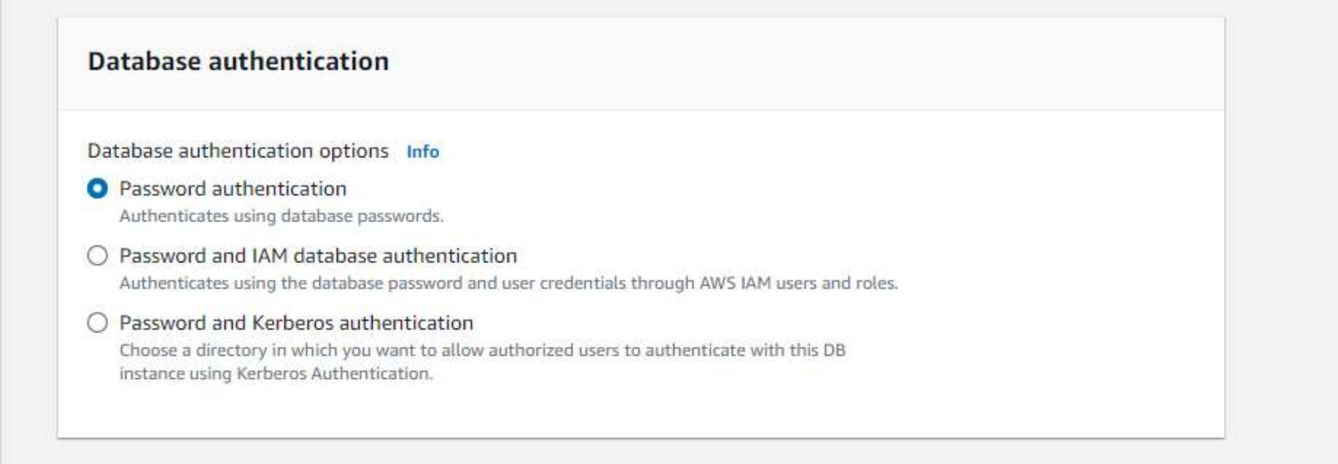
▸ Additional configuration

MySQL

MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

In 'Database authentication,' I left the default option checked.



Database authentication

Database authentication options Info

● Password authentication
Authenticates using database passwords.

○ Password and IAM database authentication
Authenticates using the database password and user credentials through AWS IAM users and roles.

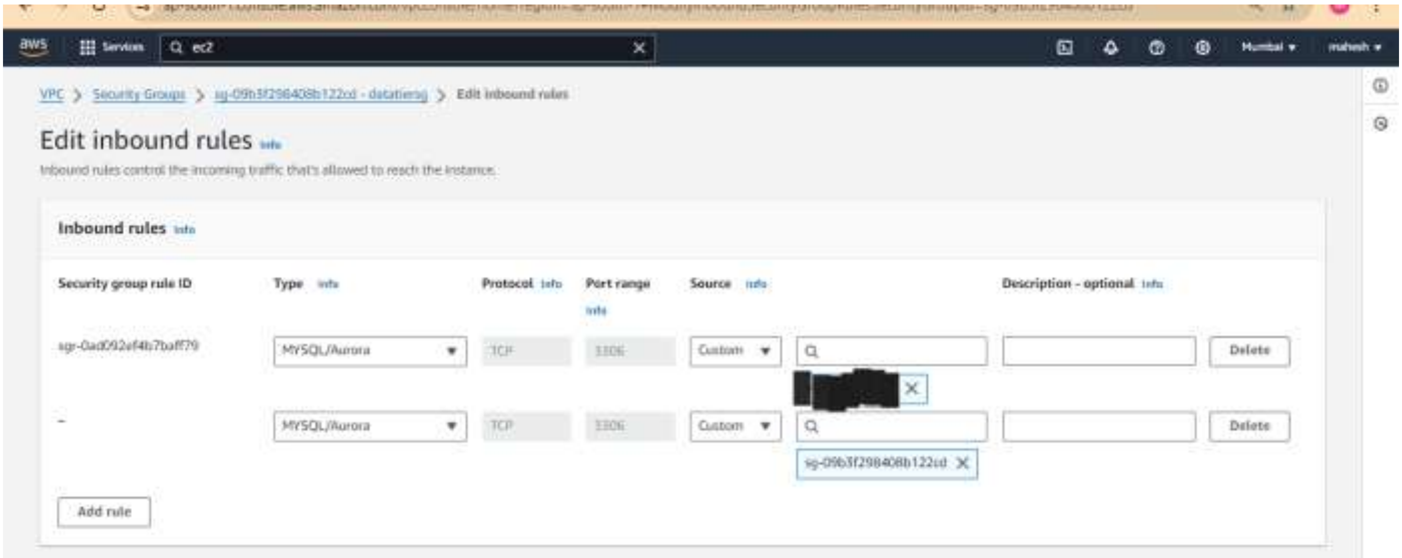
○ Password and Kerberos authentication
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

Click the 'Create database' button.

Update the Database Tier Security Group:

Navigate to the VPC console, select 'Security groups' from the left-side menu, and then find the database tier security group you just created. Select the security group you just created. You need to edit the inbound rules; by default, the database SG has an inbound rule to allow MySQL/Aurora traffic on port 3306 from your IP address. Delete this rule.

Create a new rule for MySQL/Aurora on port 3306. For the 'Source,' select 'Custom' and add your security group for your application layer (tier-2 SG).



VPC > Security Groups > sg-09b3f298408b122cd - datatiersg > Edit inbound rules

Edit inbound rules Info

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

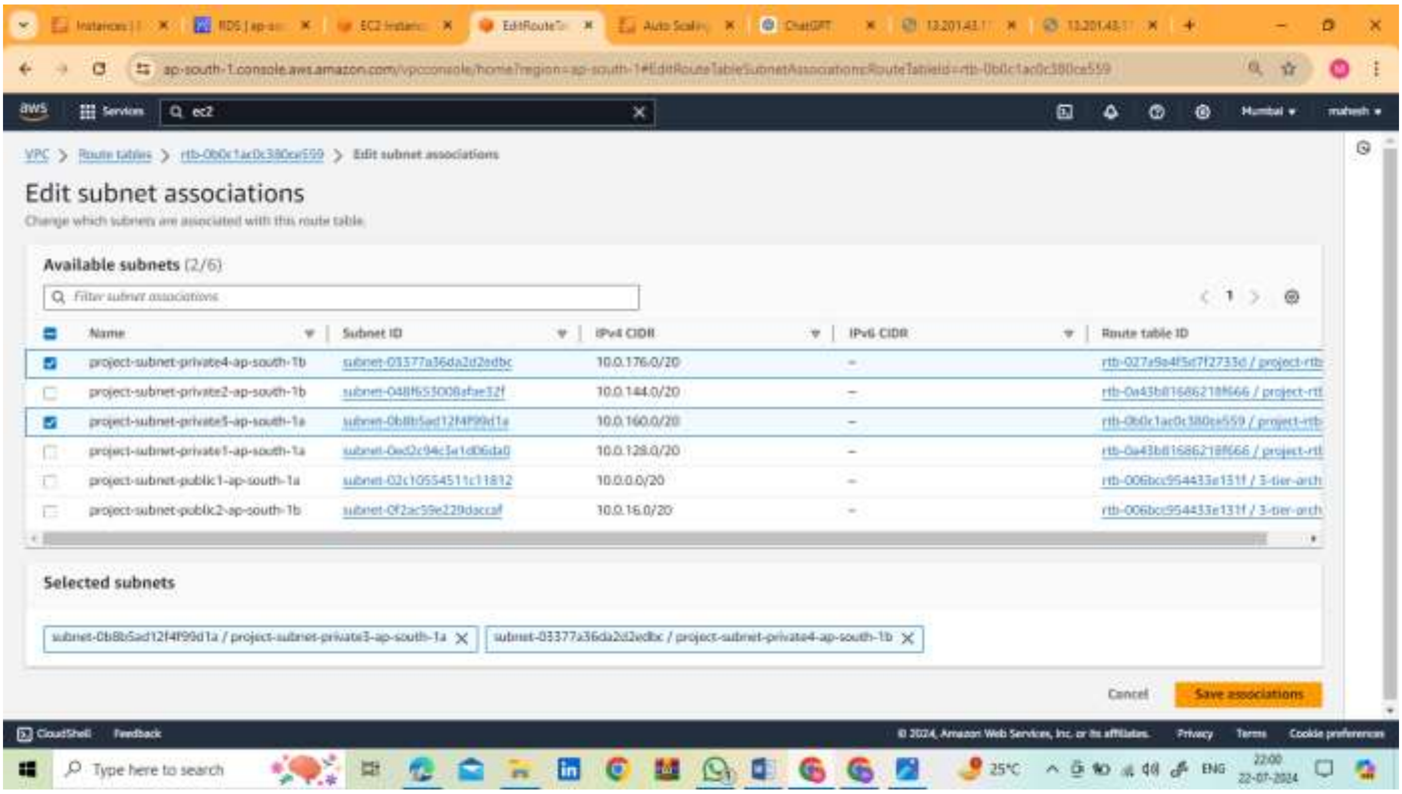
Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-0ad092ef4b7baff79	MYSQL/Aurora ▾	TCP	3306	Custom ▾	[redacted] ✕		Delete
-	MYSQL/Aurora ▾	TCP	3306	Custom ▾	sg-09b3f298408b122cd ✕		Delete

Add rule

UpdateTier3PrivateRouteTables:

In the last step for our database tier, we need to ensure that the route table associated with our database's private subnets lists both subnets in the subnet associations. If not, add the other subnet and save.



VPC > Route tables > rtb-0b0c1ac0c380ce559 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/6)

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	project-subnet-private4-ap-south-1b	subnet-03377a36da2d2edbc	10.0.176.0/20	–	rtb-027a9a4f5d7f2733d / project-rtb
□	project-subnet-private2-ap-south-1b	subnet-048f653008afae32f	10.0.144.0/20	–	rtb-0a43b81686218f666 / project-rtl
☑	project-subnet-private3-ap-south-1a	subnet-0b8b5ad12f4f99d1a	10.0.160.0/20	–	rtb-0b0c1ac0c380ce559 / project-rtb
□	project-subnet-private1-ap-south-1a	subnet-0ed2c94c3e1d06da0	10.0.128.0/20	–	rtb-0a43b81686218f666 / project-rtl
□	project-subnet-public1-ap-south-1a	subnet-02c10554511c11812	10.0.0.0/20	–	rtb-006bcc954433e131f / 3-tier-arch
□	project-subnet-public2-ap-south-1b	subnet-0f2ac59e229daccaf	10.0.16.0/20	–	rtb-006bcc954433e131f / 3-tier-arch

Selected subnets

subnet-0b8b5ad12f4f99d1a / project-subnet-private3-ap-south-1a ✕ subnet-03377a36da2d2edbc / project-subnet-private4-ap-south-1b ✕

Our three-tier architecture is complete! We have already tested our web and application layers, but we are going to go a step further here.

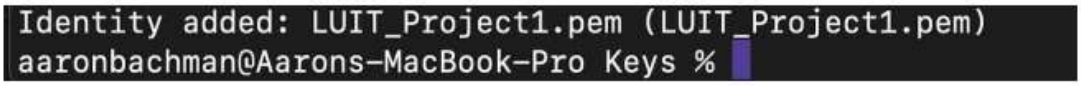
Part5: Testing

We can’t directly SSH to the database, but we can use an SSH forwarding agent to achieve this. You need to add your access key pair file to your keychain. To do this, first make sure you are on your local host (use the command `exit` to get out of any EC2 instance you’re connected to). Then use the following command:

~~~bash

ssh-add -K <keypair.pem>

```"
~~~

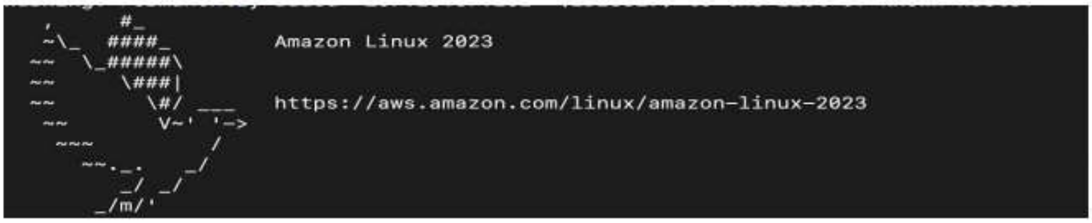


```
Identity added: LUIT_Project1.pem (LUIT_Project1.pem)
aaronbachman@Aarons-MacBook-Pro Keys %
```

Now that your key pair file is added to your keychain, the SSH agent willscanthroughallofthekeysassociatedwiththekeychainandfind your matching key.

NowreconnecttothewebtierEC2;however,thistimeuse -Atospecify you want to use the SSH agent.

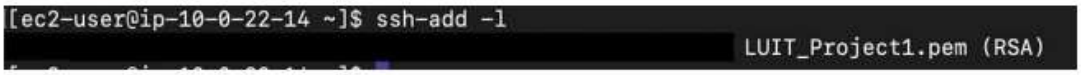
ssh-Aec2-user@<public-ip-address>



```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
```

Onceyouareloggedbackintoyourtier-1EC2,usethefollowing command to check if the SSH agent forwarded the private key.

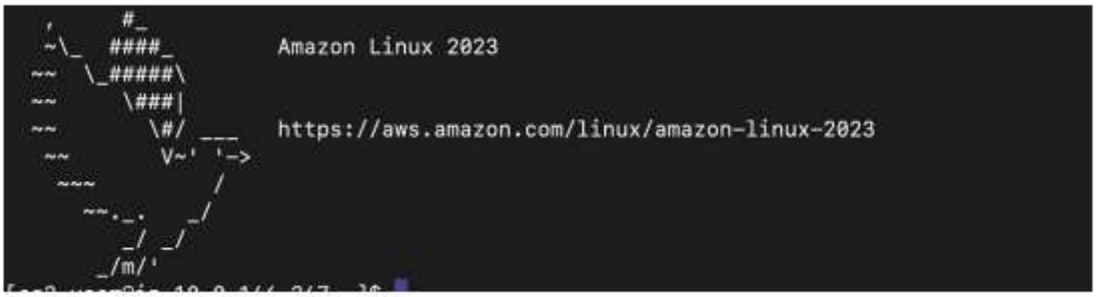
ssh-add-l



```
[ec2-user@ip-10-0-22-14 ~]$ ssh-add -l
[redacted] LUIT_Project1.pem (RSA)
```

Ourkeypairhasbeenforwardedtoourpublicinstance.Gocopyyour tier-2 application layer private IP address and copy it into the next command.

ssh-Aec2-user@<private-ip-address>



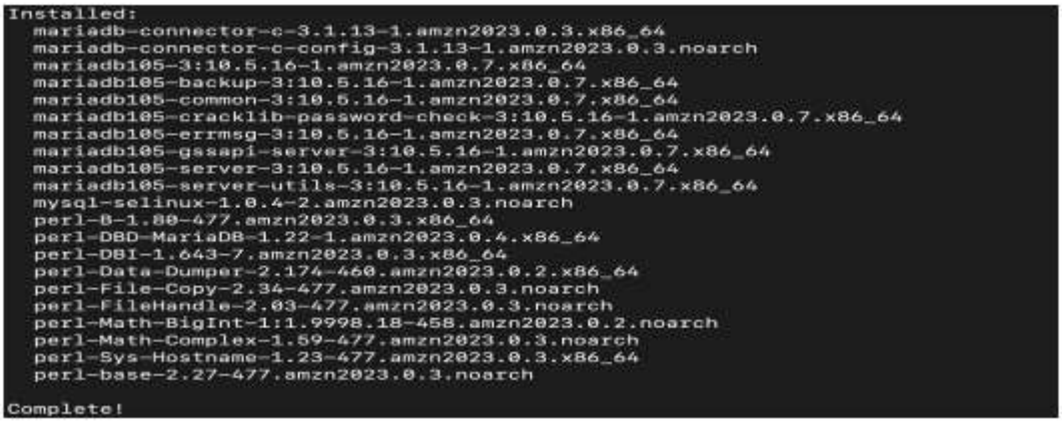
```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
```

WehavenowSSH’edfromyourpublictier1webinstanceintoyour private tier 2 application instance!

TestingConnectivity tothe Database Tier

ThereareafewwaysyoucanconnecttoyourRDS databasefromyour application tier. One way is to install MySQL on your private tier 2 instance to access your database. We are going to utilize this method. Whileloggedintoyourapplicationtierinstance,usethiscommand:

sudodnfinstallmariadb105-server

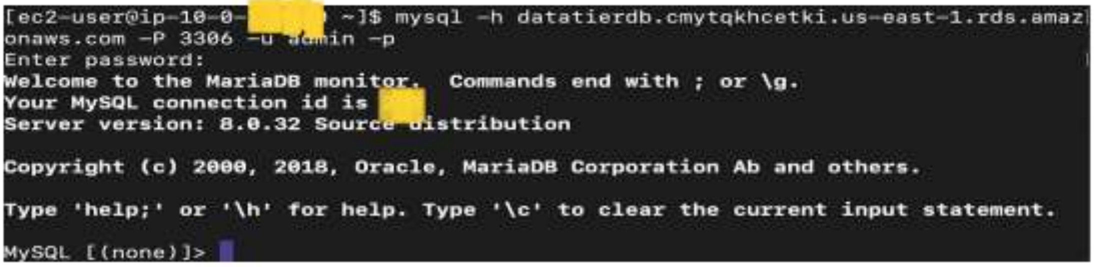


```
Installed:
  mariadb-connector-c-3.1.13-1.amzn2023.0.3.x86_64
  mariadb-connector-c-config-3.1.13-1.amzn2023.0.3.noarch
  mariadb105-3:10.5.16-1.amzn2023.0.7.x86_64
  mariadb105-backup-3:10.5.16-1.amzn2023.0.7.x86_64
  mariadb105-common-3:10.5.16-1.amzn2023.0.7.x86_64
  mariadb105-cracklib-password-check-3:10.5.16-1.amzn2023.0.7.x86_64
  mariadb105-errmsg-3:10.5.16-1.amzn2023.0.7.x86_64
  mariadb105-gssapi-server-3:10.5.16-1.amzn2023.0.7.x86_64
  mariadb105-server-3:10.5.16-1.amzn2023.0.7.x86_64
  mariadb105-server-utils-3:10.5.16-1.amzn2023.0.7.x86_64
  mysql-selinux-1.0.4-2.amzn2023.0.3.noarch
  perl-B-1.80-477.amzn2023.0.3.x86_64
  perl-DBD-MariaDB-1.22-1.amzn2023.0.4.x86_64
  perl-DBI-1.643-7.amzn2023.0.3.x86_64
  perl-Data-Dumper-2.174-460.amzn2023.0.2.x86_64
  perl-File-Copy-2.34-477.amzn2023.0.3.noarch
  perl-FileHandle-2.03-477.amzn2023.0.3.noarch
  perl-Math-BigInt-1:1.9998.18-458.amzn2023.0.2.noarch
  perl-Math-Complex-1.59-477.amzn2023.0.3.noarch
  perl-Sys-Hostname-1.23-477.amzn2023.0.3.x86_64
  perl-base-2.27-477.amzn2023.0.3.noarch

Complete!
```

This command installs the MariDB package, which is used to read MySQL. Once installed, you should be able to use the following commandtologintoyourRDSMySQLdatabase.Youwillneedyour RDS endpoint, user name, and password. To find your RDS database endpoint, navigate to the database you created and find the endpoint under Connectivity & Security.

mysql-h<rds-database-endpoint>-P3306-u<username>-p



```
[ec2-user@ip-10-0-[redacted] ~]$ mysql -h datatierdb.cmytqkhcetki.us-east-1.rds.amaz
onaws.com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is [redacted]
Server version: 8.0.32 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

WehavenowsuccessfullyconnectedtoourMySQLdatabasefromthe application tier. We have connectivity with all of our tiers!