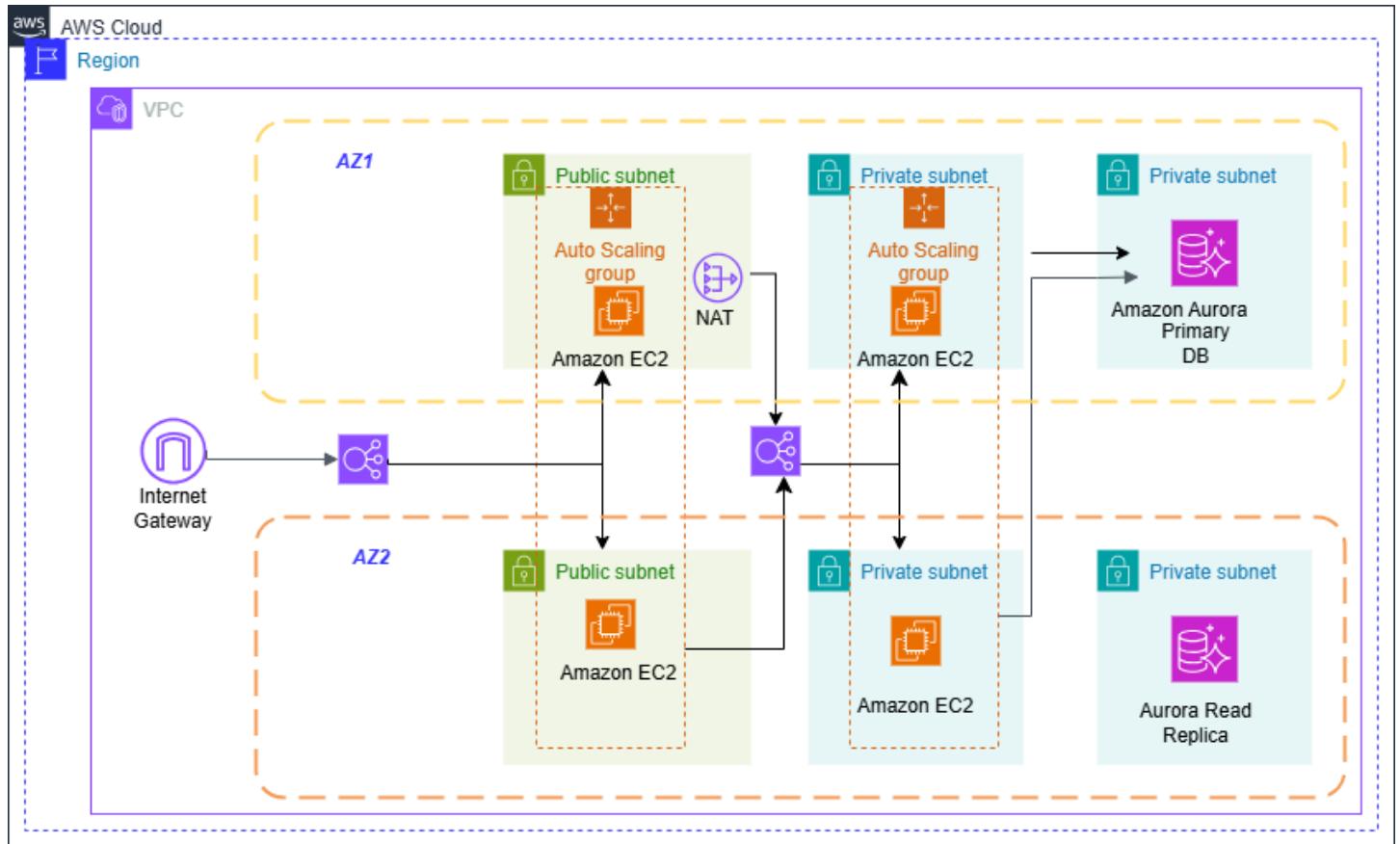


AWS 3 Tier Architecture Project

-Sadia Anjum



1. VPC Creation

Create VPC

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create

Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

Name tag auto-generation

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

Auto-generate

my-vpc-demo

IPv4 CIDR block

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

192.168.0.0/22

1,024 IPs

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

IPv6 CIDR block

No IPv6 CIDR block

Amazon-provided IPv6 CIDR block

Tenancy

Preview

VPC

Show details
Your AWS virtual network

my-vpc-demo-vpc

Subnets (4)

Subnets within this VPC

ap-south-1a

my-vpc-demo-subnet-public1-ap-
 my-vpc-demo-subnet-private1-ap-

ap-south-1b

my-vpc-demo-subnet-public2-ap-
 my-vpc-demo-subnet-private2-ap-

Route tables (3)

Route network traffic to resources

my-vpc-demo-rtb-public
my-vpc-demo-rtb-privat
my-vpc-demo-rtb-privat

Number of private subnets

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

NAT gateways (\$)

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

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**

DNS options

- Enable DNS hostnames
- Enable DNS resolution

Additional tags

[Cancel](#) [Previous page](#) [Create VPC](#)

Create VPC workflow

Success

Details

- Create VPC: vpc-0e90e1fdbe03e7211 [View](#)
- Enable DNS hostnames
- Enable DNS resolution
- Verifying VPC creation: vpc-0e90e1fdbe03e7211 [View](#)
- Create subnet: subnet-078b3a692df77cfb1 [View](#)
- Create subnet: subnet-0ba400668a413dd33 [View](#)
- Create subnet: subnet-0093645f2e11e4df5 [View](#)
- Create subnet: subnet-00c3c1067eca4d099 [View](#)
- Create subnet: subnet-0e12181446954d9d1 [View](#)
- Create subnet: subnet-0ba6bcfa110e7920 [View](#)
- Create internet gateway: igw-039938d346e692eb7 [View](#)
- Attach internet gateway to the VPC
- Create route table: rtb-0de4b4d5cc24c8197 [View](#)
- Create route
- Associate route table
- Associate route table
- Allocate elastic IP: eipalloc-0e7f66b329fffb8c7 [View](#)
- Create NAT gateway: nat-03c18014f831f9b32 [View](#)
- Wait for NAT Gateways to activate
- Create route table: rtb-05e3c07542970ac6f [View](#)

Subnets (1/9) Info

Last updated less than a minute ago Actions Create subnet

Name	Subnet ID	State	VPC	Block Pt
-	subnet-029758e935e005f2f	Available	vpc-0e26cdceb3a5dde7e	Off
-	subnet-0ce81aed3355bbc12	Available	vpc-0e26cdceb3a5dde7e	Off
demo-vpc-app1	subnet-0093645f2e11e4df5	Available	vpc-0e90e1fdb03e7211 my...	Off
demo-vpc-db1	subnet-0e12181446954d9d1	Available	vpc-0e90e1fdb03e7211 my...	Off
-	subnet-0dd02f6041275864a	Available	vpc-0e26cdceb3a5dde7e	Off
demo-vpc-web1	subnet-078b3a692df77cfb1	Available	vpc-0e90e1fdb03e7211 my...	Off
demo-vpc-db2	subnet-0ba6bcfe110e7920	Available	vpc-0e90e1fdb03e7211 my...	Off
demo-vpc-app2	subnet-00c3c1067eca4d099	Available	vpc-0e90e1fdb03e7211 my...	Off
demo-vpc-web2	subnet-0ba400668a413dd33	Available	vpc-0e90e1fdb03e7211 my...	Off

[VPC](#) > [Security Groups](#) > Create security group



Create security group Info

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

Basic details

Security group name Info

web-ALB-SG

Name cannot be edited after creation.

Description Info

web-ALB-SG

VPC Info

vpc-0e90e1fdb03e7211 (my-vpc-demo)

Inbound rules Info

Type Info

HTTP

Protocol Info

TCP

Port range Info

80

Source Info

Anyw...

Description - optional Info

0.0.0.0/0

Delete

sg-0a8725cd50c1285d1 - web-ALB-SG

Actions

Details

Security group name

web-ALB-SG

Security group ID

sg-0a8725cd50c1285d1

Description

web-ALB-SG

VPC ID

vpc-0e90e1fdb03e7211

Owner

183295428288

Inbound rules count

1 Permission entry

Outbound rules count

1 Permission entry

[Inbound rules](#)

[Outbound rules](#)

[Sharing - new](#)

[VPC associations - new](#)

[Tags](#)

Inbound rules (1)

Search

Manage tags

Edit inbound rules

< 1 >



Name

Security group rule ID

IP version

Type

Protocol

Port range

-

sgr-01db821fd02f9f1f2

IPv4

HTTP

TCP

80

Create security group Info

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

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

Inbound rules Info**Type Info****Protocol Info****Port range Info****Source Info****Description - optional Info****Delete**

Add rule**Inbound rules Info****Type Info****Protocol Info****Port range Info****Source Info****Description - optional Info****Delete**

Add rule**Success message:** Security group (sg-0c410ba5f6a30aa43 | web-tier-SG) was created successfully**Details****X****sg-0c410ba5f6a30aa43 - web-tier-SG****Actions ▾****Details****Security group name**
Security group ID
Description
VPC ID
Owner
Inbound rules count
2 Permission entries**Outbound rules count**
1 Permission entry**Inbound rules****Outbound rules****Sharing - new****VPC associations - new****Tags****Inbound rules (2)****C****Manage tags****Edit inbound rules****< 1 >****⚙**

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-03a8ed0f14f55676e	-	HTTP	TCP	80
<input type="checkbox"/>	-	sgr-0caab12aed065f4d9	IPv4	HTTP	TCP	80

Create security group Info

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

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

Inbound rules Info

This security group has no inbound rules.

[Add rule](#)

Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>	Delete
Custom TCP	TCP	4000	Custom	<input type="text" value="192.168.0.0/22"/> <input type="button" value="X"/>	<input type="button" value="Delete"/>
				<input type="text" value="192.168.0.0/22"/> <input type="button" value="X"/>	

[Add rule](#)

⌚ Security group (sg-008d4744eb544b6ce | App-SG) was created successfully

[▶ Details](#)

sg-008d4744eb544b6ce - App-SG

[Actions ▾](#)

Details

Security group name	<input type="text" value="App-SG"/> sg-008d4744eb544b6ce	Description	<input type="text" value="App-SG"/> vpc-0e90e1fdbbe03e7211
Owner	<input type="text" value="183295428288"/>	Inbound rules count	1 Permission entry

[Inbound rules](#)[Outbound rules](#)[Sharing - new](#)[VPC associations - new](#)[Tags](#)

Inbound rules (1)

Inbound rules (1)							Manage tags	Edit inbound rules		
<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	<	1	>	
<input type="checkbox"/>	-	sgr-093a76c5132a18000	IPv4	Custom TCP	TCP	4000				

VPC > Security Groups > Create security group

Create security group Info

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

Basic details

Security group name Info
Internal-ALB-SG
Name cannot be edited after creation.

Description Info
Internal-ALB-SG

VPC Info
vpc-0e90e1fdbbe03e7211 (my-vpc-demo)

Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
HTTP	TCP	80	Custom	192.168.0.0/22
				192.168.0.0/22

[Add rule](#)

✓ Security group (sg-00410f66d611ec665 | Internal-ALB-SG) was created successfully
[Details](#)

sg-00410f66d611ec665 - Internal-ALB-SG

[Actions ▾](#)

Details

Security group name Internal-ALB-SG	Security group ID sg-00410f66d611ec665	Description Internal-ALB-SG	VPC ID vpc-0e90e1fdbbe03e7211
Owner 183295428288	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

Inbound rules (1)

Manage tags		Edit inbound rules	
Name	Security group rule ID	IP version	Type
-	sgr-02bee8ed20d0051f6	IPv4	HTTP

VPC > Security Groups > Create security group

Create security group Info

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

Basic details

Security group name Info
RDS-SG
Name cannot be edited after creation.

Description Info
RDS-SG

VPC Info
vpc-0e90e1fdbbe03e7211 (my-vpc-demo)

Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
MySQL/Aurora	TCP	3306	Custom	192.168.0.0/22

[Add rule](#)

✓ Security group (sg-0b6404774772159d5 | RDS-SG) was created successfully
▶ Details

sg-0b6404774772159d5 - RDS-SG

Actions ▾

Details

Security group name	sg-0b6404774772159d5	Description	VPC ID
Owner	183295428288	1 Permission entry	vpc-0e90e1fdbbe03e7211
Inbound rules count	1 Permission entry	Outbound rules count	1 Permission entry

Inbound rules Outbound rules Sharing - new VPC associations - new Tags

Inbound rules (1)

Manage tags Edit inbound rules

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-05fc730d71569b132	IPv4	MYSQL/Aurora	TCP	3306

✓ Security group (sg-0b6404774772159d5 | RDS-SG) was created successfully
▶ Details

Security Groups (7) Info

Actions ▾

Export security groups to CSV

Create security group

<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description
<input type="checkbox"/>	-	sg-0e4c0b77d749b484e	default	vpc-0e90e1fdbbe03e7211	default VPC secu
<input type="checkbox"/>	-	sg-0c410ba5f6a30aa43	web-tier-SG	vpc-0e90e1fdbbe03e7211	web-tier-SG
<input type="checkbox"/>	-	sg-008d4744eb544b6ce	App-SG	vpc-0e90e1fdbbe03e7211	App-SG
<input type="checkbox"/>	-	sg-0b6404774772159d5	RDS-SG	vpc-0e90e1fdbbe03e7211	RDS-SG
<input type="checkbox"/>	-	sg-0db96cde0262d1d49	default	vpc-0e26cdceb3a5dde7e	default VPC secu
<input type="checkbox"/>	-	sg-00410f66d611ec665	Internal-ALB-SG	vpc-0e90e1fdbbe03e7211	Internal-ALB-SG
<input type="checkbox"/>	-	sg-0a8725cd50c1285d1	web-ALB-SG	vpc-0e90e1fdbbe03e7211	web-ALB-SG

Successfully created Security Groups for all Tiers.

2. S3 Bucket and IAM Role Setup

- Create an S3 bucket and upload the application code.
- Set up an IAM role with the necessary permissions and attach it to the EC2 instance.

aws Search [Alt+S] Asia Pacific (Mumbai) Anoora @ sadiaws

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region: Asia Pacific (Mumbai) ap-south-1

Bucket type: General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name: Info

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)

Format: s3://bucket/prefix

aws Search [Alt+S] Asia Pacific (Mumbai) Anoora @ sadiaws

Amazon S3 > Buckets > Create bucket

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

Object Ownership: ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership: Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

aws Search [Alt+S] Asia Pacific (Mumbai) Anoora @ sadiaws

Amazon S3 > Buckets > Create bucket

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning: Disable

Enable

Tags - optional (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

[Add tag](#)

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type: Server-side encryption with Amazon S3 managed keys (SSE-S3)

Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

Amazon S3 > Buckets

Successfully created bucket "demo-3-project"
To upload files and folders, or to configure additional bucket settings, choose View details.

Account snapshot - updated every 24 hours All AWS Regions

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

[View Storage Lens dashboard](#)

General purpose buckets | Directory buckets

General purpose buckets (1) [Info](#) All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
demo-3-project	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	May 6, 2025, 15:17:48 (UTC+05:30)

[Copy ARN](#) | [Empty](#) | [Delete](#) | [Create bucket](#)

Upload succeeded
For more information, see the [Files and folders](#) table.

Files and folders (33 total, 192.9 KB)

Name	Folder	Type	Size	Status	Error
Burger.styled.js	application-code/web-tier/sr...	text/javascript	940.0 B	Succeeded	-
index.js	application-code/web-tier/sr...	text/javascript	35.0 B	Succeeded	-
DatabaseDemo.css	application-code/web-tier/sr...	text/css	655.0 B	Succeeded	-
DatabaseDemo.js	application-code/web-tier/sr...	text/javascript	4.0 KB	Succeeded	-
Home.js	application-code/web-tier/sr...	text/javascript	451.0 B	Succeeded	-
index.js	application-code/web-tier/sr...	text/javascript	35.0 B	Succeeded	-
Menu.js	application-code/web-tier/sr...	text/javascript	1.0 KB	Succeeded	-
Menu.styled.js	application-code/web-tier/sr...	text/javascript	934.0 B	Succeeded	-
nginx-Without-SSL.conf	application-code/	-	1.6 KB	Succeeded	-
nginx.conf	application-code/	-	1.6 KB	Succeeded	-

aws | Search [Alt+S] | Global ▾ | Anoora @ sadiaws ▾

IAM > Roles > Create role

Step 1 **Select trusted entity**

- Select trusted entity
- Step 2
- Add permissions
- Step 3
- Name, review, and create

Select trusted entity [Info](#)

Trusted entity type

- AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- Custom trust policy Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

[Choose a service or use case](#)

[Cancel](#) | [Next](#)

IAM > Roles > Create role

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

- EC2**
Allows EC2 Instances to call AWS services on your behalf.
- EC2 Role for AWS Systems Manager**
Allows EC2 Instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- EC2 Spot Fleet Role**
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
- EC2 - Spot Fleet Auto Scaling**
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
- EC2 - Spot Fleet Tagging**
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
- EC2 - Spot Instances**
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
- EC2 - Spot Fleet**
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
- EC2 - Scheduled Instances**
Allows EC2 Scheduled Instances to manage instances on your behalf.

Cancel **Next**

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Add permissions Info

Permissions policies (1/1045) Info

Choose one or more policies to attach to your new role.

Filter by Type

Policy name	Type	Description
<input type="checkbox"/> AmazonEC2RoleforAWSCodeDeploy	AWS managed	Provides EC2 access to S3 bucket to do...
<input type="checkbox"/> AmazonEC2RoleforAWSCodeDeployLimited	AWS managed	Provides EC2 limited access to S3 buck...
<input type="checkbox"/> AmazonEC2RoleforDataPipelineRole	AWS managed	Default policy for the Amazon EC2 Rol...
<input checked="" type="checkbox"/> AmazonEC2RoleforSSM	AWS managed	This policy will soon be deprecated. Pl...
<input type="checkbox"/> AmazonEC2RolePolicyForLaunchWizard	AWS managed	Managed policy for the Amazon Launc...

Set permissions boundary - optional

Cancel **Previous** **Next**

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+', '=', '@', '-' characters.

Description
Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+-.@/\[{\}]#\$%^&`~`^`

Step 1: Select trusted entities Edit

Trust policy

```

1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Principal": "*"
7          }
8      ]
9  }

```

Step 2: Add permissions

Permissions policy summary

Policy name [AmazonEC2RoleforSSM](#)

Type

Attached as

AWS managed

Permissions policy

[Edit](#)

Step 3: Add tags

Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#)

[Previous](#)

[Create role](#)

⌚ Role demo-ec2-role-3 created.

[View role](#)

X

Roles (7) [Info](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

C

[Delete](#)

[Create role](#)

3. Database Configuration

Aurora and RDS > Subnet groups

Subnet groups (0)

No db subnet groups
You don't have any db subnet groups.

[Create DB subnet group](#)

Dashboard
Databases
Query editor
Performance insights
Snapshots
Exports in Amazon S3
Automated backups
Reserved instances
Proxies

Subnet groups
Parameter groups
Option groups
Custom engine versions
Zero-ETL integrations [New](#)

Events
Event subscriptions

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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.

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description

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.

my-vpc-demo (vpc-0e90e1fdbbe03e7211)

6 Subnets, 2 Availability Zones

Add subnets

Aurora and RDS > Subnet groups > Create DB subnet group

Add subnets

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

Choose an availability zone

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

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

Select subnets

demo-vpc-db1 Subnet ID: subnet-0e12181446954d9d1 CIDR: 192.168.2.128/26 X demo-vpc-db2 Subnet ID: subnet-0ba6bcafe110e7920 CIDR: 192.168.2.192/26 X

For Multi-AZ DB clusters, you must select 3 subnets in 3 different Availability Zones.

Subnets selected (2)

Availability zone	Subnet name	Subnet ID	CIDR block
ap-south-1a	demo-vpc-db1	subnet-0e12181446954d9d1	192.168.2.128/26
ap-south-1b	demo-vpc-db2	subnet-0ba6bcafe110e7920	192.168.2.192/26

Create

Aurora and RDS > Subnet groups

Subnet groups (1)

Successfully created DB-GRP. View subnet group

Name	Description	Status	VPC
db-grp	DB-GRP	Complete	vpc-0e90e1fdbbe03e7211

Create DB subnet group

Aurora and RDS > Create database

Create database Info

Choose a database creation method

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

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

Engine options

Engine type Info

Aurora (MySQL Compatible) 

Aurora (PostgreSQL Compatible) 

MySQL 

PostgreSQL 

MariaDB

Oracle

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Aurora and RDS > Create database

IBM Db2

Microsoft SQL Server

Edition

MySQL Community

Engine version Info

View the engine versions that support the following database features.

Hide filters

Show only versions that support the Multi-AZ DB cluster Info
Create 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 only 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.

Choosing engine versions

When you choose Aurora PostgreSQL, the global database feature is enabled for specific engine versions.

Global database

You can expand your Aurora database to span multiple AWS regions by adding a Region to the DB cluster. Writes in the primary AWS Region are replicated with typical latency of less than 1 sec to secondary AWS Regions.

Learn more 

[Adding an AWS Region to an Aurora Global Database](#)

Aurora and RDS > Create database

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

Availability and durability

Deployment options Info

Choose the deployment option that provides the availability and durability needed for your use case. AWS is committed to a certain level of uptime depending on the deployment option you choose. Learn more in the [Amazon RDS service level agreement \(SLA\)](#).

Multi-AZ DB cluster deployment (3 instances)
Creates a primary DB instance with two readable standbys in separate Availability Zones. This setup provides:

- 99.95% uptime
- Redundancy across Availability Zones
- Increased read capacity
- Reduced write latency

Multi-AZ DB instance deployment (2 instances)
Creates a primary DB instance with a non-readable standby instance in a separate Availability Zone. This setup provides:

- 99.95% uptime
- Redundancy across Availability Zones

Single-AZ DB instance deployment (1 instance)
Creates a single DB instance without standby instances. This setup provides:

- 99.95% uptime
- No data redundancy

Write/read endpoint Reader endpoints Write/read endpoint Standby (no endpoint) Write/read endpoint

Choosing engine versions

When you choose Aurora PostgreSQL, the global database feature is enabled for specific engine versions.

Global database

You can expand your Aurora database to span multiple AWS regions by adding a Region to the DB cluster. Writes in the primary AWS Region are replicated with typical latency of less than 1 sec to secondary AWS Regions.

Learn more 

[Adding an AWS Region to an Aurora Global Database](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



Credentials Settings

Master username [Info](#)

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

1 to 16 alphanumeric characters. The first character must be a letter.

Credentials management

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

Managed in AWS Secrets Manager - most secure

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

Self managed

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

Auto generate password

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

Master password [Info](#)

Password strength Very strong

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

Confirm master password [Info](#)

Choosing engine versions

When you choose Aurora PostgreSQL, the global database feature is enabled for specific engine versions.

Global database

You can expand your Aurora database to span multiple AWS regions by adding a Region to the DB cluster. Writes in the primary AWS Region are replicated with typical latency of less than 1 second to secondary AWS Regions.

[Learn more](#)

[Adding an AWS Region to an Aurora Global Database](#)

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

Allocated storage value must be 20 GiB to 6,144 GiB

Additional storage configuration

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.

Network type [Info](#)

To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

IPv4

Your resources can communicate only over the IPv4 addressing protocol.

Dual-stack mode

Your resources can communicate over IPv4, IPv6, or both.

Virtual private cloud (VPC) [Info](#)

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

my-vpc-demo (vpc-0e90efdbbe03e7211)

▼

6 Subnets, 2 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

i 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.

db-grp

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.

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

Choosing engine versions

When you choose Aurora PostgreSQL, the global database feature is enabled for specific engine versions.

Global database

You can expand your Aurora database to span multiple AWS regions by adding a Region to the DB cluster. Writes in the primary AWS Region are replicated with typical latency of less than 1 second to secondary AWS Regions.

[Learn more](#)

[Adding an AWS Region to an Aurora Global Database](#)

Aurora and RDS > Create 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

Existing VPC security groups
Choose one or more options ▾

RDS-SG [X](#)

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)
Expiration: May 20, 2061

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

[Additional configuration](#)

Choosing engine versions >

When you choose Aurora PostgreSQL, the global database feature is enabled for specific engine versions.

Global database

You can expand your Aurora database to span multiple AWS regions by adding a Region to the DB cluster. Writes in the primary AWS Region are replicated with typical latency of less than 1 sec to secondary AWS Regions.

Learn more [X](#)

Adding an AWS Region to an Aurora Global Database

Creating database database-1 [View credential details](#) X

Your database might take a few minutes to launch. You can use settings from database-1 to simplify configuration of suggested database add-ons while we finish creating your DB for you.

Databases (1)

[Filter by databases](#) ▶ 1 ▶ [⚙️](#)

[Group resources](#) [C](#) [Modify](#) [Actions](#) ▾ [Create database](#) ▾

DB identifier	Status	Role	Engine	Region ...	Size	Recommendations
database-1	Creating	Instance	MySQL Co...	ap-south-1a	db.t4g.micro	

> database-1

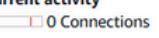
Successfully created database database-1 [View connection details](#) X

You can use settings from database-1 to simplify configuration of suggested database add-ons while we finish creating your DB for you.

database-1

[C](#) [Modify](#) [Actions](#) ▾

Summary

DB identifier database-1	Status Available	Role Instance	Engine MySQL Community	Recommendations
CPU  5.75%	Class db.t4g.micro	Current activity  0 Connections	Region & AZ ap-south-1a	

[Connectivity & security](#) [Monitoring](#) [Logs & events](#) [Configuration](#) [Zero-ETL integrations](#) [Maintenance & backups](#) [Data](#)

Connectivity & security

[Endpoint & port](#) [Networking](#) [Security](#)

4. Application Tier Setup

Deploy application-tier resources, including the configuration of an internal load balancer for traffic distribution within the tier.

5. Web Tier Setup

Provision web-tier resources and set up an external load balancer to manage incoming traffic from users.

The screenshot shows the 'Launch an instance' wizard on the AWS EC2 console. The current step is 'Name and tags'. A 'Name' field contains 'ApptierInstance'. Below it is a 'Software Image (AMI)' section with 'Amazon Linux' selected. A 'Virtual server type (instance type)' dropdown shows 't2.micro'. Under 'Storage (volumes)', there is one volume of 8 GiB. On the right, a summary panel shows 'Number of instances: 1' and a note about free tier usage. Buttons for 'Launch instance' and 'Preview code' are at the bottom.

The screenshot shows the 'Launch an instance' wizard on the AWS EC2 console. The current step is 'Application and OS Images (Amazon Machine Image)'. It lists various AMI categories like Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian. A search bar and a 'Browse more AMIs' link are present. Below this is a detailed view of the 'Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type' AMI, including its ID, publish date, and provider information. On the right, the summary panel shows 'Number of instances: 1' and a note about free tier usage. Buttons for 'Launch instance' and 'Preview code' are at the bottom.

Key pair (login) [Info](#)
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

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

Network settings [Info](#)
VPC - required [Info](#)
vpc-0e90e1fdb03e7211 (my-vpc-demo)
192.168.0.0/22

Subnet [Info](#)
subnet-0093645f2e11e4df5 demo-vpc-app1
VPC: vpc-0e90e1fdb03e7211 Owner: 183295428288 Availability Zone: ap-south-1a
Zone type: Availability Zone IP addresses available: 59 CIDR: 192.168.2.0/26

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

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.

Summary
Number of instances | [Info](#)
1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI... [read more](#)
ami-03edbe403ec8522ed

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 of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where applicable).

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

Firewall (security groups) [Info](#)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

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

App-SG sg-008d4744eb544b6cc X
VPC: vpc-0e90e1fdb03e7211

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

Advanced network configuration

Configure storage [Info](#)
Advanced
1x 8 GiB gp2 Root volume, Not encrypted

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

[Add new volume](#)

[Click refresh to view backup information](#)

Summary
Number of instances | [Info](#)
1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI... [read more](#)
ami-03edbe403ec8522ed

Virtual server type (instance type)
t2.micro

Firewall (security group)
App-SG

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

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where applicable).

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

Advanced details [Info](#)

Domain join directory [Info](#)
Select [Create new directory](#)

IAM instance profile [Info](#)
demo-ec2-role-3
arn:aws:iam::183295428288:instance-profile/demo-ec2-role-3 [Create new IAM profile](#)

Hostname type [Info](#)
IP name

Instances (1) [Info](#)
Last updated less than a minute ago [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

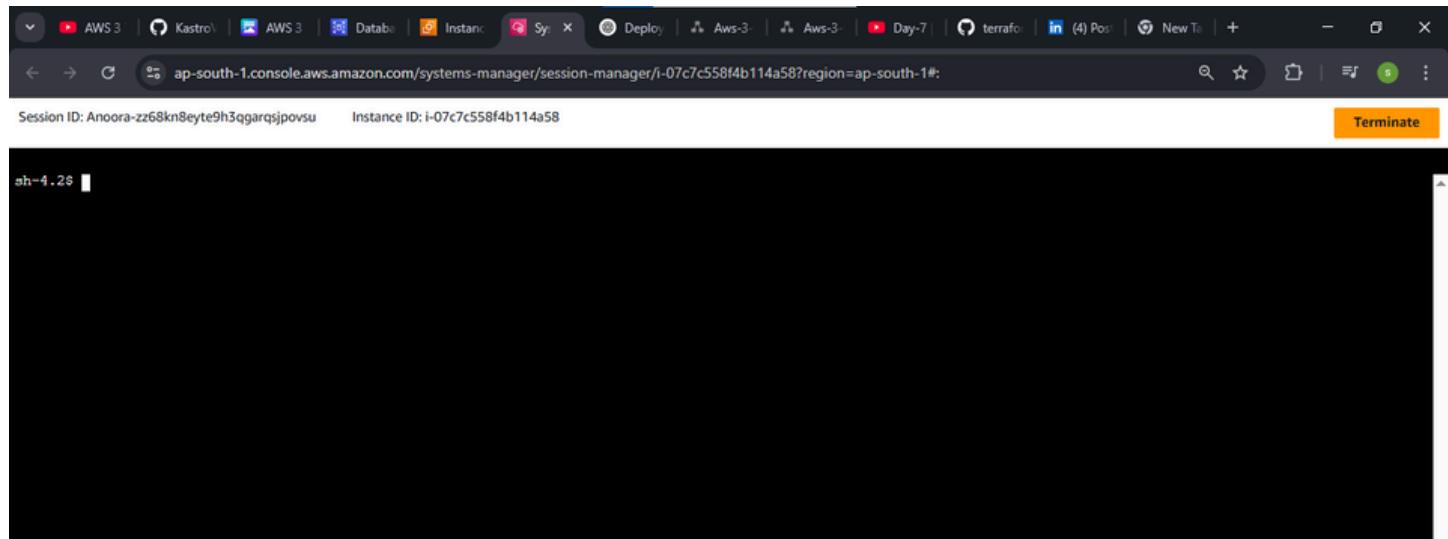
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
ApptierInstance	i-07c7c558f4b114a58	Running	t2.micro	Initializing	View alarms	ap-south-1a	-

pen 'Dbconfig.js' file and change the things accordingly as shown below;

```
module.exports = Object.freeze({  
  
  DB_HOST: 'YOUR-DATABASE-ENDPOINT.ap-south-1.rds.amazonaws.com',  
  
  DB_USER: 'admin',  
  
  DB_PWD: 'Peera146',  
  
  DB_DATABASE: 'webappdb'  
});
```

The reason for having the above info is our App Servers running in Private Subnets should be able to connect to the DB, for that connectivity it is going to use these credentials provided in DbConfig.js file.

Update the above code and upload the Dbconfig.js file in the S3 bucket of 'app-tier' folder.



```
sh-4.2$ sudo su
[root@ip-192-168-2-31 bin]# whoami
root
[root@ip-192-168-2-31 bin]# pwd
/usr/bin
[root@ip-192-168-2-31 bin]# cd..
bash: cd: command not found
[root@ip-192-168-2-31 bin]# cd ..
[root@ip-192-168-2-31 usr]# pwd
/usr
[root@ip-192-168-2-31 usr]# cd /home/ec2-user/
[root@ip-192-168-2-31 ec2-user]# pwd
/home/ec2-user
[root@ip-192-168-2-31 ec2-user]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=3.12 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=2.71 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=2.70 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=2.75 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=2.80 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=116 time=2.77 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=116 time=2.69 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=116 time=2.76 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=116 time=2.74 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=116 time=2.72 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=116 time=2.76 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=116 time=2.72 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=116 time=2.74 ms
^C
--- 8.8.8.8 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12020ms
rtt min/avg/max/mdev = 2.690/2.772/3.120/0.116 ms
[root@ip-192-168-2-31 ec2-user]#
```

In this instance we will do the App Server Setup and DB Server Configuration. Execute the below commands;

Install MySQL

```
sudo yum install mysql -y
```

```
[root@ip-192-168-2-31 ec2-user]# sudo yum install mysql -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Resolving Dependencies
--> Running transaction check
--> Package mariadb.x86_64 1:5.5.68-1.amzn2.0.1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package           Arch      Version            Repository        Size
=====
Installing:
mariadb          x86_64   1:5.5.68-1.amzn2.0.1   amzn2-core       8.8 M

Transaction Summary
=====
Install 1 Package

Total download size: 8.8 M
Installed size: 49 M
Downloading packages:
mariadb-5.5.68-1.amzn2.0.1.x86_64.rpm                                         | 8.8 MB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 1:mariadb-5.5.68-1.amzn2.0.1.x86_64                               1/1
    Verifying : 1:mariadb-5.5.68-1.amzn2.0.1.x86_64                               1/1

Installed:
  mariadb.x86_64 1:5.5.68-1.amzn2.0.1

Complete!
[root@ip-192-168-2-31 ec2-user]# mysql -h database-1.cl0uegueua0f.ap-south-1.rds.amazonaws.com -u admin -p
```

Configure MySQL Database

Connect to the database and perform basic configuration: Replace below info with your DB information

```
mysql -h database-1.cl0uegueua0f.ap-south-1.rds.amazonaws.com -u admin -p
```

Lets create a database. The database name i'm creating is "webappdb" (This is same name that you should give in DvConfig.js file);

```
CREATE DATABASE webappdb;
```

```
SHOW DATABASES;
```

```
USE webappdb; ----> You will see 'Database changed'
```

Execute the below code as a single code. Here we are creating a table with the name 'transactions'

```
CREATE TABLE IF NOT EXISTS transactions(  
    id INT NOT NULL AUTO_INCREMENT,  
    amount DECIMAL(10,2),  
    description VARCHAR(100),  
    PRIMARY KEY(id)  
);
```

To verify whether table got created or not;

```
SHOW TABLES;
```

Lets insert some info into the table

```
INSERT INTO transactions (amount, description) VALUES ('400', 'groceries');
```

To verify whether the entry is really created or not

```
SELECT * FROM transactions;
```

You will see the info you have written

To come out of the DB;

exit (You will see 'ec2-user' at the end of command line and at the beginning of command line you will see 'root')

```
Session ID: Anoora-zz68kn8eyte9h3qgarqsjpo vsu      Instance ID: i-07c7c558f4b114a58          Terminate
1/1

Verifying : 1:mariadb-5.5.68-1.amzn2.0.1.x86_64

Installed:
mariadb.x86_64 1:5.5.68-1.amzn2.0.1

Complete!
[root@ip-192-168-2-31 ec2-user]# mysql -h database-1.cl0uegueua0f.ap-south-1.rds.amazonaws.com -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 28
Server version: 8.0.35 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)]> CREATE DATABASE webappdb;
Query OK, 1 row affected (0.01 sec)

MySQL [(none)]> SHOW DATABASES;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'DATABASE' at line 1
MySQL [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| webappdb |
+-----+
5 rows in set (0.00 sec)

MySQL [(none)]>
```

```
3 rows in set (0.00 sec)

MySQL [(none)]> USE webappdb;
Database changed
MySQL [webappdb]>
```

```
MySQL [(none)]> SHOW DATABASES;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'DATABASE' at line 1
MySQL [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| webappdb |
+-----+
5 rows in set (0.00 sec)

MySQL [(none)]> USE webappdb;
Database changed
MySQL [webappdb]> CREATE TABLE IF NOT EXISTS transactions(
->     id INT NOT NULL AUTO_INCREMENT,
->     amount DECIMAL(10,2),
->     description VARCHAR(100),
->     PRIMARY KEY(id)
-> );
Query OK, 0 rows affected (0.04 sec)

MySQL [webappdb]> SHOW TABLES;
+-----+
| Tables_in_webappdb |
+-----+
| transactions |
+-----+
1 row in set (0.01 sec)

MySQL [webappdb]>
```

Session ID: Anoora-zz68kn8eyte9h3qgarqsjpoisu Instance ID: i-07c7c558f4b114a58

Terminate

```
| sys          |
| webappdb    |
+-----+
5 rows in set (0.00 sec)

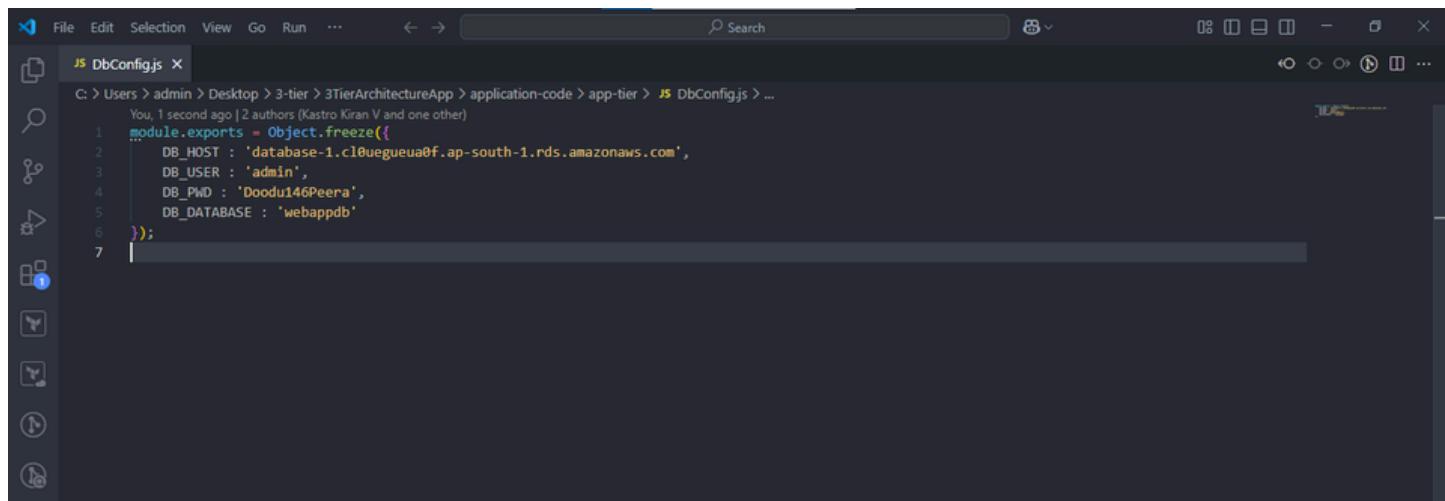
MySQL [(none)]> USE webappdb;
Database changed
MySQL [webappdb]> CREATE TABLE IF NOT EXISTS transactions(
    ->   id INT NOT NULL AUTO_INCREMENT,
    ->   amount DECIMAL(10,2),
    ->   description VARCHAR(100),
    ->   PRIMARY KEY(id)
    -> );
Query OK, 0 rows affected (0.04 sec)

MySQL [webappdb]> SHOW TABLES;
+-----+
| Tables_in_webappdb |
+-----+
| transactions      |
+-----+
1 row in set (0.01 sec)

MySQL [webappdb]> INSERT INTO transactions (amount, description) VALUES ('400', 'groceries');
Query OK, 1 row affected (0.00 sec)

MySQL [webappdb]> SELECT * FROM transactions;
+-----+
| id | amount | description |
+-----+
| 1  | 400.00 | groceries  |
+-----+
1 row in set (0.00 sec)

MySQL [webappdb]>
```



The screenshot shows a code editor window with the file `DbConfig.js` open. The file contains the following code:

```
C: > Users > admin > Desktop > 3-tier > 3TierArchitectureApp > application-code > app-tier > Js DbConfig.js > ...
You, 1 second ago | 2 authors (Kastro Kiran V and one other)
1 module.exports = Object.freeze({
2     DB_HOST : 'database-1.cl0uegueua0f.ap-south-1.rds.amazonaws.com',
3     DB_USER : 'admin',
4     DB_PWD : 'Doodu146Peera',
5     DB_DATABASE : 'webappdb'
6 });
7 |
```

S | Search [Alt+S] | Asia Pacific (Mumbai) ▾ Anoora @ sadiaws ▾

Amazon S3 > Buckets > demo-3-project > application-code/ > app-tier/

app-tier/ Copy S3 URI

Objects Properties

Objects (6) Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix:

Name	Type	Last modified	Size	Storage class
DbConfig.js	js	May 6, 2025, 16:02:16 (UTC+05:30)	195.0 B	Standard
index.js	js	May 6, 2025, 15:18:54 (UTC+05:30)	3.2 KB	Standard
package-lock.json	json	May 6, 2025, 15:18:54 (UTC+05:30)	42.9 KB	Standard
package.json	json	May 6, 2025, 15:18:54 (UTC+05:30)	682.0 B	Standard
README.md	md	May 6, 2025, 15:18:55 (UTC+05:30)	14.0 B	Standard
TransactionService.js	js	May 6, 2025, 15:18:56 (UTC+05:30)	1.8 KB	Standard

```
[root@ip-192-168-2-31 ec2-user]# curl -o- https://raw.githubusercontent.com/avizwayl/aws_3tier_architecture/main/install.sh | bash
  % Total    % Received % Xferd  Average Speed   Time     Time   Current
          Dload  Upload   Total   Spent   Left  Speed
100 14926  100 14926    0      0  36011  0:--:--:--:--:--:--:-- 36053
=> Downloading nvm as script to '/root/.nvm'

=> Appending nvm source string to /root/.bashrc
=> Appending bash_completion source string to /root/.bashrc
=> Close and reopen your terminal to start using nvm or run the following to use it now:

export NVM_DIR="$HOME/.nvm"
[ -s "$NVM_DIR/nvm.sh" ] && \. "$NVM_DIR/nvm.sh" # This loads nvm
[ -s "$NVM_DIR/bash_completion" ] && \. "$NVM_DIR/bash_completion" # This loads nvm bash_completion
[root@ip-192-168-2-31 ec2-user]# source ~/.bashrc
[root@ip-192-168-2-31 ec2-user]# nvm install 16
Downloading and installing node v16.20.2...
Downloaded https://nodejs.org/dist/v16.20.2/node-v16.20.2-linux-x64.tar.xz...
#####
Computing checksums with sha256sum
Checksums matched!
Now using node v16.20.2 (npm v8.19.4)
Creating default alias: default => 16 (> v16.20.2)
[root@ip-192-168-2-31 ec2-user]# nvm use 16
Now using node v16.20.2 (npm v8.19.4)
[root@ip-192-168-2-31 ec2-user]# nvm user 16

Node Version Manager (v0.38.0)

Note: <version> refers to any version-like string nvm understands. This includes:
  - full or partial version numbers, starting with an optional "v" (0.10, v0.1.2, v1)
  - default (built-in) aliases: node, stable, unstable, iojs, system
  - custom aliases you define with `nvm alias foo`
```

```
[root@ip-192-168-2-31 ec2-user]# npm install -g pm2
added 134 packages, and audited 135 packages in 10s

13 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
npm notice
npm notice New major version of npm available! 8.19.4 -> 11.3.0
npm notice Changelog: https://github.com/npm/cli/releases/tag/v11.3.0
npm notice Run npm install -g npm@11.3.0 to update!
npm notice
[root@ip-192-168-2-31 ec2-user]# pwd
```

```
[root@ip-192-168-2-31 ec2-user]# pwd
/home/ec2-user
[root@ip-192-168-2-31 ec2-user]# cd ..
[root@ip-192-168-2-31 home]# cd ~/
[root@ip-192-168-2-31 ~]# sudo aws s3 cp s3://demo-3-project/application-code/app-tier/ app-tier --recursive
download: s3://demo-3-project/application-code/app-tier/README.md to app-tier/README.md
download: s3://demo-3-project/application-code/app-tier/package-lock.json to app-tier/package-lock.json
download: s3://demo-3-project/application-code/app-tier/package.json to app-tier/package.json
download: s3://demo-3-project/application-code/app-tier/TransactionService.js to app-tier/TransactionService.js
download: s3://demo-3-project/application-code/app-tier/DbConfig.js to app-tier/DbConfig.js
download: s3://demo-3-project/application-code/app-tier/index.js to app-tier/index.js
[root@ip-192-168-2-31 ~]# ls
app-tier
[root@ip-192-168-2-31 ~]#
```

Session ID: Anoora-zz68kn8eyte9h3qgardsjpo vsu Instance ID: i-07c7c558f4b114a58 [Terminate](#)

```
npm notice Run npm install -g npm@11.3.0 to update!
npm notice
[root@ip-192-168-2-31 ec2-user]# pwd
/home/ec2-user
[root@ip-192-168-2-31 ec2-user]# cd ..
[root@ip-192-168-2-31 home]# cd ..
[root@ip-192-168-2-31 ~]# cd ~/
[root@ip-192-168-2-31 ~]# sudo aws s3 cp s3://demo-3-project/application-code/app-tier/ app-tier --recursive
download: s3://demo-3-project/application-code/app-tier/README.md to app-tier/README.md
download: s3://demo-3-project/application-code/app-tier/package-lock.json to app-tier/package-lock.json
download: s3://demo-3-project/application-code/app-tier/package.json to app-tier/package.json
download: s3://demo-3-project/application-code/app-tier/TransactionService.js to app-tier/TransactionService.js
download: s3://demo-3-project/application-code/app-tier/DbConfig.js to app-tier/DbConfig.js
download: s3://demo-3-project/application-code/app-tier/index.js to app-tier/index.js
[root@ip-192-168-2-31 ~]# ls
app-tier
[root@ip-192-168-2-31 ~]# cd app-tier/
[root@ip-192-168-2-31 app-tier]# npm install
bash: mpm: command not found
[root@ip-192-168-2-31 app-tier]# npm install

added 68 packages, and audited 69 packages in 2s

2 packages are looking for funding
  run `npm fund` for details

7 vulnerabilities (3 low, 4 high)

To address all issues, run:
  npm audit fix

Run 'npm audit' for details.
[root@ip-192-168-2-31 app-tier]# ls
DbConfig.js README.md TransactionService.js index.js node_modules package-lock.json package.json
[root@ip-192-168-2-31 app-tier]#
```

```
[root@ip-192-168-2-31 app-tier]# ls
DbConfig.js README.md TransactionService.js index.js node_modules package-lock.json package.json
[root@ip-192-168-2-31 app-tier]# pm2 start index.js
```



Runtime Edition

```
PM2 is a Production Process Manager for Node.js applications
with a built-in Load Balancer.

Start and Daemonize any application:
$ pm2 start app.js

Load Balance 4 instances of api.js:
$ pm2 start api.js -i 4

Monitor in production:
$ pm2 monitor
```

Runtime Edition

PM2 is a Production Process Manager for Node.js applications with a built-in Load Balancer.

Start and Daemonize any application:
\$ pm2 start app.js

Load Balance 4 instances of api.js:
\$ pm2 start api.js -i 4

Monitor in production:
\$ pm2 monitor

Make pm2 auto-boot at server restart:
\$ pm2 startup

To go further checkout:
<http://pm2.io/>

```
[PM2] Spawning PM2 daemon with pm2_home=/root/.pm2
[PM2] PM2 Successfully daemonized
[PM2] Starting /root/app-tier/index.js in fork_mode (1 instance)
[PM2] Done.
```

id	name	namespace	version	mode	pid	uptime	ø	status	cpu	mem	user	watching
0	index	default	1.0.0	fork	4317	0s	0	online	0%	24.8mb	root	disabled

[root@ip-192-168-2-31 app-tier]#

[root@ip-192-168-2-31 app-tier]# pm2 list

id	name	namespace	version	mode	pid	uptime	ø	status	cpu	mem	user	watching
0	index	default	1.0.0	fork	4317	48s	0	online	0%	51.3mb	root	disabled

```
[Service]
Type=forking
User=root
LimitNOFILE=infinity
LimitNPROC=infinity
LimitCORE=infinity
Environment=PATH=/root/.nvm/versions/node/v16.20.2/bin:/sbin:/bin:/usr/sbin:/usr/bin:/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin
Environment=PM2_HOME=/root/.pm2
PIDFile=/root/.pm2/pid
Restart=on-failure

ExecStart=/root/.nvm/versions/node/v16.20.2/lib/node_modules/pm2/bin/pm2 resurrect
ExecReload=/root/.nvm/versions/node/v16.20.2/lib/node_modules/pm2/bin/pm2 reload all
ExecStop=/root/.nvm/versions/node/v16.20.2/lib/node_modules/pm2/bin/pm2 kill

[Install]
WantedBy=multi-user.target

Target path
/etc/systemd/system/pm2-root.service
Command list
[ "systemctl enable pm2-root" ]
[PM2] Writing init configuration in /etc/systemd/system/pm2-root.service
[PM2] Making script booting at startup...
[PM2] [-] Executing: systemctl enable pm2-root...
Created symlink from /etc/systemd/system/multi-user.target.wants/pm2-root.service to /etc/systemd/system/pm2-root.service.
[PM2] [v] Command successfully executed.
+-----+
[PM2] Freeze a process list on reboot via:
$ pm2 save

[PM2] Remove init script via:
$ pm2 unstartup systemd
```

```
[root@ip-192-168-2-31 app-tier]# pm2 save
[PM2] Saving current process list...
[PM2] Successfully saved in /root/.pm2/dump.pm2
```

```
[root@ip-192-168-2-31 app-tier]# curl http://localhost:4000/health
"This is the health check"[root@ip-192-168-2-31 app-tier]#
```

aws | Search [Alt+S]

EC2 > Target groups > Create target group

Step 1 Specify group details

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

Step 2 Register targets

Basic configuration

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

Choose a target type

Instances

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

IP addresses

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

Lambda function

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

Application Load Balancer

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS EC2 Target Groups creation page for creating an Application Load Balancer target group.

Target group name: App-internal-tg

Protocol : Port:

- Protocol: HTTP (selected)
- Port: 4000
- Custom port: 1-65535

IP address type:

- IPv4 (selected)
- IPv6

VPC:

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

Screenshot of the AWS EC2 Target Groups creation page for creating an Application Load Balancer target group.

IP address type:

- IPv6 (selected)
- IPv4

VPC:

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

my-vpc-demo
vpc-0e90c1fdb03e7211
IPv4 VPC CIDR: 192.168.0.0/22

Protocol version:

- HTTP1 (selected)
- HTTP2
- gRPC

Health checks:

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

Health check protocol: HTTP

Health check path: Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.

- HTTP1**
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
- HTTP2**
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
- gRPC**
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

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

Health check protocol

HTTP ▾

Health check path

Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.

/health

Up to 1024 characters allowed.

► Advanced health check settings

Attributes

- Step 1
Specify group details
Step 2
 Register targets

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (1)

Available instances (1)				
<input type="checkbox"/> Filter instances				
Instance ID	Name	State	Security groups	Zone
<input type="checkbox"/> i-07c7c558f4b114a58	ApptierInstance	Running	App-SG	ap-south-1a

0 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.

4000
1-65535 (separate multiple ports with commas)

1 selection is now pending below. Include more or register targets when ready.

AWS Search [Alt+S] Asia Pacific (Mumbai) Anoora @ sadiaws

EC2 > Target groups > Create target group

0 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.
4000
1-65535 (separate multiple ports with commas)

Include as pending below

1 selection is now pending below. Include more or register targets when ready.

Review targets

Targets (1)

Filter targets Show only pending Remove all pending

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID
i-07c7c558f4b114a58	ApptierInstance	4000	Running	App-SG	ap-south-1a	192.168.2.31	subnet-0093645f2e1

1 pending

Cancel Previous Create target group

EC2 > Target groups > App-internal-tg

Successfully created the target group: App-internal-tg. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the Targets tab. X

App-internal-tg

Actions ▾

Details

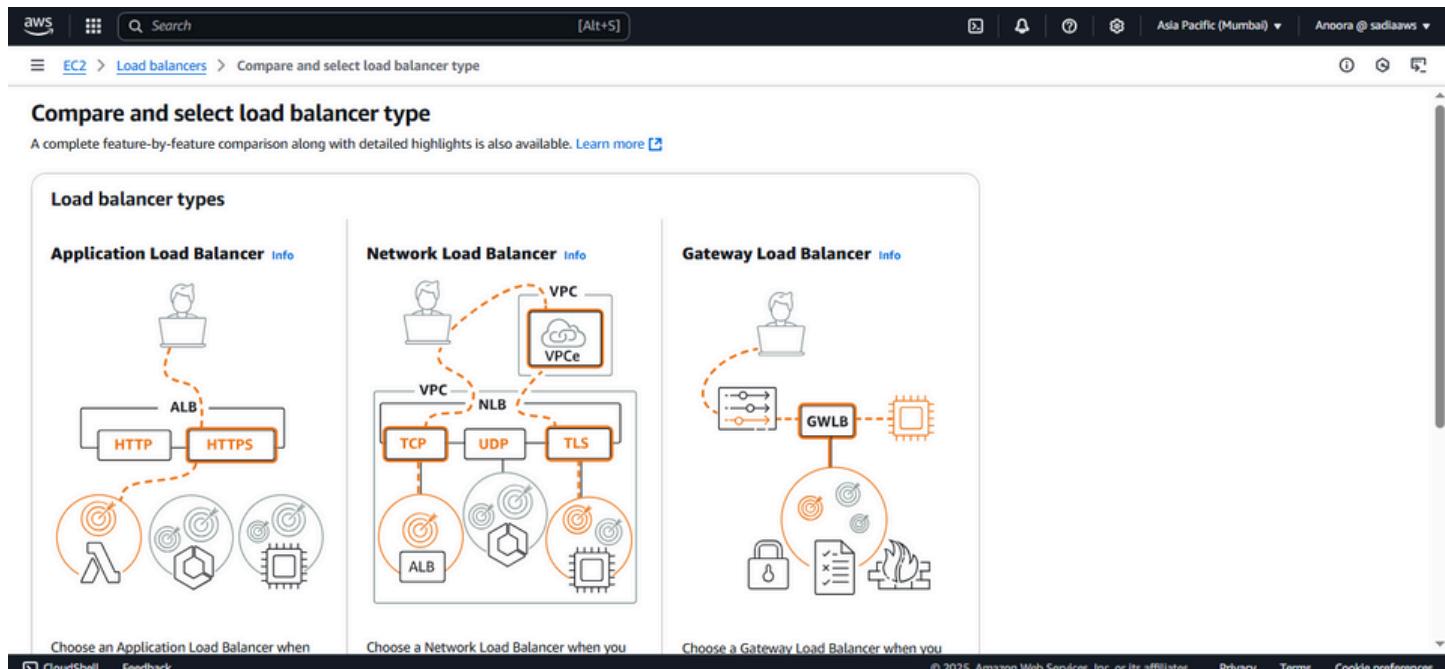
arn:aws:elasticloadbalancing:ap-south-1:183295428288:targetgroup/App-internal-tg/242a1d909f470846	VPC vpc-0e90e1fdb03e7211	
Target type Instance	Protocol : Port HTTP: 4000	Protocol version HTTP1
IP address type IPv4	Load balancer None associated	

1 Total targets	0 Healthy	0 Unhealthy	1 Unused	0 Initial	0 Draining
0 Anomalous					

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

Targets Monitoring Health checks Attributes Tags

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



AWS CloudWatch Metrics Dashboard showing metrics for Lambda functions. The dashboard includes a search bar, navigation menu, and a main content area with three cards: 'Lambda Metrics' (with a pie chart), 'Lambda Function Metrics' (with a line chart), and 'Lambda Function Metrics (Last 7 days)' (with a line chart).

Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

How Application Load Balancers work

Basic configuration

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

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

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

Internet-facing

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name resolves to public IPs.
- Requires a public subnet.

Internal

- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- Compatible with the IPv4 and Dualstack IP address types.

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

- Includes only IPv4 addresses.

AWS CloudWatch Metrics Dashboard showing metrics for Lambda functions. The dashboard includes a search bar, navigation menu, and a main content area with three cards: 'Lambda Metrics' (with a pie chart), 'Lambda Function Metrics' (with a line chart), and 'Lambda Function Metrics (Last 7 days)' (with a line chart).

Create Application Load Balancer

groups For a new VPC, [create a VPC](#)

my-vpc-demo
vpc-0e90c1f0be03e7211
IPv4 VPC CIDR: 192.168.0.0/22

IP pools - new | Info
You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view Pools in [Amazon VPC IP Address Manager console](#).
 Use IPAM pool for public IPv4 addresses

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

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

ap-south-1a (aps1-az1)
Subnet

- Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-0093645f2e11e4df5	demo-vpc-app1
--------------------------	---------------

ap-south-1b (aps1-az3)
Subnet

- Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-00c31067eca4d099	demo-vpc-app2
-------------------------	---------------

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

Security groups [Info](#)

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

Security groups

Select up to 5 security groups

▼

Internal-ALB-SG	X
sg-00410f66d611ec665	VPC: vpc-0e90e1fdb03e7211

Listeners and routing [Info](#)

A Listener is a service that checks for incoming messages from the user and performs some actions. The code that you define for a Listener executes from the background when a message is received from the external source.

Listeners and routing [Info](#)

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

▼ Listener HTTP:80 [Remove](#)

Protocol	Port	Default action	Info
HTTP	: 80 1-65535	Forward to App-internal-tg Target type: Instance, IPv4	HTTP C

[Create target group](#) 

Listener tags - optional

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

[Add listener tag](#) 

The screenshot shows the AWS CloudFormation console with the following details:

- Region:** Asia Pacific (Mumbai)
- Stack:** CloudWatchMetrics
- Outputs:**
 - CloudWatchMetrics: arn:aws:cloudwatchmetrics:ap-south-1:183295428288:metricfilter/CloudWatchMetrics/5d47215fd09827e
- Success Message:** Stack CloudWatchMetrics was successfully created.
- Actions:** Create Change Set, Delete, Export, Import, View Logs, View Metrics.

```
JS DbConfig.js      nginx.conf X
C: > Users > admin > Desktop > 3-tierArchitectureApp > application-code > nginx.conf
13 http {
31     server {
50         # HTTP TO HTTPS REDIRECTION
37             if ($http_x_forwarded_proto = 'http') {
38                 return 301 https://$host$request_uri;
39             }
40
41             #health check
42             location /health {
43                 default_type text/html;
44                 return 200 "<!DOCTYPE html><p>Web Tier Health Check</p>\n";
45             }
46
47             #react app and front end files
48             location / {
49                 root    /home/ec2-user/web-tier/build;
50                 index index.html index.htm;
51                 try_files $uri /index.html; Kastro Kiran V, 4 months ago * Add files via upload ...
52             }
53
54             #proxy for internal lb
55             location /api/ {
56                 proxy_pass http://internal-App-LB-1142538316.ap-south-1.elb.amazonaws.com:80/;
57             }
58
59         }
60     }
}

```

☰

Upload succeeded
For more information, see the [Files and folders](#) table.

Upload: status Close

After you navigate away from this page, the following information is no longer available.

Summary	
Destination	s3://demo-3-project/application-code/
Succeeded	✔ 1 file, 1.6 KB (100.00%)
Failed	✗ 0 files, 0 B (0%)

Files and folders (1 total, 1.6 KB)

Find by name		<	1	>	
Name	Folder	Type	Size	Status	Error
nginx.conf	-	-	1.6 KB	✔ Succeeded	-

aws | Search [Alt+S] | Asia Pacific (Mumbai) | Anoora @ sadiaws

Amazon S3 > Buckets > demo-3-project > application-code/

application-code/

Objects Properties

Objects (4)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix:

Name	Type	Last modified	Size	Storage class
app-tier/	Folder	-	-	-
nginx-Without-SSL.conf	conf	May 6, 2025, 15:18:53 (UTC+05:30)	1.6 KB	Standard
nginx.conf	conf	May 6, 2025, 16:26:05 (UTC+05:30)	1.6 KB	Standard
web-tier/	Folder	-	-	-

[Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

aws | Search [Alt+S] | Asia Pacific (Mumbai) | Anoora @ sadiaws

EC2 > Instances > Launch an instance

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: webtierInstance [Add additional tags](#)

Application and OS Images (Amazon Machine Image)

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

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

Recent AMIs: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, Debian

Quick Start AMIs: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, Debian

Browse more AMIs: Including AMIs from AWS, Marketplace and the Community

Summary

Number of instances: 1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI... [read more](#)
ami-03edbe403ec8522ed

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 of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where applicable).

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

aws | Search [Alt+S] | Asia Pacific (Mumbai) | Anoora @ sadiaws

EC2 > Instances > Launch an instance

Recent AMIs: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, Debian

Quick Start AMIs: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, Debian

Browse more AMIs: Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
Free tier eligible

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-03edbe403ec8522ed (64-bit (x86)) / ami-06d5bdafada20e525f (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.

Amazon Linux 2 Kernel 5.10 AMI 2.0.20250428.0 x86_64 HVM gp2

Architecture	AMI ID	Publish Date	Username	Verified provider
64-bit (x86)	ami-03edbe403ec8522ed	2025-04-25	ec2-user	Verified provider

Instance type

[Info](#) | [Get advice](#)

Summary

Number of instances: 1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI... [read more](#)
ami-03edbe403ec8522ed

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 of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where applicable).

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

EC2 > Instances > Launch an instance

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

Key pair name - required
Proceed without a key pair (Not recommended) Default value Create new key pair

Network settings Info

VPC - required | Info
vpc-0e90e1fdbbe03e7211 (my-vpc-demo)
192.168.0.0/22

Subnet | Info
subnet-078b3a692df77cfb1 demo-vpc-web1
VPC: vpc-0e90e1fdbbe03e7211 Owner: 183295428288 Availability Zone: ap-south-1a
Zone type: Availability Zone IP addresses available: 58 CIDR: 192.168.0.0/26

Create new subnet

Auto-assign public IP | Info
Disable

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

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Summary
Number of instances | Info
1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-03edbe403ec8522ed

Virtual server type (instance type)
t2.micro

Firewall (security group)

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

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where applicable).

Cancel Launch instance Preview code

EC2 > Instances > Launch an instance

192.168.0.0/22

Subnet | Info
subnet-078b3a692df77cfb1 demo-vpc-web1
VPC: vpc-0e90e1fdbbe03e7211 Owner: 183295428288 Availability Zone: ap-south-1a
Zone type: Availability Zone IP addresses available: 58 CIDR: 192.168.0.0/26

Create new subnet

Auto-assign public IP | Info
Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) | Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Common security groups | Info
Select security groups

web-tier-SG sg-0c410ba5f6a30aa43 X
VPC: vpc-0e90e1fdbbe03e7211

Compare security group rules

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

Advanced details Info

Domain join directory | Info
Select Create new directory

IAM instance profile | Info
demo-ec2-role-3
arn:aws:iam::183295428288:instance-profile/demo-ec2-role-3

Create new IAM profile

Hostname type | Info
IP name

Session ID: Anoora-s8cpv2epdu3ayj7oonb7hrkty8 Instance ID: i-00a408fb201cc84d3

sh-4.2\$ [ec2-user@ip-192-168-0-7 bin]\$ whoami

[ec2-user@ip-192-168-0-7 bin]\$ cd /home/ec2-user

[ec2-user@ip-192-168-0-7 ~]\$ pwd

/home/ec2-user

Terminate

```
sh-4.2$ sudo -su ec2-user
[ec2-user@ip-192-168-0-7 bin]$ whoami
ec2-user
[ec2-user@ip-192-168-0-7 bin]$ cd /home/ec2-user
[ec2-user@ip-192-168-0-7 ~]$ pwd
/home/ec2-user
[ec2-user@ip-192-168-0-7 ~]$ curl -o- https://raw.githubusercontent.com/avizwayl/aws_3tier_architecture/main/install.sh | bash
% Total    % Received % Xferd  Average Speed   Time     Time  Current
          Dload  Upload Total Spent   Left Speed
100 14926  100 14926    0      0  40912  0:--:-- --:--:-- --:--:-- 41005
=> Downloading nvm as script to '/home/ec2-user/.nvm'

=> Appending nvm source string to /home/ec2-user/.bashrc
=> Appending bash_completion source string to /home/ec2-user/.bashrc
=> Close and reopen your terminal to start using nvm or run the following to use it now:

export NVM_DIR="$HOME/.nvm"
[ -s "$NVM_DIR/nvm.sh" ] && . "$NVM_DIR/nvm.sh" # This loads nvm
[ -s "$NVM_DIR/bash_completion" ] && . "$NVM_DIR/bash_completion" # This loads nvm bash_completion
[ec2-user@ip-192-168-0-7 ~]$ source ~/.bashrc
[ec2-user@ip-192-168-0-7 ~]$ nvm install 16
Downloading and installing node v16.20.2...
Downloaded https://nodejs.org/dist/v16.20.2/node-v16.20.2-linux-x64.tar.xz...
#####
Computing checksum with sha256sum
Checksums matched!
Now using node v16.20.2 (npm v8.19.4)
Creating default alias: default -> 16 (<- v16.20.2)
[ec2-user@ip-192-168-0-7 ~]$ nvm use 16
Now using node v16.20.2 (npm v8.19.4)
[ec2-user@ip-192-168-0-7 ~]$
```

```

Computing checksum with sha256sum
Checksums matched!
Now using node v16.20.2 (npm v8.19.4)
Creating default alias: default -> 16 (> v16.20.2)
[ec2-user@ip-192-168-0-7 ~]$ nvm use 16
Now using node v16.20.2 (npm v8.19.4)
[ec2-user@ip-192-168-0-7 ~]$ aws s3 cp s3://demo-3-project/application-code/web-tier/ web-tier --recursive
download: s3://demo-3-project/application-code/web-tier/src/components/Burger/Burger.js to web-tier/src/components/Burger/Burger.js
download: s3://demo-3-project/application-code/web-tier/public/robots.txt to web-tier/public/robots.txt
download: s3://demo-3-project/application-code/web-tier/src/components/Burger/index.js to web-tier/src/components/Burger/index.js
download: s3://demo-3-project/application-code/web-tier/src/components/Home/Home.js to web-tier/src/components/Home/Home.js
download: s3://demo-3-project/application-code/web-tier/README.md to web-tier/README.md
download: s3://demo-3-project/application-code/web-tier/src/components/Burger/Burger.styled.js to web-tier/src/components/Burger/Burger.styled.js
download: s3://demo-3-project/application-code/web-tier/src/components/Menu/index.js to web-tier/src/components/Menu/index.js
download: s3://demo-3-project/application-code/web-tier/src/components/index.js to web-tier/src/components/index.js
download: s3://demo-3-project/application-code/web-tier/package.json to web-tier/package.json
download: s3://demo-3-project/application-code/web-tier/src/components/DatabaseDemo.css to web-tier/src/components/DatabaseDemo.css
download: s3://demo-3-project/application-code/web-tier/src/App.js to web-tier/src/App.js
download: s3://demo-3-project/application-code/web-tier/public/index.html to web-tier/public/index.html
download: s3://demo-3-project/application-code/web-tier/src/global.js to web-tier/src/global.js
download: s3://demo-3-project/application-code/web-tier/src/components/Menu/Menu.js to web-tier/src/components/Menu/Menu.js
download: s3://demo-3-project/application-code/web-tier/src/components/Menu/Menu.styled.js to web-tier/src/components/Menu/Menu.styled.js
download: s3://demo-3-project/application-code/web-tier/src/components/DatabaseDemo.js to web-tier/src/components/DatabaseDemo.js
download: s3://demo-3-project/application-code/web-tier/src/hooks.js to web-tier/src/hooks.js
download: s3://demo-3-project/application-code/web-tier/src/index.css to web-tier/src/index.css
download: s3://demo-3-project/application-code/web-tier/src/reportWebVitals.js to web-tier/src/reportWebVitals.js
download: s3://demo-3-project/application-code/web-tier/src/setupTests.js to web-tier/src/setupTests.js
download: s3://demo-3-project/application-code/web-tier/src/theme.js to web-tier/src/theme.js
download: s3://demo-3-project/application-code/web-tier/src/App.css to web-tier/src/App.css
download: s3://demo-3-project/application-code/web-tier/src/index.js to web-tier/src/index.js
download: s3://demo-3-project/application-code/web-tier/src/App.test.js to web-tier/src/App.test.js
download: s3://demo-3-project/application-code/web-tier/src/assets/3TierArch.png to web-tier/src/assets/3TierArch.png
[ec2-user@ip-192-168-0-7 ~]$ ls
web-tier
[ec2-user@ip-192-168-0-7 ~]$

```

Session ID: Anoora-s8cpv2epdu3ayj7oonb7hrkyt8 Instance ID: i-00a40fb201cc84d3

[Terminate](#)

```

npm WARN deprecated rimraf@3.0.2: Rimraf versions prior to v4 are no longer supported
npm WARN deprecated @humanwhocodes/object-schema@2.0.3: Use @eslint/object-schema instead
npm WARN deprecated @humanwhocodes/config-array@0.13.0: Use @eslint/config-array instead
npm WARN deprecated @babel/plugin-proposal-optimal-chaining@7.21.0: This proposal has been merged to the ECMAScript standard and thus this plugin is no longer maintained.
. Please use @babel/plugin-transform-optimal-chaining instead.
npm WARN deprecated @babel/plugin-proposal-private-methods@7.18.6: This proposal has been merged to the ECMAScript standard and thus this plugin is no longer maintained.
. Please use @babel/plugin-transform-private-methods instead.
npm WARN deprecated @babel/plugin-proposal-numeric-separator@7.18.6: This proposal has been merged to the ECMAScript standard and thus this plugin is no longer maintained.
. Please use @babel/plugin-transform-numeric-separator instead.
npm WARN deprecated @babel/plugin-proposal-nullish-coalescing-operator@7.18.6: This proposal has been merged to the ECMAScript standard and thus this plugin is no longer maintained. Please use @babel/plugin-transform-nullish-coalescing-operator instead.
npm WARN deprecated @babel/plugin-proposal-class-properties@7.18.6: This proposal has been merged to the ECMAScript standard and thus this plugin is no longer maintained.
. Please use @babel/plugin-transform-class-properties instead.
npm WARN deprecated @babel/plugin-proposal-private-property-in-object@7.21.11: This proposal has been merged to the ECMAScript standard and thus this plugin is no longer maintained. Please use @babel/plugin-transform-private-property-in-object instead.
npm WARN deprecated svgo@1.3.2: This SVGO version is no longer supported. Upgrade to v2.x.x.
npm WARN deprecated eslint@8.57.1: This version is no longer supported. Please see https://eslint.org/version-support for other options.

added 1503 packages, and audited 1504 packages in 1m

274 packages are looking for funding
  run 'npm fund' for details

8 vulnerabilities (2 moderate, 6 high)

To address all issues (including breaking changes), run:
  npm audit fix --force

Run 'npm audit' for details.

npm notice
npm notice New major version of npm available! 8.19.4 -> 11.3.0
npm notice Changelog: https://github.com/npm/cli/releases/tag/v11.3.0
npm notice Run npm install -g npm@11.3.0 to update!
npm notice
[ec2-user@ip-192-168-0-7 web-tier]$

```

```
[ec2-user@ip-192-168-0-7 web-tier]$ npm run build
> aws-3tier-web-layer@0.1.0 build
> react-scripts build

Creating an optimized production build...
Compiled successfully.

File sizes after gzip:

 74.93 kB  build/static/js/main.12bdb313.js
 1.79 kB   build/static/js/453.a4ec9c9e.chunk.js
 493 B     build/static/css/main.b20b6ac4.css

The project was built assuming it is hosted at ./.
You can control this with the homepage field in your package.json.

The build folder is ready to be deployed.

Find out more about deployment here:
https://cra.link/deployment

[ec2-user@ip-192-168-0-7 web-tier]$
```

Session ID: Anoora-s8cpv2epdu3ayj7oonb7hrky8 Instance ID: i-00a408fb201cc84d3

[Terminate](#)

Package	Arch	Version	Repository	Size
Installing:				
nginx	x86_64	1:1.26.3-1.amzn2.0.1	amzn2extra-nginx1	51 k
Installing for dependencies:				
generic-logos-httd	noarch	18.0.0-4.amzn2	amzn2-core	19 k
gperftools-libs	x86_64	2.6.1-1.amzn2	amzn2-core	274 k
nginx-core	x86_64	1:1.26.3-1.amzn2.0.1	amzn2extra-nginx1	639 k
nginx-filesystem	noarch	1:1.26.3-1.amzn2.0.1	amzn2extra-nginx1	25 k
openssl111-libs	x86_64	1:1.1.1zb-1.amzn2.0.1	amzn2-core	1.4 M
openssl111-pkcs11	x86_64	0.4.10-6.amzn2.0.1	amzn2-core	61 k
Transaction Summary				
Install 1 Package (+6 Dependent packages)				
Total download size: 2.5 M				
Installed size: 6.9 M				
Downloading packages:				
(1/7): generic-logos-httd-18.0.0-4.amzn2.noarch.rpm			19 kB 00:00:00	
(2/7): nginx-1.26.3-1.amzn2.0.1.x86_64.rpm			51 kB 00:00:00	
(3/7): nginx-core-1.26.3-1.amzn2.0.1.x86_64.rpm			639 kB 00:00:00	
(4/7): gperftools-libs-2.6.1-1.amzn2.x86_64.rpm			274 kB 00:00:00	
(5/7): nginx-filesystem-1.26.3-1.amzn2.0.1.noarch.rpm			25 kB 00:00:00	
(6/7): openssl111-pkcs11-0.4.10-6.amzn2.0.1.x86_64.rpm			61 kB 00:00:00	
(7/7): openssl111-libs-1.1.1zb-1.amzn2.0.1.x86_64.rpm			1.4 MB 00:00:00	
Total			6.1 MB/s 2.5 MB 00:00:00	
Running transaction check				1/7
Running transaction test				2/7
Transaction test succeeded				3/7
Running transaction				
Installing : 1:nginx-filesystem-1.26.3-1.amzn2.0.1.noarch				
Installing : 1:openssl111-libs-1.1.1zb-1.amzn2.0.1.x86_64				
Installing : openssl111-pkcs11-0.4.10-6.amzn2.0.1.x86_64				

```
40 mock available [ =stable ]
43 livepatch available [ =stable ]
45 haproxy2 available [ =stable ]
46 collectd available [ =stable ]
47 aws-nitro-enclaves-cli available [ =stable ]
48 R4 available [ =stable ]
kernel-5.4 available [ =stable ]
50 selinux-ng available [ =stable ]
52 tomcat9 available [ =stable ]
53 unbound1.13 available [ =stable ]
54 mariadb10.5 available [ =stable ]
55 kernel-5.10=latest enabled [ =stable ]
56 redis6 available [ =stable ]
59 tpostgresql13 available [ =stable ]
60 mock2 available [ =stable ]
61 dnsmasq2.85 available [ =stable ]
62 kernel-5.15 available [ =stable ]
63 tpostgresql14 available [ =stable ]
64 firefox available [ =stable ]
65 lustre available [ =stable ]
67 awscli1 available [ =stable ]
68 tphp8.2 available [ =stable ]
69 dnsmasq available [ =stable ]
70 unbound1.17 available [ =stable ]
72 collectd-python3 available [ =stable ]
† Note on end-of-support. Use 'info' subcommand.
[ec2-user@ip-192-168-0-7 web-tier]$ cd /etc/nginx
[ec2-user@ip-192-168-0-7 nginx]$ ls
conf.d fastcgi.conf fastcgi_params koi-utf mime.types nginx.conf scgi_params uwsgi_params win-utf
default.d fastcgi.conf.default fastcgi_params.default koi-win mime.types.default nginx.conf.default scgi_params.default uwsgi_params.default
[ec2-user@ip-192-168-0-7 nginx]$ cd /etc/nginx
[ec2-user@ip-192-168-0-7 nginx]$ sudo rm nginx.conf
[ec2-user@ip-192-168-0-7 nginx]$ sudo aws s3 cp s3://demo-3-project/application-code/nginx.conf .
download: s3://demo-3-project/application-code/nginx.conf to ./nginx.conf
[ec2-user@ip-192-168-0-7 nginx]$
```

```
69 dnsmasq available [ =stable ]
70 unbound1.17 available [ =stable ]
72 collectd-python3 available [ =stable ]
† Note on end-of-support. Use 'info' subcommand.
[ec2-user@ip-192-168-0-7 web-tier]$ cd /etc/nginx
[ec2-user@ip-192-168-0-7 nginx]$ ls
conf.d fastcgi.conf fastcgi_params koi-utf mime.types nginx.conf scgi_params uwsgi_params win-utf
default.d fastcgi.conf.default fastcgi_params.default koi-win mime.types.default nginx.conf.default scgi_params.default uwsgi_params.default
[ec2-user@ip-192-168-0-7 nginx]$ cd /etc/nginx
[ec2-user@ip-192-168-0-7 nginx]$ sudo rm nginx.conf
[ec2-user@ip-192-168-0-7 nginx]$ sudo aws s3 cp s3://demo-3-project/application-code/nginx.conf .
download: s3://demo-3-project/application-code/nginx.conf to ./nginx.conf
[ec2-user@ip-192-168-0-7 nginx]$ sudo service nginx restart
Redirecting to /bin/systemctl restart nginx.service
[ec2-user@ip-192-168-0-7 nginx]$ chmod -R 755 /home/ec2-user
[ec2-user@ip-192-168-0-7 nginx]$ sudo chkconfig nginx on
Note: Forwarding request to 'systemctl enable nginx.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service to /usr/lib/systemd/system/nginx.service.
[ec2-user@ip-192-168-0-7 nginx]$
```

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 <small>Info</small>	Protocol <small>Info</small>	Port range	Source <small>Info</small>	Description - optional <small>Info</small>
sgr-03a8ed0f14f55676e	HTTP	TCP	80	Custom	<input type="text"/> sg-0a8725cd50c1285d1
sgr-0caab12aed065f4d9	HTTP	TCP	80	Custom	<input type="text"/> 192.168.0.0/22
-	HTTP	TCP	80	Anyw...	<input type="text"/> 0.0.0.0/0

[Add rule](#)[Cancel](#)[Preview changes](#)[Save rules](#)

'AWS 3-TIER DEMO BY KASTRO'



X

AURORA DATABASE DEMO PAGE

DEL

ID	AMOUNT	DESC
ADD		
1	400	groceries
2	500	Dress
3	6000	Python

 HOME

 DB DEMO