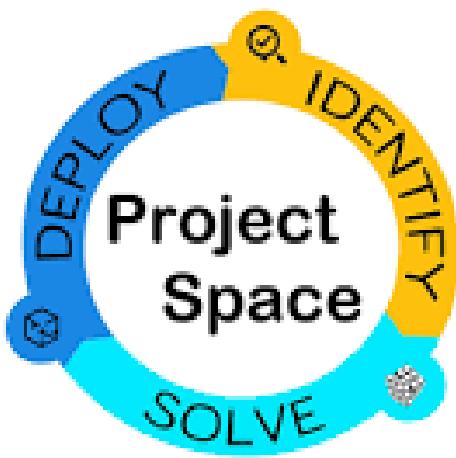


3-WEB APPLICATION DEPLOYMENT IN CLOUD



Team Name: Team Cookies

Team Number: 57

Team Members:

- Bhumika Sree (20A91A0508)
- Aakash (20A91A0544)
- Vaishnavi (20A91A0552)
- Prudhvi (20A91A0576)

3-Tier Web Application Deployment in Cloud.

Three-tier architecture is client-server architecture. The application is separated into physical computing tiers, which means the business logic, data storage, data access, and user interface are developed and maintained as single modules on separate platforms.

Similarly, to the three-layer architecture, the three-tier architecture classifies an application into three main logical components but deploy them on different physical computing tiers:

- **Presentation Tier**

The tier is the user interface of the application, where users interact with the application. Its main purpose is to display information to and collect data from users. This is the top-most level in the architecture and can be run on the web browser or a desktop/mobile application.

- **Application tier**

This is the heart of the application, better known as the logic tier or middle tier. It coordinates all business logic of the application, prescribes how business objects interact with each other. It handles collected information from the Presentation tier. During the process, this tier may need to access the Data-tier to retrieve or modify the data. In a three-tier application, all communication goes smoothly through the Application tier. The Presentation tier and the Data-tier can't communicate directly with one another.

- **Data-tier**

The Data-tier is sometimes referred to as the database tier, where it stores and manages the data processed by the Application tier.

— 3 - Computing Tiers

01. **Presentation Tier**

- The presentation tier includes the interface layers between the user and the back-end resources the user wishes to access.
- Its main purpose is to display information to and collect information from the user.

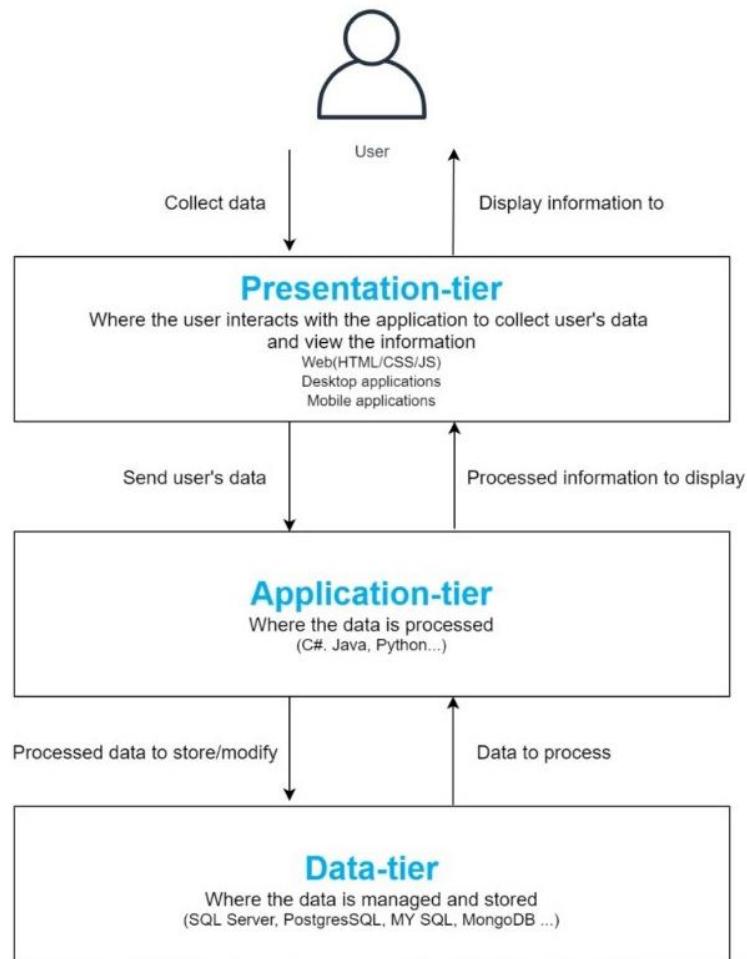
02. **Application Tier**

- It will take and process data from the persistent tier. It will then return this content to the presentation tier.
- The Presentation tier and the Data-tier can not communicate directly with one another.

03. **Data Tier**

- The data tier, sometimes called database tier, data access tier or back-end, is where the information processed by the application is stored and managed
- It is used to store the processed information so that it can be retrieved later on when required.

HOW IT WORKS?



Benefits of using 3 Tier Deployment and Cloud



Scope:

The main aim of the project is to deploy a web application by using 3-tier architecture. The scope of three-tier web application deployment in the cloud is vast and covers various aspects of the deployment process.

Infrastructure Provisioning: The scope of infrastructure provisioning includes creating a virtual private cloud (VPC), setting up subnets, configuring security groups, and deploying the necessary infrastructure components such as web servers, application servers, and database servers.

Application Architecture Design and Deployment: The scope of application architecture design includes designing and deploying the three-tier architecture, selecting the appropriate web servers, application servers, and database servers in their respective tiers, load balancers and scaling strategies, and security and access control mechanisms.

Monitoring and Logging: The scope of monitoring and logging includes configuring monitoring and logging mechanisms, setting up alerts and notifications, and monitoring the performance and availability of the application.

Security and Access Control: The scope of security and access control includes setting up authentication and authorization mechanisms, securing the network, securing the servers, and configuring firewall rules.

Purpose of the Project:

The purpose of deploying a 3-tier web application in the cloud is to leverage the benefits of cloud computing to achieve scalability, flexibility, and cost-effectiveness.

By deploying a 3-tier web application in the cloud, organizations can:

Scale the application as needed: With cloud computing, organizations can easily scale the application up or down based on demand. This means that if the application experiences a sudden surge in traffic, the organization can quickly and easily add more resources to handle the increased load.

Improve application performance: Cloud computing services often provide high-speed, low-latency connections to the internet, improving the performance of the application for users across the globe.

Reduce infrastructure costs: Cloud computing eliminates the need for organizations to purchase and maintain their own infrastructure, which can be a significant cost savings. Additionally, cloud services often provide pay-as-you-go pricing models, allowing organizations to pay only for the resources they use.

Increase agility: Cloud computing enables organizations to quickly and easily deploy and update applications, allowing them to respond quickly to changing business requirements.

Improve security: Cloud computing services often provide advanced security features, such as encryption, access controls, and threat detection, which can help organizations better protect their applications and data.

Technologies Used for this Project:

- As we are deploying the web application in the cloud, we need cloud vendors such as AWS, Azure cloud, Google cloud etc.
- Networking
- DevOps

- Front-end
- Back-end
- Database Management System

Tools and Requirements for the Projects:

There are several tools and requirements that are needed for the deployment of a three-tier web application in the cloud. Some of the key ones include:

Cloud Platform: A cloud platform is required to host the application,

- Amazon Web Services (AWS),
- Microsoft Azure,
- Google Cloud Platform (GCP).

Here, we are deploying the application using the AWS.

Virtual Private Cloud (VPC): A VPC provides the networking infrastructure needed to securely deploy the application in the cloud.

Load Balancers: Load balancers are used to distribute incoming traffic across multiple web servers in the presentation tier to ensure high availability and scalability.

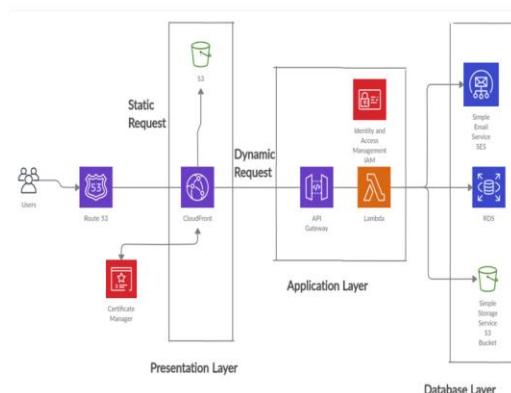
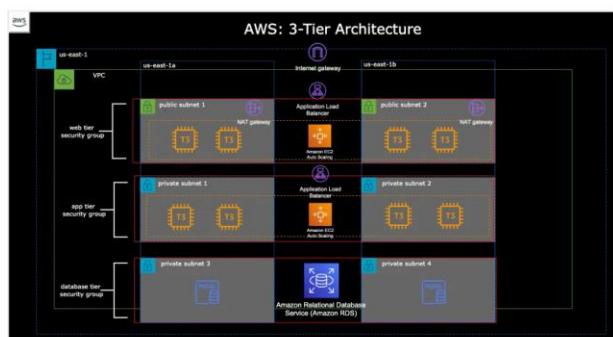
Web Server: A web server, such as Apache or Nginx, is required to serve static content and handle HTTP requests.

Application Server: An application server, such as Tomcat or JBoss, is required to run the application codebase and handle dynamic content.

Database Server: A database server, such as MySQL or PostgreSQL, is required to store and manage application data. Here, we are using MySQL Database.

Security and Access Control Tools: Security and access control tools, such as Identity and Access Management (IAM) or Key Management Service (KMS), are used to ensure that the application and infrastructure are secured and access is restricted to authorized personnel.

Deployment Tools and Requirements



Step 1:

Create a VPC for your project.

To be more secure and to be more isolated, we need to create our own VPC. Here, we are creating our own VPC with total 6 subnets, 2 are public and 4 are private.

For Presentation Tier we are creating 2 public subnets as they should be accessible by the users and clients. For public subnets, Enable the auto-assign public IPv4 address.

As the Application Tier and the Data Tier should be accessible only by the authorized users, we are making the two tiers as private by using the private subnets (2 private subnets for each tier).

Go to VPC dashboard and create new VPC and subnets.

The screenshot shows the 'Create VPC' wizard on the AWS VPC service. It consists of two main sections: 'VPC settings' and 'Tags'.

VPC settings:

- Resources to create:** A radio button group where 'VPC only' is selected.
- Name tag - optional:** An input field containing '3-Tier_VPC'.
- IPv4 CIDR block:** A radio button group where 'IPv4 CIDR manual input' is selected. Below it, the CIDR block '10.0.0.0/16' is listed.
- IPv6 CIDR block:** A radio button group where 'No IPv6 CIDR block' is selected.
- Tenancy:** A dropdown menu set to 'Default'.

Tags:

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

Key	Value - optional
Q Name	Q 3-Tier_VPC X Remove

Add new tag

You can add 49 more tags.

Cancel Create VPC

The screenshot shows the AWS VPC dashboard. In the left sidebar, under 'Virtual private cloud', 'Your VPCs' is selected. A new VPC named '3-Tier_VPC' is being created. The 'Subnets' section shows two public subnets ('app-1', 'data-1') and two private subnets ('web-1', 'web-2') within the VPC.

Step 2:

Create an Internet Gateway.

Go to Internet Gateways-> Create a new Internet Gateway for our public subnets.

Provide name for the internet gateway and give necessary tags. After creating it, attach it to the VPC that we have created. The Internet Gateway will allow the public subnets traffic to the internet.

The screenshot shows the AWS Internet Gateways page. A new Internet Gateway named 'igw-03a7a1d69dc2435f4' is being created and attached to the VPC '3-Tier_VPC'. The gateway has a single tag named 'Name' with the value '3-Tier_IG'.

Step 3:

Create the NAT gateway

Go to Nat Gateway and create a new NAT gateway. Provide the name, select the public subnet in which we want to create the NAT gateway. Select the connectivity type (Here, we are using the Public connectivity). Allocate the Elastic IP address to the NAT gateway.

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

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

The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.

Connectivity type
Select a connectivity type for the NAT gateway.

Public
 Private

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.

► Additional settings Info

The screenshot shows the AWS VPC dashboard with the 'NAT gateways' section selected. A table lists one NAT gateway:

Name	NAT gateway ID	Connectivity type	State	Primary public IPv4 address	Primary private IPv4 address	Primary network interface ID
3-Tier_NAT	nat-010399da9eff9e9d5	Public	Available	52.21.186.249	10.0.1.114	eni-03aada4d1261a7df3

Below the table, a detailed view for the 'nat-010399da9eff9e9d5 / 3-Tier_NAT' gateway is shown. The 'Details' tab is selected, displaying the following information:

NAT gateway ID nat-010399da9eff9e9d5	Connectivity type Public	State Available	State message -
NAT gateway ARN arn:aws:ec2:us-east-1:123456789012:network-interface/eni-03aada4d1261a7df3	Primary public IPv4 address 52.21.186.249	Primary private IPv4 address 10.0.1.114	Primary network interface ID eni-03aada4d1261a7df3

Step 4:

Create route tables

Create 2 route tables, one is for the public and the other is for private subnets.

Route tables->create route table.

Provide the Route table name, select the VPC and add the necessary tags.

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
3-Tier_public_route	rtb-0f29514e1202e985f	-	-	No	vpc-07c6fe43aed182858 3-Tier...	467953945382
3-Tier_private_route	rtb-0372678f984e9bd9d	-	-	No	vpc-07c6fe43aed182858 3-Tier...	467953945382
	rtb-07f7715c625d99276	-	-	Yes	vpc-07c6fe43aed182858 3-Tier...	467953945382

After creating the public route table, go to actions, edit the subnet associations. Select the public subnets that we have created for presentation tier. Save the associations.

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
app-1	subnet-0040c2fe59ff5d33	10.0.3.0/24	-	Main (rtb-07f7715c625d99276)
data-2	subnet-01bb015ebf6ea60f	10.0.6.0/24	-	Main (rtb-07f7715c625d99276)
data-1	subnet-0977c38fc76db62c	10.0.5.0/24	-	Main (rtb-07f7715c625d99276)
app-2	subnet-02baaffafff72fb	10.0.4.0/24	-	Main (rtb-07f7715c625d99276)
web-2	subnet-06a5bcbf74b1ac8d	10.0.2.0/24	-	Main (rtb-07f7715c625d99276)
web-1	subnet-0e1cc43f5b12b7897	10.0.1.0/24	-	Main (rtb-07f7715c625d99276)

Now go to edit routes, add the internet gateway as the target with destination as “0.0.0.0/0”.

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-03a7a1d69dc2435f4	-	No

Add route

Cancel **Preview** **Save changes**

Updated routes for rtb-0f29514e1202e985f / 3-Tier_public_route successfully

Details

Route table ID rtb-0f29514e1202e985f	Main No	Explicit subnet associations 2 subnets	Edge associations -
VPC vpc-07c6fe43aed182858 3-Tier_VPC	Owner ID 467953945382		

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-03a7a1d69dc2435f4	Active	No
10.0.0.0/16	local	Active	No

Now create the Private Route Table with name and necessary tags.

You have successfully updated subnet associations for rtb-0f29514e1202e985f / 3-Tier_public_route.

Route tables (1/3) info

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
5-Tier_public_route	rtb-0f29514e1202e985f	2 subnets	-	No	vpc-07c6fe43aed182858 3-Ti...	467953945382
3-Tier_private_route	rtb-0372678f984e9bd9d	-	-	No	vpc-07c6fe43aed182858 3-Ti...	467953945382
	rtb-0372678f984e9bd9d	-	-	Yes	vpc-07c6fe43aed182858 3-Ti...	467953945382

rtb-0372678f984e9bd9d / 3-Tier_private_route

Subnet associations

Explicit subnet associations (0)

Subnets without explicit associations (4)

Edit the subnet associations with the Private subnets of application tier and data tier.

VPC > Route tables > rtb-0372678f984e9bd9d > Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (4/6)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
app-1	subnet-0040c2fe59ff3fd33	10.0.3.0/24	-	Main (rtb-077715c625d99276)
data-2	subnet-08b015efbfccaa69f	10.0.6.0/24	-	Main (rtb-077715c625d99276)
data-1	subnet-09f7c3bf9c76db62c	10.0.5.0/24	-	Main (rtb-077715c625d99276)
app-2	subnet-028affadaffef72fb	10.0.4.0/24	-	Main (rtb-077715c625d99276)
web-2	subnet-06a5b0bcfe74b1acd	10.0.2.0/24	-	rtb-0f29514e1202e985f / 3-Tier_public_route
web-1	subnet-0e10c43f5b12b7897	10.0.1.0/24	-	rtb-0f29514e1202e985f / 3-Tier_public_route

Selected subnets

subnet-0040c2fe59ff3fd33 / app-1	subnet-08b015efbfccaa69f / data-2	subnet-09f7c3bf9c76db62c / data-1	subnet-028affadaffef72fb / app-2
----------------------------------	-----------------------------------	-----------------------------------	----------------------------------

Cancel **Save associations**

Edit the routes, add the NAT Gateway that we have created, as the target group with destination as “0.0.0.0/0”.

VPC dashboard X

EC2 Global View [New]

Filter by VPC: Select a VPC

Virtual private cloud

Your VPCs New

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Route tables (1/3) Info

Filter route tables

search: **vpc-07c6fe43aed182858** Clear filters

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Ov
3-Tier_public_route	rtb-0f29514e1202e985f	2 subnets	-	No	vpc-07c6fe43aed182858 3-Ti...	46
3-Tier_private_route	rtb-0372678f984e9bd9d	4 subnets	-	No	vpc-07c6fe43aed182858 3-Ti...	46
-	rtb-07f7715c625d99276	-	-	Yes	vpc-07c6fe43aed182858 3-Ti...	46

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Filter routes Both

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

VPC > Route tables > rtb-0372678f984e9bd9d > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	nat-010399da9eff9e9d5	-	No

Add route Cancel Preview Save changes

Step 5:

Create the RDS

We need a database for our server. For this we are using the Amazon RDS.

Go to RDS dashboard -> Create Database.

Choose the database creation method (we are choosing the “standard create”).

Select the Engine (we are using the MySQL). Select the template as “Free Tier”, provide the name for our database.

Create database

Choose a database creation method Info

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



MariaDB



PostgreSQL



Oracle



Microsoft SQL Server



Edition

MySQL Community



Known issues/limitations

Review the Known issues/limitations [Info](#) to learn about potential compatibility issues with specific database versions.

Hide filters

Show 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 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 8.0.32

Now create the credentials with username and strong password. In storage auto scaling, remove the storage auto scaling. Change the VPC from default to the VPC that we have created. Make the public access as NO. Create a new security group and select the availability zone. Now click on the create

Settings

DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

RDS-3-Tier

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username [Info](#)

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

Admin

1 to 16 alphanumeric characters. First character must be a letter.

Manage master credentials in AWS Secrets Manager

Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

 If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.

[Learn more](#) 

Auto generate a password

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

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).

Confirm master password [Info](#)

database

Instance configuration

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



Amazon RDS Optimized Writes - [new](#) [Info](#)

Show instance classes that support Amazon RDS Optimized Writes

DB instance class [Info](#)

- 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

Include previous generation classes

Storage

Storage type [Info](#)

General Purpose SSD (gp2)

Baseline performance determined by volume size

Allocated storage [Info](#)

200

GiB

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

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.

Connectivity [Info](#)



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.

3-Tier_VPC (vpc-07c6fe43aed182858)

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.

Create new DB Subnet Group

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

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

*Make sure that the availability zones for both the database and private instance are same.

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

3-Tier-RDS-SG

Availability Zone Info

us-east-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-2019 (default)

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

► Additional configuration

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.

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.

Monitoring

Monitoring

Enable Enhanced monitoring
Enabling Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU.

► Additional configuration

Database options, encryption turned on, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

Estimated monthly costs

The Amazon RDS Free Tier is available to you for 12 months. Each calendar month, the free tier will allow you to use the Amazon RDS resources listed below for free:

- 750 hrs of Amazon RDS in a Single-AZ db.t2.micro, db.t3.micro or db.t4g.micro Instance.
- 20 GB of General Purpose Storage (SSD).
- 20 GB for automated backup storage and any user-initiated DB Snapshots.

[Learn more about AWS Free Tier.](#)

When your free usage expires or if your application use exceeds the free usage tiers, you simply pay standard, pay-as-you-go service rates as described in the [Amazon RDS Pricing page](#).

ⓘ You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

[Cancel](#) [Create database](#)

Now select the database that we have created and go to the security groups and edit the inbound rules. Select the add rule with type as MySQL/Aurora and destination as 0.0.0.0/0 or the public instance security group that we are going to create later.

Connection setup successfully for RDS database rds-3-tier and EC2 instance i-03ff79c4ab6fd70d3

► Details

RDS > Databases > rds-3-tier

rds-3-tier

[Modify](#) [Actions ▾](#)

Summary			
DB identifier rds-3-tier	CPU <div style="width: 2.48%;">2.48%</div>	Status Available	Class db.t3.micro
Role Instance	Current activity <div style="width: 0%;">0 Connections</div>	Engine MySQL Community	Region & AZ us-east-1a

[Connectivity & security](#) [Monitoring](#) [Logs & events](#) [Configuration](#) [Maintenance & backups](#) [Tags](#)

Connectivity & security		
Endpoint & port Endpoint rds-3-tier.cfqzzk6znf0b.us-east-1.rds.amazonaws.com Port	Networking Availability Zone us-east-1a VPC	Security VPC security groups rds-e2-1 (sg-0a5ba6690013bc669) Active 3-Tier-RDS-SG (sg-00795a6d333ad8191) Inactive

Security Groups (1/2) Info

search: sg-00795a6d333ad8191 Clear filters

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count
-	sg-0d6aa283fb265f65	app1_SG	vpc-07c6fe43aed182858	app1_SG created 2023...	467953945382	4 Permission entries
<input checked="" type="checkbox"/>	sg-00795a6d333ad8191	3-Tier-RDS-SG	vpc-07c6fe43aed182858	Created by RDS manag...	467953945382	1 Permission entry

sg-00795a6d333ad8191 - 3-Tier-RDS-SG

Details Inbound rules Outbound rules Tags

Inbound rules (1/1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
<input checked="" type="checkbox"/>	sgr-070f521363829e0...	IPv4	MySQL/Aurora	TCP	3306	117.205.68.99/32

EC2 > Security Groups > sg-00795a6d333ad8191 - 3-Tier-RDS-SG > 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 <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
sgr-070f521363829e0b3	MySQL/Aurora	TCP	3306	Anywhere... <small>Info</small>	<input type="text"/> 0.0.0.0/0 <small>X</small>

Add rule Cancel Preview changes Save rules

New EC2 Experience Tell us what you think

Security Groups (1/12) Info

Filter security groups

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count
-	sg-0d6aa283fb265f69	rds-e2-1	vpc-07c6fe43aed182858	Security group attache...	467953945382	1 Permission entr...
<input checked="" type="checkbox"/>	sg-00795a6d333ad8191	3-Tier-RDS-SG	vpc-07c6fe43aed182858	Created by RDS manag...	467953945382	1 Permission entr...
-	sg-02eb7049336e44f17	launch-wizard-3	vpc-072d21b69f1ab682	launch-wizard-3 create...	467953945382	1 Permission entr...

sg-00795a6d333ad8191 - 3-Tier-RDS-SG

Details Inbound rules Outbound rules Tags

Inbound rules (1/1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
<input checked="" type="checkbox"/>	sgr-070f521363829e0...	IPv4	MySQL/Aurora	TCP	3306	0.0.0.0/0

Step 6:

Create the EC2 instances

Creating the Public Server:

Go to Ec2 dashboard -> launch instance

Provide the name and tags. Select the AMI (Here, we are using the Ubuntu) and instance type. Give the keypair for the instance. Now, edit the Network settings. Select the VPC that we have created, public subnet that we have created for the presentation tier. Create the security group with ssh, http, https. Launch the instance.

Launch an instance Info

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 Info

Name Add additional tags

Application and OS Images (Amazon Machine Image) Info

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

Recents
Quick Start

S

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type
ami-007855ac798b5175e (64-bit (x86)) / ami-0c6c29c5125214c77 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Instance type Info

Instance type Free tier eligible

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 Create new key pair

Network settings Info

VPC - required Info
vpc-07c6fe43aeb182858 (3-Tier_VPC)
10.0.0.0/16

Subnet Info
VPC: vpc-07c6fe43aeb182858 Owner: 467953945382 Availability Zone: us-east-1a
IP addresses available: 249 CIDR: 10.0.1.0/24

Create new subnet

Auto-assign public IP Info
Enable

Firewall (security groups) Info

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

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
web_1_sg created 2023-04-07T09:23:15.235Z

Inbound security groups rules

Security group rule 1 (TCP, 22, 0.0.0.0/0)
 Type Info: ssh Protocol Info: TCP Port range Info: 22
 Source type Info: Anywhere
 Description - optional Info: e.g. SSH for admin desktop
 0.0.0.0/0

Security group rule 2 (TCP, 443, 0.0.0.0/0)
 Type Info: HTTPS Protocol Info: TCP Port range Info: 443
 Source type Info: Anywhere
 Description - optional Info: e.g. SSH for admin desktop
 0.0.0.0/0

Security group rule 3 (TCP, 80, 0.0.0.0/0)
 Type Info: HTTP Protocol Info: TCP Port range Info: 80

Summary

Number of instances Info

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-007855ac798b5175e

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, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel
Launch instance
Review commands

Cancel
Launch instance
Review commands

Create another public instance for load balancing.

[EC2 > Instances > Launch an instance](#)

Launch an instance Info

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 Info

Name Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

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

Recents
Quick Start

Amazon Linux
macOS
Ubuntu
Windows
Red Hat

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type
 ami-007855ac798b5175e (64-bit (x86)) / ami-0c6c29c5125214c77 (64-bit (Arm))
 Virtualization: hvm ENA enabled: true Root device type: ebs

Description
 Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-03-25

▼ Instance type Info

Instance type All generations

t2.micro Family: t2 1 vCPU 1 GiB Memory Free tier eligible

On-Demand Windows pricing: 0.0162 USD per Hour
 On-Demand SUSE pricing: 0.0116 USD per Hour
 On-Demand RHEL pricing: 0.0716 USD per Hour
 On-Demand Linux pricing: 0.0116 USD per Hour

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 Create new key pair

▼ Network settings Info

VPC - required

Subnet

Auto-assign public IP

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

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

▼ Summary

Number of instances Info

Software Image (AMI)
 Canonical, Ubuntu, 22.04 LTS, ...read more
 ami-007855ac798b5175e

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, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel
Launch instance
Review commands

Security group name - required
web_2_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
web_2_SG created 2023-04-07T09:23:13.233Z

Inbound security groups rules

- Security group rule 1 (TCP, 22, 0.0.0.0/0)**
 - Type Info: ssh
 - Protocol Info: TCP
 - Port range Info: 22
 - Source type Info: Anywhere
 - Description - optional Info: e.g. SSH for admin desktop
- Security group rule 2 (TCP, 443, 0.0.0.0/0)**
 - Type Info: HTTPS
 - Protocol Info: TCP
 - Port range Info: 443
 - Source type Info: Anywhere
 - Description - optional Info: e.g. SSH for admin desktop
- Security group rule 3 (TCP, 80, 0.0.0.0/0)**
 - Type Info: HTTP
 - Protocol Info: TCP
 - Port range Info: 80
 - Source type Info: Anywhere
 - Description - optional Info: e.g. SSH for admin desktop

Summary

Number of instances Info
1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...[read more](#)
ami-007855ac79865175e

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, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance Review commands

Step 7:

Creating the Private Server

Go to Ec2 dashboard -> launch instance

Provide the name and tags. Select the AMI (Here, we are using the Ubuntu) and instance type. Give the keypair for the instance. Now, edit the Network settings. Select the VPC that we have created, Private subnet that we have created for the presentation tier. *Make sure that the availability zones for both the database and private instance are same. Create the security group with inbound rules as, ssh and source as the public instance Security group, MySQL/Aurora with custom source type and RDS security group. Launch the instance.

Launch an instance [Info](#)

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 [Info](#)

Name Add additional tags

Application and OS Images (Amazon Machine Image) [Info](#)

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

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

Recent | Quick Start

Amazon Linux AWS macOS Ubuntu Windows Red Hat ...

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type
ami-007855ac798b5175e (64-bit (x86)) / ami-0c6c29c5125214c77 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description
Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-03-25

Architecture AMI ID
64-bit (x86) ami-007855ac798b5175e Verified provider

Summary

Number of instances [Info](#)
1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...[read more](#)
ami-007855ac798b5175e

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, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel **Launch instance** Review commands

Instance type [Info](#)

Instance type
t2.micro All generations

Family: t2 1 vCPU 1 GiB Memory
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0176 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour

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
vaishu26 [Create new key pair](#)

Network settings [Info](#)

VPC - required [Info](#)
vpc-07c6fe43aed182858 (3-Tier_VPC)
10.0.0.0/16

Subnet [Info](#)
subnet-0040c2fe59ff3fd33 app-1
VPC: vpc-07c6fe43aed182858 Owner: 467953945382 Availability Zone: us-east-1a
IP addresses available: 251 CIDR: 10.0.3.0/24

Create new subnet [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

Summary

Number of instances [Info](#)
1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...[read more](#)
ami-007855ac798b5175e

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, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel **Launch instance** Review commands

Security group name - required
app1_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
app1_SG created 2023-04-08T05:37:50.843Z

Inbound security groups rules

- ▼ Security group rule 1 (TCP, 22, sg-03b448e3a5c3930fb)

Type Info	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Source Info	Description - optional Info
Custom	<input type="text" value="Q, Add CIDR, prefix list or security"/>	e.g. SSH for admin desktop
<input type="text" value="sg-03b448e3a5c3930fb"/> X		
- ▼ Security group rule 2 (TCP, 3306, sg-00795a6d333ad8191)

Type Info	Protocol Info	Port range Info
MySQL/Aurora	TCP	3306
Source type Info	Source Info	Description - optional Info
Custom	<input type="text" value="Q, Add CIDR, prefix list or security"/>	e.g. SSH for admin desktop
<input type="text" value="sg-00795a6d333ad8191"/> X		

Add security group rule

► Advanced network configuration

▼ Configure storage Info Advanced

1x GiB gp2 ▾ Root volume (Not encrypted)

Create another instance with same configuration for load balancing and auto scaling.

Step 8:

Setup the connection for RDS and Private Instance

RDS > Databases > Set up EC2 connection

Step 1 Set up EC2 connection

Step 2 Review and confirm

Set up EC2 connection Info

Select EC2 instance

Database rds-3-tier

EC2 instance

Choose the EC2 instance to connect to this database. Only EC2 instances in the same VPC as the database are shown. If no EC2 instances in the same VPC are available, you can create a new EC2 instance.

i-03ff79c4ab6fd70d3	▼	
3-Tier_app1 us-east-1a		

Create EC2 instance [\[\]](#)

Cancel Continue

Step 9:

Connecting to the Public Server

Get connected to the public instance using ssh.

**Connect to instance** Info

Connect to your instance i-0129a3e989cc2f523 (3-Tier_Web1) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

 [i-0129a3e989cc2f523 \(3-Tier_Web1\)](#)

Public IP address

 [54.147.39.183](#)

User name

Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ubuntu.

Note: In most cases, the default user name, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

[Cancel](#)[Connect](#)

Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-1031-aws x86_64)

- * Documentation: <https://help.ubuntu.com>
- * Management: <https://landscape.canonical.com>
- * Support: <https://ubuntu.com/advantage>

System information as of Fri Apr 7 12:38:40 UTC 2023

```
System load: 0.0205078125      Processes:          97
Usage of /: 20.4% of 7.57GB    Users logged in:     0
Memory usage: 22%              IPv4 address for eth0: 10.0.1.84
Swap usage: 0%
```

* Ubuntu Pro delivers the most comprehensive open source security and compliance features.

<https://ubuntu.com/aws/pro>

* Introducing Expanded Security Maintenance for Applications. Receive updates to over 25,000 software packages with your Ubuntu Pro subscription. Free for personal use.

<https://ubuntu.com/aws/pro>

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates. See <https://ubuntu.com/esm> or run: sudo pro status

i-0129a3e989cc2f523 (3-Tier_Web1)

Public IPs: 54.147.39.183 Private IPs: 10.0.1.84

In the presentation tier, we are going to deploy the user interface to which the user can interact with the backend. For this we are going to deploy the web application code in the public instance. To run any application, we need to install its related servers. For demo purpose we are going to run the PHP application so we need to install an apache server.

Follow the commands to install the apache server and PHP.

1. sudo apt update
2. sudo apt install apache2
3. sudo apt install php libapache2-mod-php php-mysql

```
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Apr  7 12:37:23 2023 from 157.48.200.8
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-1-84:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [108 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:6 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [728 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [147 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [9020 B]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [701 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [109 kB]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [576 B]
Get:13 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [716 kB]
Get:14 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [118 kB]
Get:15 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [14.2 kB]
Get:16 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [19.4 kB]
Get:17 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [4068 B]
```

i-0129a3e989cc2f523 (3-Tier_Web1)

PublicIPs: 54.147.39.183 PrivateIPs: 10.0.1.84

```

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Apr  7 12:37:23 2023 from 157.48.200.8
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-1-84:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [108 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:6 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [728 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [147 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [9020 B]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [701 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [109 kB]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [576 B]
Get:13 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [716 kB]
Get:14 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [118 kB]
Get:15 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [14.2 kB]
Get:16 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [19.4 kB]
Get:17 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [4068 B]
```

i-0129a3e989cc2f523 (3-Tier_Web1)

PublicIPs: 54.147.39.183 PrivateIPs: 10.0.1.84

```

12 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-10-0-1-84:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1 libaprutil1-db-sqlite3 libaprutil1-ldap liblua5.3-0 mailcap mime-support ssl-cert
Suggested packages:
apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser bzip2-doc
The following NEW packages will be installed:
apache2 apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1 libaprutil1-db-sqlite3 libaprutil1-ldap liblua5.3-0 mailcap mime-support ssl-cert
0 upgraded, 13 newly installed, 0 to remove and 12 not upgraded.
Need to get 2138 kB of archives.
After this operation, 8505 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapr1 amd64 1.7.0-8ubuntu0.22.04.1 [108 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1 amd64 1.6.1-Subuntu4.22.04.1 [92.6 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-db-sqlite3 amd64 1.6.1-Subuntu4.22.04.1 [11.3 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-ldap amd64 1.6.1-Subuntu4.22.04.1 [9168 B]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 liblua5.3-0 amd64 5.3.6-1build1 [144 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-bin amd64 2.4.52-lubuntu4.4 [1345 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-data all 2.4.52-lubuntu4.4 [165 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-utils amd64 2.4.52-lubuntu4.4 [89.5 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 mailcap all 3.70+mulubuntul [23.8 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 mime-support all 3.66 [3696 B]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2 amd64 2.4.52-lubuntu4.4 [97.8 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 bzip2 amd64 1.0.8-5build1 [34.8 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 ssl-cert all 1.1.2 [17.4 kB]
Fetched 2138 kB in 0s (20.3 MB/s)
Preconfiguring packages ...
Selecting previously unselected package libapr1:amd64.
(Reading database ... 63657 files and directories currently installed.)
```

i-0129a3e989cc2f523 (3-Tier_Web1)

PublicIPs: 54.147.39.183 PrivateIPs: 10.0.1.84

```
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36.1-4build1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-10-0-1-84:~$
```

i-0129a3e989cc2f523 (3-Tier_Web1)
PublicIPs: 54.147.39.183 PrivateIPs: 10.0.1.84

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-10-0-1-84:~$ sudo apt install php libapache2-mod-php php-mysql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libapache2-mod-php8.1 php-common php8.1-cli php8.1-common php8.1-mysql php8.1-opcache php8.1-readline
Suggested packages:
php-pear
The following NEW packages will be installed:
libapache2-mod-php libapache2-mod-php8.1 php php-common php-mysql php8.1 php8.1-cli php8.1-common php8.1-mysql php8.1-opcache php8.1-readline
0 upgraded, 11 newly installed, 0 to remove and 12 not upgraded.
Need to get 5262 kB of archives.
After this operation, 21.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 php-common all 2:92ubuntul [12.4 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 php8.1-common amd64 8.1.2-1ubuntu2.11 [1126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 php8.1-opcache amd64 8.1.2-1ubuntu2.11 [365 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 php8.1-readline amd64 8.1.2-1ubuntu2.11 [13.5 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 php8.1-cli amd64 8.1.2-1ubuntu2.11 [1833 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapache2-mod-php8.1 amd64 8.1.2-1ubuntu2.11 [1765 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 libapache2-mod-php8.1 amd64 8.1.2-1ubuntu2.11 [2898 B]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 php8.1 all 8.1.2-1ubuntu2.11 [9150 B]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 php all 2:8.1+92ubuntul [2756 B]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 php8.1-mysql amd64 8.1.2-1ubuntu2.11 [130 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 php-mysql all 2:8.1+92ubuntul [1834 B]
Fetched 5262 kB in 0s (37.7 MB/s)
Selecting previously unselected package php-common.
(Reading database ... 64426 files and directories currently installed.)
Preparing to unpack .../00-php-common_2%3a92ubuntul_all.deb ...
Unpacking php-common (2:92ubuntul) ...
```

i-0129a3e989cc2f523 (3-Tier_Web1)
PublicIPs: 54.147.39.183 PrivateIPs: 10.0.1.84

```
Setting up php8.1-cli (8.1.2-1ubuntu2.11) ...
update-alternatives: using /usr/bin/php8.1 to provide /usr/bin/php (php) in auto mode
update-alternatives: using /usr/bin/phar8.1 to provide /usr/bin/phar (phar) in auto mode
update-alternatives: using /usr/bin/phar.phar8.1 to provide /usr/bin/phar.phar (phar.phar) in auto mode

Creating config file /etc/php/8.1/cli/php.ini with new version
Setting up libapache2-mod-php8.1 (8.1.2-1ubuntu2.11) ...

Creating config file /etc/php/8.1/apache2/php.ini with new version
Module mpm event disabled.
Enabling module mpm_prefork.
apache2_switch mpm Switch to prefork
apache2_invoke: Enable module php8.1
Setting up php8.1 (8.1.2-1ubuntu2.11) ...
Setting up libapache2-mod-php (2:8.1+92ubuntul) ...
Setting up php (2:8.1+92ubuntul) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for php8.1-cli (8.1.2-1ubuntu2.11) ...
Processing triggers for libapache2-mod-php8.1 (8.1.2-1ubuntu2.11) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

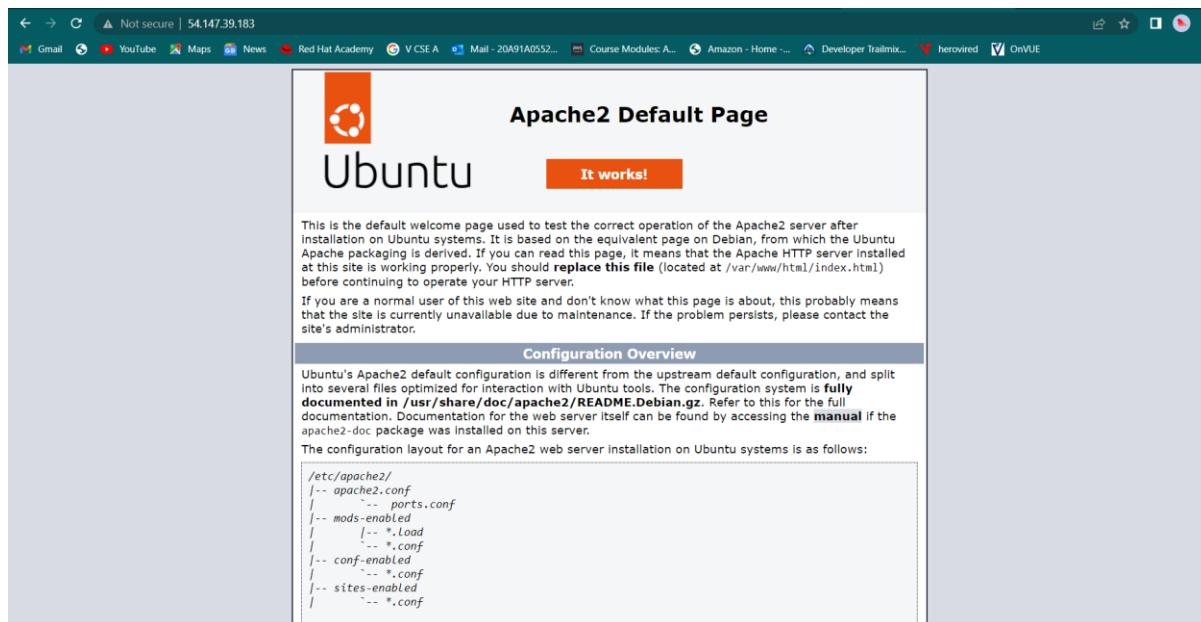
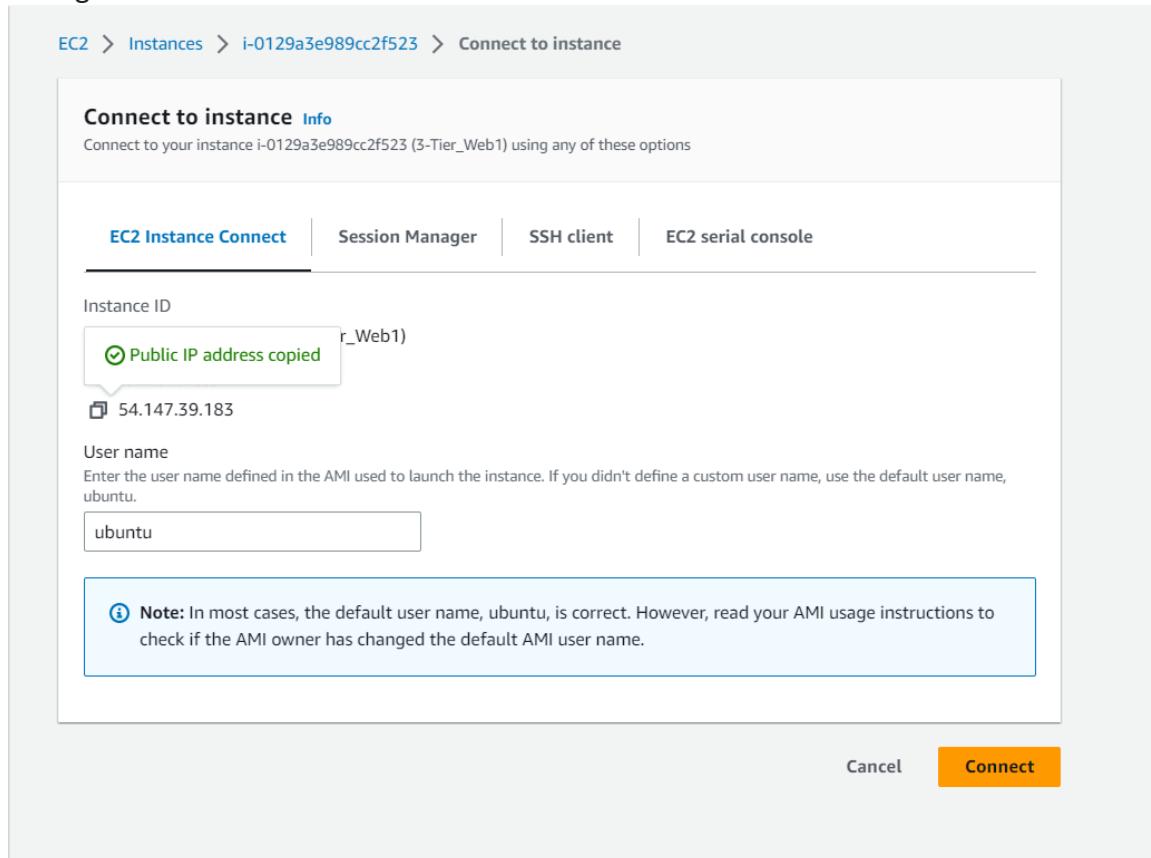
No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-10-0-1-84:~$
```

i-0129a3e989cc2f523 (3-Tier_Web1)
PublicIPs: 54.147.39.183 PrivateIPs: 10.0.1.84

Now open your web browser and type your public IP in my case again it is 54.147.39.183 and you must see the below Apache2 Ubuntu Default Page. This means we have installed Apache on the Ubuntu server and it is working fine.



Now, whenever a user goes to your web app the Apache server will return HTML files; that means index.html. So we are going to replace the html code in the index.html with our application's login page code.

Now we are going to write the login page program that displays the login template and host it on our server. The following are the commands for that.

1. cd /var/www/html

2. sudo nano index.html

```
[root@ip-10-0-1-84 ~]# cd /var/www/html
[root@ip-10-0-1-84 /var/www/html]# ls
index.html
[root@ip-10-0-1-84 /var/www/html]# sudo nano index.html
[root@ip-10-0-1-84 /var/www/html]#
```

The code that we are using here is,

```
1  <!DOCTYPE html>
2  <html>
3
4  <head>
5      <title>Login Page</title>
6      <style>
7          form {
8              margin-top: 3%;
9              margin-bottom: 7%;
10         }
11
12         h1 {
13             margin-top: 10%;
14         }
15
16         div {
17             border: 2px solid black;
18             width: 40%;
19             margin-top: 15%;
20             background-color: white;
21         }
22
23         .ss {
24             background-image: url(cookiesimg.png);
25             background-repeat: none;
26             background-size: cover;
27         }
28
29         .trans {
30             margin-right: 7%;
31             background: transparent;
32             width: 350px;
33             padding: 30px;
34             box-sizing: border-box;
35             border-radius: 20px;
36             transition: transform .5s;
37             box-sizing: border-box;
38
39             -transition: transform .5s,
40             box-sizing: border-box;
41             border-radius: 20px;
42             transition: transform .5s;
43             box-sizing: border-box;
44             border-radius: 20px;
45             transition: transform .5s;
46             box-shadow: 5px 5px 8px;
47         }
48
49         .trans:hover {
50             transform: scale(1.10);
51         }
52
53         .dd {
54             color: white;
55         }
56
57         .inputs {
58             background: transparent;
59         }
60     </style>
61
62 </head>
63
64 <body class="ss">
65     <center>
66         <div class="trans">
67             <h1 style="color: black;">LOGIN</h1>
68             <form action="authenticate.php" method="post">
69                 <label for="username" class="dd"><b>Username:</b></label>
70                 <input type="text" id="username" name="username" required style="border-radius: 5%; height: 25px; color: black;" class="inputs"><br><br>
71                 <label for="password" class="dd"><b>Password:</b></label>
72                 <input type="password" id="password" name="password" required style="border-radius: 5%; height: 25px; color: black;" class="inputs"><br><br>
73                 <input type="submit" value="Submit" style="background-color: antiquewhite; color: black; height: 30px; border-radius: 20px;">
74             </form>
75         </div>
76     </center>
77 </body>
78 </html>
```

Now write this code and press CTRL+O and CTRL+X.

Upload the necessary images that are required for the website by using the git and move them to the /var/www/html

aws Services Search [Alt+S]

```

ubuntu@ip-10-0-1-84:/var/www/html$ cd ~
ubuntu@ip-10-0-1-84:~$ git
usage: git [--version] [--help] [-C <path>] [-c <name>=<value>]
           [-e <exec-path[=<path>]] [--html-path] [--man-path] [--info-path]
           [-p | --paginate | -P | --no-pager] [--no-replace-objects] [--bare]
           [--git-dir=<path>] [--work-tree=<path>] [--namespace=<name>]
           [--super-prefix=<path>] [--config-env=<name>=<envvar>]
           <command> [<args>]

These are common Git commands used in various situations:

start a working area (see also: git help tutorial)
  clone      Clone a repository into a new directory
  init       Create an empty Git repository or reinitialize an existing one

work on the current change (see also: git help everyday)
  add        Add file contents to the index
  mv         Move or rename a file, a directory, or a symlink
  restore    Restore working tree files
  rm         Remove files from the working tree and from the index

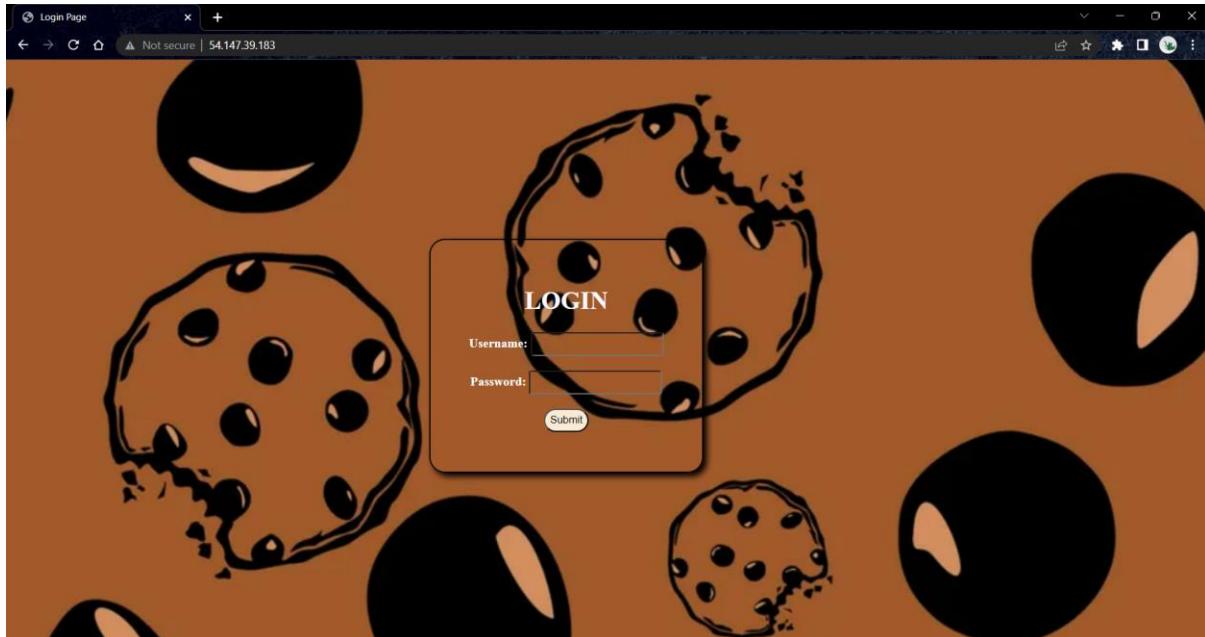
examine the history and state (see also: git help revisions)
  bisect     Use binary search to find the commit that introduced a bug
  diff       Show changes between commits, commit and working tree, etc
  grep       Print lines matching a pattern
  log        Show commit logs
  show      Show various types of objects
  status     Show the working tree status

grow, mark and tweak your common history
  branch    List, create, or delete branches
  commit    Record changes to the repository

i-0129a3e989cc2f523 (3-Tier_Web1)
PublicIPs: 54.147.39.183 PrivateIPs: 10.0.1.84

'git help -a' and 'git help -g' list available subcommands and some
concept guides. See 'git help <command>' or 'git help <concept>'
to read about a specific subcommand or concept.
See 'git help git' for an overview of the system.
ubuntu@ip-10-0-1-84:~$ git clone https://github.com/aakash-namala/img.git
Cloning into 'img'...
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 6 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (6/6), 358.45 KiB | 23.90 MiB/s, done.
ubuntu@ip-10-0-1-84:~$ ls
img
ubuntu@ip-10-0-1-84:~$ cd /var/www/html
ubuntu@ip-10-0-1-84:/var/www/html$ ls
index.html
ubuntu@ip-10-0-1-84:/var/www/html$ cd ~
ubuntu@ip-10-0-1-84:~$ cd img
ubuntu@ip-10-0-1-84:~/img$ ls
README.md  cookiesimg.png
ubuntu@ip-10-0-1-84:~/img$ sudo cp cookiesimg.png /var/www/html/cookiesimg.png
ubuntu@ip-10-0-1-84:~/img$ cd /var/www/html
ubuntu@ip-10-0-1-84:/var/www/html$ ls
cookiesimg.png  index.html
ubuntu@ip-10-0-1-84:/var/www/html$ 
```

Now go to your web browser and enter your public IP and you must see the login page.
(In our case, the login page looks like this)



Step 10:

Connecting to the Private server.

Now we are going to deploy the database in the private instance, so that it can be accessible only by the authorized users.

To get connected to the private instance, we are using the public instance as a intermediate.

We must need a keypair to connect the instance. So, create a nano file that contains a keypair. After creating a file, change its permissions using the command chmod.

```
ubuntu@ip-10-0-1-84:~$ ls  
ubuntu@ip-10-0-1-84:~$ sudo nano key.pem
```

Now use the keypair and ssh and get connected to private instance.

```
ubuntu@ip-10-0-1-84:~$ sudo nano key.pem
ubuntu@ip-10-0-1-84:~$ ssh -i "key.pem" ubuntu@10.0.3.92
The authenticity of host '10.0.3.92 (10.0.3.92)' can't be established.
ED25519 key fingerprint is SHA256:5110BKjKP+fInPMNn07xn2IlhFfK4+V/kAT0IhD4Jug.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.92' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-1031-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Fri Apr  7 13:17:00 UTC 2023

System load:  0.0          Processes:           94
Usage of /:   20.4% of 7.57GB  Users logged in:  0
Memory usage: 21%          IPv4 address for eth0: 10.0.3.92
Swap usage:   0%

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-3-92:~$ █
```

i-0129a3e989cc2f523 (3-Tier_Web1)
PublicIPs: 54.147.39.183 PrivateIPs: 10.0.1.84

Now use the command, sudo apt update

```

ubuntu@ip-10-0-3-92:~$ ls
ubuntu@ip-10-0-3-92:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [108 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [990 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [210 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [13.9 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [744 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [115 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [576 B]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [899 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [180 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [18.6 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [24.1 kB]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [6312 B]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [444 B]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [40.6 kB]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [9800 B]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [388 B]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 B]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [20.3 kB]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [14.4 kB]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [480 B]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [728 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [147 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [9020 B]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [701 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [109 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [576 B]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [716 kB]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [118 kB]
Get:39 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [14.2 kB]
Get:40 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [19.4 kB]
Get:41 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [4068 B]
Get:42 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [228 B]
Fetched 26.6 MB in 5s (5681 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
12 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-10-0-3-92:~$ 

```

i-0129a3e989cc2f523 (3-Tier_Web1)

PublicIPs: 54.147.39.183 PrivateIPs: 10.0.1.84

Step 11:

Connecting to Database

Now use the command, “sudo apt install mysql-client” to interact with the mysql server.

```

ubuntu@ip-10-0-3-92:~$ sudo apt install mysql-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  mysql-client-8.0 mysql-client-core-8.0 mysql-common
The following NEW packages will be installed:
  mysql-client mysql-client-8.0 mysql-client-core-8.0 mysql-common
0 upgraded, 4 newly installed, 0 to remove and 12 not upgraded.
Need to get 2716 kB of archives.
After this operation, 62.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 mysql-client-core-8.0 amd64 8.0.32-0ubuntu0.22.04.2 [2677 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 mysql-common all 5.8+1.0.8 [7212 B]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 mysql-client-8.0 amd64 8.0.32-0ubuntu0.22.04.2 [22.7 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 mysql-client all 8.0.32-0ubuntu0.22.04.2 [9350 B]
Fetched 2716 kB in 0s (35.5 MB/s)
Selecting previously unselected package mysql-client-core-8.0.
(Reading database ... 63657 files and directories currently installed.)
Preparing to unpack .../mysql-client-core-8.0_8.0.32-0ubuntu0.22.04.2_amd64.deb ...
Unpacking mysql-client-core-8.0 (8.0.32-0ubuntu0.22.04.2) ...
Selecting previously unselected package mysql-common.
Preparing to unpack .../mysql-common_5.8+1.0.8_all.deb ...
Unpacking mysql-common (5.8+1.0.8) ...
Selecting previously unselected package mysql-client.
Preparing to unpack .../mysql-client_8.0.32-0ubuntu0.22.04.2_all.deb ...
Unpacking mysql-client (8.0.32-0ubuntu0.22.04.2) ...
Setting up mysql-common (5.8+1.0.8) ...
update-alternatives: using /etc/mysql/my.cnf.fallback to provide /etc/mysql/my.cnf (my.cnf) in auto mode
Selecting previously unselected package mysql-client-core-8.0.
(Reading database ... 63657 files and directories currently installed.)
Preparing to unpack .../mysql-client-core-8.0_8.0.32-0ubuntu0.22.04.2_amd64.deb ...
Unpacking mysql-client-core-8.0 (8.0.32-0ubuntu0.22.04.2) ...
Selecting previously unselected package mysql-common.
Preparing to unpack .../mysql-common_5.8+1.0.8_all.deb ...
Unpacking mysql-common (5.8+1.0.8) ...
Selecting previously unselected package mysql-client-8.0.
Preparing to unpack .../mysql-client-8.0_8.0.32-0ubuntu0.22.04.2_amd64.deb ...
Unpacking mysql-client-8.0 (8.0.32-0ubuntu0.22.04.2) ...
Selecting previously unselected package mysql-client.
Preparing to unpack .../mysql-client_8.0.32-0ubuntu0.22.04.2_all.deb ...
Unpacking mysql-client (8.0.32-0ubuntu0.22.04.2) ...
Setting up mysql-common (5.8+1.0.8) ...
update-alternatives: using /etc/mysql/my.cnf.fallback to provide /etc/mysql/my.cnf (my.cnf) in auto mode
Setting up mysql-client-core-8.0 (8.0.32-0ubuntu0.22.04.2) ...
Setting up mysql-client-8.0 (8.0.32-0ubuntu0.22.04.2) ...
Setting up mysql-client (8.0.32-0ubuntu0.22.04.2) ...
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-10-0-3-92:~$ 
```

i-0129a3e989cc2f523 (3-Tier_Web1)

PublicIPs: 54.147.39.183 PrivateIPs: 10.0.1.84

Connect to MySQL using the command “mysql -h endpoint -u username -p”.

We can get the endpoint in the database dashboard.

Endpoint	Availability Zone	Security
rds-3-tier.cfqzzk6zmf0.us-east-1.rds.amazonaws.com	us-east-1a	VPC security groups rds-ec2-1 (sg-045ba6690013bc669) 3-Tier-RDS-SG (sg-00795a6d333ad8191)
Port	VPC	Active
3306	Subnet group	Publicly accessible No
	default-vpc-07c6fe43aed182858	

```
ubuntu@ip-10-0-3-92:~$ mysql -h rds-3-tier.cfqzzk6znf0b.us-east-1.rds.amazonaws.com -u Admin -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 33
Server version: 8.0.32 Source distribution

copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> [REDACTED]
```

i-0129a3e989cc2f523 (3-Tier_Web1)
PublicIPs: 54.147.39.183 PrivateIPs: 10.0.1.84

We successfully connected to our database.

Now create a database and use it. After creating add the data to our database.

```
mysql> create database detailsDB;
Query OK, 1 row affected (0.01 sec)

mysql> use detailsDB
Database changed
mysql> [REDACTED]

mysql> use detailsDB
Database changed
mysql> create table detailsTable(
    -> username varchar(20),
    -> password varchar(20));
Query OK, 0 rows affected (0.05 sec)

mysql> show tables;
+-----+
| Tables_in_detailsDB |
+-----+
| detailsTable        |
+-----+
1 row in set (0.01 sec)

mysql> [REDACTED]
```

Insert data into database

```
mysql> insert into detailsTable(username,password) values("cookies","57");
Query OK, 1 row affected (0.01 sec)

mysql> select * from detailsTable;
+-----+-----+
| username | password |
+-----+-----+
| cookies  | 57      |
+-----+-----+
1 row in set (0.00 sec)

mysql> [REDACTED]
```

Go back to public server

```

mysql> exit
Bye
ubuntu@ip-10-0-3-92:~$ exit
logout
Connection to 10.0.3.92 closed.
ubuntu@ip-10-0-1-84:~$ cd /var/www/html
ubuntu@ip-10-0-1-84:/var/www/html$ ls
cookiesimg.png index.html
ubuntu@ip-10-0-1-84:/var/www/html$ 

```

We have created our login page in the public instance and made it available to the users. Then we have created a database and deployed it in the private instance.

Whenever the clients or the users access the login page and enter the details, it must check with the database which is in private server. The authentication code will check whether the user is authorized or unauthorized. And only the authorized users can be able to access the data. For this we are adding the authentication code in the public server.

```

ubuntu@ip-10-0-1-84:/var/www/html$ sudo nano authenticate.php
ubuntu@ip-10-0-1-84:/var/www/html$ 

```

Add the following code and press CTRL+O and CTRL+X

```

1  <?php
2  // Retrieve user input
3  $username = $_POST['username'];
4  $password = $_POST['password'];
5
6  // Connect to RDS
7  $servername = "<your-rds-endpoint>";
8  $db_username = "<your-db-username>";
9  $db_password = "<your-db-password>";
10 $dbname = "<your-db-name>";
11 $conn = new mysqli($servername, $db_username, $db_password, $dbname);
12
13 // Check connection
14 if ($conn->connect_error) {
15     die("Connection failed: " . $conn->connect_error);
16 }
17
18 // Prepare SQL statement
19 $stmt = $conn->prepare("SELECT * FROM users WHERE username=? AND password=?");
20 $stmt->bind_param("ss", $username, $password);
21 $stmt->execute();
22 $result = $stmt->get_result();
23
24 // Check if user exists
25 if ($result->num_rows > 0) {
26     echo "Welcome " . $username . "!";
27 } else {
28     echo "Invalid username or password.";
29 }
30
31 // Close connection
32 $stmt->close();
33 $conn->close();
34 ?>

```

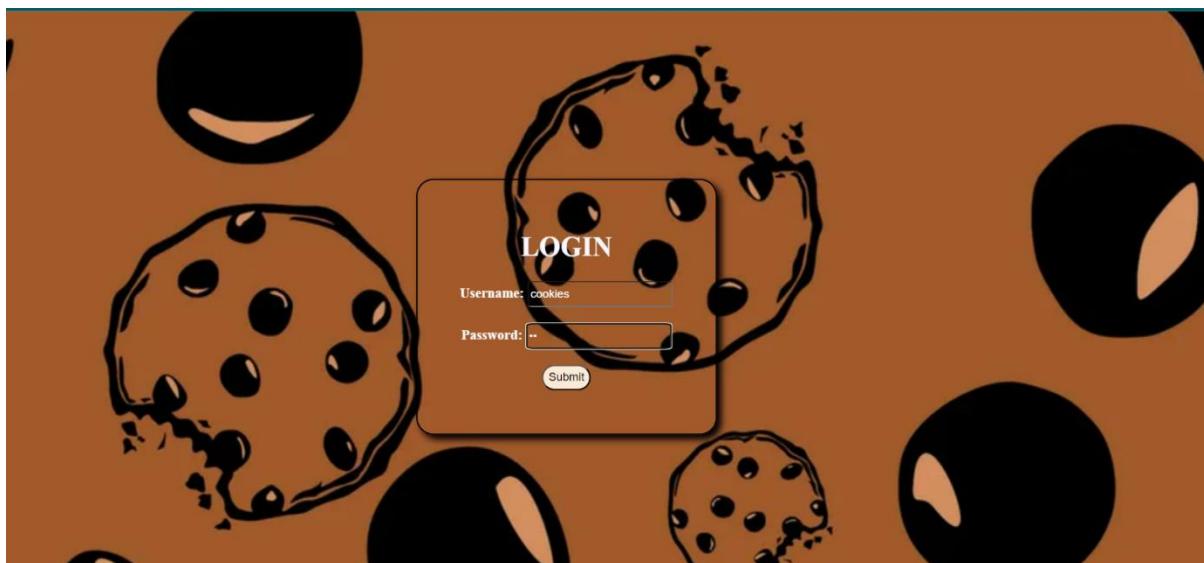
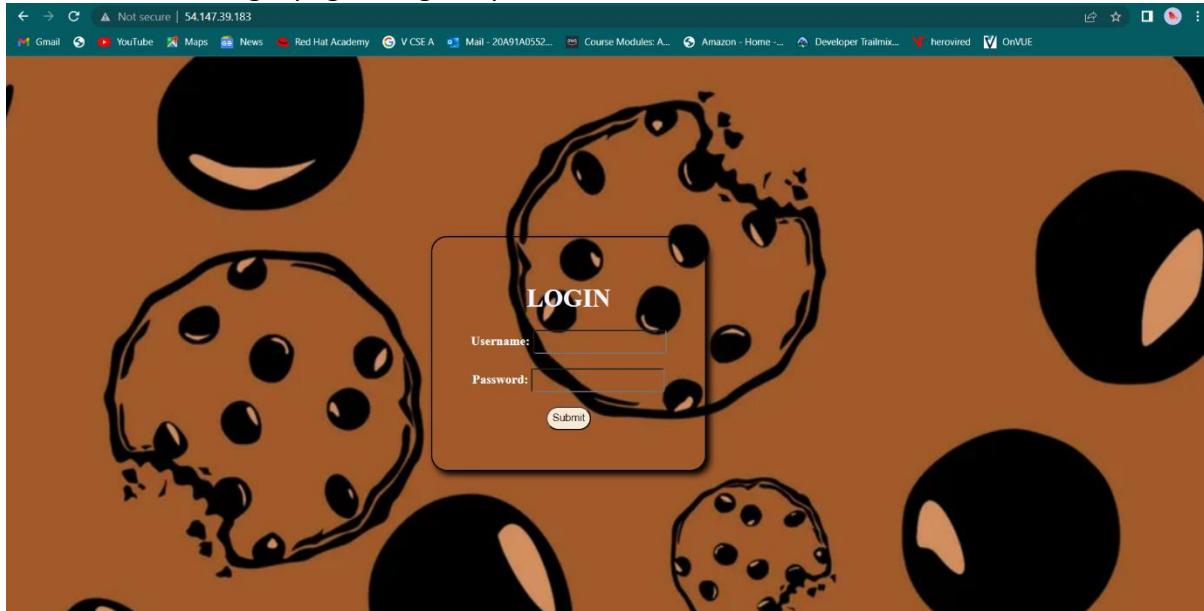
Now we need to add authenticate.php in /etc/apache2/mods-enabled/dir.conf

That's how we deploy the web application in the server.

Proof of Concept:

We have successfully deployed the web application into the cloud.

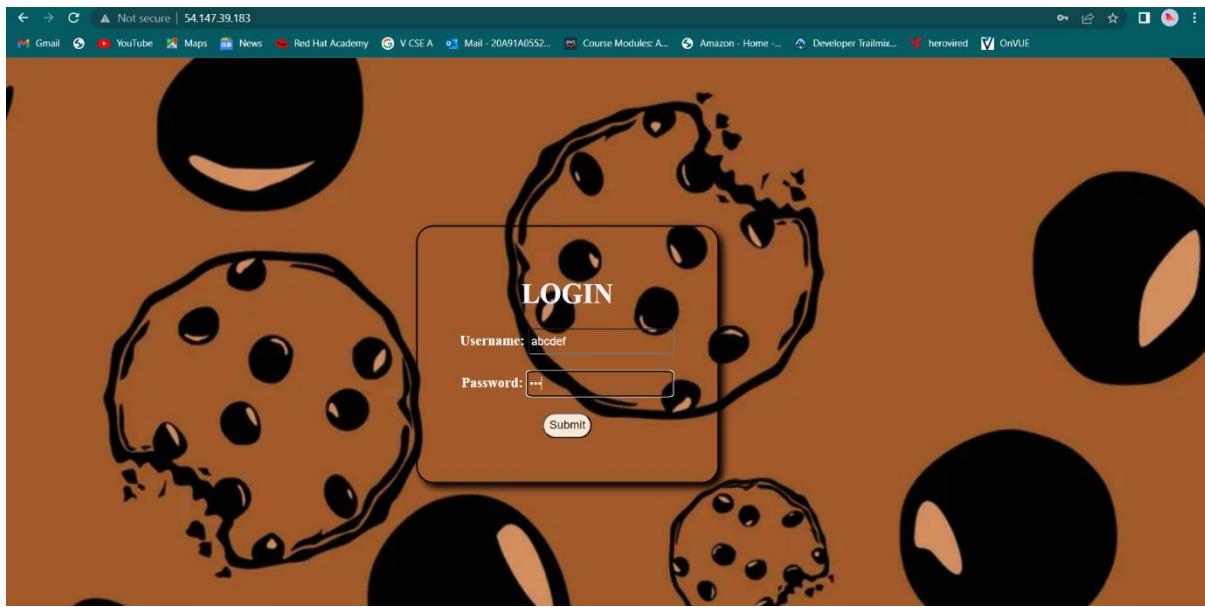
Now, access the login page using the public IP in the browser.



Click the Submit button after entering the credentials.



Invalid details



Click the Submit button after entering the credentials.



Invalid username or password.

Autoscaling and load balancing

Now, we are going to add auto scaling and load balancing, which works as the application tier, we have to create an image from required instance

A screenshot of the AWS Management Console, specifically the EC2 Instances page. On the left, there is a navigation sidebar with various options like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images, AMIs, and AMI Catalog. The main content area shows a table of instances. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Availability Zone. Two instances are listed: "3-Tier_Web1" (Instance ID i-0129a3e989cc2f523) and "3-Tier_Web2" (Instance ID i-07fa91d4e31bb7042). Both instances are shown as "Running". The "Actions" dropdown menu for the first instance contains options like "Connect", "View details", "Manage instance state", "Create image", "Create template from instance", and "Launch more like this". The "Create image" option is highlighted with a blue border. The "Details" tab is selected for the first instance, showing detailed information such as Public IPv4 address (54.147.39.183), Private IP4 address (10.0.1.84), Instance type (t2.micro), and VPC ID (vpc-07c6fe43aed182858).

EC2 > Instances > i-0129a3e989cc2f523 > Create image

Create image Info

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

Instance ID
i-0129a3e989cc2f523 (3-Tier_Web1)

Image name
image_from_web

Maximum 127 characters. Can't be modified after creation.

Image description - optional
image_from_web

Maximum 255 characters

No reboot
 Enable

Instance volumes

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/sda1	Create new snapshot from volume	8	EBS General Purpose S...	100		<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

Add volume

No reboot
 Enable

Instance volumes

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/sda1	Create new snapshot from volume	8	EBS General Purpose S...	100		<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

Add volume

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

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

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

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

No tags associated with the resource.

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

Create image

AWS Services Search [Alt+S]

Amazon Machine Images (AMIs) (1/1) **Info**

Owned by me	Find AMI by attribute or tag	Actions	Launch instance from AMI				
<input checked="" type="checkbox"/>	Name	AMI ID	AMI name	Source	Owner	Visibility	Status
<input checked="" type="checkbox"/>	-	ami-09a891d5483f8aeb2	image_from_web1	467953945382/image_from_web1	467953945382	Private	Available

AMI ID: ami-09a891d5483f8aeb2

Details	Permissions	Storage	Tags
AMI ID ami-09a891d5483f8aeb2	Image type machine	Platform details Linux/UNIX	Root device type EBS
AMI name image_from_web1	Owner account ID 467953945382	Architecture x86_64	Usage operation RunInstances
Root device name /dev/sda1	Status Available	Source 467953945382/image_from_web1	Virtualization type hvm
Boot mode -	State reason -	Creation date Fri Apr 07 2023 21:02:44 GMT+0530 (India Standard Time)	Kernel ID -

We have to create a launch template

Create launch template

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

Launch template name and description

Launch template name - required

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

Template version description

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](#)

Summary

Software Image (AMI)

-

Virtual server type (instance type)

-

Firewall (security group)

-

Storage (volumes)

-

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, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Create launch template

Launch template contents

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

Launch template contents

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

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI 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

Recents My AMIs Quick Start

Don't include in launch template

Owned by me

Shared with me



Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

image_from_web1
ami-09a891d5483f8aeb2
2023-04-07T15:32:44.000Z Virtualization: hvm ENA enabled: true Root device type: ebs

Summary

Software Image (AMI)

-

Virtual server type (instance type)

-

Firewall (security group)

-

Storage (volumes)

-

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, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Create launch template

Description

image_from_web1

Architecture

AMI ID

x86_64

ami-09a891d5483f8aeb2

Instance type [Info](#)

Advanced

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour

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

vaishu26

[Create new key pair](#)

Summary

Software Image (AMI)

image_from_web1
ami-09a891d5483f8aeb2

Virtual server type (instance type)

t2.micro

Firewall (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, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Create launch template

Network settings

Subnet Info

subnet-0e1cc43f5812b7897 web-1
VPC: vpc-07c6fe43aed182858 Owner: 467953945382 Availability Zone: us-east-1a IP addresses available: 248 CIDR: 10.0.1.0/24

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 (radio button selected) or Create security group.

Common security groups Info

Select security groups: web-1_SG sg-03b448e3a5c3930fb X
VPC: vpc-07c6fe43aed182858

Show all selected (+1)

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

Advanced network configuration

Storage (volumes)

1 volume(s) - 8 GiB

Summary

Software Image (AMI)
image_from_web1 ami-09a891d5483f8aeb2

Virtual server type (instance type)
t2.micro

Firewall (security group)
2 security groups

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, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Create launch template

New EC2 Experience Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Launch Templates

- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Scheduled Instances
- Capacity Reservations

Images

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

EC2 > Launch templates

Launch templates (1/1) Info

Launch template ID	Launch template name	Default version	Latest version	Create time
lt-0f3af4bf9e717102e	temp_from_web1	1	1	2023-04-02

temp_from_web1 (lt-0f3af4bf9e717102e)

Launch template details

Launch template ID	Launch template name	Default version	Owner
lt-0f3af4bf9e717102e	temp_from_web1	1	arn:aws:iam::467953945382:root

Details **Versions** **Template tags**

Launch template version details

After launching a template we have to create autoscaling group

Step 1

Choose launch template or configuration

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

Name

Auto Scaling group name
Enter a name to identify the group.
3-Tier_AG

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

Launch template Switch to launch configuration

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

temp_from_web1

Create a launch template

Version

Default (1)

Create a launch template version

Description

temp_from_web1

Launch template

temp_from_web1 lt-0f3af4bf9e717102e

Instance type

t2.micro

Step 6 - optional
Add tags

Step 7
Review

Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

[Create a launch template](#) [Info](#)

Version

[Create a launch template version](#) [Info](#)

Description temp_from_web1	Launch template temp_from_web1 Info lt-0f3af4bf9e717102e	Instance type t2.micro
AMI ID ami-09a891d5483f8aeb2	Security groups -	Request Spot Instances No
Key pair name vaishu26	Security group IDs sg-03b448e3a5c3930fb Info sg-02873647d3bae7466 Info	

Additional details

Storage (volumes) -	Date created Fri Apr 07 2023 21:04:24 GMT+0530 (India Standard Time)
------------------------	--

Step 3 - optional
Configure advanced options

Step 4 - optional
Configure group size and scaling policies

Step 5 - optional
Add notifications

Step 6 - optional
Add tags

Step 7
Review

Network [Info](#)

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

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

[Create a VPC](#) [Info](#)

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

us-east-1a | subnet-0e1cc43f5812b7897 (web-1) [X](#)
10.0.1.0/24

us-east-1b | subnet-06a5bcfe74b1ac8d (web-2) [X](#)
10.0.2.0/24

[Create a subnet](#) [Info](#)

Instance type requirements [Info](#)

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

Launch template temp_from_web1 Info lt-0f3af4bf9e717102e	Version Default	Description temp_from_web1
Instance type t2.micro		

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template or configuration

Step 2
Choose instance launch options

Step 3 - optional
Configure advanced options

Step 4 - optional
Configure group size and scaling policies

Step 5 - optional
Add notifications

Step 6 - optional
Add tags

Step 7
Review

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.

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](#) [Info](#)

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.

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 [Info](#)

- Turn on Elastic Load Balancing health checks
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.
- 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

[Cancel](#) [Skip to review](#) [Previous](#) [Next](#)

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1 Choose launch template or configuration

Step 2 Choose instance launch options

Step 3 - optional Configure advanced options

Step 4 - optional Configure group size and scaling policies

Step 5 - optional Add notifications

Step 6 - optional Add tags

Step 7 Review

Configure group size and scaling policies - optional [Info](#)

Set the desired, minimum, and maximum capacity of your Auto Scaling group. You can optionally add a scaling policy to dynamically scale the number of instances in the group.

Group size - optional [Info](#)

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

Desired capacity

Minimum capacity

Maximum capacity

Scaling policies - optional

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. [Info](#)

Target tracking scaling policy Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.

None

Instance scale-in protection - optional

[Cancel](#) [Skip to review](#) [Previous](#) [Next](#)

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1 Choose launch template or configuration

Step 2 Choose instance launch options

Step 3 - optional Configure advanced options

Step 4 - optional Configure group size and scaling policies

Step 5 - optional Add notifications

Step 6 - optional Add tags

Step 7 Review

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 notification](#)

[Cancel](#) [Skip to review](#) [Previous](#) [Next](#)

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template or configuration

Step 2
Choose instance launch options

Step 3 - optional
Configure advanced options

Step 4 - optional
Configure group size and scaling policies

Step 5 - optional
Add notifications

Step 6 - optional
Add tags

Step 7
Review

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

Scaling policy

No scaling policy

Instance scale-in protection

Instance scale-in protection
 Enable instance protection from scale in

Step 5: Add notifications

Notifications

No notifications

Step 6: Add tags

Tags (0)

Key	Value	Tag new instances
No tags		

Cancel Previous Create Auto Scaling group

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

Target Groups

EC2 > Auto Scaling groups

Auto Scaling groups (1) Info

Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
3-Tier_AG	temp_from_web1 Version Default	2	-	2	1	3	us-east-1a, us-east-1b

0 Auto Scaling groups selected

Select an Auto Scaling group

Create an Auto Scaling group

Once the Auto Scaling Group(ASG) is created successfully ,then the desired instances will be created by the ASG.

The screenshot shows the AWS Auto Scaling Groups page. The main table lists one Auto Scaling group named "3-Tier_AG" with the following details:

Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
3-Tier_AG	temp_from_web1 Version Default	2	-	2	1	3	us-east-1a, us-east-1b

Below the table, the "Instance management" tab is selected. It displays two instances:

Instance ID	Lifecycle	Instance type	Weighted capacity	Launch template/c...	Availability Zone	Health status	Protected from
i-02f46745faf57c3bc	InService	t2.micro	-	temp_from_web1 Ver: us-east-1a	us-east-1a	Healthy	
i-0c5bf28a97aa1870e	InService	t2.micro	-	temp_from_web1 Ver: us-east-1b	us-east-1b	Healthy	

The screenshot shows the AWS Instances page. The main table lists six instances across three availability zones:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
3-Tier_app1	i-03f7f9acab6fd70d3	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	-	-	-	-
-	i-02f46745faf57c3bc	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	-	-	-	-
3-Tier_app2	i-03d0d27e1c1d7721a	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	-	-	-	-
-	i-0c5bf28a97aa1870e	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	-	-	-	-
3-Tier_Web1	i-0129a3e989c2f523	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	-	54.147.39.183	-	-
3-Tier_Web2	i-07fa91d4e31bb7042	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	-	52.90.208.7	-	-

Connect to ec2(web-2)

Update the Server.

```
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-1031-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Fri Apr 7 16:27:20 UTC 2023

System load: 0.0      Processes:         95
Usage of /: 21.1% of 7.57GB  Users logged in: 0
Memory usage: 22%      IPv4 address for eth0: 10.0.2.159
Swap usage: 0%

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Apr 7 15:48:08 2023 from 18.206.107.29
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-2-159:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [108 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
```

```
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module authn_iframe.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized_error_pages.
Enabling conf other_vhosts_access_log.
Enabling conf security.
Enabling conf serve_cgi-bin.
Enabling site-000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Processing triggers for ufw (0.36.1-4ubuntu1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

ubuntu@ip-10-0-2-159:~$
```

```

Fetched 26.6 MB in 5s (5677 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
12 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-10-0-2-159:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
apache2-bin apache2-data apache2-utils bzip2 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.3-0 mailcap mime-support ssl-cert
Suggested packages:
apache2-mpm-prefork apache2-suexec-pristine | apache2-suexec-custom www-browser bzip2-doc
The following NEW packages will be installed:
apache2 apache2-bin apache2-data apache2-utils bzip2 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.3-0 mailcap mime-support ssl-cert
0 upgraded, 13 newly installed, 0 to remove and 12 not upgraded.
Need to get 2138 kB of archives.
After this operation, 8505 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapr1 amd64 1:7.0.0-Subuntu0.22.04.1 [150 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 libapr1 libapr1-dbd-sqlite3 libaprutil1 libaprutil1-ldap liblua5.3-0 mailcap mime-support ssl-cert [22.6 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-dbd-sqlite3 libaprutil1-ldap amd64 1:6.1-Subuntu4.22.04.1 [11.3 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-ldap amd64 1:6.1-Subuntu4.22.04.1 [9168 B]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 liblua5.3-0 amd64 5.3.6-1build1 [140 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-bin amd64 2.4.52-1ubuntu4.4 [1345 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-data all 2.4.52-1ubuntu4.4 [165 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-utils amd64 2.4.52-1ubuntu4.4 [89.5 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 mailcap all 3.70+nmu1ubuntu1 [23.8 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 mime-support all 3.66-1 [369 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2 amd64 2.4.52-1ubuntu4.4 [97.8 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 bzip2 amd64 1:0.0-Subuid1 [34.8 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 ssl-cert all 1.1.2 [17.4 kB]
Fetched 2138 kB in 0s (30.3 kB/s)
Preconfiguring packages...
Selecting previously unselected package libapr1:amd64.
(Reading database ... 63657 files and directories currently installed.)
Preparing to unpack .../00-libapr1_1.7.0-Subuntu0.22.04.1_amd64.deb ...
Unpacking libapr1:amd64 (1:7.0.0-Subuntu0.22.04.1) ...
Selecting previously unselected package libaprutil1:amd64.

```

i-07fa91d4e31b7042 (3-Tier_Web2)

PublicIPs: 52.90.208.7 PrivateIPs: 10.0.2.159

To create Elastic load balancer we have to create target group and security group.

Creating Target groups

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 cannot 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

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

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

Protocol	Port
----------	------

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

Protocol Port

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

Protocol version
 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

Health check path
Use the default path of "/" to ping the root, or specify a custom path if preferred.
 Up to 1024 characters allowed.

► Advanced health check settings

Health check path
Use the default path of "/" to ping the root, or specify a custom path if preferred.
 Up to 1024 characters allowed.

► Advanced health check settings

Attributes

ⓘ Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

► **Tags - optional**
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

Cancel **Next**

Now we have to register targets

Step 1
Specify group detailsStep 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 (4/6)						
Instance ID	Name	State	Security groups	Zone	Subnet ID	
i-03f794ab6fd70d3	3-Tier_app1	running	app1_5G, ec2-rcs-1	us-east-1a	subnet-0040c2f59ff3fd33	
<input checked="" type="checkbox"/> i-02f46745faf57c3bc		running	web-1_5G, web-2_5G	us-east-1a	subnet-0e1cc43f5812b7897	
i-020d2d7e1c1d72f2a	3-Tier_app2	running	app2_5G	us-east-1b	subnet-028affdafe72fb	
<input checked="" type="checkbox"/> i-0cfbf28a97aa1870e		running	web-1_5G, web-2_5G	us-east-1b	subnet-06a5bcbe74b1ac8d	
<input checked="" type="checkbox"/> i-0129a3e989cc2f523	3-Tier_Web1	running	web-1_5G	us-east-1a	subnet-0e1cc43f5812b7897	
<input checked="" type="checkbox"/> i-07fa91d4e31bb7042	3-Tier_Web2	running	web-2_5G	us-east-1b	subnet-06a5bcbe74b1ac8d	

4 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.
80
1-65535 (separate multiple ports with commas)

Include as pending below

4 selections are now pending below. Include more or register targets when ready.

Instance ID	Name	Health status	Port	Security groups	Zone	Subnet ID
i-01194396391a1d19d5	3-Tier_Web1	running	80	web-1_5G	us-east-1a	subnet-0e1cc43f5812b7897
<input checked="" type="checkbox"/> i-07fa91d4e31bb7042	3-Tier_Web2	running	80	web-2_5G	us-east-1b	subnet-06a5bcbe74b1ac8d

4 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.
80
1-65535 (separate multiple ports with commas)

Include as pending below

4 selections are now pending below. Include more or register targets when ready.

Review targets						
Targets (4)						
Remove	Health status	Instance ID	Name	Port	State	Security groups
X	Pending	i-02f46745faf57c3bc		80	running	web-1_5G, web-2_5G
X	Pending	i-0cfbf28a97aa1870e		80	running	web-1_5G, web-2_5G
X	Pending	i-0129a3e989cc2f523	3-Tier_Web1	80	running	web-1_5G
X	Pending	i-07fa91d4e31bb7042	3-Tier_Web2	80	running	web-2_5G

4 pending

Create target group

Targets (4)	Ports for routing traffic to the selected instances. 80 1-65535 (separate multiple ports with commas)	Include as pending below
Register pending targets only?		
We noticed you have some selections that are not included as pending. If you want to include them in your target group, click Cancel to manage your selections. Otherwise, click Continue to register pending targets only.		
Cancel	Continue	

w targets

targets (4)

Health status	Instance ID	Name	Port	Security groups	Zone	Subnet ID
Pending	i-02f46745faf57c3bc		80	running	web-1_5G, web-2_5G	us-east-1a
Pending	i-0cfbf28a97aa1870e		80	running	web-1_5G, web-2_5G	us-east-1b
Pending	i-0129a3e989cc2f523	3-Tier_Web1	80	running	web-1_5G	us-east-1a
Pending	i-07fa91d4e31bb7042	3-Tier_Web2	80	running	web-2_5G	us-east-1b

The screenshot shows the AWS EC2 Target Groups console. A success message at the top says "Successfully created target group: 3-Tier-TG". Below it, the "Target groups" list shows one item: "3-Tier-TG" with ARN "arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/3-Tier-TG/07c6fe43aed182858". The "Registered targets" section shows four targets, each with a status of "unused":

- i-0c5bf28a97aa1870e
- i-07fe91d4e31bb7042
- i-02f46745fa57c3bc
- i-0129a3e989cc2f523

Now we have to create security group for load balancer.

Create security group

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: **3-Tier_ALB_SG**
 Description: **3-Tier_ALB_SG**
 VPC: **vpc-07c6fe43aed182858**

Inbound rules

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Anywhere-IPv4	0.0.0.0/0

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	0.0.0.0/0

Details

Security group name 3-Tier_ALB_SG	Security group ID sg-06c0532832891f3dc	Description 3-Tier_ALB_SG	VPC ID vpc-07cf043aed182858
Owner 467953945382	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules (1/1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sg-06c0532832891f3dc	IPv4	HTTP	TCP	80	0.0.0.0/0	-

Now we have to create Load balancer.

Load balancers

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

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created	Instance ID
No load balancers							
You don't have any load balancers in us-east-1							

0 load balancers selected

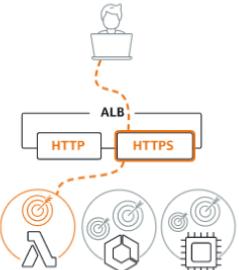
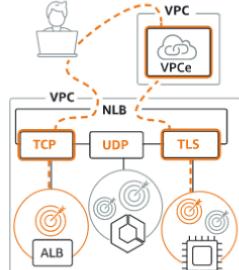
Select a load balancer above.

Create load balancer

Select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

Load balancer types

Application Load Balancer Info	Network Load Balancer Info	Gateway Load Balancer Info
		
Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers. Create	Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies. Create	Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls. Create

▶ [Classic Load Balancer - previous generation](#)

[Close](#)

[EC2](#) > [Load balancers](#) > [Create Application Load Balancer](#)

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 Elastic Load balancing works

Basic configuration

Load balancer name
Name must be unique within your AWS account and cannot be changed after the load balancer is created.
3-Tier-ALB
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme [Info](#)
Scheme cannot be changed after the load balancer is created.

Internet-facing
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

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

IP address type [Info](#)
Select the type of IP addresses that your subnets use.

IPv4
Recommended for internal load balancers.

Dualstack
Includes IPv4 and IPv6 addresses.

Network mapping [Info](#)

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

VPC [Info](#)
Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

3-Tier_VPC vpc-07cfe43aed182858 IPv4: 10.0.0.0/16	Edit
---	----------------------

Network mapping [Info](#)

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

VPC [Info](#)

Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

3-Tier_VPC
vpc-07c6fe43aed182858
IPv4: 10.0.0.0/16



Mappings [Info](#)

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

us-east-1a (use1-az4)

Subnet

subnet-0e1cc43f5812b7897 web-1 ▾

IPv4 settings

Assigned by AWS

us-east-1b (use1-az6)

Subnet

subnet-06a5bcbfe74b1ac8d web-2 ▾

IPv4 settings

Assigned by AWS

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer.

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer.

Security groups

Select up to 5 security groups



Create new security group

3-Tier_ALB_SG sg-06c0532832891f5dc X
VPC: vpc-07c6fe43aed182858

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](#)

Forward to

3-Tier-TG

HTTP ▾



1-65535

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

You can add up to 50 more tags.

Add listener

▼ Add-on services - optional

Additional AWS services can be integrated with this load balancer at launch. You can also add these and other services after your load balancer is created by reviewing the "Integrated Services" tab for the selected load balancer.

AWS Global Accelerator [Info](#)

Add-on services - optional
Additional AWS services can be integrated with this load balancer at launch. You can also add these and other services after your load balancer is created by reviewing the "Integrated Services" tab for the selected load balancer.

AWS Global Accelerator Info
 Create an accelerator to get static IP addresses and improve the performance and availability of your applications. [Additional charges apply](#)

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

Summary
Review and confirm your configurations. [Estimate cost](#)

Basic configuration Edit	Security groups Edit	Network mapping Edit	Listeners and routing Edit
3-Tier_ALB • Internet-facing • IPv4	• 3-Tier_ALB_SG sg-06c0532832891f3dc	VPC vpc-07c6fe43aed182858 3-Tier_VPC • us-east-1a subnet-0e1cc43f5812b7897 web-1 • us-east-1b subnet-06a5bcbe74b1ac8d web-2	• HTTP:80 defaults to 3-Tier-TG
Add-on services Edit	Tags Edit	None	
Attributes Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.			

Cancel **Create load balancer**

Check the status of targets.

EC2 > Target groups

Target groups (1/1) [Info](#)

Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
3-Tier-TG	arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/3-Tier-TG/01234567890123456789	80	HTTP	Instance	3-Tier ALB	vpc-07c6fe43aed182858

Target group: 3-Tier-TG

[Details](#) **Targets** [Monitoring](#) [Health checks](#) [Attributes](#) [Tags](#)

Registered targets (4)

Instance ID	Name	Port	Zone	Health status	Health status details
i-0c5bf28a97aa1870e		80	us-east-1b	Initial	Target registration is in progress
i-07ff91d4e31bb7042	3-Tier_Web2	80	us-east-1b	Initial	Target registration is in progress
i-0246745ef17c5b0c		80	us-east-1a	Initial	Target registration is in progress
i-0129a3c969c2f523	3-Tier_Web1	80	us-east-1a	Initial	Target registration is in progress

Targets statuses are Healthy.

Screenshot of the AWS EC2 Target groups interface showing a single target group named "3-Tier-TG".

Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
3-Tier-TG	arn:aws:elasticloadbalancing:us-east-1:147953945382:loadbalancer/app/3-Tier-ALB/9bf0d4b48e3022dd	80	HTTP	Instance	3-Tier-ALB	vpc-07c6fe43aed182858

Target group: 3-Tier-TG

Registered targets (4)

Instance ID	Name	Port	Zone	Health status	Health status details
i-0c5bf28b97aa1870e	3-Tier_Web2	80	us-east-1b	healthy	
i-07fa21d4c31b67042	3-Tier_Web2	80	us-east-1b	healthy	
i-02f46745fa5f7c3bc	3-Tier_Web1	80	us-east-1a	healthy	
i-0129a3e089c2f523	3-Tier_Web1	80	us-east-1a	healthy	

Copy the DNS in Elastic load balance.

Screenshot of the AWS EC2 Load balancers interface showing a single load balancer named "3-Tier-ALB".

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
3-Tier-ALB	3-Tier-ALB-1740531511.us-east-1.elb.amazonaws.com	Active	vpc-07c6fe43aed182858	2 Availability Zones	application	April 7, 2023, 22:21 (UTC+05:30)

Load balancer: 3-Tier-ALB

Details

Details

Load balancer type: Application

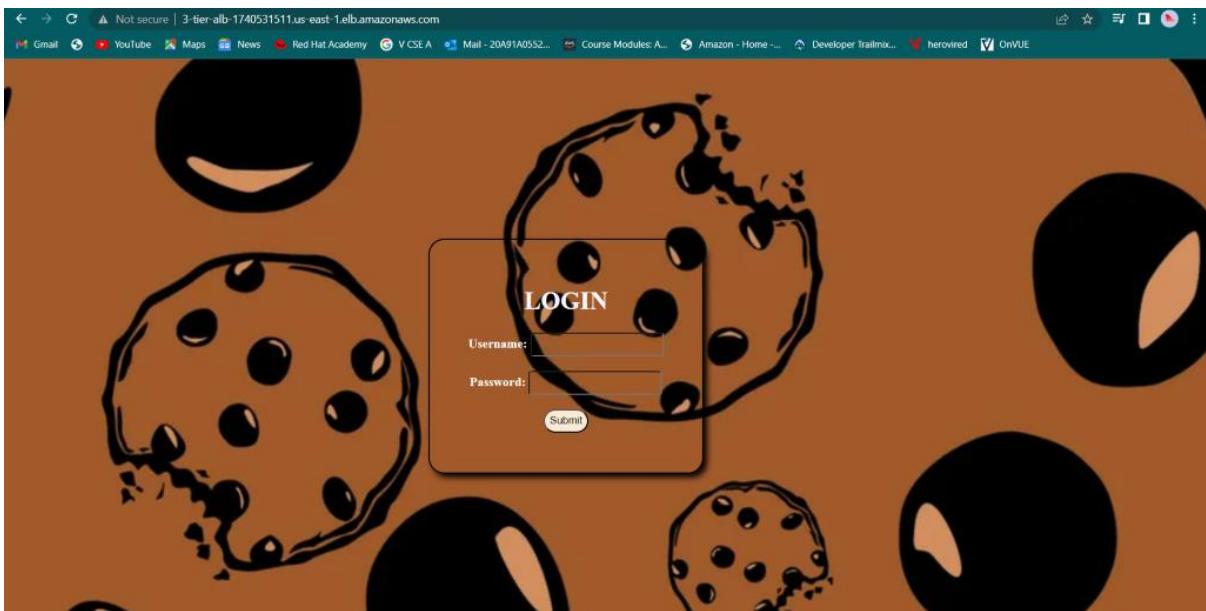
DNS name copied: 3-Tier-ALB-1740531511.us-east-1.elb.amazonaws.com (A Record)

Status: Active

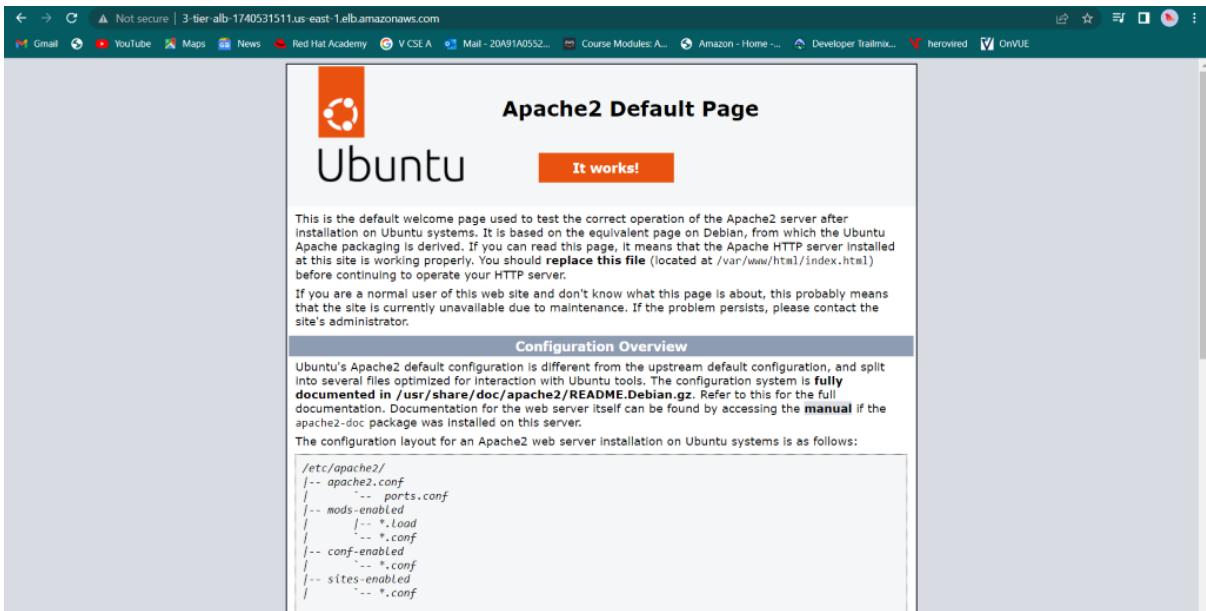
VPC: vpc-07c6fe43aed182858

We need to paste the DNS in any browser and run it, then we will get this output shown below.

This is output of web server-1



Reload the above page and we will get this page



Connect to the web-2 Server

Add the code to index.html

```
System load: 0.0          Processes:          101
Usage of /: 23.6% of 7.57GB  Users logged in:    0
Memory usage: 24%          IPv4 address for eth0: 10.0.2.159
Swap usage: 0%          

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

  https://ubuntu.com/aws/pro

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

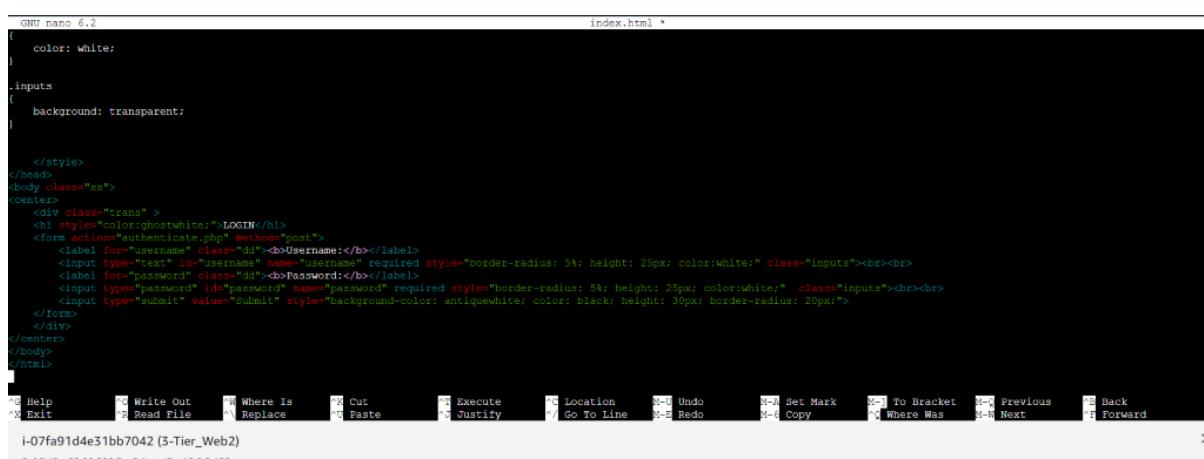
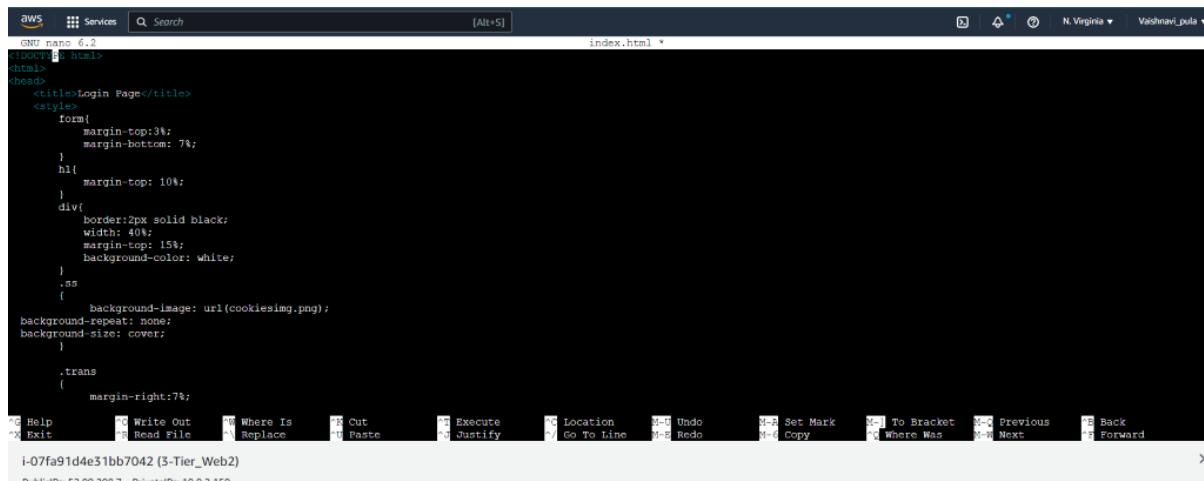
16 updates can be applied immediately.
12 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Fri Apr  7 16:27:21 2023 from 18.206.107.29
ubuntu@ip-10-0-2-159:~$ cd /var/www/html
ubuntu@ip-10-0-2-159:/var/www/html$ ls
index.html
ubuntu@ip-10-0-2-159:/var/www/html$ sudo nano index.html
ubuntu@ip-10-0-2-159:/var/www/html$ █
```

i-07fa91d4e31bb7042 (3-Tier_Web2)

Public IPs: 52.90.208.7 Private IPs: 10.0.2.159



Now establish connection between private web server(app2) and RDS.

The screenshot shows the Amazon RDS Databases page. On the left, there's a sidebar with various navigation options like Dashboard, Databases, Query Editor, etc. The main area shows a table of databases. One database, 'rds-3-tier', is selected. A context menu is open over this database, with 'Set up EC2 connection' highlighted. Other options in the menu include Reboot, Delete, Create read replica, and Create Aurora read replica. The database details show it's an Instance of MySQL Community, located in us-east-1a.

This is the 'Set up EC2 connection' step 1 page. It shows the selected database 'rds-3-tier'. Under 'EC2 instance', a dropdown menu lists an EC2 instance: 'i-020d2d7e1c1d72f2a' (3-Tier, app2, us-east-1b). There's a 'Create EC2 instance' button. At the bottom are 'Cancel' and 'Continue' buttons.

This is the 'Changes to EC2 instance' step 2 page. It shows a diagram where an RDS instance (rds-3-tier, Port: 3306) and an EC2 instance (i-020d2d7e1c1d72f2a) are connected via a VPC security group. Below the diagram, a note says 'Bold indicates an addition being made to set up a connection.' The table shows changes to the EC2 instance's security group:

Attribute	Current value	New value
Security group	app2_SG	app2_SG, ec2-rds-1

A warning message at the bottom states: 'Cross Availability Zone (AZ) charges might apply. The RDS database rds-3-tier (us-east-1a) and EC2 instance i-020d2d7e1c1d72f2a (us-east-1b) are in different AZs. Cross AZ charges might apply. Data transfer within same region'.

At the bottom are 'Cancel', 'Previous', and 'Confirm and set up' buttons.

Connection setup successfully for RDS database rds-3-tier and EC2 instance i-020d267e1c1d72f2a [2]

Details

RDS > Databases

Consider creating a Blue/Green Deployment to minimize downtime during upgrades
You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for changes to production databases. [RDS User Guide](#) [Aurora User Guide](#)

Databases

Group resources Modify Actions ▾ Restore from S3 Create database

DB identifier Role Engine Region & AZ Size Status Actions CPU Current activity Maintenance

rds-3-tier Instance MySQL Community us-east-1a db.t3.micro Available 3 Actions 2.59% 0 Connections none

Edit the security group rules of Private Ec2 and add MYSQL .

New EC2 Experience Tell us what you think

EC2 Dashboard EC2 Global View Events Tags Limits Instances Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Scheduled Instances Capacity Reservations Images Elastic Block Store Volumes Snapshots Lifecycle Manager Network & Security Security Groups

EC2 > Security Groups > sg-0cc2b17702c2467d3 - app2_SG

sg-0cc2b17702c2467d3 - app2_SG

Actions ▾

Details

Security group name: app2_SG Security group ID: sg-0cc2b17702c2467d3 Description: app2_SG created 2023-04-07T09:40:00.530Z VPC ID: vpc-07c6fe43aed182858

Owner: 467953945382 Inbound rules count: 3 Permission entries Outbound rules count: 1 Permission entry

Inbound rules | Outbound rules | Tags

You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer

Inbound rules (3)

Filter security group rules

Name	Type	Protocol	Port range	Source	Description
sgr-019b5dfce88f1f83	SSH	TCP	22	0.0.0.0/0	-
sgr-053561fffc2f3e167	HTTPS	TCP	443	0.0.0.0/0	-
sgr-0fbx9522991668a...	HTTP	TCP	80	0.0.0.0/0	-

EC2 > Security Groups > sg-0cc2b17702c2467d3 - app2_SG > 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-019b5dfce88f1f83	SSH	TCP	22	Custom <input type="button" value="Q"/> 0.0.0.0/0 <input type="button" value="X"/>	<input type="button" value="Delete"/>
sgr-053561fffc2f3e167	HTTPS	TCP	443	Custom <input type="button" value="Q"/> 0.0.0.0/0 <input type="button" value="X"/>	<input type="button" value="Delete"/>
-	HTTP	TCP	80	Custom <input type="button" value="Q"/> sg-02873647d3bae7466 <input type="button" value="X"/>	<input type="button" value="Delete"/>
-	MYSQL/Aurora	TCP	3306	Custom <input type="button" value="Q"/> sg-00795a6d5333ad8191 <input type="button" value="X"/>	<input type="button" value="Delete"/>

Add rule

New EC2 Experience Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

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

Images

Elastic Block Store

- Volumes
- Snapshots
- Lifecycle Manager

Network & Security

- Security Groups

Actions ▾

EC2 > Security Groups > sg-0cc2b17702c2467d3 - app2_SG

sg-0cc2b17702c2467d3 - app2_SG

Details

Security group name app2_SG	Security group ID sg-0cc2b17702c2467d3	Description app2_SG created 2023-04-07T09:40:00.530Z	VPC ID vpc-07c6fe43aed182852
Owner 467953945382	Inbound rules count 4 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags

You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#)

Inbound rules (4)

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-019b3dfdc08ff1f83	IPv4	SSH	TCP	22	0.0.0.0/0	-
<input type="checkbox"/>	-	sgr-0dec501e4397351...	-	MySQL/Aurora	TCP	3306	sg-00795a6d335ad81...	-
<input type="checkbox"/>	-	sgr-05561fdf12f5e167	IPv4	HTTPS	TCP	443	0.0.0.0/0	-
<input type="checkbox"/>	-	sgr-0517408fc2819b06	-	HTTP	TCP	80	sg-02873647d3bae74...	-

Connect to private server (app2) through the Public server(web2)

```
ubuntu@ip-10-0-2-159:~$ sudo nano key1.pem
```

```
aws Services Search [Alt+S] key.pem *
```

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAzGHLicjGdSYgx2Bw2rCLFKvTq3JeeRhEghWk0wXiYBbG
Hvv7zX2nVnbub2xhuagQ16rRn0WNrc1tqqJds6eWm8ax7yHd9w7vLGicitB
MoFf1NgZne67vvCn7t8Naovj1omw16cBav3A61tjjLBz-t-/pfnujTVONLCKX
cizatDUDBTF8NBGq5B
-----END RSA PRIVATE KEY-----

```
ubuntu@10.0.4.174: Permission denied (publickey).
ubuntu:~$ ip -10 -o 2-159-5 ssh -i "key1.pem" ubuntu@10.0.4.174
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-1031-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Fri Apr 7 17:36:11 UTC 2023

System load: 0.0          Processes: 95
Usage of /: 20.4% of 7.57GB Users logged in: 0
Memory usage: 21%          IPv4 address for eth0: 10.0.4.1
Swap usage: 0%             IPv6 address for eth0: fe80::500c:ff%eth0

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
see https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted
by applicable law.

i-07fa91d4e31bb7042 (3-Tier_Web2)
PublicIPs: 52.90.208.7 PrivateIPs: 10.0.2.159
```

Update the server.

```

the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-4-174:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [108 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [728 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [147 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [9020 B]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [701 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [990 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [210 kB]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [13.9 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [744 kB]
Get:19 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [109 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [115 kB]
Get:21 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [576 B]
Get:22 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [716 kB]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [576 B]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [899 kB]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [180 kB]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [18.6 kB]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [24.1 kB]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [6312 B]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [444 B]
```

Now install mysql-client.

```

Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [6312 B]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [444 B]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [40.6 kB]
Get:31 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [9800 B]
Get:32 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [388 B]
Get:33 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 Packages [116 B]
Get:34 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 Translation-en [20.3 kB]
Get:35 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Translation-en [114.4 kB]
Get:36 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [480 B]
Get:37 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [116 B]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [118 kB]
Get:39 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-security/universe amd64 Translation-en [14.2 kB]
Get:40 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [19.4 kB]
Get:41 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [4068 B]
Get:42 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [228 B]
Fetched 26.6 MB in 5s (5823 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
12 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-10-0-4-174:~$ sudo apt install mysql-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  mysql-client-8.0 mysql-client-core-8.0 mysql-common
The following NEW packages will be installed:
  mysql-client mysql-client-8.0 mysql-client-core-8.0 mysql-common
0 upgraded, 4 newly installed, 0 to remove and 12 not upgraded.
Need to get 2716 kB of archives.
After this operation, 5472 kB of additional disk space will be used.
[*****]
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 mysql-client-core-8.0 amd64 8.0.32-Ubuntu0.22.04.2 [2677 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 mysql-common all 5.0+1.0.0 [7212 B]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 mysql-client-8.0 amd64 8.0.32-Ubuntu0.22.04.2 [22.7 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 mysql-client all 8.0.32-Ubuntu0.22.04.2 [9350 B]
Fetched 2910 kB in 0s (22.2 MB/s)
Reading package lists...
mysql>
```

i-07fa91d4e31bb7042 (3-Tier_Web2)

PublicIPs: 52.90.208.7 PrivateIPs: 10.0.2.159

Connect to RDS .

```

ubuntu@ip-10-0-4-174:~$ mysql -h rds-3-tier.cfqzzk6znf0b.us-east-1.rds.amazonaws.com -u Admin -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 116
Server version: 8.0.32 Source distribution

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql>
```

i-07fa91d4e31bb7042 (3-Tier_Web2)

PublicIPs: 52.90.208.7 PrivateIPs: 10.0.2.159

Check for the changes made using private server-1(app1) are reflected here.

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

mysql> use detailsDB
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_detailsDB |
+-----+
| detailsTable         |
+-----+
1 row in set (0.00 sec)

mysql> select * from detailsTable;
+-----+-----+
| username | password |
+-----+-----+
| cookies  | 57      |
+-----+-----+
1 row in set (0.00 sec)

mysql>
```

i-07fa91d4e31bb7042 (3-Tier_Web2)

PublicIPs: 52.90.208.7 PrivateIPs: 10.0.2.159

The final output is as follows



Repository details:

The index.html, authenticate.php and the images required for the web application can be found in this repository.

<https://github.com/aakash-namala/3-tier web application deployment>

Outcomes:

We have successfully deployed the web application in the cloud.

Deploying a three-tier web application in the cloud can bring several outcomes, including:

Scalability: Cloud computing provides the ability to scale up or down resources on demand, allowing a three-tier web application to handle varying levels of traffic and user demand.

High availability: Cloud infrastructure offers high availability and redundancy through load balancing, automatic failover, and backup and recovery mechanisms, ensuring that the application is always accessible to users.

Cost-effectiveness: Cloud computing offers cost savings by eliminating the need for on-premises infrastructure and reducing operational expenses associated with maintaining hardware and software.

Flexibility: Cloud-based three-tier web applications can be easily modified or updated to meet changing business needs and user requirements.

Security: Cloud providers offer robust security measures and compliance certifications, which can ensure that the three-tier web application is protected against cyber-attacks and data breaches.

Collaboration: Cloud-based three-tier web applications provide a collaborative environment for development and operations teams, enabling them to work together more efficiently and effectively.

Overall, deploying a three-tier web application in the cloud can bring many advantages to organizations, including improved scalability, high availability, cost-effectiveness, flexibility, security, and collaboration. These outcomes can help organizations achieve their business objectives and deliver high-quality services to their users.

Conclusion:

The deployment of a three-tier web application in the cloud requires careful planning and execution to ensure a successful deployment. It involves designing and implementing the presentation layer, application layer, and data storage layer separately, ensuring they work together seamlessly. The use of appropriate technologies, such as load balancers, web servers, application servers, databases, and containerization, can facilitate the deployment process and provide scalability, high availability, and flexibility.

The project scope for a three-tier web application deployment in the cloud involves identifying the business requirements, designing the application architecture, selecting the appropriate technology stack, testing and debugging the application, and deploying it to the cloud environment. Documentation for the project should include the project objectives, architecture design, deployment process, testing results, and recommendations for future improvements.

The benefits of deploying a three-tier web application in the cloud include scalability, high availability, cost-effectiveness, flexibility, security, and collaboration. This architecture is widely adopted by organizations across various industries due to its maintainability, reusability, security, performance, and flexibility.

Overall, a well-planned and executed three-tier web application deployment in the cloud can bring significant benefits to an organization, such as improved user experience, increased productivity, reduced costs, and enhanced security. It is essential to follow industry best practices and utilize appropriate technologies to ensure a successful deployment and maximize the benefits of a three-tier web application in the cloud.

REFERENCES:

- Git Tutorial(<https://git-scm.com/docs>)
- AWS Documentation (<https://docs.aws.amazon.com/>)
- PHP Documentation (<https://www.php.net/manual/en/tutorial.php>)
- HTML and CSS Documentation (<https://devdocs.io/css/>)

For queries and details, contact:

Bhumika 20A91A0508@aec.edu.in

Aakash 20A91A0544@aec.edu.in

Vaishnavi 20A91A0552@aec.edu.in

Prudhvi 20A91A0576@aec.edu.in