

# **HOW TO: GUIDE TO GAIN FAMILIARITY WITH AWS**

**BY NUTAN SONALE**

**HOW TO:**

**GUIDE TO GAIN  
FAMILIARITY  
WITH AWS**

**BY NUTAN SONALE**

This short guide aims to give basic exercises that makes one familiar and curious with fundamental functionality of AWS services

nutan sonale  
[www.nutansonale.in](http://www.nutansonale.in)

# INDEX

1. Launch a linux and windows server by creating VPC, Route table
2. Create storage space using s3 services in cloud
3. Demonstrate Load balancer and Elastic IPs
4. Create new user from root using IAM
5. Create RDS server and connect using MySQL workbench
6. Run PHP code on EC2 instance that retrieve data from RDS server
7. Build own static website and hosting application
8. Demonstrate ECLIPSE integration with cloud
9. Run java application by connecting to RDS server
10. Demonstrate auto scaling group

# BASICS

Before starting doing anything, one should create an AWS root account. This will give access to was console via web browser. If the user wishes to do perform the tasks from CLI they have to configure their AWS CLI with the user token.

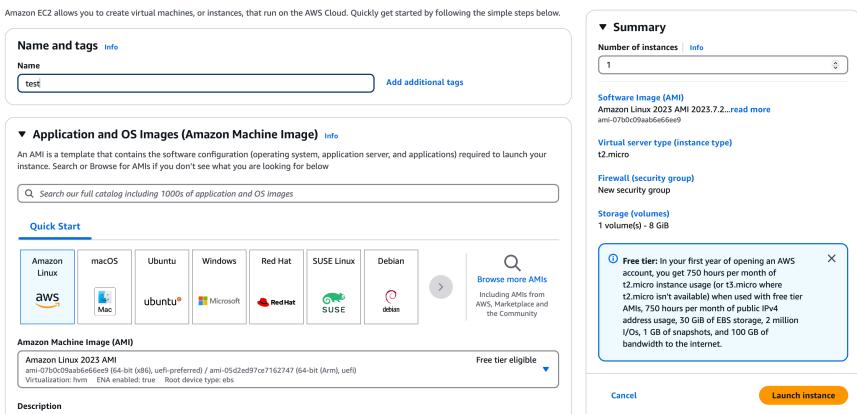
- Install AWS CLI package from [CLI Documentation page](#).
- After following the installation guide for your operating system you should be able to view the CLI version. For CLI options use command “`aws help`”

```
nutansonale@nutans-MacBook-Pro ~ % aws help
nutansonale@nutans-MacBook-Pro ~ % aws help
nutansonale@nutans-MacBook-Pro ~ % aws --version
aws-cli/2.27.7 Python/3.13.2 Darwin/24.1.0 exe/x86_64
nutansonale@nutans-MacBook-Pro ~ % █
```

1

# LAUNCH A LINUX AND WINDOWS SERVER WITH VPC AND ROUTE TABLE

1. At the top of console search bar type EC2 and this will lead to EC2 control panel.
  2. In navigation pane select **Instances**.
  3. choose **Launch Instances**
  4. Select OS type for linux select **Amazon linux 2023 AMI** and for windows select **Microsoft Windows server 2022 base**



5. Make sure you select t2.micro instance type and it shows free tier eligible.

6. For Linux VM you need to create key pairs for login via SSH. For windows you need to use RDP so you can login using the UI.

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

Q Search our full catalog including 1000s of application and OS Images

**Quick Start**

Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, Debian, > Browse more AMIs Including AMIs from AWS Marketplace and the Community

**Amazon Machine Image (AMI)**

Amazon Linux 2023 AMI ami-07bdc959ab6e6ed (64-bit (x86), uefi-preferred) / ami-05d2ed97e7162747 (64-bit (Arm), uefi) Free tier eligible

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Cancel Launch instance Random code

7. For creating a VPC with subnet and its route table, choose VPC in console search. Select **Create VPC**.

8. Under VPC settings sections choose **VPC and more** and for making the VPC available in multiple availability zones you need to select **Number of Availability Zone** as **2**, for Subnets we need **1 public subnet** and **1 private subnet**.

**Create VPC Info**

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

**VPC settings**

Resources to create **Info**  
Create only the VPC resource or the VPC and other networking resources.

VPC only  VPC and more

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

Auto-generate project

**IPv4 CIDR block Info**  
Determine the starting IP and the size of your VPC using CIDR notation.  
10.0.0.0/16 65,536 IP CIDR block must be between /16 and /28.

**IPv6 CIDR block Info**  
 No IPv6 CIDR block  
 Amazon-provided IPv6 CIDR block

**Tenancy Info**  
Default

**Preview**

**VPC show details**  
Your AWS Virtual network

project-vpc

**Subnets (4)**  
Subnets within this VPC

- us-west-2a
  - project-subnet-public1-us-west-2a
  - project-subnet-private1-us-west-2a
- us-west-2b
  - project-subnet-public2-us-west-2b
  - project-subnet-private2-us-west-2b

**Route table:**  
Route network tra

project-rtb-prv

9. We need 1 **NAT Gateway** and 1 **Internet Gateway**

10. If we want to access S3 buckets from the VPC we need to enable **VPC Endpoints**.

### Create VPC Info

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

The screenshot shows the 'Create VPC' interface. On the left, under 'VPC settings', there are sections for 'Name tag auto-generation', 'IPv4 CIDR block', and 'IPv6 CIDR block'. Under 'Name tag auto-generation', the 'Auto-generate' checkbox is checked, and the prefix 'project-' is selected. Under 'IPv4 CIDR block', the range '10.0.0.0/16' is specified, with '65,536 IP' available. Under 'IPv6 CIDR block', the 'No IPv6 CIDR block' option is selected. On the right, the 'Preview' section shows the 'VPC Show details' panel with 'Subnets (4)' listed: 'us-west-2a' (with subnets 'project-subnet-public1-us-west-2a' and 'project-subnet-private1-us-west-2a') and 'us-west-2b' (with subnets 'project-subnet-public2-us-west-2b' and 'project-subnet-private2-us-west-2b'). A 'Route table' panel is also visible.

11. The Subnets will be associated with route tables the public subnet should be routed to internet gateway as target, the private subnet should be routed to NAT gateway. The NAT gateway will be in public subnet all the traffic will be translated/transferred to internet gateway from NAT gateway. The inbound network to private subnet from the internet will be denied.

12. The EC2 instances should be assigned with these VPC configuration

13. After completing all these configuration add SSH and RPD ports to accept traffic from internet(all hosts).

14. After these changes launch the instances, once the instance status shows running you should be able to access the instance via SSH or RDP login.

# 2.

# CREATE STORAGE SPACE USING S3

1. Select S3 service in AWS console
2. Choose **Create Bucket**. Bucket names must be between 3 and 63 characters long and consist of only lowercase letters, numbers, or hyphens. The bucket name must be globally unique across all of Amazon S3, regardless of account or region, and cannot be changed after the bucket is created
3. In object ownership section select ACL(Access Control List)

The screenshot shows the AWS S3 Bucket Properties page for a bucket named 'reportbucket1235678'. The top navigation bar includes tabs for Objects, Properties (which is selected), Permissions, Metrics, Management, and Access Points. The main content area is divided into several sections:

- Bucket overview:** Shows the AWS Region (Asia Pacific (Sydney) ap-southeast-2), the Amazon Resource Name (ARN) (arn:aws:s3:::reportbucket1235678), and the Creation date (May 4, 2025, 14:30:39 (UTC+05:30)).
- Bucket Versioning:** Enabled. A note explains that versioning allows keeping multiple variants of an object in the same bucket, aiding recovery from user errors and application failures. A 'Learn more' link is provided.
- Multi-factor authentication (MFA) delete:** Disabled. A note states it requires MFA for changing settings and deleting objects. A 'Learn more' link is provided.
- Tags (0):** A table with columns for Key and Value, showing a single entry: 'No tags associated with this resource.'

4. Upload an object into the bucket, copy the URL of the object. Try accessing the object from web browser you will receive access denied.
5. To make the object publicly accessible first we have to disable the bucket policy for blocking all public access

6. Next we have to select the object and choose **Action** select **Make public via ACL**.

7. Then we can access the object via the URL without any authentication.

8. To maintain backup of old version of the object in bucket policies we have to enable versioning

The screenshot shows the AWS S3 Bucket Properties page for a bucket named "reportbucket1235678". The top navigation bar includes tabs for Objects, Properties (which is selected), Permissions, Metrics, Management, and Access Points. The main content area is divided into several sections:

- Bucket overview**: Shows the AWS Region as Asia Pacific (Sydney) ap-southeast-2, the Amazon Resource Name (ARN) as arn:aws:s3:::reportbucket1235678, and the Creation date as May 4, 2025, 14:30:39 (UTC+05:30). There is an "Edit" button for the ARN.
- Bucket Versioning**: Describes versioning as a means of keeping multiple variants of an object in the same bucket. It states that you can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. A link to "Learn more" is provided. The status is set to "Enabled".
- Multi-factor authentication (MFA) delete**: Describes MFA delete as an additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. It provides links to "Learn more" and "Edit". The status is set to "Disabled".
- Tags (0)**: Allows users to track storage costs and organize buckets. A link to "Learn more" is provided. The table shows "Key" and "Value" columns, both currently empty. A note indicates "No tags associated with this resource". An "Edit" button is located at the top right of this section.

# 3.

## DEMONSTRATE LOAD BALANCER AND ELASTIC IP

- 
1. Create two EC2 instances as shown in chapter 1 with VPC configuration. While creation of EC2 in the field of **user data** in **Advance details** section paste the below code.

```
#!/bin/sh
yum -y install httpd php
chkconfig httpd on
systemctl start httpd.service
cd /var/www/html
wget https://us-west-2-tcprod.s3.amazonaws.com/courses/spl-03/
v4.3.23.prod-5c8094c0/scripts/examplefiles-elb.zip
unzip examplefiles-elb.zip
```

requests. Applications or agents that use V1 for instance metadata access will break.

Metadata response hop limit | Info

2



Allow tags in metadata | Info

Select



User data - optional | Info

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

```
#!/bin/sh
yum -y install httpd php
chkconfig httpd on
systemctl start httpd.service
cd /var/www/html
wget https://us-west-2-tcprod.s3.amazonaws.com/courses/spl-03/v4.3.23.prod-5c8094c0/scripts/examplefiles-elb.zip
unzip examplefiles-elb.zip
```

User data has already been base64 encoded

2. After launching the EC2 in the property of the instance copy **Public ipv4 DNS** and view the page in the browser. The output of zone and instance ID should be shown.



EC2 Instance ID: i-04abee401a5bae4cc

Zone: us-west-2b

3. In the main page of the EC2 service the navigation pane holds a section for load balancers, select load balancer.

4. Choose **Create load balancer**, this will load a page where we have to select the type of load balancer we want to create, choose **Application load balancer**.

5. Enter the name of the load balancer and select the VPC that was created earlier, make sure the public subnet is selected.

6. Assign a security group where the web port 80 are reachable from any host.

7. In **listener and routing** section choose **create target group**, here enter name to the target group and in the **Register target** select the EC2 instance with the web application running.

The screenshot shows the AWS Lambda console with a success message: "Successfully created the target group: myTarget. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the Targets tab." Below the message, the "myTarget" target group details are displayed. The "Details" section includes:

- arn:aws:elasticloadbalancing:us-west-2:126018152079:targetgroup/myTarget/1a6d2866aa9e0207
- Target type: Instance
- Protocol: Port: HTTP: 80
- Protocol version: HTTP1
- VPC: vpc-0b227b38f2134f05d
- IP address type: IPv4
- Load balancer: None associated

Below the details, a summary table shows target status:

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

A note below the table says: "► Distribution of targets by Availability Zone (AZ) Select values in this table to see corresponding filters applied to the Registered targets table below."

The screenshot shows the "Registered targets" section of the AWS Lambda console. It displays two targets:

- Target 1: Info, Status: Anomaly mitigation: Not applicable, Deregister, Register targets
- Target 2: Info, Status: Anomaly mitigation: Not applicable, Deregister, Register targets

Below the targets, there is a note: "Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target groups' health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets." A filter bar and pagination controls are also visible.

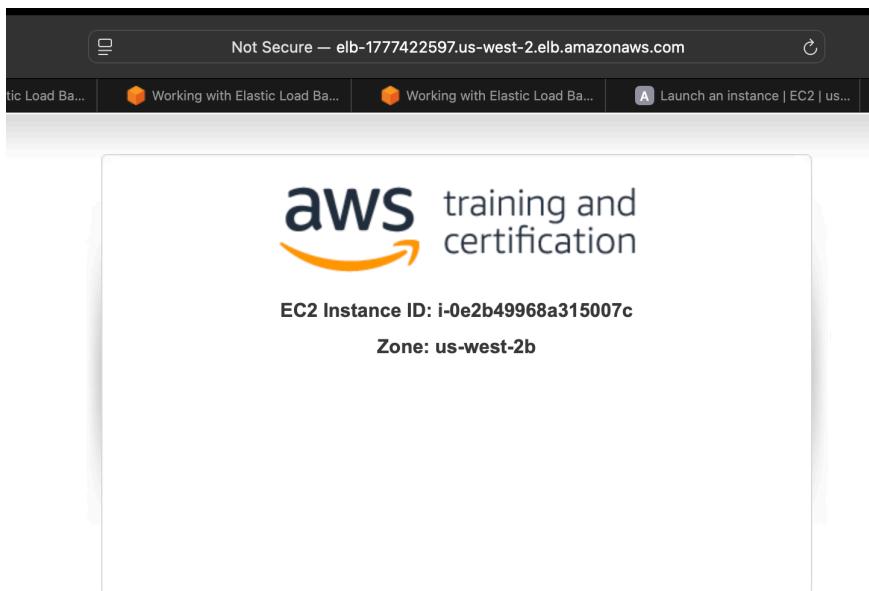
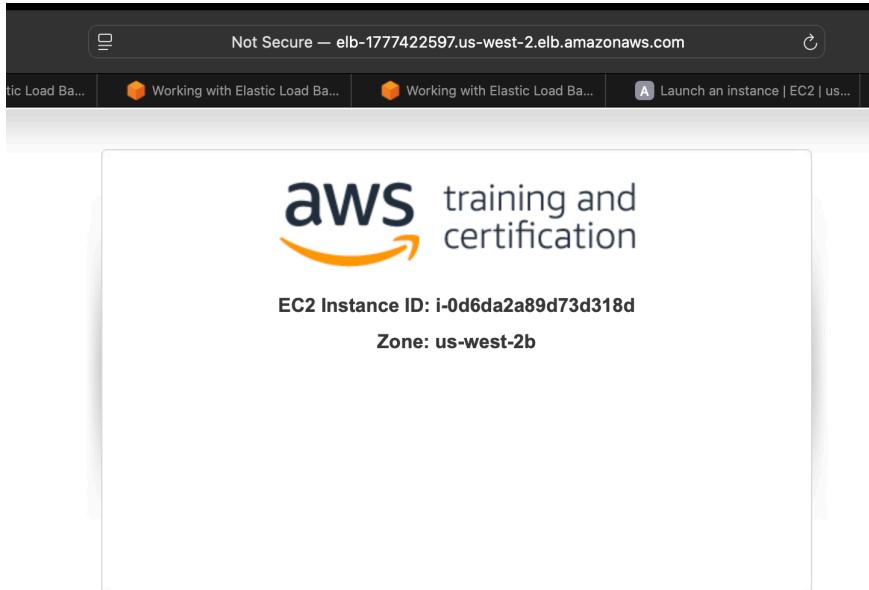
8. In the load balancer page select the newly created target group and launch the load balancer by confirming the configurations.

The screenshot shows the "Load balancer: ELB" configuration page. The "Details" section includes:

- Load balancer type: Application
- Status: Active
- VPC: vpc-0b227b38f2134f05d
- Load balancer IP address: IPv4
- Scheme: Internet-facing
- Hosted zone: Z1H1FL5HABSF5
- Availability Zones: subnet-045fc9ab63ae002d0 (us-west-2b (usw2-aaz)), subnet-098fdf0feb2603bd3 (us-west-2a (usw2-aaz))
- Date created: May 4, 2025, 17:38

At the bottom, a message says: "DNS name copied" and "ELB-1777422597.us-west-2.elb.amazonaws.com (A Record)".

9. Now copy the **DNS name** from the load balancer details section and view the page in the browser, if you refresh the page multiple times it will show different instance ID which proves the response is coming from different instances.



# 4.

# CREATE NEW USER FROM ROOT FROM IAM

1. Login to the AWS console with root account.
2. Go to IAM control panel and choose users from navigation panel
3. Choose **Create user** and enter username for the new user

**User details**

User name  
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . \_ - (hyphen)

Provide user access to the AWS Management Console - *optional*  
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

**Are you providing console access to a person?**

User type  
 Specify a user in Identity Center - Recommended  
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

I want to create an IAM user  
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

**Console password**

Autogenerated password  
You can view the password after you create the user.

Custom password  
Enter a custom password for the user.

Show password

Users must create a new password at next sign-in - Recommended  
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

4. To create a traditional IAM user check the box where it says “provide user access to management console”
5. Then in the next field select “I want to create an IAM user”
6. Then select the password handling approach by which the user should login first time the choose next
7. In next step we need to add permission to the user, it is recommended to assign a user to a group

The screenshot shows the 'Set permissions' step of the IAM user creation wizard. It includes sections for 'Permissions options', 'Get started with groups', and 'Set permissions boundary - optional', along with navigation buttons for 'Cancel', 'Previous', and 'Next'.

**Set permissions**  
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

**Permissions options**

**Add user to group**  
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

**Copy permissions**  
Copy all group memberships, attached managed policies, and inline policies from an existing user.

**Attach policies directly**  
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

**Get started with groups**  
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

**Create group**

**Set permissions boundary - optional**

Cancel Previous Next

8. If there is no existing user group create a new group, you can add policy to the group or can create a custom policy

## Create user group



Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

### User group name

Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+,-,@,\_' characters.

### Permissions policies (1046)

[Create policy](#)

#### Filter by Type

[All types](#)

14 matches



1



<input type="checkbox"/>	Policy name	Type	Use...	Description
<input type="checkbox"/>	<a href="#">AmazonDMSRedsh...</a>	AWS managed	None	Provides access to manage S3 set
<input type="checkbox"/>	<a href="#">AmazonS3FullAccess</a>	AWS managed	Permis...	Provides full access to all buckets
<input type="checkbox"/>	<a href="#">AmazonS3ObjectL...</a>	AWS managed	None	Provides AWS Lambda functions p
<input type="checkbox"/>	<a href="#">AmazonS3Outpost...</a>	AWS managed	None	Provides full access to Amazon S3
<input type="checkbox"/>	<a href="#">AmazonS3Outpost...</a>	AWS managed	None	Provides read only access to Amaz
<input type="checkbox"/>	<a href="#">AmazonS3ReadOn...</a>	AWS managed	None	Provides read only access to all bu
<input type="checkbox"/>	<a href="#">AmazonS3TablesF...</a>	AWS managed	None	Provides full access to all S3 table
<input type="checkbox"/>	<a href="#">AmazonS3TablesR...</a>	AWS managed	None	Provides read only access to all S3
<input type="checkbox"/>	<a href="#">assume_s3_full_acces...</a>	Customer man...	None	-
<input type="checkbox"/>	<a href="#">AWSBackupService...</a>	AWS managed	None	Policy containing permissions nec

9. After adding user to a group click on next to review the user and create the user account, the user login details can be shared via email through the console.

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

[View user](#)

Step 1  Specify user details

Step 2  Set permissions

Step 3  Review and create

Step 4  Retrieve password

**Retrieve password**

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

**Console sign-in details**

Console sign-in URL <https://848771820849.signin.aws.amazon.com/console> [Email sign-in instructions](#)

User name

Console password  [Show](#)

[Cancel](#) [Download .CSV file](#) [Return to users list](#)

# 5.

# CREATE RDS SERVER AND CONNECT USING MYSQL WORKBENCH

1. In AWS management console go to Aurora RDS control panel
2. In navigation panel select databases and choose **Create database**
3. In **choose a database creation method** select standard create

**Choose a database creation method**

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

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

**MySQL**

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

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

**Engine options**

Engine type: [Info](#)

<input type="radio"/> Aurora (MySQL Compatible) 	<input type="radio"/> Aurora (PostgreSQL Compatible) 
<input checked="" type="radio"/> MySQL 	<input type="radio"/> PostgreSQL 
<input type="radio"/> MariaDB 	<input type="radio"/> Oracle 
<input type="radio"/> Microsoft SQL Server 	<input type="radio"/> IBM Db2 

4. For **Engine options** select Mysql
5. In **Templates section** choose free tire

**Choose a database creation method**

- Standard create  
You set all of the configuration options, including ones for availability, security, backups, and maintenance.
- Easy create  
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

**Engine options**

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

<input type="radio"/> Aurora (MySQL Compatible)	<input type="radio"/> Aurora (PostgreSQL Compatible)
	
<input checked="" type="radio"/> MySQL	<input type="radio"/> PostgreSQL
	
<input type="radio"/> MariaDB	<input type="radio"/> Oracle
	
<input type="radio"/> Microsoft SQL Server	<input type="radio"/> IBM Db2
	

**MySQL**

- MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL Community edition with the flexibility to easily scale compute resources or storage capacity for your databases.
- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

## 6. Set admin user credentials in **credential settings**

## 7. In **Connectivity** section enable public access and disable EC2 connectivity.

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.

**Default VPC: vpc-449e602f**  
3 Subnets, 3 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

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

**DB subnet group** [Info](#)  
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

**default-vpc-449e602f**  
3 Subnets, 3 Availability Zones

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

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

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

**VPC security group (firewall)** [Info](#)  
Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

Choose existing  
Choose existing VPC security groups

Create new  
Create new VPC security group

**Existing VPC security groups**  
Choose one or more options

**MySQL**

- MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL Community edition with the flexibility to easily scale compute resources or storage capacity for your databases.
- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

## 8. Leave other things to default and click **Create database**

## 9. After the database is available go to its security group configuration, and in details panel verify its inbound rule. We have to add a MYSQL/Aurora rule to be accepted from all the source or your local machines public IP.

**Security Groups (1/7) Info**

**sg-4d74d036 - default**

**Inbound rules (2)**

Port range	Source	Type	Protocol	IP version	Name
3306	0.0.0.0/0	MySQL/Aurora	TCP	IPv4	-0b1d12444276071ed
All	All	All traffic	All	-	-0cff560463cc6d32

10. After this step go to the database panel and copy the **endpoint** and **port** values from the connectivity panel

**Connectivity & security**

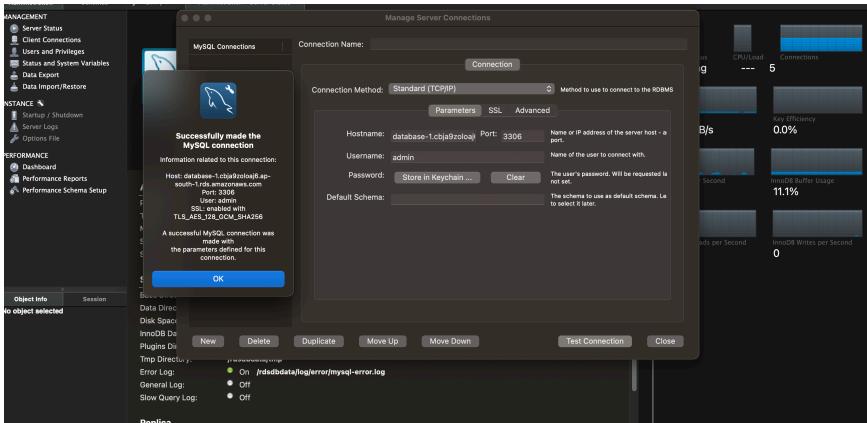
**Endpoint & port**

**Networking**

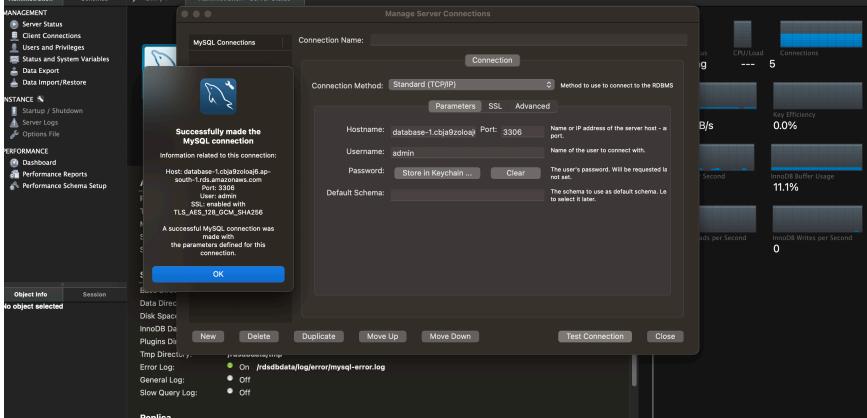
**Security**

Setting	Value
Endpoint	database-1.cbjaj9zoloaj6.ap-south-1.rds.amazonaws.com
VPC	vpc-449e602f
Subnet group	default-vpc-449e602f
Subnets	subnet-44698d2f, subnet-d08d12ab, subnet-f99c6b5
Network type	IPv4
VPC security groups	default (sg-4d74d036)
Certificate authority	rds-ca-rsa2048-g1
Certificate authority date	May 20, 2061, 00:10 (UTC+05:30)
DB instance certificate expiration date	May 08, 2026, 21:41 (UTC+05:30)

11. In MySQL workbench in databases option add the endpoint as host name and the port as port in the connection setting, with your admin credentials.



## 12. Test your connection once its successful connect to the database



# 6.

## RUN PHP CODE ON EC2 INSTANCE THAT RETRIEVE DATA FROM RDS SERVER

1. Create EC2 instance with similar configurations in earlier exercise

2. In user data section add the below commands, at this stage you should see error for connecting to the database

```
#!/bin/sh  
yum -y install httpd php php-mysqlnd  
chkconfig httpd on  
systemctl start httpd.service  
cd /var/www/html  
wget https://github.com/nutansonale/PHP_sample_resource/archive/  
refs/heads/main.zip  
unzip main.zip  
cp PHP_sample_resource/*.  
systemctl restart httpd.service
```

3. Go to RDS control panel and follow initial steps of selecting the RDS instance type and it has to be MYSQL as our PHP code is written for MYSQL engine

Aura and RDS > Create database

**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.

**EC2 instance** [Info](#)  
Choose the EC2 instance to add as the compute resource for this database. A VPC security group is added to this EC2 instance. A VPC security group is also added to the database with an inbound rule that allows the EC2 instance to access the database.

i-0ed65e24510fb0d29  
PHP\_EC2

**Some VPC settings can't be changed when a compute resource is added**  
Adding an EC2 compute resource automatically selects the VPC, DB subnet group, and public access settings for this database. To allow the EC2 instance to access the database, a VPC security group rds-ec2-X is added to the database and another called ec2-rds-X to the EC2 instance. You can remove the new security group for the database only by removing the compute resource.

**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.

Default VPC (vpc-4496602f)  
6 Subnets, 3 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

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

**MySQL**

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

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

4. In connectivity section you have to select Connect to an EC2 compute resource

5. Keep other selections default as it will create a security group suitable for the the EC2 to connect to the RDS but RDS server wont be available for public access.

6. The output for the configuration should be like this

The screenshot shows the AWS RDS CRUD interface for managing users. At the top, there's a toolbar with various icons. Below it, a header bar displays "Not Secure – 43.204.103.230". The main area has tabs for "Create / Update User" and "Delete User". Under "Create / Update User", there are fields for "Name" and "Email", and buttons for "Create" and "Update". Under "Delete User", there's a "User ID" field and a "Delete" button. At the bottom, there's a section titled "All Users" with two items listed:

- ID: 2 | sag (sag@mail.com)
- ID: 3 | sagar (sag@mail.com)

# 7.

# BUILD OWN STATIC WEBSITE AND HOSTING APPLICATION

1. Create a general purpose S3 bucket, similar to that of in earlier exercise
2. In the S3 control panel click on the bucket you have created and go to properties tab, enable **Static website hosting**

The screenshot shows the 'Edit static website hosting' configuration page for an S3 bucket named 'statictestrvc'. The 'Static website hosting' section is enabled. Under 'Hosting type', 'Host a static website' is selected, with the endpoint set to 'statictestrvc.s3.amazonaws.com'. A note at the bottom of this section states: 'For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access.' Below this, the 'Index document' is set to 'index.html' and the 'Error document' is set to 'error.html'. A 'Redirection rules' section is present but empty.

3. While enabling this feature make sure you give the landing page of the web site, remember if you need to

add any dynamic features it need to be via client side script.

The screenshot shows the 'Edit static website hosting' configuration page for a bucket named 'statictestrvc'. The 'Static website hosting' section is enabled. Under 'Hosting type', 'Host a static website' is selected. The 'Index document' field contains 'index.html'. The 'Error document - optional' field contains 'error.html'. A note at the bottom states: 'For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access.' Below these fields is a 'Redirection rules - optional' section with a JSON editor containing the number '1'.

4. Now add the html page into the bucket using upload function

5. Now the buck should be made publicly accessible, so in permissions uncheck all blocking permissions for public access

This screenshot is identical to the one above, showing the 'Edit static website hosting' configuration page for the 'statictestrvc' bucket. The 'Static website hosting' section is enabled, 'Host a static website' is selected, and the index/error documents are set to 'index.html' and 'error.html' respectively. The same note about making content publicly readable is present, along with the 'Redirection rules - optional' section.

6. Finally be need to add the below bucket policy to allow all users to have get access to the objects in the bucket this will not be handled by above steps

Edit static website hosting [Info](#)

## Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

## Static website hosting

Disable

Enable

## Hosting type

Host a static website

Use the bucket endpoint as the web address. [Learn more](#)

Redirect requests for an object

Redirect requests to another bucket or domain. [Learn more](#)

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

## Index document

Specify the home or default page of the website.

index.html

## Error document - optional

This is returned when an error occurs.

error.html

## Redirection rules - optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

1

{

"Version": "2012-10-17",

"Statement": [

{

    "Sid": "PublicReadGetObject",

    "Effect": "Allow",

    "Principal": "\*",

    >Action": "s3:GetObject",

    "Resource": "arn:aws:s3:::statictestrvce/\*"

}

]

}

# 8.

## DEMONSTRATE ECLIPSE INTEGRATION WITH CLOUD

AWS earlier had AWS toolkit support for eclipse IDE for enable faster development, as this has reached its end of life by 2023 developers are using AWS SDKs as they contain prebuilt functions.

Toolkits are still available for Intelij IDEA platform but its a professional platform that need to be subscribed.

# 9.

## RUN JAVA APPLICATION BY CONNECTING TO RDS SERVER

1. Follow the same steps to create RDS and EC2 instance as previously created for PHP script, but there is a slight difference. I have used serverlet approach to keep dependencies as small as possible
2. Here we need to install tomcat externally

```
#!/bin/sh
yum -y install tomcat10
Wget https://repo1.maven.org/maven2/com/mysql/mysql-connector-j/8.3.0/mysql-connector-j-8.3.0.jar
Wget https://github.com/nutansonale/PHP\_sample\_resource/archive/refs/heads/java.zip
Unzip java.zip
cp PHP_sample_resource/webapp-0.0.1-SNAPSHOT.war /var/lib/tomcat10/webapps/
cp mysql-connector-j-8.3.0.jar /usr/share/tomcat10/lib/
Systemctl enable tomcat10
Systemctl start tomcat10
```



### Create / Update User

ID (for update) sag Email Create Update

### Delete User

ID Delete

#### All Users

- ID: 2 | sag | sag@mail.com | Created: 2025-05-09 17:51:31
- ID: 3 | sagar | sag@mail.com | Created: 2025-05-09 17:52:57

3. Note tomcat runs at 8080 port hence the inbound rule in security group of the EC2 should allow that port similar to 80

A screenshot of the AWS EC2 Security Groups console. On the left, there's a navigation sidebar with sections like Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, and Placement Groups. The main content area shows a security group named "sg-0addf4d01c7c22292 - EC2\_publisch".

Name	Security group rule ID	IP version	Type	Protocol	Port range
sgr-0ba2d90a70c2ed022	IPv4	Custom TCP	TCP	8080	
sgr-0100644d4262f2897	IPv4	SSH	TCP	22	
sgr-0d4ef0b1019hd4b25	IPv4	HTTP	TCP	80	

# 10.

## DEMONSTRATE AUTO SCALING GROUP

1. Open the Amazon EC2 console and choose Auto Scaling Groups from the navigation pane.
2. On the navigation bar at the top of the screen, choose the same AWS Region that you used when you created the launch template.
3. Choose Create an Auto Scaling group.
4. On the Choose launch template or configuration page, do the following:
  - For Auto Scaling group name, enter a name for your Auto Scaling group.
  - For Launch template, choose an existing launch template.
  - For Launch template version, choose whether the Auto Scaling group uses the default, the latest, or a specific version of the launch template when scaling out.
  - Verify that your launch template supports all of the options that you are planning to use, and then choose Next.
5. On the Choose instance launch options page, if you're not using multiple instance types, you can skip the Instance type requirements section to use the EC2 instance type that is specified in the launch template.

6. Under Network, for VPC, choose a VPC. The Auto Scaling group must be created in the same VPC as the security group you specified in your launch template.
7. For Availability Zones and subnets, choose one or more subnets in the specified VPC. Use subnets in multiple Availability Zones for high availability.
8. If you created a launch template with an instance type specified, then you can continue to the next step to create an Auto Scaling group that uses the instance type in the launch template.  
Alternatively, you can choose the Override launch template option if no instance type is specified in your launch template or if you want to use multiple instance types for auto scaling.
9. Choose Next to continue to the next step.  
Or, you can accept the rest of the defaults, and choose Skip to review.