

lab 8 : static website hosting using AWS S3

1. Create an S3 bucket

The screenshot shows the 'Create bucket' wizard in the AWS S3 console. It consists of two main sections: 'General configuration' and 'Object Ownership'.

General configuration:

- AWS Region:** Asia Pacific (Mumbai) ap-south-1
- Bucket type:** General purpose (selected)
- Bucket name:** static_bucket
- Copy settings from existing bucket - optional:** Choose bucket (button)
- Format:** s3://bucket/prefix

Object Ownership:

- Object Ownership:** Bucket owner enforced
- ACLs disabled (recommended):** All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
- ACLs enabled:** Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Success message: Successfully created bucket "shravstaticbucket". To upload files and folders, or to configure additional bucket settings, choose View details.

Account snapshot: Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more.

General purpose buckets: 1 item listed: shravstaticbucket (created on March 12, 2025).

2. Edit Object Ownership to enable Access Control Lists (ACLs)

The screenshot shows the 'Edit Object Ownership' page for the 'shrawastibucket' bucket. In the 'Object Ownership' section, the 'ACLs enabled' option is selected, which is highlighted with a blue border. A note below it states: 'Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.' There is also a warning message: '⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.' Below this, there is a note: '⚠️ Enabling ACLs turns off the bucket owner enforced setting for Object Ownership. Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.' A checkbox labeled 'I acknowledge that ACLs will be restored.' is present. In the 'Object Ownership' dropdown, 'Bucket owner preferred' is selected. A note below it says: 'If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.' Another option, 'Object writer', is also listed. At the bottom right, there are 'Cancel' and 'Save changes' buttons.

3. Upload an HTML file to the bucket

The screenshot shows the 'Upload' page for the 'shrawastibucket' bucket. In the 'Upload' section, there is a large input field with the placeholder 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Below this, a table lists the uploaded file: 'Files and folders (1 total, 13.8 KB)'. The file is named 'pretty-static-website.html', has a type of 'text/html', and a size of '13.8 KB'. There are 'Remove', 'Add files', and 'Add folder' buttons at the top of the table. In the 'Destination' section, the destination is set to 's3://shrawastibucket'. The 'Destination details' section notes that 'Bucket settings that impact new objects stored in the specified destination.' Below this, there are sections for 'Permissions' (with a note about granting public access) and 'Properties' (with a note about specifying storage class, encryption settings, tags, and more). At the bottom right, there are 'Cancel' and 'Upload' buttons.

The screenshot shows the AWS S3 console interface. At the top, there's a green success message: "Upload succeeded. For more information, see the Files and folders table." Below it, a summary table shows one file uploaded: "Succeeded" (1 file, 13.8 KB (100.00%)) and "Failed" (0 files, 0 B (0%)). A "Close" button is at the top right of the summary table. Below the summary, there are two tabs: "Files and folders" (selected) and "Configuration". Under "Files and folders", a table lists the uploaded file: "pretty-static-website.html" (text/html, 13.8 KB, Status: Succeeded). The table has columns for Name, Folder, Type, Size, Status, and Error. At the bottom of the page, there are links for CloudShell, Feedback, and a footer with copyright information.

4. Navigate to bucket properties → static website hosting

The screenshot shows the "Edit static website hosting" configuration page for the "shrawastibucket" bucket. The "Static website hosting" section is enabled. The "Hosting type" is set to "Host a static website". A note says: "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." The "Index document" is set to "pretty-static-website.html". The "Error document - optional" is set to "error.html". There is a "Redirection rules - optional" section with a JSON input field containing the number "1". The page includes standard AWS navigation links like CloudShell, Feedback, and a footer with copyright information.

5. Paste the bucket website endpoint link in a browser

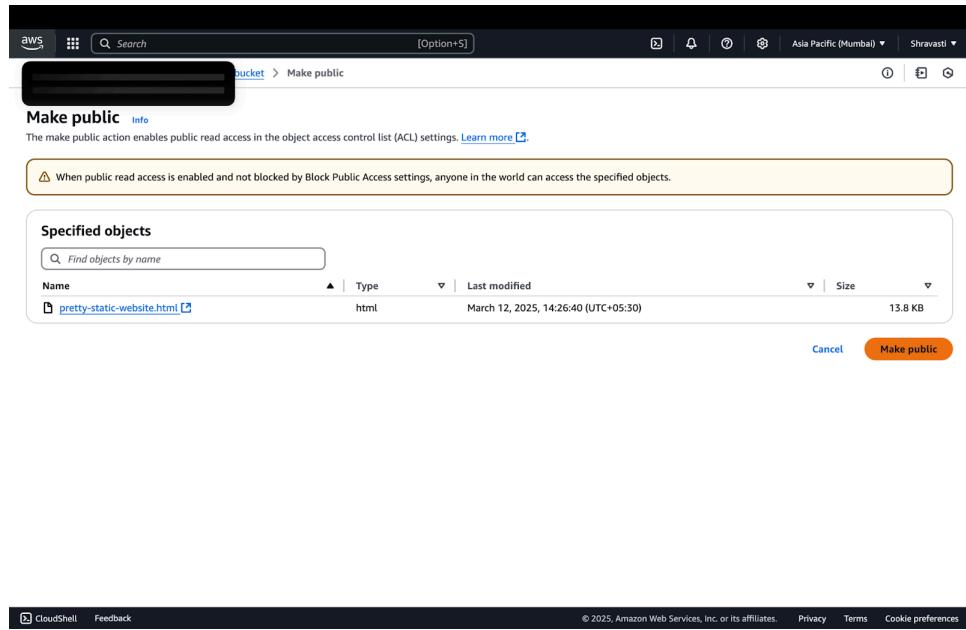
6. Access is denied to the website, since no access policy is written for it

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: D572HY956XHMY9SA
- HostId: cPr8WKIwNwlXarojjKRNTTZ2nzUpV/wOza09ImSI6GFp8QnJ+W7rK75zG2yO4ZNpd7mqGPu/0E=

7. Make bucket objects public using ACL

The screenshot shows the AWS S3 console interface. The top navigation bar includes the AWS logo, search bar, and region selector (Asia Pacific (Mumbai)). The current path is 'Amazon S3 > Buckets > shravstaticbucket'. The main content area displays the 'Objects' tab for the 'shravstaticbucket'. It lists one object, 'pretty-static-website.html', which is an HTML file. A context menu is open over this object, with the 'Actions' dropdown expanded. The 'Actions' dropdown includes options like 'Download as', 'Share with a presigned URL', 'Calculate total size', 'Copy', 'Move', 'Initiate restore', 'Query with S3 Select', 'Edit actions', 'Rename object', 'Edit storage class', 'Edit server-side encryption', 'Edit metadata', 'Edit tags', and 'Make public using ACL'. The 'Make public using ACL' option is highlighted with a yellow box.



8. Refresh the page and the website will now be visible

A screenshot of a static website. The header includes a logo 'YourBrand' and navigation links for 'Services', 'About', 'Testimonials', and 'Contact'. The main content features a large blue banner with the title 'Creative Solutions for Modern Challenges' and a subtitle explaining their mission to help businesses transform ideas into reality. A 'Get Started' button is located below the banner. The footer contains a section titled 'Our Services' with three blurred service categories.

9. Revert ownership and public access settings

The screenshot shows the AWS S3 console. The top navigation bar includes the AWS logo, a search bar, and links for 'Amazon S3 > Buckets > shravssstaticbucket'. On the right, there are icons for notifications, help, and account information ('Asia Pacific (Mumbai) Shravasti'). Below the navigation, the bucket name 'shravssstaticbucket' is displayed with an 'Info' link. A horizontal menu bar contains 'Objects', 'Properties', **Permissions**, 'Metrics', 'Management', and 'Access Points'. The main content area is titled 'Permissions overview' and contains a section for 'Access finding'. It notes that findings are provided by IAM external access analyzers and links to 'How IAM analyzer findings work'. A 'View analyzer for ap-south-1' button is present. Another section, 'Block public access (bucket settings)', is shown with an 'Edit' button. It indicates that public access is granted through ACLs, bucket policies, access point policies, or all. It recommends turning on 'Block all public access'. A note states that these settings apply only to the bucket and its access points. A 'Block all public access' setting is listed as 'Off' with an 'Edit' button and a link to 'Individual Block Public Access settings for this bucket'. The bottom section is titled 'Bucket policy' with 'Edit' and 'Delete' buttons. It states that the bucket policy provides access to objects stored in the bucket and notes that bucket policies don't apply to objects owned by other accounts. A note says 'No policy to display.' with a 'Copy' button. The footer includes links for 'CloudShell', 'Feedback', and copyright information ('© 2025, Amazon Web Services, Inc. or its affiliates.'), along with 'Privacy', 'Terms', and 'Cookie preferences'.

The screenshot shows the 'Edit Block public access (bucket settings)' page. The top navigation bar is identical to the previous screenshot. The main content area is titled 'Edit Block public access (bucket settings)' with an 'Info' link. It contains a section for 'Block public access (bucket settings)'. A note explains that public access is granted through ACLs, bucket policies, access point policies, or all. It recommends turning on 'Block all public access'. A note states that these settings apply only to the bucket and its access points. A 'Block all public access' setting is checked with an 'Edit' button and a note that turning it on is the same as turning on all four settings below. Below this, there are four checkboxes: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. The footer includes 'Cancel' and 'Save changes' buttons.

This screenshot is identical to the one at the top of the page, showing the 'Permissions overview' section of the 'shravssstaticbucket' bucket settings.

Object Ownership [Info](#)

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

Object Ownership
Bucket owner preferred

ACLs are enabled and can be used to grant access to this bucket and its objects. If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#)

The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: ea9c3acf9b5cf904cc564b350439cfdb0b87a206f716f2cd32352871091153ad	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-

S3 Log delivery group

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

Edit Object Ownership [Info](#)

Object Ownership

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

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

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

Object Ownership
Bucket owner enforced

Cancel **Save changes**

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

Successfully edited Object Ownership.

shravssstaticbucket Info

Objects Properties **Permissions** Metrics Management Access Points

Permissions overview

Access finding
Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#).
[View analyzer for ap-south-1](#)

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
 On
► Individual Block Public Access settings for this bucket

Edit

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

ⓘ Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#).

[Edit](#) [Delete](#)

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

10. Create another bucket in a different region

The screenshot shows the AWS S3 console. At the top, there's a search bar and a 'Search' button. To the right are account details for 'Shravasti' and a 'View Storage Lens dashboard' button. Below the header, a banner displays 'Account snapshot - updated every 24 hours' and 'Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more'. A 'Create bucket' button is visible on the right.

General purpose buckets Directory buckets

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

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	IAM Access Analyzer	Creation date
shravstaticbucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	March 12, 2025, 14:22:35 (UTC+05:30)

This screenshot is similar to the one above, but it includes a sidebar on the right listing AWS regions. The sidebar shows regions grouped by continent: United States, Asia Pacific, Canada, Europe, and South America. Each region is listed with its name and corresponding AWS ID. A 'Create bucket' button is also present in the sidebar.

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

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	IAM Access Analyzer
shravstaticbucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1

United States

N. Virginia	us-east-1
Ohio	us-east-2
N. California	us-west-1
Oregon	us-west-2

Asia Pacific

Mumbai	ap-south-1
Osaka	ap-northeast-3
Seoul	ap-northeast-2
Singapore	ap-southeast-1
Sydney	ap-southeast-2
Tokyo	ap-northeast-1

Canada

Central	ca-central-1
---------	--------------

Europe

Frankfurt	eu-central-1
Ireland	eu-west-1
London	eu-west-2
Paris	eu-west-3
Stockholm	eu-north-1

South America

São Paulo	sa-east-1
-----------	-----------

There are 15 Regions that are not enabled for this account

[Manage Regions](#) | [Manage Local Zones](#)

This screenshot is identical to the one above, showing the AWS S3 console with the account snapshot and general purpose buckets section, and the same sidebar listing AWS regions by continent.

Screenshot of the AWS S3 'Create bucket' configuration page.

General configuration

AWS Region: US East (N. Virginia) us-east-1

Bucket type: General purpose

Bucket name: nvirginiabucketshravas

Copy settings from existing bucket - optional: Choose bucket

Object Ownership: Bucket owner enforced

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

Screenshot of the AWS S3 'Create bucket' configuration page.

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

No tags associated with this bucket. Add tag

Default encryption

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

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

Bucket Key: Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Create bucket

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

The screenshot shows the AWS S3 Buckets page. At the top, there is a success message: "Successfully created bucket 'nvirginiabucketshrav'". Below it, an account snapshot is displayed, mentioning "updated every 24 hours" and "Storage lens provides visibility into storage usage and activity trends". The main section shows two General purpose buckets:

Name	AWS Region	IAM Access Analyzer	Creation date
nvirginiabucketshrav	US East (N. Virginia) us-east-1	View analyzer for us-east-1	March 12, 2025, 14:42:15 (UTC+05:30)
shravstaticbucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	March 12, 2025, 14:22:35 (UTC+05:30)

At the bottom of the page, there are links for CloudShell, Feedback, and various AWS services.

11. Select the bucket created in Mumbai region → navigate to Management tab → Create replication rule

The screenshot shows the 'Create replication rule' configuration page in the AWS S3 console. The top navigation bar includes the AWS logo, search bar, and account information for 'Asia Pacific (Mumbai)' and 'Shravasti'. The breadcrumb path is 'Amazon S3 > Buckets > shravsstaticbucket > Replication rules > Create replication rule'. The main section is titled 'Replication rule configuration'.

Replication rule name: repreleone

Status: Enabled (radio button selected)

Priority: 0

Source bucket:

- Source bucket name:** shravsstaticbucket
- Source Region:** Asia Pacific (Mumbai) ap-south-1
- Choose a rule scope:** Apply to all objects in the bucket (radio button selected)

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

The screenshot continues the 'Create replication rule' configuration process. The top navigation bar and breadcrumb path remain the same. The main section is titled 'Destination'.

Destination: Choose a bucket in this account (radio button selected)

Bucket name: nvirginiabucketshrvs

Warning: Amazon S3 can't detect whether versioning is enabled on the destination bucket. Amazon S3 must be able to read the versioning property of the destination bucket. Make sure that your destination bucket has the required bucket policy for reading the versioning property. If versioning is not enabled on the destination bucket, then rule creation will fail. **Retry**

Destination Region: US East (N. Virginia) us-east-1

IAM role:

- Create new role (radio button selected)
- Choose from existing IAM roles
- Enter IAM role ARN

Encryption: Server-side encryption protects data at rest.

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

The screenshot shows the 'Create replication rule' page in the AWS S3 console. At the top, there's a navigation bar with the AWS logo, search bar, and various icons. Below it, the breadcrumb trail shows 'bucket' > 'Replication rules' > 'Create replication rule'. The main content area is divided into several sections:

- Encryption**: A section about server-side encryption, with an option to "Replicate objects encrypted with AWS Key Management Service (AWS KMS)".
- Destination storage class**: A section about Amazon S3 storage classes, with an option to "Change the storage class for the replicated objects".
- Additional replication options**: A section with four options:
 - Replication Time Control (RTC)**: Describes replicating 99.99% of new objects within 15 minutes.
 - Replication metrics**: Describes monitoring replication progress and failures.
 - Delete marker replication**: Describes replicating delete marker operations.
 - Replica modification sync**: Describes replicating metadata changes from destination to source.

At the bottom right are 'Cancel' and 'Save' buttons.

A modal dialog box titled "Replicate existing objects?" is displayed. It contains the following text:

You can enable a one-time Batch Operations job from this replication configuration to replicate objects that already exist in the bucket and to synchronize the source and destination buckets. [Learn more](#) or [see pricing](#)

Existing objects

No, do not replicate existing objects.
 Yes, replicate existing objects.

At the bottom right are "Cancel" and "Submit" buttons.

Objects will be replicated in the destination bucket

The screenshot shows the AWS S3 console interface. The left sidebar has a navigation tree: 'Amazon S3' (selected), 'General purpose buckets', 'nvirginiabucketshrvs' (selected), 'Objects (1)', 'Upload', 'Find objects by prefix', 'Show versions', and a table listing one object: 'pretty-static-website.html' (html type, March 12, 2025, 14:56:58, 13.8 KB, Standard storage class). The top bar includes the AWS logo, search bar, and various navigation icons.

Name	Type	Last modified	Size	Storage class
pretty-static-website.html	html	March 12, 2025, 14:56:58 (UTC+05:30)	13.8 KB	Standard

12. KMS

- a. Navigate to Properties → Encryption

The screenshot shows the AWS S3 console with the path: Amazon S3 > Buckets > shrvsstaticbucket > Replication rules > Create replication rule.

Encryption

Server-side encryption protects data at rest.

Replicate objects encrypted with AWS Key Management Service (AWS KMS)
Replicate SSE-KMS and DSSE-KMS encrypted objects.

Warning: Replication might increase the number of KMS requests you will make in the source and destination AWS Regions. Learn more about [KMS operation quotas](#).

AWS KMS key for encrypting destination objects | [Info](#)

- Choose from your AWS KMS keys
- Enter AWS KMS key ARN

AWS KMS key ARN

[Create a KMS key](#)

Format (using key id): arn:aws:kms:<region>:<account-ID>/key/<key-id>
(using alias): arn:aws:kms:<region>:<account-ID>/alias/<alias-name>

Destination storage class

Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#).

Change the storage class for the replicated objects

Additional replication options

Replication Time Control (RTC)

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

b. Key type - Symmetric; Key usage - encrypt and decrypt

The screenshot shows the AWS KMS console with the path: KMS > Customer-managed keys > Create key.

Introducing the new Create key experience
We've improved the create key experience with an enhanced policy editor. [Let us know what you think or you can use the old experience.](#)

Step 1 Configure key

Configure key

Key type [Help me choose](#)

- Symmetric
A single key used for encrypting and decrypting data or generating and verifying HMAC codes.
- Asymmetric
A public and private key pair used for encrypting and decrypting data, signing and verifying messages, or deriving shared secrets

Key usage [Help me choose](#)

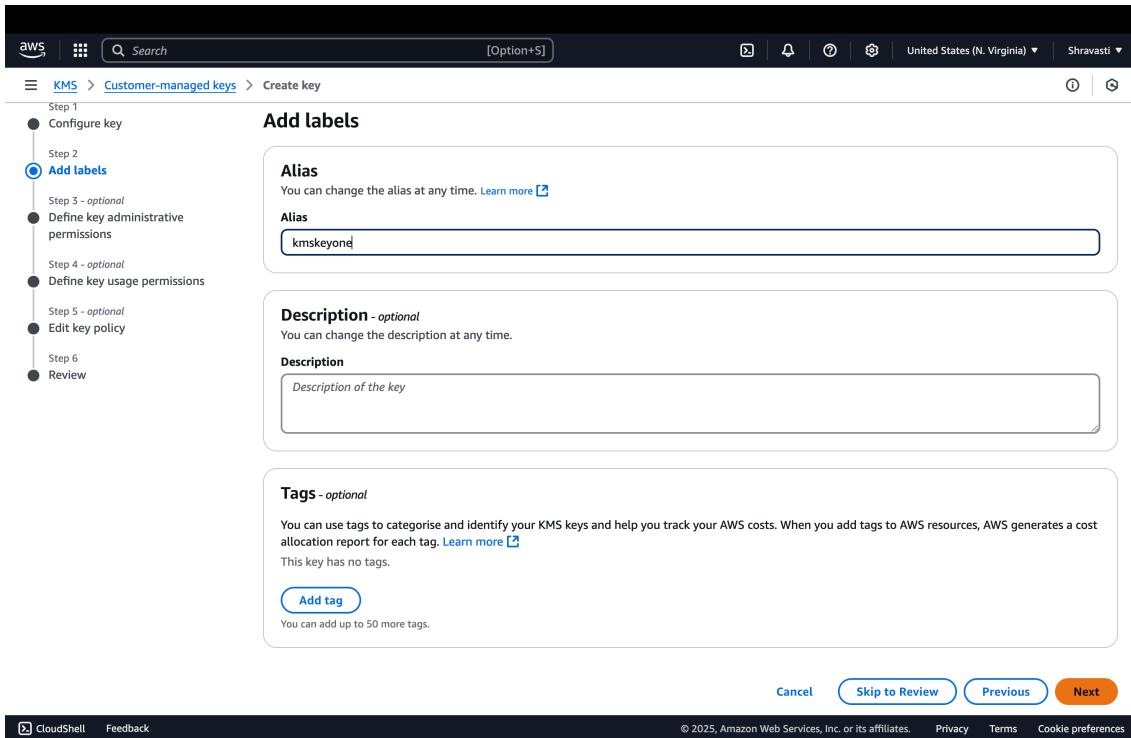
- Encrypt and decrypt
Use the key only to encrypt and decrypt data.
- Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

Advanced options

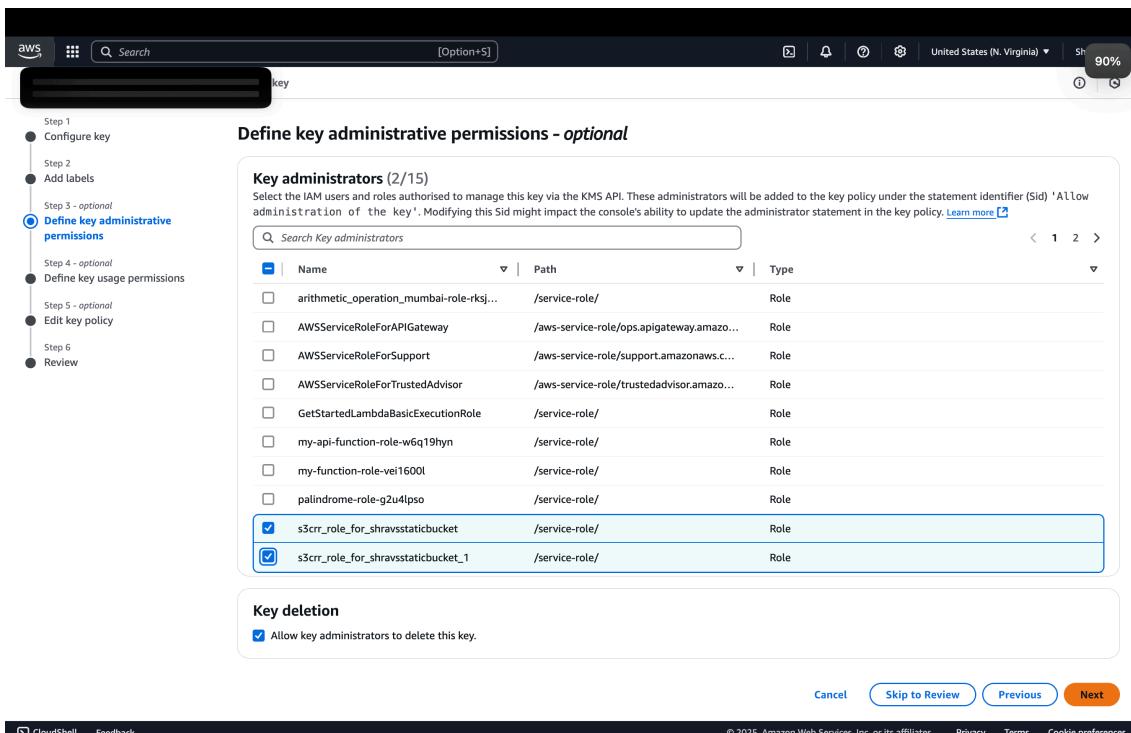
Cancel [Next](#)

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

c. Add a name for the key



d. Add bucket IAM roles as key administrators



e. Add bucket IAM users as key users

Step 1
Configure key

Step 2
Add labels

Step 3 - optional
Define key administrative permissions

Step 4 - optional
Define key usage permissions

Step 5 - optional
Edit key policy

Step 6
Review

Define key usage permissions - optional

Key users (2/15)
Select the IAM users and roles authorised to use this key in cryptographic operations. These users will be added to the key policy under the statement identifiers (Sids) 'Allow use of the key' and 'Allow attachment of persistent resources'. Modifying these Sids might impact the console's ability to update the user statements in the key policy. [Learn more](#)

Name	Path	Type
arithmetic_operation_mumbai-role-rksj0fn7	/service-role/	Role
AWSServiceRoleForAPIGateway	/aws-service-role/ops.apigateway.amazonaws.com/	Role
AWSServiceRoleForSupport	/aws-service-role/support.amazonaws.com/	Role
AWSServiceRoleForTrustedAdvisor	/aws-service-role/trustedadvisor.amazonaws.com/	Role
GetStartedLambdaBasicExecutionRole	/service-role/	Role
my-api-function-role-w6q19hyh	/service-role/	Role
my-function-role-veil1600l	/service-role/	Role
palindrome-role-g2u4lpso	/service-role/	Role
<input checked="" type="checkbox"/> s3crr_role_for_shravstaticbucket	/service-role/	Role
<input checked="" type="checkbox"/> s3crr_role_for_shravstaticbucket_1	/service-role/	Role

Other AWS accounts
Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

Add another AWS account

Cancel Skip to Review Previous Next

f. Copy paste key ARN

Amazon S3 > Buckets > shravstaticbucket > Replication rules > Create replication rule

AWS KMS key for encrypting destination objects

Choose from your AWS KMS keys [Info](#)

Enter AWS KMS key ARN

AWS KMS key ARN
Format (using key id): arn:aws:kms:<region><account-ID>/key/<key-id>
(using alias): arn:aws:kms:<region><account-ID>/alias/<alias-name>

Destination storage class
Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

Change the storage class for the replicated objects

Additional replication options

Replication Time Control (RTC)
Replication Time Control replicates 99.99% of new objects within 15 minutes and includes replication metrics. Additional fees will apply. [Learn more](#)

Replication metrics
With replication metrics, you can monitor the total number and size of objects that are pending replication, and the maximum replication time to the destination Region. You can also view and diagnose replication failures. CloudWatch metrics fees apply. [Learn more](#) or see [Amazon CloudWatch pricing](#)

Delete marker replication
Delete markers created by S3 delete operations will be replicated. Delete markers created by lifecycle rules are not replicated. [Learn more](#)

Replica modification sync
Replicate metadata changes made to replicas from the destination bucket to the source bucket. [Learn more](#)

Cancel Save

13. Upload a new file to the source bucket i.e. bucket in Mumbai region

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 total, 5.0 MB)

All files and folders in this table will be uploaded.

Find by name			
<input checked="" type="checkbox"/> Name	Folder	Type	Size
<input checked="" type="checkbox"/> apoovrCTF_stats.pdf	-	application/pdf	5.0 MB

Destination [Info](#)

Destination <s3://shrvsstaticbucket>

Destination details
Bucket settings that impact new objects stored in the specified destination.

Permissions
Grant public access and access to other AWS accounts.

This bucket has the **bucket owner enforced** setting applied for Object Ownership. Use bucket policies to control access. [Learn more](#)

Server-side encryption [Info](#)

Server-side encryption protects data at rest.

Server-side encryption

- Don't specify an encryption key
The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.
- Specify an encryption key
The specified encryption key is used to encrypt objects before storing them in Amazon S3.

Encryption settings [Info](#)

- Use bucket settings for default encryption
- Override bucket settings for default encryption

Encryption type [Info](#)

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

AWS KMS key [Info](#)

- Choose from your AWS KMS keys
- Enter AWS KMS key ARN

AWS KMS key ARN

[Create a KMS key](#)

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- Disable
- Enable

The screenshot shows the AWS S3 Object Overview page for a file named 'apourvCTF_stats.pdf'. At the top, there are buttons for 'Copy S3 URI', 'Download', 'Open', and 'Object actions'. Below this, tabs for 'Properties' (selected), 'Permissions', and 'Versions' are visible. The 'Object overview' section contains the following details:

Owner ea9c3acf9b5cf904cc564b350439cfdb0b87a206f716f2cd3235287109115 3ad	S3 URI s3://shravstaticbucket/apourvCTF_stats.pdf
AWS Region Asia Pacific (Mumbai) ap-south-1	Amazon Resource Name (ARN) arn:aws:s3:::shravstaticbucket/apourvCTF_stats.pdf
Last modified March 12, 2025, 15:13:29 (UTC+05:30)	Entity tag (Etag) 430414576f7c8e6f1dd502a68fc894e3
Size 5.0 MB	Object URL https://shravstaticbucket.s3.ap-south-1.amazonaws.com/apourvCTF_stats.pdf
Type pdf	
Key apourvCTF_stats.pdf	

RDS Database

1. Create an RDS database

click on create database

AWS | Search [Option+S] Asia Pacific (Mumbai) Shravasti

RDS > Dashboard

Amazon RDS

Resources

You are using the following Amazon RDS resources in the Asia Pacific (Mumbai) region (used/quota)

DB Instances (0/20)	Parameter groups (0)
Allocated storage (0 TB/100 TB)	Default (0)
Instances and storage include Neptune and DocumentDB. Increase DB instances limit	Custom (0/40)
DB Clusters (0/40)	Option groups (0)
Reserved instances (0/20)	Default (0)
Snapshots (0)	Custom (0/20)
Manual	Subnet groups (0/20)
DB Cluster (0/100)	Supported platforms VPC
DB Instance (0/100)	Default network vpc-007543eb92d582d02
Automated	
DB Cluster (0)	
DB Instance (0)	
Recent events (0)	
Event subscriptions (0/20)	

Create database

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale a relational database in the cloud.

[Create database](#) [Restore from S3](#)

Note: your DB instances will launch in the Asia Pacific (Mumbai) region

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

choose standard creation → MySQL as engine

AWS | Search [Option+S] Asia Pacific (Mumbai) Shravasti

RDS > Create database

Create database [Info](#)

Choose a database creation method

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

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

Engine options

Engine type [Info](#)

<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

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.

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

choose free tier template

The screenshot shows the AWS RDS MySQL configuration interface. In the top navigation bar, the region is set to 'Asia Pacific (Mumbai)' and the user is 'Shravasti'. The main section is titled 'Templates' with the sub-section 'Choose a sample template to meet your use case.' It lists three options: 'Production' (radio button), 'Dev/Test' (radio button), and 'Free tier' (radio button, selected). The 'Free tier' section includes a link to 'Amazon RDS service level agreement (SLA)'. Below this, the 'Availability and durability' section is shown, with 'Deployment options' and a note about uptime. It lists three deployment types: 'Multi-AZ DB cluster deployment (3 instances)', 'Multi-AZ DB instance deployment (2 instances)', and 'Single-AZ DB instance deployment (1 instance)'. Each option has a detailed description and a diagram. The 'Single-AZ DB instance deployment (1 instance)' diagram shows a primary instance in AZ 1 with a write/read endpoint. The right sidebar contains information about MySQL and a bulleted list of features for the Free tier.

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.

add a name for the database instance → use self-managed credentials → add master password

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.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 63 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.

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

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

Managed in AWS Secrets Manager - **most secure**
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

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

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

Master password [Info](#)

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

Confirm master password [Info](#)

[CloudShell](#) [Feedback](#) © 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

let the other configurations be default

Instance configuration

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

DB instance class [Info](#)
 Show instance classes that support Amazon RDS Optimized Writes [Info](#)
Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.
 Include previous generation classes

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

2 vCPUs 1 GiB RAM Network: Up to 2,085 Mbps

Storage

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

Baseline performance determined by volume size

Allocated storage [Info](#)
 GiB
Allocated storage value must be 20 GiB to 6,144 GiB

Additional storage configuration

[CloudShell](#) [Feedback](#) © 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Connectivity [Info](#)

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

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

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

Virtual private cloud (VPC) [Info](#)
Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

Default VPC (vpc-007543eb92d582d02)
3 Subnets, 3 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

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.

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.

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

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

database authentication method → password authentication

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.

Monitoring [Info](#)
Choose monitoring tools for this database. Database Insights provides a combined view of Performance Insights and Enhanced Monitoring for your fleet of databases.

Database Insights - Advanced

- Retains 15 months of performance history
- Fleet-level monitoring
- Integration with CloudWatch Application Signals

Database Insights - Standard

- Retains 7 days of performance history, with the option to pay for the retention of up to 24 months of performance history

Database Insights pricing is separate from RDS monthly estimates. See [Amazon CloudWatch pricing](#).

Additional monitoring settings
Enhanced Monitoring, CloudWatch Logs and DevOps Guru

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

Log exports
Select the log types to publish to Amazon CloudWatch Logs

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.

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

database will be created successfully

The screenshot shows the AWS RDS Databases page. At the top, there is a green success message: "Successfully created database database-1508. You can use settings from database-1508 to simplify configuration of suggested database add-ons while we finish creating your DB for you." Below this, the "Databases (1)" section is displayed. The table has columns: DB identifier, Status, Role, Engine, Region ..., and Size. One row is shown: database-1508, Backin..., Instance, MySQL Co..., ap-south-1a, db.t4g.micro. There are buttons for "Group resources", "Modify", "Actions", "Restore from S3", and "Create database". On the left sidebar, under the "Databases" section, the "Databases" link is highlighted. Other sections include "Dashboard", "Performance insights", "Snapshots", "Exports in Amazon S3", "Automated backups", "Reserved instances", "Proxies", "Subnet groups", "Parameter groups", "Option groups", "Custom engine versions", "Zero-ETL integrations", "Events", "Event subscriptions", "Recommendations (0)", and "Certificate update". At the bottom, there are links for "CloudShell", "Feedback", "© 2025, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", and "Cookie preferences".

2. Navigate to the search bar and search for security group

The screenshot shows the AWS EC2 Security Groups page. The left sidebar includes links for Dashboard, EC2 Global View, Events, Instances (Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), and Network & Security (Security Groups, Elastic IPs, Placement Groups). The main content area displays a table titled "Security Groups (1) Info". The table has columns for Name, Security group ID, Security group name, and VPC ID. One row is listed: Name is "sg-000f28cce01d8879", Security group ID is "sg-000f28cce01d8879", Security group name is "default", and VPC ID is "vpc-007543eb92d582d02". There are buttons for Actions, Export security groups to CSV, and Create security group.

Name	Security group ID	Security group name	VPC ID
-	sg-000f28cce01d8879	default	vpc-007543eb92d582d02

3. 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	Protocol	Port range	Source	Description - optional
sgr-06c75a0df49bf9a73	All traffic	Info	All	All	mysqrule
-	MySQL/Aurora	TCP	3306	Cu...	sg-000f28cceea01d8879

Add rule Cancel Preview changes Save rules

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

4. outbound rule

Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules Info

Security group rule ID	Type	Protocol	Port range	Destination	Description - optional
sgr-03f2ea9d6c9298cbf	All traffic	All	All	Cu... 0.0.0.0/0	<input type="text"/> Delete
-	MySQL/Aurora	TCP	3306	An... 0.0.0.0/0	<input type="text"/> Delete

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

5. Navigate to the connectivity and security tab in RDS service → copy the endpoint link given there

database-1508.cpwi88a8e8aa.ap-south-1.rds.amazonaws.com

6. Open MySQL Workbench

