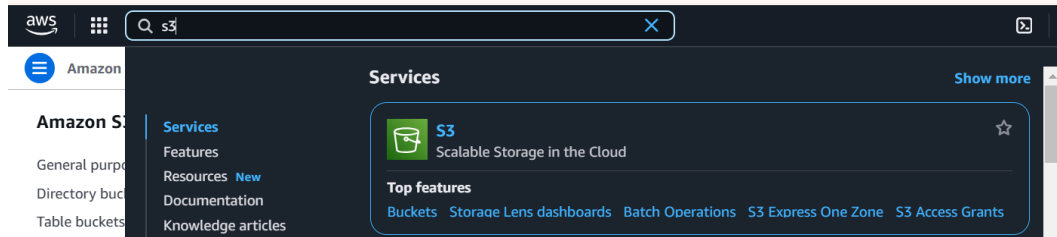


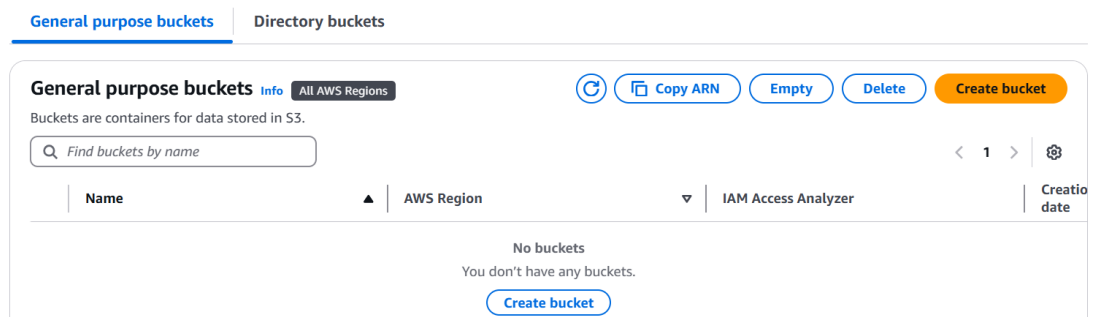
# Project: 2 Scalable File Storage Solution

## 1. Create an S3 Bucket

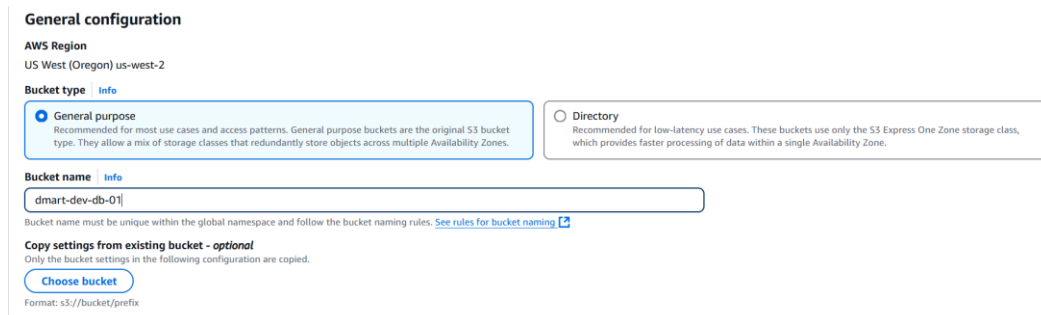
1. Open the AWS Management Console.



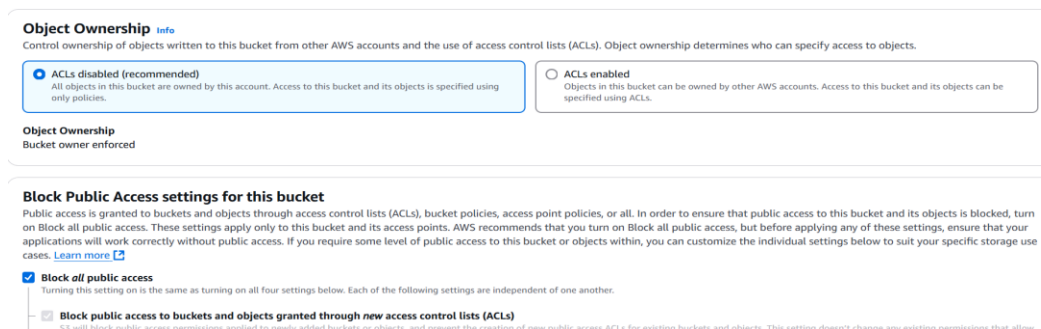
2. Navigate to **S3** and click **Create Bucket**.



3. Provide a unique bucket name, e.g., dmart-dev-db-01.



4. Select the region as per requirement.
5. Under **Block Public Access settings**, select **Block all public access**.



## 6. Enable **Bucket Versioning** (useful for restoring files if deleted or modified).

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

**Bucket Versioning**  
☐ Disable  
☒ Enable

## 7. Click **Create Bucket**.

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

**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](#).

**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

**Advanced settings**

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

[Cancel](#) [Create bucket](#)

## 2. Upload Files to S3

### 1. View the bucket created.

**General purpose buckets (1)** [Info](#) [All AWS Regions](#)  
Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
<a href="#">dmart-dev-db-03</a>	US West (Oregon) us-west-2	<a href="#">View analyzer for us-west-2</a>	January 29, 2025, 11:41:50 (UTC+05:30)

### 2. Open the created bucket.

[Amazon S3](#) > [Buckets](#) > [dmart-dev-db-03](#)

**dmart-dev-db-03** [Info](#)

[Objects](#) [Metadata](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

**Objects (0)** [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)  
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

☐ Show versions

Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.				

[Upload](#)

### 3. Click **Upload**.

**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 (0)** Remove Add files Add folder

All files and folders in this table will be uploaded.

Name	Folder	Type	Size
No files or folders			

You have not chosen any files or folders to upload.

#### 4. Select files from your local system and click **Upload**.

**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 (0)** Remove Add files Add folder

All files and folders in this table will be uploaded.

Name	Folder	Type	Size
No files or folders			

You have not chosen any files or folders to upload.

---

**Files and folders (1 total, 250.4 KB)** Remove Add files Add folder

All files and folders in this table will be uploaded.

Name	Folder	Type	Size
Screenshot (278).png	-	image/png	250.4 KB

**Destination** [Info](#)

**Destination**

[s3://dmart-dev-dlb-03](#)

**Destination details**

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

**Permissions**

Grant public access and access to other AWS accounts.

**Properties**

Specify storage class, encryption settings, tags, and more.

Cancel Upload

#### 5. Verify that the files are uploaded successfully.

**Files and folders (1 total, 250.4 KB)**

Name	Folder
<a href="#">Screenshot (278).png</a>	-

### 3. Grant Public Access to S3 Objects

1. Open the bucket and click on an uploaded file.
2. Copy the **Object URL** and paste it into the browser.

Properties Permissions Versions

**Object overview**

**Owner**  
ashaparakash278

**AWS Region**  
US West (Oregon) us-west-2

**Last modified**  
January 29, 2025, 11:50:31 (UTC+05:30)

**Size**  
250.4 KB

**Type**  
png

**Key**  
Screenshot (278).png

**S3 URI**  
[s3://dmart-dev-db-03/Screenshot \(278\).png](s3://dmart-dev-db-03/Screenshot (278).png)

**Amazon Resource Name (ARN)**  
[arn:aws:s3:::dmart-dev-db-03/Screenshot \(278\).png](arn:aws:s3:::dmart-dev-db-03/Screenshot (278).png)

**Entity tag (Etag)**  
[ddd6d920b83116f0885cb267ebe8eacf](#)

**Object URL**  
[https://dmart-dev-db-03.s3.us-west-2.amazonaws.com/Screenshot+\(278\).png](https://dmart-dev-db-03.s3.us-west-2.amazonaws.com/Screenshot+(278).png)

3. You will see an "Access Denied" error because public access is blocked.

← → ↻ 🔍 dmart-dev-db-03.s3.us-west-2.amazonaws.com/Screenshot+(278).png

⌵

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```

<?xml version="1.0" encoding="UTF-8"?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>XX10X1TQCS39RZSM</RequestId>
  <HostId>FhV0sQx0vGwGHIJYw+YBtU7h4JSr+fZAqf8ReRtougII4VXYC1oRM9wc8FEi01/zRTJdeF/pgQtC=</HostId>
</Error>

```

4. To allow public access:

- Navigate to **Permissions > Bucket Policy**.

dmart-dev-db-03 Info

Objects Metadata Properties **Permissions** Metrics Management Access Points

**Objects (1)**

🔄 Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

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

Find objects by prefix Show versions

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#">Screenshot (278).png</a>	png	January 29, 2025, 11:50:31 (UTC+05:30)	250.4 KB	Standard

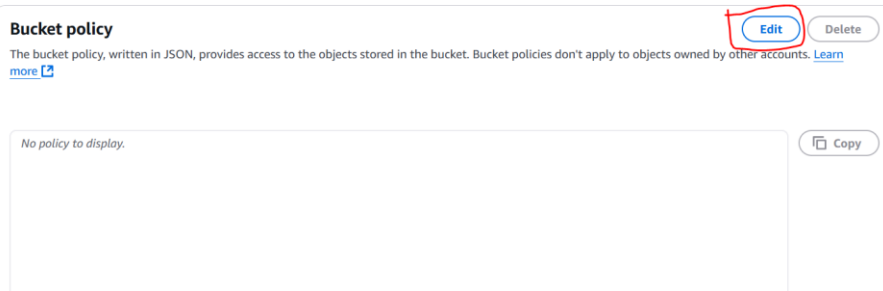
**Block public access (bucket settings)**

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 you 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, b 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 w customize the individual settings below to suit your specific storage use cases. [Learn more](#)

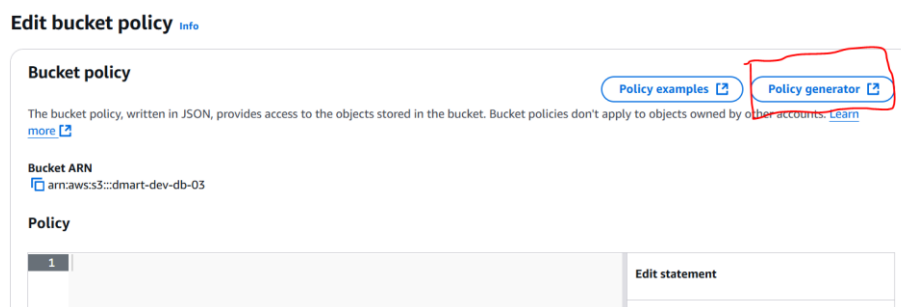
☒ **Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

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

- Click **Edit** and open **Policy Generator**.



- Select **S3 Bucket Policy** and configure the policy for public read access.



- Generate the policy and copy it.

**AWS Policy Generator**

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resource information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

**Step 1: Select Policy Type**

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, Policy, and an SQS Queue Policy.

Select Type of Policy: S3 Bucket Policy

**Step 2: Add Statement(s)**

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect: ☒ Allow ☐ Deny

Principal:

Use a comma to separate multiple values.

AWS Service: Amazon S3 ☐ All Services (\*\*)

Use multiple statements to add permissions for more than one service.

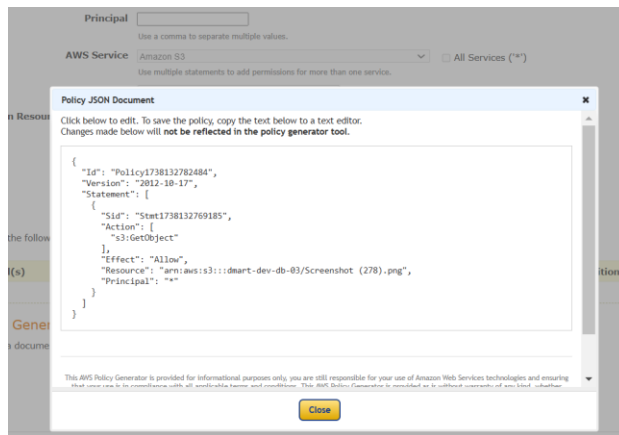
Actions: -- Select Actions -- ☐ All Actions (\*\*)

Amazon Resource Name (ARN):

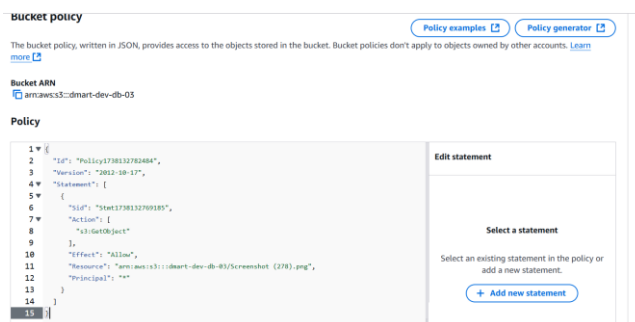
ARNs should follow the following format: arn:aws:s3:::{bucketname}/{keyname}. Use a comma to separate multiple values.

Add Conditions (Optional)

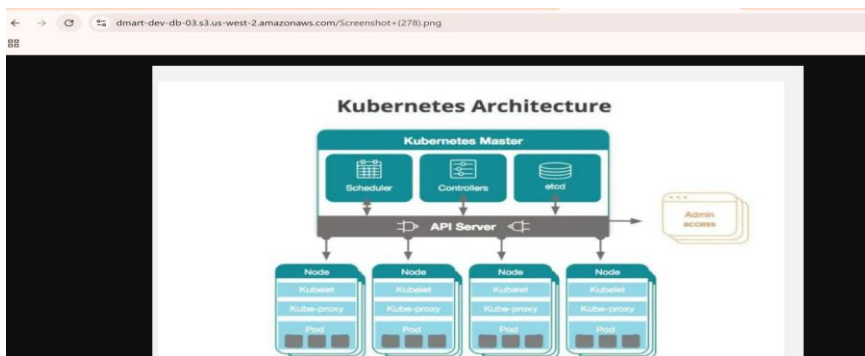
Add Statement No Action selected. You must select at least one Action



- Paste the policy into the **Bucket Policy** editor and save.



5. Now, accessing the file via the URL should be successful.



6. Upload another file and verify whether it is accessible (it will not be accessible until permissions are updated).

**Screenshot (279).png** Info

Copy S3 URI Download Open Object actions

Properties Permissions Versions

**Object overview**

**Owner**  
ashaparakash278

**AWS Region**  
US West (Oregon) us-west-2

**Last modified**  
January 29, 2025, 12:13:54 (UTC+05:30)

**Size**  
318.6 KB

**Type**  
png

**Key**  
Screenshot (279).png

**S3 URI**  
s3://dmart-dev-db-03/Screenshot (279).png

**Amazon Resource Name (ARN)**  
arn:aws:s3:::dmart-dev-db-03/Screenshot (279).png

**Entity tag (Etag)**  
167951c4f94d197e7c2dc36

Object URL Copied

Object URL  
https://dmart-dev-db-03.s3.us-west-2.amazonaws.com/Screenshot+(279).png

dmart-dev-db-03.s3.us-west-2.amazonaws.com/Screenshot+(279).png

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>9JJ3C3HWW93ME4FY</RequestId>
  <HostId>9Wrdsdsvb10+gQ7oZCPC45k5LAagCuEUeoX41f9hQuXQ3cj2itJrceIXwCZxrKLYSjQ3V87H9XKbmr1uha/5kPg==</HostId>
</Error>
```

Again, try to do the same process

#### 4. Enable S3 Static Website Hosting

1. Upload an index.html file to the bucket.

Try to open it; it will open, but not on a website. Instead, it will open in AWS. It will not open on a regular website.

**static\_web.html.png** Info

Copy S3 URI Download Open Object actions

Properties Permissions Versions

**Object overview**

**Owner**  
ashaparakash278

**AWS Region**  
US West (Oregon) us-west-2

**Last modified**  
January 29, 2025, 12:23:38 (UTC+05:30)

**Size**  
318.6 KB

**Type**  
png

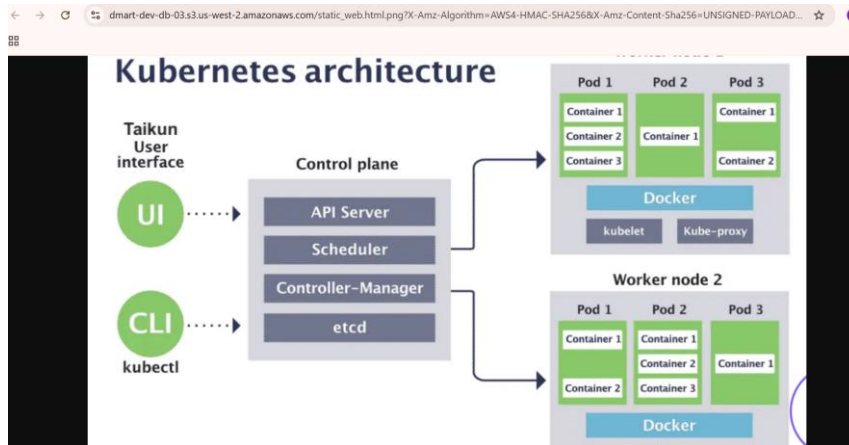
**Key**  
static\_web.html.png

**S3 URI**  
s3://dmart-dev-db-03/static\_web.html.png

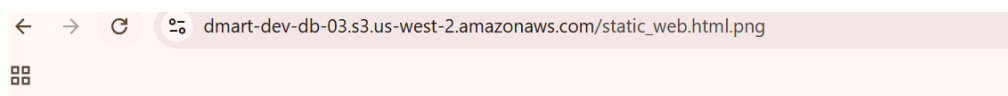
**Amazon Resource Name (ARN)**  
arn:aws:s3:::dmart-dev-db-03/static\_web.html.png

**Entity tag (Etag)**  
166f34b2d367951c4f94d197e7c2dc36

**Object URL**  
https://dmart-dev-db-03.s3.us-west-2.amazonaws.com/static\_web.html.png



Opening through url:

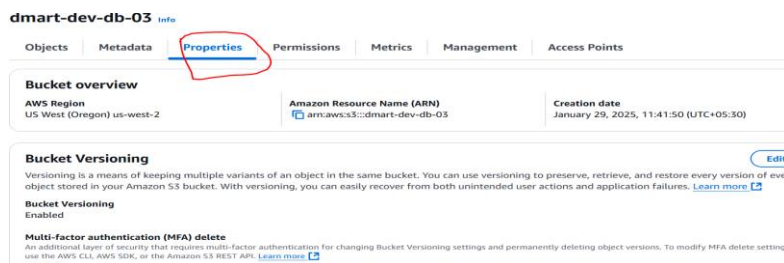


This XML file does not appear to have any style information associated with it. The document tree is shown below.

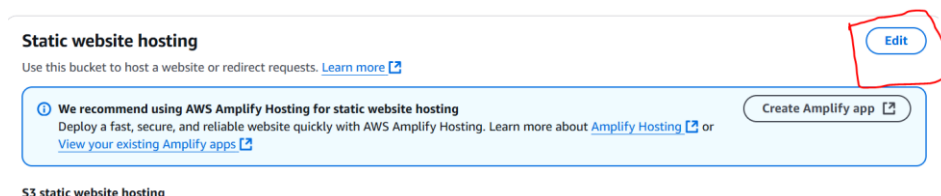
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>56960SH8CSWM7GPP</RequestId>
  <HostId>FBe08KaF8L/8+ME9HV552Ae8wb13pNqzZGdD7G44c6WTT19Yao06A99LKnTcrXt5GpWbtbe9rI=</HostId>
</Error>
```

## 2. Enable **Static Website Hosting**:

- Open the bucket and go to **Properties**.



- Click **Edit** in the **Static Website Hosting** section.



- Enable it and specify **index.html** as the index document.



**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](#)

**Index document**  
Specify the home or default page of the website.

static\_web.html.png

**Error document - optional**  
This is returned when an error occurs.

error.html

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

- Save the configuration.

- The index.html file will now open when accessed via the AWS S3 static website endpoint.

**Static website hosting** [Edit](#)

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

**We recommend using AWS Amplify Hosting for static website hosting**  
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. [Learn more about Amplify Hosting](#) or [View your existing Amplify apps](#) [Create Amplify app](#)

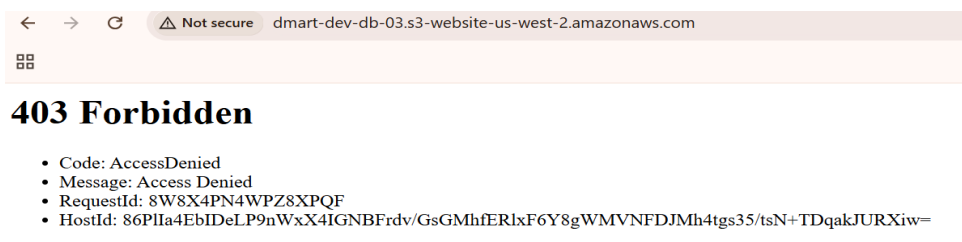
**S3 static website hosting**  
Enabled

**Hosting type**  
Bucket hosting

**Bucket website endpoint**  
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

<http://dmart-dev-db-03.s3-website-us-west-2.amazonaws.com>

- If you open the file directly in AWS, it will open, but it will not function as a website until public access is enabled and the correct policies are set.



- Go to **Permissions > Bucket Policy** and add:

### Bucket policy

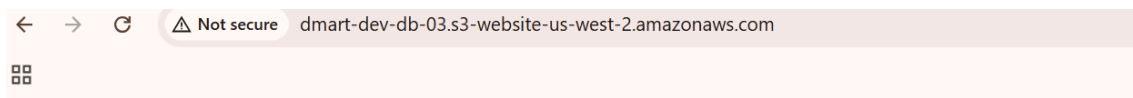
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

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

```
{
  "Version": "2012-10-17",
  "Id": "Policy1738132782484",
  "Statement": [
    {
      "Sid": "Stmnt1738132769185",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3::dmart-dev-db-03/static_web.htm"
    }
  ]
}
```

[Copy](#)

6. Save the changes.
7. The static website is now accessible via the provided S3 static website endpoint.

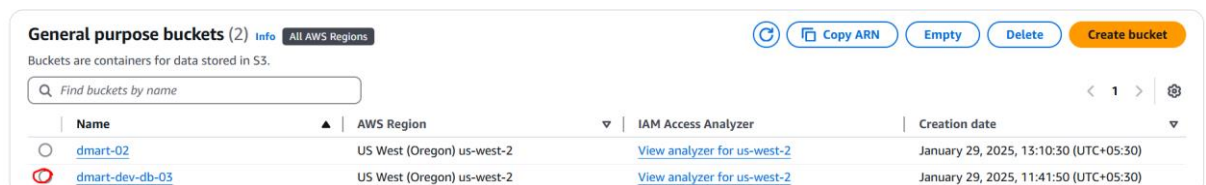


## Lorem Ipsum

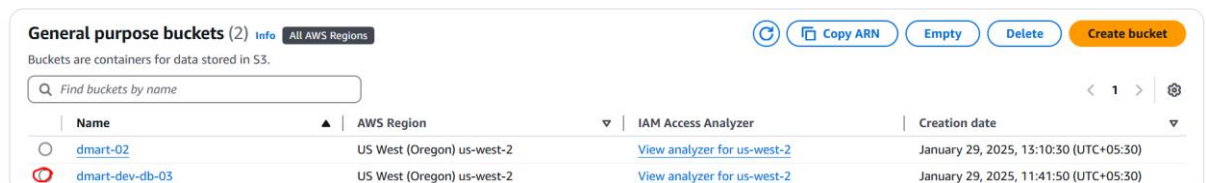
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam vel laoreet ante, id luctus nibh. Vestibulum a porttitor nibh. Vivamus fringilla tincidunt. Quisque tortor sapien, imperdiet sit amet euismod elementum, imperdiet nec elit. Phasellus tellus velit, lacinia nec vestibulum vel, sagittis rutrum leo. Quisque mollis tempor leo nec aliquam. Fusce eu eros quis nibh malesuada rhoncus ut ac venenatis lobortis, lorem purus interdum magna, ac dignissim purus felis eu dolor. Fusce at quam vel velit vestibulum ultricies. Nunc efficitur. Integer gravida tincidunt elit, eu eleifend lectus fringilla vel.

## 5. Configure S3 Replication for Backup

1. Create another bucket as a backup bucket.



2. Open the main bucket (dmart-dev-db-01) and navigate to **Replication Rules**.



3. Create a **Replication Rule**:
  - Choose the backup bucket as the destination.

**dmart-dev-db-03** info

Objects Metadata Properties Permissions Metrics **Management** Access Points

**Objects (3)** [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

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

☐ Show versions

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#">Screenshot (278).png</a>	png	January 29, 2025, 11:50:31 (UTC+05:30)	250.4 KB	Standard
<input type="checkbox"/>	<a href="#">Screenshot (279).png</a>	png	January 29, 2025, 12:13:54 (UTC+05:30)	318.6 KB	Standard
<input type="checkbox"/>	<a href="#">static_web.htm</a>	htm	January 29, 2025, 12:49:11 (UTC+05:30)	4.0 KB	Standard

**Replication rules (0)** [View details](#) [Edit rule](#) [Delete](#) [Actions](#) [Create replication rule](#)

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. [Learn more](#)

Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects (SSE-KMS or DSSE-KMS)	Replica modification sync
No replication rules										

You don't have any rules in the replication configuration.

[Create replication rule](#)

- Create a new IAM role to manage replication.

**Replication rule configuration**

**Replication rule name**

Up to 255 characters. In order to be able to use CloudWatch metrics to monitor the progress of your replication rule, the replication rule name must only contain English characters.

**Status**

Choose whether the rule will be enabled or disabled when created.

☒ Enabled

☐ Disabled

**Priority**

The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication rules table.

**Source bucket**

**Source bucket name**

**Source Region**

Choose a rule scope

☐ Limit the scope of this rule using one or more filters

☒ Apply to all objects in the bucket

**Destination**

**Destination**

You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. [Learn more](#)

☒ Choose a bucket in this account

☐ Specify a bucket in another account

**Bucket name**

Choose the bucket that will receive replicated objects.

[Browse S3](#)

**Destination Region**

4. Save the rule.
5. Upload a new file to the main bucket and verify that it is automatically replicated in the backup bucket.

**dmart-02** info

Objects Metadata Properties Permissions Metrics Management Access Points

**Objects (1)** [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

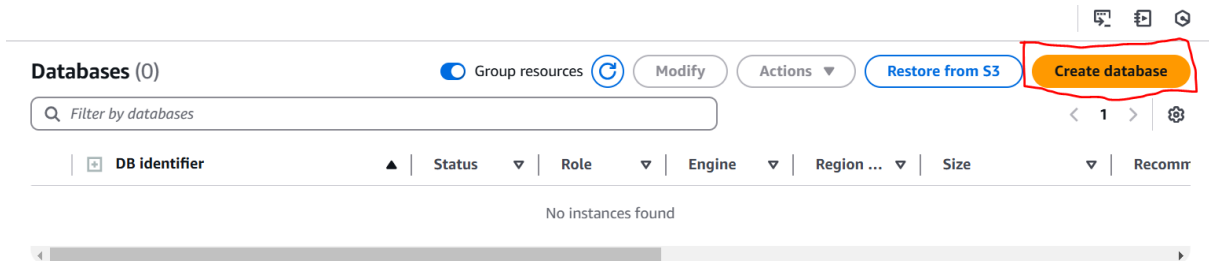
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

☐ Show versions

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	<a href="#">Screenshot (250).png</a>	png	January 29, 2025, 13:17:59 (UTC+05:30)	505.3 KB	Standard

## 6. Set Up RDS (MySQL Database)

1. Open AWS and search for **RDS**.
2. Click **Create Database**.



3. Select **MySQL** as the engine type.

**Choose a database creation method**

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

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

**Engine options**

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

☐ Aurora (MySQL Compatible)

☐ Aurora (PostgreSQL Compatible)

☒ **MySQL**

☐ PostgreSQL

4. Choose **Free Tier** template.

**Templates**  
Choose a sample template to meet your use case.

☐ **Production**  
Use defaults for high availability and fast, consistent performance.

☐ **Dev/Test**  
This instance is intended for development use outside of a production environment.

☒ **Free tier**  
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. [Info](#)

**Availability and durability**

5. Set:
  - **Username:** admin
  - **Password:** admin@123
6. Configure storage:
  - **Allocated Storage:** 500GB
  - **Maximum Storage:** 1000GB
7. Enable **Public Access**.

8. Click **Create Database**.

## 7. Configure Security Group for MySQL Access

1. Navigate to **EC2 > Security Groups**.
2. Locate the security group associated with the RDS instance.
3. Edit inbound rules to allow MySQL (port 3306) from your IP or a specific range.

## Conclusion

This process establishes a **Scalable File Storage Solution** by leveraging AWS S3 for storage, enabling replication for backup, and setting up an RDS database for managing structured data. The system ensures high availability and scalability while maintaining security and controlled access.