Guided Lab: Creating an Amazon S3 bucket

Description

Amazon Simple Storage Service (S3) is a secure, durable, and highly scalable object storage solution. It allows you to upload multimedia files such as photos, videos, and static documents by creating a logical storage bucket within an AWS region. With your bucket set up, you can easily upload numerous objects. Both buckets and objects are valuable resources, and Amazon S3 offers you the flexibility to manage them through APIs and a user-friendly web console.

Amazon S3 can function independently or be used with other AWS services, including Amazon EC2, Amazon Elastic Block Store (Amazon EBS), and Amazon Glacier. It's also compatible with third-party storage solutions and gateways. This cost-effective object storage service caters to many use cases, including web applications, content distribution, backup and archiving, disaster recovery, and big data analytics.

This lab will help you create buckets and establish policies for efficient access management and restrictions.

Objectives

In this lab, you will:

- Learn how to create an S3 bucket in the AWS Console
- Learn how to implement bucket policies to manage and restrict access.
- Learn how to upload and download objects in an S3 bucket.

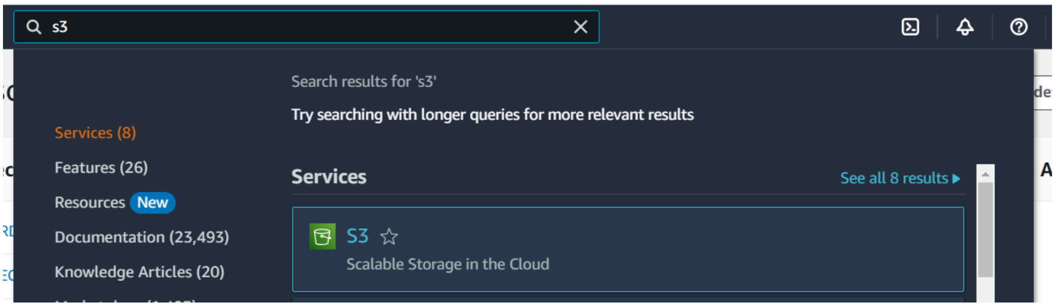
Subscribe to access AWS

PlayCloud Labs

Lab Steps

Creating an S3 Bucket

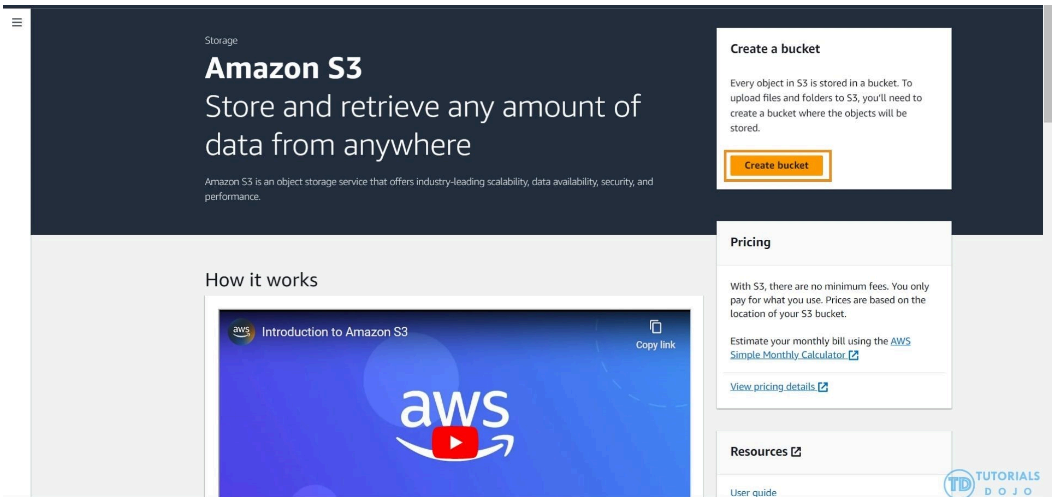
1. In the AWS Management Console, search for “S3” using the search bar and select the S3 result under Services.



Search results for 's3'

Try searching with longer queries for more relevant results

2. Once you’re in the S3 console, click the Create Bucket button.



Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

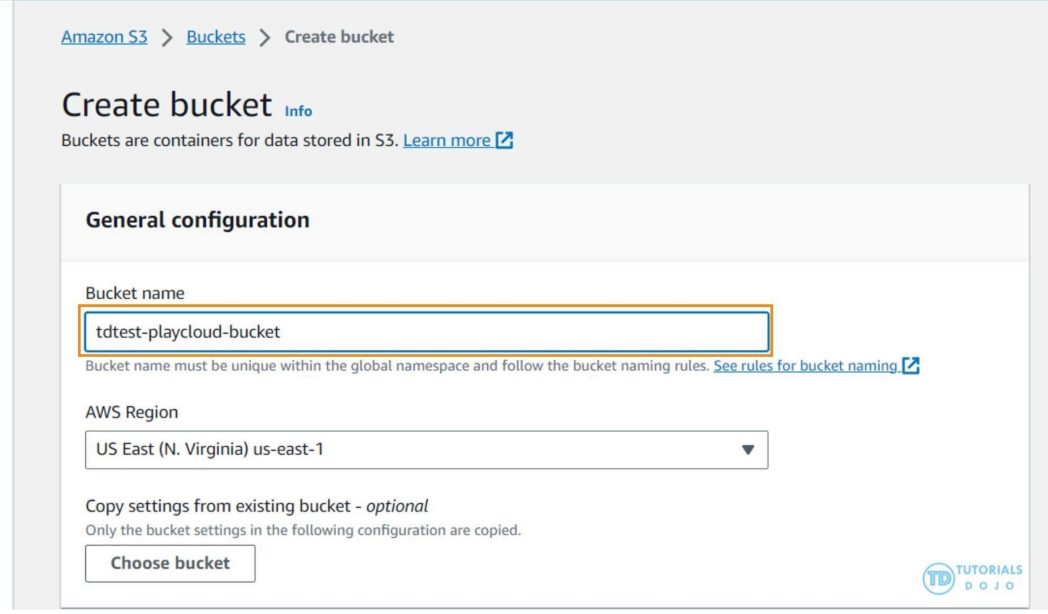
Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

3. Enter a unique name for your bucket, such as *tdtest-playcloud-bucket* or any preferred name, in the Name field.

- For the region, select US East (N. Virginia).



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name: tdtest-playcloud-bucket

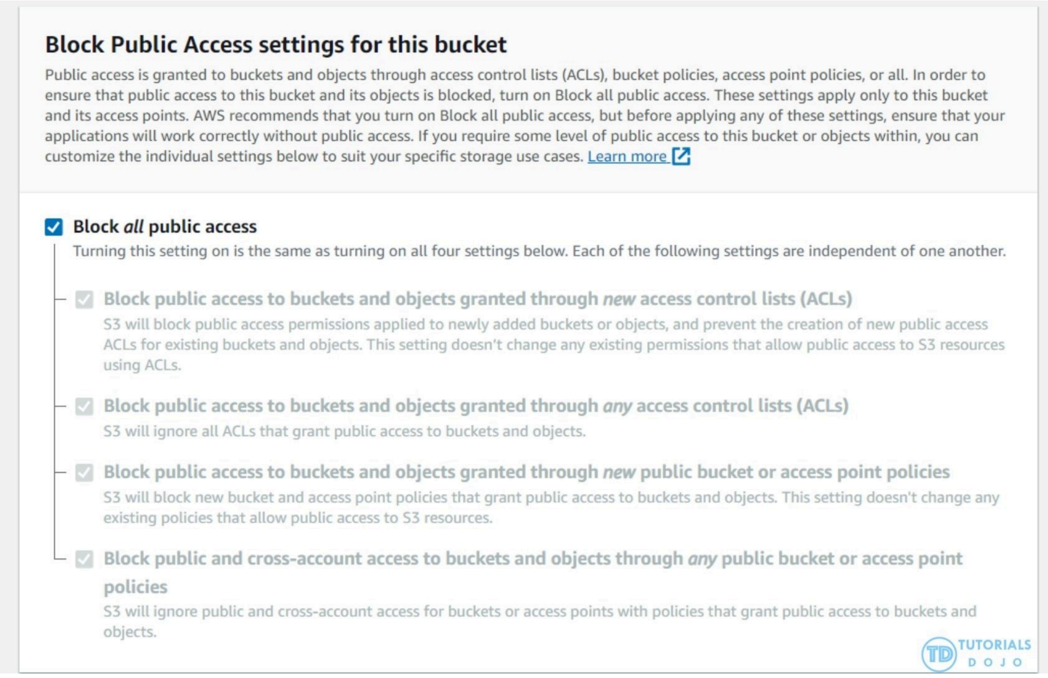
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

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

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

4. Leave the Block public access (bucket settings) at the default values. This is where you can set public access permissions.



Block Public Access settings for this bucket

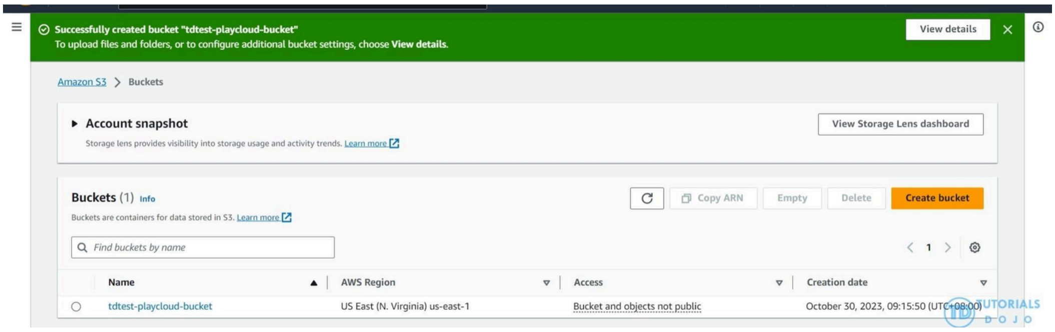
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access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

☑ Block *all* public access

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

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

5. Click on Create bucket. You should see a green notification that your bucket was created successfully.



Successfully created bucket "tdtest-playcloud-bucket"

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. Learn more

Buckets (1) Info

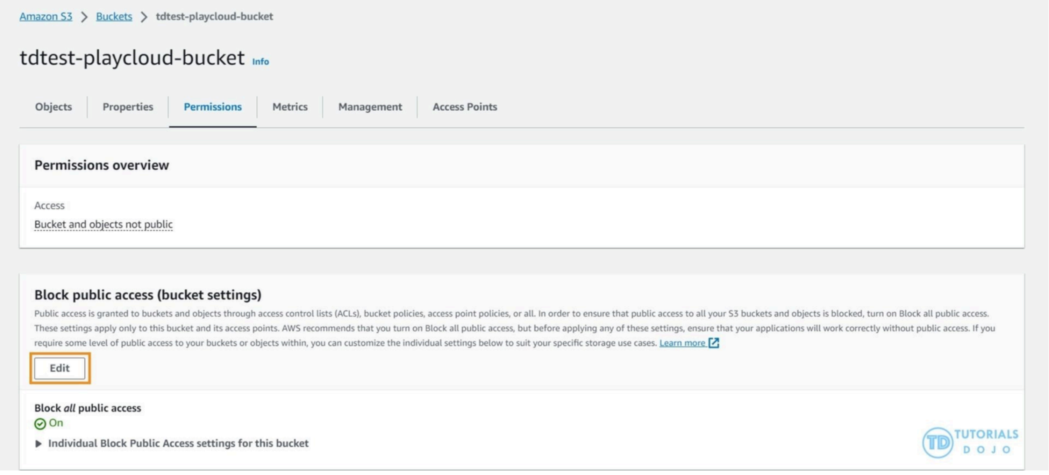
Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	tdtest-playcloud-bucket	US East (N. Virginia) us-east-1	Bucket and objects not public	October 30, 2023, 09:15:50 (UTC+08:00)

Implementing bucket policies to manage and restrict access

1. In the Buckets table, click the name of your bucket in the Name column. This will take you to a page with tabs at the top.

2. Click the Permissions tab and select Edit in the Block public access section.



Amazon S3 > Buckets > tdtest-playcloud-bucket
tdtest-playcloud-bucket Info
Objects
Properties
Permissions
Metrics
Management
Access Points

Permissions overview

Access

Bucket and objects not public

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

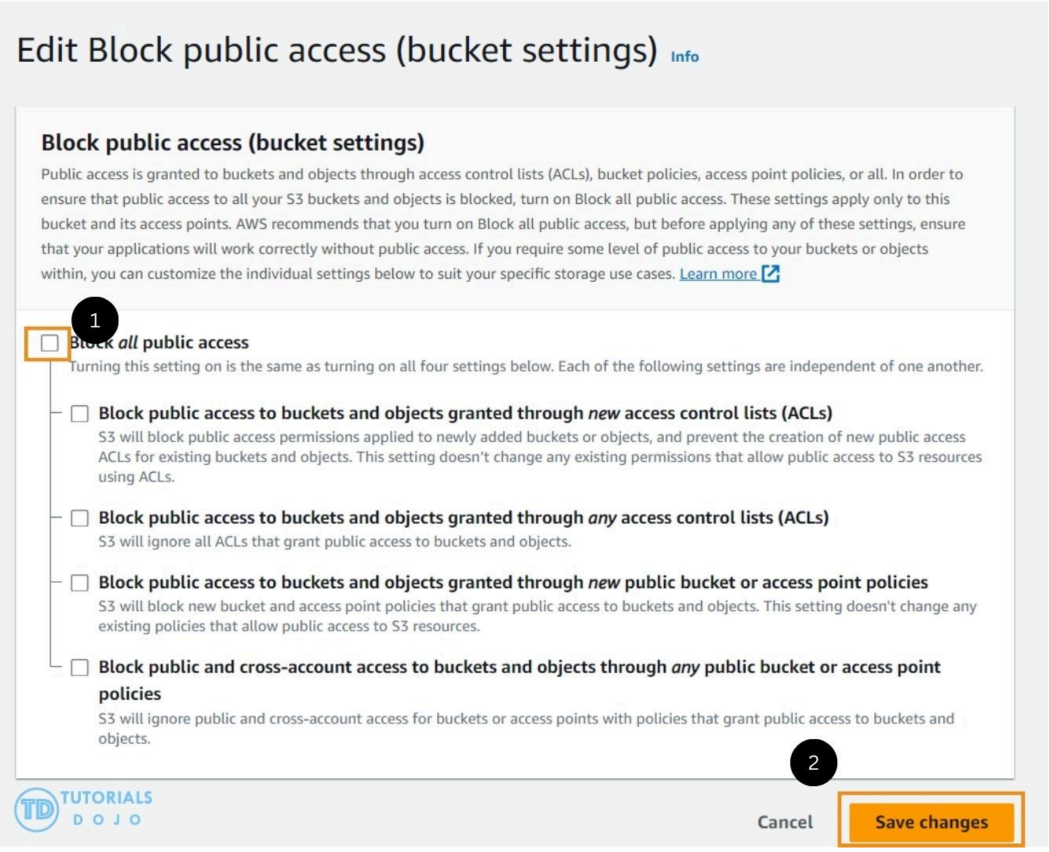
Block *all* public access

✓ On

▶ Individual Block Public Access settings for this bucket

2. Uncheck all the options. However, please note that allowing public access to S3 buckets is serious, and you should be cautious before deciding. AWS has implemented various security features to prevent data breaches, and granting public access may pose a risk of unauthorized data access.

3. There is no sensitive data for this lab. Thus, we will set it to allow public access. Therefore, you can proceed with disabling the Block all public access feature.



Edit Block public access (bucket settings) Info

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

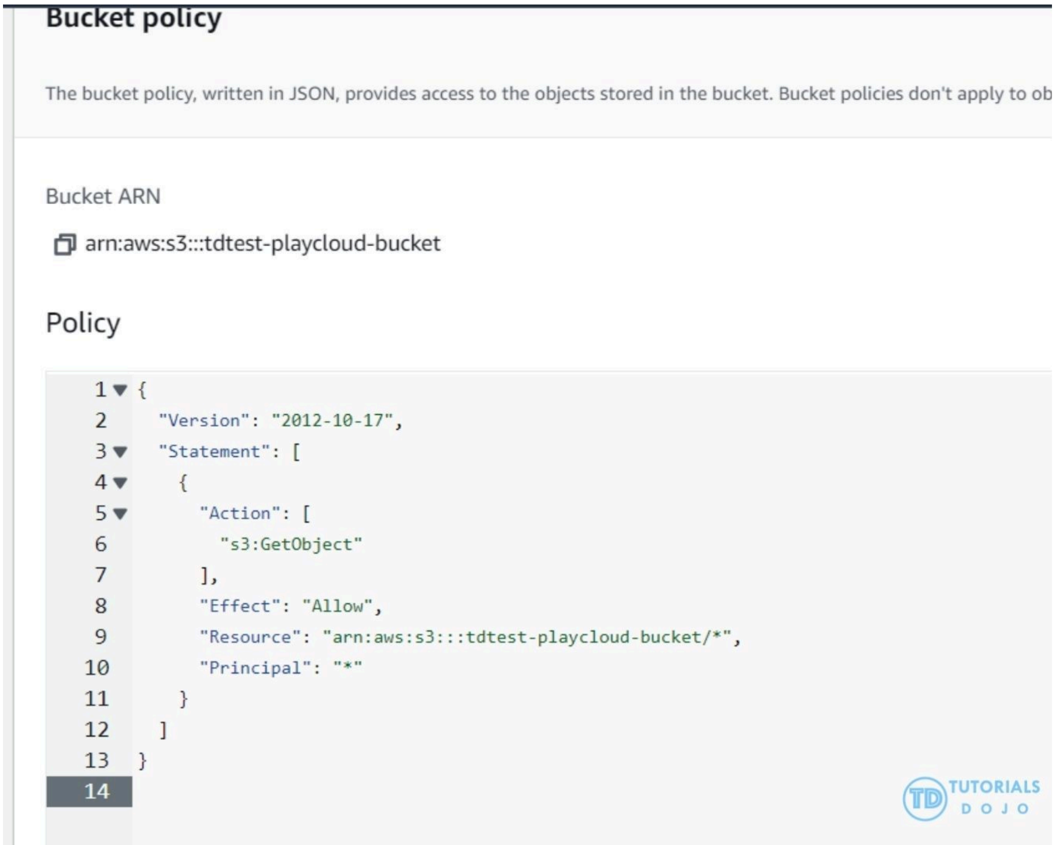
- □ Block public access to buckets and objects granted through *new* access control lists (ACLs)
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing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

4. Click on Save Changes at the bottom of the page. A confirmation dialog box will appear. Enter “confirm” in the box and click Confirm. You will see a green notification that the public access settings have been edited.

5. Please note that simply turning off the “**Block all public access**” setting in an Amazon S3 bucket does not automatically make the objects within it publicly accessible. To grant public access to these objects, explicit permissions must be defined in the bucket policy.

6. In this lab, we will use a Bucket policy to grant public access to your Amazon S3 bucket. To do this, scroll to the Bucket policy section and select Edit.

7. On the Edit bucket policy page, specify a JSON policy to control your Amazon S3 bucket access. Replace the contents of the Policy editor with the permissive policy provided below.



Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to ob

Bucket ARN

arn:aws:s3:::tdtest-playcloud-bucket

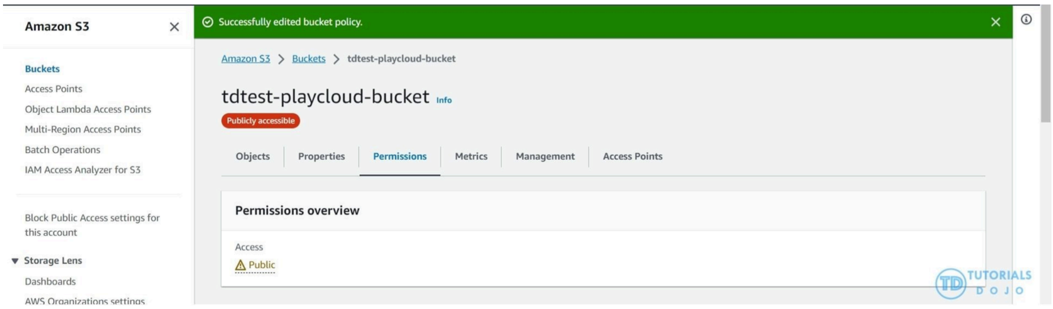
Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::tdtest-playcloud-bucket/*",
      "Principal": "*"
    }
  ]
}
```

8. Replace the Resource key with the ARN of the bucket you created. To do this, click on the copy icon under Bucket ARN and paste the ARN in the value of the Resource key. Ensure that you preserve the `/*` at the end of the value, apply the policy to all objects inside the bucket recursively.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "BUCKET_ARN/*",
      "Principal": "*"
    }
  ]
}
```

9. Click on Save Changes at the bottom of the page. You will see a green notification that the bucket policy was edited.


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Amazon S3 > Buckets > tdtest-playcloud-bucket
Objects
Properties
Permissions
Metrics
Management
Access Points
TUTORIALS DOJO

Successfully edited bucket policy.

tdtest-playcloud-bucket Info

Publicly accessible

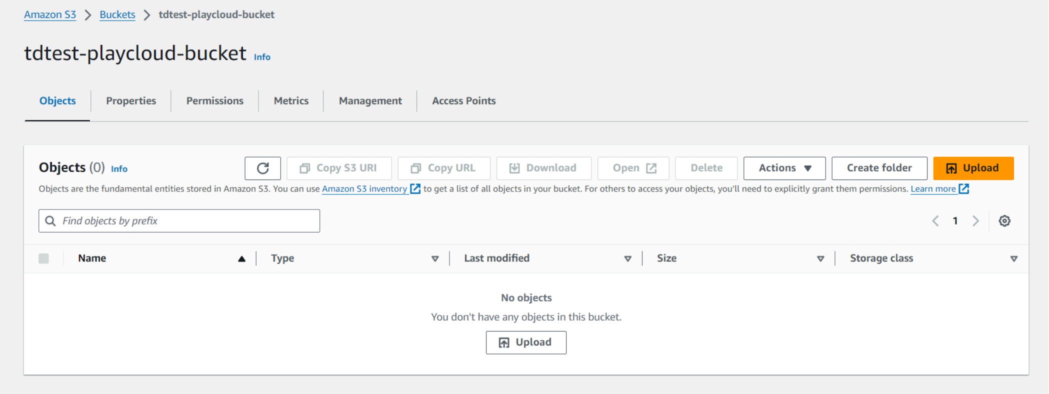
Permissions overview

Access: Public

Please note that poorly managed Amazon S3 permissions can lead to unauthorized data access. AWS ensures you understand the implications of allowing public access to an Amazon S3 bucket. Therefore, it is advisable to carefully consider the impact before granting public access.

Uploading and Downloading Objects in a S3 Bucket

1. In your S3 bucket, click the **Upload** button.



tdtest-playcloud-bucket Info

Objects (0) Info

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

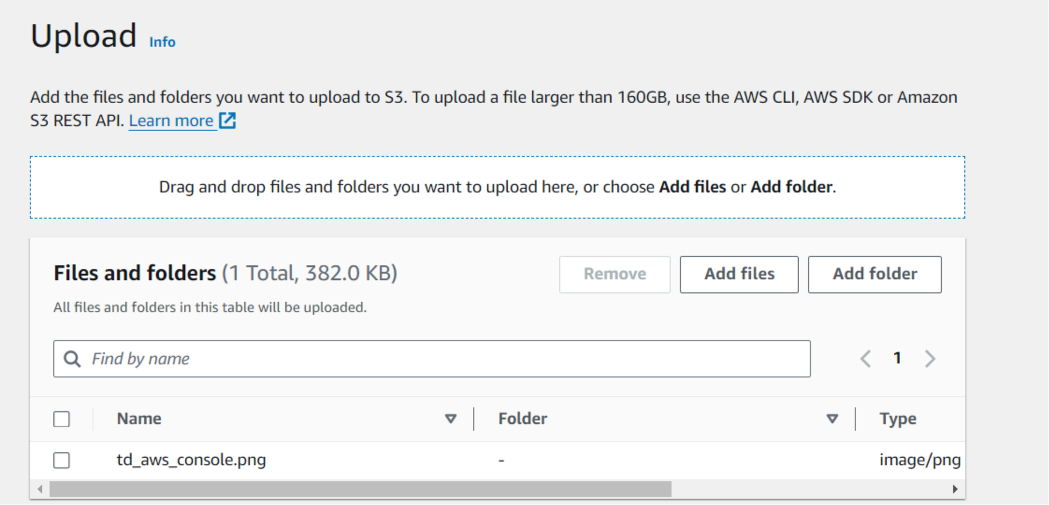
Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

2. Download and save the following file to your computer and upload it to your S3 bucket. You may upload by either browsing and selecting or dragging and dropping. If you prefer to browse and select, click **Add Files**.

https://media.tutorialsdojo.com/public/td_aws_console.png



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 SDK or Amazon S3 REST API. Learn more

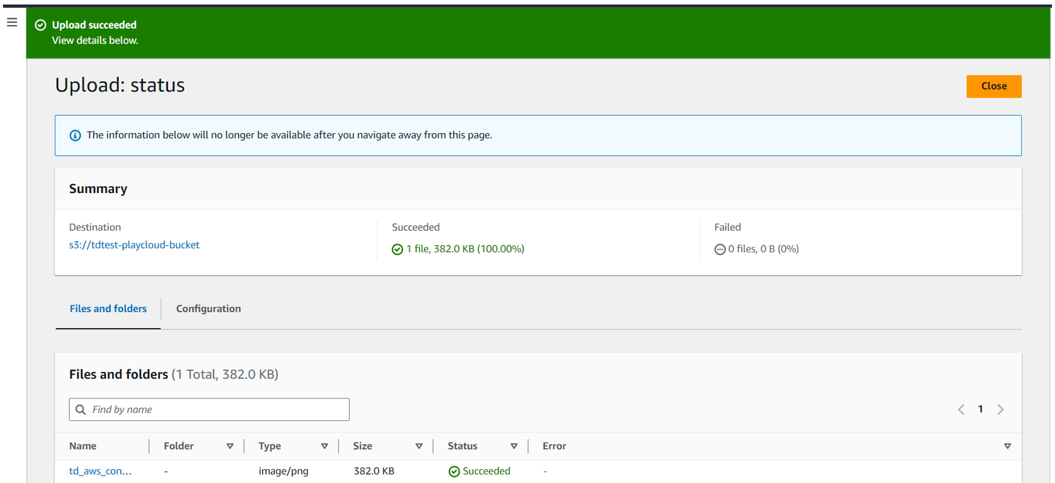
Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 Total, 382.0 KB)

All files and folders in this table will be uploaded.

□	Name	Folder	Type
□	td_aws_console.png	-	image/png

3. Scroll down to the page's bottom and select **Upload** to initiate the file upload process. A blue notification will indicate that the file is currently uploading, followed by a green notification confirming the successful completion of the upload.



Upload succeeded
View details below.

Upload: status

Close

The information below will no longer be available after you navigate away from this page.

Summary

Destination
s3://tdtest-playcloud-bucket

Succeeded
1 file, 382.0 KB (100.00%)

Failed
0 files, 0 B (0%)

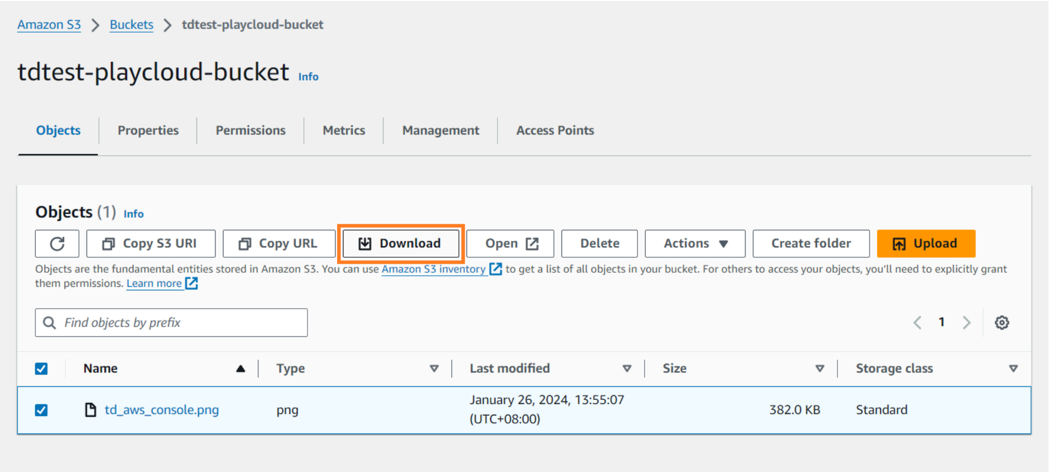
Files and folders | Configuration

Files and folders (1 Total, 382.0 KB)

Find by name

Name	Folder	Type	Size	Status	Error
td_aws_con...	-	image/png	382.0 KB	Succeeded	-

4. To download the object, go to your S3 bucket, select the object, and click on the Download button.



Amazon S3 > Buckets > tdtest-playcloud-bucket

tdtest-playcloud-bucket Info

Objects | Properties | Permissions | Metrics | Management | Access Points

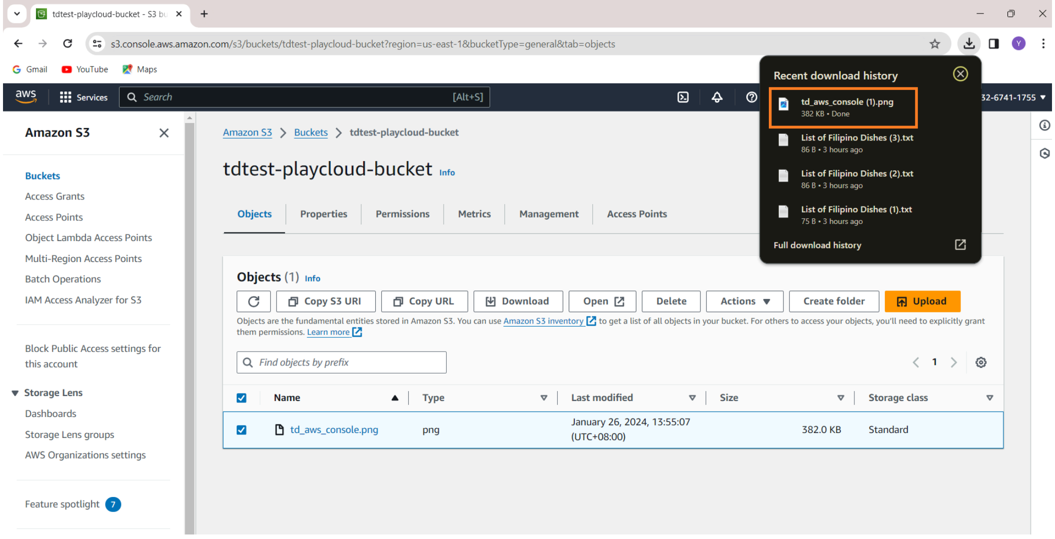
Objects (1) Info

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

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

Find objects by prefix

☑	Name	Type	Last modified	Size	Storage class
☑	td_aws_console.png	png	January 26, 2024, 13:55:07 (UTC+08:00)	382.0 KB	Standard



tdtest-playcloud-bucket - S3 b

s3.console.aws.amazon.com/s3/buckets/tdtest-playcloud-bucket?region=us-east-1&bucketType=general&tab=objects

Gmail | YouTube | Maps

Services | Search | [Alt+S]

Recent download history

td_aws_console (1).png
382 KB • Done

List of Filipino Dishes (3).txt
86 B • 3 hours ago

List of Filipino Dishes (2).txt
86 B • 3 hours ago

List of Filipino Dishes (1).txt
75 B • 3 hours ago

Full download history

Amazon S3

Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings

Feature spotlight 7

Amazon S3 > Buckets > tdtest-playcloud-bucket

tdtest-playcloud-bucket Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (1) Info

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

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

Find objects by prefix

☑	Name	Type	Last modified	Size	Storage class
☑	td_aws_console.png	png	January 26, 2024, 13:55:07 (UTC+08:00)	382.0 KB	Standard