

## whatismy1storage Info

Objects

Metadata

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 us-east-1](#)

### Block public access (bucket settings)

Edit

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

Off

Individual Block Public Access settings for this bucket

### Bucket policy

Edit

Delete

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](#)

{

Copy

```
{
  "Effect": "Allow",
  "Principal": "*",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::whatismy1storage/*"
}
```

### Object Ownership Info

Edit

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 enforced

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

### Access control list (ACL)

Edit

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

This bucket has the bucket owner enforced setting applied for Object Ownership  
When [bucket owner enforced](#) is applied, use bucket policies to control access. [Learn more](#)

Grantee	Objects	Bucket ACL
<b>Bucket owner (your AWS account)</b> Canonical ID: <a href="#">b1a6bcb3f67f20914fad9b2efe756c76cbe068e74a01cc850bf0bc433f03607</a>	List, Write	Read, Write
<b>Everyone (public access)</b> Group: <a href="#">http://acs.amazonaws.com/groups/global/AllUsers</a>	-	-
<b>Authenticated users group (anyone with an AWS account)</b> Group: <a href="#">http://acs.amazonaws.com/groups/global/AuthenticatedUsers</a>	-	-
<b>S3 log delivery group</b> Group: <a href="#">http://acs.amazonaws.com/groups/s3/LogDelivery</a>	-	-

### Cross-origin resource sharing (CORS)

Edit

The CORS configuration, written in JSON, defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. [Learn more](#)

No configurations to display

Copy

Account ID: 7546-2191-8308

usd4h4/aaa4272205+2403a51451qmuuwhu3n

United States (N. Virginia)

Alt+S

Search

Amazon S3 > Buckets > whatismy1storage

whatismy1storage

ObjectsMetadataPropertiesPermissionsMetricsManagementAccess Points

Bucket overview

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

Amazon Resource Name (ARN)  
arn:aws:s3::whatismy1storage

Creation date  
August 23, 2025, 16:06:07 (UTC+05:45)

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  
Disabled

Multi-factor authentication (MFA) delete  
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Tags (0)

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

Key	Value
-----	-------

CloudShellFeedback© 2025, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

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  
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

Enabled

Intelligent-Tiering Archive configurations (0)

[View details](#)[Edit](#)[Delete](#)[Create configuration](#)

Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. [Learn more](#)

Find Intelligent-Tiering Archive configurations

Name	Status	Scope	Days until transition to Archive Acc...	Days until transition to Deep Archi...
No archive configurations No configurations to display.				

Create configuration

Server access logging

Log requests for access to your bucket. Use [CloudWatch](#) to check the health of your server access logging. [Learn more](#)

Server access logging  
Disabled

AWS CloudTrail data events (0)

[Configure in CloudTrail](#)

Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. [Learn more](#)

Name	Access
No data events No data events to display.	

Configure in CloudTrail

Event notifications (0)

[Edit](#)[Delete](#)[Create event notification](#)

Send a notification when specific events occur in your bucket. [Learn more](#)

Name	Event types	Filters	Destination type	Destination
No event notifications Choose Create event notification to be notified when a specific event occurs.				

Create event notification

Amazon EventBridge

For additional capabilities, use Amazon EventBridge to build event-driven applications at scale using S3 event notifications. [Learn more](#) or see [EventBridge pricing](#)

Send notifications to Amazon EventBridge for all events in this bucket  
Off

Transfer acceleration

Use an accelerated endpoint for faster data transfers. [Learn more](#)

Transfer acceleration  
Disabled

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

Object Lock  
Disabled

Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays  
Disabled

Static website hosting

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://whatismy1storage.s3-website-us-east-1.amazonaws.com>

## Create bucket [Info](#)

Buckets are containers for data stored in S3.

### General configuration

#### AWS Region

US East (N. Virginia) us-east-1

#### Bucket type [Info](#)

##### ☒ General purpose

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

##### ☐ Directory

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

#### Bucket name [Info](#)

myawsbucket

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

#### Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

### 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.

##### ☒ 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

### 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 is 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.

### 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

#### Tags - optional (0)



Amazon S3 > Buckets > Create bucket

[Add new tag](#)

You can add up to 50 tags.

### Default encryption [Info](#)

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](#)

Amazon S3

General purpose buckets

Directory buckets

Table buckets

Vector buckets

Access Grants

Access Points (General Purpose Buckets, FSx file systems)

Access Points (Directory Buckets)

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 11


Amazon S3 > Buckets > whatismy1storage


Objects (8)





 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](#)

☐

Name

▲

Type

▼

Last modified

▼


Size

▼

Storage class

▼

☐

 [ABOUT THIS TEMPLATE.txt](#)


txt

August 20, 2025, 16:11:00 (UTC+05:45)

453.0 B

Standard

☐

 [about.html](#)


html

August 20, 2025, 16:11:01 (UTC+05:45)

8.9 KB

Standard

☐

 [assets/](#)


Folder

-

-

-

☐

 [contact.html](#)


html

August 20, 2025, 16:10:57 (UTC+05:45)

9.8 KB

Standard

☐

 [index.html](#)


html

August 20, 2025, 16:10:57 (UTC+05:45)

10.4 KB

Standard

☐

 [products.html](#)


html

August 20, 2025, 16:10:58 (UTC+05:45)

11.0 KB

Standard

☐

 [single-product.html](#)


html

August 20, 2025, 16:10:59 (UTC+05:45)

12.8 KB

Standard

☐

 [vendor/](#)

Folder

-

-

-



## Bucket ARN

arn:aws:s3::whatismy1storage

## Policy

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": "*",
7       "Action": "s3:GetObject",
8       "Resource": "arn:aws:s3:::whatismy1storage/*"
9     }
10  ]
11 }
```

### Edit statement

### Select a statement

Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

CloudShell Feedback

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

[+ Add new statement](#)

JSON Ln 11, Col 1

🛡️ Security: 0 🚫 Errors: 0 ⚠️ Warnings: 0 💡 Suggestions: 0

[Preview external access](#)

### ⚠️ You need permissions

User: arn:aws:sts::754621515506:assumed-role/voclabs/user4272065=2403a51461@sru.edu.in is not authorized to perform: access-analyzer:ValidatePolicy on resource: arn:aws:access-analyzer:us-east-1:754621515506:\*

[🔍 Diagnose with Amazon Q](#)

Cancel

Save changes

## Ecommerce HTML Template

Pixel HTML Template can be converted into your desired CMS theme. Total **5 pages** included. You can use this Bootstrap v4.1.3 layout for any CMS.

Please tell your friends about [Tooplate](#) free template site. Thank you. Photo credit goes to [Pexels website](#).

[ORDER NOW!](#)

## Featured Items



Proin vel ligula  
\$15.00



Erat odio rhoncus  
\$25.00



Integer vel turpis  
\$35.00



Sed purus quam  
\$45.00



## Subscribe on PIXIE now!

Integer vel turpis ultricies, lacinia ligula id, lobortis augue. Vivamus porttitor dui id dictum efficitur. Phasellus vel interdum elit.

[SUBSCRIBE NOW!](#)