

aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

Shivani R Shankar

Global

Support

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Successfully created bucket "mybucketshi"

To upload files and folders, or to configure additional bucket settings choose [View details](#).

Follow security best practices for S3.

[Learn more](#)

Amazon S3

Account snapshot

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)

Buckets (2)

Info

Refresh

Copy ARN

Empty

Delete

Create bucket

Find buckets by name

< 1 >

Settings

	Name	AWS Region	Access	Creation date
<input type="radio"/>	elasticbeanstalk-us-west-1-680352856869	US West (N. California) us-west-1	Objects can be public	September 30, 2021, 12:53:26 (UTC+05:45)
<input type="radio"/>	mybucketshi	US West (N. California) us-west-1	Bucket and objects not public	September 30, 2021, 13:33:50 (UTC+05:45)

Activate Windows
Go to Settings to activate Windows.

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > mybucketshi

mybucketshi

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (1)

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](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

< 1 >

	Name	Type	Last modified	Size	Storage class
	Capture1.PNG	PNG	September 30, 2021, 13:35:28 (UTC+05:45)	53.5 KB	Standard

Activate Windows

Go to Settings to activate Windows.

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

```
▼ <Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>P9TBQJNBXXW2Y5AT</RequestId>
  <HostId>tNrnS8sTo3RYKJ#N/S/mNQvLzk2hnBvUR9oCf1xbFHJhCFNmpvEnXXWdY6svA2m1R75pxmhqaLr8=</HostId>
</Error>
```

Activate Windows
Go to Settings to activate Windows.

aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

Shivani R Shankar

Global

Support

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > mybucketshi > Edit Block public access (bucket settings)

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

Feedback

English (US)

© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

Cookie preferences

Activate Windows
Go to Settings to activate Windows.

aws

Services

Q

Search for services, features, marketplace products, and docs

[Alt+S]

Shivani R Shankar

Global

Support

☰

✔ Successfully edited public access

View details below.

✕

Make public: status

Close

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

Summary

Source	Successfully edited public access	Failed to edit public access
s3://mybucketshi	✔ 1 object, 53.5 KB	0 objects

Failed to edit public access

Configuration

⊗ Failed to edit public access (0)

Q Find objects by name

Activate Windows 1 >

Go to Settings to activate Windows.

Feedback

English (US)

© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

Cookie preferences

Capture1.PNG (1362x612) x>Welcome x>Elastic Beanstalk x>Elastic Beanstalk x>i-0d6b276c9715a9a5d (Serve x>+ x>

mybucketshi.s3.us-west-1.amazonaws.com/Capture1.PNG

Star x

aws

Services

Search for services, features, marketplace products, and docs [Alt+S]

Shivani R Shankar Global Support

Identity and Access Management (IAM)

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report

Feedback English (US)

Introducing the new Users list experience

We've redesigned the Users list experience to make it easier to use. [Let us know what you think.](#)

The user **Chocolate** have been created.

IAM > Users

Users (1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

< 1 >

Refresh Delete Add users

	User name	Groups	Last activity	MFA	Password a...	Active
<input type="checkbox"/>	Chocolate	None	Never	None	✓	✓

© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences