

NAME: VATSAL MANVAR

ROLL NO: 19BCE120

SUBJECT CLOUD COMPUTING

PRACTICAL: 3

The screenshot shows the AWS S3 Management Console. On the left, the navigation pane includes 'Buckets', 'Storage Lens' (with 'Dashboards' and 'AWS Organizations settings'), and a 'Feature spotlight'. The main area displays the 'Account snapshot' with metrics: Total storage (91.9 KB), Object count (66), and Avg. object size (1.4 KB). It also shows a note about enabling advanced metrics. Below this is a table of existing buckets:

Name	AWS Region	Access	Creation date
ql-cf-templates-1646710228-fc0c5232d216c49a-us-west-2	US West (Oregon) us-west-2	Objects can be public	March 8, 2022, 09:00:30 (UTC+0:30)
qltrail-lab-2543-1646710230	US East (N. Virginia) us-east-1	Objects can be public	March 8, 2022, 09:00:33 (UTC+0:30)

The screenshot shows the 'Create bucket' wizard. The first step, 'General configuration', is displayed. It asks for a 'Bucket name' (vatsal12345), 'AWS Region' (US West (Oregon) us-west-2), and provides an option to 'Copy settings from existing bucket - optional' (Choose bucket). The second step, 'Object Ownership', is shown with the note: '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.' It offers two options: 'ACLs disabled (recommended)' (All objects in this bucket are owned by this account.) and 'ACLs enabled' (Objects in this bucket can be owned by other AWS accounts.).

Screenshot of the AWS S3 Bucket Creation Wizard - Step 2: Set Bucket Settings.

Tags (0) - optional
Track storage cost or other criteria by tagging your bucket. [Learn more](#)

No tags associated with this bucket.
[Add tag](#)

Default encryption
Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption
 Disable
 Enable

Advanced settings

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

[Create bucket](#)

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 preferred
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.
 Object writer
The object writer remains the object owner.

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.

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
t: 4.30 KB/s i: 2.56 KB/s ENG IN 09:07 AM 08-03-2022

S3 Management Console

Successfully created bucket "reportbucket28122001"

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

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

Feedback English (US) ▾

Successfully created bucket "reportbucket28122001"

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

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

Feedback English (US) ▾

new-report.png

Report

File

Search for services, features, blogs, docs, and more [Alt+S]

Global aw@student @ 1247-4583-6095 ▾

View Storage Lens dashboard

Buckets (3) Info

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

Name	AWS Region	Access	Creation date
ql-cf-templates-1646710228-fc0c5232d216c49a-us-west-2	US West (Oregon) us-west-2	Objects can be public	March 8, 2022, 09:00:30 (UTC+05:30)
qltrail-lab-2543-1646710230	US East (N. Virginia) us-east-1	Objects can be public	March 8, 2022, 09:00:33 (UTC+05:30)
reportbucket28122001	US West (Oregon) us-west-2	Bucket and objects not public	March 8, 2022, 09:07:24 (UTC+05:30)

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

t: 74.7 KB/s i: 32.6 KB/s ENG IN 09:07 AM 08-03-2022

Show all

Feedback English (US) ▾

new-report.png

Report

File

Search for services, features, blogs, docs, and more [Alt+S]

Global aw@student @ 1247-4583-6095 ▾

View Storage Lens dashboard

Buckets (3) Info

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

Name	AWS Region	Access	Creation date
ql-cf-templates-1646710228-fc0c5232d216c49a-us-west-2	US West (Oregon) us-west-2	Objects can be public	March 8, 2022, 09:00:30 (UTC+05:30)
qltrail-lab-2543-1646710230	US East (N. Virginia) us-east-1	Objects can be public	March 8, 2022, 09:00:33 (UTC+05:30)
reportbucket28122001	US West (Oregon) us-west-2	Bucket and objects not public	March 8, 2022, 09:07:24 (UTC+05:30)

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

t: 0.05 KB/s i: 0.41 KB/s ENG IN 09:08 AM 08-03-2022

The screenshot shows the AWS S3 console interface. On the left, a sidebar titled "Amazon S3" lists various options like Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and Access analyzer for S3. Below this is a section for "Block Public Access settings for this account". Under "Storage Lens", there are links for Dashboards and AWS Organizations settings. A "Feature spotlight" section is also present. At the bottom of the sidebar, there's a link to "AWS Marketplace for S3".

The main content area is titled "reportbucket28122001" and shows the "Objects" tab selected. It displays a message stating "Objects (0)" and "No objects". There are buttons for Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, and Upload. A search bar "Find objects by prefix" is also present. The status bar at the bottom right indicates "t: 23.1 KB/s i: 0.80 KB/s ENG IN 09:09 AM 08-03-2022".

This screenshot shows the "Upload" step in the AWS S3 Management Console. It displays a file selection dialog with "new-report.png" selected. The file details are shown as "1 Total, 84.0 KB". The "Destination" field is set to "s3://reportbucket28122001". The status bar at the bottom right indicates "t: 0.00 KB/s i: 0.00 KB/s ENG IN 09:09 AM 08-03-2022".

The screenshot shows the AWS S3 Management Console interface. At the top, there is a progress bar indicating the upload status: "Uploading" with "0%" completed. Below the progress bar, the "Summary" section displays the destination as "s3://reportbucket28122001" and the upload status as "Succeeded" with "0 files, 0 B (0%)".

Destination	Succeeded	Failed
s3://reportbucket28122001	0 files, 0 B (0%)	0 files, 0 B (0%)

Below the summary, there are tabs for "Files and folders" and "Configuration", with "Files and folders" being selected. The "Files and folders" section shows one item: "new-report.png" (1 Total, 84.0 KB). A detailed view of the file is shown below:

Name	Type	Size	Status
new-report.png	image/png	84.0 KB	Succeeded

At the bottom of the page, there is a navigation bar with links for "Feedback", "English (US)", and "Cookie preferences", along with system status indicators for network speed (t: 2.47 KB/s, l: 9.23 KB/s), language (ENG IN), and date/time (09:09 AM, 08-03-2022).

reportbucket28122001

Objects (1)

Name	Type	Last modified	Size	Storage class
new-report.png	png	March 8, 2022, 09:09:50 (UTC+05:30)	84.0 KB	Standard

new-report.png

Object overview

Owner	s3 URI
aws033862	s3://reportbucket28122001/new-report.png
AWS Region	Amazon Resource Name (ARN)
US West (Oregon) us-west-2	arn:aws:s3:::reportbucket28122001/new-report.png
Last modified	Entity tag (Etag)
March 8, 2022, 09:09:50 (UTC+05:30)	75acf5a0dd2f6bdd67c36fa2748a1a19
Size	Object URL
84.0 KB	https://reportbucket28122001.s3.us-west-2.amazonaws.com/new-report.png
Type	
png	
Key	
new-report.png	

Introduction to Amazon Simple Storage Service

reportbucket28122001 - S3 bucket

s3.console.aws.amazon.com/s3/object/reportbucket28122001?region=us-west-2&prefix=new-report.png

AWS Services Search for services, features, blogs, docs, and more [Alt+S]

Global awsstudent @ 1247-4583-6095

Properties Permissions Versions

Object overview

Owner: aws033862

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

Last modified: March 8, 2022, 09:09:50 (UTC+05:30)

Size: 84.0 KB

Type: png

Key: new-report.png

S3 URI: s3://reportbucket28122001/new-report.png

Amazon Resource Name (ARN): arn:aws:s3:::reportbucket28122001/new-report.png

Entity tag (Etag): 75acf5a0dd2f6bdd67c36fa2748a1a19

Object URL: https://reportbucket28122001.s3.us-west-2.amazonaws.com/new-report.png

Object management overview

The following bucket properties and object management configurations impact the behavior of this object.

Feedback English (US) © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

t: 0.13 KB/s ENG IN 09:12 AM 08-03-2022

Apps https://reportbucket28122001.s3.us-west-2.amazonaws.com/new-report.png

https://reportbucket28122001.s3.us-west-2.amazonaws.com/new-report.png

Search Google or type a URL

Add shortcut

On International Women's Day, we're celebrating progress on the path to gender equality.

Bits + Pieces by Laci Jordan

t: 7.84 KB/s ENG IN 09:13 AM 08-03-2022



The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with navigation links like 'Buckets', 'Storage Lens', 'Feature spotlight', and 'AWS Marketplace for S3'. The main area displays a file named 'new-report.png' with its properties. The 'Properties' tab is selected, showing details such as the owner (aws033862), AWS Region (US West (Oregon) us-west-2), Last modified (March 8, 2022, 09:09:50 (UTC+05:30)), Size (84.0 KB), Type (png), and Key (new-report.png). To the right of the file details, there's an 'Object actions' dropdown menu with 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'. At the bottom of the page, there are links for 'Feedback', 'English (US)', and various AWS services.

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with navigation links like 'Buckets', 'Storage Lens', 'AWS Marketplace for S3', etc. The main area displays the properties of an object named 'new-report.png'. The 'Properties' tab is selected, showing details such as Owner (aws033862), AWS Region (US West (Oregon) us-west-2), Last modified (March 8, 2022, 09:09:50 (UTC+05:30)), Size (84.0 KB), Type (png), and Key (new-report.png). To the right, there's a detailed view of the object's metadata, including S3 URI, ARN, Entity tag (Etag), Object URL, and a context menu with options like 'Copy S3 URI', 'Download', 'Open', 'Object actions', 'Edit actions', and 'Make public using ACL'. The status bar at the bottom indicates the browser version (Edge 96.0.1054.47), language (ENG IN), and date (08-03-2022).

Properties

Object overview

Owner: aws033862

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

Last modified: March 8, 2022, 09:09:50 (UTC+05:30)

Size: 84.0 KB

Type: png

Key: new-report.png

S3 URI: s3://reportbucket28122001/new-report.png

Amazon Resource Name (ARN): arn:aws:s3:::reportbucket28122001/new-report.png

Entity tag (Etag): 75acf5a0dd2f6bdd67c36fa2748a1a19

Object URL: https://reportbucket28122001.s3.us-west-2.amazonaws.com/new-report.png

Object actions

- Download
- Open
- Copy S3 URI
- Object actions
- 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
- Make public using ACL

Feedback English (US)

Make public

The make public action enables public read access in the object access control list (ACL) settings. Learn more [\[Link\]](#).

Specified objects

Name	Type	Last modified	Size
new-report.png	png	March 8, 2022, 09:09:50 (UTC+05:30)	84.0 KB

Cancel **Make public**

Feedback English (US)

Introduction to Amazon Simple Storage Service | reportbucket28122001 - S3 bucket | https://reportbucket28122001.s3.amazonaws.com/ | +

s3.console.aws.amazon.com/s3/buckets/reportbucket28122001/object/edit_public_read_access?region=us-west-2&showversions=false [Alt+S]

aws Services Search for services, features, blogs, docs, and more Global aw@student @ 1247-4583-6095

Failed to edit public access
For more information, see the Error column in the Failed to edit table below.

Make public: status

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 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://reportbucket28122001	0 objects	1 object, 84.0 KB

Failed to edit public access Configuration

Failed to edit public access (1 object, 84.0 KB)

Find objects by name

Feedback English (US) © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 0.00 KB/s i: 0.00 KB/s 09:15 AM ENG IN 08-03-2022

Introduction to Amazon Simple Storage Service | reportbucket28122001 - S3 bucket | https://reportbucket28122001.s3.amazonaws.com/?region=us-west-2&tab=permissions [Alt+S]

aws Services Search for services, features, blogs, docs, and more Global aw@student @ 1247-4583-6095

Amazon S3 > reportbucket28122001

reportbucket28122001 [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](#)

Edit

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

https://s3.console.aws.amazon.com/s3/#

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 33.3 KB/s i: 12.2 KB/s 09:16 AM ENG IN 08-03-2022

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.

[Cancel](#) [Save changes](#)

Feedback English (US) ▾ © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 0.05 KB/s ENG IN 09:16 AM

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.

[Cancel](#) [Save changes](#)

Feedback English (US) ▾ © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 0.06 KB/s ENG IN 08-03-2022 09:16 AM

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.

[Cancel](#) [Save changes](#)

Feedback English (US) ▾ © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 0.00 KB/s ENG IN 09:17 AM

The screenshot shows the AWS S3 console interface. At the top, there are three tabs: "Introduction to Amazon Simple" (highlighted), "reportbucket28122001 - S3 buck", and "https://reportbucket28122001.s3...". The main navigation bar includes "aws", "Services", "Search for services, features, blogs, docs, and more", and "[Alt+S]". The status bar at the bottom right shows "Global", "awsstudent @ 1247-4583-6095", and system icons.

The main content area displays the "Edit Block public access (bucket settings)" dialog. It contains a warning message: "Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public." Below this is a text input field with the placeholder "To confirm the settings, enter confirm in the field." and a "confirm" button. On the left, there are four checkboxes:

- Block all public access**: Turning this setting on is the same as turning on all four settings below it.
- Block public access to buckets and objects grants**: S3 will block public access permissions applied to newly added ACLs for existing buckets and objects. This setting doesn't affect existing ACLs.
- Block public access to buckets and objects grant**: S3 will ignore all ACLs that grant public access to buckets and objects.
- 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.

At the bottom of the dialog are "Cancel" and "Confirm" buttons. Below the dialog, there are "Save changes" and "Cancel" buttons. A green success message at the top of the page reads: "Successfully edited Block Public Access settings for this bucket."

The URL in the address bar is <https://s3.console.aws.amazon.com/s3/buckets/reportbucket28122001?region=us-west-2&tab=permissions>.

The "Permissions" tab is selected in the S3 bucket navigation bar. Other tabs include "Objects", "Properties", "Metrics", "Management", and "Access Points".

The "Permissions overview" section shows an "Access" section with a single entry: "Block public access (bucket settings)".

The "Block public access (bucket settings)" section contains a detailed description of how public access is granted and the effects of turning it off. It also includes a "Learn more" link.

The "Bucket policy" section is shown at the bottom, with a "Bucket policy" tab selected. The URL here is <https://s3.console.aws.amazon.com/s3/buckets/reportbucket28122001?region=us-west-2&tab=policy>.

Introduction to Amazon Simple Storage Service

reportbucket28122001 - S3 bucket

https://reportbucket28122001.s3.us-west-2.amazonaws.com/new-report.png

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Global awsstudent @ 1247-4583-6095

Amazon S3 > reportbucket28122001 > new-report.png

new-report.png Info

Properties Permissions Versions

Object overview

Owner	aws035862
AWS Region	US West (Oregon) us-west-2
Last modified	March 8, 2022, 09:09:50 (UTC+05:30)
Size	84.0 KB
Type	png
Key	new-report.png

S3 URI: s3://reportbucket28122001/new-report.png

Amazon Resource Name (ARN): arn:aws:s3:::reportbucket28122001/new-report.png

Entity tag (Etag): 75acf5a0dd2f6bdd67c36fa2748a1a19

Object URL: https://reportbucket28122001.s3.us-west-2.amazonaws.com/new-report.png

Object actions ▾

- 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
- Make public using ACL

Feedback English (US) © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

t: 0.05 KB/s i: 0.79 KB/s ENG IN 09:18 AM 08-03-2022

Introduction to Amazon Simple Storage Service

reportbucket28122001 - S3 bucket

https://reportbucket28122001.s3.us-west-2.amazonaws.com/object/edit_public_read_access?region=us-west-2&showversions=false

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Global awsstudent @ 1247-4583-6095

Successfully edited public access

View details below.

Make public: status

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

Summary

Source	s3://reportbucket28122001	Successfully edited public access	Failed to edit public access
		1 object, 84.0 KB	0 objects

Failed to edit public access Configuration

Failed to edit public access (0)

Name	Folder	Type	Last modified	Size	Error
No objects failed to edit					

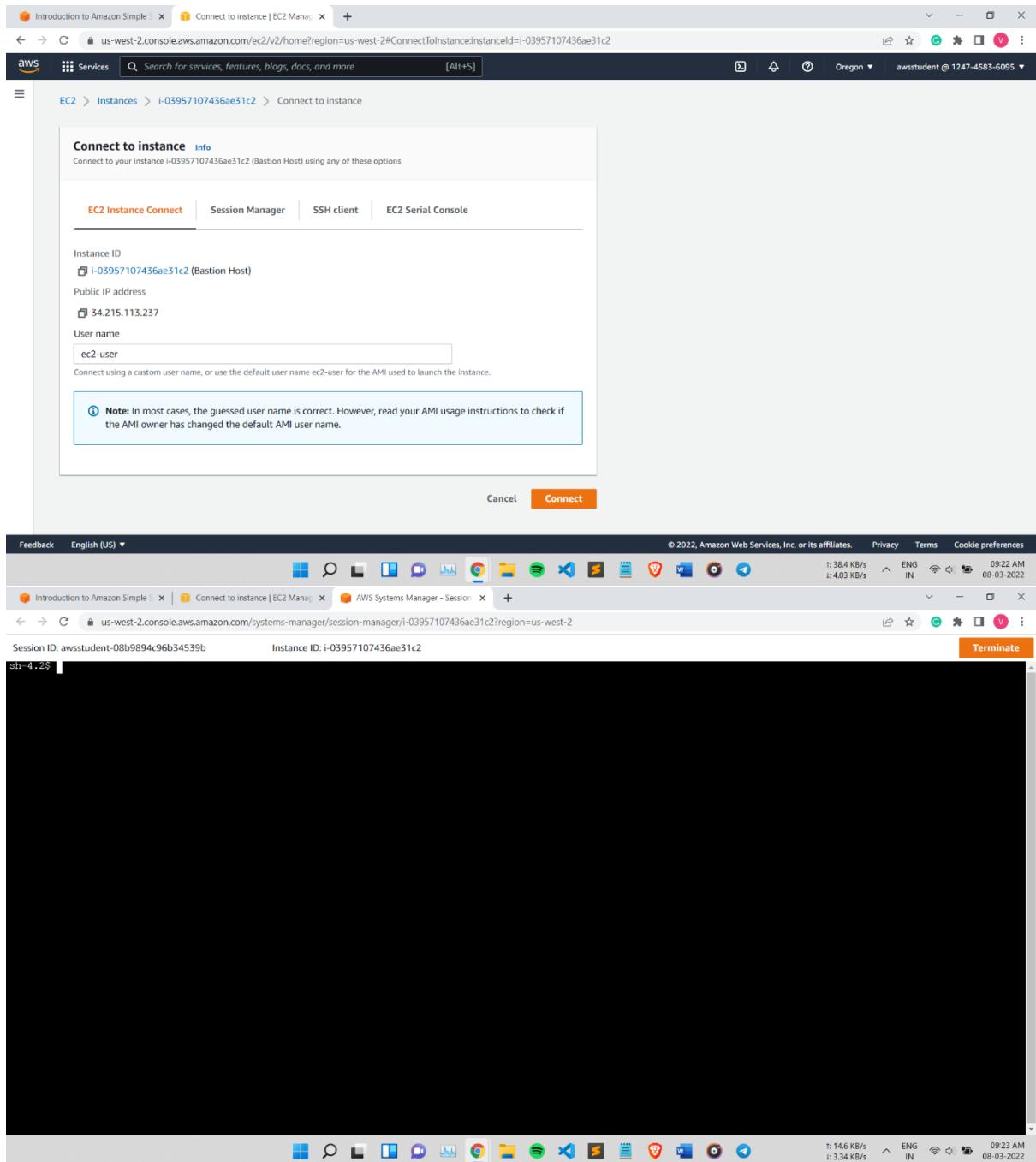
Feedback English (US) © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

t: 1.43 KB/s i: 2.38 KB/s ENG IN 09:18 AM 08-03-2022

Screenshot of a Microsoft Excel spreadsheet titled "sample-report" showing a log of AWS S3 operations. The data includes columns for Service, Operation, UsageType, Resource, StartTime, EndTime, and UsageValue.

A	B	C	D	E	F	G
Service	Operation	UsageType	Resource	StartTime	EndTime	UsageValue
1 AmazonS3	HeadBucket	USW2-C3DataTransfer-Out-Bytes	lab-test-bucket-77	10/31/2020 0:00	12/31/2020 11:59	15309
2 AmazonS3	PutObject	USW2-C3DataTransfer-In-Bytes	admin-test-77	10/31/2020 0:00	12/31/2020 11:59	19032
3 AmazonS3	HeadBucket	USW2-Requests-Tier2	admin-test-77	10/31/2020 0:00	12/31/2020 11:59	128
4 AmazonS3	PutObjectForReplication	USW1-Requester-SIA-Tier1	mybucket-98765	10/31/2020 0:00	12/31/2020 11:59	56888
5 AmazonS3	GetObjectFor Replication	USW1-USW2-AWS-In-Bytes	mybucket-98766	10/31/2020 0:00	12/31/2020 11:59	254587
6 AmazonS3	GetObjectFor Replication	USW2-C3DataTransfer-Out-Bytes	mybucket-98767	10/31/2020 0:00	12/31/2020 11:59	235
7 AmazonS3	GetObjectFor Replication	USW2-C3DataTransfer-In-Bytes	mybucket-98768	10/31/2020 0:00	12/31/2020 11:59	25589
8 AmazonS3	HeadBucket	USW2-Requests-Tier2	mybucket-98769	10/31/2020 0:00	12/31/2020 11:59	2348
9 AmazonS3	PutObject	USW1-Requester-SIA-Tier1	mybucket-98770	10/31/2020 0:00	12/31/2020 11:59	15309
10 AmazonS3	PutObjectForReplication	USW1-USW2-AWS-In-Bytes	mybucket-98771	10/31/2020 0:00	12/31/2020 11:59	19032
11 AmazonS3	GetObjectForReplication	USW2-C3DataTransfer-Out-Bytes	lab-example-bucket	10/31/2020 0:00	12/31/2020 11:59	128
12 AmazonS3	GetObjectForReplication	USW2-C3DataTransfer-In-Bytes	lab-example-bucket	10/31/2020 0:00	12/31/2020 11:59	56888
13 AmazonS3	HeadBucket	USW2-Requests-Tier2	lab-example-bucket	10/31/2020 0:00	12/31/2020 11:59	254587
14 AmazonS3	PutObject	USW1-Requester-SIA-Tier1	lab-example-bucket	10/31/2020 0:00	12/31/2020 11:59	235
15 AmazonS3	PutObjectForReplication	USW1-USW2-AWS-In-Bytes	lab-example-bucket	10/31/2020 0:00	12/31/2020 11:59	25589
16 AmazonS3	GetObjectForReplication	USW1-USW2-AWS-In-Bytes				

Screenshot of the AWS S3 console showing the file "new-report.png" details. The object overview shows the file was last modified on March 8, 2022, at 09:09:50 (UTC+05:30), has a size of 84.0 KB, and is of type png. The S3 URI is s3://reportbucket28122001/new-report.png.



The image shows two separate AWS Systems Manager sessions running on an EC2 instance. Both sessions have the same title bar: "Introduction to Amazon Simple..." and "AWS Systems Manager - Session". The session IDs are "awsstudent-0fe7274d8b06b9be3" and "i-03957107436ae31c2".

The terminal window displays the AWS CLI version 2 help text for the "aws s3" command. It includes notes about the latest major version being stable and recommended, and instructions for installing the CLI. It also lists valid subcommands: ls, cp, rm, mb, presign, and aws help.

```
sh-4.2$ aws s3 ls
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installati
on instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb
presign
sh-4.2$ aws s3 ls://reportbucket28122001
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installati
on instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb
presign
sh-4.2$ ls
dolphins.jpg  files.zip  report-test1.txt  report-test2.txt  report-test3.txt  whale.jpg
sh-4.2$ 
```

The taskbar at the bottom of each session window shows various icons for file operations, communication, and system status.

The screenshot shows a Windows desktop environment with several open windows:

- Terminal Window:** A black terminal window titled "AWS Systems Manager - Session" showing AWS CLI command output. It includes usage instructions, help commands, and a note about the AWS CLI version 2 being stable and recommended. It also shows a failed upload attempt to an S3 bucket.
- Browsers:** Two browser tabs are visible:
 - "Introduction to Amazon Simple Storage Service (S3)"
 - "amazon.qwiklabs.com/focuses/2421?catalog_rank=%7B"rank%3A1%2C"num_filters%3A0%2C"has_search%3Atrue%7D&parent=catalog&search_id=15198707"
- Taskbar:** The taskbar at the bottom shows various pinned icons and system status indicators.

Task 5: Create a bucket policy

A bucket policy is a set of permissions associated with an S3 bucket. It is used to control access to an entire bucket or to specific directories within a bucket.

In this task, you use the AWS Policy Generator to create a bucket policy to enable read and write access from the EC2 instance to the bucket to ensure your reporting application can successfully write to S3.

- Right-click this link [sample-file.txt](#), choose **Save link as**, and save the file locally.
- Return to the AWS Management Console, go to the **Services** menu and select **S3**.
- In the **S3 Management Console** tab, select the name of your bucket.
- Choose **Upload** and use the same upload process as in the previous task to upload the **sample-file.txt**.
- Choose the **sample-file.txt** file name. The sample-file.txt overview page opens.

Task Summary:

- Start Lab
- Task 1: Create a bucket
- Task 2: Upload an object to the bucket
- Task 3: Make an object public
- Task 4: Test connectivity from the EC2 instance
- Task 5: Create a bucket policy** (Currently selected)
- Task 6: Explore versioning
- Summary:
- Conclusion
- End Lab
- Additional resources

Screenshot of the AWS S3 Management Console showing the upload process for a file named "sample-file.txt".

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 folders.

Files and folders (1 Total, 113.0 B)

Name	Type	Size
sample-file.txt	text/plain	113.0 B

Destination

Destination
[s3://reportbucket28122001](#)

Destination details

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

Feedback English (US) ▾

Upload succeeded
View details below.

Upload: status

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

Summary

Destination	Succeeded	Failed
s3://reportbucket28122001	1 file, 113.0 B (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 113.0 B)

Name	Type	Size	Status	Error
sample-file.txt	text/plain	113.0 B	Succeeded	-

Screenshot of the AWS S3 Management Console showing the properties of an object named "sample-file.txt". The object was last modified on March 8, 2022, at 09:33:54 UTC+05:30. It has a size of 113.0 B and a type of txt. The key is sample-file.txt. The S3 URI is s3://reportbucket28122001/sample-file.txt. The ARN is arn:aws:s3:::reportbucket28122001/sample-file.txt. The Entity tag (Etag) is 4a0b2a536384728d06b8a9c5ceae0581. A tooltip indicates that the Object URL has been copied.

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>NEPQAFTN895CAM3</RequestId>
<HostId>j1A3UZpxPBz1SXahhSiKoTYg4oLfuqePUrYGb1G1odEE6Igg1LtvYt0gUaV0ocVtWx6Ng=</HostId>
</Error>
```

Windows taskbar at the bottom:

- t: 0.26 KB/s
- i: 0.57 KB/s
- ENG IN
- 09:34 AM
- 08-03-2022

Introduction to Amazon Simple ... | IAM Management Console | reportbucket28122001 - S3 buck... | AWS Systems Manager - Session | https://reportbucket28122001.s... | +

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Introducing the new IAM roles experience
We've redesigned the IAM roles experience to make it easier to use. Let us know what you think.

IAM > Roles

Roles (22) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

EC2InstanceProfileRole

Role name Trusted entities Last activity

EC2InstanceProfileRole AWS Service: ec2 17 minutes ago

Delete Create role

Feedback English (US) ▾

Introduction to Amazon Simple ... | IAM Management Console | reportbucket28122001 - S3 buck... | AWS Systems Manager - Session | https://reportbucket28122001.s... | +

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Introducing the new IAM roles experience
We've redesigned the IAM roles experience to make it easier to use. Let us know what you think.

IAM > Roles > EC2InstanceProfileRole

EC2InstanceProfileRole

Summary

Creation date March 08, 2022, 09:00 (UTC+05:30)

Last activity 17 minutes ago

ARN Copied

arn:aws:iam::124745836095:role/EC2InstanceProfileRole

Instance profile ARN arn:aws:iam::124745836095:instance-profile/EC2InstanceProfile

Maximum session duration 1 hour

Permissions Trust relationships Tags Access Advisor Revoke sessions

Permissions policies (2)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter

Policy name Type Description

ARN Copied

Simulate Remove Add permissions

Feedback English (US) ▾

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

t: 0.00 KB/s ENG IN 09:36 AM 08-03-2022

The screenshot shows the AWS IAM Management Console with the EC2InstanceProfileRole page open. A context menu is displayed over the ARN field, with the 'Copy' option selected. A tooltip 'ARN Copied' is visible. The ARN arn:aws:iam::124745836095:role/EC2InstanceProfileRole is copied to the clipboard.

EC2InstanceProfileRole

Summary

Creation date: March 08, 2022, 09:00 (UTC+05:30)

Last activity: 17 minutes ago

Maximum session duration: 1 hour

Permissions | Trust relationships | Tags | Access analysis

Permissions policies (2)

You can attach up to 10 managed policies.

Policy name ▾ Type Description

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

Objects (2)

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](#)

Actions ▾ Create folder Upload

Name	Type	Last modified	Size	Storage class
new-report.png	png	March 8, 2022, 09:09:50 (UTC+05:30)	84.0 KB	Standard
sample-file.txt	txt	March 8, 2022, 09:33:54 (UTC+05:30)	113.0 B	Standard

Feedback English (US) ▾ © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

t: 0.00 KB/s i: 0.00 KB/s ENG IN 09:37 AM 08-03-2022

Screenshot of the AWS S3 console showing the bucket permissions overview. The 'Permissions' tab is selected. It shows that 'Access' is set to 'Objects can be public'. A note states: '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.' A 'Learn more' link is provided.

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](#)

Edit

Block all public access

Off

Individual Block Public Access settings for this bucket

https://s3.console.aws.amazon.com/s3/#

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 26.5 KB/s ENG IN 09:37 AM

Introduction to Amazon Simple ... reportbucket28122001 - S3 buck... reportbucket28122001 - S3 buck... AWS Systems Manager - Session https://reportbucket28122001.s...

AWS Services Search for services, features, blogs, docs, and more [Alt+S] Global awsstudent @ 1247-4583-6095

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 > reportbucket28122001

reportbucket28122001 Info

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access Objects can be 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](#)

Edit

Block all public access

Off

Individual Block Public Access settings for this bucket

https://s3.console.aws.amazon.com/s3/#/property/policy/edit?region=us-west-2

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 1.46 KB/s ENG IN 08-03-2022

Introduction to Amazon Simple ... reportbucket28122001 - S3 buck... reportbucket28122001 - S3 buck... AWS Systems Manager - Session https://reportbucket28122001.s...

AWS Services Search for services, features, blogs, docs, and more [Alt+S] Global awsstudent @ 1247-4583-6095

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 > reportbucket28122001 > Edit bucket policy

Edit bucket policy Info

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](#)

Policy examples Policy generator

Bucket ARN arn:aws:s3:::reportbucket28122001

Policy

```

1  {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Principal": {},
7       "Effect": "Allow",
8       "Action": [],
9       "Resource": []
10    }
11  ]
12 }

```

Edit statement Statement1 Remove

1. Add actions

Choose a service

Available AMP API Gateway API Gateway V2 Access Analyzer

Feedback English (US) ▾

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 0.21 KB/s ENG IN 09:38 AM

Screenshot of the AWS S3 Bucket Policy configuration page:

The page shows a JSON policy document with a single statement:

```

1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Sid": "Statement1",
6        "Principal": {},
7        "Effect": "Allow",
8        "Action": [],
9        "Resource": []
10       ]
11     }
12   }

```

A context menu is open over the policy document, showing options like "Edit statement Statement1" and "Remove".

Screenshot of the AWS Policy Generator:

The "Step 1: Select Policy Type" section is shown, with "SQS Queue Policy" selected.

The "Step 2: Add Statement(s)" section shows the following configuration:

- Effect:** Allow (radio button selected)
- Principal:**
- AWS Service:** Amazon SQS (dropdown selected)
- Actions:** All Actions ("*")
- Amazon Resource Name (ARN):**

At the bottom, there is an "Add Statement" button.

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 arn:aws:iam::124745836095

AWS Service Amazon S3

Actions 2 action(s) Selected All Actions (*)

Amazon Resource Name (ARN) arn:aws:s3:::reportbucket28122001

Add Conditions (Optional)

Add Statement

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Add one or more statements above to generate a policy.

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided *as is* without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

An amazon.com company

AWS Service Amazon S3

Actions ...Select Actions... All Actions (*)

Amazon Resource Name (ARN)

Add Conditions (Optional)

Add Statement

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
arn:aws:iam::124745836095:role/EC2InstanceProfileRole	Allow	s3:GetObject s3:PutObject	arn:aws:s3:::reportbucket28122001/*	None

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Generate Policy **Start Over**

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided *as is* without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

An amazon.com company

t: 0.00 KB/s ^ ENG IN 09:44 AM 08-03-2022

Screenshot of the AWS Policy Generator tool showing a JSON policy document for an S3 bucket.

```
{
  "Id": "Policy1646712848643",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1646712832931",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::reportbucket28122001/*",
      "Principal": {
        "AWS": [
          "arn:aws:iam::124745836095:role/EC2InstanceProfileRole"
        ]
      }
    }
  ]
}
```

The policy grants the EC2 Instance Profile Role permission to read and write objects in the bucket.

Conditions: None

Step 3: Review and Save

A policy is a set of rules that define who can access your data and what they can do with it. You can use policies to control access to your data at the object level, or to grant permissions to specific users or groups.

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.
An amazon.com company

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

Bucket ARN: arn:aws:s3:::reportbucket28122001

Policy

```
1 {
  2   "Id": "Policy1646712848643",
  3   "Version": "2012-10-17",
  4   "Statement": [
  5     {
  6       "Sid": "Stmt1646712832931",
  7       "Action": [
  8         "s3:GetObject",
  9         "s3:PutObject"
  10      ],
  11      "Effect": "Allow",
  12      "Resource": "arn:aws:s3:::reportbucket28122001/*",
  13      "Principal": {
  14        "AWS": [
  15          "arn:aws:iam::124745836095:role/EC2InstanceProfileRole"
  16        ]
  17      }
  18    }
  19  ]
  20 }
```

Edit statement Stmt1646712832931 Remove

1. Add actions Choose a service Filter services

Included S3

Available AMP API Gateway API Gateway V2 Access Analyzer Account Activate Alexa for Business Amplify Amplify Admin

Feedback English (US) ▾ © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 0.00 KB/s ENG IN 09:46 AM 08-03-2022

Screenshot of the AWS S3 console showing the successful editing of a bucket policy:

The screenshot shows the AWS S3 console with the bucket "reportbucket28122001" selected. The "Permissions" tab is active, displaying the "Permissions overview" section. A success message at the top states "Successfully edited bucket policy." The "Block public access (bucket settings)" section is visible, containing instructions and a "Learn more" link.

Screenshot of the AWS Systems Manager session manager terminal window:

The terminal window shows the AWS CLI being used to upload files to an S3 bucket. It includes the command `aws s3 cp report-test1.txt s3://reportbucket28122001`, which fails with an Access Denied error. The terminal also displays a note about the AWS CLI version 2.

Session ID: aw@student-0fe7274d8b06b9be3 Instance ID: i-03957107436ae31c2

```

aws help
aws <command> help
aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb

presign
sh-4.2$ cd reports
sh-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg
sh-4.2$ aws s3 cp report-test1.txt s3://reportbucket28122001
upload failed: ./report-test1.txt to s3://reportbucket28122001/report-test1.txt An error occurred (AccessDenied) when calling the PutObject operation: access Denied
sh-4.2$ pwd
/home/ssm-user/reports
sh-4.2$ aws s3 ls s3://reportbucket28122001
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installati
on instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb

presign
sh-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg
sh-4.2$ 
```

t: 6.28 KB/s
i: 0.20 KB/s ENG IN 09:48 AM
08-03-2022

Session ID: aw@student-0fe7274d8b06b9be3 Instance ID: i-03957107436ae31c2

```

aws <command> help
aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb

presign
sh-4.2$ cd reports
sh-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg
sh-4.2$ aws s3 cp report-test1.txt s3://reportbucket28122001
upload failed: ./report-test1.txt to s3://reportbucket28122001/report-test1.txt An error occurred (AccessDenied) when calling the PutObject operation: Access Denied
sh-4.2$ pwd
/home/ssm-user/reports
sh-4.2$ aws s3 ls s3://reportbucket28122001
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installati
on instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb

presign
sh-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg
sh-4.2$ aws s3 cp report-test1.txt s3://reportbucket28122001
upload: ./report-test1.txt to s3://reportbucket28122001/report-test1.txt
sh-4.2$ 
```

t: 1.22 KB/s
i: 0.56 KB/s ENG IN 09:49 AM
08-03-2022

Session ID: aw@student-0fe7274d8b06b9be3 Instance ID: i-03957107436ae31c2

```
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb
presign
sh-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg
sh-4.2$ aws s3 cp report-test1.txt s3://reportbucket28122001
upload: ./report-test1.txt to s3://reportbucket28122001/report-test1.txt
sh-4.2$ aws s3 ls s3://reportbucket28122001
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb
presign
sh-4.2$
```

Session ID: aw@student-0fe7274d8b06b9be3 Instance ID: i-03957107436ae31c2

```
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb
presign
sh-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg
sh-4.2$ aws s3 cp report-test1.txt s3://reportbucket28122001
upload: ./report-test1.txt to s3://reportbucket28122001/report-test1.txt
sh-4.2$ aws s3 ls s3://reportbucket28122001
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb
presign
sh-4.2$ aws s3 cp s3://reportbucket28122001/sample-file.txt sample-file.txt
download: s3://reportbucket28122001/sample-file.txt to ./sample-file.txt
sh-4.2$
```

```
Session ID: aw@student-0fe7274d8b06b9be3           Instance ID: i-03957107436ae31c2
sh-4.2$ aws s3 ls://reportbucket28122001
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installati
on instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

    aws help
    aws <command> help
    aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb
presign
sh-4.2$ cd reports
sh-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg
sh-4.2$ aws s3 cp report-test1.txt s3://reportbucket28122001
upload failed: ./report-test1.txt to s3://reportbucket28122001/report-test1.txt An error occurred (AccessDenied) when calling the PutObject operation: Access Denied
sh-4.2$ pwd
/home/ssm-user/reports
sh-4.2$ aws s3 ls s3://reportbucket28122001
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installati
on instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

    aws help
    aws <command> help
    aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv

t: 7.58 KB/s  i: 0.95 KB/s  ENG IN  09:50 AM 08-03-2022

Session ID: aw@student-0fe7274d8b06b9be3           Instance ID: i-03957107436ae31c2
sh-4.2$ To see help text, you can run:
aws help
aws <command> help
aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb
presign
sh-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg
sh-4.2$ aws s3 cp report-test1.txt s3://reportbucket28122001
upload: ./report-test1.txt to s3://reportbucket28122001/report-test1.txt
sh-4.2$ aws s3 ls s3://reportbucket28122001
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installati
on instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

    aws help
    aws <command> help
    aws <command> <subcommand> help
aws: error: argument subcommand: Invalid choice, valid choices are:

ls          | website
cp          | mv
rm          | sync
mb          | rb
presign
sh-4.2$ aws s3 cp s3://reportbucket28122001/sample-file.txt sample-file.txt
download: s3://reportbucket28122001/sample-file.txt to ./sample-file.txt
sh-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt sample-file.txt whale.jpg
sh-4.2$ t: 0.13 KB/s  i: 0.05 KB/s  ENG IN  09:51 AM 08-03-2022
```

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>NEMQAF3RWB95CAN3</RequestId>
<HostId>jIA3UZpxPBzis5XAhhsikoTVgg4o0LtuqedPUrYgb1G1odEf6Iggh1lvty0t0gUaV0ocVtWx6lg=</HostId>
</Error>
```

Successfully edited bucket policy.

Amazon S3 > reportbucket28122001

reportbucket28122001 [Info](#)

Permissions tab selected.

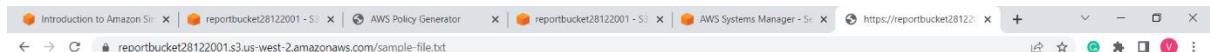
Permissions overview

Access

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](#)

Feedback English (US) ▾ © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



This sample text file is used to illustrate the use of versioning in an Amazon S3 bucket.
Make it a great day!

A screenshot of the AWS S3 console. The left sidebar shows navigation options like Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and Access analyzer for S3. Under Storage Lens, there are links for Dashboards and AWS Organizations settings. A Feature spotlight section is also present. The main content area shows the permissions tab for the bucket 'reportbucket28122001'. It displays a 'Permissions overview' section with a 'Public' access status. Below this is a 'Block public access (bucket settings)' section with a note about enabling 'Block all public access' via an 'Edit' button. The bottom of the screen shows standard browser navigation and status bars.

The screenshot shows the AWS S3 console for the bucket `reportbucket28122001`. The left sidebar includes links for Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and Access analyzer for S3. Under Storage Lens, there are links for Dashboards and AWS Organizations settings. A Feature spotlight section is present, along with a link to the AWS Marketplace for S3.

Bucket overview

AWS Region	Amazon Resource Name (ARN)	Creation date
US West (Oregon) us-west-2	arnaws:s3:::reportbucket28122001	March 8, 2022, 09:07:24 (UTC+05:30)

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](#)

Tags

Track storage cost or other criteria by tagging your bucket. [Learn more](#)

Edit Bucket Versioning

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

Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.

Enable

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

Save changes

Introduction to Amazon Simple Storage Service (S3)

Start Lab 01:30:00

87. Under the **Bucket Versioning** section, choose **Edit**

88. Select **Enable** and then choose **Save changes**

Versioning is enabled for an entire bucket and all objects within the bucket. It cannot be enabled for individual objects.

There are also cost considerations when enabling versioning. Refer to the Additional Resources section at the end of the lab for links to more information.

89. Right-click this link and save the text file to your computer **using the same name as the text file in the previous task**: [sample-file.txt](#).

While this file has the same name as the previous file, it contains new text.

90. In the S3 Management Console, on the reportbucket, choose the **Objects** tab.

Under the **Objects** section look for **Show versions**.

91. Choose **Upload** and use the same upload process in the previous task to upload the new sample-file.txt file.

92. Go to the browser tab that has the contents of the sample-file.txt file.

sample-file.txt

S3 Management Console

AWS Services

Search for services, features, blogs, docs, and more [Alt+S]

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

Files and folders (1 Total, 171.0 B)
All files and folders in this table will be uploaded.

Name	Folder	Type	Size
sample-file.txt	-	text/plain	171.0 B

Destination

Destination
<s3://reportbucket28122001>

▶ 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

Feedback English (US) ▾ © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 0.00 KB/s ENG IN 10:06 AM 08-03-2022

Start Lab

Task 1: Create a bucket

Task 2: Upload an object to the bucket

Task 3: Make an object public

Task 4: Test connectivity from the EC2 instance

Task 5: Create a bucket policy

Task 6: Explore versioning

Summary

Conclusion

End Lab

Additional resources

Introduction to Amazon S3 | S3 Management Console | AWS Policy Generator | reportbucket28122001 - S3 | AWS Systems Manager - S | https://reportbucket28122001.s3.us-west-2.amazonaws.com/sample-file.txt | + | - | X

aws Services Search for services, features, blogs, docs, and more [Alt+S] Global aw@student @ 1247-4583-6095

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	Succeeded	Failed
s3://reportbucket28122001	1 file, 171.0 B (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 171.0 B) Find by name < 1 >

Name	Folder	Type	Size	Status	Error
sample-file.txt	-	text/plain	171.0 B	Succeeded	-

This sample text file is used to illustrate the use of versioning in an Amazon S3 bucket.
This file has been modified.
This is version 2 of the file.
Have a lovely day!

Feedback English (US) © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 10.0 KB/s i: 3.67 KB/s ENG IN 10:07 AM 08-03-2022

Introduction to Amazon S3 | S3 Management Console | AWS Policy Generator | reportbucket28122001 - S3 | AWS Systems Manager - S | https://reportbucket28122001.s3.us-west-2.amazonaws.com/sample-file.txt | + | - | X

t: 0.21 KB/s i: 2.04 KB/s ENG IN 10:07 AM 08-03-2022

The screenshot shows the AWS S3 console interface. The left sidebar is collapsed, and the main area displays the 'sample-file.txt' object within the 'reportbucket28122001' bucket. The 'Versions' tab is selected, showing two versions of the file:

Version ID	Type	Last modified	Size	Storage class
rl2jud5fUEF99ECcEAQ7Ft0z0v9iWFWB (Current version)	txt	March 8, 2022, 10:07:04 (UTC+05:30)	171.0 B	Standard
null	txt	March 8, 2022, 09:33:54 (UTC+05:30)	113.0 B	Standard

Below this, the 'Objects' tab is selected, showing four objects in the bucket:

Name	Type	Version ID	Last modified	Size	Storage class
new-report.png	png	null	March 8, 2022, 09:09:50 (UTC+05:30)	84.0 KB	Standard
report-test1.txt	txt	null	March 8, 2022, 09:49:17 (UTC+05:30)	31.0 B	Standard
sample-file.txt	txt	rl2jud5fUEF99ECcEAQ7Ft0z0v9iWFWB	March 8, 2022, 10:07:04 (UTC+05:30)	171.0 B	Standard
sample-file.txt	txt	null	March 8, 2022, 09:33:54 (UTC+05:30)	113.0 B	Standard

The screenshot shows the AWS S3 console interface. On the left, the navigation pane is visible with sections like Buckets, Storage Lens, Dashboards, and AWS Marketplace for S3. The main content area displays the 'reportbucket28122001' bucket. It shows a table of objects with columns: Name, Type, Last modified, Size, and Storage class. The objects listed are:

Name	Type	Last modified	Size	Storage class
new-report.png	png	March 8, 2022, 09:09:50 (UTC+05:30)	84.0 KB	Standard
report-test1.txt	txt	March 8, 2022, 09:49:17 (UTC+05:30)	31.0 B	Standard
sample-file.txt	txt	March 8, 2022, 10:07:04 (UTC+05:30)	171.0 B	Standard

The screenshot shows the 'Delete objects' confirmation dialog. It includes a message about adding delete markers, a list of specified objects, and a delete confirmation step. The 'sample-file.txt' object is selected for deletion.

Specified objects

Name	Type	Last modified	Size
sample-file.txt	txt	March 8, 2022, 10:07:04 (UTC+05:30)	171.0 B

Delete objects?

To confirm deletion, type **delete** in the text input field.

Cancel **Delete objects**

Screenshot of the AWS S3 console showing the 'Delete objects' confirmation dialog.

The dialog displays a list of specified objects:

Name	Type	Last modified	Size
sample-file.txt	txt	March 8, 2022, 10:07:04 (UTC+05:30)	171.0 B

A text input field contains the word "delete".

Buttons: Cancel, Delete objects.

Screenshot of the AWS S3 console showing the 'Successfully deleted objects' confirmation message.

Summary table:

Source	Successfully deleted	Failed to delete
s3://reportbucket28122001	1 object, 171.0 B	0 objects

Failed to delete (0) table:

Name	Folder	Type	Last modified	Size	Error
No objects failed to delete.					

The screenshot shows the AWS S3 console interface. The top navigation bar includes tabs for Introduction, S3 Management, reportbucket, https://report, https://report, AWS Policy, reportbucket, AWS Systems, and https://report. The main title is "reportbucket28122001". Below the title, it says "Publicly accessible". The "Objects" tab is selected. A table lists five objects:

Name	Type	Version ID	Last modified	Size	Storage class
new-report.png	png	null	March 8, 2022, 09:09:50 (UTC+05:30)	84.0 KB	Standard
report-test1.txt	txt	null	March 8, 2022, 09:49:17 (UTC+05:30)	31.0 B	Standard
sample-file.txt	Delete marker	bXF29VC8qpto.T0Y12BZ1dSypk5mH7QX	March 8, 2022, 10:12:28 (UTC+05:30)	0 B	-
sample-file.txt	txt	rI2jud5fUEF99ECcEAQ7Ft0z0v9iWFWB	March 8, 2022, 10:07:04 (UTC+05:30)	171.0 B	Standard
sample-file.txt	txt	null	March 8, 2022, 09:33:54 (UTC+05:30)	113.0 B	Standard

The screenshot shows the "Delete objects" dialog. At the top, a warning message reads: "⚠ Deleting the specified objects can't be undone. [Learn more](#)". Below this is a table titled "Specified objects" showing one object:

Name	Version ID	Type	Last modified	Size
sample-file.txt	bXF29VC8qpto.T0Y12BZ1dSypk5mH7QX	Delete marker	March 8, 2022, 10:12:28 (UTC+05:30)	0 B

Below the table, a section titled "Permanently delete objects?" contains the instruction "To confirm deletion, type *permanently delete* in the text input field." A text input field contains the text "permanently deleted". At the bottom right are "Cancel" and "Delete objects" buttons.

Screenshot of the AWS S3 Management Console showing the successful deletion of objects from a bucket.

The browser address bar shows: `s3.console.aws.amazon.com/s3/buckets/reportbucket28122001/object/delete?region=us-west-2&showversions=true`

The main interface displays a green banner: "Successfully deleted objects. View details below."

Delete objects: status

The status summary table:

Source	Successfully deleted	Failed to delete
<code>s3://reportbucket28122001</code>	1 object	0 objects

Below the summary, there are two tabs: "Failed to delete" (selected) and "Configuration".

Failed to delete (0)

No objects failed to delete.

Feedback bar: English (US) ▾ © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 0.00 KB/s i: 0.00 KB/s ENG IN 10:13 AM 08-03-2022

Second screenshot: The user has navigated to the "Delete objects" page for the "reportbucket28122001" bucket.

The browser address bar shows: `s3.console.aws.amazon.com/s3/buckets/reportbucket28122001/object/delete?region=us-west-2&showversions=false`

Delete objects

Information box: Deleting the specified objects adds delete markers to them. If you need to undo the delete action, you can delete the delete markers. Learn more ⓘ

Specified objects

Name	Type	Last modified	Size
sample-file.txt	txt	March 8, 2022, 10:07:04 (UTC+05:30)	171.0 B

Delete objects?

To confirm deletion, type `delete` in the text input field.

Buttons: Cancel, Delete objects

Feedback bar: English (US) ▾ © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences t: 0.11 KB/s i: 0.05 KB/s ENG IN 10:15 AM 08-03-2022

Screenshot of the AWS S3 console showing the successful deletion of objects from a bucket.

The browser tab bar shows multiple tabs related to AWS services, including S3 Management, AWS Policy Generator, and AWS Systems Manager.

The main content area displays a summary of deleted objects:

Source	Successfully deleted	Failed to delete
s3://reportbucket28122001	1 object, 171.0 B	0 objects

Below the summary, there are two tabs: "Failed to delete" (selected) and "Configuration".

The "Failed to delete" section shows a table with the following columns: Name, Type, Last modified, Size, and Error. A search bar at the top of the table allows filtering by object name.

Name	Type	Last modified	Size	Error
No objects failed to delete.				

At the bottom of the page, there is a snippet of XML error code:

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>V8GJAY0M2FT62W0C</RequestId>
<HostId>JoSTCGx7/OT4lw+1BMP0F5GoRILQvtDcmfuDjp1c3IAHPS2UmwOvmeIuH8+euT4OBPgEBfwyQI=</HostId>
</Error>
```

The taskbar at the bottom of the screen shows various pinned application icons, including File Explorer, Task View, Edge, Spotify, and others.

AWS CloudWatch Metrics dashboard showing metrics for AWS Lambda functions. The top navigation bar includes links for Introduction, S3 Management, reportbucket, https://report, https://report, AWS Policy, AWS Systems, https://report, and Global. The main content area displays a chart for the 'Lambda Functions' metric, which shows a significant increase in吞吐量 (Throughput) over time. The chart includes a legend for吞吐量 (Throughput), 错误率 (Error Rate), and 呼叫数 (Invocation). The right sidebar provides details for the selected metric, including the metric name, unit, and dimensions.

The screenshot shows a CloudWatch Metrics dashboard. At the top, there are tabs for 'Metrics' and 'CloudWatch Metrics'. Below that, a search bar and a filter section for 'Region' and 'Metric Name'. The main area features a line chart titled 'Lambda Functions' with three data series: 'Throughput' (blue), 'Invocation' (green), and 'Error Rate' (orange). The 'Throughput' series shows a massive spike from approximately 100,000 to over 1,000,000 units of throughput between March 8 and March 9. The 'Invocation' series also shows a significant increase, while the 'Error Rate' remains relatively low. The right side of the screen displays detailed metrics for the selected 'Throughput' series, including a table with data points for each hour from 08:00 to 18:00 on March 9, and a histogram showing the distribution of throughput values.