

CBE 321 Cloud Computing & Security

SHRAVASTI OHOL 2022BCY0012

AWS - Simple Storage Service (S3)

1. Navigate to S3 service. Click on Create Bucket.

The screenshot shows the Amazon S3 homepage. On the left, there's a section titled "Amazon S3" with the sub-headline "Store and retrieve any amount of data from anywhere". Below this is a brief description of S3 as an object storage service. On the right, there's a "Create a bucket" button and a "Pricing" section. The "Pricing" section states that there are no minimum fees and provides a link to an AWS Simple Monthly Calculator. There's also a "View pricing details" link. At the bottom, there's a "How it works" section featuring a video thumbnail for an "Introduction to Amazon S3" video on YouTube.

2. Configure settings accordingly

The screenshot shows the "Create bucket" configuration page in the AWS Management Console. The top navigation bar shows "Amazon S3 > Buckets > Create bucket". The main form has several sections:

- General configuration:** Includes "AWS Region" (Asia Pacific (Mumbai) ap-south-1), "Bucket type" (set to "general purpose"), and a "Bucket name" field containing "shravasti's bucket".
- Copy settings from existing bucket - optional:** A "Choose bucket" button is present.
- Object Ownership:** Shows "Object Ownership info" with "ACLs disabled (recommended)" selected. It notes that all objects in the bucket are owned by the account.
- Block Public Access settings for this bucket:** A note states that public access is disabled.

At the bottom, there are links for "CloudShell", "Feedback", and copyright information.

Block Public Access settings for this bucket

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

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

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

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)

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

Not yet associated with this bucket

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

3. After the bucket is successfully created, create an object inside the bucket i.e. a folder

shrawastibucket [Info](#)

Objects (0) [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
No objects				
You don't have any objects in this bucket.				
Upload				

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

4. After creating a folder, upload a file in it.

The screenshot shows the AWS S3 console interface. The URL in the address bar is `Amazon S3 > Buckets > shravastibucket > bucketfolder1/`. The page title is "bucketfolder1/". Below the title, there are tabs for "Objects" and "Properties", with "Objects" being the active tab. A sub-header "Objects (0)" is displayed. A note states: "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](#)". Below this is a search bar labeled "Find objects by prefix" and a sorting dropdown. A message "No objects" is shown, followed by "You don't have any objects in this folder." At the bottom is a large orange "Upload" button.

The screenshot shows the AWS S3 console interface during the upload process. The URL in the address bar is `Amazon S3 > Buckets > shravastibucket > bucketfolder1/ > Upload`. The page title is "Upload". A note says: "Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)". Below is a dashed box for dragging files and a "Choose files" button. A table titled "Files and folders (1 total, 8.3 MB)" lists one file: "0Y4A4750.JPG" (image/jpeg, 8.3 MB). Buttons for "Remove", "Add files", and "Add folder" are available. The "Destination" section shows the destination as "`s3://shravastibucket/bucketfolder1/`". The "Destination details" section notes: "Bucket settings that impact new objects stored in the specified destination." Below are sections for "Permissions" and "Properties". At the bottom right are "Cancel" and "Upload" buttons.

5. Once the upload is successful, you will get a notification.

The screenshot shows the AWS S3 console with the following details:

- Upload succeeded**: A green notification bar at the top left indicates a successful upload.
- Upload: status**: A sub-section showing upload progress. It lists "Succeeded" (1 file, 8.3 MB (100.00%)) and "Failed" (0 files, 0 B (0%)).
- Files and folders**: A table showing one file: "OY4A4750.JPG" (image/jpeg, 8.3 MB, Status: Succeeded).

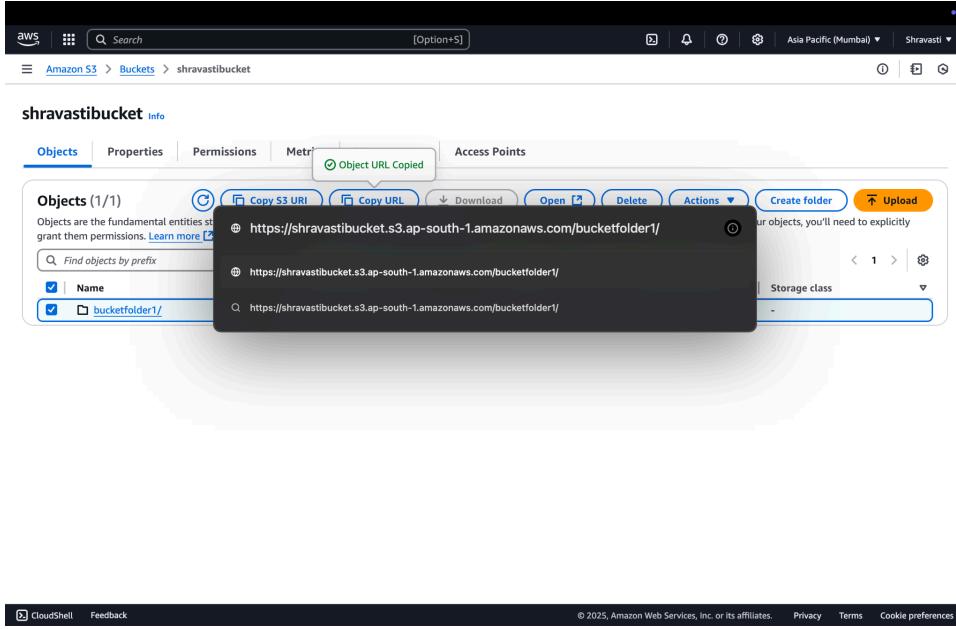
6. Select the bucket created and copy its URL

The screenshot shows the AWS S3 console with the following details:

- shrawastibucket**: The selected bucket name.
- Objects (1/1)**: A table showing one object: "bucketfolder1/" (Folder).
- Action buttons**: Includes "Copy S3 URI", "Copy URL", "Download", "Open", "Delete", "Actions", "Create folder", and "Upload".
- Object URL Copied**: A green message indicating the URL has been copied.

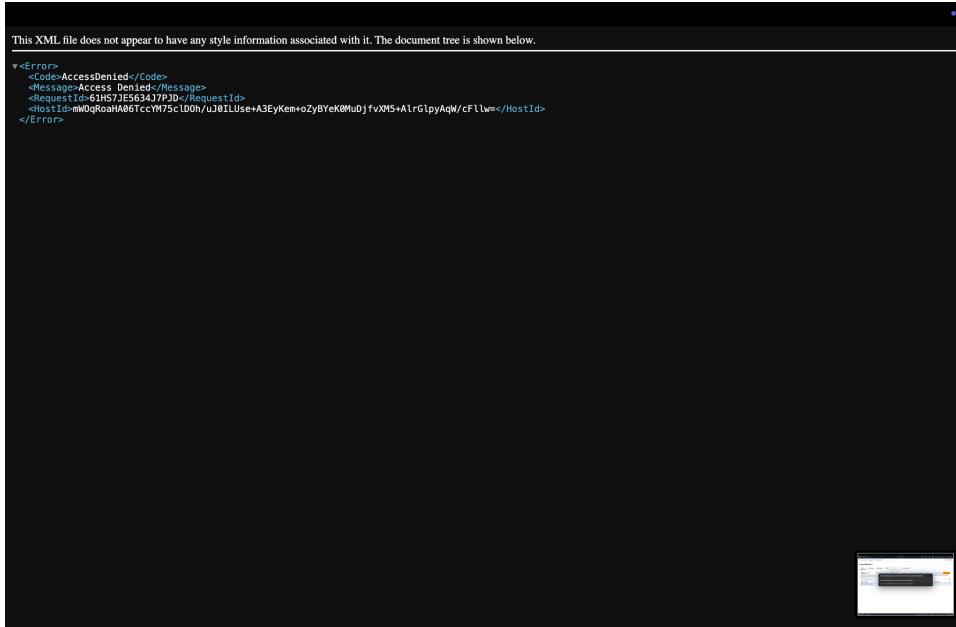


7. Paste it in a new tab



The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and various icons. Below that, the path 'Amazon S3 > Buckets > shravastibucket' is shown. The main area is titled 'shravastibucket' with a 'Info' tab. There are tabs for 'Objects', 'Properties', 'Permissions', and 'Metrics'. The 'Objects' tab is selected, showing one object: 'Objects (1/1)'. The object name is 'bucketfolder1/'. Below the object name, there's a note: 'Objects are the fundamental entities stored in your buckets. You can grant them permissions.' followed by a 'Learn more' link. There are filters for 'Name' and 'bucketfolder1/'. On the right side of the objects list, there are buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A 'Storage class' dropdown is also present. At the bottom of the objects list, there's a note: 'To make your objects publicly accessible, you'll need to explicitly grant them permissions.' A 'CloudShell' button is at the bottom left, and a footer at the bottom right contains links for 'CloudShell', 'Feedback', '© 2025, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

8. Access to the resource will be denied. This is because public access to the bucket and its contents was restricted while creating the bucket.



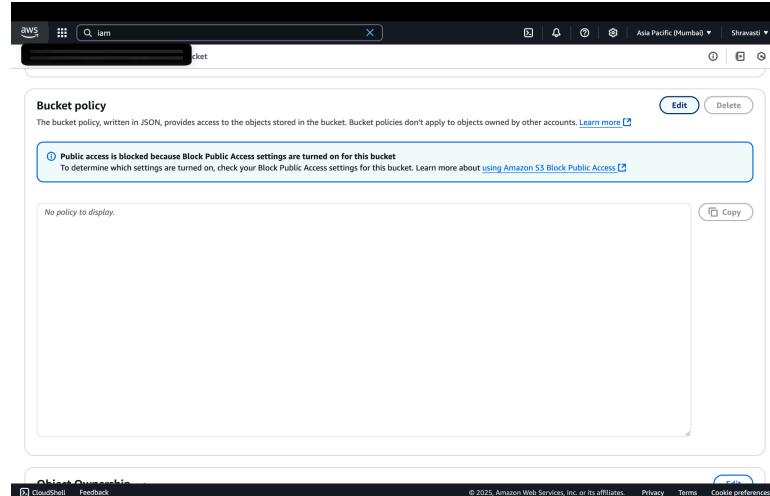
The screenshot shows a browser window displaying an XML error response. The error message is as follows:

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>61H57JE5634J7PJD</RequestId>
<HostId>mWUqRoAH0bIccMf5cUDn/UJb0lUse+A5EyKem+oZyBYeK0MuDffvXW5+AlrGipyAqW/cFlw=</HostId>
</Error>
```

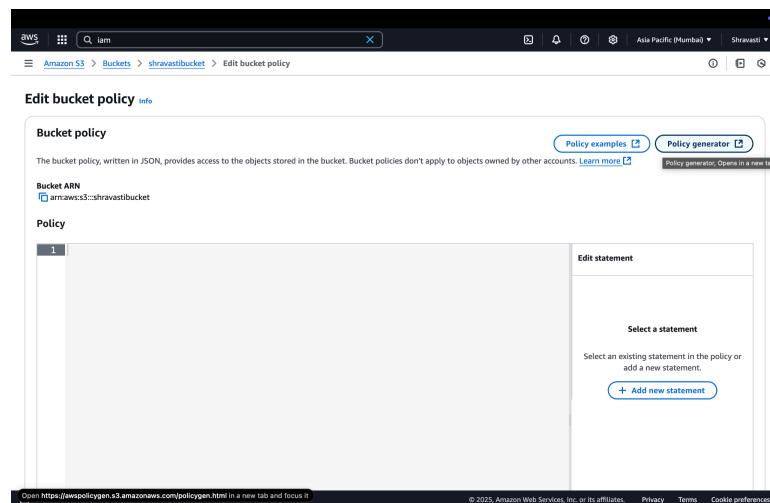
9. Two ways to do this

a. Changing bucket policies

i. Under the bucket, go to the Permissions tab



ii. Click on Policy generator



iii. Select policy type as 'S3 Bucket Policy'



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources.

For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

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

Select Type of Policy

S3 Bucket Policy

IAM Policy

VPC Endpoint Policy

SNS Topic Policy

Step 2: Add Statement(s)

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

Effect Allow Deny

Principal

Use a comma to separate multiple values.

AWS Service Amazon S3

All Services (*)

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

Actions All Actions (*)

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:s3::\$(Region)::\$(Account)::\$(QueueName).

Use a comma to separate multiple values.

Add Conditions (Optional)

Step 3: Generate Policy

iv. Paste the ARN for the bucket



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources.

For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

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

Select Type of Policy

S3 Bucket Policy

Step 2: Add Statement(s)

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

Effect Allow Deny

Principal

Use a comma to separate multiple values.

AWS Service Amazon S3

All Services (*)

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

Actions All Actions (*)

Amazon Resource Name (ARN) arn:s3::shrawanbucket

ARN should follow the following format: arn:aws:s3::\$(Region)::\$(Account)::\$(BucketName)::\$(Keyname).

Use a comma to separate multiple values.

Add Conditions (Optional)

Step 3: Generate Policy

v. Click on generate policy

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

Effect Allow Deny

Principal

Use a comma to separate multiple values.

AWS Service Amazon S3

All Services (*)

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

Actions All Actions (*)

Amazon Resource Name (ARN) arn:s3::shrawanbucket

ARN should follow the following format: arn:aws:s3::\$(Region)::\$(Account)::\$(BucketName)::\$(Keyname).

Use a comma to separate multiple values.

Add Conditions (Optional)

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

Principal(s)	Effect	Action	Resource	Conditions
*	Allow	s3:*	arn:aws:s3:::shrawanbucket	None

Step 3: Generate Policy

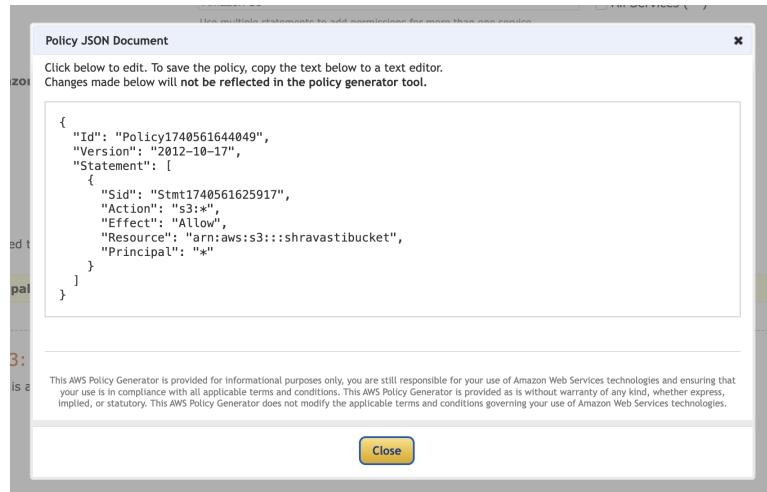
A policy is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

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 of your use of Amazon Web Services technologies.

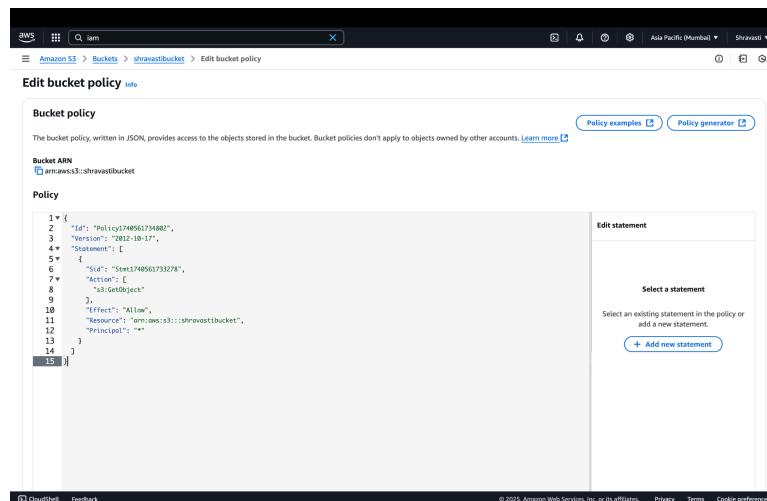
©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

An [amazon.com](#) company

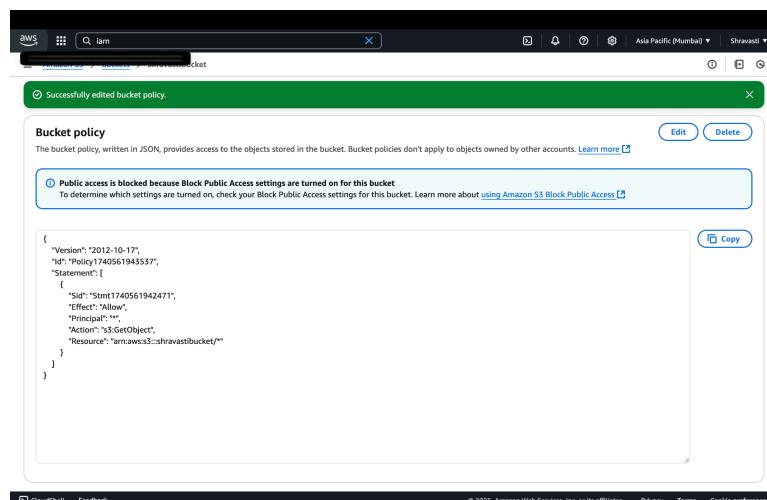
vi. Copy the generated policy



vii. Paste the policy in the bucket policy section



viii. Create the policy



ix. The resource will be publicly accessible through the URL

b. Using Object Ownership

i. Under Object ownership, click on edit

The screenshot shows the 'Object Ownership' section of the AWS IAM console. It displays the following information:

- 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.
- Object Ownership:** Bucket owner enforced
- Access control list (ACL):** This bucket has the bucket owner enforced setting applied for Object Ownership. When bucket owner enforced is applied, use bucket policies to control access.
- Grantee** table:
 - Bucket owner (your AWS account):** Canonical ID: ea9c3ae9b5cf904cc564b350439c1db0b87x206f716f2cd32352871091153ad; Objects: List, Write; Bucket ACL: Read, Write
 - Everyone (public access):** Group: http://acs.amazonaws.com/groups/global/AllUsers; Objects: -; Bucket ACL: -
 - Authenticated users group (anyone with an AWS account):** Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers; Objects: -; Bucket ACL: -

ii. Select ACL enabled → bucket owner preferred

The screenshot shows the 'Edit Object Ownership' configuration page. The 'ACLs enabled' option is selected, and the 'Bucket owner preferred' radio button is selected under 'Object Ownership'. Other options like 'Object writer' and 'Bucket owner enforced' are also shown.

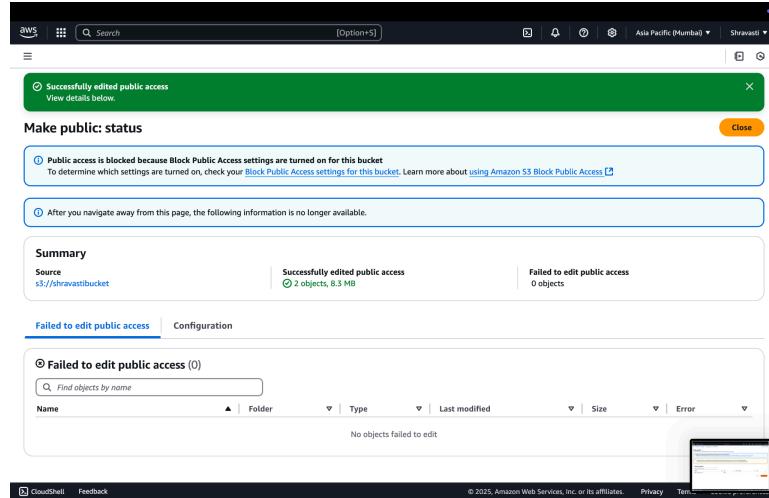
iii. Go to the bucket and select it. Under Actions, select 'make public using ACL'

The screenshot shows the AWS S3 console interface. At the top, there's a search bar and navigation links for 'Amazon S3 > Buckets > shravastibucket'. Below the navigation, the bucket name 'shravastibucket' is displayed with an 'Info' link. The main area shows a table of objects with one item listed: 'bucketfolder1/' (Type: Folder). To the right of the table, a context menu is open under the 'Actions' button. The menu includes options like 'Copy', 'Move', 'Initiate restore', 'Edit actions', and 'Make public using ACL'. The 'Make public using ACL' option is highlighted with a blue border.

iv. Click on make public

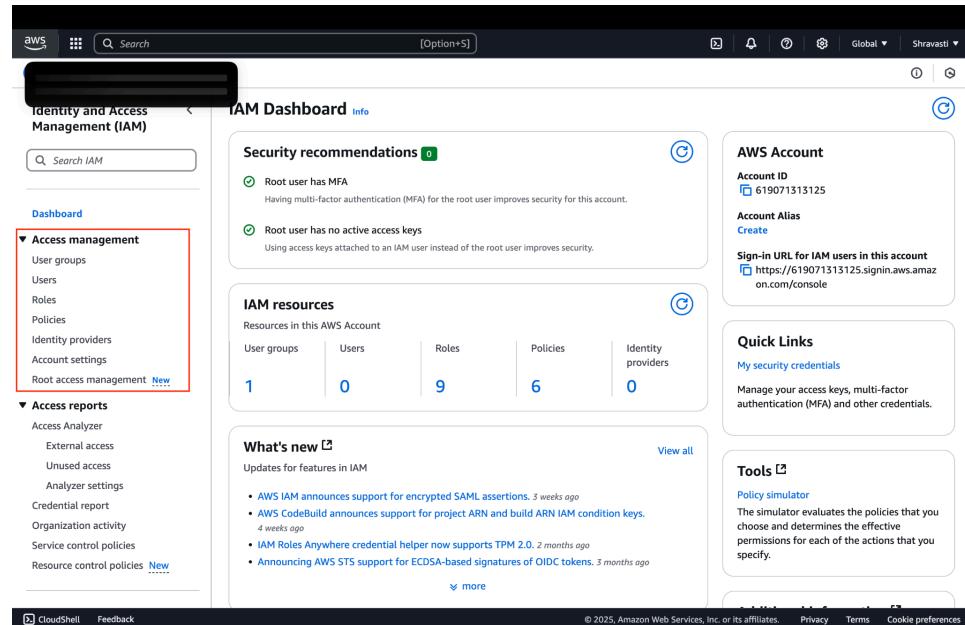
This screenshot shows the 'Make public' dialog box. At the top, it says 'The make public action enables public read access in the object access control list (ACL) settings.' Below that, a yellow warning box states 'Public access is blocked because Block Public Access settings are turned on for this bucket.' It also notes that 'To determine which settings are turned on, check your Block Public Access settings for this bucket.' A note below the warning says 'When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.' Another note says 'This action applies to all objects within the specified folders. Objects added to these folders while the action is in progress might be affected.' At the bottom, there's a table titled 'Specified objects' with one entry: 'bucketfolder1/'. There are 'Cancel' and 'Make public' buttons at the bottom right.

v. Public access will be successfully enabled and objects will be visible publicly.



10. Creating an IAM user and giving that user access to the bucket and its contents

a. Navigate to the IAM service



b. Click on create user

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, a navigation pane lists various IAM management options like User groups, Users, Roles, Policies, and Access reports. The main content area is titled "Users (0) info" and contains a brief description of what an IAM user is. A search bar and a "Create user" button are at the top right. Below the header, there's a table with columns for User name, Path, Group, Last activity, MFA, Password age, and Cons. A message "No resources to display" is centered in the table area.

c. Configure the settings to provide access to the console

This screenshot shows the "Specify user details" step of the IAM user creation wizard. It's Step 1 of 4. The user name is set to "bucketuser1". There's an option to "Provide user access to the AWS Management Console - optional", which is checked. The "User type" section shows "I want to create an IAM user" selected. The "Console password" section has "Autogenerated password" selected. At the bottom, there are two notes about password complexity: "Must be at least 8 characters long" and "Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _".

aws [Option+S] Search Global Shravasti

Identity > Users > Create user

Are you providing console access to a person?

Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

Autogenerated password
You can view the password after you create the user.

Custom password
Enter a custom password for the user.

* Must be at least 8 characters long
* Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } ^

Show password

Users must create a new password at next sign-in - Recommended
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel Next

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

aws [Option+S] Search Global Shravasti

Step 1 Specify user details Step 2 Set permissions Step 3 Review and create Step 4 Retrieve password

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Get started with groups

Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

Create group

Set permissions boundary - optional

Cancel Previous Next

aws [Option+S] Global ▾ Shravasti ▾

IAM > Users > Create user

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password

Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name bucketuser1	Console password type Autogenerated	Require password reset Yes
--------------------------	--	-------------------------------

Permissions summary

Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous **Create user**

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

aws [Option+S] Global ▾ Shravasti ▾

IAM > Users > Create user

User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password

Retrieve password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL https://619071313125.signin.aws.amazon.com/console	Email sign-in instructions
User name bucketuser1	
Console password *****	

Cancel Download .csv file Return to users list

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

d. Download the .csv file. Navigate to Console Sign-in

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password

Retrieve password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL
https://619071313125.signin.aws.amazon.com/console

User name
bucketuser1

Console password
***** Show

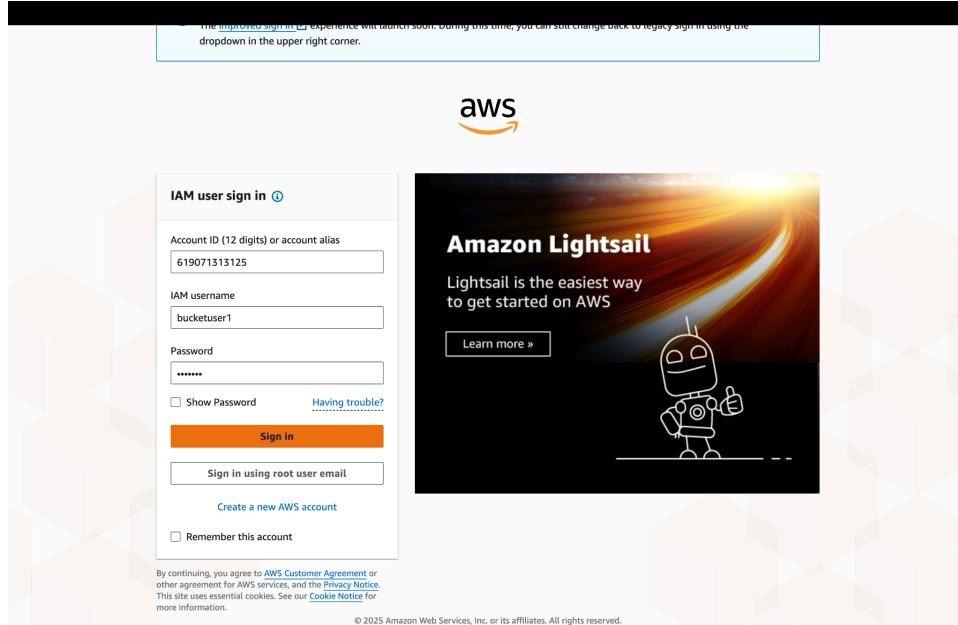
Email sign-in instructions

Cancel Download .csv file Return to users list

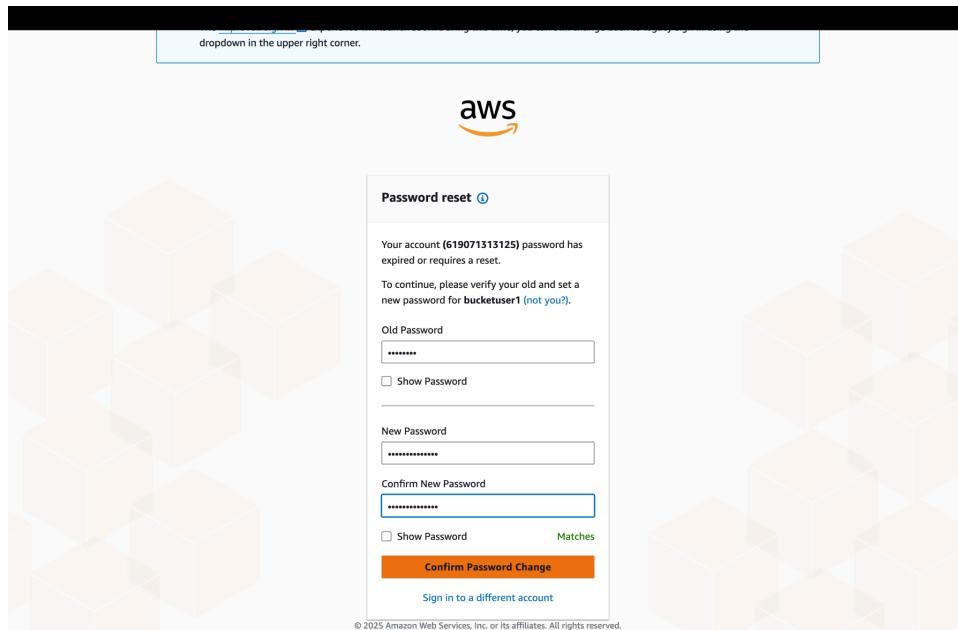
e. Downloaded .csv file contains IAM user credentials

```
bucketuser1_credentials.csv
Users > shravasti010 > Downloads > bucketuser1_credentials.csv
1 User name,Password,Console sign-in URL
2 bucketuser1,_8cUf0@,https://619071313125.signin.aws.amazon.com/console
3
```

f. Sign-in using the credentials provided

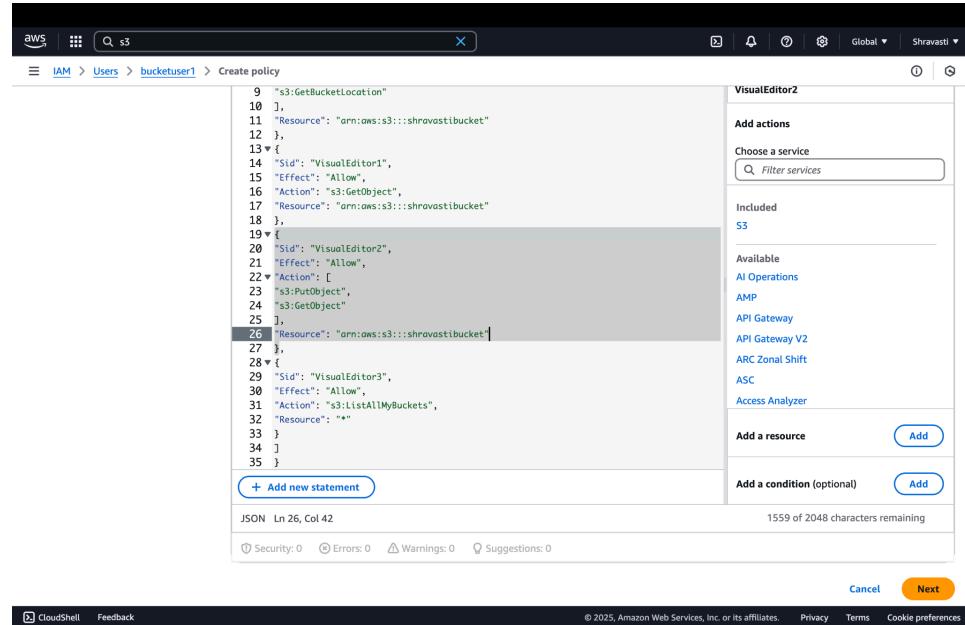


g. Reset the password



- h. Access to the bucket and its contents will be denied.
i. Configure inline permissions for the IAM user through the root user.

j. Write the inline policy



```
aws | s3 | IAM > Users > bucketuser1 > Create policy
  9 "s3:GetBucketLocation"
 10 ],
 11 "Resource": "arn:aws:s3:::shrawastibucket"
 12 },
 13 ▼ {
 14 "Sid": "VisualEditor1",
 15 "Effect": "Allow",
 16 "Action": "s3:GetObject",
 17 "Resource": "arn:aws:s3:::shrawastibucket"
 18 },
 19 ▼ {
 20 "Sid": "VisualEditor2",
 21 "Effect": "Allow",
 22 ▼ "Action": [
 23 "s3:PutObject",
 24 "s3:GetObject"
 25 ],
 26 "Resource": "arn:aws:s3:::shrawastibucket"
 27 },
 28 ▼ {
 29 "Sid": "VisualEditor3",
 30 "Effect": "Allow",
 31 "Action": "s3:ListAllMyBuckets",
 32 "Resource": "*"
 33 }
 34 ]
 35 }
```

+ Add new statement

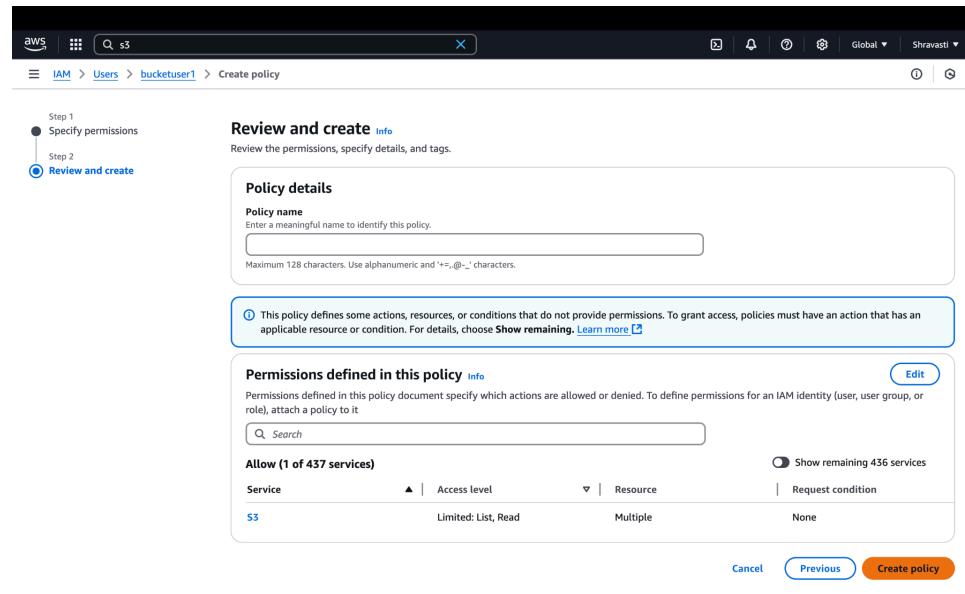
JSON Ln 26, Col 42 1559 of 2048 characters remaining

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Add actions Choose a service Filter services Included S3 Available AI Operations AMP API Gateway API Gateway V2 ARC Zonal Shift ASC Access Analyzer Add a resource Add Add a condition (optional) Add

Cancel Next

k. Name the policy and create it



Step 1
Specify permissions

Step 2
Review and create

Review and create [Info](#)
Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.
Maximum 128 characters. Use alphanumeric and '+-=_,@_-' characters.

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose Show remaining. [Learn more](#)

Permissions defined in this policy [Info](#)
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Allow (1 of 437 services)

Service	Access level	Resource	Request condition
S3	Limited: List, Read	Multiple	None

Cancel Previous Create policy

Identity and Access Management (IAM)

bucketuser1

Summary

ARN: arn:aws:iam::619071313125:user/bucketuser1

Console access: Enabled without MFA

Created: February 26, 2025, 15:17 (UTC+05:30)

Last console sign-in: Today

Access key 1: Create access key

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

Policy name	Type	Attached via
bucketfileaccesspolicy	Customer inline	Inline
IAMUserChangePassword	AWS managed	Directly

Permissions boundary (not set)

I. Bucket and its contents will now be visible

Amazon S3

General purpose buckets

Bucket: shrawastibucket

Region: Asia Pacific (Mumbai)

Creation date: February 26, 2025, 14:28:13 (UTC+05:30)

Storage Lens

Buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3