

Practical 2: Storage as a Service Using AWS

Name : Khushi
Roll No. : A073

1. Log in to AWS Management Console:

- o Go to [AWS Management Console](#).
- o Sign in with your credentials.

The screenshot shows two side-by-side web pages. On the left is the 'Sign in as IAM user' page, which includes fields for 'Account ID (12 digits) or account alias', 'IAM user name', 'Password', and a 'Remember this account' checkbox. Below these is a large blue 'Sign in' button. At the bottom are links for 'Sign in using root user email' and 'Forgot password?'. On the right is the 'Amazon Lightsail' landing page, featuring a bright orange and yellow background with a cartoon robot character. The text reads 'Amazon Lightsail' and 'Lightsail is the easiest way to get started on AWS', with a 'Learn more »' button.

2. Navigate to S3:

- o In the AWS Management Console, search for "S3."
- o Click on "S3" to open the Amazon S3 dashboard.

The screenshot shows the AWS Management Console Home page. At the top, there's a navigation bar with 'Services', a search bar, and a user dropdown for 'Khushi'. Below the navigation is a 'Console Home' section with a 'Recently visited' sidebar containing links to IAM, S3, Billing and Cost Management, and EC2. To the right of this is an 'Applications' section showing '0' applications with a 'Create application' button. Further down are sections for 'Welcome to AWS' (with a 'Getting started with AWS' link), 'AWS Health' (showing 'Open issues 0' and 'Past 7 days'), and 'Cost and usage' (showing 'Current month costs \$0' and 'Forecasted month end costs \$0').

3. Create a Bucket:

- Click on the “Create bucket” button.

The screenshot shows the AWS S3 service page. On the left, there's a sidebar with options like Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings, Storage Lens (with sub-options like Dashboards, Storage Lens groups, and AWS Organizations settings), Feature spotlight, and AWS Marketplace for S3. The main area is titled "Amazon S3" and "Amazon S3". It features an "Account snapshot - updated every 24 hours" section with a link to "All AWS Regions" and a "View Storage Lens dashboard" button. Below this is a navigation bar with tabs for "General purpose buckets" (which is selected) and "Directory buckets". A table lists "General purpose buckets" (1). The first row shows a bucket named "prac2ofcc" in the "Asia Pacific (Mumbai) ap-south-1" region, created on "July 27, 2024, 15:58:07 (UTC+05:30)". Buttons for "Copy ARN", "Empty", "Delete", and "Create bucket" are visible at the top of the table.

4. Configure Bucket Settings:

- **Bucket Name:** Enter a unique name for your bucket (bucket names must be globally unique across all AWS users).
- **Region:** Choose the AWS region where you want to create the bucket. Select the region closest to you or where your application is hosted to minimize latency.

The screenshot shows the "Create bucket" configuration page. At the top, it says "Create bucket" with a link to "Info". Below that, it says "Buckets are containers for data stored in S3." Under "General configuration", there's a "AWS Region" dropdown set to "Asia Pacific (Mumbai) ap-south-1", a "Bucket name" input field containing "pracofcc", and a note about naming rules. There's also a "Choose bucket" button and a "Format: s3://bucket/prefix" note. In the "Object Ownership" section, there are two radio buttons: "ACLs disabled (recommended)" (selected) and "ACLs enabled". The "ACLs disabled" option notes that objects are owned by the account and access is controlled by policies. The "ACLs enabled" option notes that objects can be owned by other accounts and access can be controlled by ACLs. At the bottom, there are "Object Ownership" and "Next Step" buttons.

5. Configure Bucket Options:

- **Block Public Access:** By default, block all public access to keep your data private. You can modify this later if needed.
- **Versioning:** Enable versioning if you want to keep multiple versions of objects in the bucket.
- **Tags:** Add any tags to categorize and manage your bucket.
- **Object Lock:** Enable if you need to prevent objects from being deleted or overwritten (often used for regulatory compliance).

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

[CloudShell](#) [Feedback](#) © 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Tags - optional (0)

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

No tags associated with this bucket.

[Add tag](#)

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

Server-side encryption with Amazon S3 managed keys (SSE-S3)
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Disable
 Enable

[Advanced settings](#)

[CloudShell](#) [Feedback](#) © 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

6. Review and Create:

- Review your settings to ensure everything is configured as needed.
- Click on the “Create bucket” button to finalize the creation.

The screenshot shows the 'Default encryption' section of the AWS S3 Bucket Creation wizard. It includes options for 'Encryption type' (Server-side encryption with Amazon S3 managed keys (SSE-S3) is selected), 'Bucket Key' (Enable is selected), and a note about using an S3 Bucket Key for SSE-KMS. A 'Create bucket' button is at the bottom.

The screenshot shows the AWS S3 Buckets dashboard. A green banner at the top indicates 'Successfully created bucket "pracofcc"'. Below it, the 'General purpose buckets' tab is selected, showing two buckets: 'prac2ofcc' and 'pracofcc'. The 'pracofcc' bucket details are shown in a modal, including its name, region (Asia Pacific (Mumbai) ap-south-1), and creation date (August 30, 2024). A 'Create bucket' button is visible at the top right of the table.

Uploading Files to Your S3 Bucket

1. Open Your Bucket:

- Click on your newly created bucket in the S3 dashboard.

2. Upload Files:

- Click on the “Upload” button.
- Drag and drop files into the console or click “Add files” to browse your computer.
- Optionally, click “Add folder” to upload entire folders.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'Services' and a search bar. Below it, the path 'Amazon S3 > Buckets > pracofcc' is shown. The main content area is titled 'pracofcc Info'. A horizontal menu bar at the top of this section includes 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Under the 'Objects' tab, there's a sub-menu with 'Info' and several actions: 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A message 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 with placeholder text 'Find objects by prefix'. A table header row shows columns for 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. A message 'No objects' indicates 'You don't have any objects in this bucket.' A large 'Upload' button is centered at the bottom.

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

3. Set Permissions (Optional):

- By default, files are private. You can modify permissions during the upload process if you want to make them public or restrict access.

4. Upload:

- Click on the “Upload” button to start uploading your files.

The screenshot shows the 'Upload' page within the AWS S3 console. The path 'Amazon S3 > Buckets > pracofcc > Upload' is visible. The main area is titled 'Upload Info'. A message says: '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](#)'. Below this is a large dashed blue rectangular area with the placeholder text 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' A table titled 'Files and folders (82 Total, 7.1 MB)' lists 82 items. It has a 'Remove' button and two action buttons: 'Add files' and 'Add folder'. A search bar 'Find by name' is at the top of the table. The table columns are 'Name', 'Folder', and 'Type'. The data in the table is as follows:

Name	Folder	Type
3rd-april-2018-guwahati-assam-600w-1...	My project work/	image/webp
download (1).jpg	My project work/	image/jpeg
kerala.jpg	My project work/	image/jpeg
rajasthan.html	My project work/	text/html
conclusion.html	My project work/	text/html
shyam-rai-temple-bishnupur-west-beng...	My project work/	image/jpeg
karnataka-map-shape-on-coffee-260nw-...	My project work/	image/webp
punjab.html	My project work/	text/html
andhra.html	Mv project work/	text/html

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

S | Services | Search | [Option+S] | Mumbai | Khushi | ⓘ | ⓘ

Files and folders (82 Total, 7.1 MB)

All files and folders in this table will be uploaded.

	Name	Folder	Type
<input type="checkbox"/>	punjab.html	My project work/	text/html
<input type="checkbox"/>	andhra.html	My project work/	text/html
<input type="checkbox"/>	gujrat.jpeg	My project work/	image/jpeg

Destination Info

Destination
<s3://pracofcc>

▶ **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**

CloudShell | Feedback | © 2024, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

5. Wait for some time to upload the files.

S | Services | Search | [Option+S] | Mumbai | Khushi | ⓘ | ⓘ

Uploading

Total remaining: 69 files: 6.5 MB(91.45%)
Estimated time remaining: 2 minutes
Transfer rate: 68.4 KB/s

Cancel

Files and folders (82 Total, 7.1 MB)

Name	Folder	Type	Size	Status	Error
3rd-april-20...	My project w...	image/webp	29.8 KB	Success	-
download (1...	My project w...	image/jpeg	13.0 KB	Success	-
kerala.jpg	My project w...	image/jpeg	5.3 KB	Success	-
rajasthan.ht...	My project w...	text/html	12.0 KB	Success	-
conclusion.h...	My project w...	text/html	4.6 KB	Success	-
shyam-rai-te...	My project w...	image/jpeg	52.7 KB	Success	-
karnataka-m...	My project w...	image/webp	6.7 KB	Success	-
punjab.html	My project w...	text/html	12.5 KB	Success	-
andhra.html	My project w...	text/html	12.8 KB	Success	-
gujrat.jpeg	My project w...	image/jpeg	9.3 KB	Success	-

CloudShell | Feedback | © 2024, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

AWS Services Search [Option+S] Mumbai ▾ Khushi ▾

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://pracofcc	82 files, 7.1 MB (100.00%)	0 files, 0 B (0%)

[Files and folders](#) Configuration

Files and folders (82 Total, 7.1 MB)

Name	Folder	Type	Size	Status	Error
3rd-april-20...	My project w...	image/webp	29.8 KB	Succeeded	-
download (1...)	My project w...	image/jpeg	13.0 KB	Succeeded	-
Icons-in-...	My project w...	image/png	5.7 KB	Succeeded	-

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Option+S] Mumbai ▾ Khushi ▾

Amazon S3

Buckets

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

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight 7

AWS Marketplace for S3

rajasthan.html Info

Copy S3 URI Download Open Object actions

Properties Permissions Versions

Object overview

Owner	s3://pracofcc/My project work/rajasthan.html
AWS Region	Asia Pacific (Mumbai) ap-south-1
Last modified	August 30, 2024, 22:26:19 (UTC+05:30)
Size	12.0 KB
Type	html
Key	My project work/rajasthan.html
S3 URI	s3://pracofcc/My project work/rajasthan.html
Amazon Resource Name (ARN)	arn:aws:s3:::pracofcc/My project work/rajasthan.html
Entity tag (Etag)	d35d597fe3827b1d1cc0f54a46027cd9
Object URL	https://pracofcc.s3.ap-south-1.amazonaws.com/My+project+work/rajasthan.html

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Option+S] Mumbai Khushi

Amazon S3

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

- Block Public Access settings for this account

- Storage Lens**
- Dashboards
- Storage Lens groups
- AWS Organizations settings

- Feature spotlight 7

- AWS Marketplace for S3

[Amazon S3 > Buckets](#)

Account snapshot - updated every 24 hours All AWS Regions

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

[View Storage Lens dashboard](#)

General purpose buckets Directory buckets

General purpose buckets (2) Info All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
prac2ofcc	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	July 27, 2024, 15:58:07 (UTC+05:30)
pracofcc	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	August 30, 2024, 22:15:35 (UTC+05:30)

Find buckets by name

< 1 > ⌂

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Option+S] Mumbai Khushi

Amazon S3

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

- Block Public Access settings for this account

- Storage Lens**
- Dashboards
- Storage Lens groups
- AWS Organizations settings

- Feature spotlight 7

- AWS Marketplace for S3

[Amazon S3 > Buckets > pracofcc > My project work/](#)

My project work/

[Copy S3 URI](#)

Objects (82) Info

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

Name	Type	Last modified	Size	Storage class
14863676540.jpg	jpg	August 30, 2024, 22:26:30 (UTC+05:30)	88.2 KB	Standard
1517913671-him_2810_20180529223322.jpg	jpg	August 30, 2024, 22:26:26 (UTC+05:30)	30.7 KB	Standard
1553521054_forts_maha_ha.jpg.jpg	jpg	August 30, 2024, 22:26:21 (UTC+05:30)	414.1 KB	Standard
2018030794.jpg	jpg	August 30, 2024, 22:26:36 (UTC+05:30)	55.8 KB	Standard
3rd-april-2018-guwahati-assam-600w-1062288055.webp	webp	August 30, 2024, 22:26:18 (UTC+05:30)	29.8 KB	Standard
458.jpg	jpg	August 30, 2024, 22:26:25 (UTC+05:30)	79.5 KB	Standard
5449316980_4849084a2e_s.jpg	jpg	August 30, 2024, 22:26:29 (UTC+05:30)	5.2 KB	Standard
5467961742_efcbc59288_b_20170920134940.jpg	jpg	August 30, 2024, 22:26:26 (UTC+05:30)	85.4 KB	Standard

Find objects by prefix

< 1 > ⌂

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS S3 Object Details page for the file "abstract-visakhapatnam-skyline-color-buildings-260nw-647925325.webp".

Properties:

- Owner: fb98bbf5ac8db684d1b07837d03f65e86a9e64ad9022a79a87fb48934bebb5cf
- AWS Region: Asia Pacific (Mumbai) ap-south-1
- Last modified: August 30, 2024, 22:26:33 (UTC+05:30)
- Size: 26.6 KB
- Type: webp
- Key: My project work/abstract-visakhapatnam-skyline-color-buildings-260nw-647925325.webp
- S3 URI: s3://pracofcc/My project work/abstract-visakhapatnam-skyline-color-buildings-260nw-647925325.webp
- Amazon Resource Name (ARN): arnaws3::pracofcc/My project work/abstract-visakhapatnam-skyline-color-buildings-260nw-647925325.webp
- Entity tag (Etag): 9811c1aea7b6779324c7cad8a19b07d9
- Object URL: https://pracofcc.s3.ap-south-1.amazonaws.com/My+project+work/abstract-visakhapatnam-skyline-color-buildings-260nw-647925325.webp

Object management overview:

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

Bucket properties	Management configurations
Bucket Metrics	Bucket Logging

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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>117RC151K0S9BR4W</RequestId>
<HostId>ORIVQt+9j/AjBW7gqbRGVBUNQSJ+sJjjF+FPULisBiwxX8gBTKfodTuRPqPAQM9B0zLMXPFhssA=</HostId>
</Error>
```

Screenshot of the AWS S3 Buckets page.

General purpose buckets (2):

Name	AWS Region	IAM Access Analyzer	Creation date
prac2ofcc	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	July 27, 2024, 15:58:07 (UTC+05:30)
pracofcc	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	August 30, 2024, 22:15:55 (UTC+05:30)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Amazon S3

Buckets

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

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight ?

AWS Marketplace for S3

pracofcc Info

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#).

[View analyzer for ap-south-1](#)

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#).

Block all public access

On

► Individual Block Public Access settings for this bucket

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](#).

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](#).

No policy to display.

Edit Delete Copy

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Amazon S3

Buckets

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

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight ?

AWS Marketplace for S3

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:::pracofcc

Policy

1 | Edit statement

Select a statement

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

+ Add new statement

CloudShell Feedback

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](#).

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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 1 Action(s) Selected

All Actions (*)

- GetMultiRegionAccessPointPolicy
- GetMultiRegionAccessPointPolicyStatus
- GetMultiRegionAccessPointRoutes
- GetObject
- GetObjectAcl
- GetObjectAttributes
- GetObjectLegalHold

:\${BucketName}/\${KeyName}.

alid. You must enter a valid ARN.

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.

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

-- Select Actions --

All Actions ('*')

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}.

Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

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

Principal(s)	Effect	Action	Resource	Conditions
* *	Allow	s3:GetObject	arn:aws:s3:::pracofcc	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

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 -- Select Actions -- All Actions ('*')

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will not be reflected in the policy generator tool.

```
{ "Id": "Policy1725038843326", "Version": "2012-10-17", "Statement": [ { "Sid": "Stmt1725038838581", "Action": [ "s3:GetObject" ], "Effect": "Allow", "Resource": "arn:aws:s3:::pracofcc", "Principal": "*" } ] }
```

You added the following statements:

Principal(s)	Effect	Action	Resource	Conditions
* *	Allow	s3:GetObject	arn:aws:s3:::pracofcc	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 governing your use of Amazon Web Services technologies.

Close

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.
An [amazon.com](#) company

Amazon S3

Buckets

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

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight 7

AWS Marketplace for S3

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](#)

Bucket ARN

arn:aws:s3:::pracofcc

Policy

```

1  {
2   "Id": "Policy1725038925375",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Stmt1725038838581",
7       "Action": [
8         "s3:GetObject"
9       ],
10      "Effect": "Allow",
11      "Resource": "arn:aws:s3:::pracofcc",
12      "Principal": "*"
13    }
14  ]
15 }
```

Edit statement

Select a statement

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

+ Add new statement

Amazon S3

Buckets

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

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight 7

AWS Marketplace for S3

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

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

- Block public access to buckets and objects granted through new access control lists (ACLs)**
- Block public access to buckets and objects granted through any access control lists (ACLs)**
- Block public access to buckets and objects granted through new public bucket or access point policies**
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**

Cancel **Save changes**

Amazon S3

Buckets

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

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight 7

AWS Marketplace for S3

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases.

Edit Block public access (bucket settings)

⚠️ 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.

To confirm the settings, enter **confirm** in the field.

confirm

Cancel **Confirm**

Cancel **Save changes**

The screenshot shows the AWS S3 console interface. On the left, a sidebar menu includes 'Buckets', 'Storage Lens', and 'Feature spotlight'. The main area displays a single object named 'tourism.html' in the bucket 'pracofcc'. The object details show it is an HTML file uploaded on August 30, 2024, at 22:50:38 (UTC+05:30), with a size of 3.2 KB and a storage class of Standard.

You can see your file by copy paste it on the chrome

The screenshot shows a website for tourism in India. The header features a red banner with the text 'Welcome to Incredible India'. Below the banner, there are four main sections: 'About India' (describing India's diverse cultures, languages, and landscapes), 'Top Attractions' (listing Taj Mahal, Agra, Jaipur, Rajasthan, Goa Beaches, Kerala Backwaters, and Varanasi, Uttar Pradesh), 'Culture & Heritage' (describing India's rich cultural heritage with ancient temples, historic monuments, traditional music and dance, and colorful festivals), and 'Contact Us' (providing email and phone number for inquiries). The footer contains a copyright notice: '© 2024 Tourism of India. All rights reserved.'