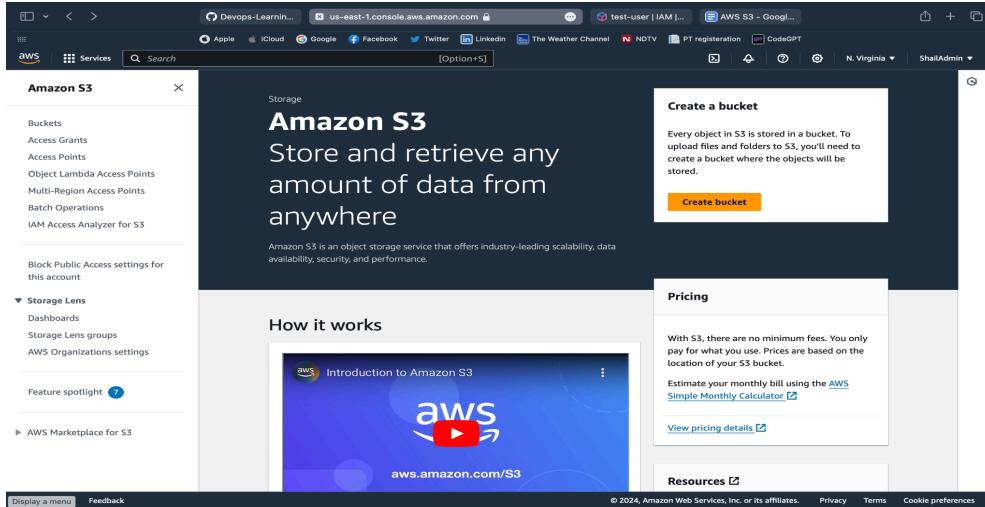
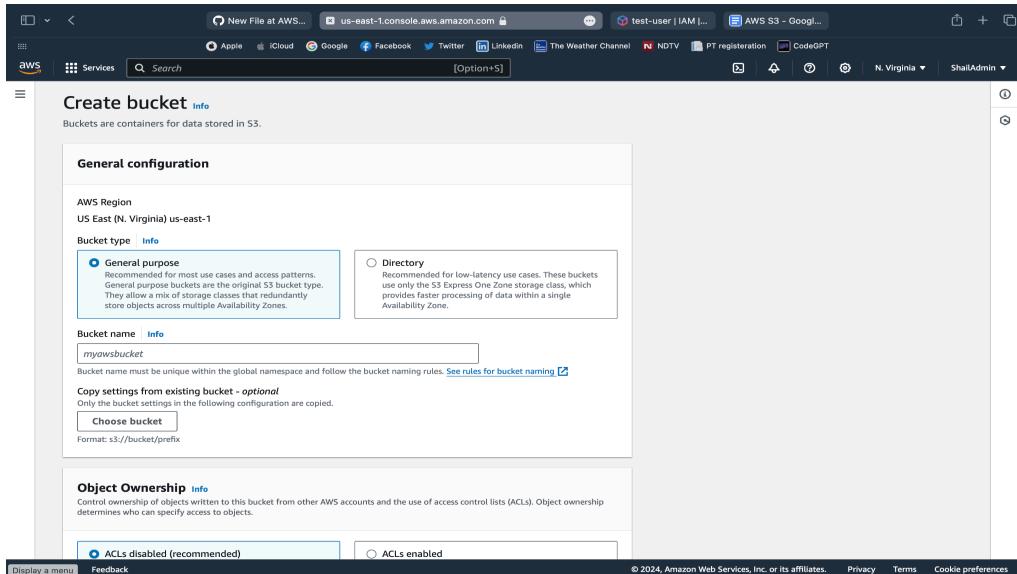


# S3 Bucket



Click on create bucket.



The screenshot shows the 'Object Ownership' section of the AWS S3 Bucket Properties page. It includes two radio button options: 'ACLs disabled (recommended)' (selected) and 'ACLs enabled'. The 'ACLs disabled' option states: 'All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.' The 'ACLs enabled' option states: 'Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.' Below this, the 'Bucket owner enforced' setting is shown.

**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.

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

The screenshot shows the 'Bucket Versioning' section of the AWS S3 Bucket Properties page. It includes two radio button options: 'Disable' (selected) and 'Enable'. Below this, the 'Tags - optional (0)' section is shown, which is currently empty. The 'Default encryption' section indicates that server-side encryption is automatically applied to new objects stored in the bucket.

**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

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

## Create S3 Bucket. Playaround with console

How to enable versioning in S3 Bucket

Go to bucket objects

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Below this, a toolbar includes actions like 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A search bar and a 'Find objects by prefix' input field are also present. The main area displays a table of objects:

Name	Type	Last modified	Size	Storage class
s1.pdf	pdf	August 31, 2024, 07:56:13 (UTC+05:30)	91.2 KB	Standard
s2.pdf	pdf	August 31, 2024, 07:56:38 (UTC+05:30)	91.7 KB	Standard

## Go to Properties – Bucket Versioning - Enable bucket versioning

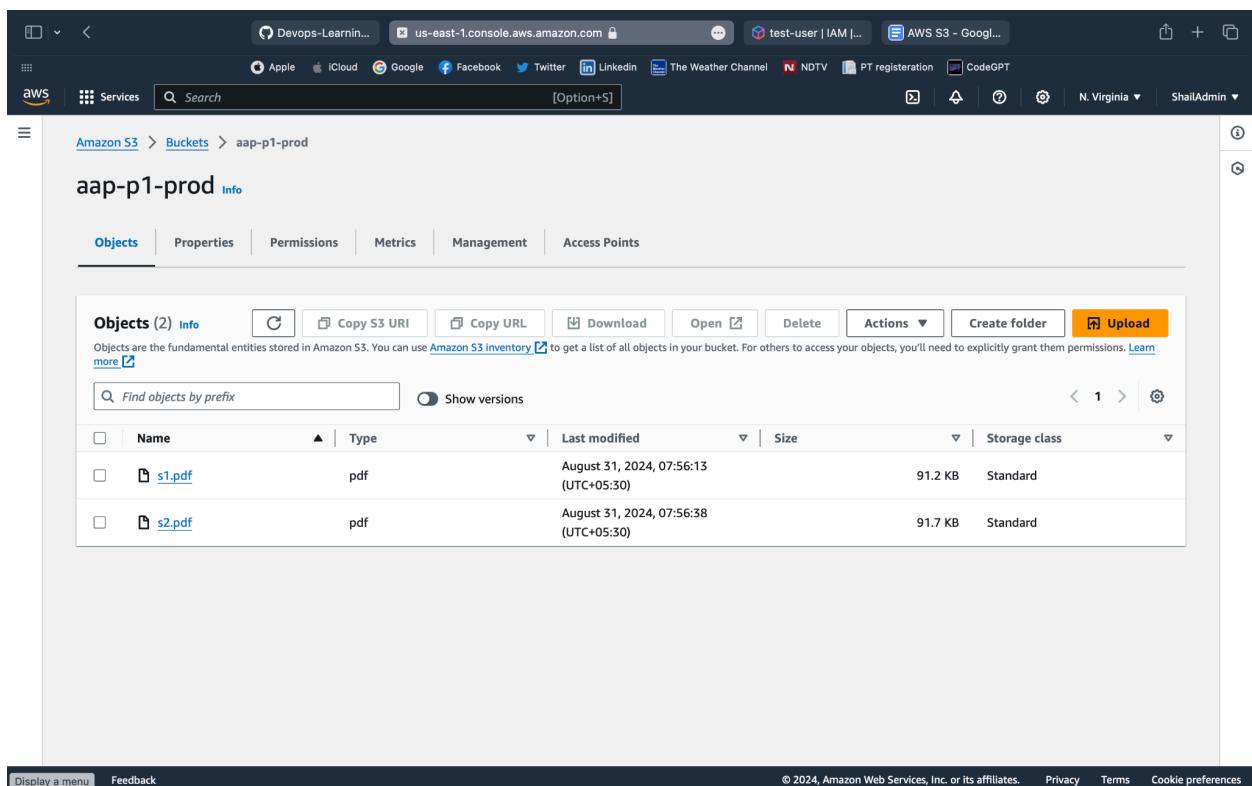
The screenshot shows the 'Edit Bucket Versioning' page. It features a 'Bucket Versioning' section with a descriptive paragraph about versioning. Below this, there are two options: 'Suspend' (radio button) and 'Enable' (radio button, which is selected). Underneath, there's a note about Multi-factor authentication (MFA) delete and a dropdown menu set to 'Disabled'. At the bottom, there are 'Cancel' and 'Save changes' buttons.

Save Changes.

Once you upload the same file again you can see different version of file stored which can be retrieved.

For the test – upload the same file again.

Go to the object



The screenshot shows the AWS S3 console interface. The top navigation bar includes links for Devops-Learning, us-east-1.console.aws.amazon.com, test-user | IAM | ..., AWS S3 - Google Sheets, and other services like Apple, iCloud, Google, Facebook, Twitter, LinkedIn, The Weather Channel, NDTV, PT registration, and CodeGPT. The region is set to N. Virginia, and the user is ShallAdmin. The main navigation bar shows AWS Services and a search bar. Below it, the breadcrumb navigation shows Amazon S3 > Buckets > aap-p1-prod. The current view is on the 'Objects' tab, with other tabs for Properties, Permissions, Metrics, Management, and Access Points. A prominent orange 'Upload' button is visible. The object list table shows two entries:

Name	Type	Last modified	Size	Storage class
s1.pdf	pdf	August 31, 2024, 07:56:13 (UTC+05:30)	91.2 KB	Standard
s2.pdf	pdf	August 31, 2024, 07:56:38 (UTC+05:30)	91.7 KB	Standard

At the bottom, there are links for Display a menu, Feedback, © 2024, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

Click on the object you want to see. Here s1 for ex,

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with links like 'Devops-Learnin...', 'us-east-1.console.aws.amazon.com', 'test-user | IAM ...', 'AWS S3 - Google Sheets', and various social media and news links. Below the navigation bar, the main content area shows the 'Amazon S3 > Buckets > aap-p1-prod > s1.pdf' path. The file 's1.pdf' is listed with its details: Type: pdf, Last modified: August 31, 2024, 07:56:13 (UTC+05:30), Size: 91.2 KB, Storage class: Standard. There are buttons for 'Copy S3 URI', 'Download', 'Open', and 'Object actions'. Below the file details, there's a 'Versions' section header with a table showing one version:

Version ID	Type	Last modified	Size	Storage class
t9wHWL2.bUqOG2xJL81WTmj3q.k159P9 (Current version)	pdf	August 31, 2024, 07:56:13 (UTC+05:30)	91.2 KB	Standard

At the bottom of the page, there are links for 'Display a menu', 'Feedback', '© 2024, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

Go to version. You can find different permission of the file.

S3 bucket with IAM users.

Create a test IAM user

The screenshot shows the 'Specify user details' step of the AWS IAM 'Create user' wizard. The 'User name' field contains 'test-IAM'. Under 'User type', the 'I want to create an IAM user' option is selected. In the 'Console password' section, 'Custom password' is chosen, and a password is entered. The sidebar on the left lists steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The bottom of the screen includes standard AWS navigation links and copyright information.

Click on Next.

The screenshot shows the 'Set permissions' step of the AWS IAM 'Create user' wizard. Under 'Permissions options', 'Add user to group' is selected. Below it, 'Get started with groups' provides instructions for creating a group and attaching policies. The 'Set permissions boundary - optional' section is collapsed. At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons. The sidebar and footer are consistent with the previous screenshot.

For now lets keep it as add user to group

Click on next. Review and Create.

Once user is created.

The screenshot shows the AWS Management Console with the URL `us-east-1.console.aws.amazon.com`. The top navigation bar includes links for DevOps-Learn..., s1.pdf - Object i..., us-east-1.console.aws.amazon.com, AWS S3 - Google..., and other services like Apple, iCloud, Google, Facebook, Twitter, LinkedIn, The Weather Channel, NDTV, PT registration, and CodeGPT. The IAM service is selected in the sidebar.

The main content area displays a success message: "User created successfully". Below it, a note says: "You can view and download the user's password and email instructions for signing in to the AWS Management Console." A "View user" button is available.

The process is at Step 4: "Retrieve password". On the left, a vertical navigation pane shows "Step 1: Specify user details", "Step 2: Set permissions", "Step 3: Review and create", and "Step 4: Retrieve password".

The central panel is titled "Retrieve password" and contains the "Console sign-in details" section. It shows the "Console sign-in URL" as `https://637423339839.signin.aws.amazon.com/console`, the "User name" as "test-IAM", and the "Console password" (redacted). A "Show" link is provided to reveal the password. A "Email sign-in instructions" button is also present.

At the bottom, there are "Cancel", "Download .csv file", and "Return to users list" buttons.

Navigate to console sign-in url and sign in incognito mode.

The screenshot shows a browser window with the URL `eu-north-1.signin.aws.amazon.com`. The top navigation bar includes links for Apple, iCloud, Google, Facebook, Twitter, LinkedIn, The Weather Channel, NDTV, PT registration, and CodeGPT. A modal dialog box at the top says "Try the new sign in UI" and "See our new improved Amazon Web Services sign in experience before we officially launch." with a "Enable new sign in" button.

The main content area features the AWS logo and a sign-in form. The form fields are: "Account ID (12 digits) or account alias" (value: 637423339839), "IAM user name" (value: test-IAM), and "Password" (redacted). There is a "Remember this account" checkbox and a "Sign in" button. Below the form is a link to "Sign in using root user email" and a "Forgot password?" link.

To the right of the sign-in form is a promotional banner for "Amazon Lightsail". It features a cartoon robot character and the text: "Amazon Lightsail" and "Lightsail is the easiest way to get started on AWS". A "Learn more »" button is at the bottom of the banner.

At the bottom of the page, there is a language selection dropdown set to "English" and a small "Display a menu" link.

Once you login. You will find no S3 buckets

The screenshot shows the Amazon S3 service page. A modal window titled 'Create' is open, prompting the user to 'Create a new bucket'. It includes instructions: 'New: AWS User Notifications quick setup' and 'Enable common notifications for CloudWatch, EC2, and Health using the new quick setup feature in AWS User Notifications.' Below this, it says 'Every time you upload a file to create a new bucket, the file will be stored.' There are 'Done' and 'Create bucket' buttons. In the background, there's a video player titled 'Introduction to Amazon S3' and a 'Pricing' section.

Now lets go an S3 access policy

The screenshot shows the IAM service's 'Users' page. On the left, a navigation menu is visible with sections like 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'Related consoles'. The main area displays a table for 'Users (1) Info'. The table has one row for 'test-IAM', which is highlighted. The columns include 'User name' (test-IAM), 'Path' (/), 'Groups' (0), 'Last activity' (1 minute ago), 'MFA' (-), 'Password age' (3 minutes), and 'Console' (Augus). There are 'Edit', 'Delete', and 'Create user' buttons at the top of the table.

Go to users

Click on the users

The screenshot shows the AWS IAM User Details page for a user named 'test-IAM'. The left sidebar is collapsed, and the main content area displays the 'Summary' section. Key details shown include:

- ARN: arn:aws:iam::637423339839:user/test-IAM
- Console access: Enabled without MFA
- Access key 1: Create access key
- Created: August 31, 2024, 08:05 (UTC+05:30)
- Last console sign-in: Today

The 'Permissions' tab is active, showing 0 policies attached. Below this, there is a search bar and a table header for 'Permissions policies (0)'. The table has columns for Policy name, Type, and Attached via. The message 'No resources to display' is shown.

Click on add permissions. Attach policies directly. AmazonS3 fullaccess.

The screenshot shows the 'Add permissions' step in the AWS IAM User Details page for 'test-IAM'. The 'Step 1' and 'Step 2' tabs are visible at the top. The 'Permissions options' section contains three radio buttons:

- Add user to group: Adds user to an existing group or creates a new one.
- Copy permissions: Copies all group memberships, attached managed policies, inline policies, and any existing permission boundaries from an existing user.
- Attach policies directly: Attaches a managed policy directly to a user.

The 'Permissions policies' section shows a table with 12 matches for 'S3'. The table includes columns for Policy name, Type, and Attached entities. One policy, 'AmazonS3FullAccess', is highlighted with a blue border.

Click on Next – Add Permissions.

Refresh the root user and you will find he has all the permission.  
Now as Devops Engineer I want to deny access to S3 bucket for all users except me

The screenshot shows the AWS S3 console with the 'Permissions' tab selected. In the 'Block public access (bucket settings)' section, the status is set to 'On'. A note at the bottom of this section states: 'Public access is blocked because Block Public Access settings are turned on for this bucket'. The 'Edit' button is visible next to the status indicator.

Go to S3 buckets > Permissions > bucket Policy > Edit

The screenshot shows the 'Edit bucket policy' page for the 'aap-p1-prod' bucket. The left sidebar lists various AWS services like Buckets, Access Grants, and Storage Lens. The main area has tabs for 'Bucket policy' (selected), 'Policy examples', and 'Policy generator'. It displays the JSON policy:

```
arn:aws:s3:::aap-p1-prod
```

The 'Policy' section contains a code editor with the following JSON:

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

To the right of the editor is a panel titled 'Edit statement' with a 'Select a statement' dropdown and a '+ Add new statement' button.

## Go to Add new Statement

The screenshot shows the same 'Edit bucket policy' page. A red circle highlights the 'Add actions' dropdown in the 'Edit statement' panel. The dropdown menu is open, showing the search bar 'Choose a service' with 'S3' typed in, and a list of available services: 'Available', 'S3', 'S3 Express', 'S3 Object Lambda', and 'S3 Outposts'.

Choose services S3. All actions.

The screenshot shows the AWS IAM Policy editor for an S3 access point policy named 'armaws:s3:aap-p1-prod'. The left sidebar lists various AWS services like Buckets, Access Grants, and Storage Lens. The main area displays a JSON-based policy document:

```
1  {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Principal": {},  
7       "Effect": "Allow",  
8       "Action": [  
9         "s3:*"  
10      ],  
11      "Resource": "  
12    }  
13  ]  
14 }
```

On the right, there's a sidebar for managing statements, showing 'Statement1' selected. It includes options to 'Edit statement', 'Remove', 'Add actions' (with a dropdown for 'All services > S3'), 'Access level - list' (with several checkboxes for S3 actions), and buttons for 'Add a resource' and 'Add a condition (optional)'. At the bottom, there are buttons for '+ Add new statement', 'JSON', 'Ln 5, Col 21', and links for 'Display a menu', 'Feedback', '© 2024, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

Click on Add Resource .

The screenshot shows the same AWS IAM Policy editor interface, but now with an 'Add resource' dialog open over the policy document. The dialog title is 'Add resource' and it contains the instruction 'Specify the resource type and ARN to add for the selected service.' Below this, there are dropdown menus for 'Service' (set to 'S3') and 'Resource type' (set to 'bucket'), and a text input field for 'Resource ARN' containing 'app-p1-prod'. At the bottom of the dialog are 'Cancel' and 'Add resource' buttons. The background policy document and sidebar remain visible.

Click on add condition

The screenshot shows the AWS S3 Policy editor interface. On the left, there's a sidebar with various AWS services like Buckets, Access Grants, Access Points, etc. The main area is titled 'Policy' and contains a JSON code editor with the following content:

```
1 var {  
2   3   4   5   6   7   8   9   10  11  12  13  14  15  16 }  
17 }  
18 }
```

A modal window titled 'Add condition' is open over the policy editor. It has fields for 'Condition key' (set to 'aws:PrincipalArn'), 'Qualifier' (set to 'Select qualifier'), 'Operator' (set to 'StringNotEquals'), and 'Value' (set to '"aws:PrincipalArn":"arn:aws:iam:637423339839:root"'). At the bottom of the modal are 'Cancel' and 'Add condition' buttons.

For AWS account id

Go to

<https://github.com/Gopi1892/Devops-Learning-Material/tree/main/AWS/Bucket-Policies>

And cross-reference policies and save the policies. The test-user will not be able to view the buckets.

The screenshot shows the AWS Identity and Access Management (IAM) service in the AWS Management Console. A green banner at the top indicates "1 policy added". The main navigation bar includes links for DevOps Learn..., Edit bucket poli..., us-east-1.console.aws.amazon.com, AWS S3 - Google, Apple, iCloud, Google, Facebook, Twitter, LinkedIn, The Weather Channel, NDTV, PT registration, and CodeGPT. The left sidebar shows the IAM navigation path: Identity and Access Management (IAM) > Users > test-IAM. The main content area displays the "test-IAM" user profile under the "Info" tab. The "Summary" section shows the ARN (arn:aws:iam::657423339839:user/test-IAM), which is enabled without MFA. It also shows the creation date as August 31, 2024, 08:05 (UTC+05:30). The "Permissions" tab is selected, showing one attached policy: "AmazonS3FullAccess". The "Security credentials" tab is also visible. On the right side, there are links for Account, Organization, Service Quotas, Billing and Cost Management, and Security credentials, along with a "Sign out" button.