

Create and attach your first customer managed policy

In this tutorial, you use the AWS Management Console to create a customer managed policy and then attach that policy to an IAM user in your account. The policy you create allows an IAM user to sign in directly to the AWS Management Console with read-only permissions.

The workflow has five basic steps

- Step 1: Create two Amazon S3 buckets
- Step 2: Create a customer managed policy
- Step 3: Create an IAM user while attaching the custom IAM policy to it
- Step 4: Test user access

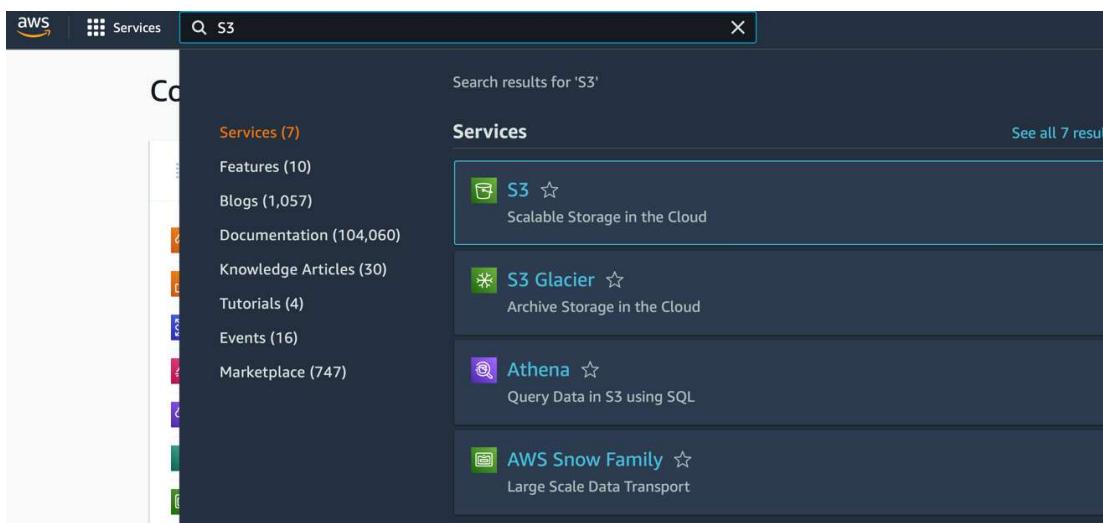
Step 1: Create two Amazon S3 buckets

In this step, you will create two Amazon S3 buckets with basic parameters.

To create S3 buckets:

- Login to AWS Management Console and search for S3 via the search menu bar provided at the top of this website.

Once clicked, it will take you to the S3 dashboard.



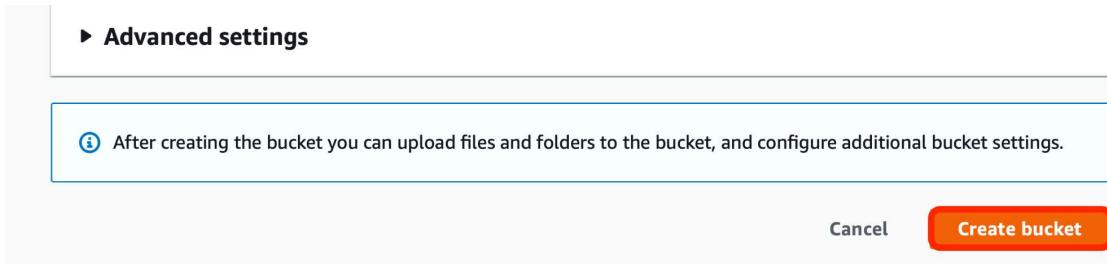
- Click **Create bucket** at top right corner of the page.



- Assign a name to this first S3 bucket while making sure that it should be unique, and choose any of the listed AWS regions.

The screenshot shows the 'Create bucket' wizard. The 'General configuration' step is active, with a red box highlighting the 'Bucket name' field containing 'demo-s3-bucket-iampolicy-one' and the 'AWS Region' dropdown set to 'US East (N. Virginia) us-east-1'. The 'Object Ownership' step is shown below, with 'ACLs disabled (recommended)' selected. The 'Choose bucket' button is visible in the 'General configuration' step.

- Accept all other default values, scroll down, and click **Create bucket**.



- Once again, you will land back to the **Buckets** dashboard. Click **Create Bucket** and start creating the second one.

Successfully created bucket "demo-s3-bucket-iampolicy-one"
To upload files and folders, or to configure additional bucket settings choose [View details](#).

View details

Amazon S3

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

[View Storage Lens dashboard](#)

Buckets (64) [Info](#)

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

[Create bucket](#)

Name	AWS Region	Access	Creation date
demo-s3-bucket-iampolicy-one	US East (N. Virginia) us-east-1	Bucket and objects not public	December 24, 2021, 12:18:50 (UTC+05:30)
myintel-lambda-s3-bucket	EU (Frankfurt) eu-central-1	Bucket and objects not public	December 11, 2021, 22:45:12 (UTC+05:30)
elasticbeanstalk-eu-central-1-001831820155	EU (Frankfurt) eu-central-1	Objects can be public	December 11, 2021, 22:20:16 (UTC+05:30)
intel-rohan-s3-demobucket	EU (Frankfurt) eu-central-1	Objects can be public	December 11, 2021, 20:45:57 (UTC+05:30)
aws-cloudtrail-logs-001831820155-827716500	Asia Pacific (Sydney) ap-southeast-2	Bucket and objects not public	December 4, 2021, 22:24:57 (UTC+05:30)

- Assign a unique name to this second S3 bucket, choose any of the listed AWS regions.

Amazon S3 > Create bucket

Create bucket Info

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

General configuration

Bucket name
 Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and granted using 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 enforced

- Scroll down to the bottom of this webpage and click **Create bucket**.

► Advanced settings

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

[Cancel](#) [Create bucket](#)

This leads to the completion of your first step where you've created two Amazon S3 buckets.

The screenshot shows the Amazon S3 console. At the top, a green banner indicates "Successfully created bucket 'demo-s3-bucket-lampolicy-two'". Below this, there's an "Account snapshot" section with a link to "View Storage Lens dashboard". The main area is titled "Buckets (65) Info" and contains a table of buckets. The table has columns: Name, AWS Region, Access, and Creation date. Two specific buckets are highlighted with a red border: "demo-s3-bucket-lampolicy-two" and "demo-s3-bucket-lampolicy-one". Both of these buckets have "Bucket and objects not public" access and were created on December 24, 2021.

Name	AWS Region	Access	Creation date
demo-s3-bucket-lampolicy-two	US East (N. Virginia) us-east-1	Bucket and objects not public	December 24, 2021, 12:36:07 (UTC+05:30)
demo-s3-bucket-lampolicy-one	US East (N. Virginia) us-east-1	Bucket and objects not public	December 24, 2021, 12:18:50 (UTC+05:30)
myintel-lambda-s3-bucket	EU (Frankfurt) eu-central-1	Bucket and objects not public	December 11, 2021, 22:45:12 (UTC+05:30)
elasticbeanstalk-eu-central-1-001831820155	EU (Frankfurt) eu-central-1	Objects can be public	December 11, 2021, 22:20:16 (UTC+05:30)
intel-rohan-s3-demobucket	EU (Frankfurt) eu-central-1	Objects can be public	December 11, 2021, 20:45:57 (UTC+05:30)
aws-cloudtrail-logs-001831820155-82771650	Asia Pacific (Sydney) ap-southeast-2	Bucket and objects not public	December 4, 2021, 22:24:57 (UTC+05:30)
aws-cloudtrail-logs-001831820155-82771650	Asia Pacific (Sydney) ap-southeast-2	Bucket and objects not public	December 4, 2021, 22:22:40 (UTC+05:30)
cf-templates-i9ukpc874r4-ap-southeast-2	Asia Pacific (Sydney) ap-southeast-2	Objects can be public	December 3, 2021, 07:54:46 (UTC+05:30)

Step 2: Create a customer managed policy

Now, you will be creating a customer managed policy via Identity and Access Management (IAM) console, which will provide read-only access for an IAM user to the first S3 bucket and full access to the second one.

- Look for IAM service via the search bar provided at the top of the page and click it to get access to the IAM dashboard.

The screenshot shows the AWS IAM service search results. The search bar at the top contains "IAM". On the left, there's a sidebar with "Services (5)" and a list of services: Features (15), Blogs (1,291), Documentation (100,356), Knowledge Articles (30), Events (4), and Marketplace (296). The main area displays a list of services under "Services". The "IAM" service is highlighted with a teal border. It has the description "Manage access to AWS resources". Other listed services include "Resource Access Manager", "Amazon VPC IP Address Manager", and "Serverless Application Repository".

- Click **Policies** which is one of the navigation menu options located at the left side of the IAM dashboard.

The screenshot shows the AWS Identity and Access Management (IAM) dashboard. The left sidebar has a 'Policies' item highlighted with a red box. The main content area is titled 'IAM dashboard' and includes sections for 'Security recommendations' (with two alerts: 'Add MFA for root user' and 'Deactivate or delete access keys for root user') and 'IAM resources'.

- Click **Create Policy** located at the right-hand corner of the Policies dashboard.

The screenshot shows the 'Policies' list page. The 'Create Policy' button is highlighted with a red box. The table lists two customer-managed policies: 'AWSCodePipelineServiceRole-sp-south-1-nodejsapppipeline' and 'AWSCodePipelineServiceRole-sp-south-1-nodejsdemopipeline'.

- For this demo, use **Visual editor** designed to select relevant options and produce a JSON policy as an output. Click **Choose a service** to get started.

The screenshot shows the 'Create policy' visual editor. The 'Visual editor' tab is selected. The 'Actions' section contains a 'Service' dropdown with a 'Choose a service' button, which is highlighted with a red box. Other sections include 'Resources' and 'Request conditions'.

- Type 'S3' as a keyword and select S3.

The screenshot shows the 'Create policy' interface in the AWS Management Console. At the top, there are three numbered tabs: 1 (blue), 2 (white), and 3 (white). Below them is a header with 'Create policy' and tabs for 'Visual editor' (selected) and 'JSON'. A note below the tabs states: 'A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more'.

The main area is titled 'S3' with a dropdown menu 'Service Select a service below' and a search bar 'Q S3'. Other services listed are 'S3 Object Lambda' and 'S3 Outposts'. There are buttons for 'Clone' and 'Remove' at the top right. Below the service list are sections for 'Actions' (with a 'Select actions' button) and 'Resources' (with a 'Choose actions before applying resources' link). At the bottom are 'Request conditions' and 'Choose actions before specifying conditions'.

- Go to **Actions** and select **List** and **Read** actions within **Access Level**.

The screenshot shows the 'Create policy' interface with the 'Actions' section highlighted by a red box. The title is 'Specify the actions allowed in S3'. It includes a search bar 'Q Filter actions' and a note 'Manual actions (add actions)' with a link 'All S3 actions (63+)'. Below this is the 'Access level' section, which contains two checked checkboxes: 'List (10 selected)' and 'Read (50 selected)'. There are also other options like 'Tagging', 'Write', and 'Permissions management' with their respective checkboxes. The right side of the screen has buttons for 'Clone' and 'Remove' and a note 'Switch to deny permissions'.

- Scroll down and click **Resources** where you will be specifying the bucket and object details.

The screenshot shows the AWS IAM Policy Editor for the S3 service. At the top, it says "S3 (60 actions) ▲ 8 warnings". Below that, under "Actions", there is a section titled "Specify the actions allowed in S3" with a "Filter actions" input field. It lists several actions: "List (10 selected)", "Read (50 selected)", "Tagging", "Write", and "Permissions management". Under "Resources", it specifies "accesspoint" resource ARN for the GetAccessPointPolicy and 1 more action, and "bucket" resource ARN for the GetBucketLocation and 24 more actions. At the bottom, there is a "Request conditions" section with a "Specify request conditions (optional)" link.

- Click **Add ARN** within the bucket resource section.

The screenshot shows the "Resources" section of the AWS IAM Policy Editor. It includes options for "Specific" or "All resources". Under "Resources", there are several items listed: "accesspoint", "bucket", "job", "multiregionacces...", "multiregionacces...", "object", "objectlambdaacc...", and "storagelensconfig...". The "bucket" item is highlighted with a red border, and the "Add ARN" button next to it is also highlighted with a red border.

- Now, specify the name of the very first Amazon S3 bucket here. This will automatically specify the Amazon Resource Name (ARN) of this very bucket.

Please note that this will automatically fill in the ARN for this bucket in **Specify ARN for**

bucket field. Click **Add**.

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. [Learn more](#)

Specify ARN for bucket [List ARNs manually](#)

arn:aws:s3:::demo-s3-bucket-iampolicy-one

Bucket name * Any

[Cancel](#) [Add](#)

- Once you get back to the **Resources** section, click **Add ARN** in the object resource section.

▼ Resources Specific All resources [close](#)

accesspoint ?	Specify accesspoint resource ARN for the GetAccessPointPolicy and 1 more action. i	<input type="checkbox"/> Any in this account
Add ARN to restrict access		
bucket ?	arn:aws:s3:::demo-s3-bucket-iampolicy-one EDIT X	<input type="checkbox"/> Ar
Add ARN to restrict access		
job ?	Specify job resource ARN for the DescribeJob and 1 more action. i	<input type="checkbox"/> Any in this account
Add ARN to restrict access		
multiregionacces... ?	Specify multiregionaccesspoint resource ARN for the GetMultiRegionAccessPoint and 2 more actions. i	<input type="checkbox"/> Any in this account
Add ARN to restrict access		
multiregionacces... ?	Specify multiregionaccesspointrequestarn resource ARN for the DescribeMultiRegionAccessPointOperation action.	<input type="checkbox"/> Any in this account
Add ARN to restrict access		
object ?	Specify object resource ARN for the ListMultipartUploadParts and 11 more actions. i	<input type="checkbox"/> Ar
Add ARN to restrict access		
objectlambdaacc... ?	Specify objectlambdaaccesspoint resource ARN for the GetAccessPointPolicyForObjectLambda and 3 more actions. i	<input type="checkbox"/> Any in this account
Add ARN to restrict access		

- In the **Add ARN(s)** box, mention the name of your first bucket and check mark **Any** right to the **Object name**. This will make this custom policy applied to all the objects of this very S3 bucket. Click **Add** after entering the required parameters.

Add ARN(s) ×

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. [Learn more](#)

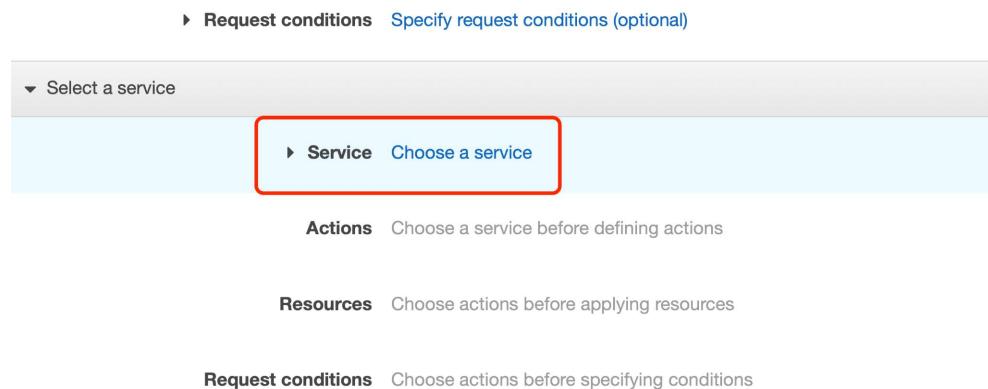
Specify ARN for object	List ARNs manually						
<input type="text" value="arn:aws:s3:::demo-s3-bucket-iampolicy-one/*"/>							
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; padding: 5px;">Bucket name *</td> <td style="width: 40%; padding: 5px; border: none;">demo-s3-bucket-iampolicy-</td> <td style="width: 30%; padding: 5px; text-align: center;"><input type="checkbox"/> Any</td> </tr> <tr> <td style="padding: 5px;">Object name *</td> <td style="padding: 5px; border: none;">*</td> <td style="padding: 5px; text-align: center;"><input checked="" type="checkbox"/> Any</td> </tr> </table>		Bucket name *	demo-s3-bucket-iampolicy-	<input type="checkbox"/> Any	Object name *	*	<input checked="" type="checkbox"/> Any
Bucket name *	demo-s3-bucket-iampolicy-	<input type="checkbox"/> Any					
Object name *	*	<input checked="" type="checkbox"/> Any					
Cancel Add							

- You will get back to the Create Policy page. Now, you will be adding more permissions for the second bucket.

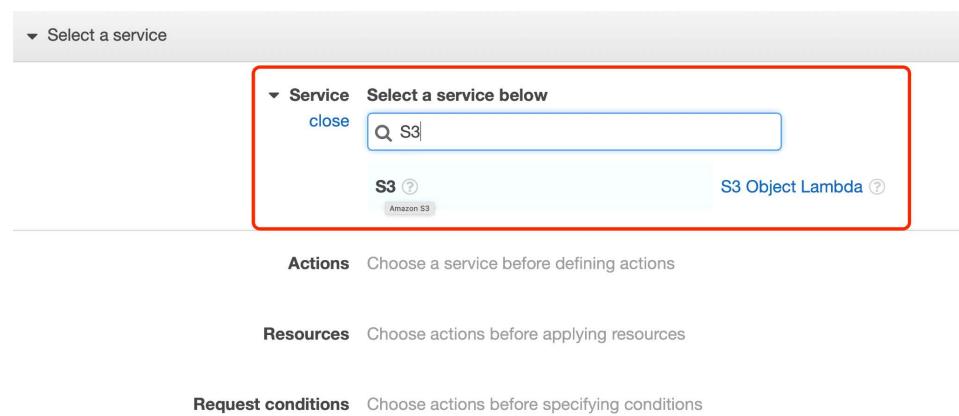
Scroll down to the bottom of this page and click **Add additional permissions**.

object	arn:aws:s3:::demo-s3-bucket-iampolicy-one/*	EDIT ✖ <input type="checkbox"/> A
Add ARN to restrict access		
objectlambdaaccesspoint resource ARN for the GetAccessPointPolicyForObjectLambda and 3 more actions. ⓘ Add ARN to restrict access		
storagelensconfiguration resource ARN for the GetStorageLensDashboard and 2 more actions. ⓘ Add ARN to restrict access		
▶ Request conditions Specify request conditions (optional)		
Add additional permission		

- Click **Choose a service** within the ‘Select a service’ section.



- Type the keyword 'S3' in the search menu bar and click **S3**.



- Select **All S3 actions (s3:*)** within Manual actions. This will ensure that full access to the second S3 bucket is allowed.

► Service S3

▼ Actions Specify the actions allowed in S3 [?](#)

[close](#)

Manual actions (add actions)

All S3 actions (s3:*)

Access level

- List (10 selected)
- Read (50 selected)
- Tagging (10 selected)
- Write (40 selected)
- Permissions management (15 selected)

Action warnings [?](#)

- s3:CreateJob action requires **1 more action** to provide full permissions
- s3:PutReplicationConfiguration action requires **1 more action** to provide full permissions

- Go to **Resources** underneath, click and expand to view all available options.

▼ S3 (All actions) [▲ 8 warnings](#) [Clone](#) [Remove](#)

► Service S3

► Actions Manual actions *

► Resources Specify accesspoint resource ARN for the **GetAccessPointPolicy** and 5 more actions. [?](#)
 Specify bucket resource ARN for the **GetBucketLocation** and 48 more actions. [?](#)
 Specify job resource ARN for the **DescribeJob** and 5 more actions. [?](#)
 Specify multiregionaccesspoint resource ARN for the **CreateMultiRegionAccessPoint** and 5 more actions. [?](#)
 Specify multiregionaccesspointrequestarn resource ARN for the **DescribeMultiRegionAccessPointOperation** action.
 Specify object resource ARN for the **PutObjectRetention** and 29 more actions. [?](#)
 Specify objectlambdaaccesspoint resource ARN for the **PutAccessPointConfigurationForObjectLambda** and 8 more actions. [?](#)
 Specify storagelensconfiguration resource ARN for the **DeleteStorageLensConfiguration** and 5 more actions. [?](#)

► Request conditions Specify request conditions (optional)

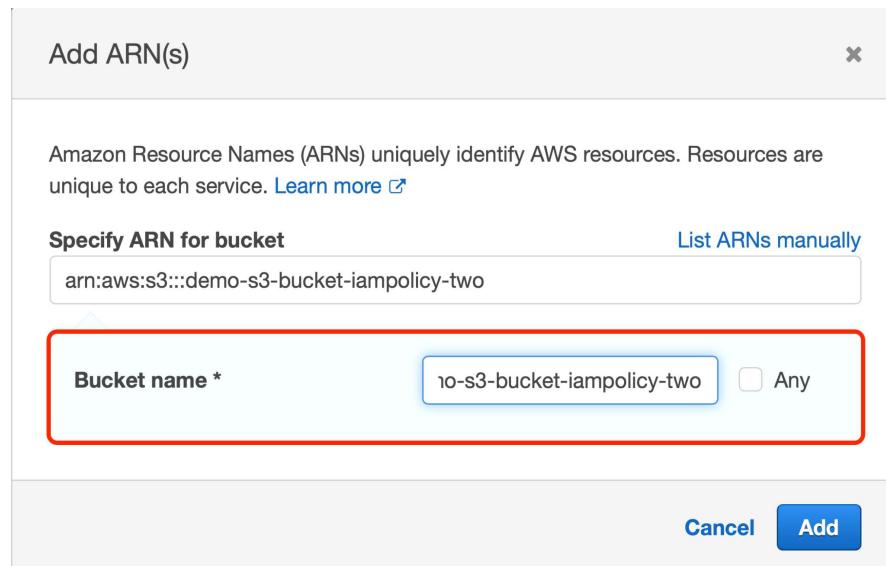
- Click **Add ARN** in the **bucket** resource section.

▼ Resources Specific [close](#) All resources

accesspoint ?	Specify accesspoint resource ARN for the GetAccessPointPolicy and 5 more actions. ? Add ARN to restrict access	<input type="checkbox"/> Any in this account
bucket ?	Specify bucket resource ARN for the GetBucketLocation and 48 more actions. ? Add ARN to restrict access	<input type="checkbox"/> Any
job ?	Specify job resource ARN for the DescribeJob and 5 more actions. ? Add ARN to restrict access	<input type="checkbox"/> Any in this account
multiregionacces... ?	Specify multiregionaccesspoint resource ARN for the CreateMultiRegionAccessPoint and 5 more actions. ? Add ARN to restrict access	<input type="checkbox"/> Any in this account
multiregionacces... ?	Specify multiregionaccesspointrequestarn resource ARN for the DescribeMultiRegionAccessPointOperation action. Add ARN to restrict access	<input type="checkbox"/> Any in this account
object ?	Specify object resource ARN for the PutObjectRetention and 29 more actions. ? Add ARN to restrict access	<input type="checkbox"/> Any

- Mention the name of the second S3 bucket in the **Bucket name** field.

Please note that this will automatically fill in the ARN for this bucket in **Specify ARN for bucket** field. Click **Add**.



The screenshot shows a modal dialog titled "Add ARN(s)". Inside, there's a note about ARNs identifying AWS resources. Below it, there are two options: "Specify ARN for bucket" (selected) and "List ARNs manually". Under "Specify ARN for bucket", an ARN is listed: "arn:aws:s3:::demo-s3-bucket-iampolicy-two". A red box highlights the "Bucket name *" input field, which contains "1o-s3-bucket-iampolicy-two". To the right of this field is a checkbox labeled "Any" and an unchecked checkbox. At the bottom of the dialog are "Cancel" and "Add" buttons.

- You will then get back to the Create Policy page. Search for object resource type and click **Add ARN**.

The screenshot shows the AWS IAM Policy editor interface. A policy document is being edited, containing the following resources and their permissions:

- bucket**: ARN: arn:aws:s3:::demo-s3-bucket-iampolicy-two. Permissions: Any.
- job**: Specify job resource ARN for the **DescribeJob** and 5 more actions. Permissions: Any in this account.
- multiregionaccesspoint**: Specify multiregionaccesspoint resource ARN for the **CreateMultiRegionAccessPoint** and 5 more actions. Permissions: Any in this account.
- multiregionaccesspointrequestarn**: Specify multiregionaccesspointrequestarn resource ARN for the **DescribeMultiRegionAccessPointOperation** action. Permissions: Any in this account.
- object**: Specify object resource ARN for the **PutObjectRetention** and 29 more actions. Permissions: Any. This row is highlighted with a red box.
- objectlambdaaccesspoint**: Specify objectlambdaaccesspoint resource ARN for the **PutAccessPointConfigurationForObjectLambda** and 8 more actions. Permissions: Any in this account.
- storagelensconfiguration**: Specify storagelensconfiguration resource ARN for the **DeleteStorageLensConfiguration** and 5 more actions. Permissions: Any in this account.

- Specify the name of the second bucket and select **Any** beside the Object name. This will ensure that this policy is applied to all the objects of this very S3 bucket.

The screenshot shows the "Add ARN(s)" dialog box. It includes the following fields:

- Specify ARN for object**: arn:aws:s3:::demo-s3-bucket-policy-two/*
- Bucket name ***: demo-s3-bucket-policy-two. Permissions: Any.
- Object name ***: *. Permissions: Any. This row is highlighted with a red box.

At the bottom right of the dialog are **Cancel** and **Add** buttons.

- As the permissions for S3 buckets are added successfully, click **Next: Tags**.

The screenshot shows the AWS IAM Policy Editor interface. A complex policy document is displayed, containing several conditions and ARN inputs. Key sections include:

- object**: ARN: arn:aws:s3:::demo-s3-bucket-policy-two/*
- objectlambdaacc...**: Specify objectlambdaaccesspoint resource ARN for the PutAccessPointConfigurationForObjectLambda and 8 more actions.
- storagelensconfi...**: Specify storagelensconfiguration resource ARN for the DeleteStorageLensConfiguration and 5 more actions.

Below the policy editor, there are tabs for "Request conditions" and "Specify request conditions (optional)". At the bottom right, there is a link to "Add additional permissions".

Add additional permissions

Character count: 1,735 of 6,144.

Cancel

Next: Tags

- Adding a tag to this policy is optional. Hence, you may skip this step and click **Next: Review**.

Create policy

1 2 3

Add tags (Optional)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add tag

You can add up to 50 more tags

Cancel

Previous

Next: Review

- Assign a name to this policy and a description (optional).

Create policy

1 2 3

Review policy

Name* CustomS3IAMPolicy
Use alphanumeric and '+=_@-' characters. Maximum 128 characters.

Description This custom policy provides read only access to our first S3 bucket and full access to the second one.
Maximum 1000 characters. Use alphanumeric and '+=_@-' characters.

Summary 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](#)

Service	Access level	Resource	Request condition
S3	Full: List Limited: Read, Write, Permissions management, Tagging	Multiple	None

- Scroll down and click **Create Policy** to finish this process.

Tags

Key	Value
No tags associated with the resource.	

Cancel Previous Create policy

Step 3: Create an IAM user while attaching the custom IAM policy to it

In this step, we will create an IAM user and attach the custom IAM policy we've created beforehand.

- Click **Users** on the navigation pane located on the left side of the IAM dashboard.

The policy **CustomS3IAMPolicy** has been created.

Policies (959) Info

A policy is an object in AWS that defines permissions.

Policy name	Type	Actions
AWSCodePipelineServiceRole-ap-south-1-nodejsapppipeline	Customer managed	Permi...

- Click **Add users** on the right-hand corner of the web page.

Add users

- Assign any name to this dummy user and enable password option to access AWS Management Console.

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*	chris
+ Add another user	

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*	<input type="checkbox"/> Access key - Programmatic access
	Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.
<input checked="" type="checkbox"/> Password - AWS Management Console access	Enables a password that allows users to sign-in to the AWS Management Console.

- Set a custom console password for this user and uncheck the **Require password reset** option. Click **Next: Permissions**.

Console password* Autogenerated password Custom password

***** Show password

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

* Required Cancel **Next: Permissions**

- Choose **Attach existing policies directly** under 'Set permissions', type the policy name in 'Filter policies' search bar, select it and click **Next: Tags** to proceed.

▼ Set permissions

Add user to group Copy permissions from existing user **Attach existing policies directly**

Create policy

Filter policies ▾

	Policy name ▾	Type	Used as
<input checked="" type="checkbox"/>	CustomS3IAMPolicy	Customer managed	None

Showing 1 result

▶ Set permissions boundary

Cancel Previous **Next: Tags**

- Attaching a tag to a user is an optional parameter. Skip this step and click **Next: Review**.

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

[Cancel](#) [Previous](#) [Next: Review](#)

- On the Review page, click **Create user** to complete this very step.

Review

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

User details

User name	chris
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

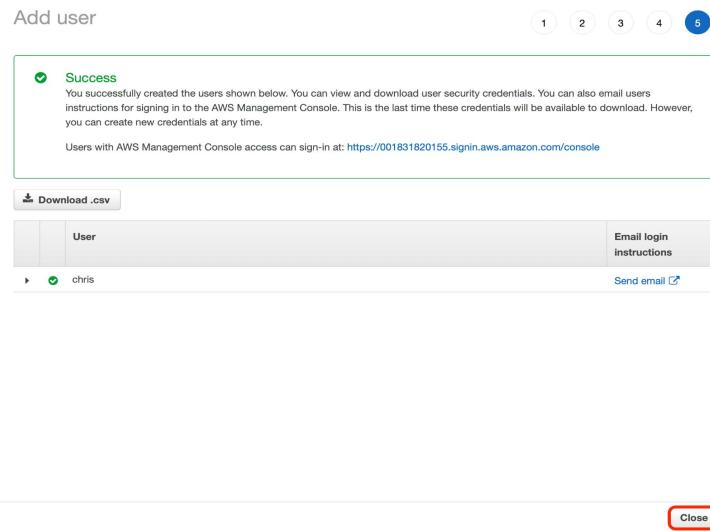
Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	CustomS3IAMPolicy

[Cancel](#) [Previous](#) [Create user](#)

- This creates a new IAM user for us to test. Click **Close** to exit.



Step 4: Test user access

- Since we need to test how this IAM user can access S3 buckets using the custom IAM policy attached to it, click **Dashboard** on the left side within navigation menu options.

The screenshot shows the AWS IAM Dashboard. On the left, a navigation sidebar lists 'Identity and Access Management (IAM)' with 'Dashboard' selected. Other options include 'Access management', 'Users' (which is currently selected), 'Policies', 'Identity providers', and 'Account settings'. Under 'Access reports', there are 'Access analyzer', 'Analyzers', 'Settings', 'Credential report', 'Organization activity', and 'Service control policies (SCPs)'. The main pane displays a confirmation message: 'The user chris have been created.' Below this, the 'Users (1) Info' section shows a table with one row for 'chris'. The table columns are 'User name', 'Groups', 'Last activity', 'MFA', 'Password age', and 'Active key age'. The 'User name' column shows 'chris', 'Groups' shows 'None', 'Last activity' shows 'Never', 'MFA' shows 'None', 'Password age' shows '3 minutes ago', and 'Active key age' shows '-'. There are 'Delete' and 'Add users' buttons at the top of the table.

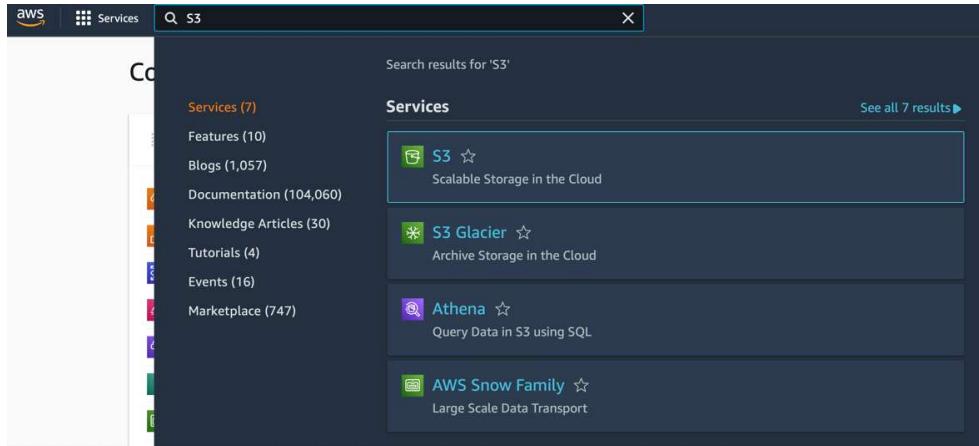
- On the Dashboard, copy the **Sign-in URL for IAM users in this account**.

The screenshot shows the AWS Identity and Access Management (IAM) dashboard. On the left, there's a sidebar with navigation links like 'Access management', 'Access reports', and 'AWS CloudTrail'. The main area has a header 'Introducing the new IAM dashboard experience' with a note: 'We've redesigned the IAM dashboard experience to make it easier to use. Let us know what you think.' Below this is the 'IAM dashboard' section with 'Security recommendations' (including 'Add MFA for root user' and 'Deactivate or delete access keys for root user'), 'IAM resources' (User groups: 2, Users: 1, Roles: 79, Policies: 44, Identity providers: 0), and a 'What's new' section with recent updates from the IAM Access Analyzer and AWS Amplify.

- Access this very link via a different browser and put in IAM username and password. Click **Sign in** to get access to AWS Management Console.

The left screenshot shows the 'Sign in as IAM user' page. It has fields for 'Account ID (12 digits) or account alias' (containing '001831820155'), 'IAM user name' (containing 'chris'), 'Password' (redacted), and a 'Remember this account' checkbox. A 'Sign in' button is at the bottom. Below the form are links for 'Sign in using root user email' and 'Forgot password?'. The right screenshot shows the 'Amazon Lightsail' landing page with the tagline 'Lightsail is the easiest way to get started on AWS' and a 'Learn more »' button.

- Search for **S3** via the search menu bar provided at the top of this web page and click S3 within the Services list.

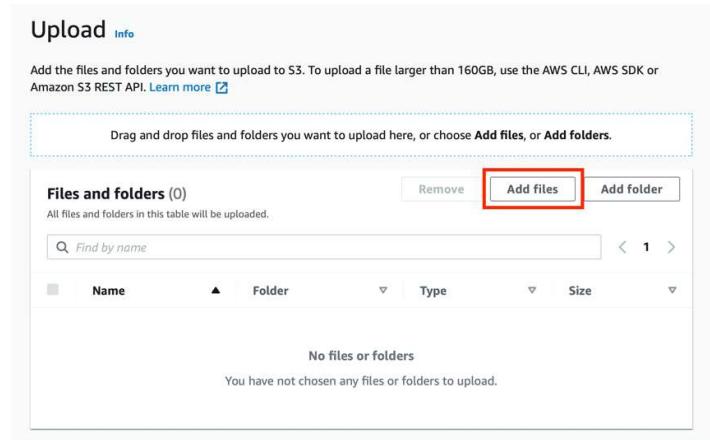


- Once you land on the S3 dashboard, search for the S3 buckets created before.

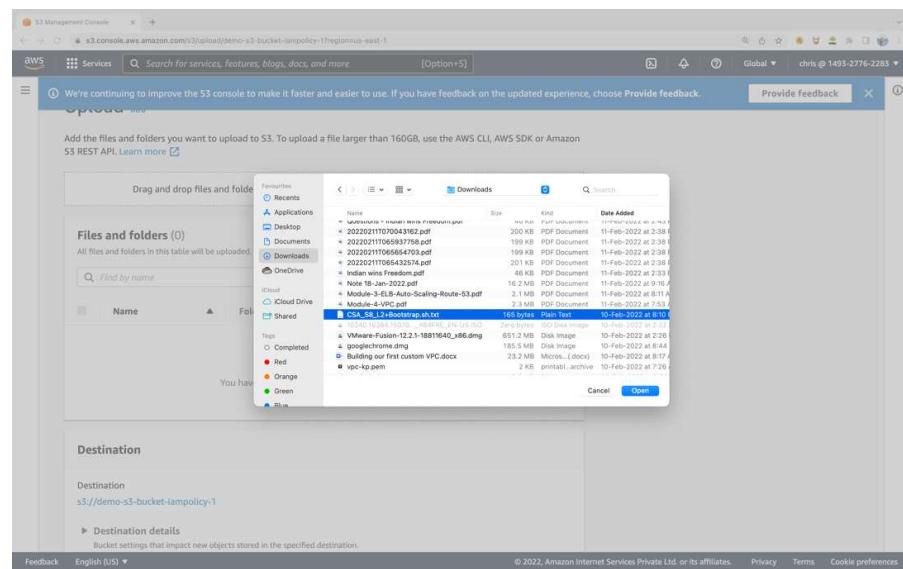
Name	AWS Region	Access	Creation date
demo-s3-bucket-iampolicy-one	US East (N. Virginia) us-east-1	Bucket and objects not public	December 24, 2021, 12:18:50 (UTC+05:30)
demo-s3-bucket-iampolicy-two	US East (N. Virginia) us-east-1	Bucket and objects not public	December 24, 2021, 12:36:07 (UTC+05:30)

- Click and go to the first S3 bucket (which IAM user should have read-only access to) and click any of the available **Upload** options.

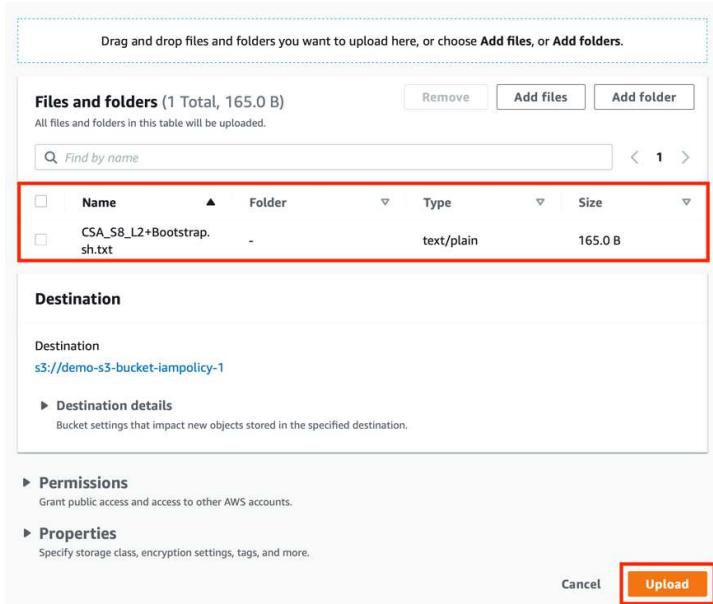
- Click **Add files**.



- Select and upload any of the available documents or images stored on your local computer.



- Once the file is selected, click **Upload**.

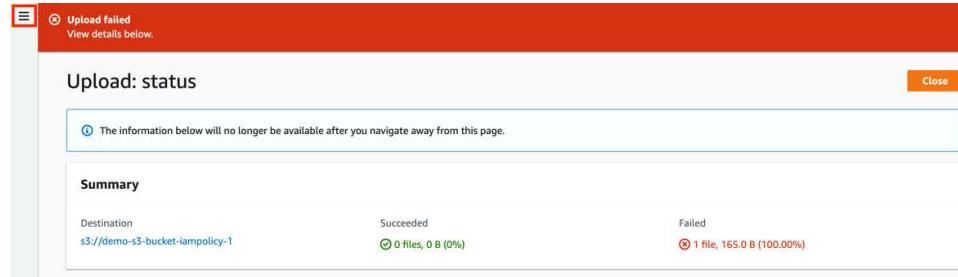


- As expected, the IAM user should be denied access from uploading or writing any object to this S3 bucket.

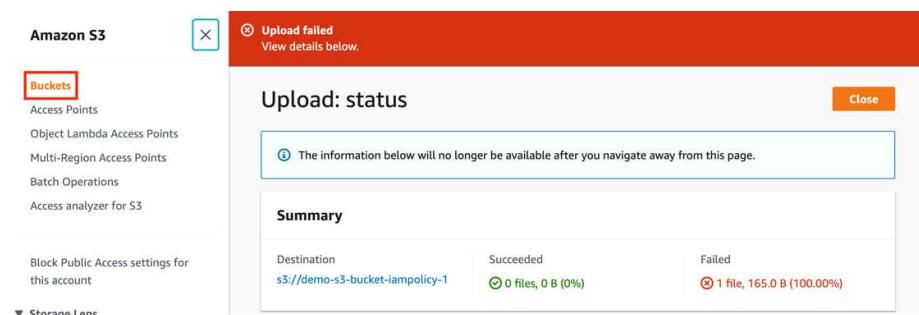
Name	Type	Size	Status	Error
CSA_S8_L2+Bootstrap.sh.txt	text/plain	165.0 B	Failed	Access Denied

Now, you need to perform the same operation with the second S3 bucket.

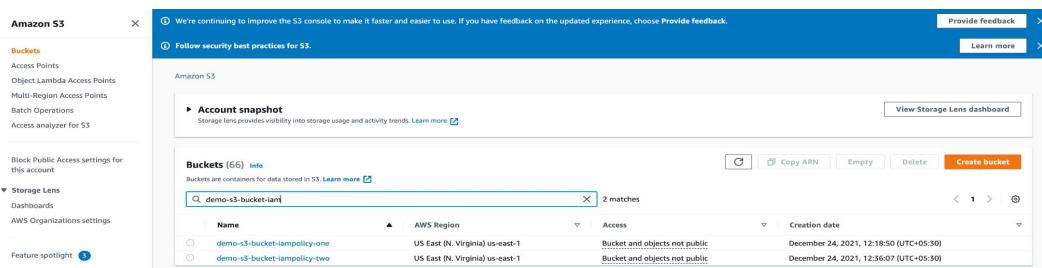
- Click on three vertical lines on the left side of the page.



- Choose **Buckets** to access the list of S3 buckets.



- Search for and go to the second S3 bucket (which IAM user should have full access to).



- Perform steps 14-17 for the second S3 bucket. Consequently, the upload will be successful.

The screenshot shows the AWS S3 'Upload: status' page. At the top, a green header bar displays the message 'Upload succeeded' and 'View details below.' Below this, the main title 'Upload: status' is centered. A note in a box states: 'The information below will no longer be available after you navigate away from this page.' The 'Summary' section provides details about the upload:

Destination	Succeeded	Failed
s3://demo-s3-bucket-iampolicy-2	1 file, 165.0 B (100.00%)	0 files, 0 B (0%)

Below the summary, there are two tabs: 'Files and folders' (selected) and 'Configuration'. The 'Files and folders' tab shows a single item in a table:

Name	Folder	Type	Size	Status	Error
CSA_58_L2>Bootstrap.sh.txt	-	text/plain	165.0 B	Succeeded	-