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

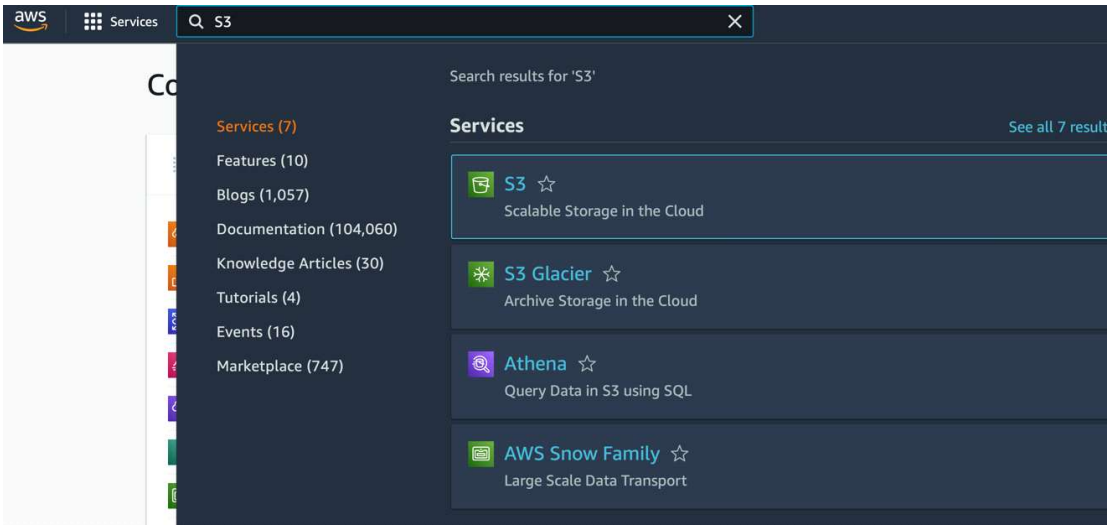
Step 1: Create two Amazon S3 buckets

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

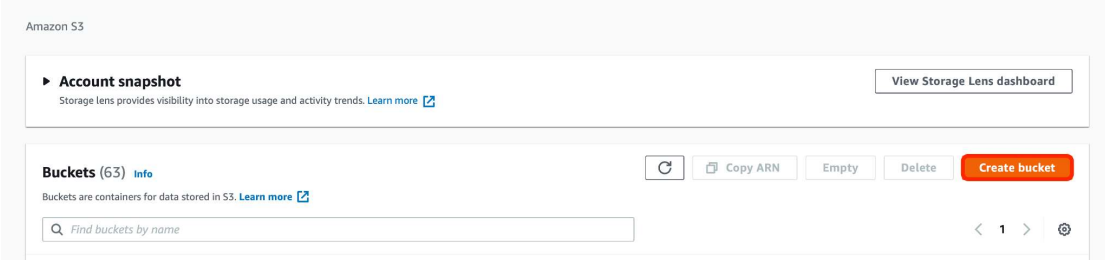
To create S3 buckets:

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

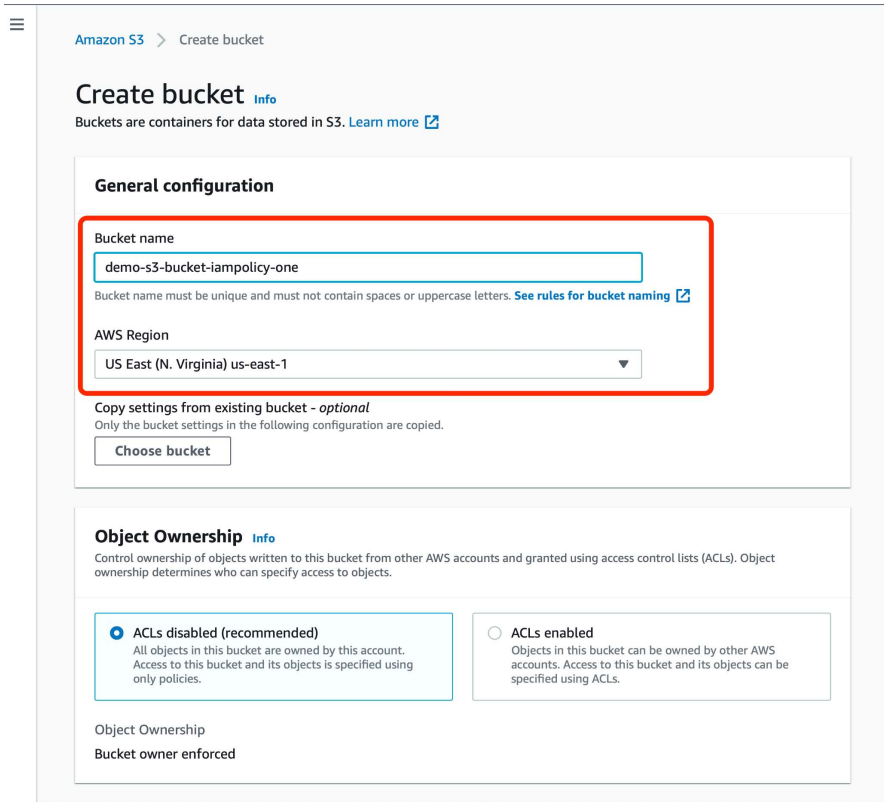
Once clicked, it will take you to the S3 dashboard.



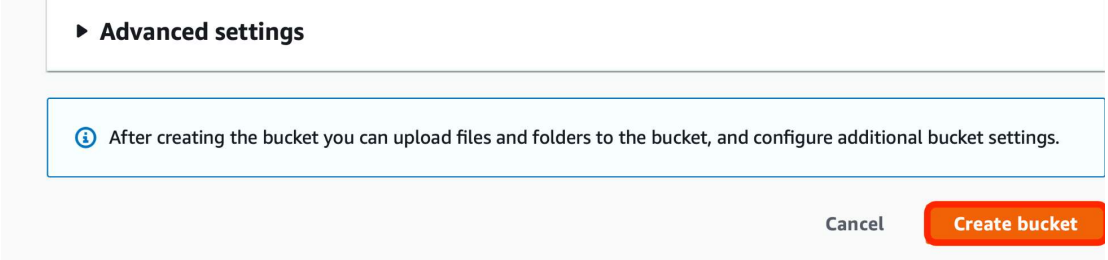
- Click **Create bucket** at top right corner of the page.



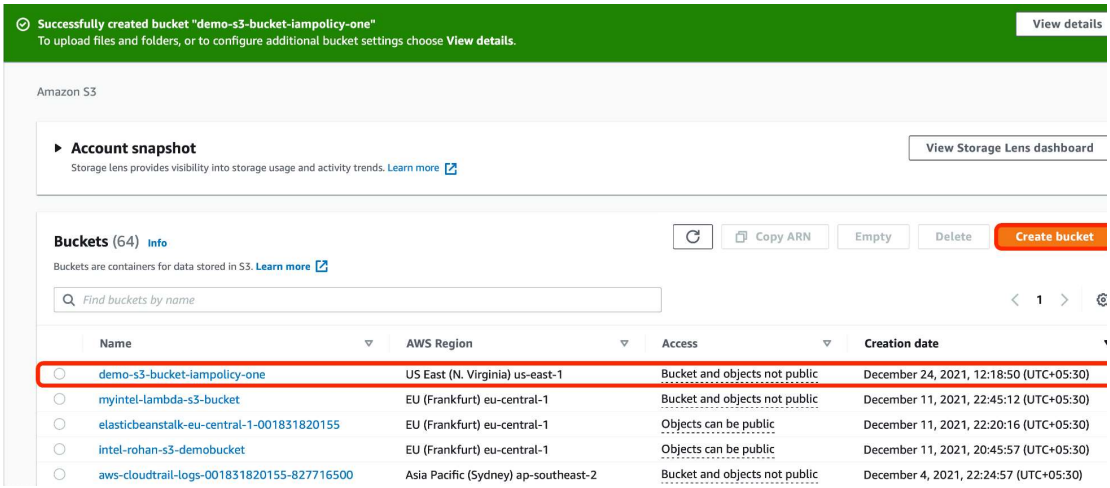
- Assign a name to this first S3 bucket while making sure that it should be unique, and choose any of the listed AWS regions.



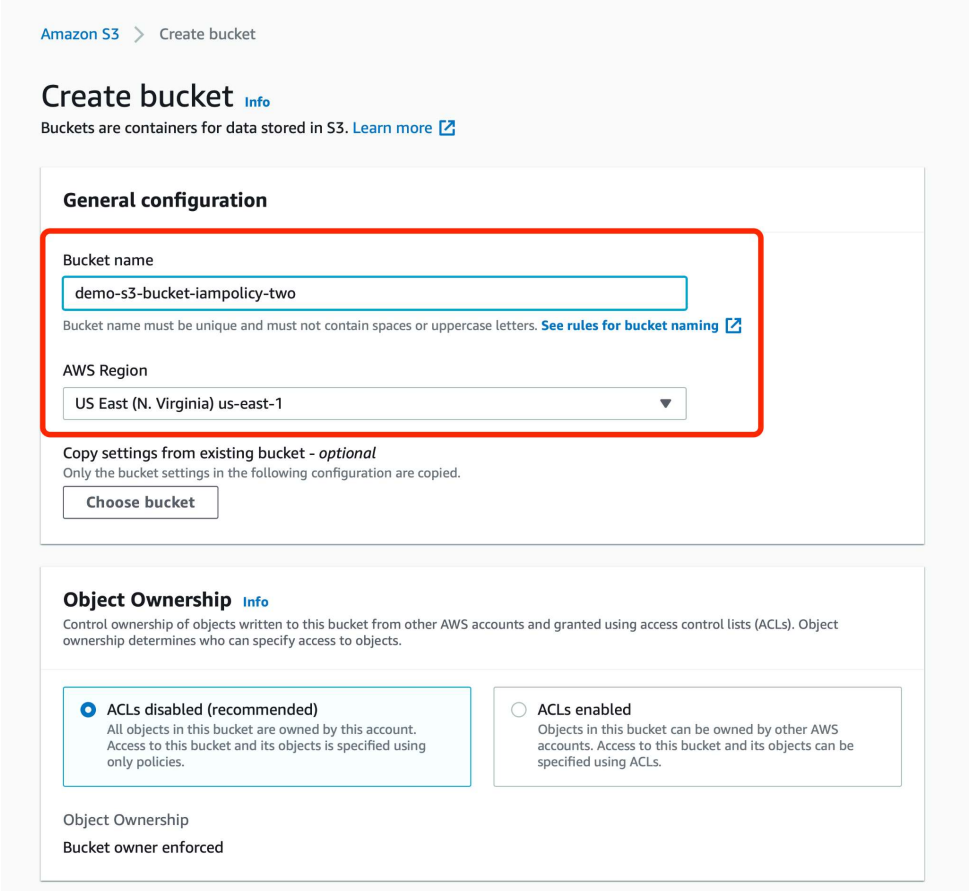
- Accept all other default values, scroll down, and click **Create bucket**.



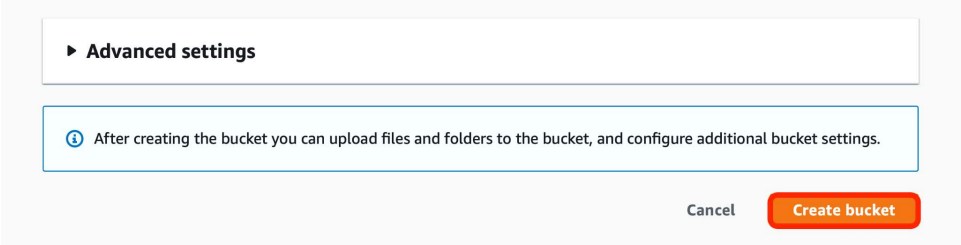
- Once again, you will land back to the **Buckets** dashboard. Click **Create Bucket** and start creating the second one.



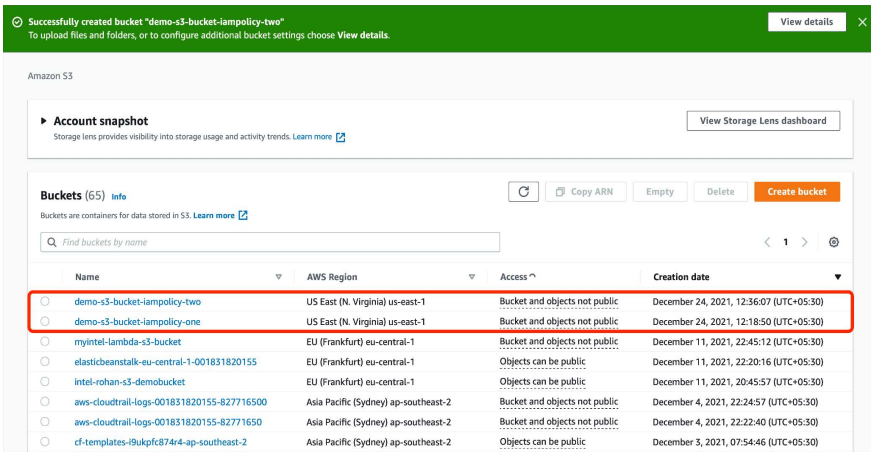
- Assign a unique name to this second S3 bucket, choose any of the listed AWS regions.



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



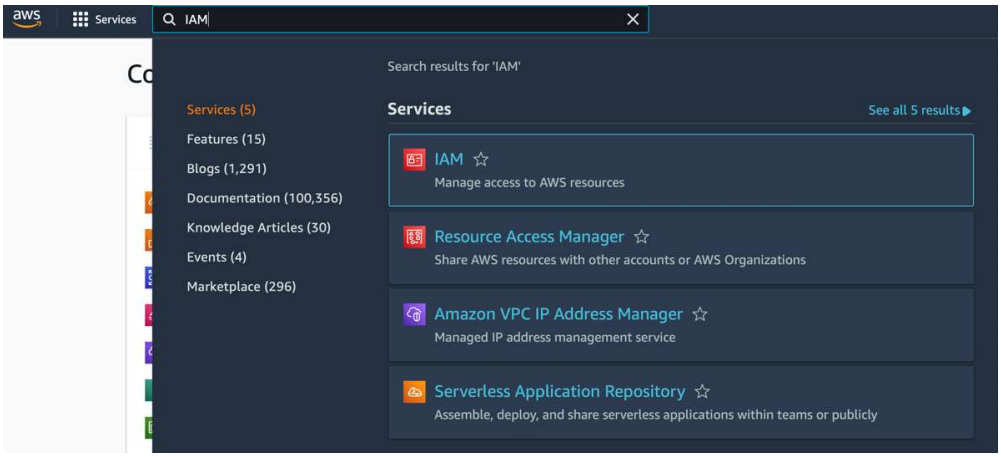
This leads to the completion of your first step where you've created two Amazon S3 buckets.



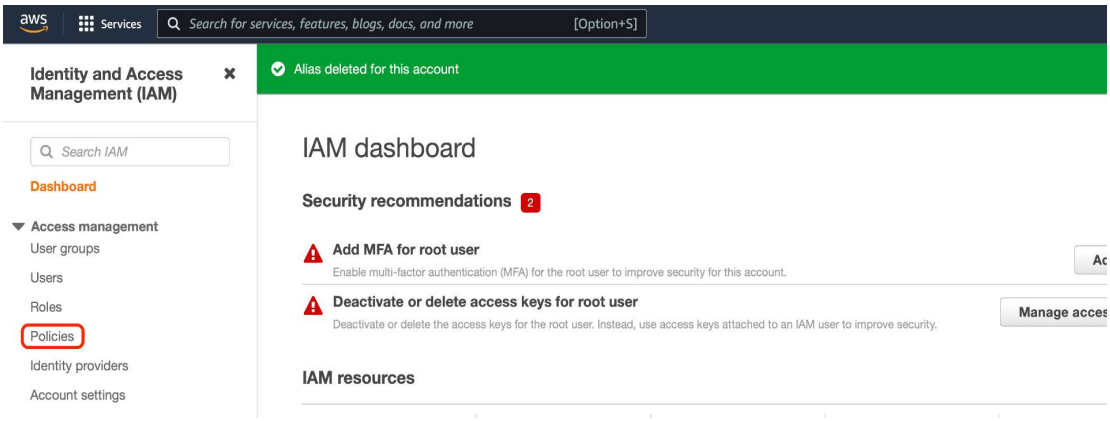
Step 2: Create a customer managed policy

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.

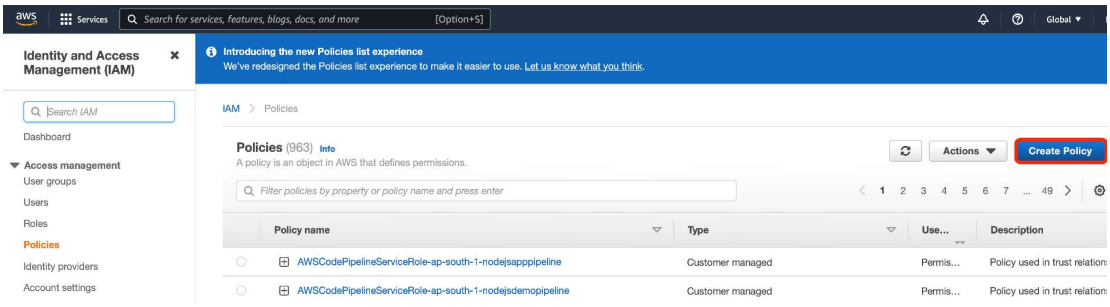
- Look for IAM service via the search bar provided at the top of the page and click it to get access to the IAM dashboard.



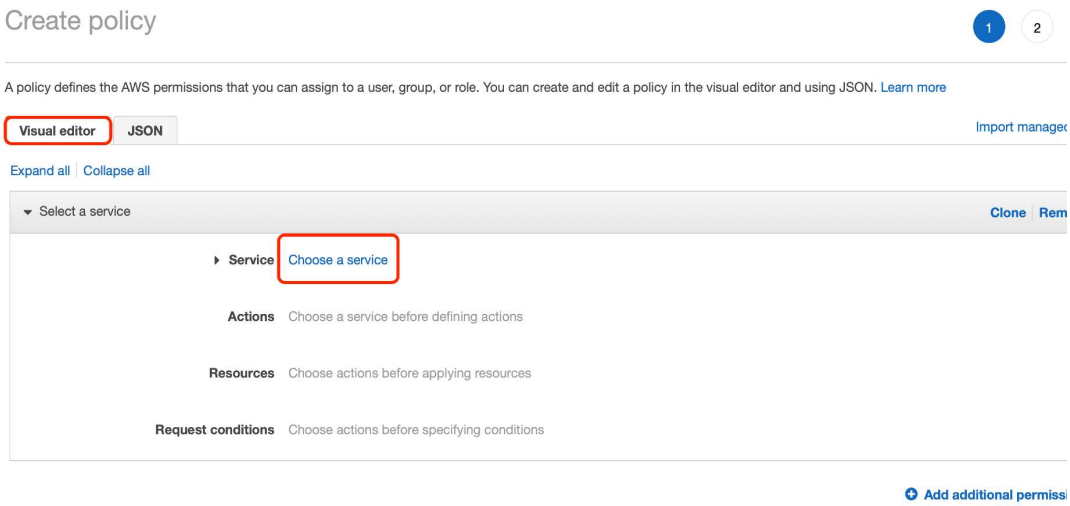
- Click **Policies** which is one of the navigation menu options located at the left side of the IAM dashboard.



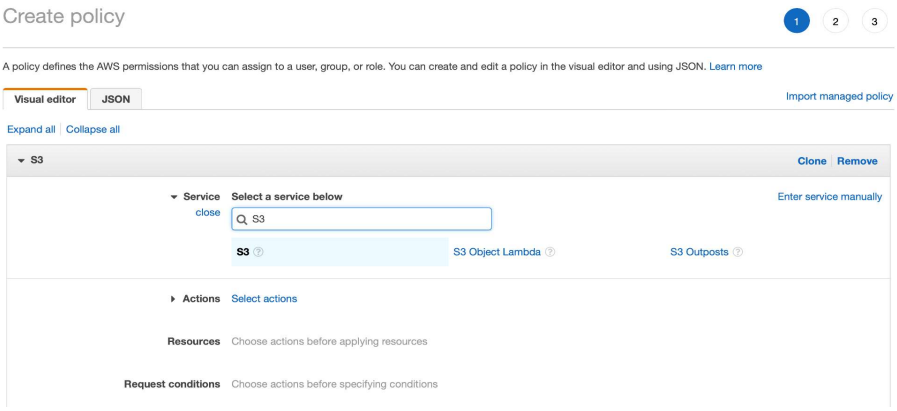
- Click **Create Policy** located at the right-hand corner of the Policies dashboard.



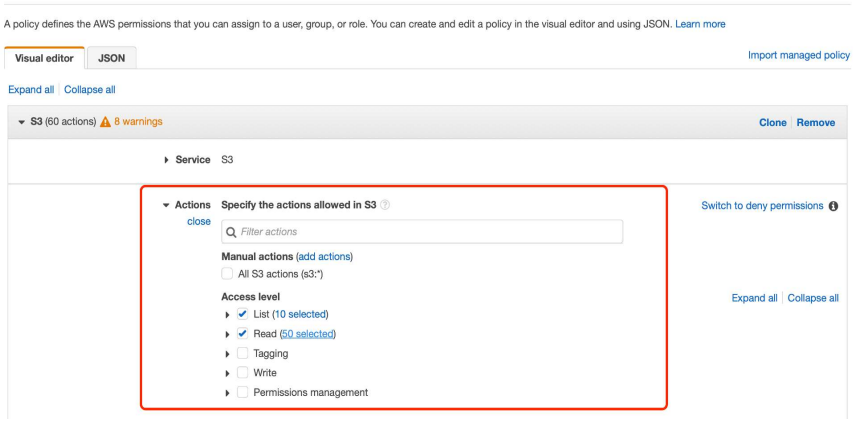
- For this demo, use **Visual editor** designed to select relevant options and produce a JSON policy as an output. Click **Choose a service** to get started.



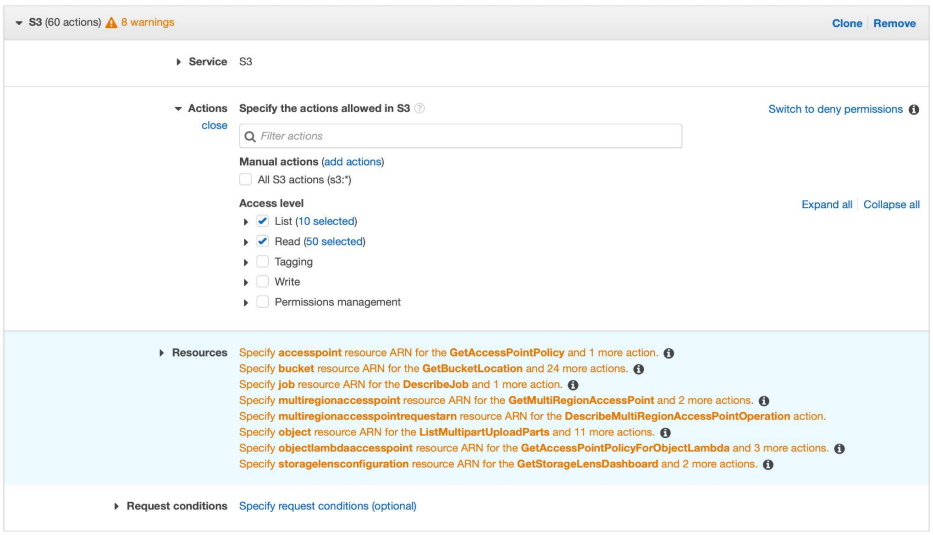
- Type ‘S3’ as a keyword and select S3.



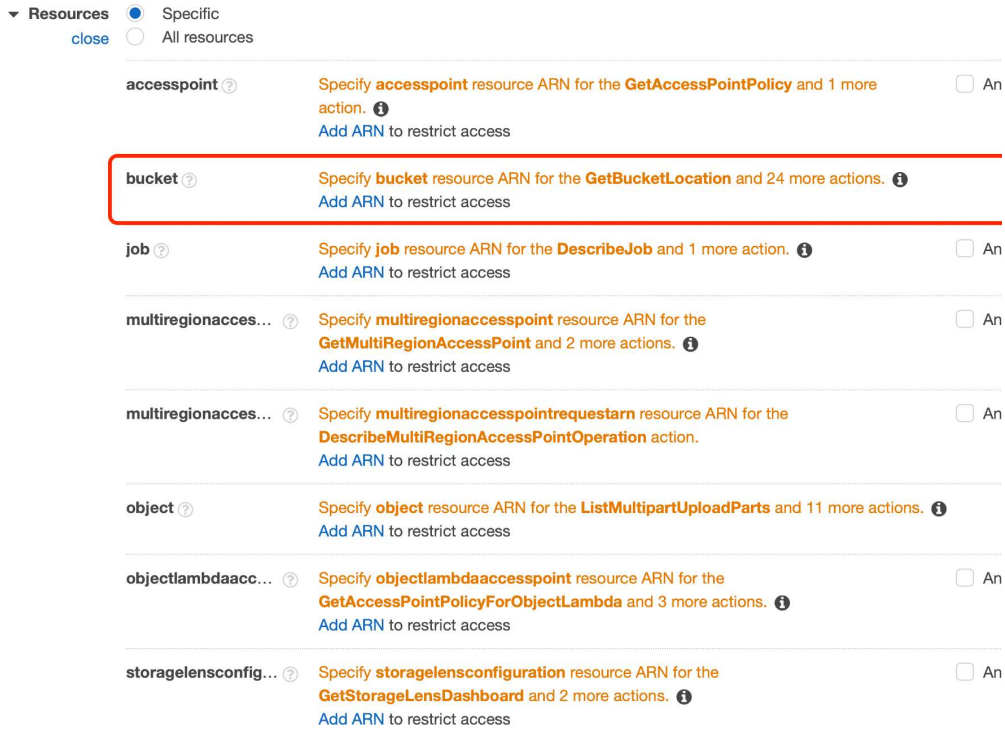
- Go to **Actions** and select **List** and **Read** actions within **Access Level**.



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



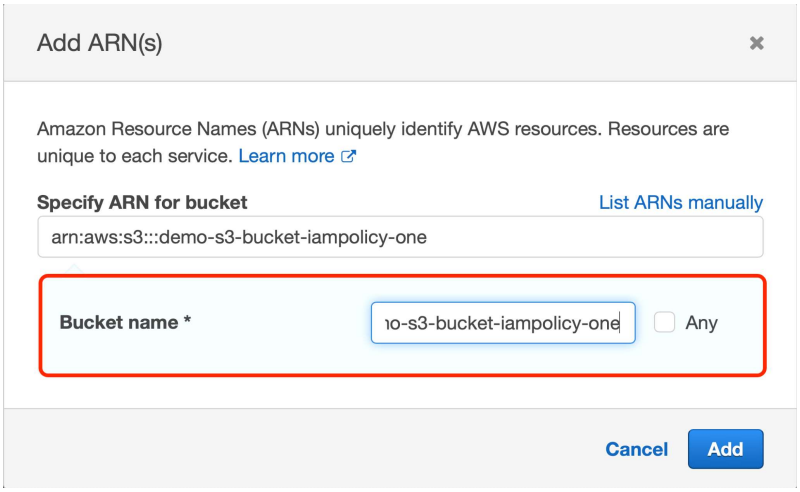
- Click **Add ARN** within the bucket resource section.



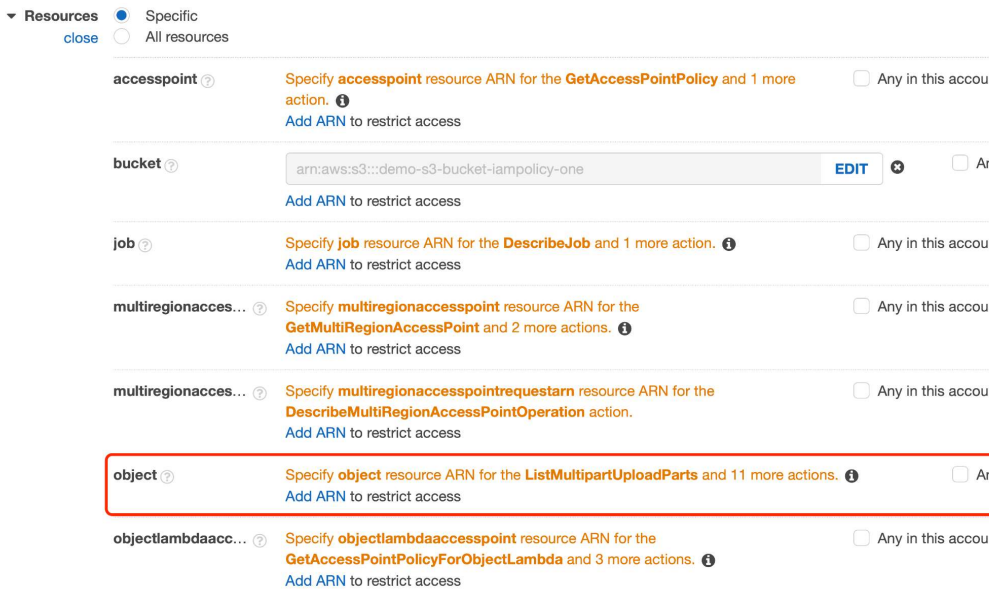
- Now, specify the name of the very first Amazon S3 bucket here. This will automatically specify the Amazon Resource Name (ARN) of this very bucket.

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

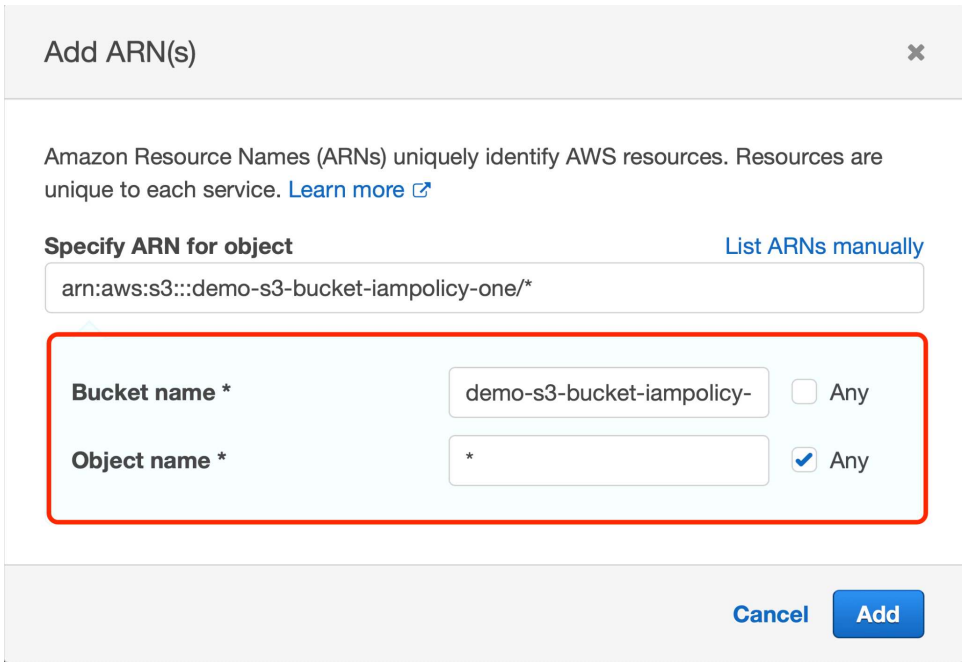
bucket field. Click **Add**.



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

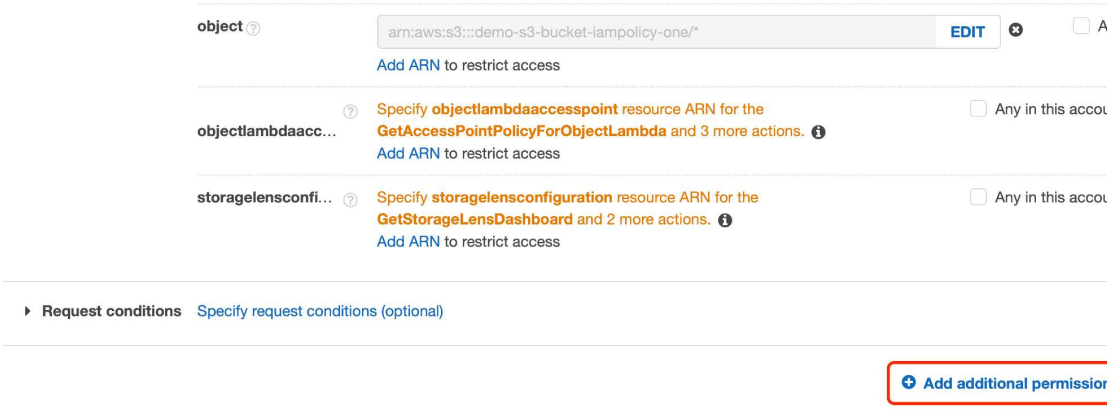


- In the **Add ARN(s)** box, mention the name of your first bucket and check mark **Any** right to the **Object name**. This will make this custom policy applied to all the objects of this very S3 bucket. Click **Add** after entering the required parameters.

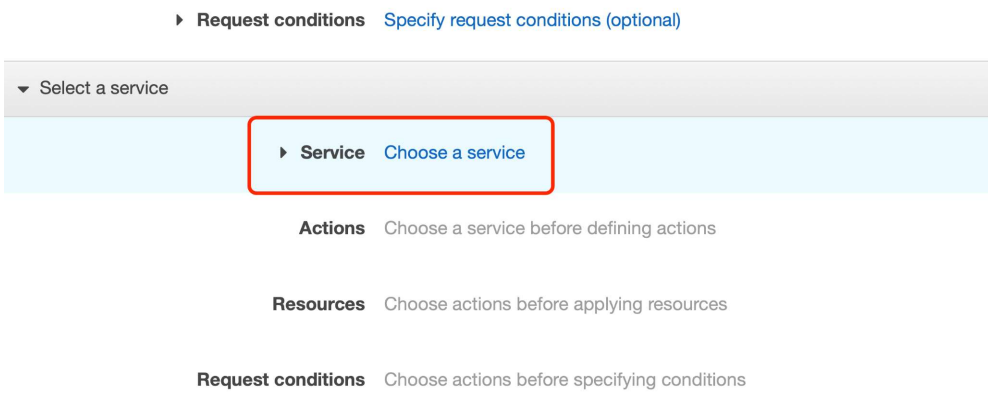


- You will get back to the Create Policy page. Now, you will be adding more permissions for the second bucket.

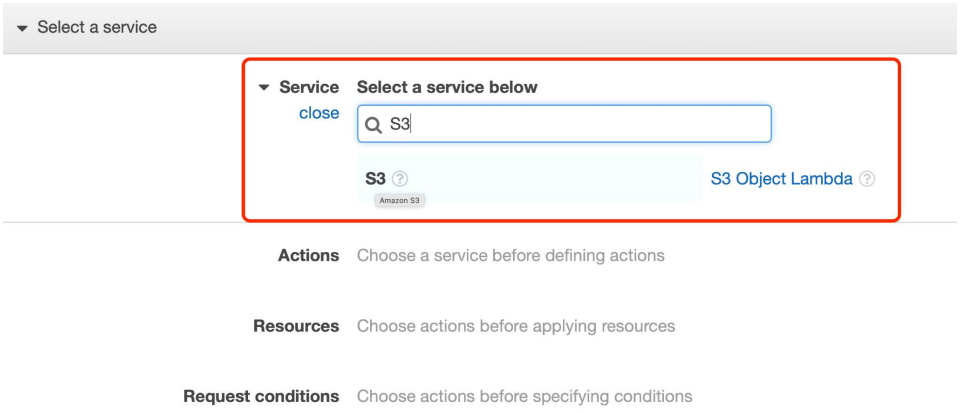
Scroll down to the bottom of this page and click **Add additional permissions**.



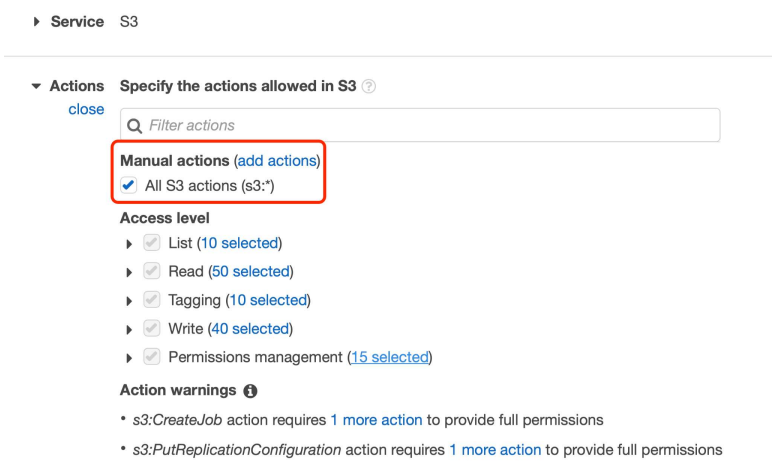
- Click **Choose a service** within the 'Select a service' section.



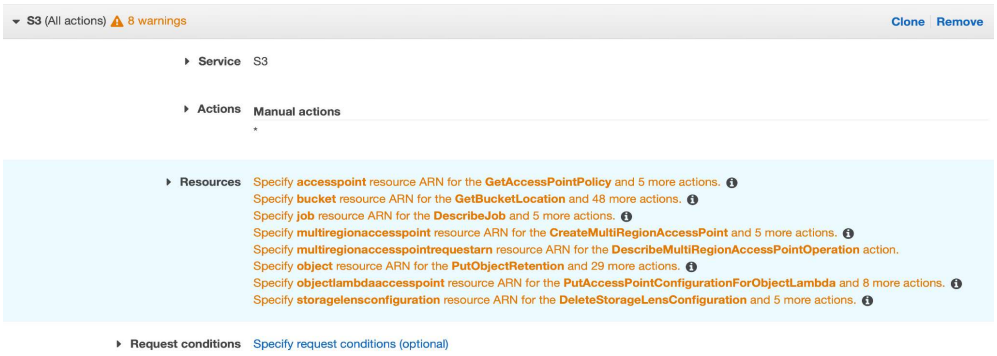
- Type the keyword ‘S3’ in the search menu bar and click **S3**.



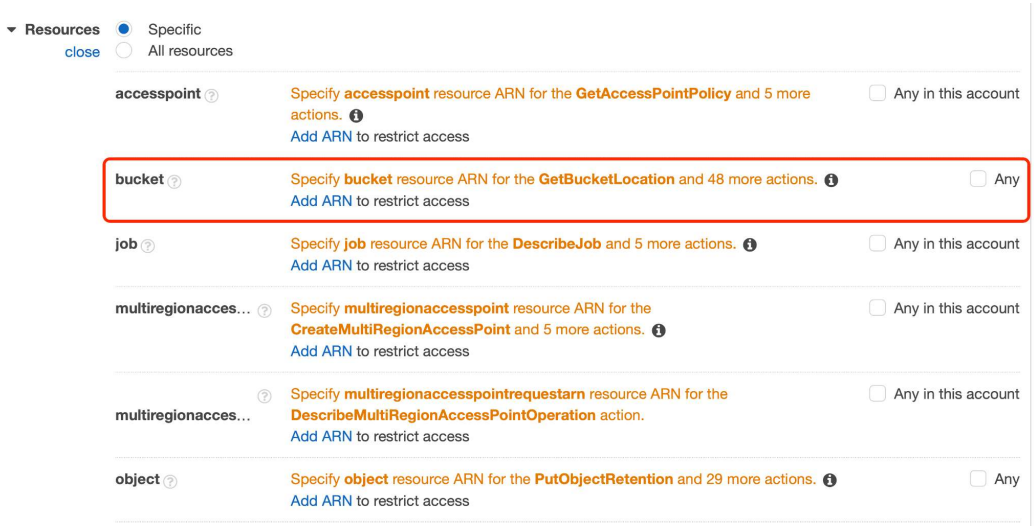
- Select **All S3 actions (s3:*)** within Manual actions. This will ensure that full access to the second S3 bucket is allowed.



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

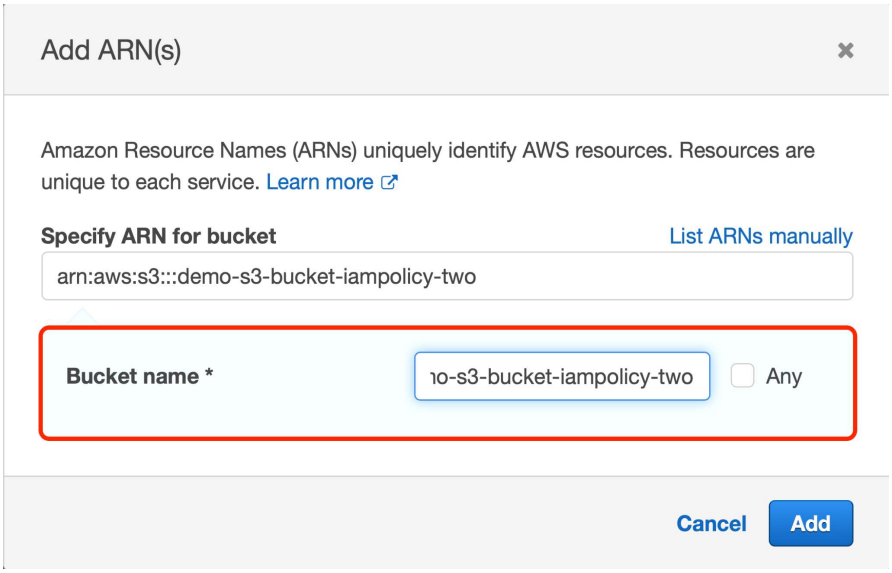


- Click **Add ARN** in the **bucket** resource section.

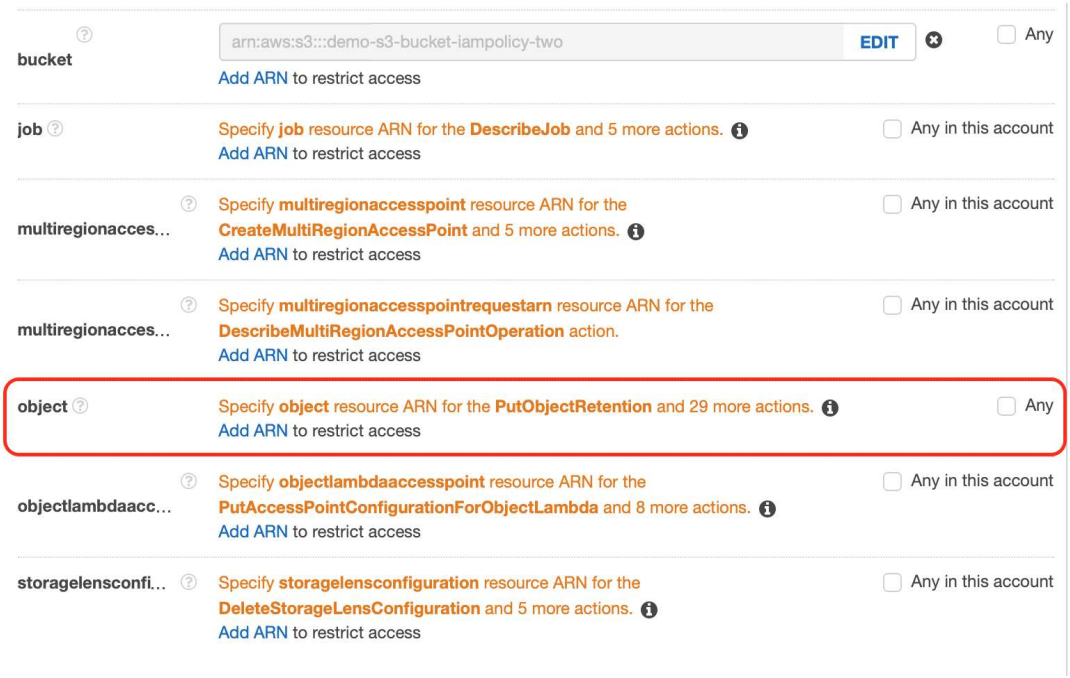


- Mention the name of the second S3 bucket in the **Bucket name** field.

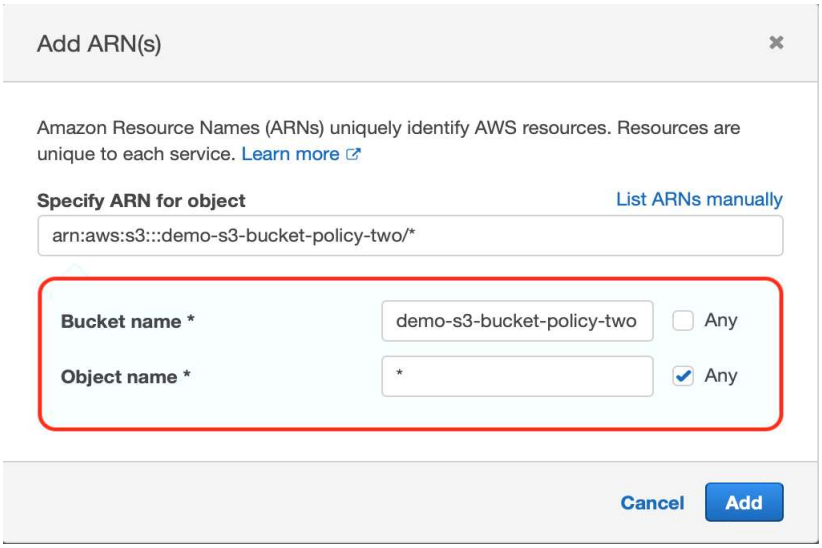
Please note that this will automatically fill in the ARN for this bucket in **Specify ARN for bucket** field. Click **Add**.



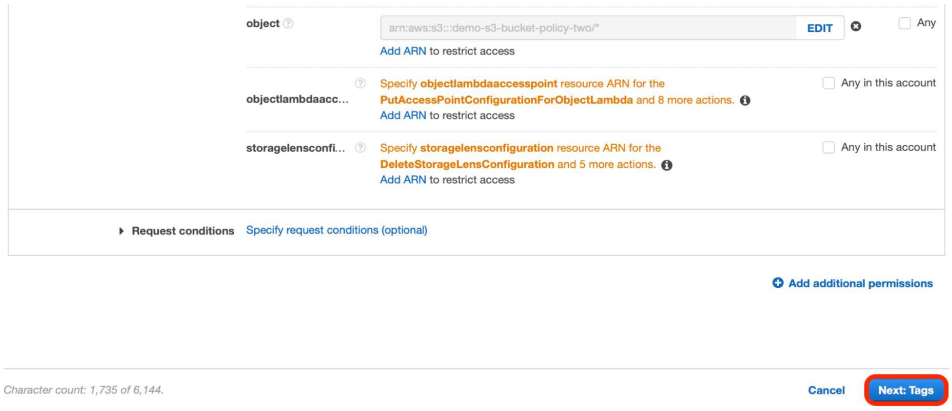
- You will then get back to the Create Policy page. Search for object resource type and click **Add ARN**.



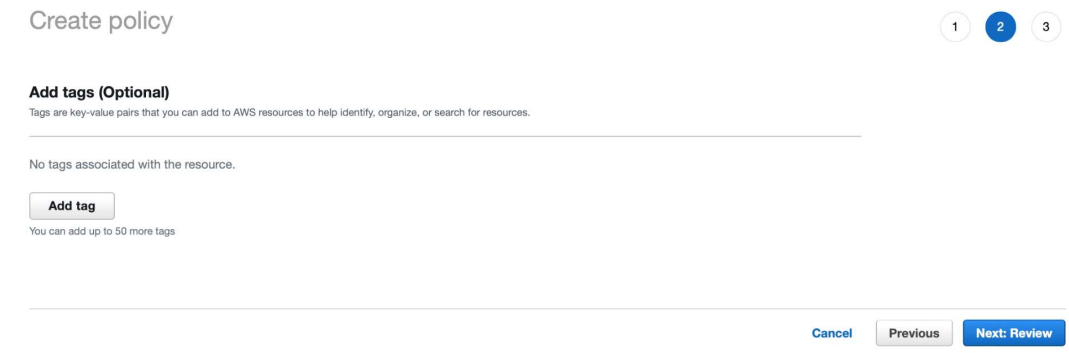
- Specify the name of the second bucket and select **Any** beside the Object name. This will ensure that this policy is applied to all the objects of this very S3 bucket.



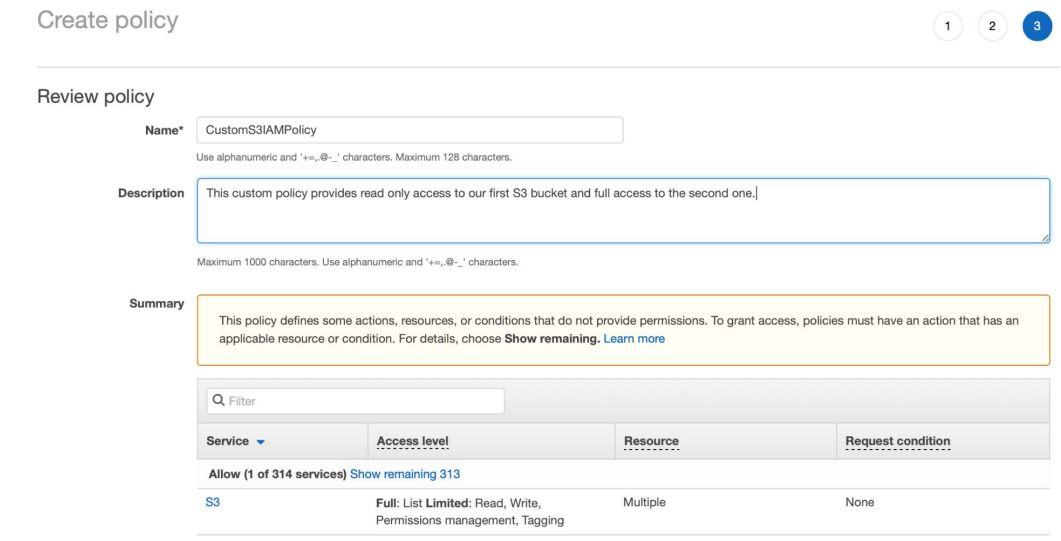
- As the permissions for S3 buckets are added successfully, click **Next: Tags**.



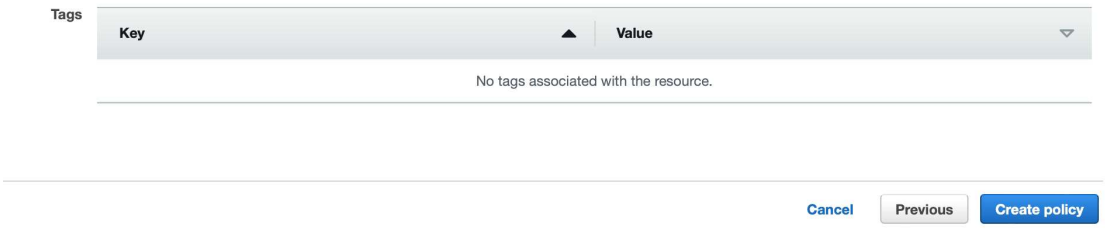
- Adding a tag to this policy is optional. Hence, you may skip this step and click **Next: Review**.



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



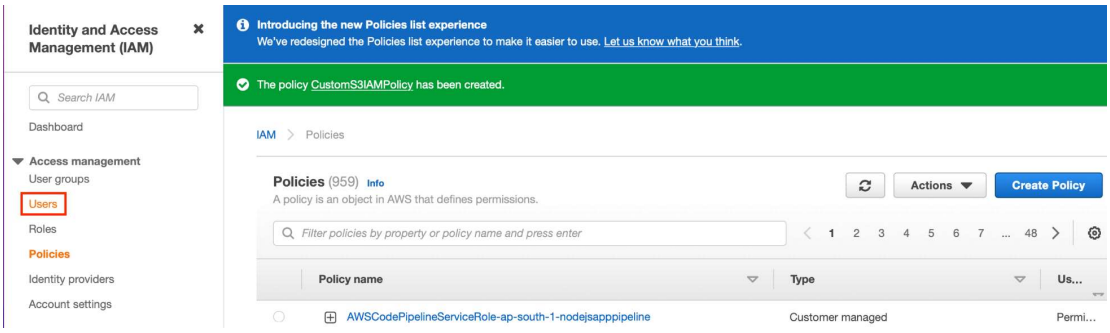
- Scroll down and click **Create Policy** to finish this process.



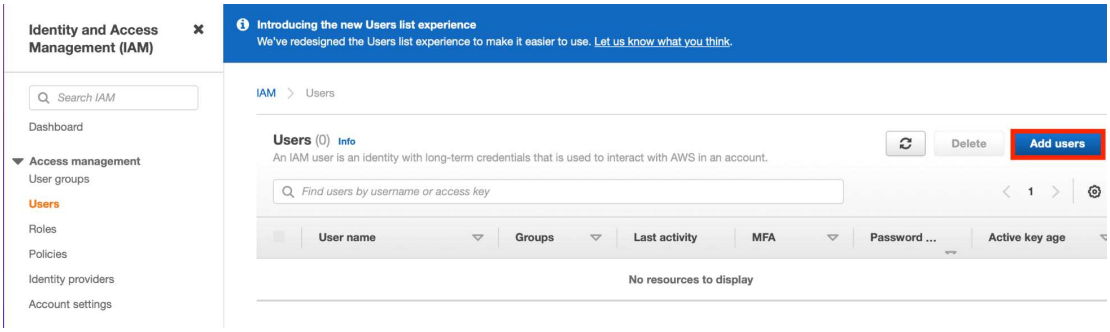
Step 3: Create an IAM user while attaching the custom IAM policy to it

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

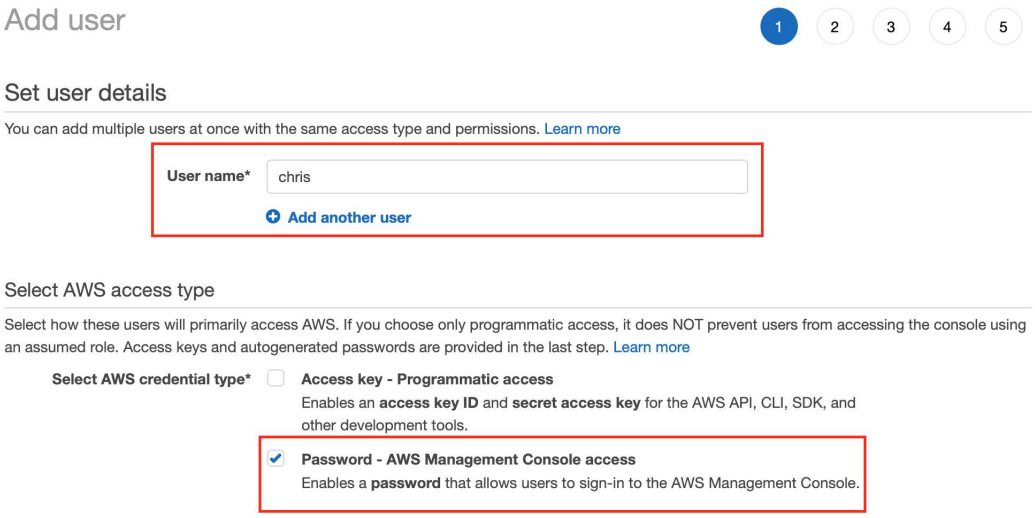
- Click **Users** on the navigation pane located on the left side of the IAM dashboard.



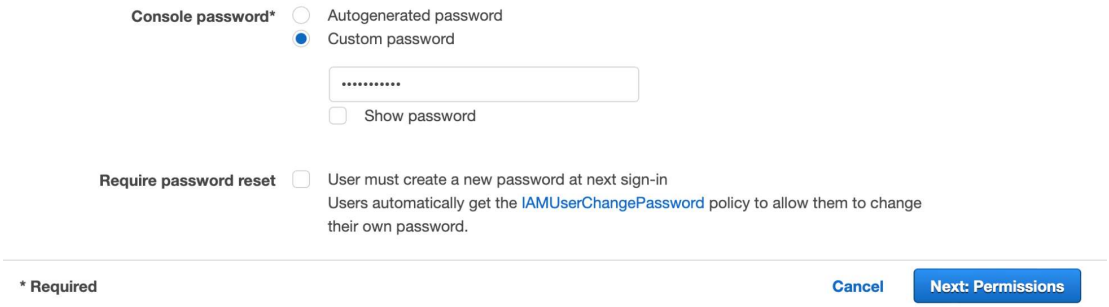
- Click **Add users** on the right-hand corner of the web page.



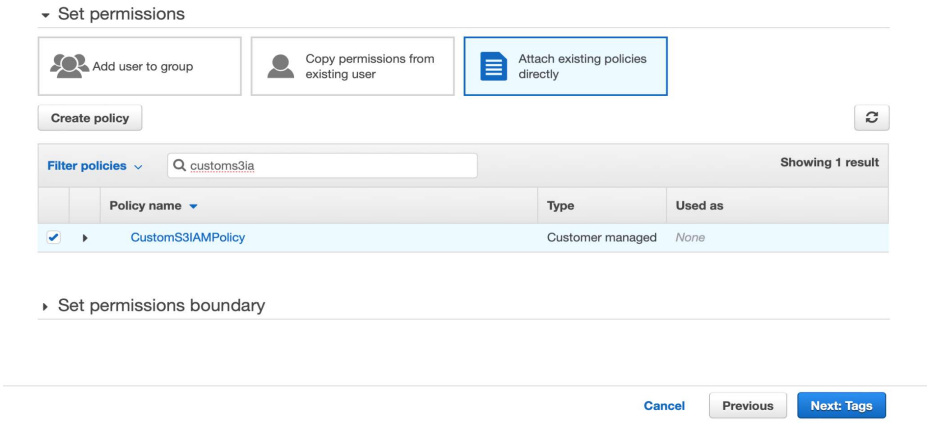
- Assign any name to this dummy user and enable password option to access AWS Management Console.



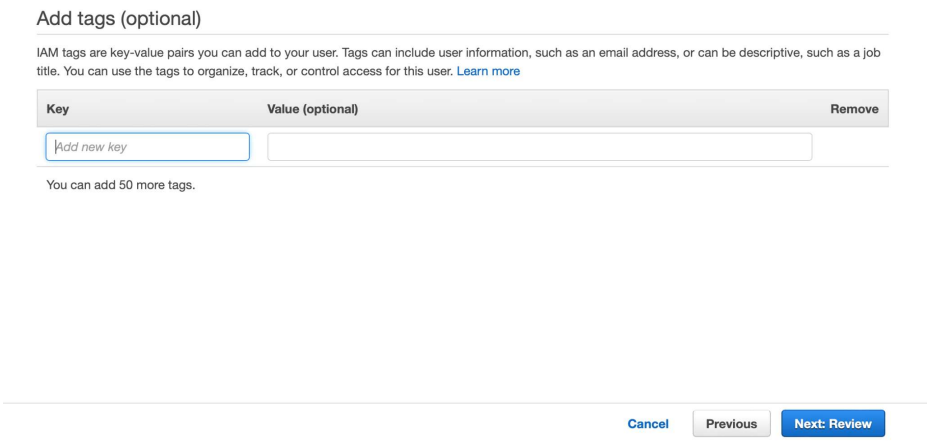
- Set a custom console password for this user and uncheck the **Require password reset** option. Click **Next: Permissions**.



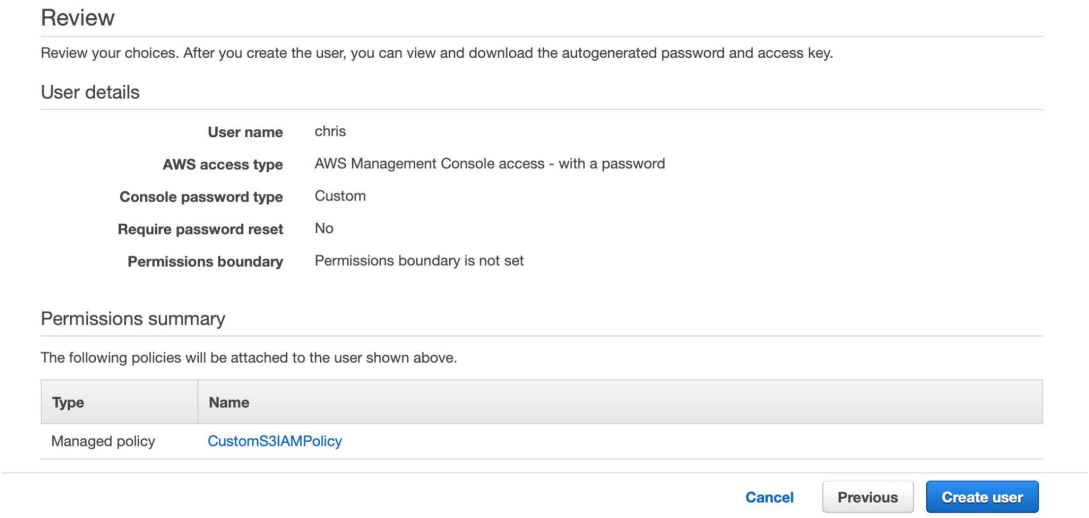
- Choose **Attach existing policies directly** under 'Set permissions', type the policy name in 'Filter policies' search bar, select it and click **Next: Tags** to proceed.



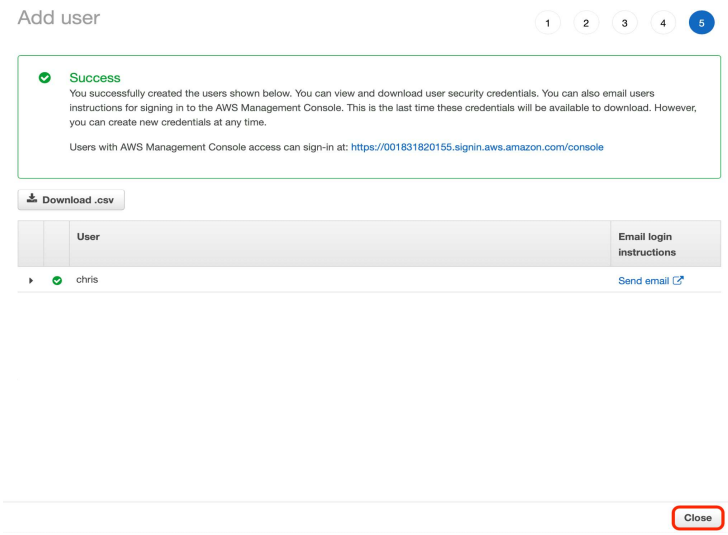
- Attaching a tag to a user is an optional parameter. Skip this step and click **Next: Review**.



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

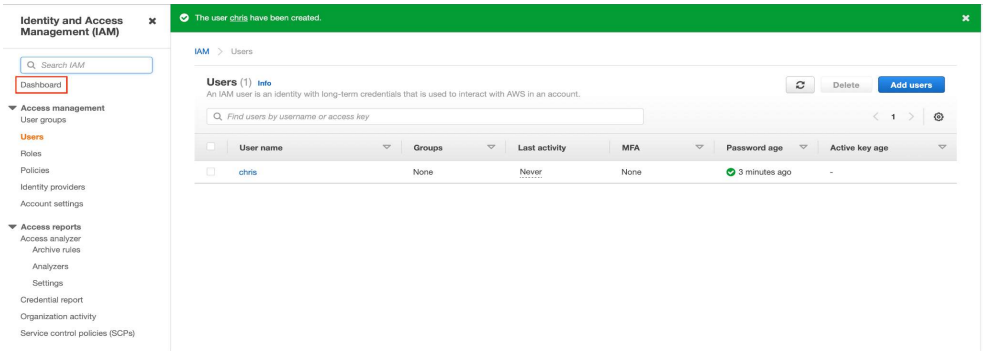


- This creates a new IAM user for us to test. Click **Close** to exit.

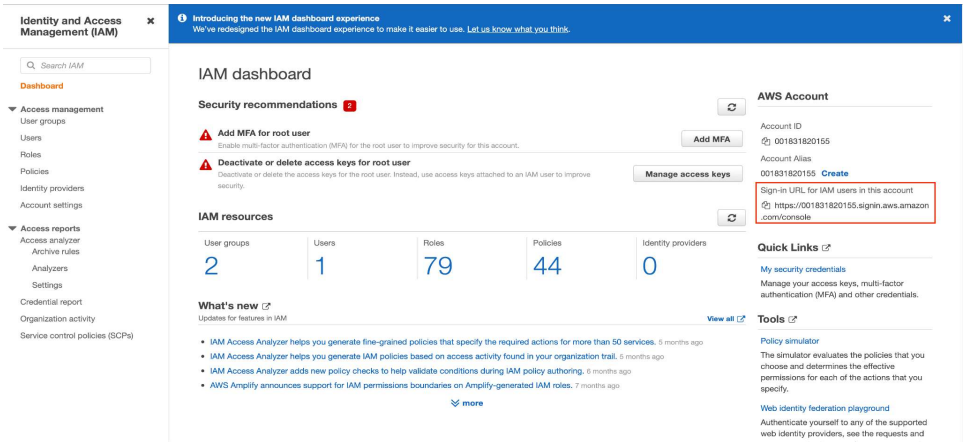


Step 4: Test user access

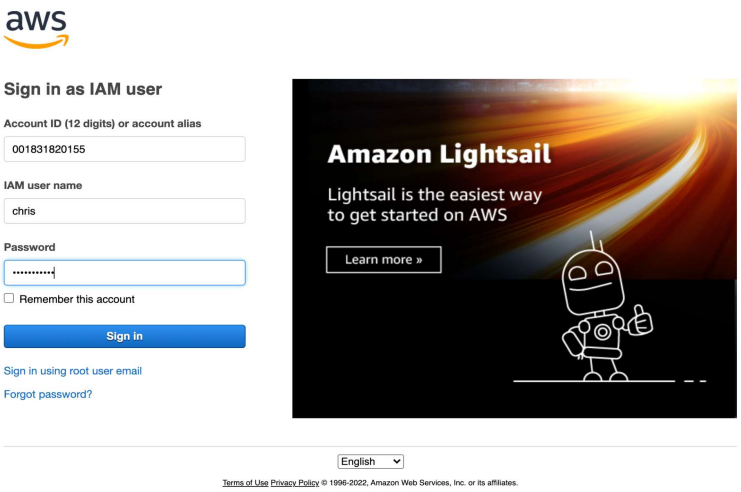
- Since we need to test how this IAM user can access S3 buckets using the custom IAM policy attached to it, click **Dashboard** on the left side within navigation menu options.



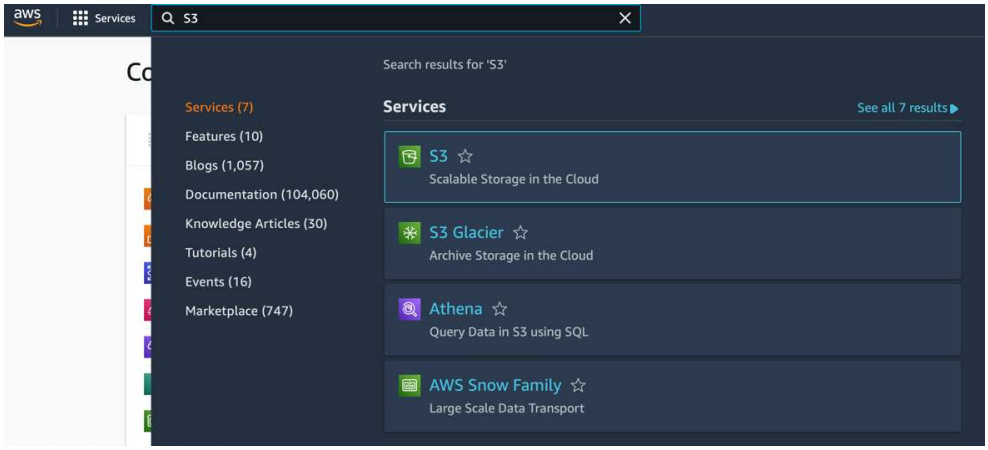
- On the Dashboard, copy the Sign-in **URL for IAM users in this account**.



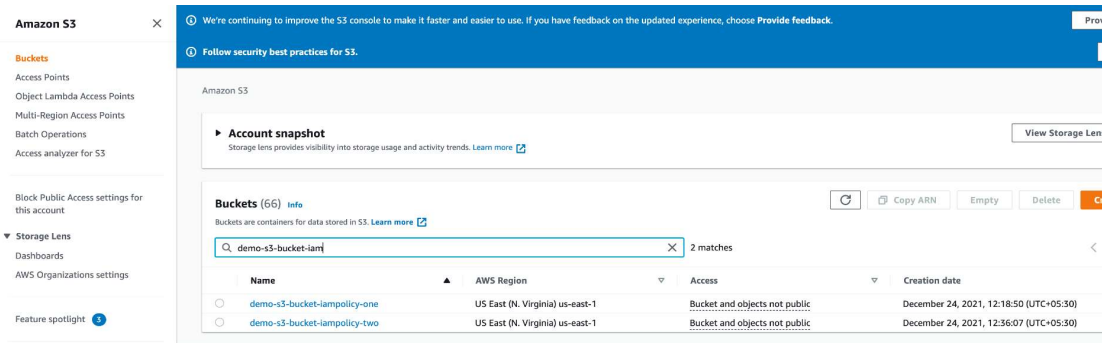
- Access this very link via a different browser and put in IAM username and password. Click **Sign in** to get access to AWS Management Console.



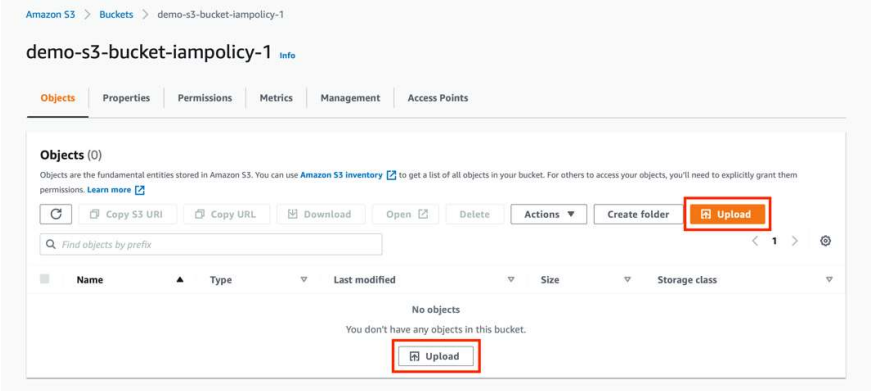
- Search for **S3** via the search menu bar provided at the top of this web page and click S3 within the Services list.



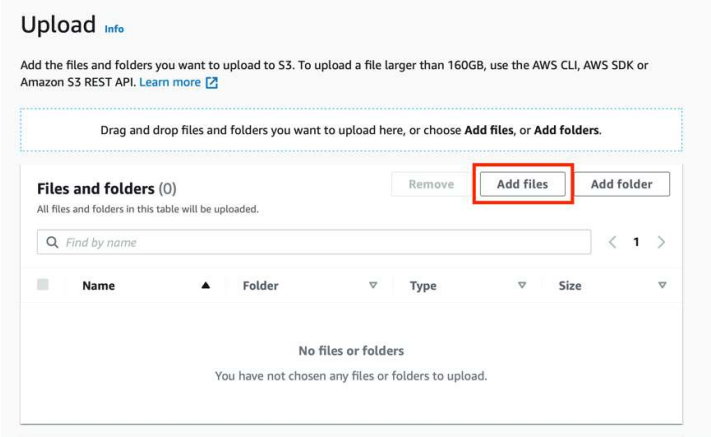
- Once you land on the S3 dashboard, search for the S3 buckets created before.



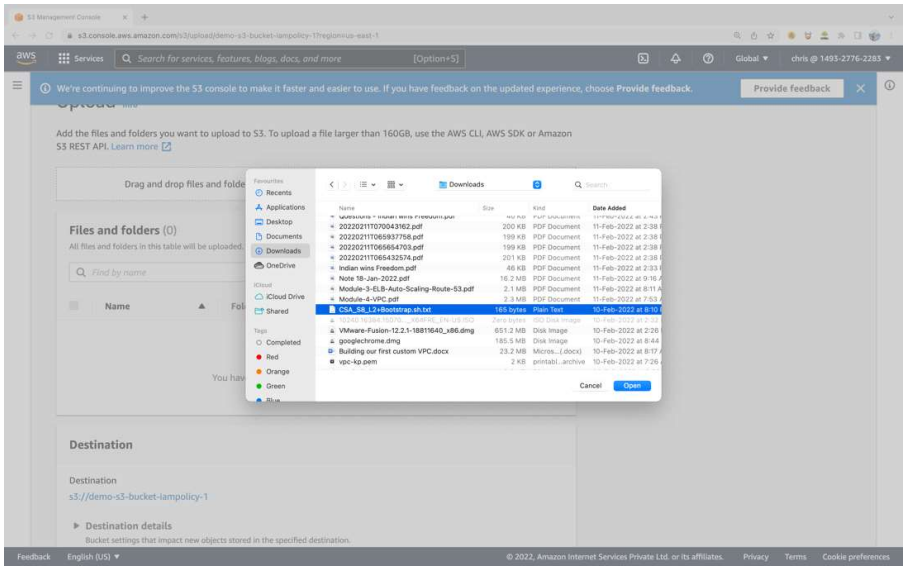
- Click and go to the first S3 bucket (which IAM user should have read-only access to) and click any of the available **Upload** options.



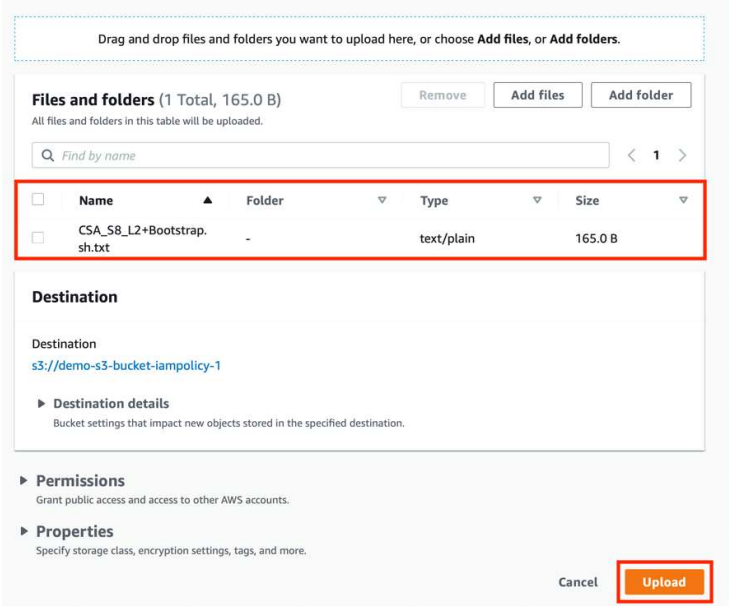
- Click **Add files**.



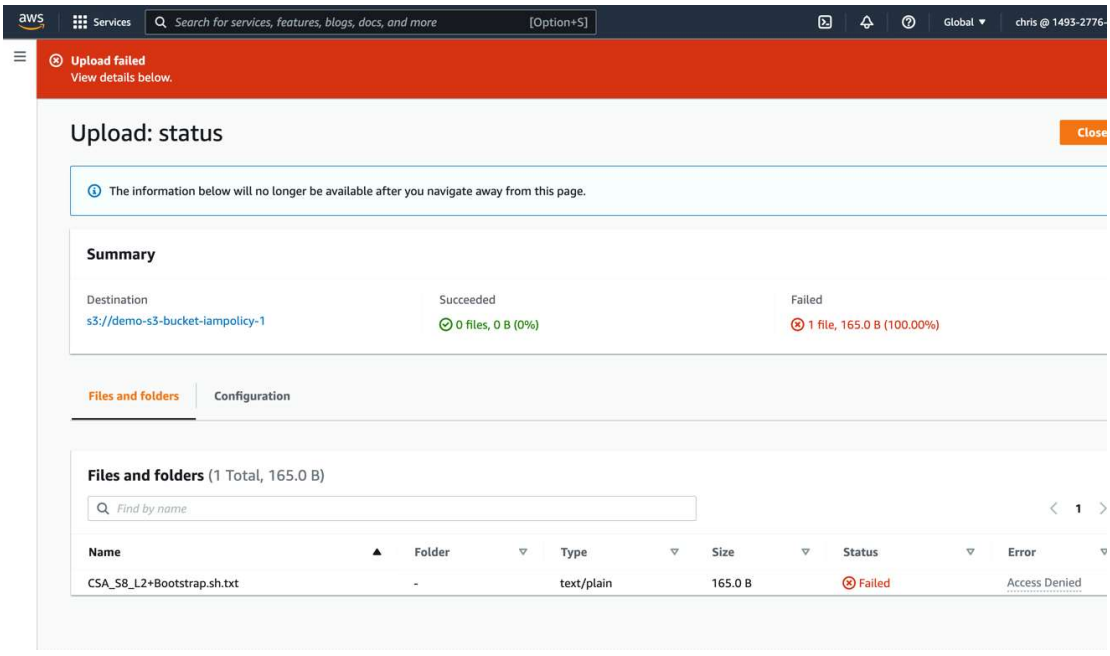
- Select and upload any of the available documents or images stored on your local computer.



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

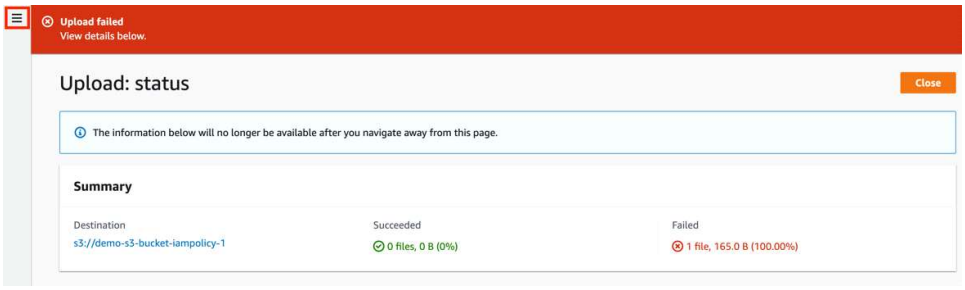


- As expected, the IAM user should be denied access from uploading or writing any object to this S3 bucket.

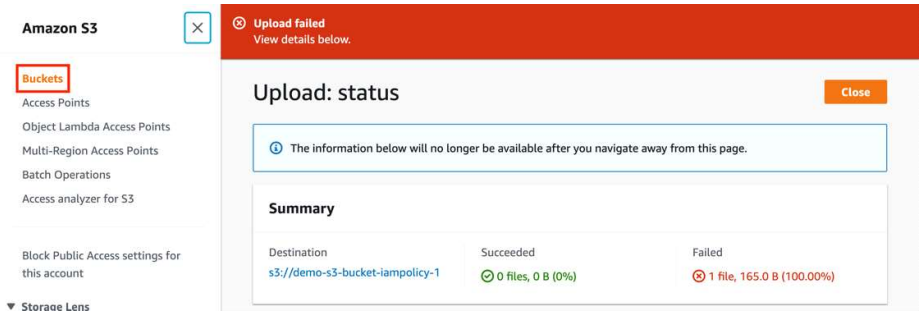


Now, you need to perform the same operation with the second S3 bucket.

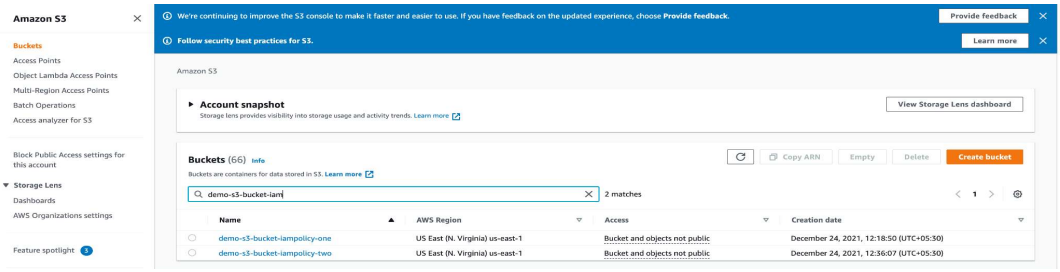
- Click on three vertical lines on the left side of the page.



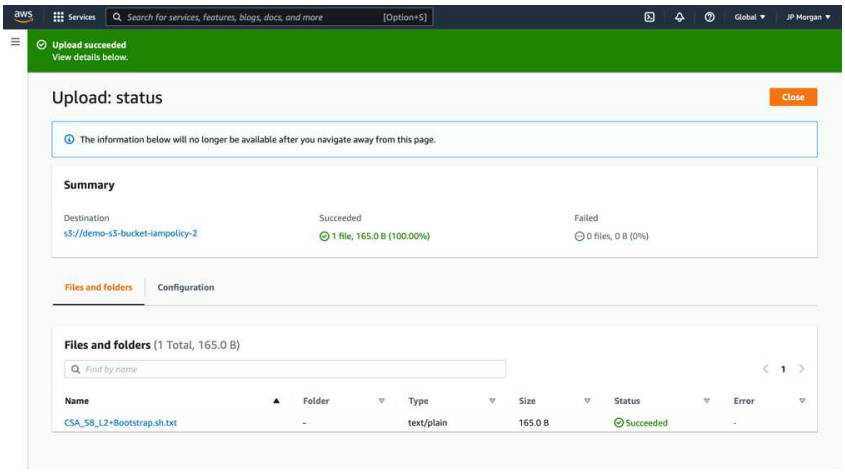
- Choose **Buckets** to access the list of S3 buckets.



- 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.


Services
Search for services, features, blogs, docs, and more
[Option+S]
Global
JP Morgan
Upload succeeded
View details below.
Upload: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://demo-s3-bucket-iampolicy-2
Succeeded
1 file, 165.0 B (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 Total, 165.0 B)
Find by name
1
Name
Folder
Type
Size
Status
Error
CSA_S8_L2+Bootstrap.sh.txt
-
text/plain
165.0 B
Succeeded
-