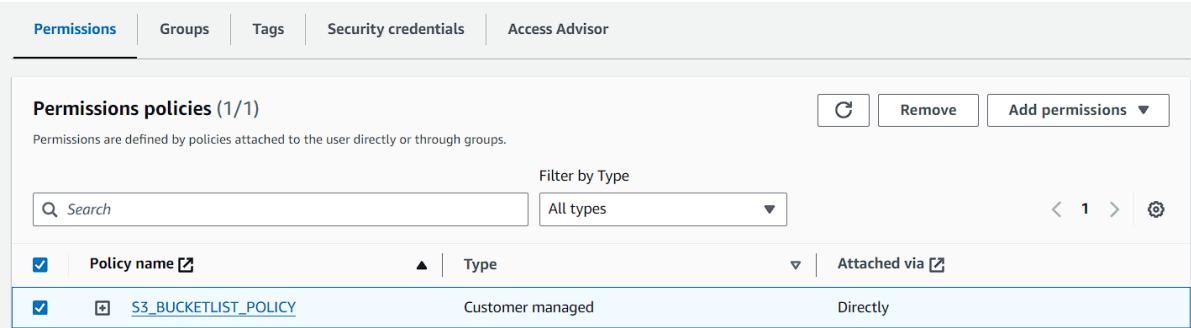


IAM POLICY

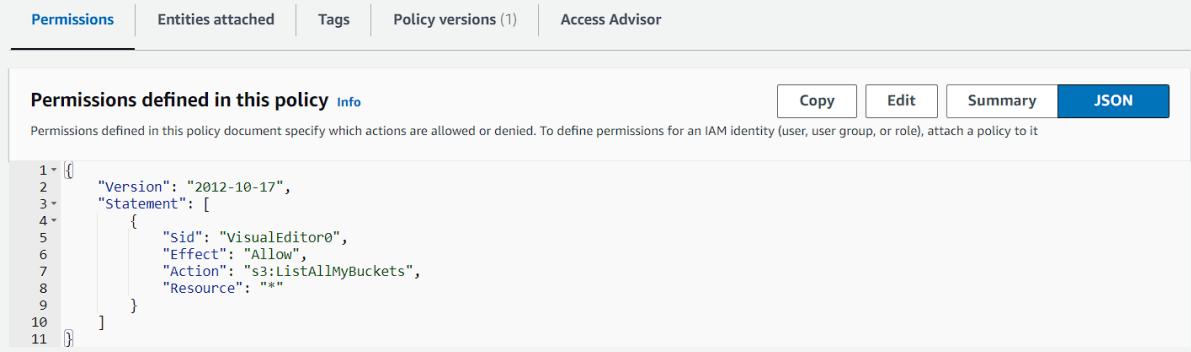
ALLOW ACCESS TO AN S3 BUCKET

1. So, in the previous lab you created a policy in IAM for your User.
2. The policy was just to list the bucket that are in you S3.
3. But in this lab, you are going to provide access to a single bucket which you want to access.
4. For that navigate to IAM, then to policy.
5. Now open your custom policy which you created. You have to make some changes with the policy.



The screenshot shows the AWS IAM Permissions page. The top navigation bar includes tabs for Permissions, Groups, Tags, Security credentials, and Access Advisor. Under the Permissions tab, there is a section titled "Permissions policies (1/1)". It displays a single policy named "S3_BUCKETLIST_POLICY". The policy is listed as "Customer managed" and attached "Directly". There are buttons for "Edit", "Remove", and "Add permissions". A search bar and a filter dropdown are also present.

6. Now if you want to view JSON representation of the policy, you can also do that by selecting JSON in the permissions section.



The screenshot shows the AWS IAM Policy Versions page. The top navigation bar includes tabs for Permissions, Entities attached, Tags, Policy versions (1), and Access Advisor. The "Policy versions (1)" tab is selected. Below it, there is a section titled "Permissions defined in this policy" with a "JSON" button highlighted with a red box. The JSON code shown is:

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Sid": "VisualEditor0",
6        "Effect": "Allow",
7        "Action": "s3>ListAllMyBuckets",
8        "Resource": "*"
9      }
10 ]
11 }
```

7. To make changes to your policy you need to click on edit.



The screenshot shows the AWS IAM Policy Editor. At the bottom, there are four buttons: "Copy", "Edit", "Summary", and "JSON". The "Edit" button is highlighted with a red box. A tooltip above the buttons says "Select the entity (user, user group, or role), attach a policy to it".

8. In the policy editor select it to Visual.
9. This time click on add more permission.

Modify permissions in S3_BUCKETLIST_POLICY [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

S3
Allow 1 Action

+ Add more permissions

Visual JSON Actions ▾

Cancel Next

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

10. Again, you need to choose S3 as your service.

11. Expand list and select list bucket action.

Access level [Expand all](#) [Collapse all](#)

▼ List (Selected 1/15)

<input type="checkbox"/> All list actions	<input type="checkbox"/> ListAccessGrants Info	<input type="checkbox"/> ListAccessGrantsInstances Info	<input type="checkbox"/> ListAccessGrantsLocations Info
<input type="checkbox"/> ListAccessPoints Info	<input type="checkbox"/> ListAccessPointsForObjectLambda Info	<input type="checkbox"/> ListAllMyBuckets Info	
<input checked="" type="checkbox"/> ListBucket Info	<input type="checkbox"/> ListBucketMultipartUploads Info	<input type="checkbox"/> ListBucketVersions Info	
<input type="checkbox"/> ListJobs Info	<input type="checkbox"/> ListMultipartUploadParts Info	<input type="checkbox"/> ListMultiRegionAccessPoints Info	
<input type="checkbox"/> ListStorageLensConfigurations Info	<input type="checkbox"/> ListStorageLensGroups Info	<input type="checkbox"/> ListTagsForResource Info	

12. Then in Read, expand it. Then scroll a little you will see an action for Get bucket, select this.

▼ Read (Selected 1/60)

- All read actions
- [DescribeJob](#) | [Info](#)
- [GetAccessGrant](#) | [Info](#)
- [GetAccessGrantsInstanceResourcePolicy](#) | [Info](#)
- [GetAccessPointConfigurationForObjectLambda](#) | [Info](#)
- [GetAccessPointPolicyForObjectLambda](#) | [Info](#)
- [GetAccountPublicAccessBlock](#) | [Info](#)
- [GetBucketCORS](#) | [Info](#)
- [GetBucketNotification](#) | [Info](#)
- [GetBucketPolicy](#) | [Info](#)
- [GetBucketRequestPayment](#) | [Info](#)
- [GetBucketWebsite](#) | [Info](#)
- [GetIntelligentTieringConfiguration](#) | [Info](#)
- [GetLifecycleConfiguration](#) | [Info](#)
- [GetMultiRegionAccessPointPolicy](#) | [Info](#)
- [GetObject](#) | [Info](#)

13. After selecting these two actions if you scroll down to the bottom.
14. You will see some options for resources. Now this option is to select specific bucket which you need by adding its ARN (Amazon Resource Name)
15. Do not select all because you don't want your other buckets to be accessed.
16. Now click on add ARNs and add your bucket name

▼ Resources

Specify resource ARNs for these actions.

All

Specific

bucket Info	<small>⚠ Specified bucket resource ARN for the CreateBucket and 48 more actions. Add ARNs to restrict access.</small>	<input type="checkbox"/> Any
object Info	<small>⚠ Specified object resource ARN for the AbortMultipartUpload and 32 more actions. Add ARNs to restrict access.</small>	<input type="checkbox"/> Any

17. So, when you will click on bucket ARN just give this the name of your bucket.
18. But for the object ARN the name is same but you need to tick at Any object name. This will give you full access to any object within the bucket.

Specify ARN(s)

Visual Text

Resource bucket name

Any bucket name

datausr1234

Resource object name

Any object name

*

Resource ARN

arn:aws:s3:::datausr1234/*

Cancel

Add ARNs

19. After adding both the ARNs just save it.

▼ Resources

Specify resource ARNs for these actions.

All

Specific

bucket [Info](#)

arn:aws:s3:::datausr1234



Any

object [Info](#)

arn:aws:s3:::datausr1234/*



Any

► Request conditions - optional

Actions on resources are allowed or denied only when these conditions are met.

20. Once you have saved everything, now go back and log in with IAM user in a different browser.

21. Then navigate to S3. In the buckets you will see that you still have insufficient permission.

S3 Buckets			
Name	AWS Region	Access	Creation date
datausr1234	Europe (London) eu-west-2	Insufficient permissions	January 12, 2024, 19:46:48 (UTC+05:30)

22. But if you will open your bucket. You can view its content.

Amazon S3 > Buckets > datausr1234

datausr1234 [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (2) [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](#)

[C](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Find objects by prefix [Show versions](#) [<](#) [1](#) [>](#) [@](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	Dockerfile	-	January 12, 2024, 23:07:36 (UTC+05:30)	113.0 B	Standard
<input type="checkbox"/>	scripts/	Folder	-	-	-

23. Let's check for other buckets that you can access their buckets or not.

24. As you can see you don't have any access other the bucket that you desired to give access.

Amazon S3 > Buckets > aws-s3-bucket07

aws-s3-bucket07 [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects [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](#)

[C](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Find objects by prefix [Show versions](#) [<](#) [1](#) [>](#) [@](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	Insufficient permissions to list objects				

After you or your AWS administrator has updated your permissions to allow the s3>ListBucket action, refresh the page. Learn more about [Identity and access management in Amazon S3](#)