



IAM POLICY- ACCESS TO LIST BUCKETS

IAM, or Identity and Access Management, is a framework that helps organizations manage and control access to their resources in cloud environments. An IAM policy is a set of rules that define the permissions and access control for entities such as users, groups, and roles within an IAM system.

In cloud computing platforms like Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure, IAM policies are used to specify what actions users, groups, or roles are allowed or denied to perform on various resources. These resources can include virtual machines, databases, storage, and other cloud services.

IAM policies are typically written in a specific syntax or using a visual interface provided by the cloud platform. They consist of statements that define the following:

1. **Effect:** Whether the policy allows or denies the specified actions.
2. **Action:** The specific actions or operations that are allowed or denied.
3. **Resource:** The resources on which the actions can be performed (e.g., specific buckets in a storage service, instances in a compute service).
4. **Condition:** Optional conditions that must be satisfied for the policy to take effect.

Here's a simplified example of an IAM policy in AWS that allows a user to list the contents of a specific S3 bucket:

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "s3>ListBucket",  
      "Resource": "arn:aws:s3:::example-bucket",  
      "Condition": {}  
    }  
  ]  
}
```

In this example:

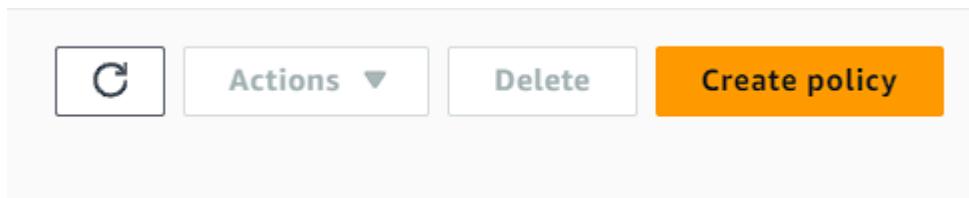
- **Effect:** Allows the action.
- **Action:** `s3>ListBucket` allows listing the contents of an S3 bucket.

- **Resource:** Specifies the ARN (Amazon Resource Name) of the target S3 bucket.
- **Condition:** No additional conditions are specified in this simple example.

IAM policies play a crucial role in ensuring that users and systems have the appropriate level of access to resources while maintaining security and compliance in cloud environments.

👉 TO BEGIN WITH THE LAB

1. Login to AWS Console.
2. Then navigate IAM and remove the S3 read only access policy from your user.
3. In this lab you are going to create your own IAM Policy and attach it with the IAM user that you created earlier.
4. Once you have removed the policy from your IAM user, it's time to navigate to policies.
5. There you need to click on create policy.



6. In the create policies tab you will see that you have an option to choose the service prior to write your own JSON code.

Specify permissions Info

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

Policy editor

Visual JSON Actions ▾

▼ Select a service

Specify what actions can be performed on specific resources in a service.

Service

Choose a service

Q Filter services

Commonly used services

- Auto Scaling
- CloudFront
- EC2
- IAM
- Lambda
- RDS
- S3
- SNS

Other services

Cancel Next

7. So, here you can see S3 service in place choose it.
8. After choosing S3 you will that you have different action to choose from.
9. If you will expand each of the action one by one you will see you have a lot options through which you can create your own policies.

▼ S3

Set permissions for S3

Specify what actions can be performed on specific resources in S3.

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect
Allow Deny

Manual actions | Add actions
 All S3 actions (s3:*)

Access level
▶ List (15)
▶ Read (60)
▶ Write (56)
▶ Permissions management (15)
▶ Tagging (12)

Expand all | Collapse all

10. But for now, expand List, you will see a bunch of different options which you can choose but you have to select List all my buckets.

▼ List (Selected 1/15)

All list actions
 ListAccessGrants | Info
 ListAccessPoints | Info
 ListBucket | Info
 ListJobs | Info
 ListStorageLensConfigurations | Info
 ListAccessGrantsInstances | Info
 ListAccessPointsForObjectLambda | Info
 ListBucketMultipartUploads | Info
 ListMultipartUploadParts | Info
 ListStorageLensGroups | Info
 ListAllMyBuckets | Info
 ListBucketVersions | Info
 ListMultiRegionAccessPoints | Info
 ListTagsForResource | Info

11. Then just go to next page and name your policy then create it.

Policy details

Policy name
Enter a meaningful name to identify this policy.
 S3_BUCKETLIST_POLICY

Description - optional
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+,-,@,_' characters.

Permissions defined in this policy [Info](#) [Edit](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Search

Allow (1 of 403 services)

Show remaining 402 services

Service	▲ Access level	▼ Resource	Request condition
S3	Limited: List	All resources	None

12. Here you can see your policy.

Policy name	▲ Type	▼ Used as	▼ Description
<input type="radio"/> S3_BUCKETLIST_POLICY	Customer managed	None	-

13. Now open your policy. Then click on Entities attached.

S3_BUCKETLIST_POLICY [Info](#) [Delete](#)

Policy details

Type Customer managed	Creation time January 14, 2024, 19:24 (UTC+05:30)	Edited time January 14, 2024, 19:24 (UTC+05:30)	ARN arn:aws:iam::463646775279:policy/S3_BUCKETLIST_POLICY
--------------------------	--	--	--

Permissions **Entities attached** (highlighted) **Tags** **Policy versions (1)** **Access Advisor**

Permissions defined in this policy [Info](#) [Edit](#) [Summary](#) [JSON](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Search

Allow (1 of 403 services)

Show remaining 402 services

Service	Access level	Resource	Request condition
S3	Limited: List	All resources	None

14. Now you have to click on attach.

Attached as a permissions policy (0) [Attach](#) [Detach](#)

To grant permissions to an entity, attach a permissions policy to it.

Filter by Entity type Search All types

Entity name	Entity type
Policy not attached to any entity.	

Attach (highlighted)

15. Here you to search for your IAM user account name. Then click on Attach policy.

16. This will attach your policy directly to your IAM user.

17. This is another method to attach policies to your IAM users.

Filter by Entity type s3-usr01 All types 1 match [Cancel](#) [Attach policy](#)

Entity name	Entity type
s3-usr01	IAM Users

18. Just to cross verify, if you go back to your IAM user in IAM then you will see that the policy is attach to your user.

S3-usr01 [Info](#)

[Delete](#)

Summary

ARN arn:aws:iam::463646775279:user/s3-usr01	Console access	Access key 1 Create access key
Created January 14, 2024, 16:16 (UTC+05:30)	Last console sign-in	

[Permissions](#) | [Groups](#) | [Tags](#) | [Security credentials](#) | [Access Advisor](#)

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type	
Search	All types
<input type="checkbox"/> Policy name S3_BUCKETLIST_POLICY	Type Customer managed
<input type="checkbox"/> S3_BUCKETLIST_POLICY	Attached via Directly

19. If you again login with your IAM user account in any other browser.
20. Then navigate to S3, you will see that you can see your bucket but it is also showing you the insufficient permissions.

[datausr1234](#) [Info](#)

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

[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](#)

Actions				
	Copy S3 URI	Copy URL	Download	Open
<input type="button" value="Actions"/>	<input type="button" value="Create folder"/>	<input type="button" value="Upload"/>		

Find objects by prefix Show versions

Name	Type	Last modified	Size	Storage class
✖ 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				

21. This is happening because the policy that you created, was just for listing the bucket not reading or making any changes to them.