

Lesson 07 Demo 02

Configuring Resource-Based Policy Using Principals

Objective: To demonstrate the process of configuring resource-based policies using principals to enable the access to AWS resources

Tools required: AWS Management Console

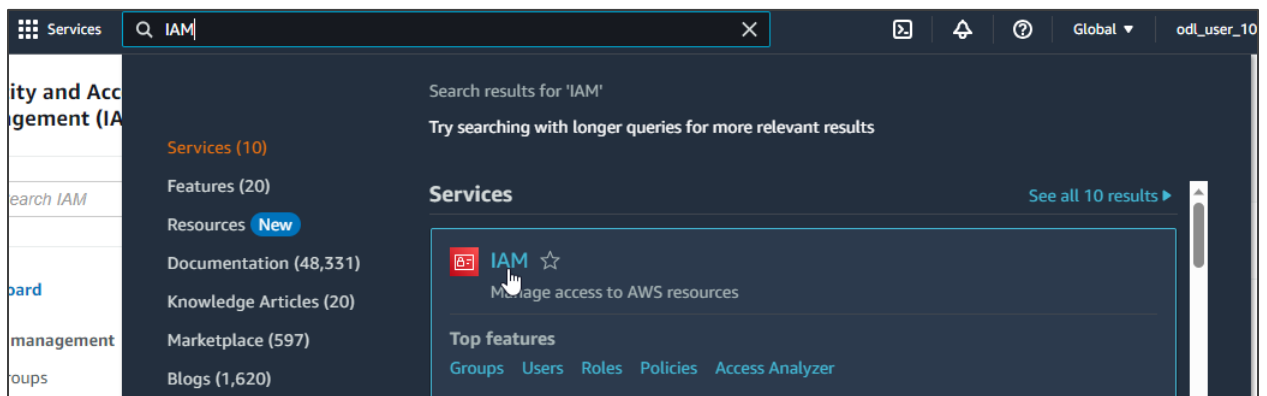
Prerequisites: None

Steps to be followed:

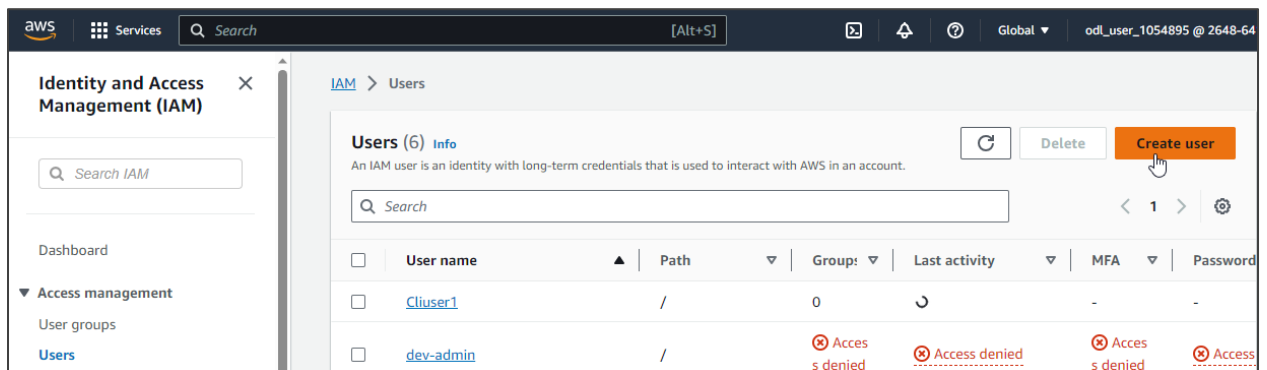
1. Create users and attach policies to them
2. Generate the policy using principals

Step 1: Create users and attach policies to them

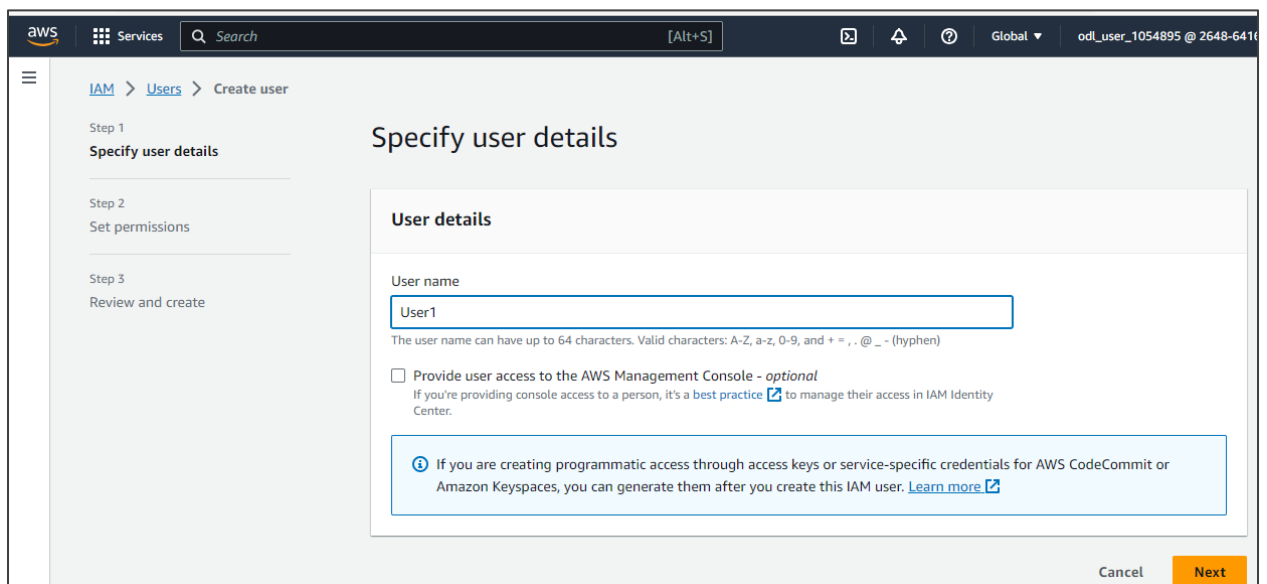
1.1 Navigate to the AWS portal, search for and select **IAM** from the services



1.2 In the IAM dashboard, select **Users** and click on **Create user**



1.3 Provide a name for the user and click on **Next**



1.4 On the **Permissions** page, select **Attach policies directly**. Then, select the **UserCreationRestriction** policy and click on **Next**.

Step 3
Review and create

☐ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ **Attach policies directly**
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1125)
Choose one or more policies to attach to your new user.

Filter by Type
 X All types 1 match

<input checked="" type="checkbox"/>	Policy name	Type	Attached entities
<input checked="" type="checkbox"/>	UserCreationRestriction	Customer managed	4

► Set permissions boundary - optional

Cancel Previous **Next**

1.5 Now, click on **Create user**

Step 3
Review and create

User name: User1
 Console password type: None
 Require password reset: No

Permissions summary

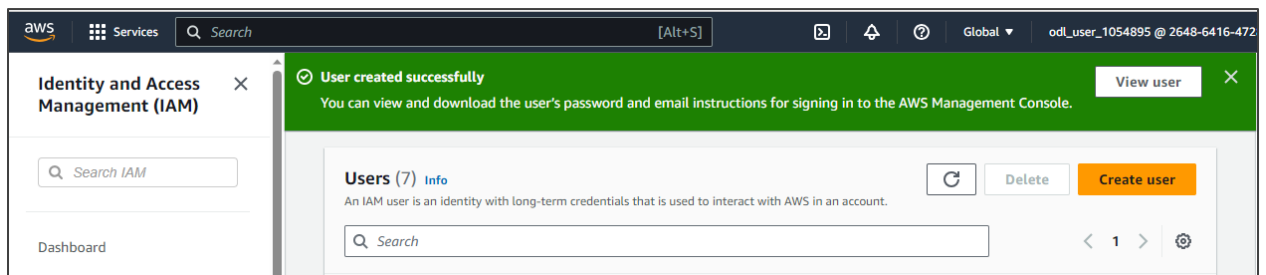
Name	Type	Used as
UserCreationRestriction	Customer managed	Permissions policy

Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)
You can add up to 50 more tags.

Cancel Previous **Create user**



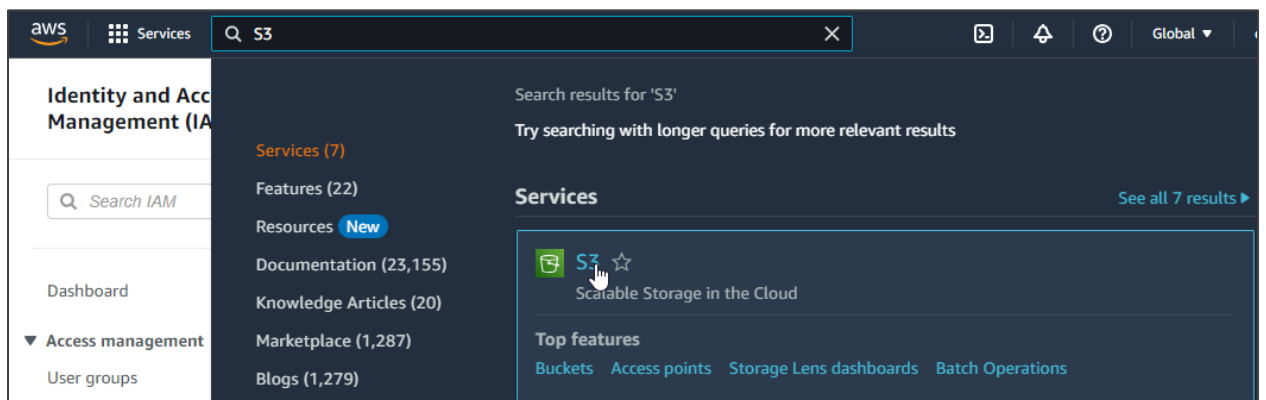
The user is created successfully.

1.6 Follow the same steps to create another user

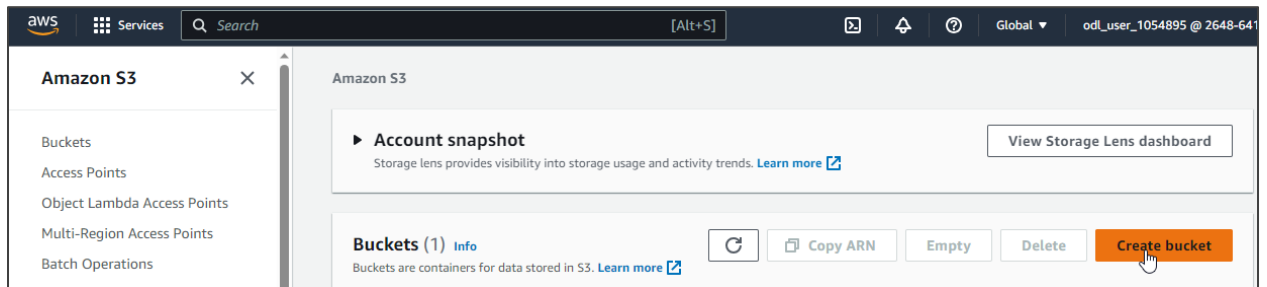
<input type="checkbox"/>	User1	/	0	-	-	-
<input type="checkbox"/>	User2	/	0	-	-	-

Step 2: Generate the policy using principals

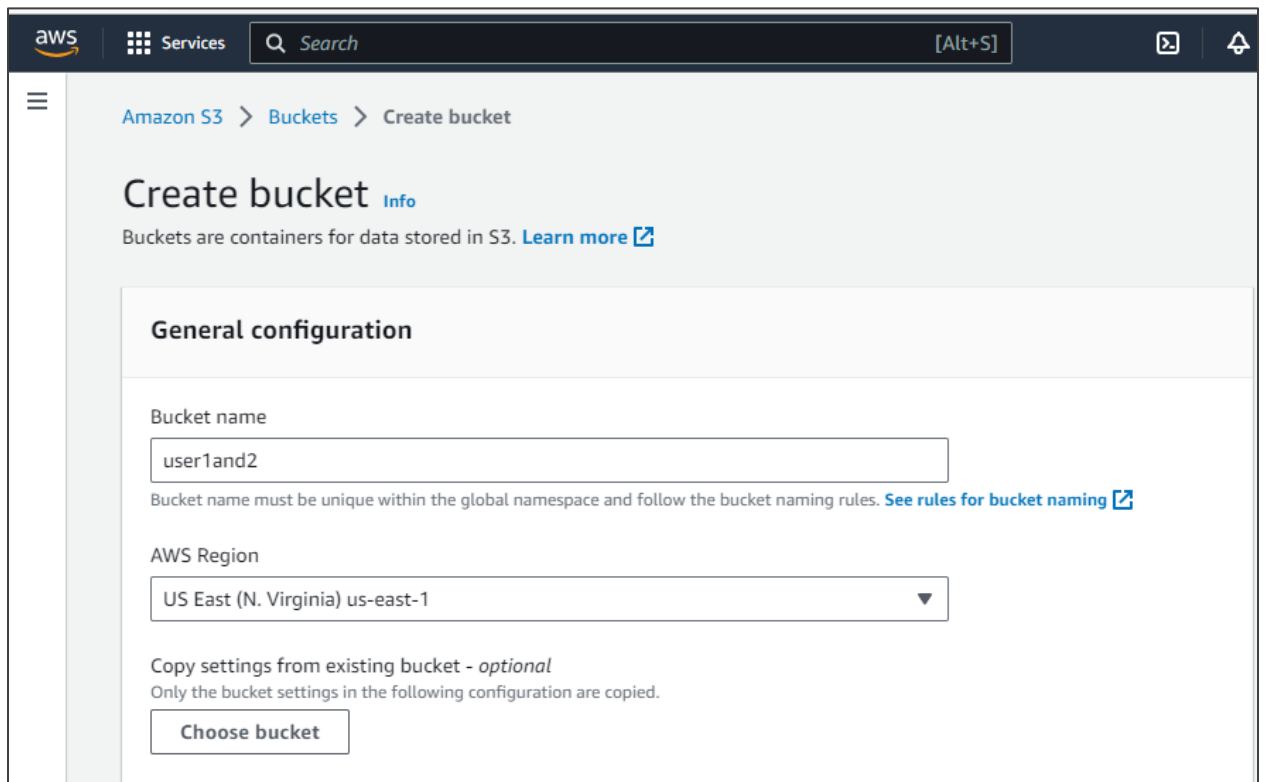
2.1 Now, search for and select **S3** from the **Services**

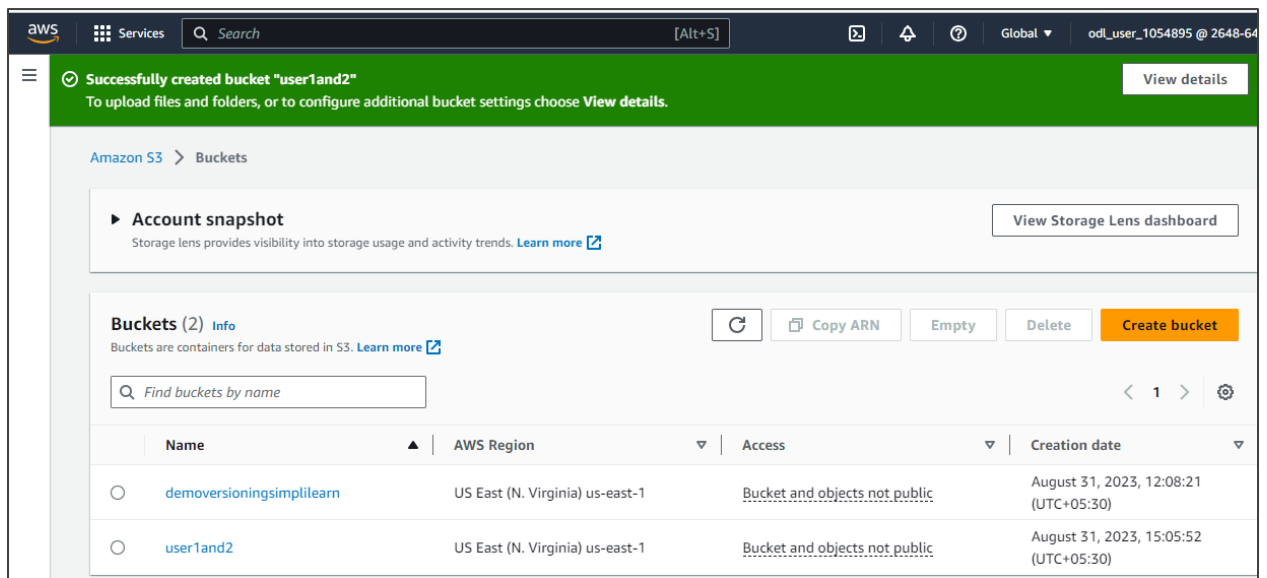


2.2 In the S3 dashboard, click on **Create bucket**



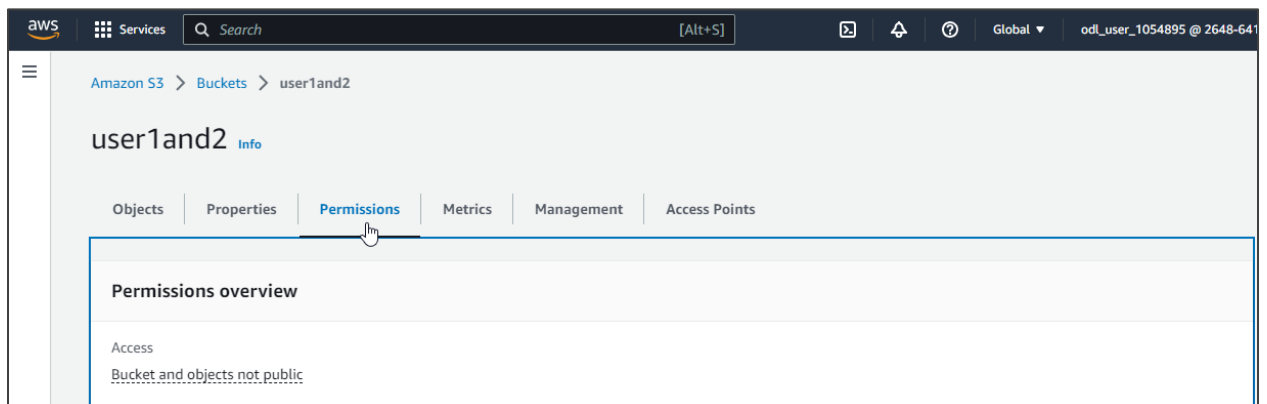
2.3 Provide a name for the bucket and select the **AWS Region**



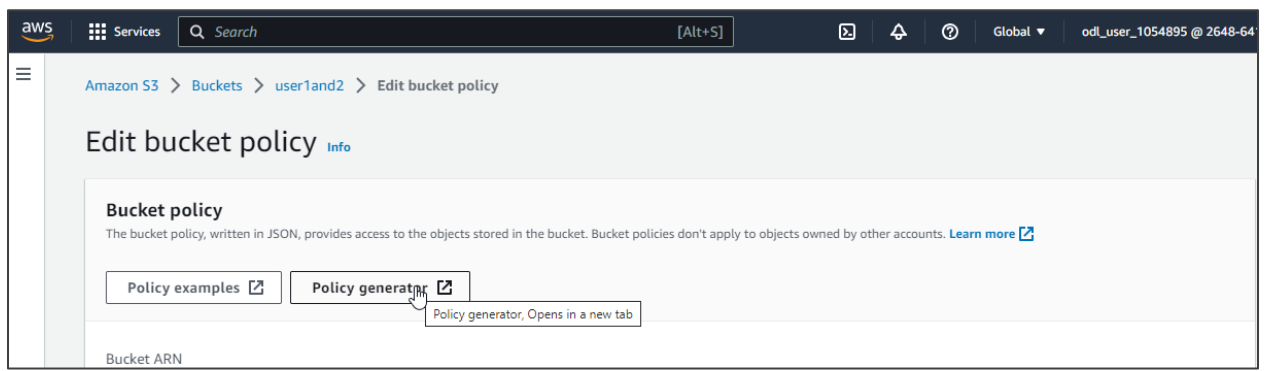
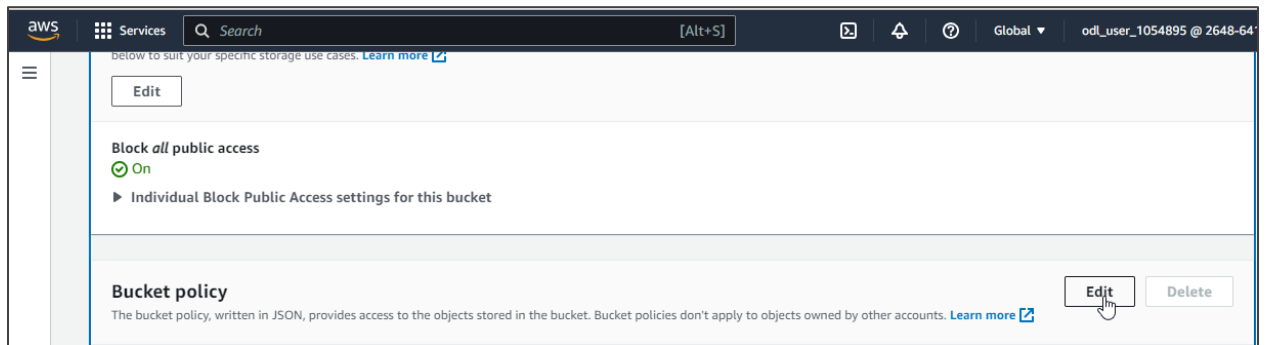


The bucket is successfully created.

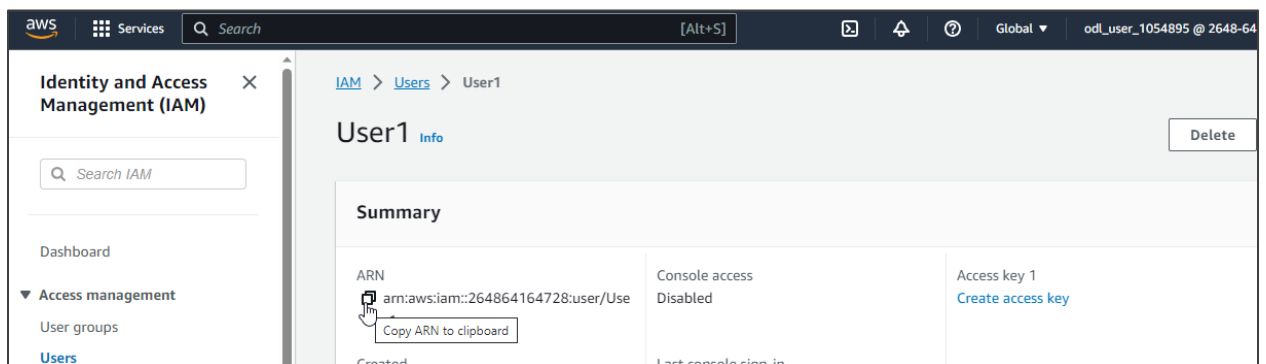
2.4 Select the bucket you created and go to **Permissions** as shown here:



2.5 Click **Edit** under **Bucket policy** section and then click on **Policy generator**



2.6 To enter the value in the principal, go to IAM users, click on **User1**, and then copy the user ARN



2.7 Paste the copied ARN in the **Principal** tab

← ↻ 🔒 https://awspolicygen.s3.amazonaws.com/policygen.html

amazon web services

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal arn:aws:iam::26486416472:

2.8 For Amazon Resource Name (ARN), go to the S3 bucket, select the bucket, and click on the **Copy ARN** button

aws Services 🔍 Search [Alt+S] Global odl_user_1054895 @ 2648-64

Amazon S3

Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens
Dashboards
AWS Organizations settings

Amazon S3

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

Buckets (2) Info

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

Find buckets by name

	Name	AWS Region	Access	Creation date
<input type="radio"/>	demoversioningsimplilearn	US East (N. Virginia) us-east-1	Bucket and objects not public	August 31, 2023, 12:08:21 (UTC+05:30)
<input checked="" type="radio"/>	user1and2	US East (N. Virginia) us-east-1	Bucket and objects not public	August 31, 2023, 15:05:52 (UTC+05:30)

Buttons: Refresh, Copy ARN, Empty, Delete, Create bucket

2.9 Paste the copied ARN in the ARN tab and click on **Add Statement**

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a [description of elements](#) that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal arn:aws:iam::26486416472:
Use a comma to separate multiple values.

AWS Service Amazon S3 ☐ All Services (*)
Use multiple statements to add permissions for more than one service.

Actions -- Select Actions -- ☒ All Actions (*)

Amazon Resource Name (ARN) arn:aws:s3:::user1and2
ARN should follow the following format: arn:aws:s3:::{BucketName}/{KeyName}.
Use a comma to separate multiple values.

[Add Conditions \(Optional\)](#)

Add Statement

2.10 Now, click on **Generate Policy**

You added the following statements. Click the button below to Generate a policy.

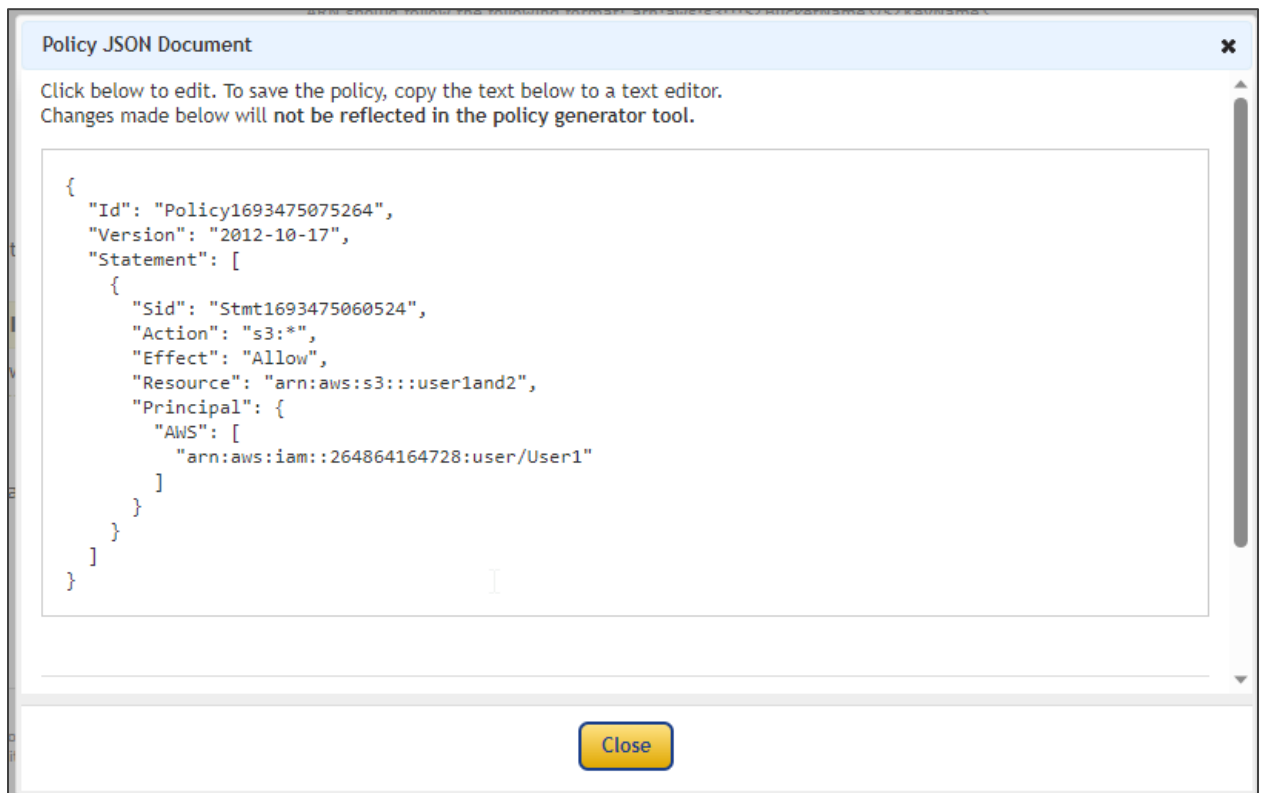
Principal(s)	Effect	Action	Resource	Conditions
• arn:aws:iam::26486416472:user/User1	Allow	s3:*	arn:aws:s3:::user1and2	None

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Generate Policy [Start Over](#)

The policy will be generated as shown here:



The screenshot shows a dialog box titled "Policy JSON Document" with a close button (X) in the top right corner. Below the title bar, there is a text area containing the following JSON document:

```
{
  "Id": "Policy1693475075264",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmnt1693475060524",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::userland2",
      "Principal": {
        "AWS": [
          "arn:aws:iam::264864164728:user/User1"
        ]
      }
    }
  ]
}
```

Below the text area, there is a "Close" button.

2.11 Copy the JSON and paste it into the bucket policy as shown here:

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

[Edit](#) [Delete](#)

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)

```

{
  "Version": "2012-10-17",
  "Id": "Policy1693475075264",
  "Statement": [
    {
      "Sid": "Stmnt1693475060524",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::264864164728:user/User1"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::user1and2"
    }
  ]
}

```

[Copy](#)

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Successfully edited bucket policy.

Amazon S3 > Buckets > user1and2

user1and2 Info

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access

Bucket and objects not public

The policy has been successfully updated.

By following these steps, you have successfully demonstrated the process of creating users, attaching policies to them, and then configuring the policy generator using principals.