Lesson 07 Demo 02

Configuring Resource-Based Policy Using Principals

Objective: To configure resource-based policies using principals to enable the access to AWS resources

Tools required: AWS Management Console

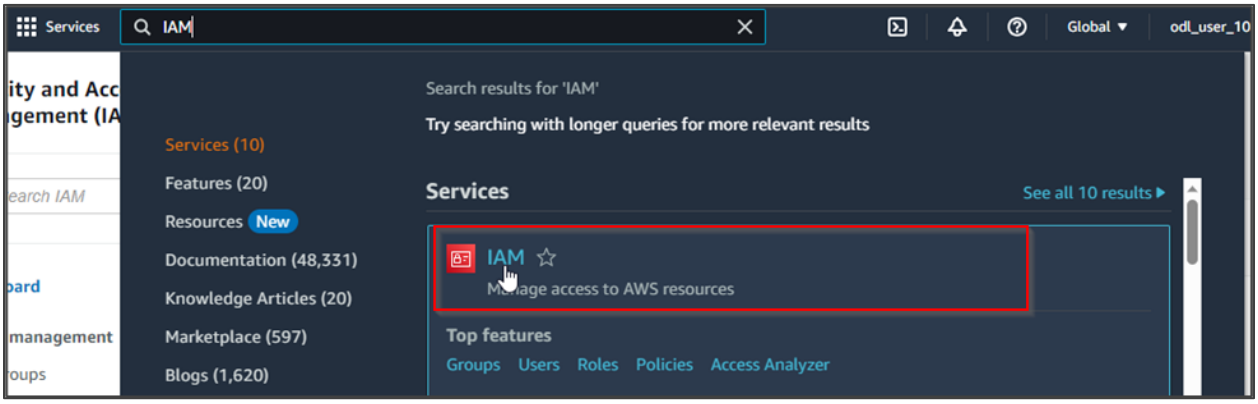
Prerequisites: None

Steps to be followed:

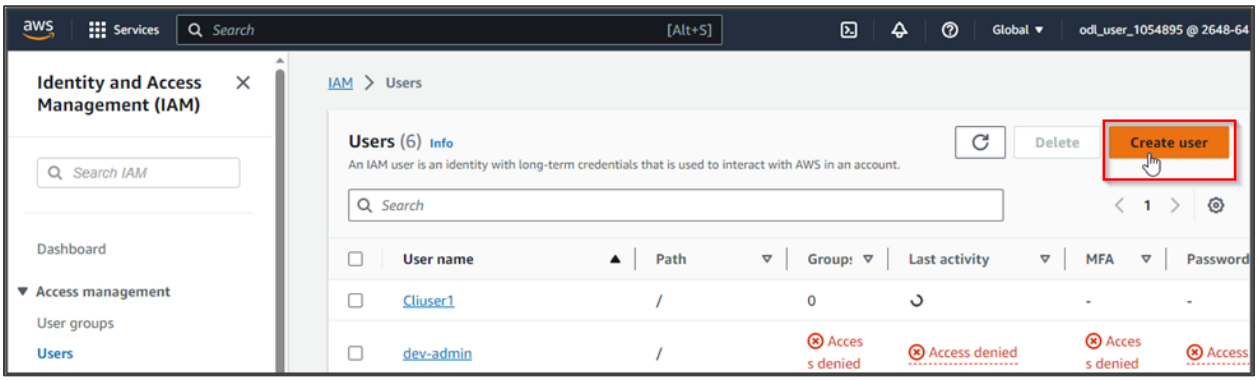
1. Create users and attach policies to them
2. Generate the policy using principals

Step 1: Create users and attach policies to them

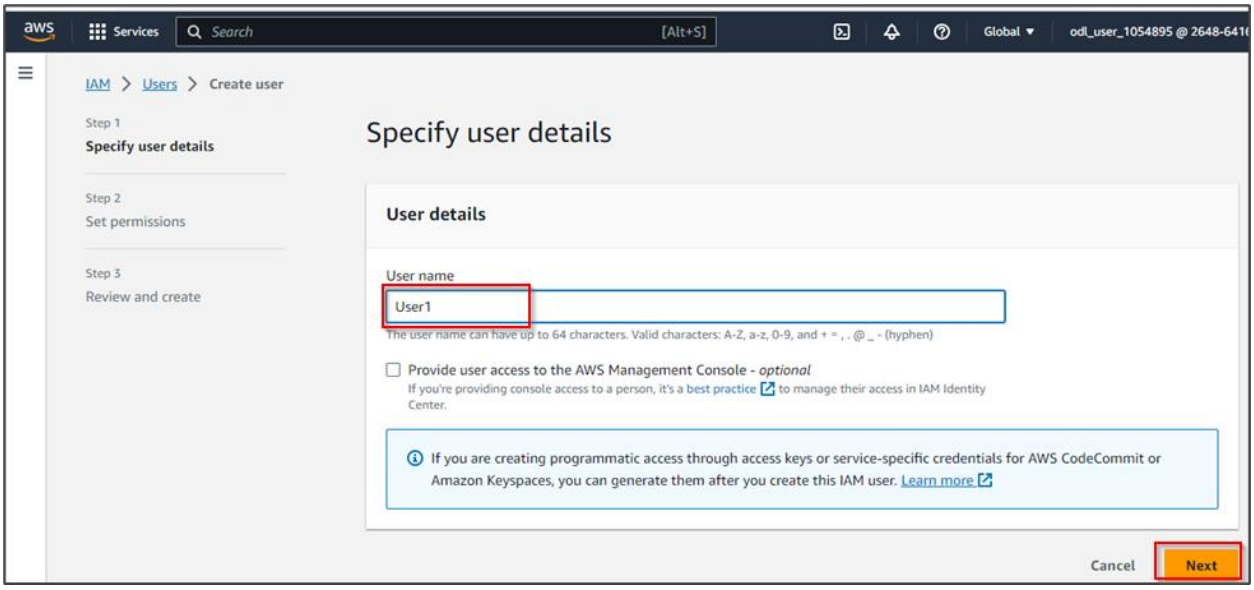
1.1 Navigate to the AWS portal, search for and select **IAM** from the services



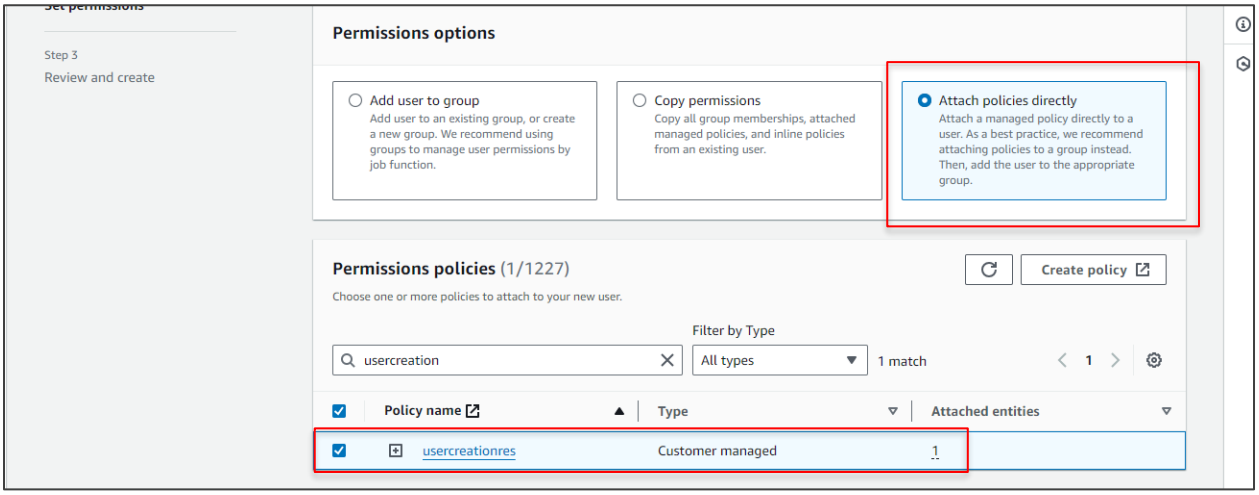
1.2 In the IAM dashboard, select **Users** and click on **Create user**

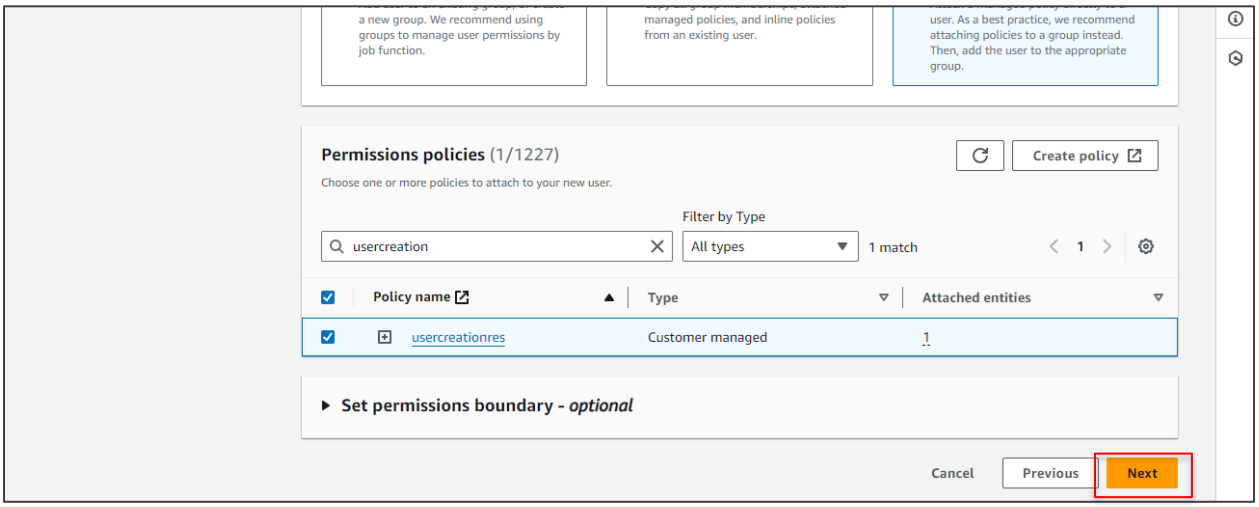


1.3 Provide a name for the user and click on **Next**

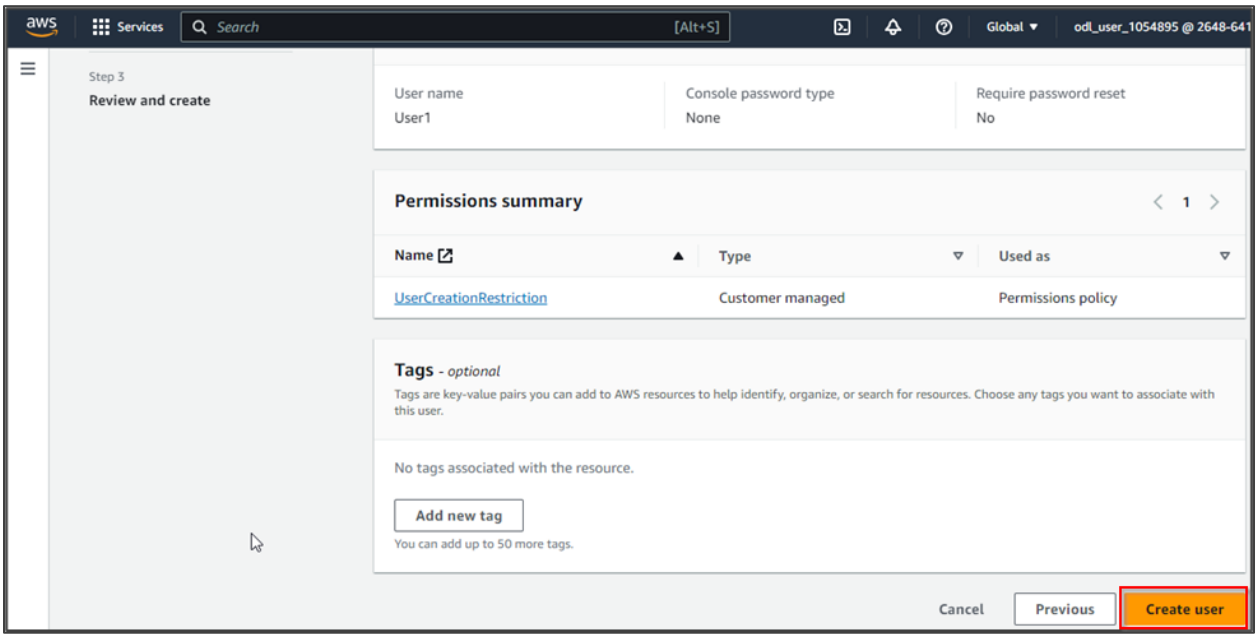


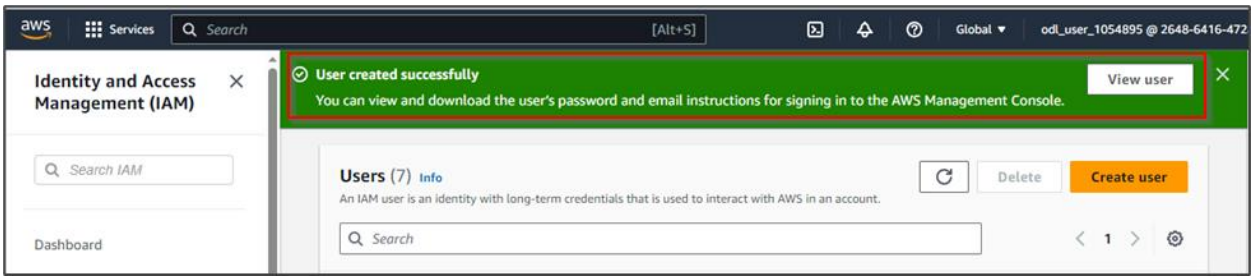
1.4 On the **Permissions** page, select **Attach policies directly**. Then, select the **usercreationres** policy and click on **Next**





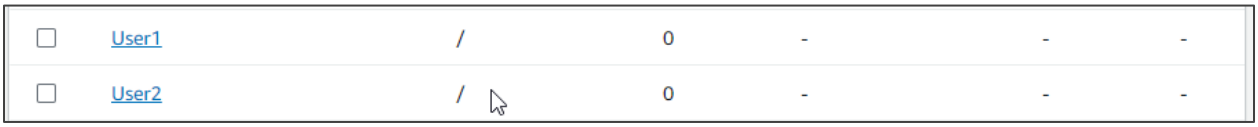
1.5 Click on **Create user**





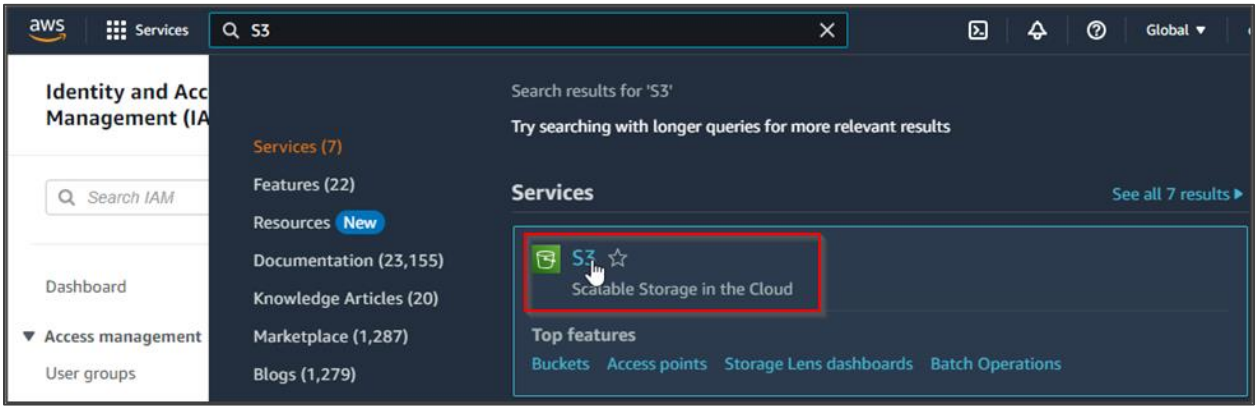
The user is successfully created.

1.6 Follow the same steps to create another user

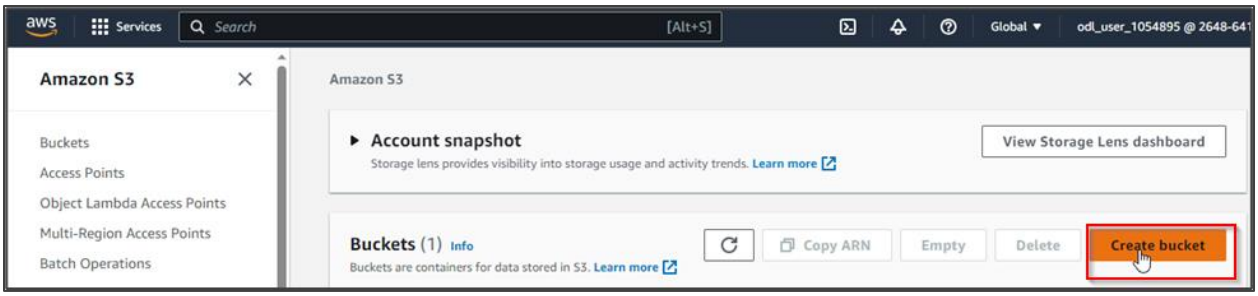


Step 2: Generate the policy using principals

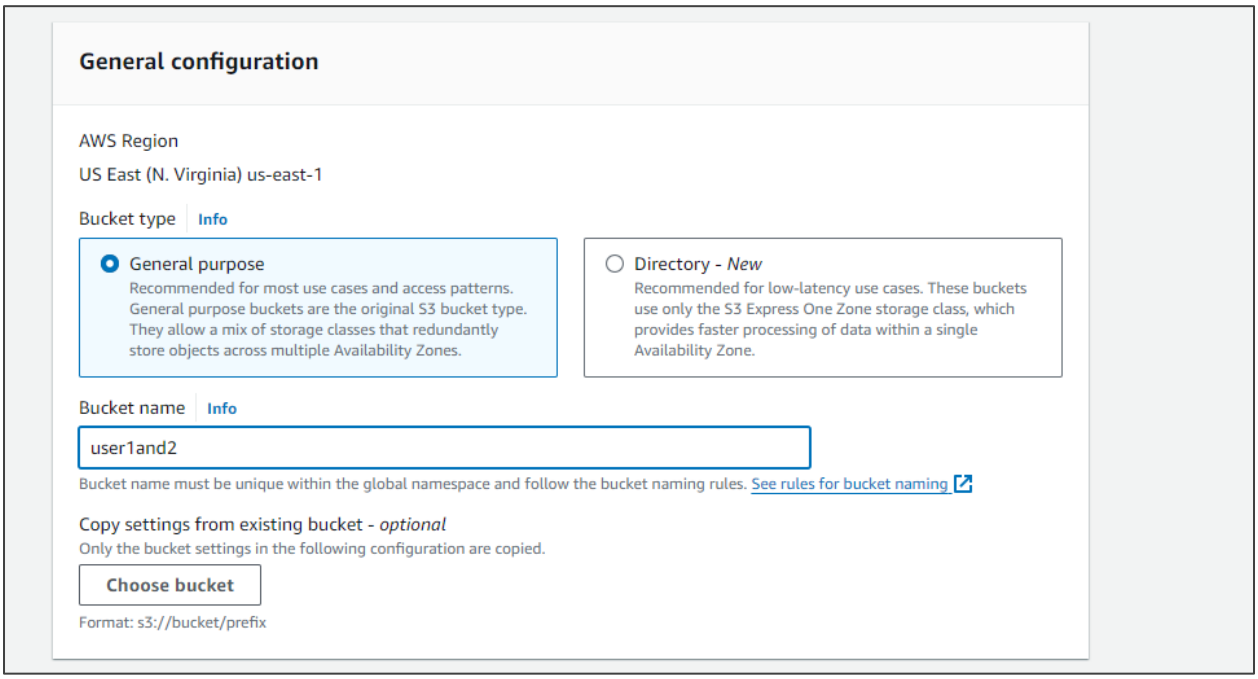
2.1 Search for and select **S3** from the **Services**

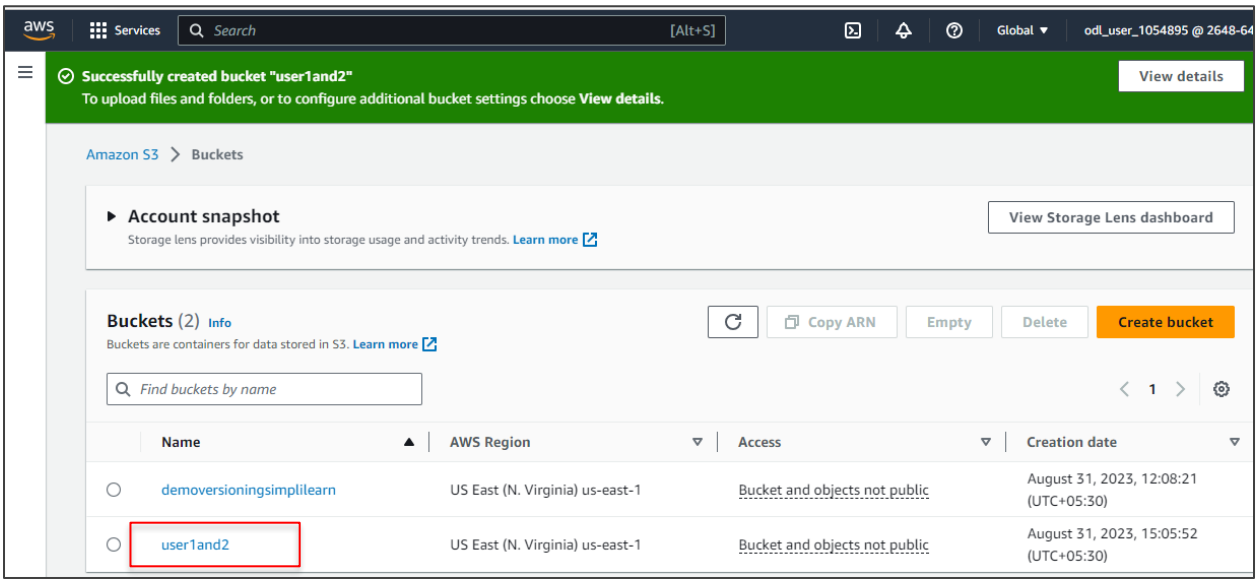


2.2 In the S3 dashboard, click on **Create bucket**



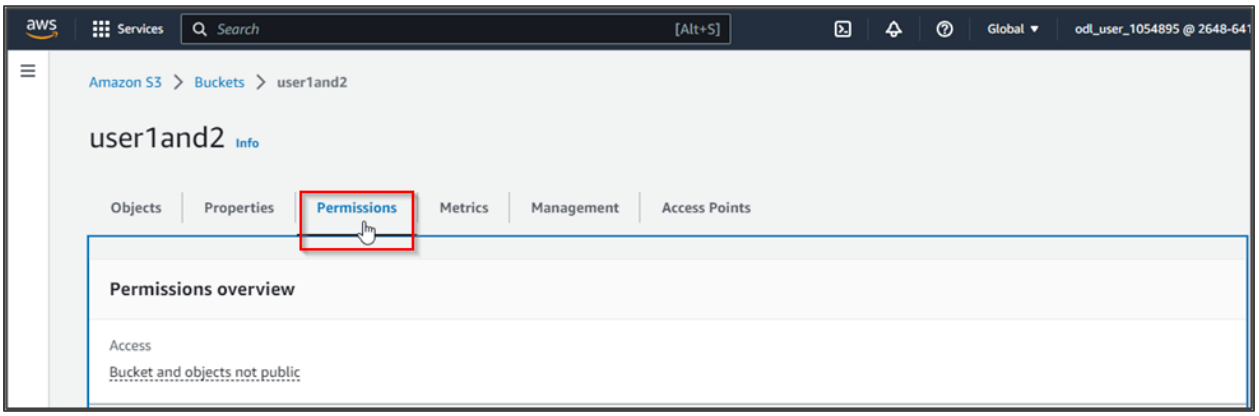
2.3 Provide a name for the bucket and select the AWS Region as given below:



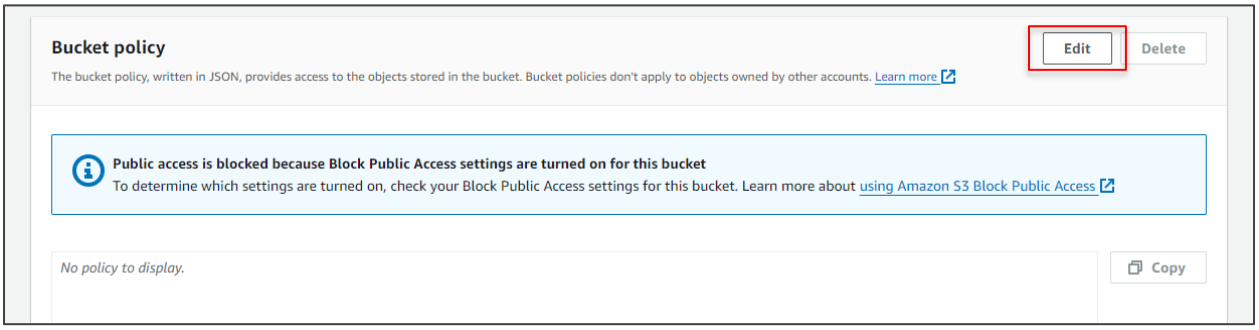


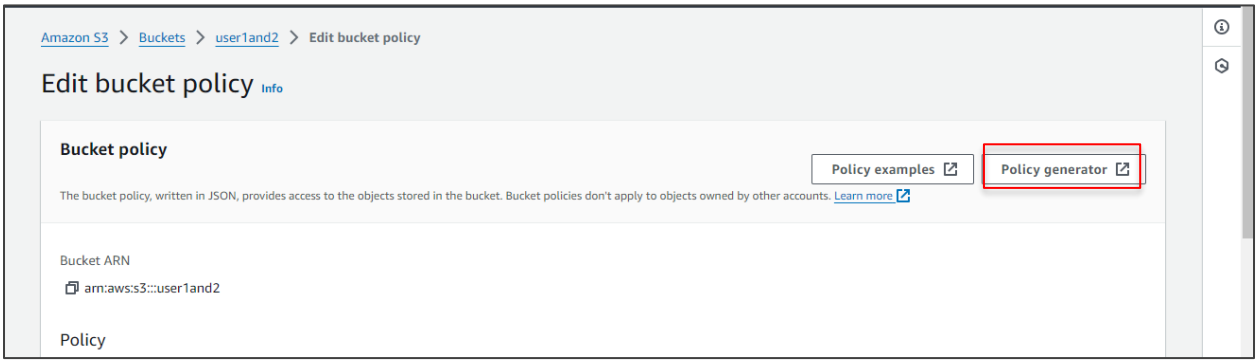
The bucket is successfully created.

2.4 Select the bucket you created and navigate to the **Permissions** tab as shown:

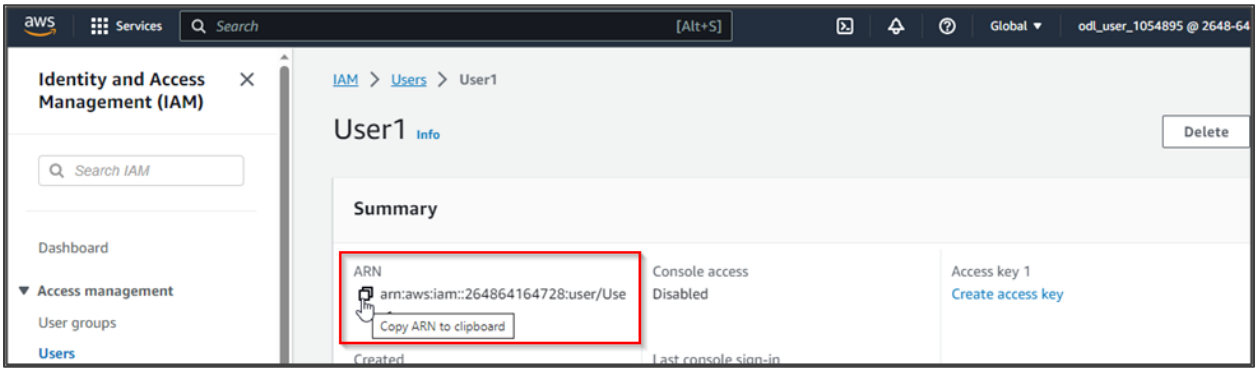


2.5 Click **Edit** under **Bucket policy** section and then click on **Policy generator**

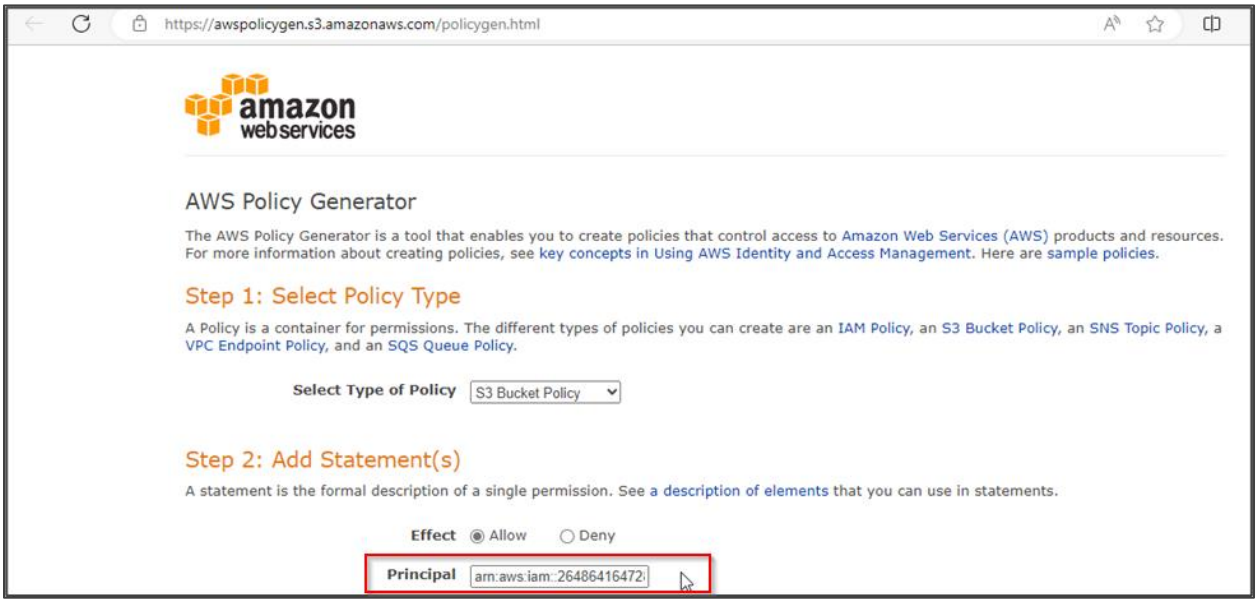




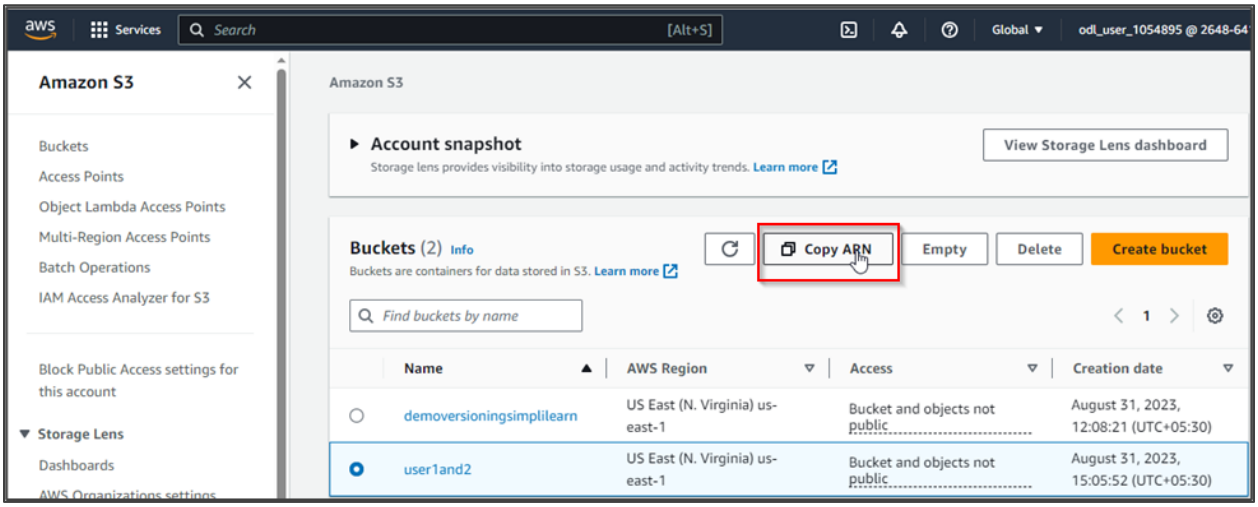
2.6 To enter the value in the principal, go to IAM users, click on **User1**, and then copy the user ARN



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



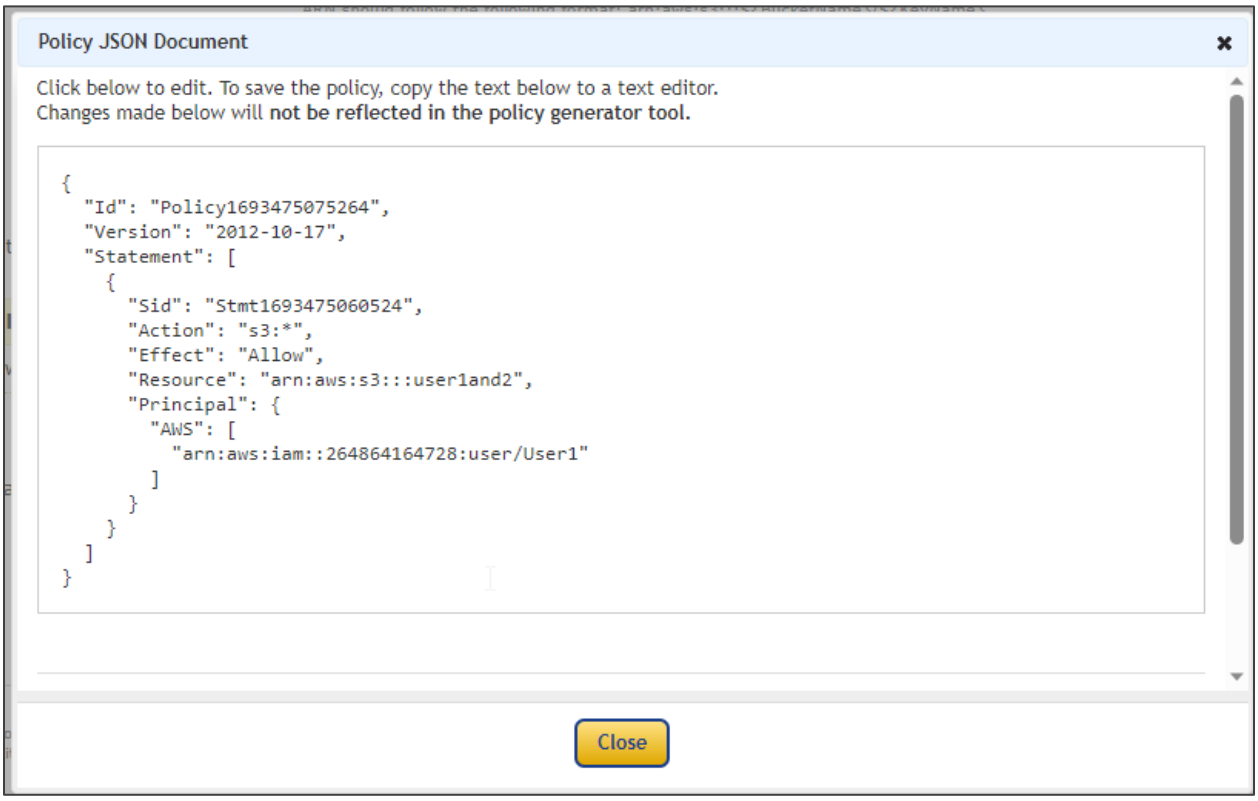
2.8 For Amazon Resource Name (ARN), go to the S3 bucket, select the bucket, and click on the **Copy ARN** button



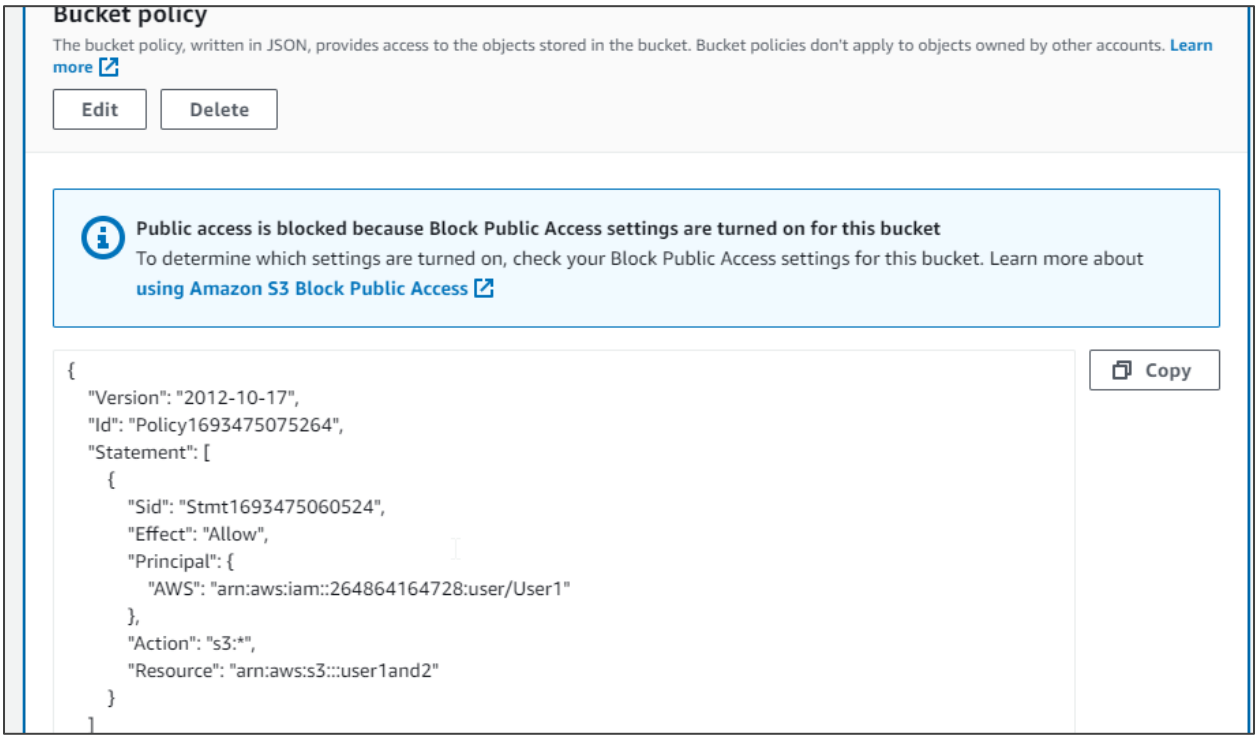
2.9 Paste the copied ARN in the ARN tab and click on **Add Statement**

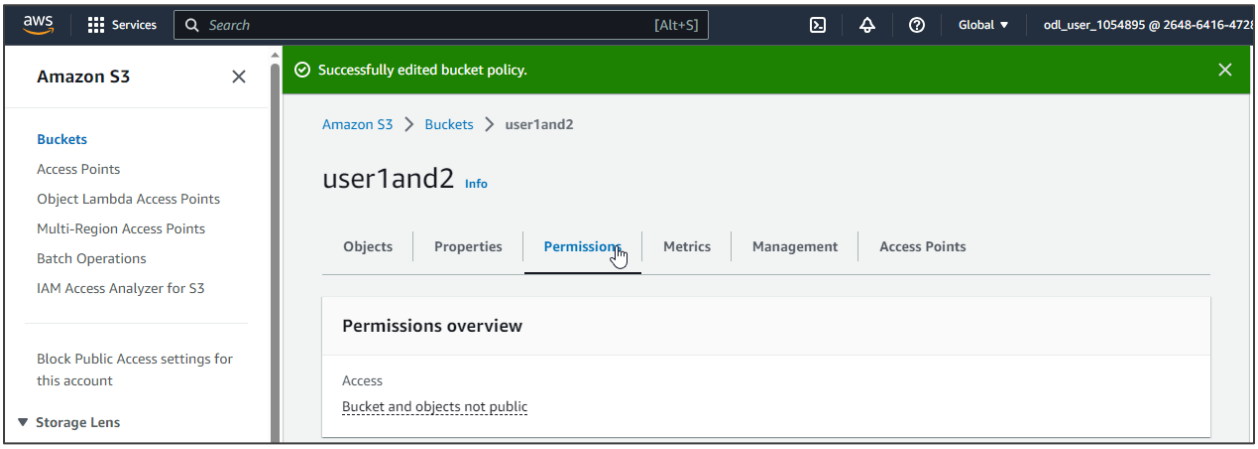
2.10 Now, click on **Generate Policy**

The policy will be generated as shown:



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





The policy has been successfully updated.

By following these steps, you have successfully configured resource-based policies using principals to enable the access to AWS resources.