Lesson 07 Demo 01

Creating and Adding Policies to Groups Using Users

Objective: To create and add a policy to the group using a user to enable security management in various systems and applications

Tools required: AWS Management Console

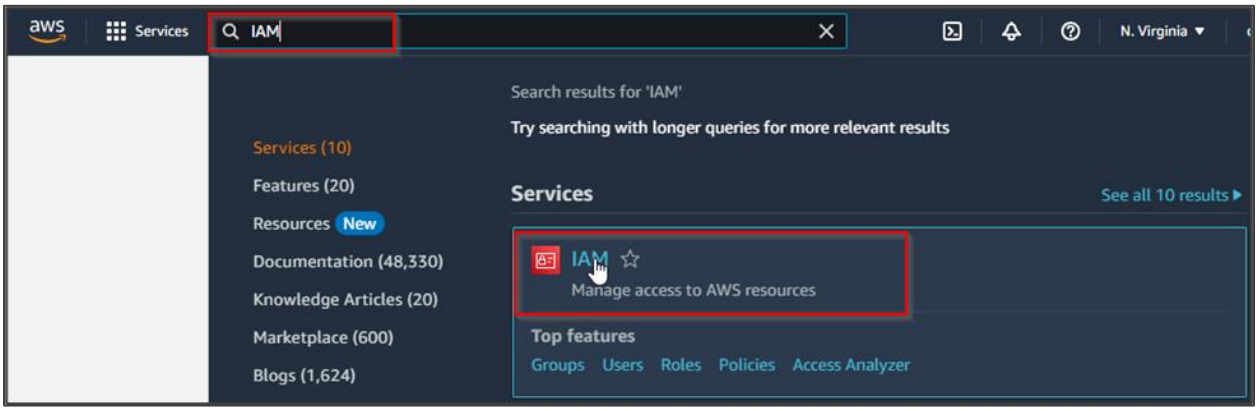
Prerequisites: None

Steps to be followed:

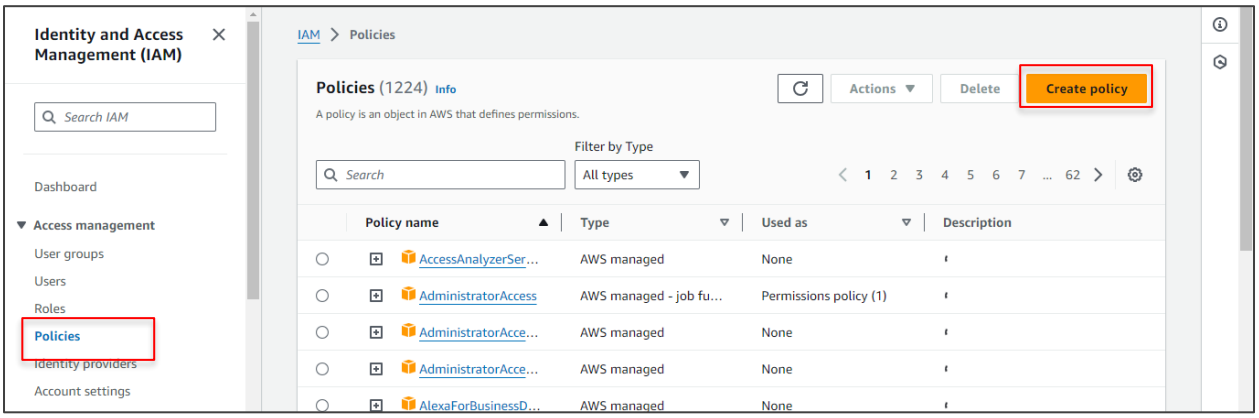
1. Create and manage policy
2. Attach policy and permissions directly to the group using group users
3. Create and manage S3 versioning

Step 1: Create and manage policy

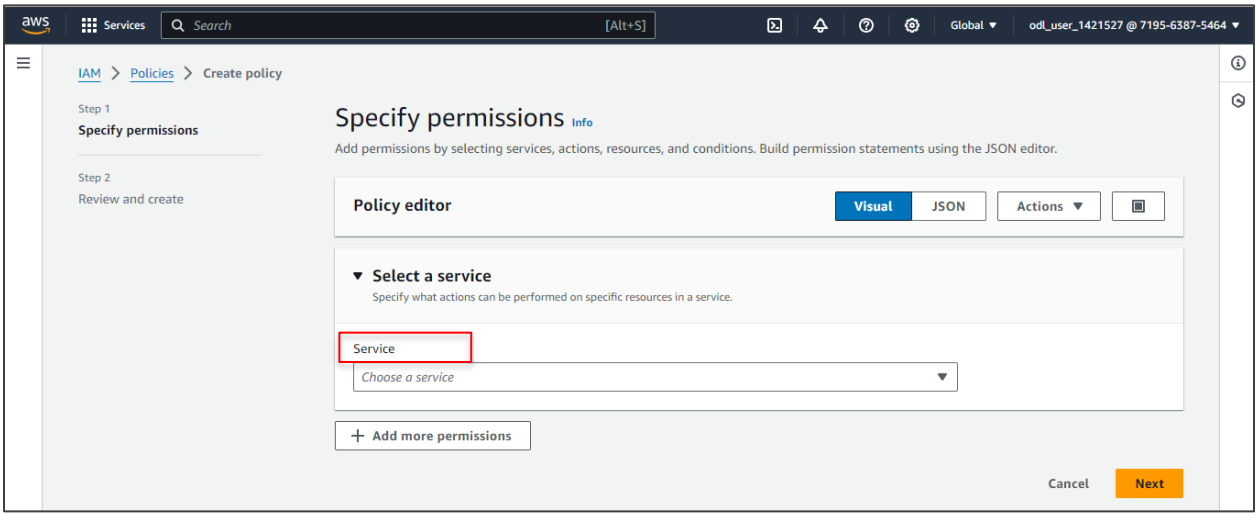
1.1 Navigate to the AWS Management Console, search for and select **IAM** in the search bar

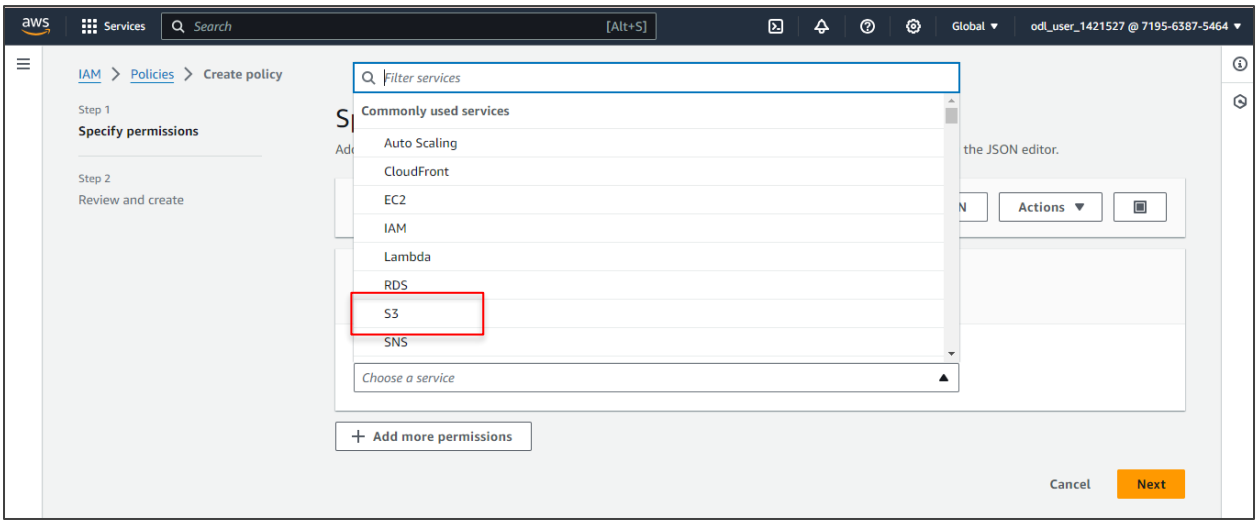


1.2 In the **IAM** dashboard, select **Policies** and click on **Create policy**

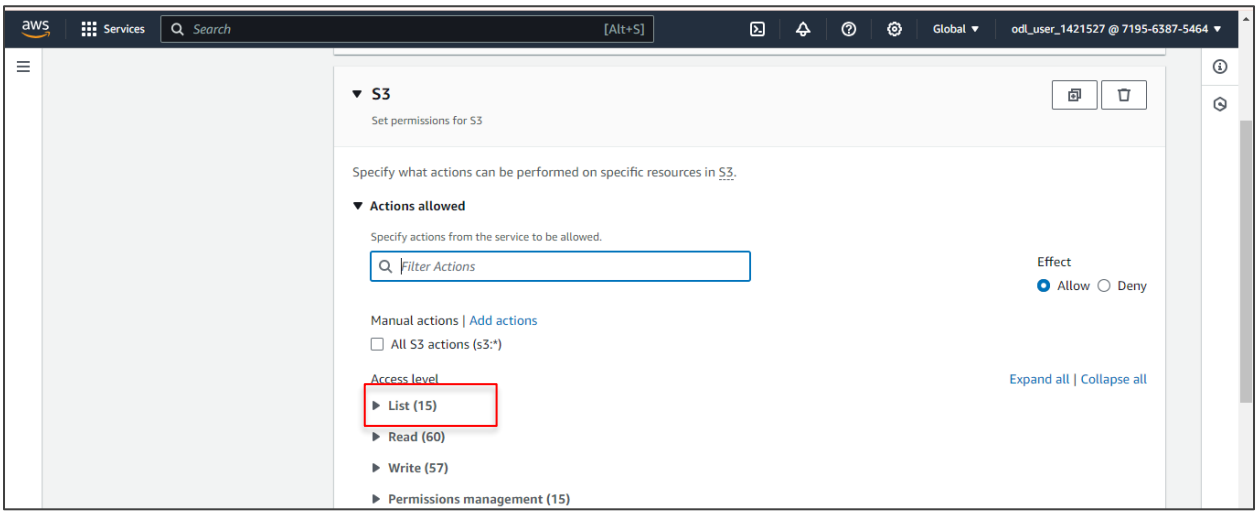


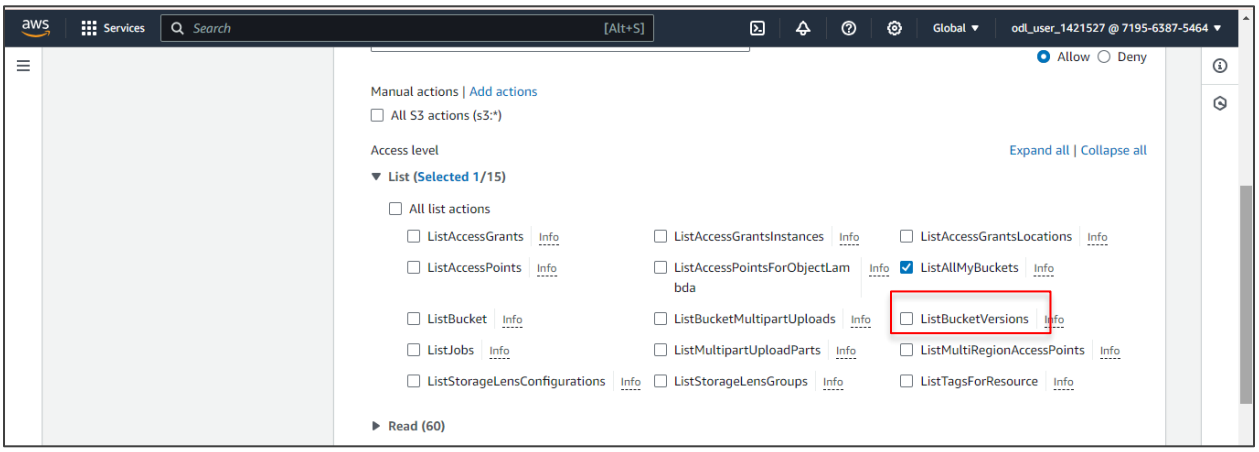
1.3 Select **S3** in the **Service** options



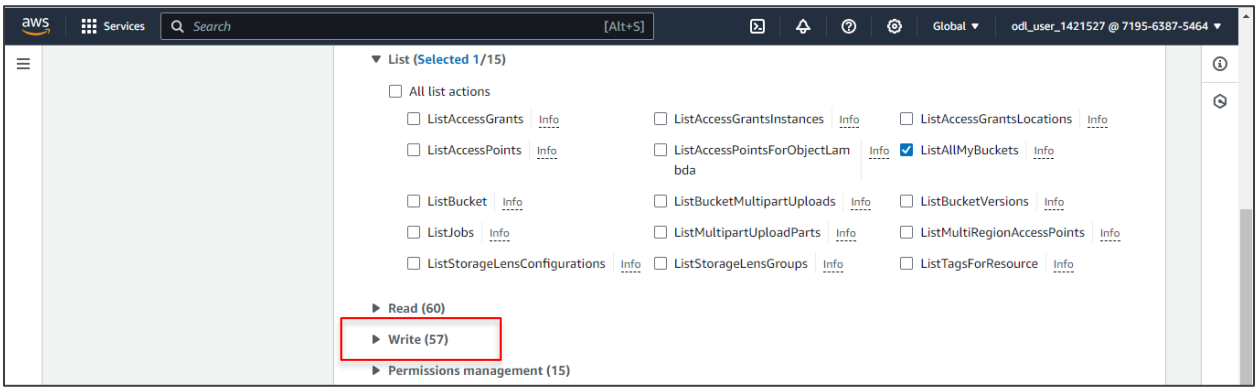


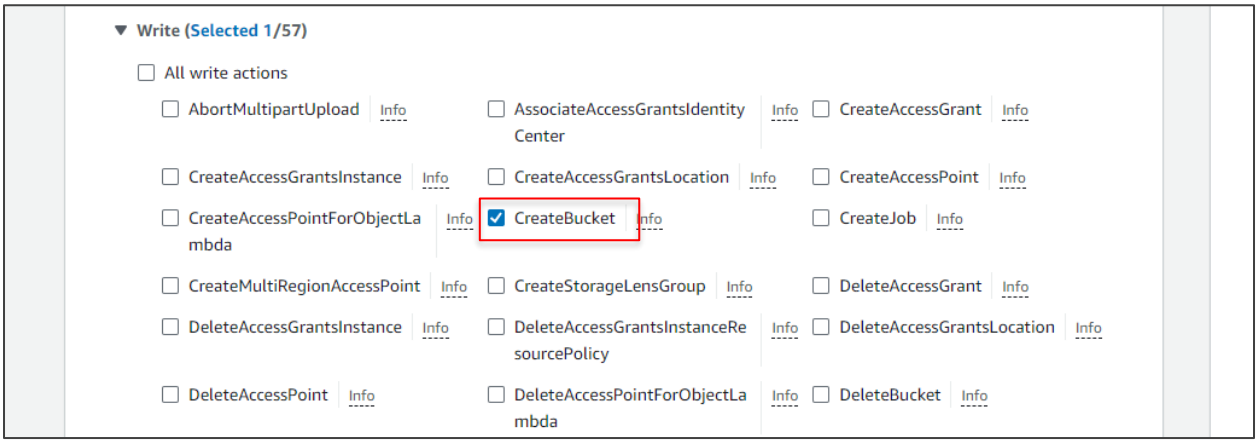
1.4 Choose **ListAllMyBuckets** from the **List** section in the **Access level**



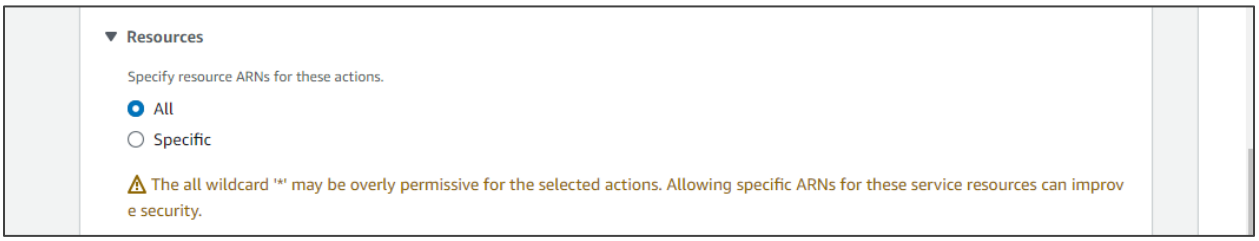


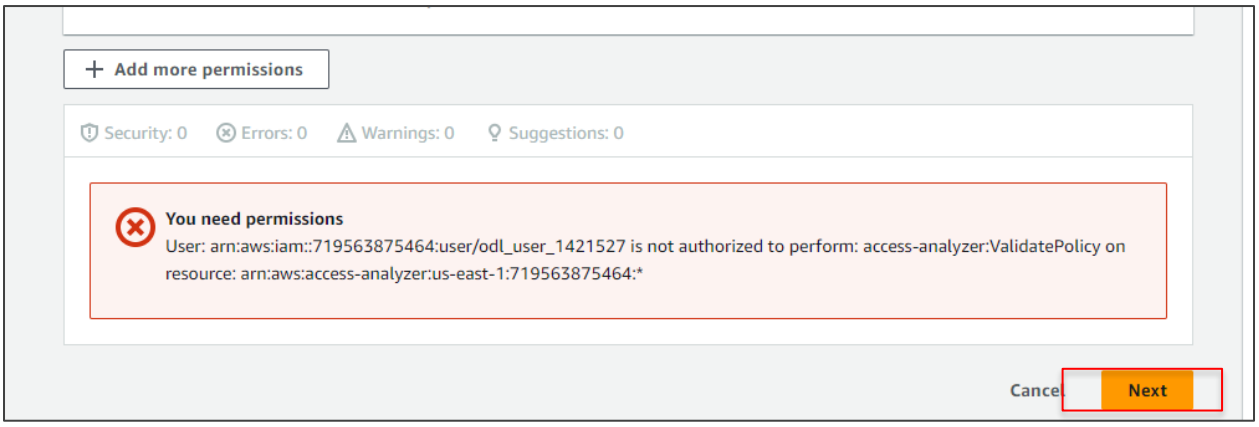
1.5 Choose **CreateBucket** from the **Write** section



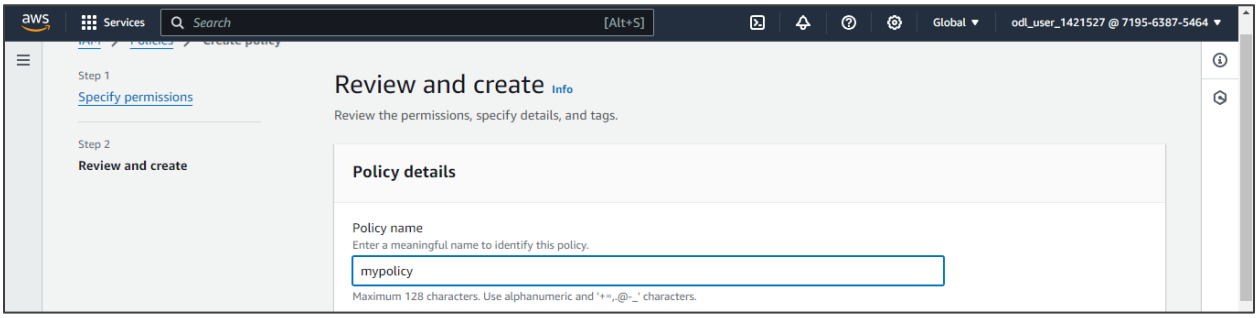


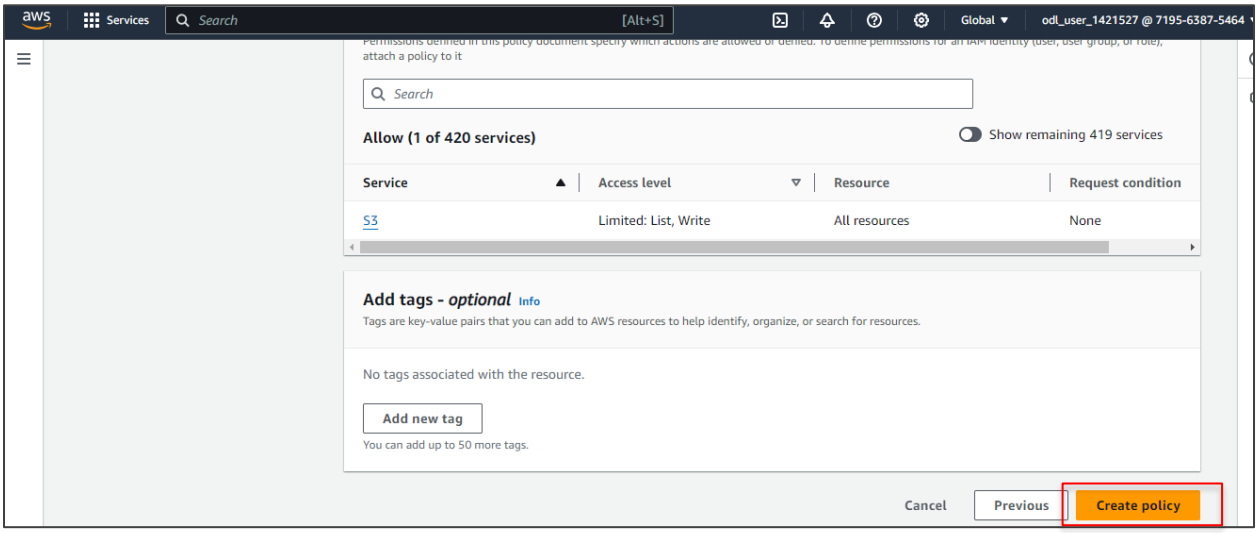
1.6 Scroll down to the **Resources** section, select **All**, and then click on **Next**

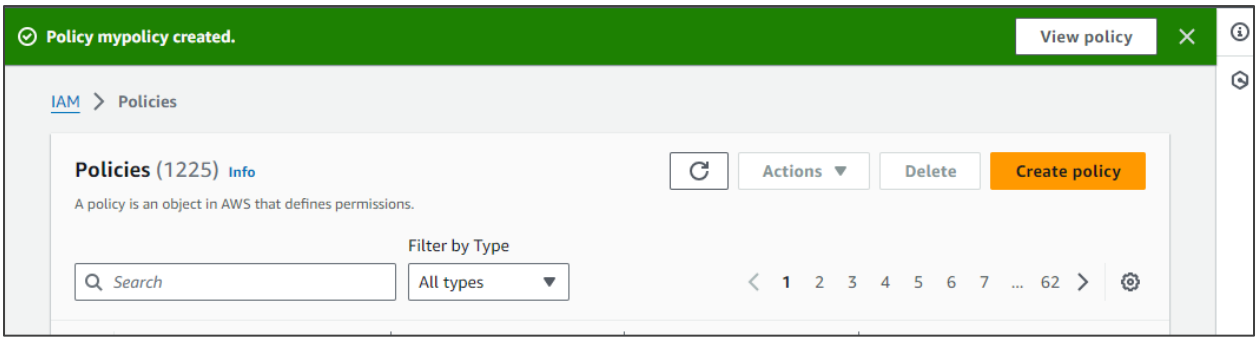




1.7 Enter your policy name and click on **Create policy**

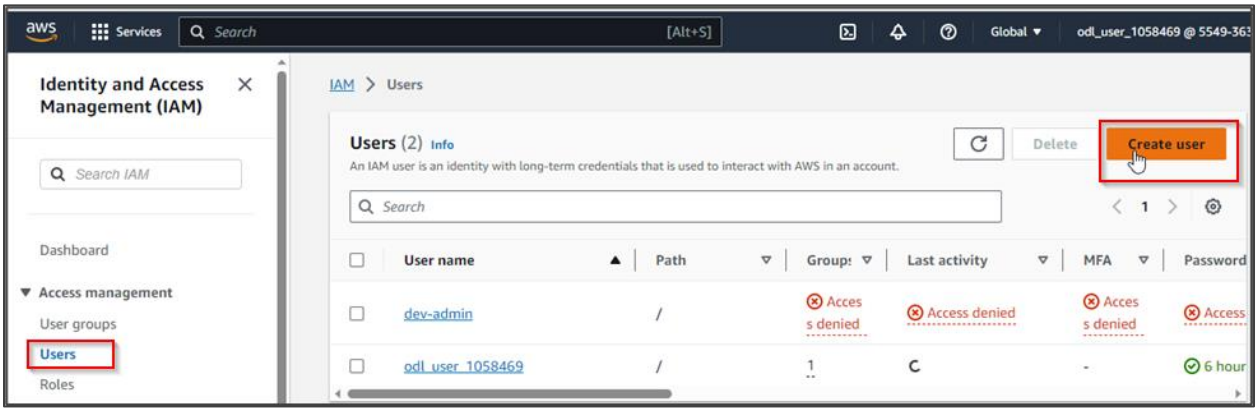




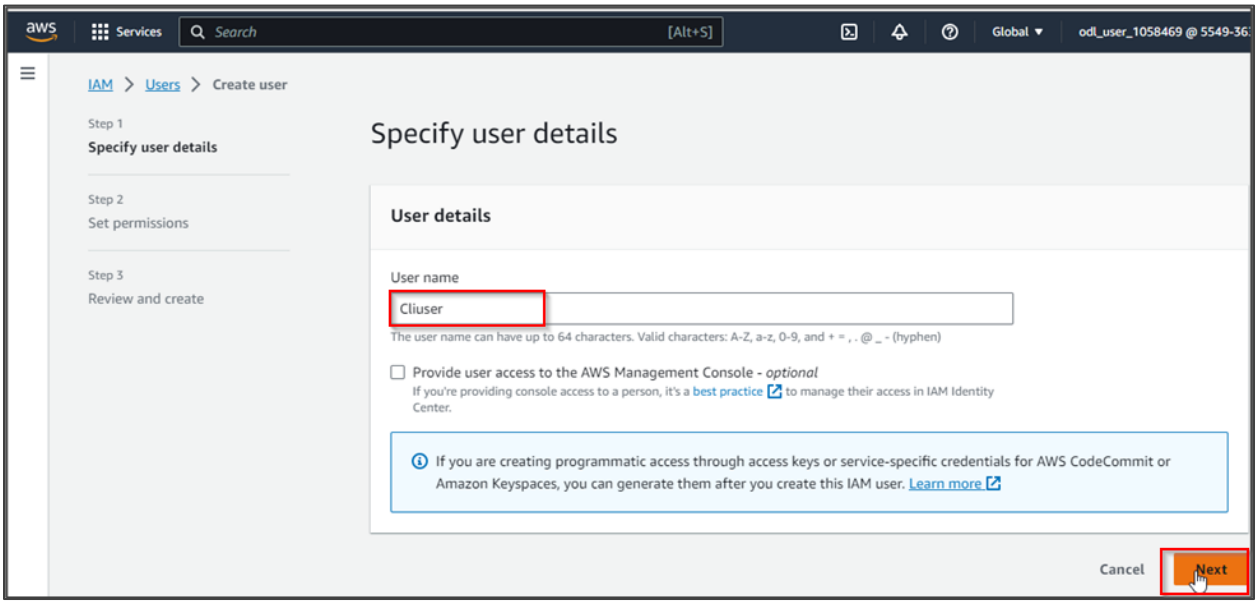


The policy is successfully created.

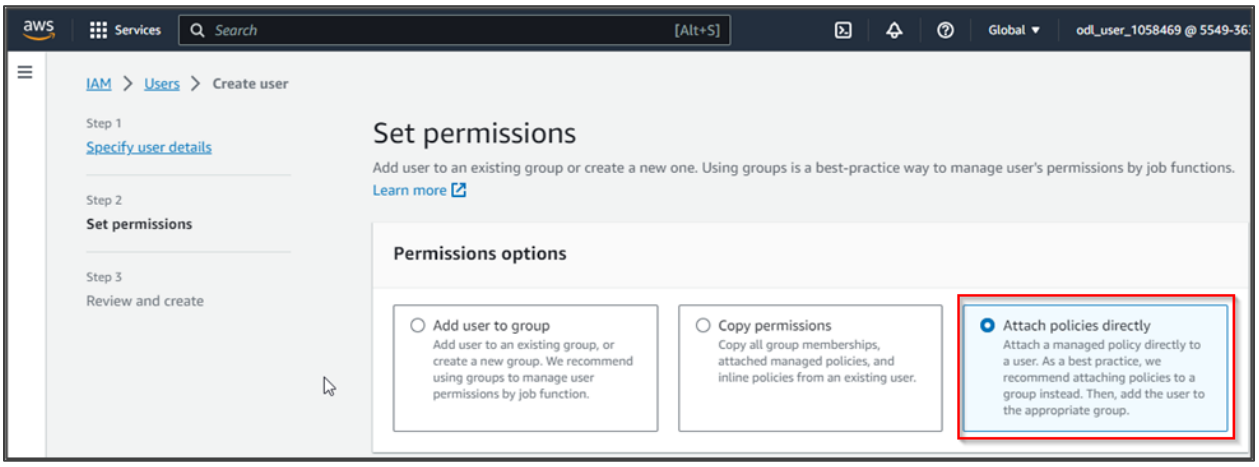
1.8 Navigate to the IAM dashboard, select **Users**, and click on **Create user**



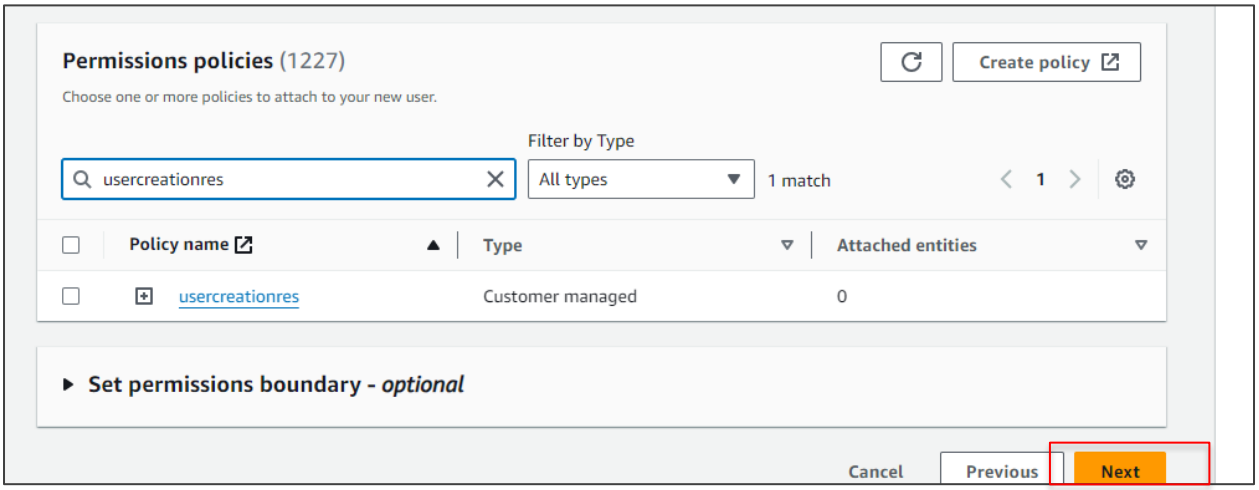
1.9 Provide a name to the user and click on **Next**



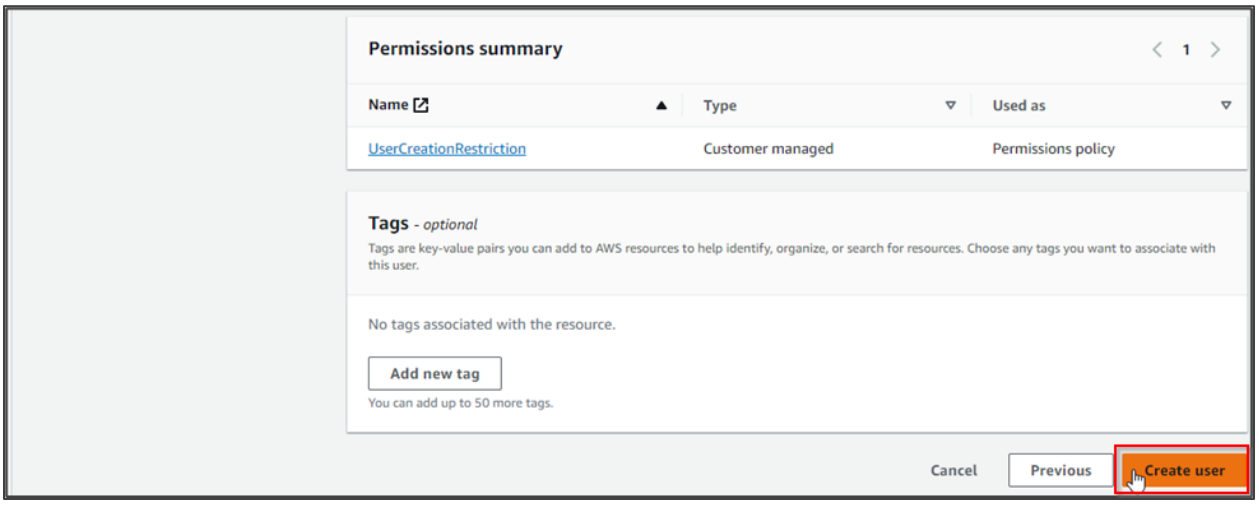
1.10 In the permissions page, select **Attach policies directly**

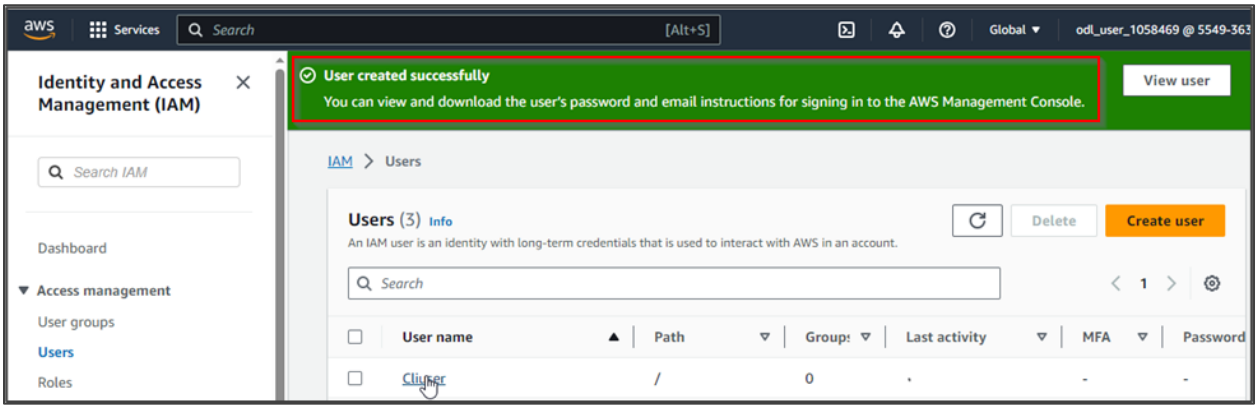


1.11 Select **usercreationres** policy from the list and then click on **Next**



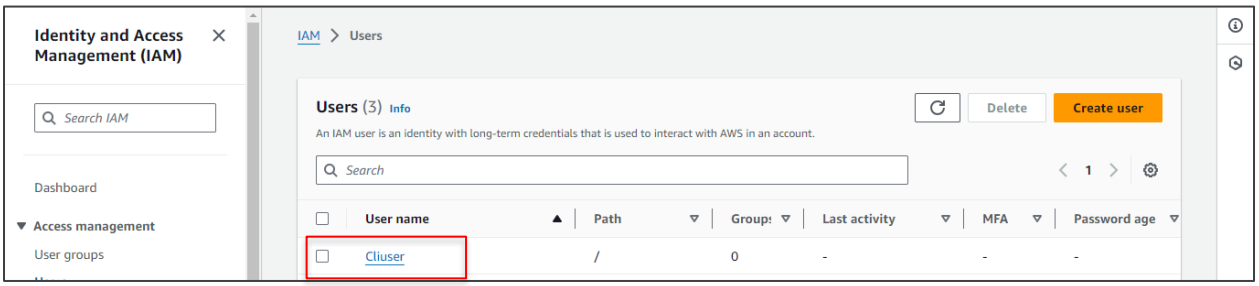
1.12 Click on **Create user**



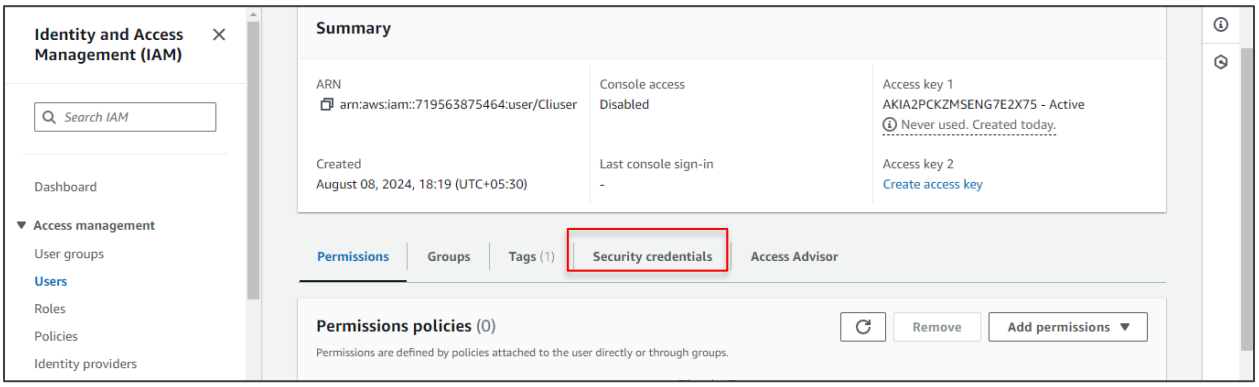


The user is successfully created.

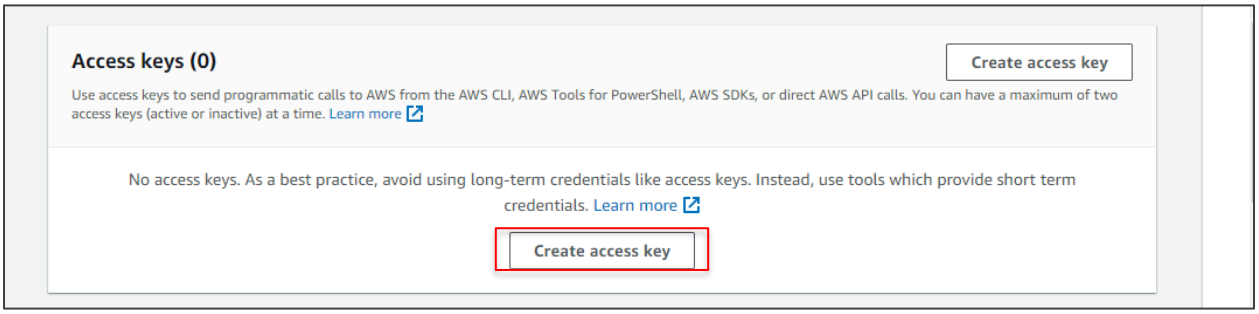
1.13 Click on the created user



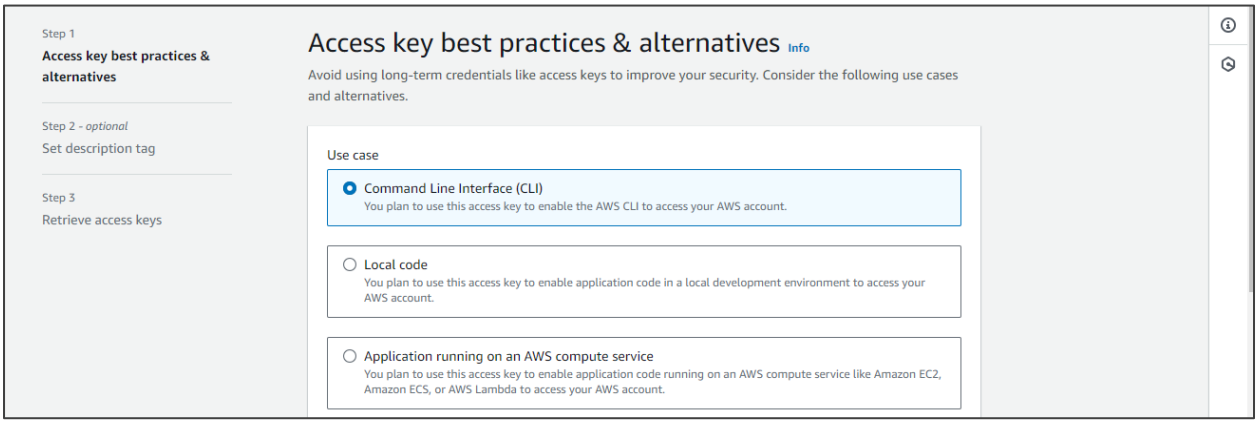
1.14 Select **Security credentials**



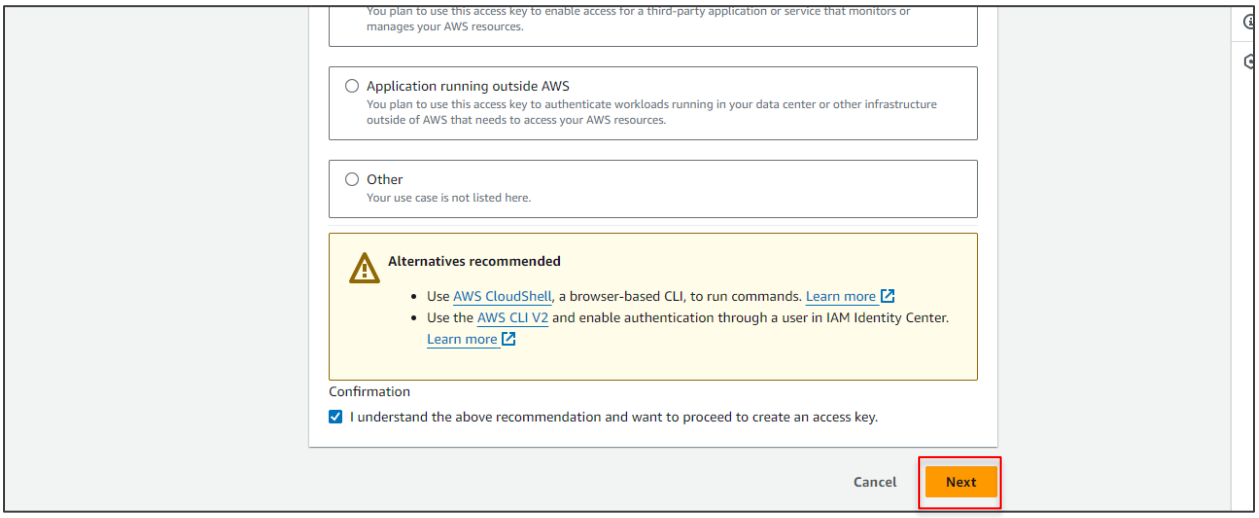
1.15 Scroll down and click on **Create access key**



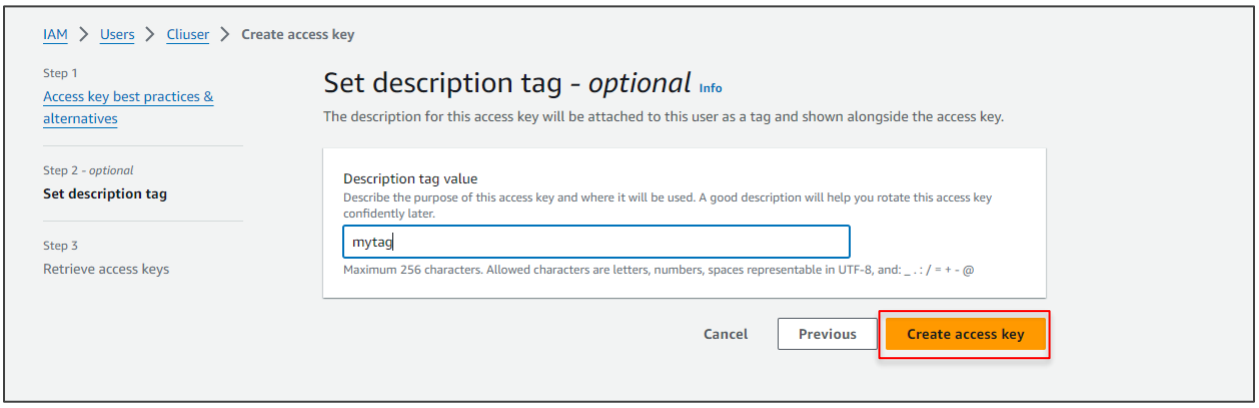
1.16 Select **Command Line Interface(CLI)** as Use case

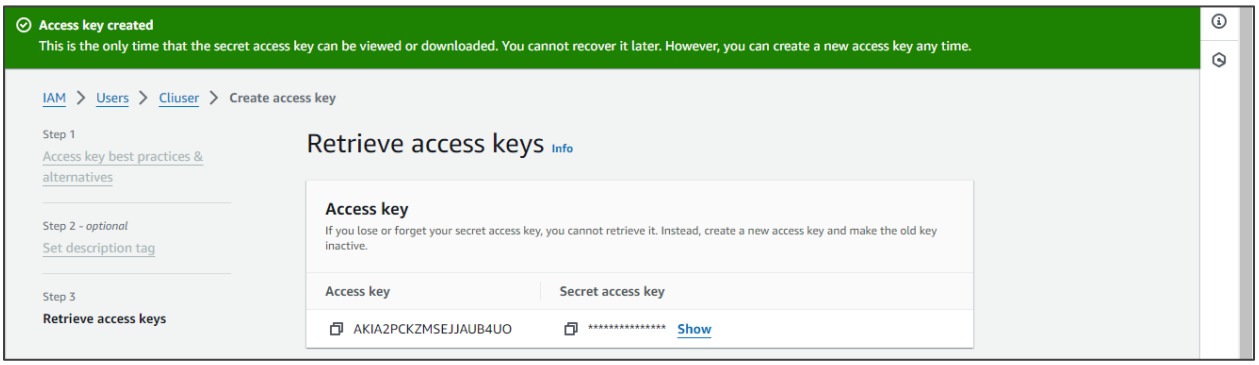


1.17 Scroll down, check the confirmation, and then click on **Next**



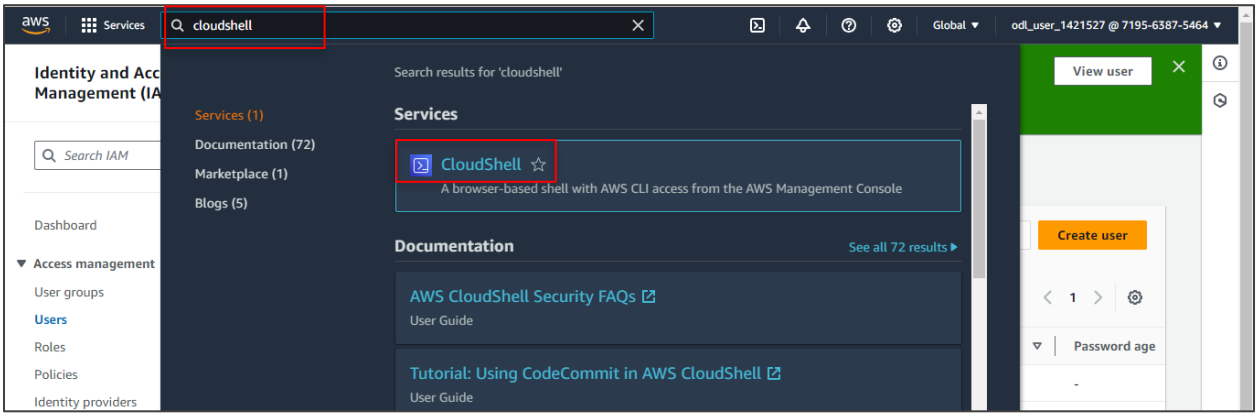
1.18 Enter your tag name and click on **Create access key**



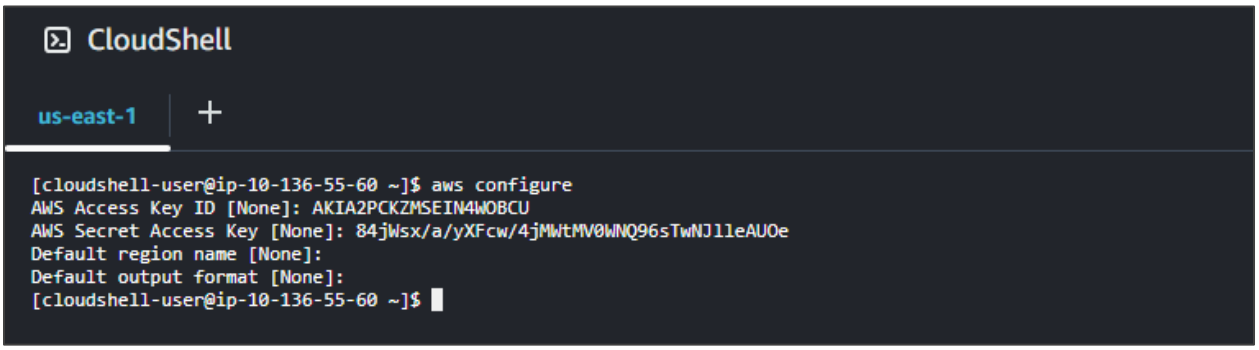


Make a note of the access key and secret key

1.19 Search and click on **CloudShell** to configure the user



1.20 Enter the command **aws configure**, then enter the Access Key ID, and the Secret Access Key

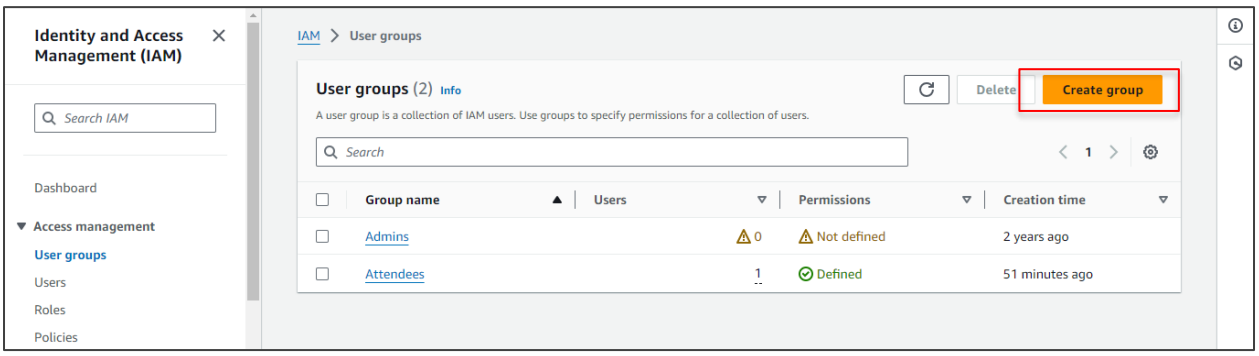


1.21 Use the following command to view the buckets in the account:
aws s3api list-buckets

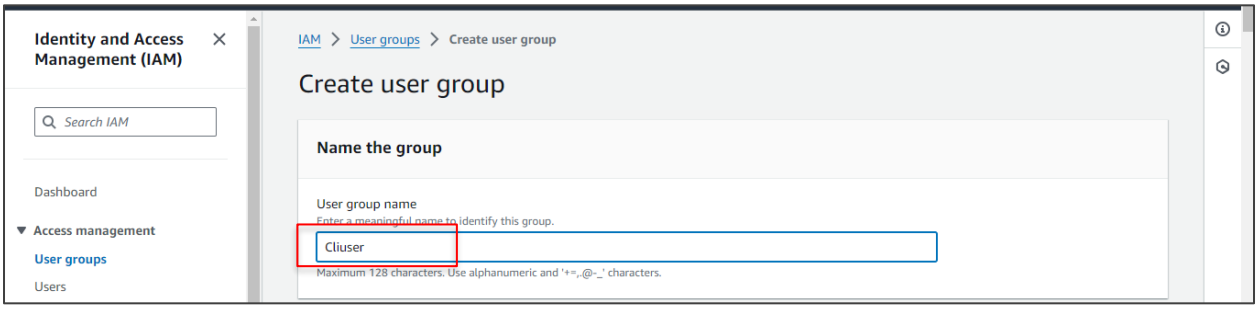
```
[cloudshell-user@ip-10-2-121-48 ~]$ aws s3api list-buckets
{
    "Buckets": [
        {
            "Name": "config-bucket-554936332221",
            "CreationDate": "2023-09-05T19:14:58+00:00"
        }
    ],
    "Owner": {
        "DisplayName": "simplilearnlabs138",
        "ID": "c5b1b62071b10455d245b195860383f520de51926755eba5d5a6d01cfc570b40"
    }
}
[cloudshell-user@ip-10-2-121-48 ~]$
```

Step 2: Attach policy and permissions directly to the group using group users

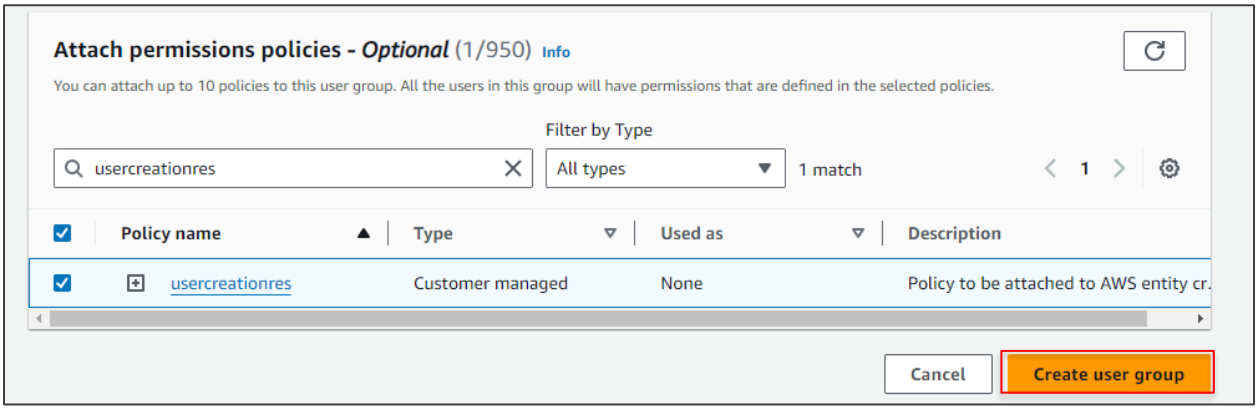
2.1 Select **User groups** and click on the **Create group** button

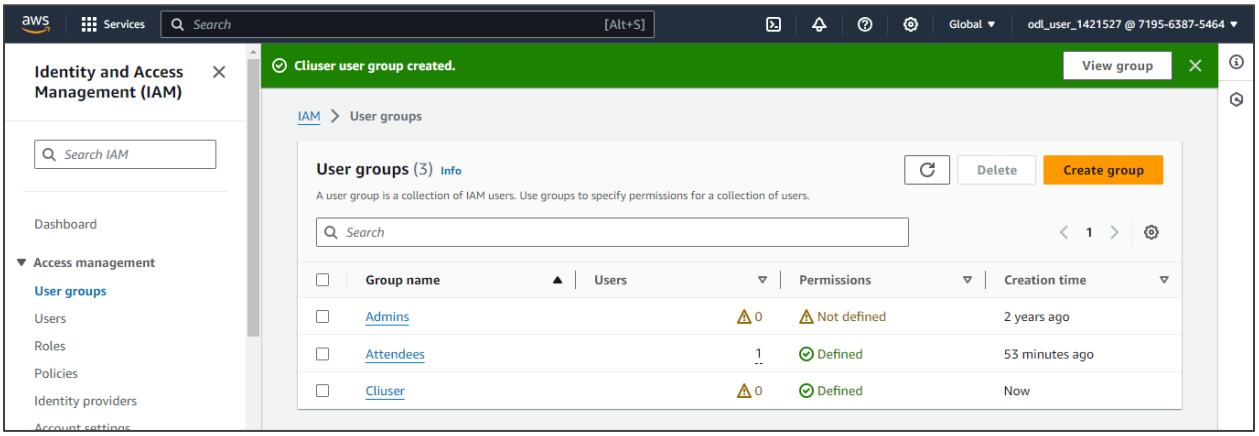


2.2 Enter **Cliuser** in the **User group name** field



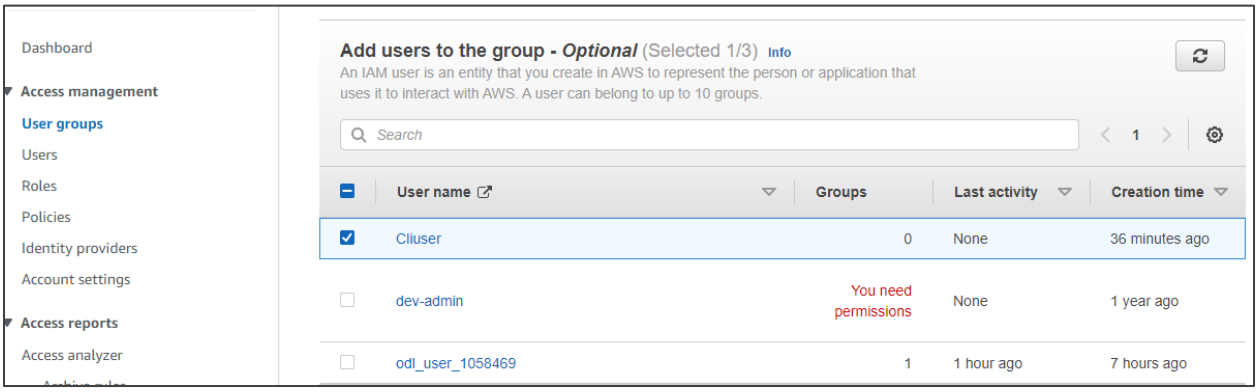
2.3 In the **Attach permissions policies** section, search for the **usercreationres** policy, select it, and then click on **Create user group**





The user group is created successfully.

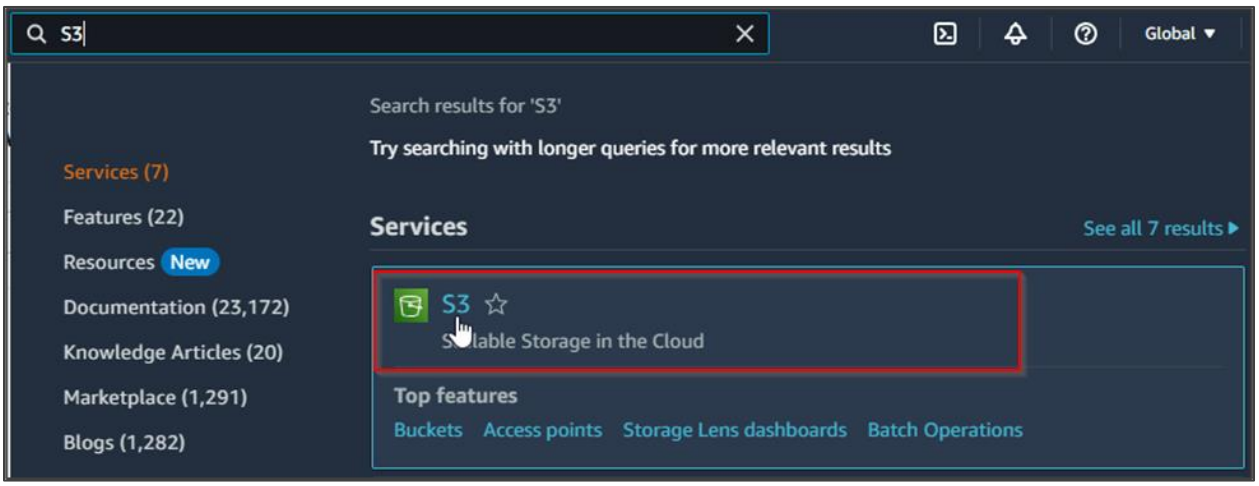
2.4 Under **User groups**, select **Cliuser** and click on the **Add users** button



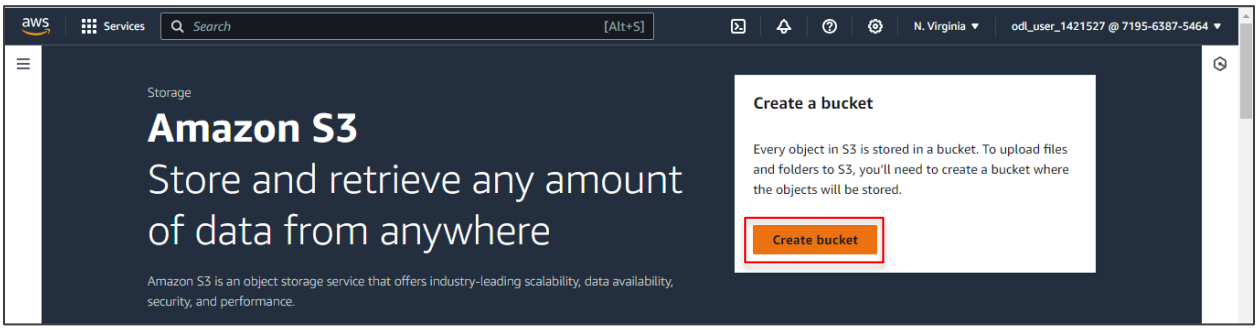
This will add the selected user to the group.

Step 3: Create and manage S3 versioning

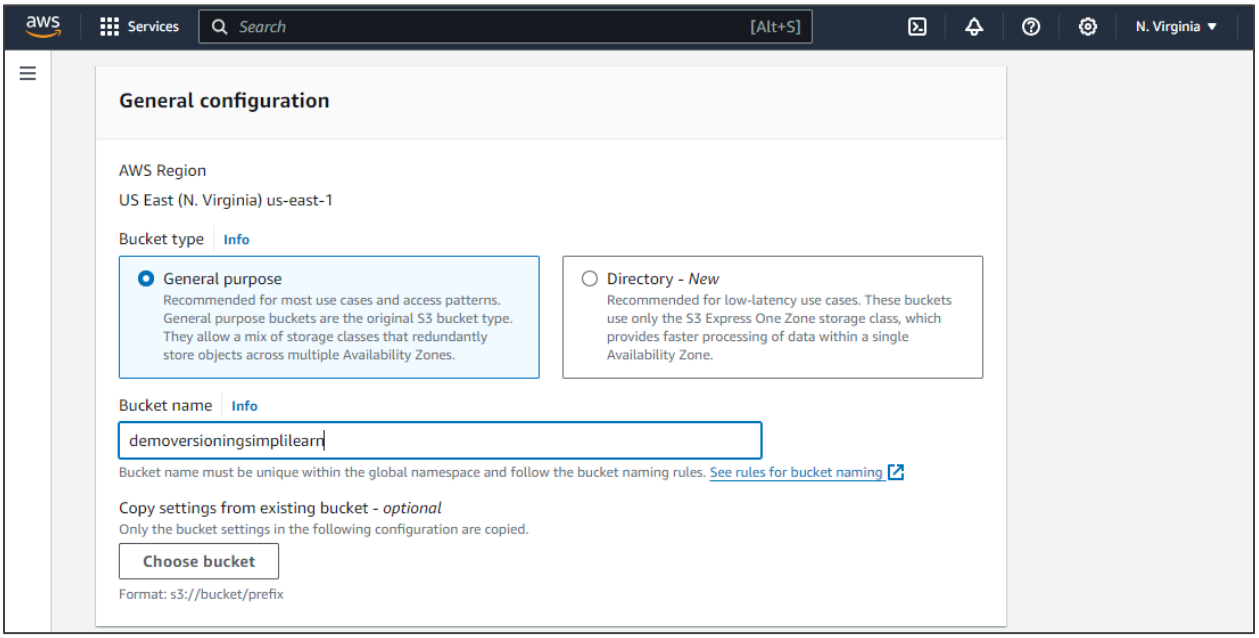
3.1 Search for and select **S3** from the services

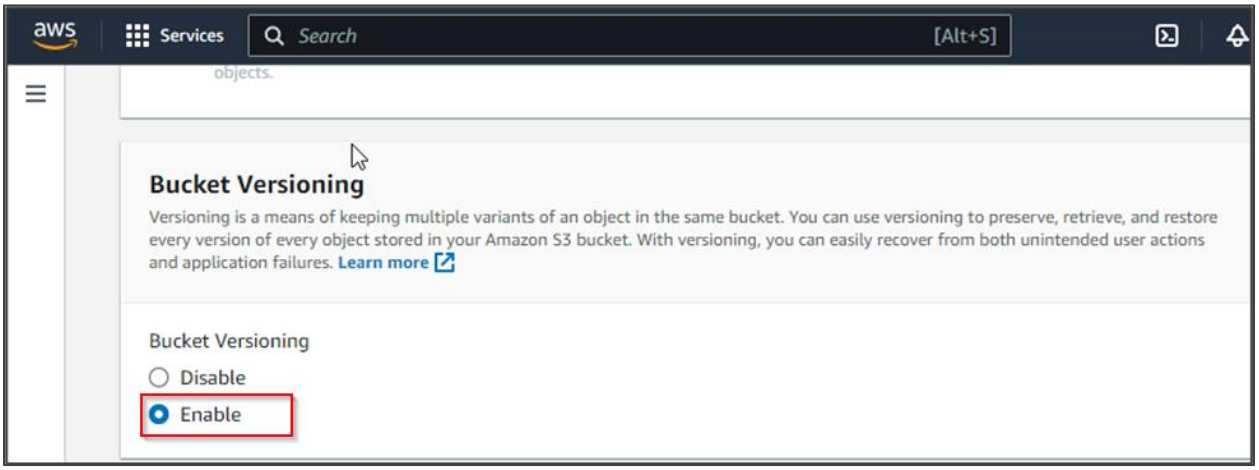


3.2 Click on the **Create bucket** button

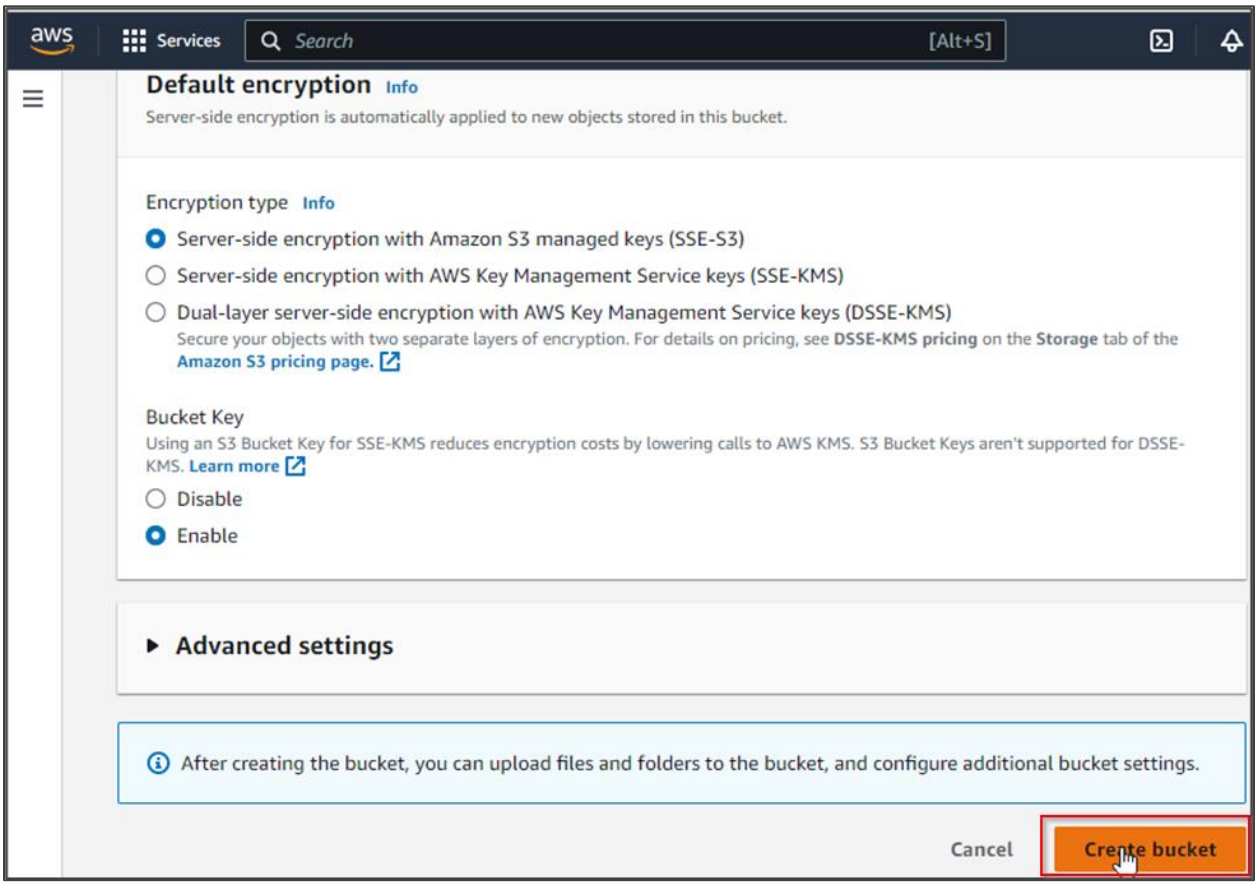


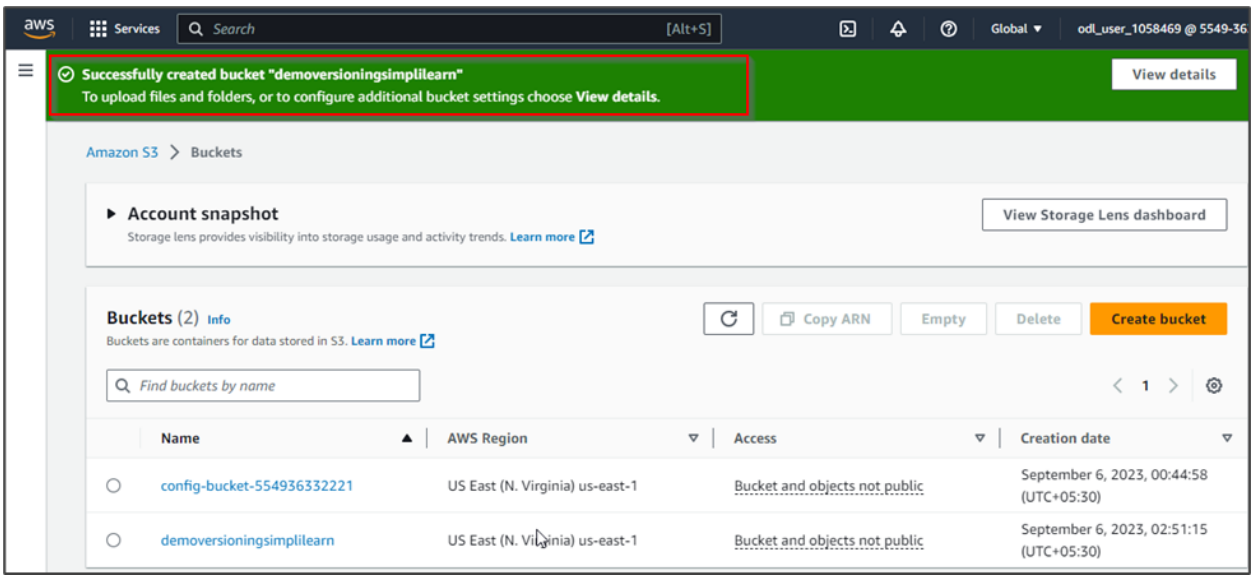
3.3 Add the bucket name, select **US East (N. Virginia) us-east-1** from the AWS Region drop-down, and click on **Enable** in the **Bucket Versioning** section





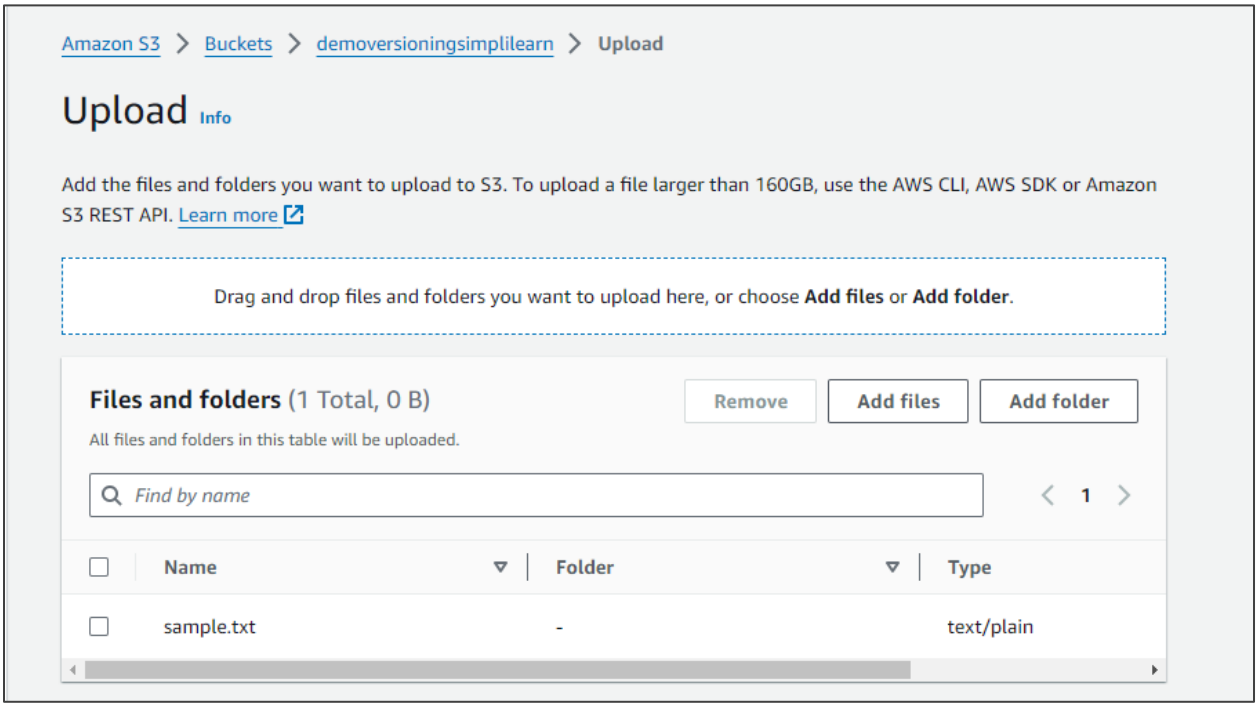
3.4 Click on the **Create bucket** button



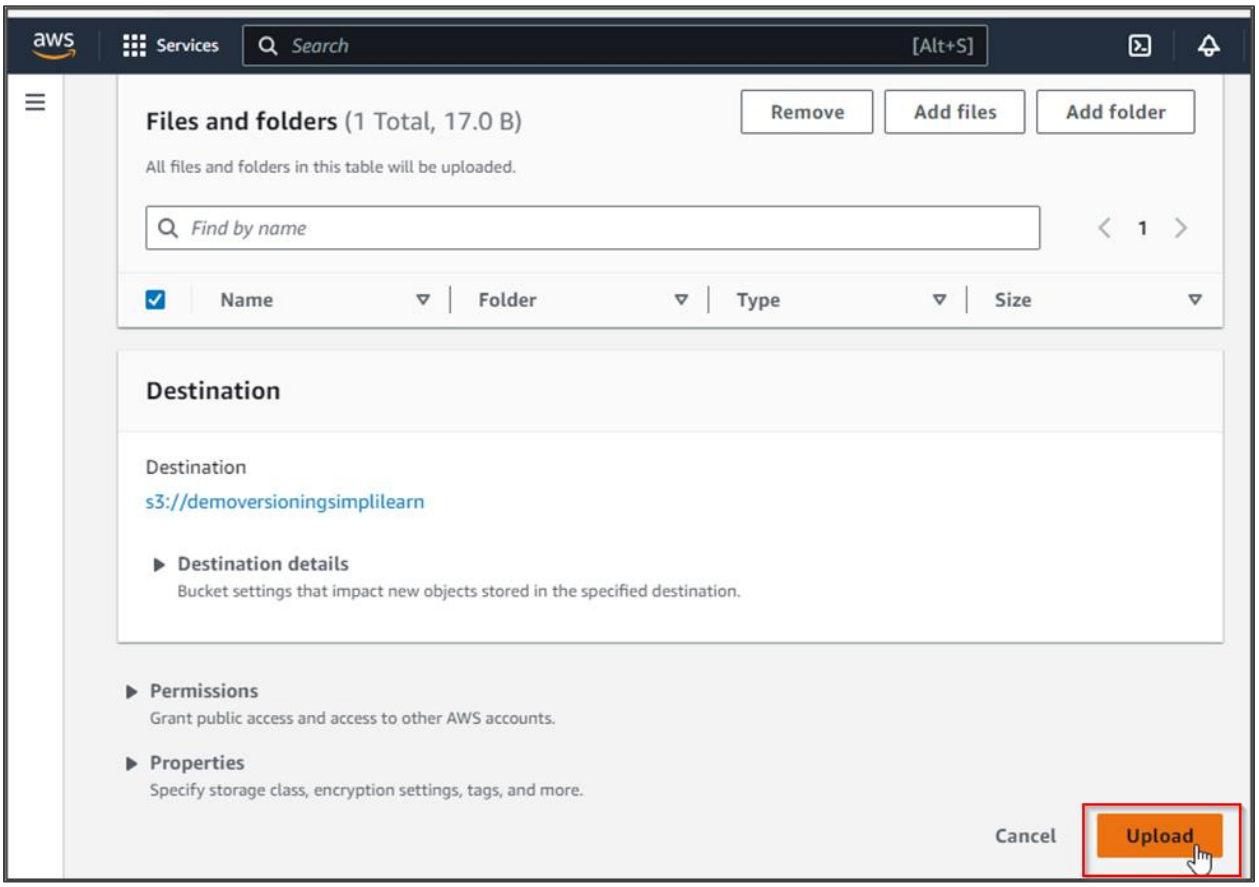


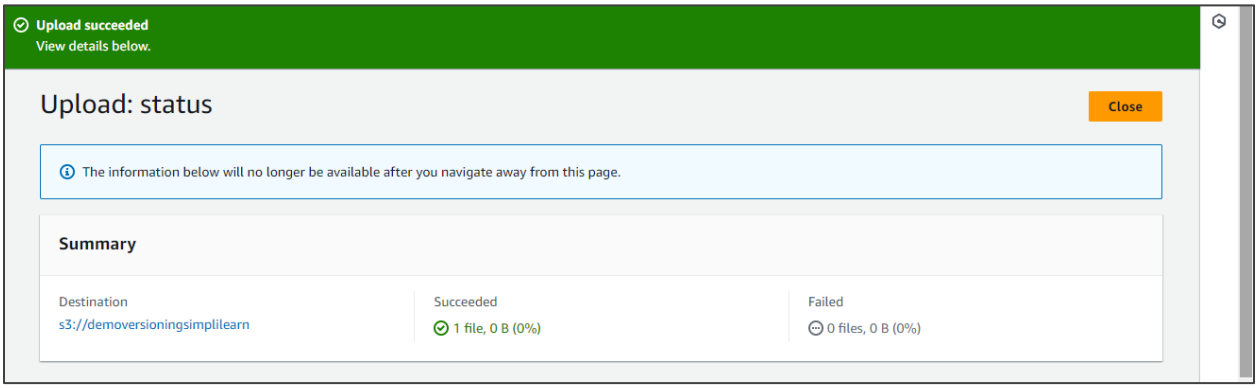
The bucket is created successfully.

3.5 Click on the bucket that you created and in the Objects section, upload a simple txt file as shown below:



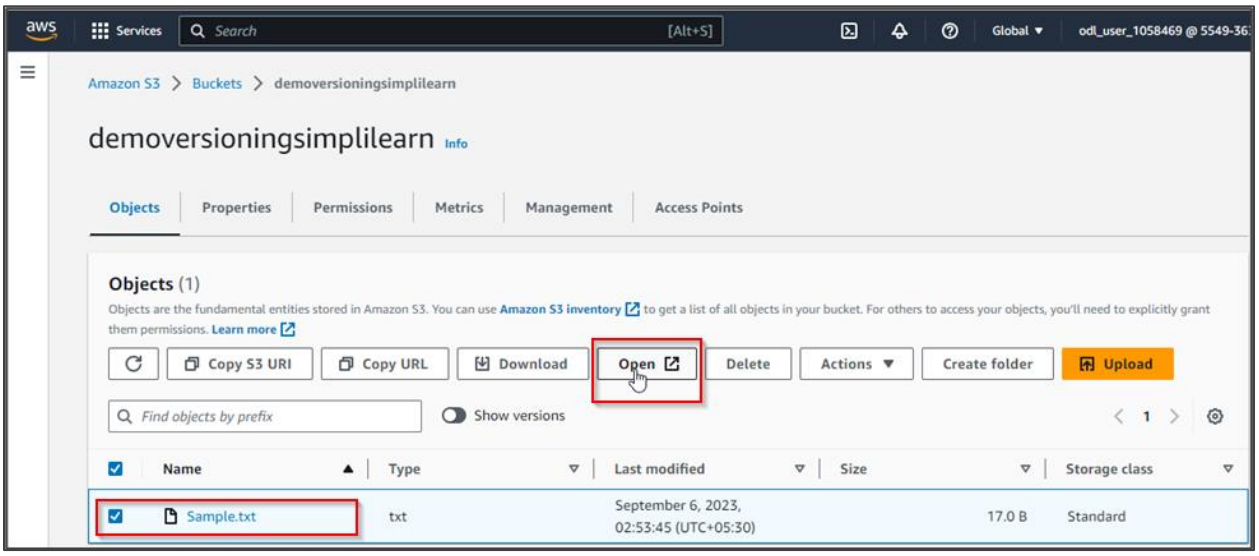
3.6 Click on the **Upload** button





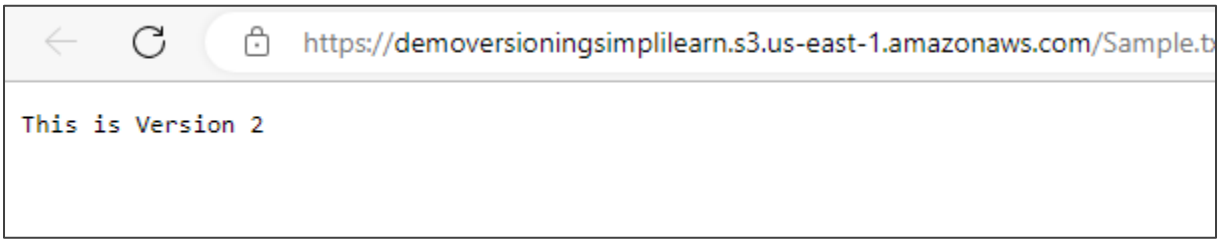
The file is successfully uploaded.

3.7 Select the text file and click on **Open**



3.8 The output will be displayed as follows:

3.9 Edit the text file, save it, and then re-upload the file. The updated output will appear as follows:



By following these steps, you have successfully created and added a policy to the group using a user to enable security management in various systems and applications.