

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

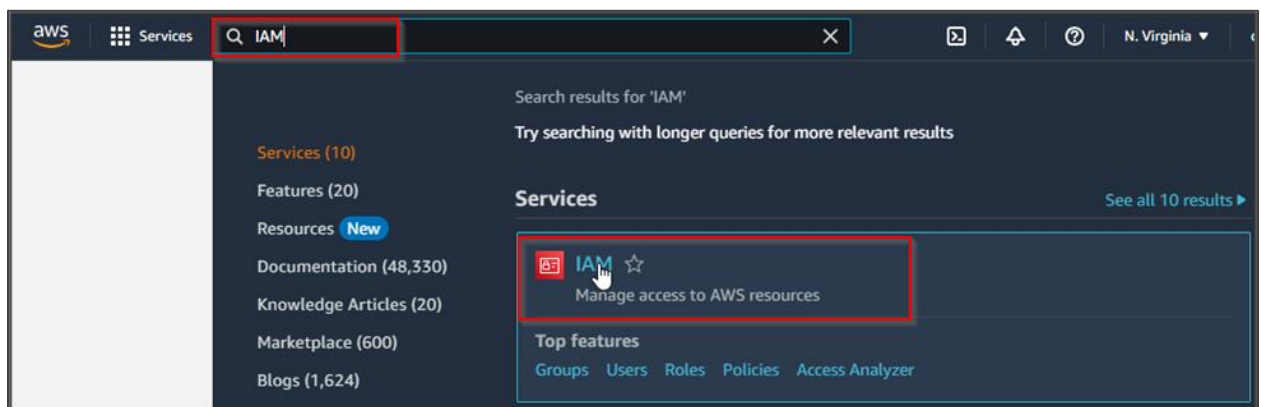
Prerequisites: None

Steps to be followed:

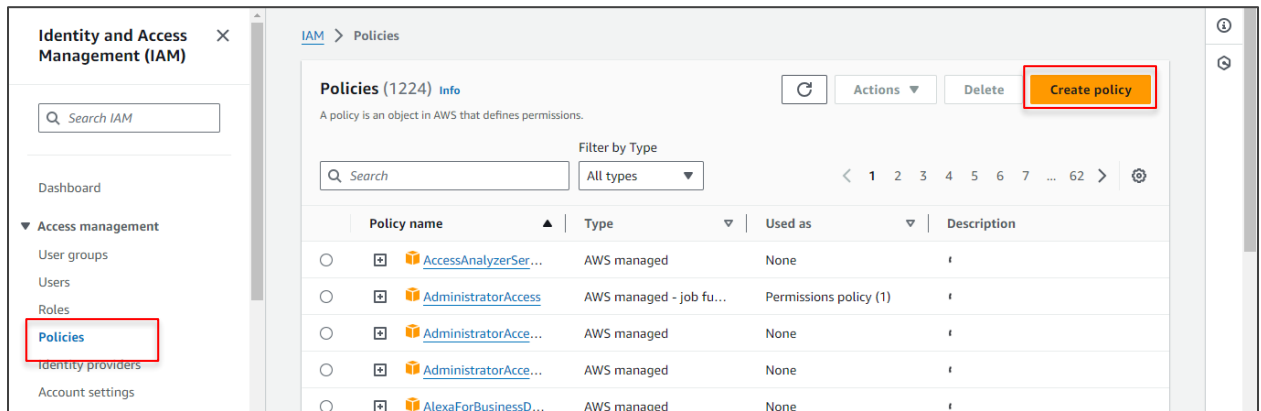
1. Create and manage policy
2. Attach policy and permissions directly to the group using group users
3. Create and manage S3 versioning

Step 1: Create and manage policy

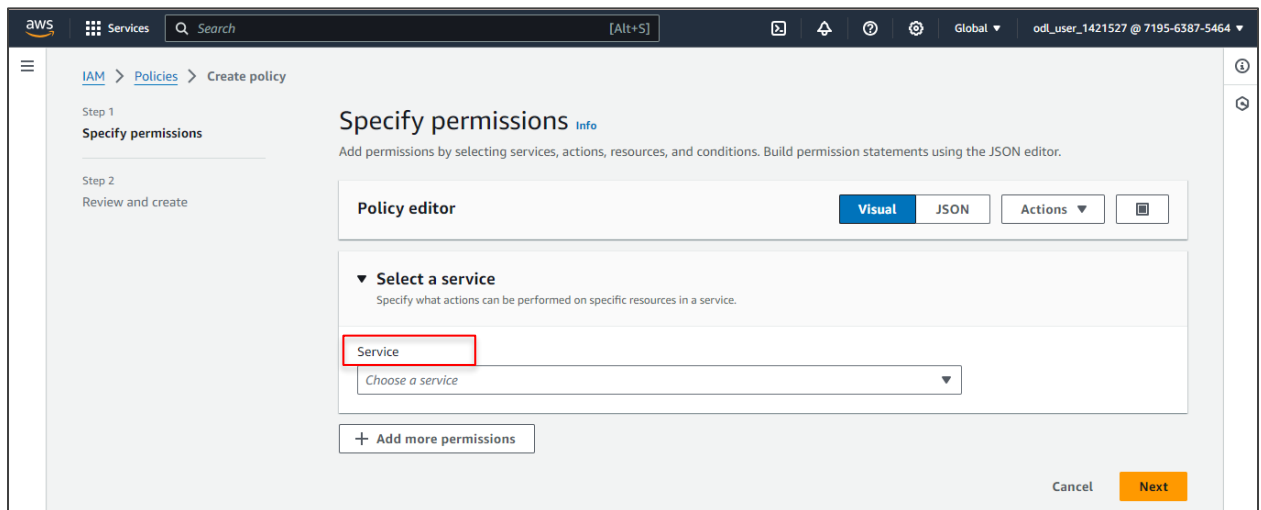
1.1 Navigate to the AWS Management Console, search for and select **IAM** in the search bar

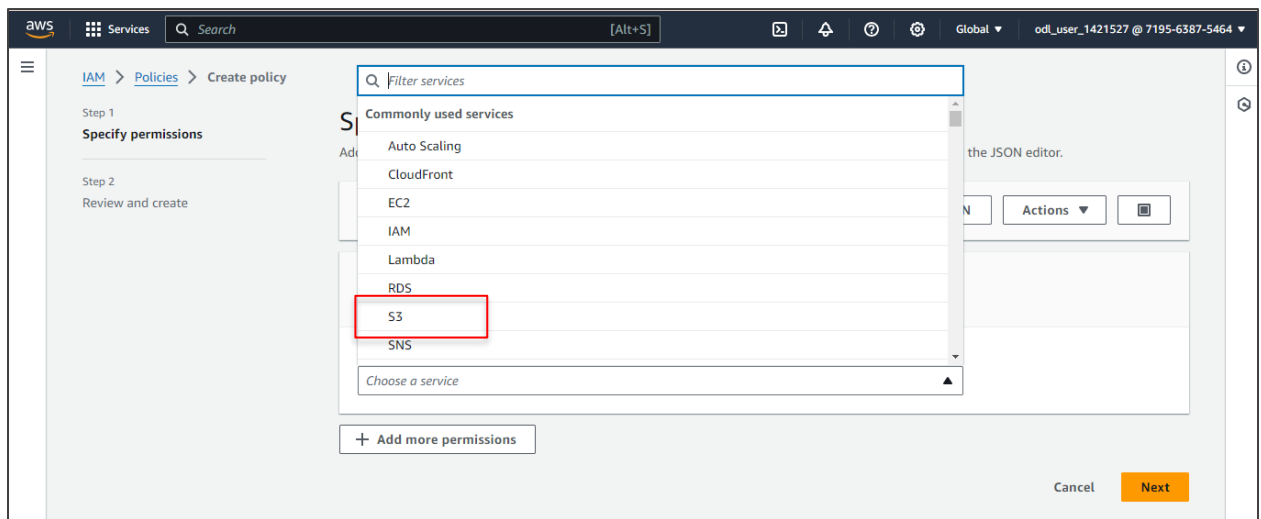


1.2 In the IAM dashboard, select **Policies** and click on **Create policy**

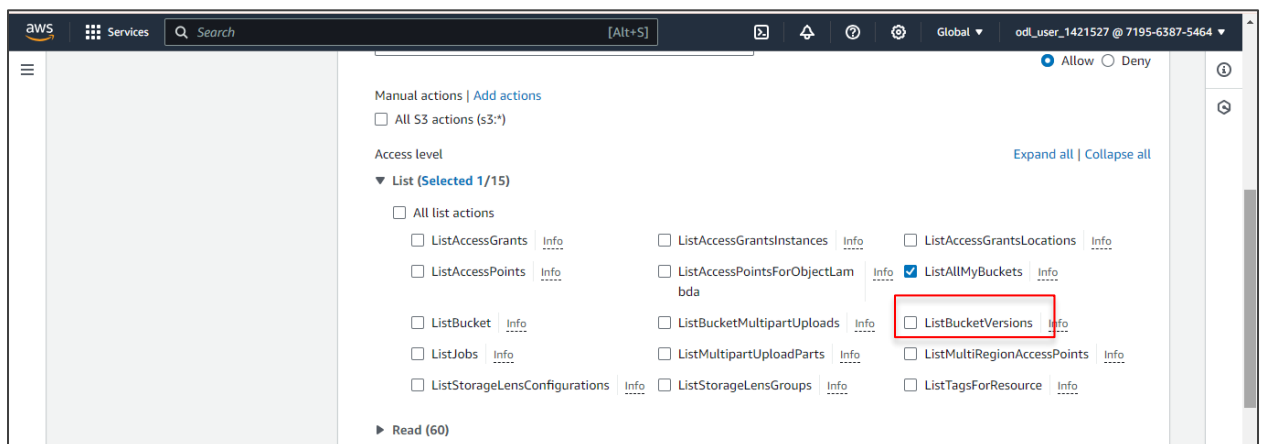
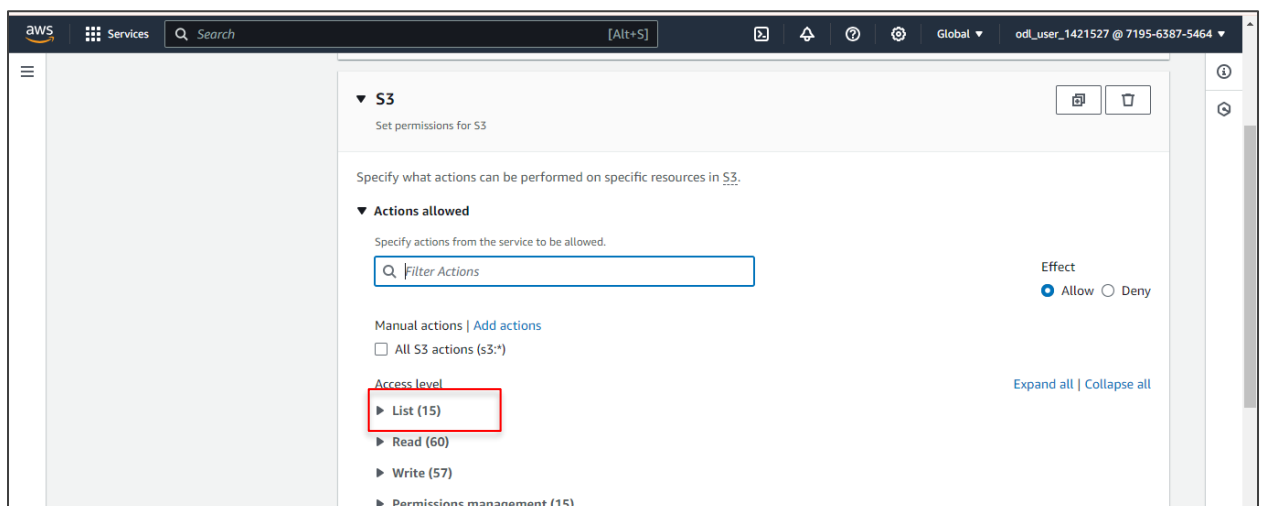


1.3 Select **S3** in the **Service** options

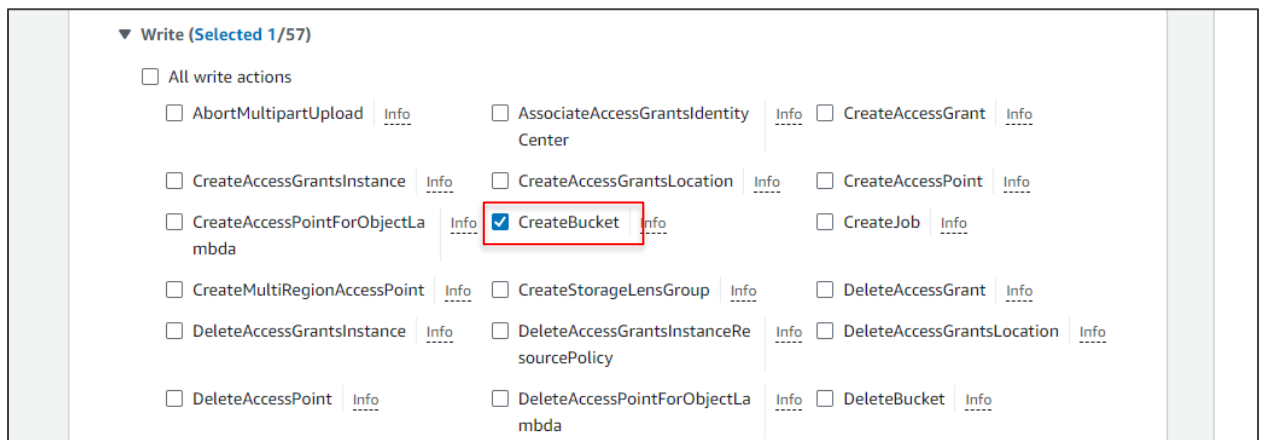
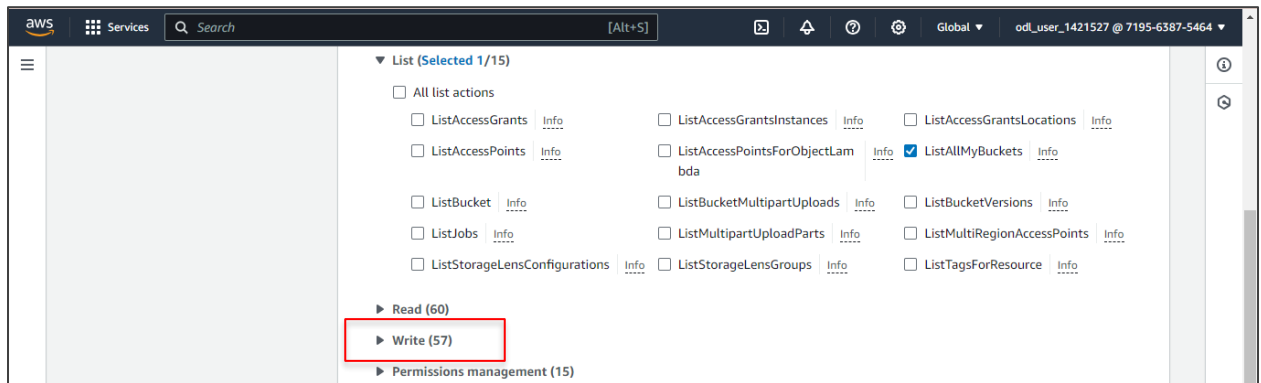




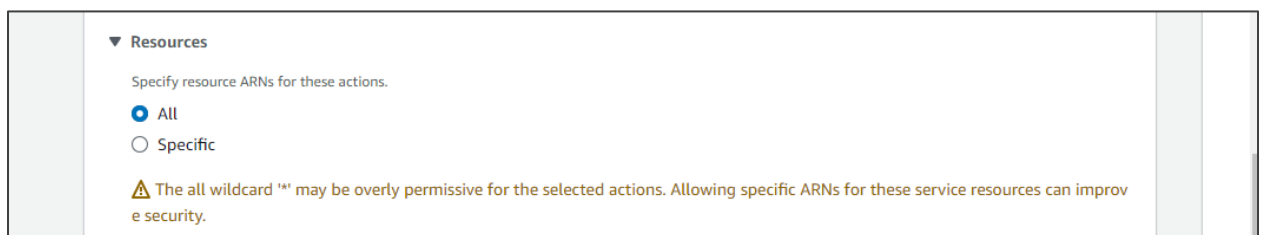
1.4 Choose **ListAllMyBuckets** from the **List** section in the **Access level**

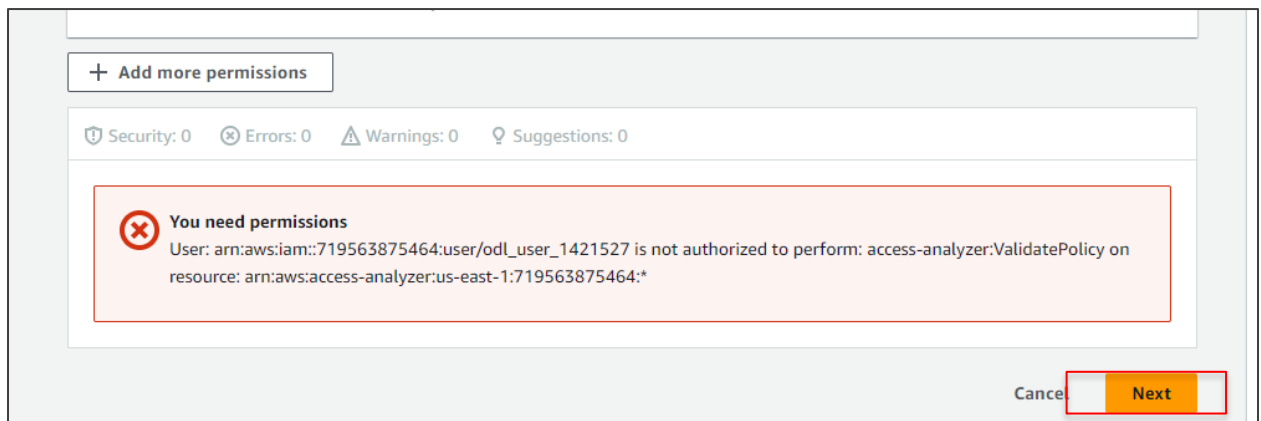


1.5 Choose **CreateBucket** from the **Write** section

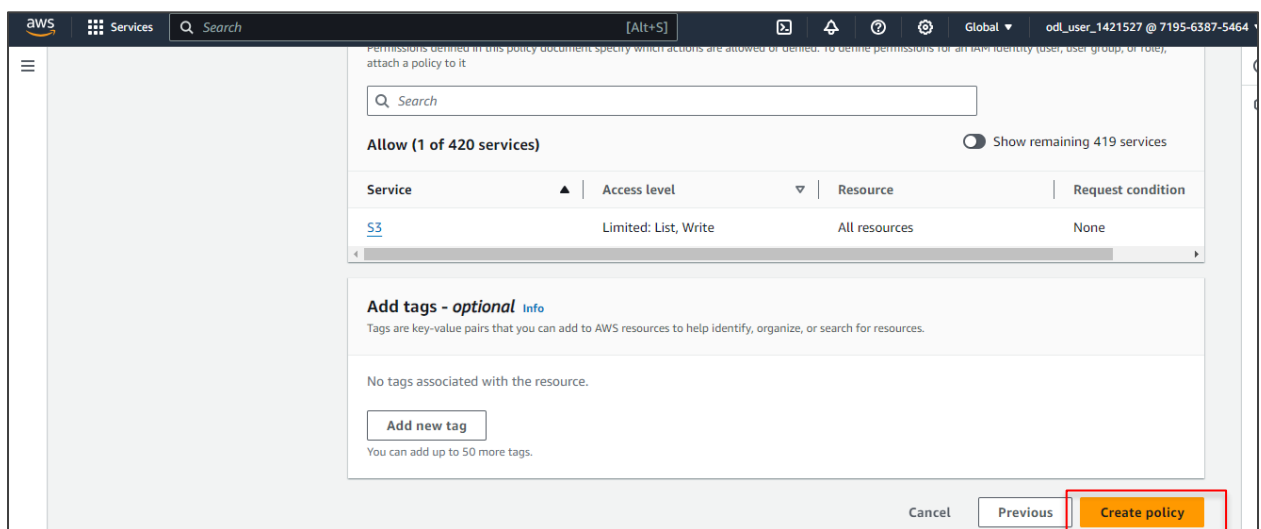
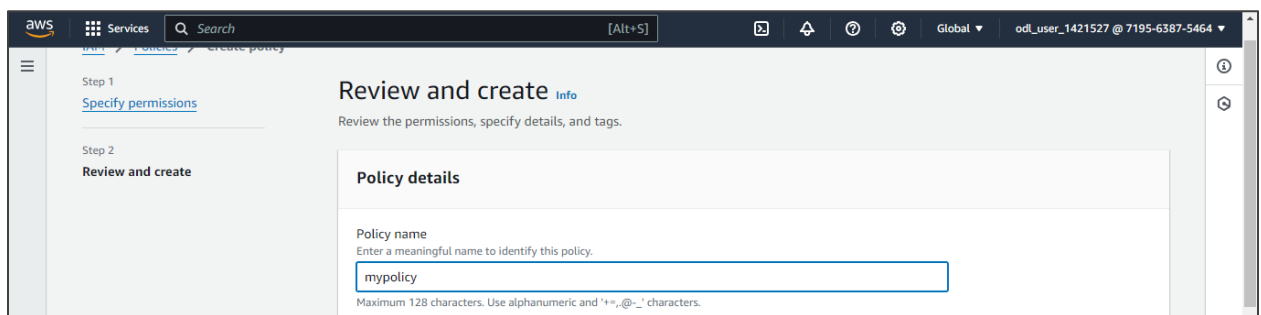


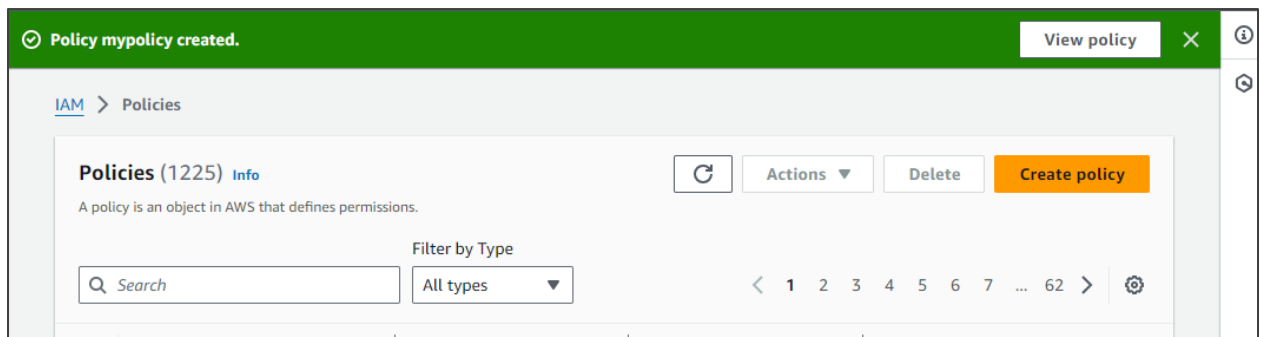
1.6 Scroll down to the **Resources** section, select **All**, and then click on **Next**





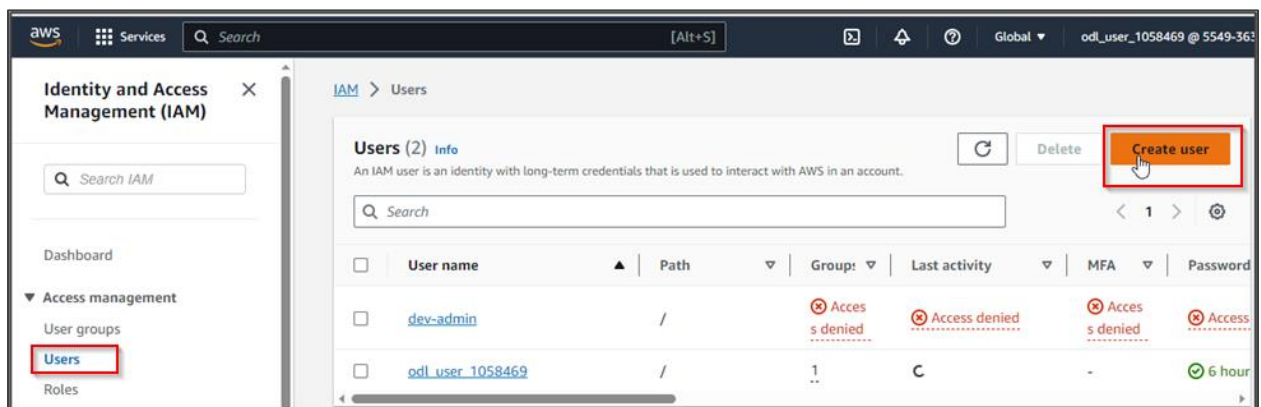
1.7 Enter your policy name and click on **Create policy**



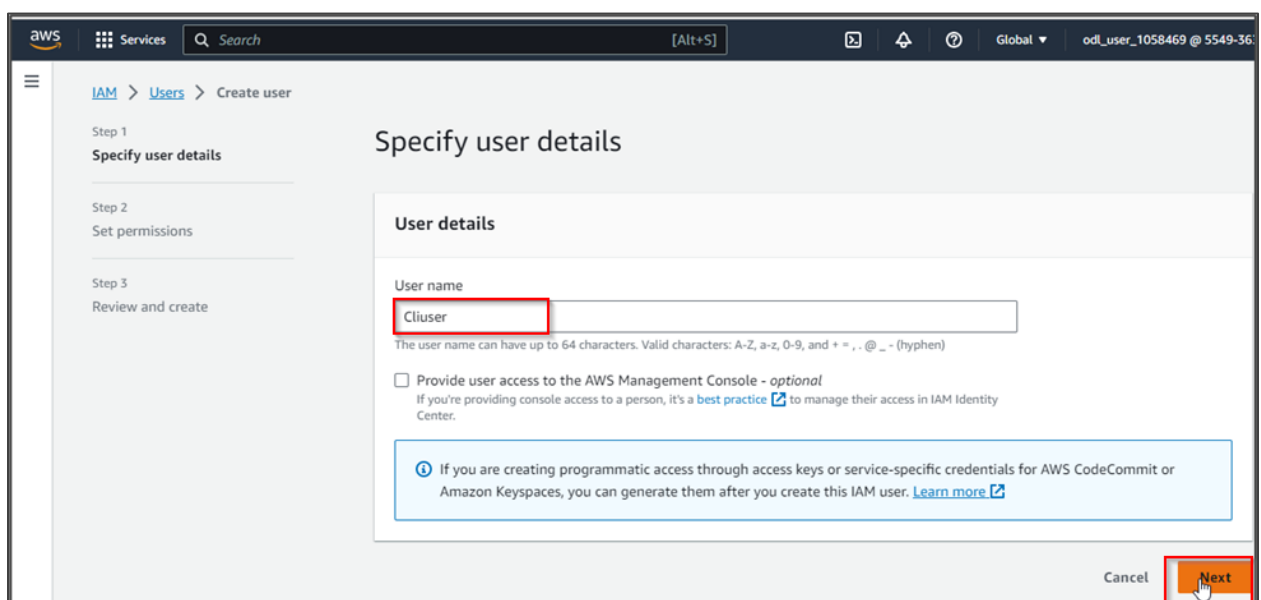


The policy is successfully created.

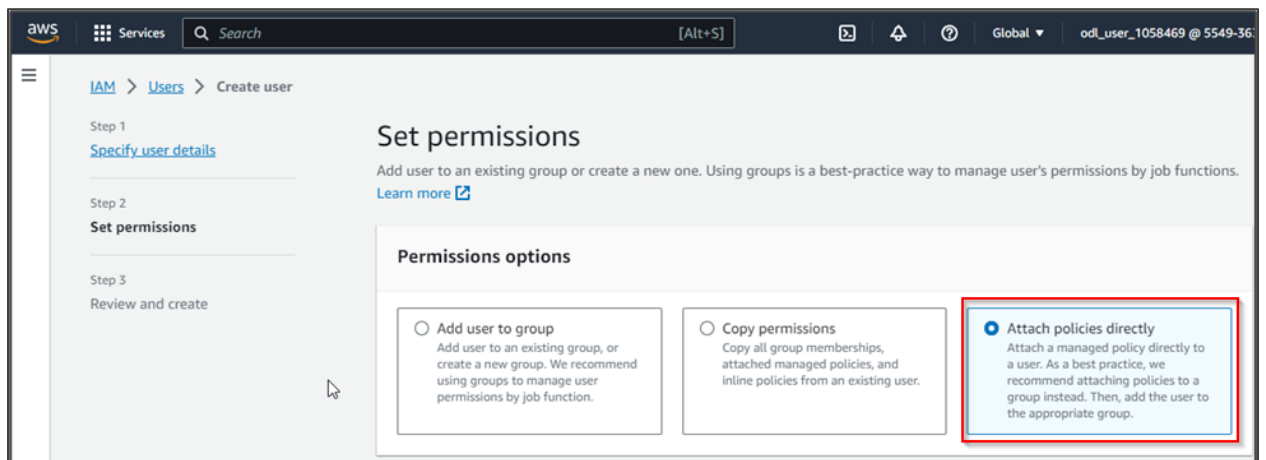
1.8 Navigate to the IAM dashboard, select **Users**, and click on **Create user**



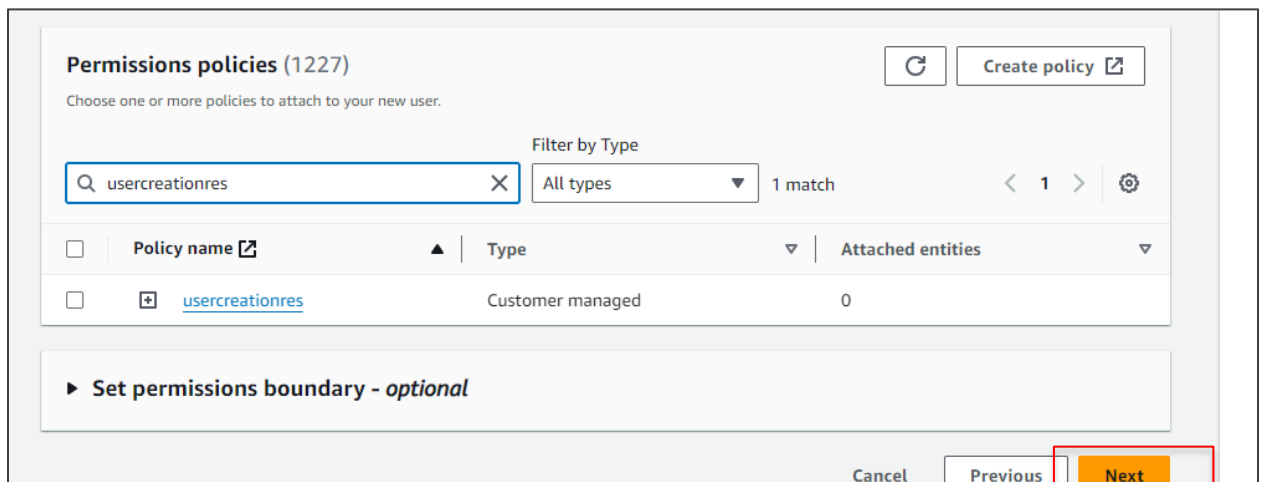
1.9 Provide a name to the user and click on **Next**



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**

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**

User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

[View user](#)

Users (3) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

[Search](#)

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password
<input type="checkbox"/>	Clouser	/	0	-	-	-

The user is successfully created.

1.13 Click on the created user

Users (3) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

[Search](#)

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password age
<input type="checkbox"/>	Clouser	/	0	-	-	-

1.14 Select **Security credentials**

The screenshot shows the AWS IAM console interface. On the left is a navigation pane with 'Identity and Access Management (IAM)' selected. The main area displays the 'Summary' for a user with ARN 'arn:aws:iam::719563875464:user/Cluser'. The 'Security credentials' tab is highlighted with a red box. Below the summary, there are tabs for 'Permissions policies (0)', 'Groups', 'Tags (1)', 'Security credentials', and 'Access Advisor'. The 'Permissions policies (0)' section shows a message: 'Permissions are defined by policies attached to the user directly or through groups.' and buttons for 'Remove' and 'Add permissions'.

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

The screenshot shows the 'Access keys (0)' page. At the top right is a 'Create access key' button. Below it, a message states: 'Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)'. Further down, another message says: 'No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)'. At the bottom, a 'Create access key' button is highlighted with a red box.

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

The screenshot shows the 'Access key best practices & alternatives' page. On the left, a sidebar lists steps: 'Step 1: Access key best practices & alternatives', 'Step 2 - optional: Set description tag', and 'Step 3: Retrieve access keys'. The main content area is titled 'Access key best practices & alternatives' with an 'Info' icon. It contains a warning: 'Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.' Below this, under the 'Use case' section, three options are listed: 'Command Line Interface (CLI)' (selected with a radio button), 'Local code', and 'Application running on an AWS compute service'. The 'Command Line Interface (CLI)' option is highlighted with a blue box and contains the text: 'You plan to use this access key to enable the AWS CLI to access your AWS account.'

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

You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

☐ Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

☐ Other
Your use case is not listed here.

Alternatives recommended

- Use [AWS CloudShell](#), a browser-based CLI, to run commands. [Learn more](#)
- Use the [AWS CLI V2](#) and enable authentication through a user in IAM Identity Center. [Learn more](#)

Confirmation

☒ I understand the above recommendation and want to proceed to create an access key.

Cancel **Next**

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

[IAM](#) > [Users](#) > [Clouser](#) > Create access key

Step 1
[Access key best practices & alternatives](#)

Step 2 - optional
Set description tag

Step 3
Retrieve access keys

Set description tag - *optional* [Info](#)

The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidentially later.

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @

Cancel Previous **Create access key**

Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

[IAM](#) > [Users](#) > [Clouser](#) > Create access key

Step 1
[Access key best practices & alternatives](#)

Step 2 - optional
[Set description tag](#)

Step 3
Retrieve access keys

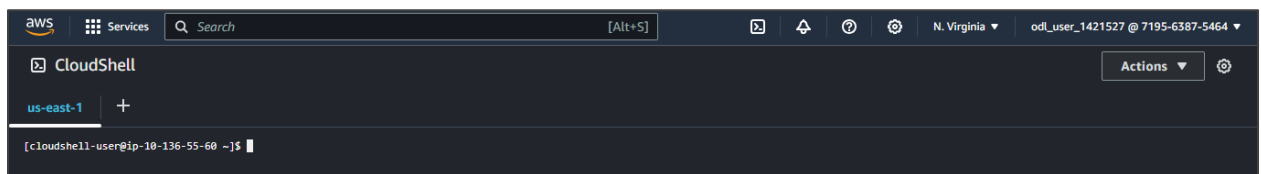
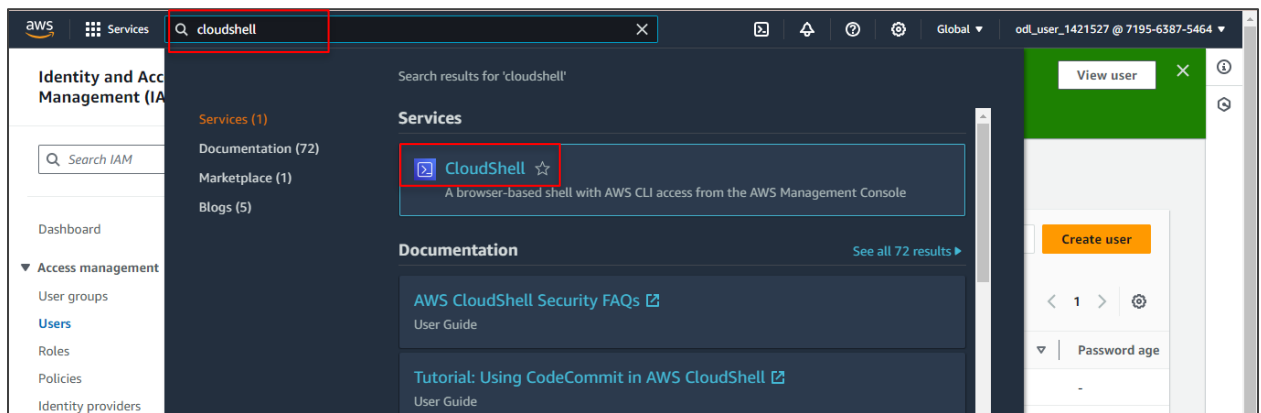
Retrieve access keys [Info](#)

Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

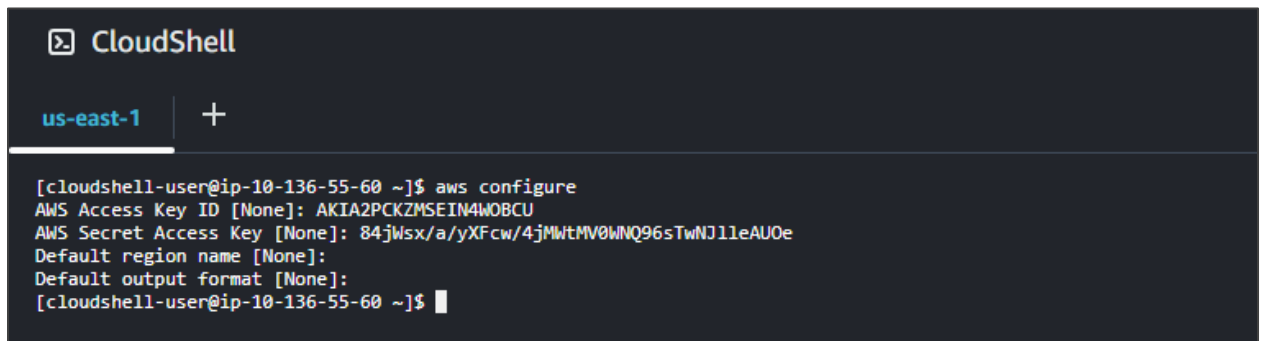
Access key	Secret access key
AKIA2PCKZMSEJJAUB4UO	***** Show

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

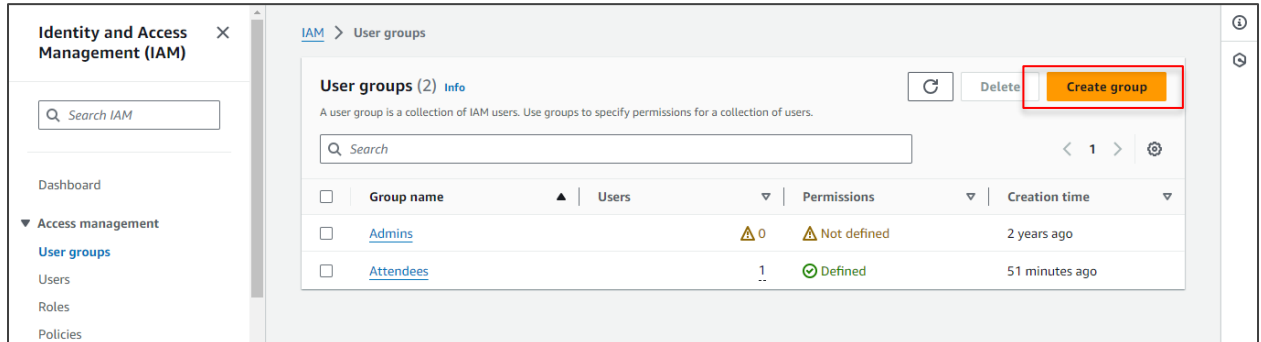


1.21 Use the following command to view the buckets in the account:
aws s3api list-buckets

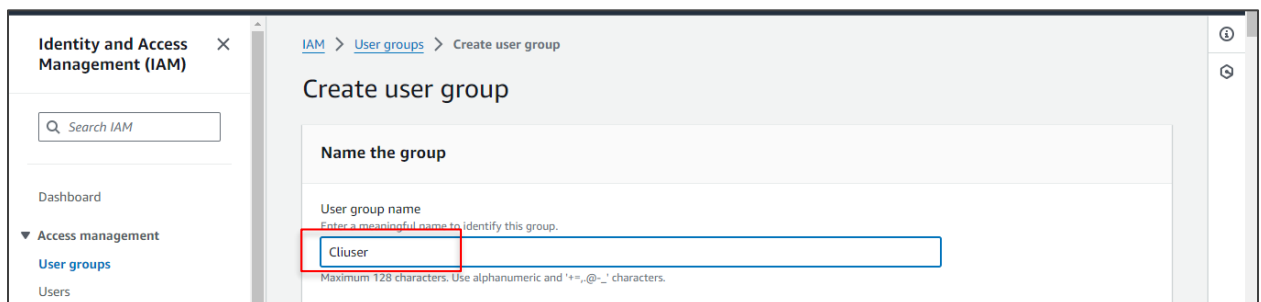
```
[cloudshell-user@ip-10-2-121-48 ~]$ aws s3api list-buckets
{
  "Buckets": [
    {
      "Name": "config-bucket-554936332221",
      "CreationDate": "2023-09-05T19:14:58+00:00"
    }
  ],
  "Owner": {
    "DisplayName": "simplilearnlabs138",
    "ID": "c5b1b62071b10455d245b195860383f520de51926755eba5d5a6d01cfc570b40"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

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

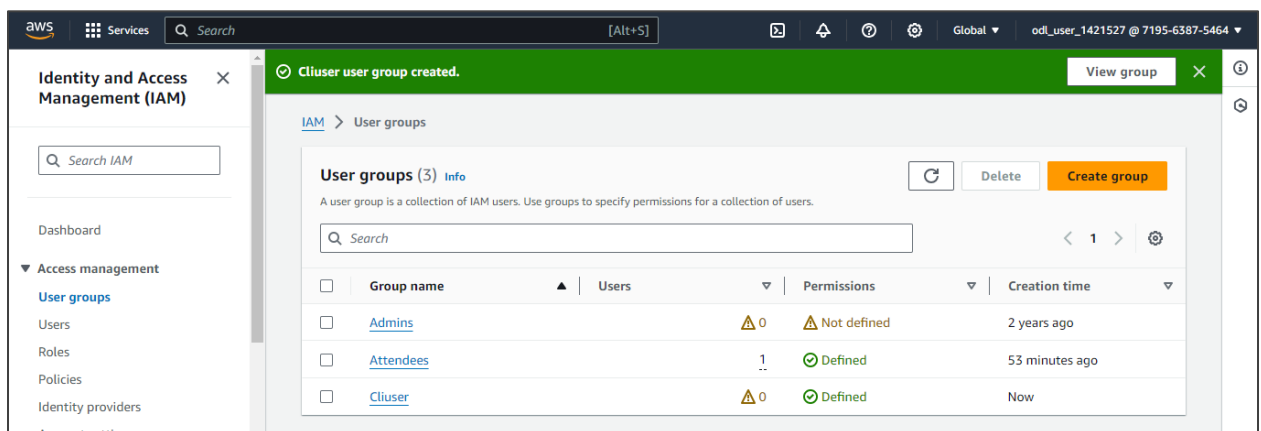
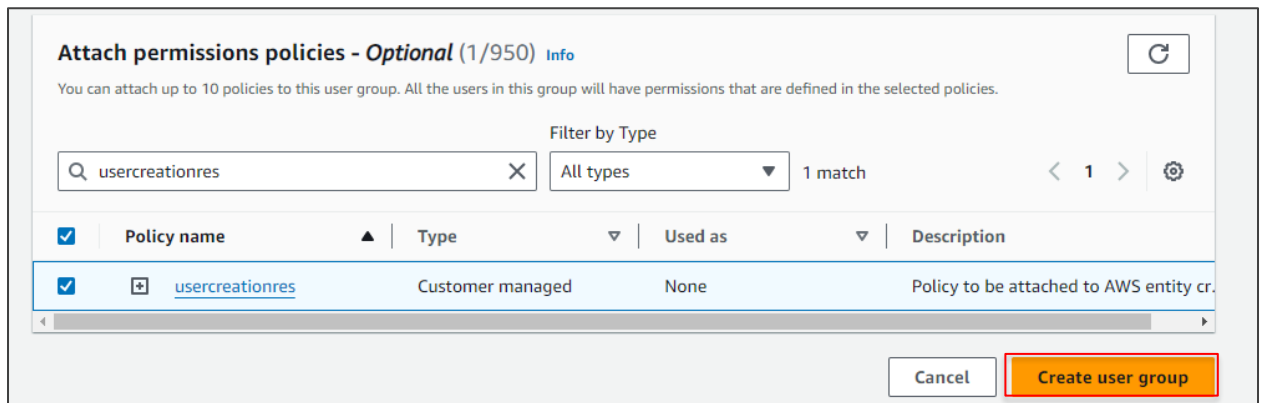
2.1 Select **User groups** and click on the **Create group** button



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

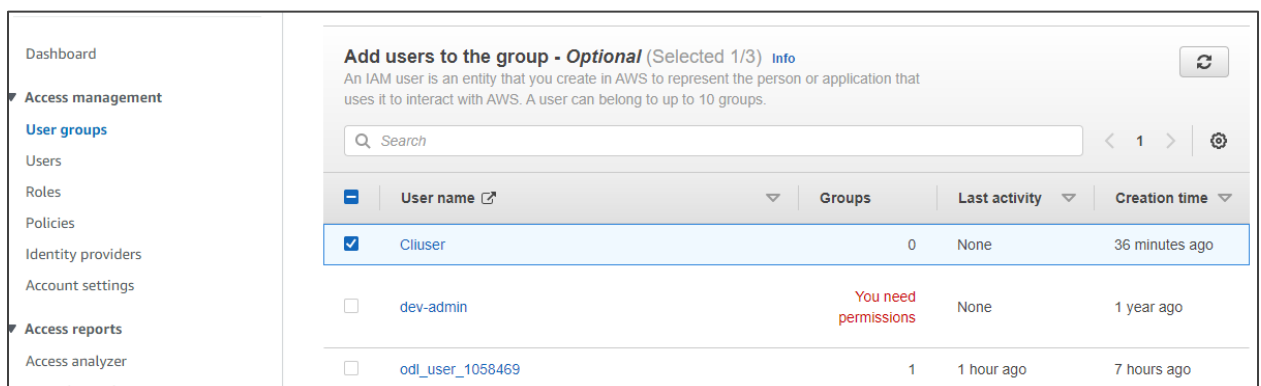


2.3 In the **Attach permissions policies** section, search for the **usercreationres** policy, select it, and then click on **Create user group**



The user group is created successfully.

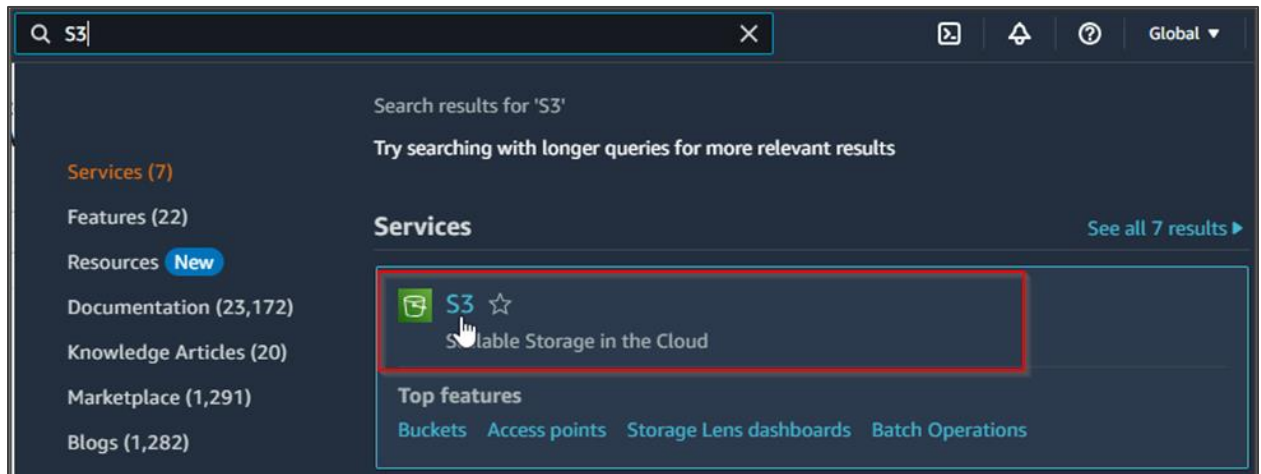
2.4 Under **User groups**, select **Cliuser** and click on the **Add users** button



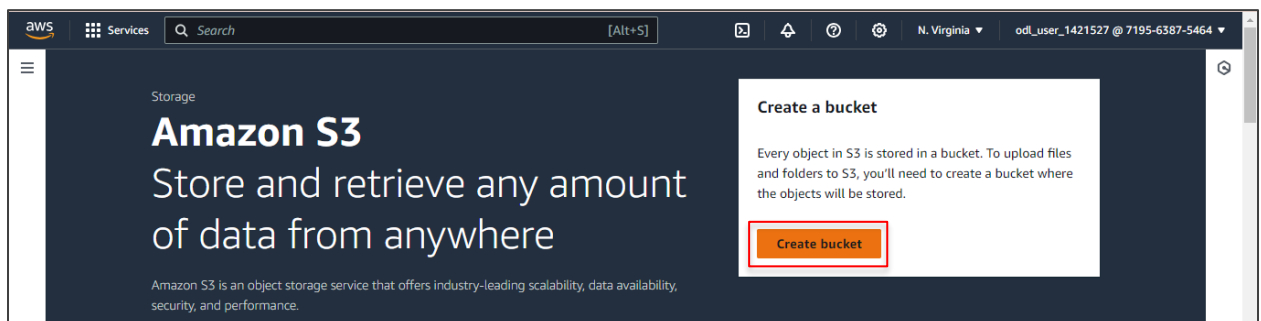
This will add the selected user to the group.

Step 3: Create and manage S3 versioning

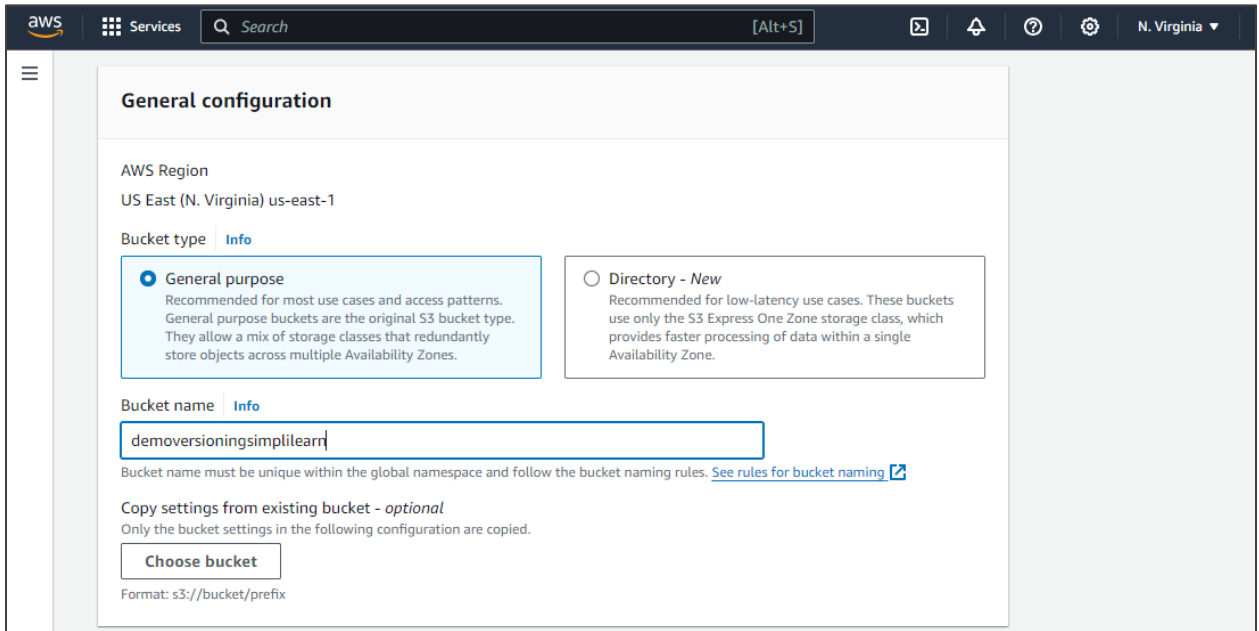
3.1 Search for and select S3 from the services



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 dropdown, and click on **Enable** in the **Bucket Versioning** section



The screenshot shows the 'General configuration' page in the AWS S3 console. The 'AWS Region' is set to 'US East (N. Virginia) us-east-1'. Under 'Bucket type', the 'General purpose' option is selected. The 'Bucket name' field contains 'demoversioningsimplilearn'. Below the name field, there is a note about bucket naming rules and a link to 'See rules for bucket naming'. There is also a section for 'Copy settings from existing bucket - optional' with a 'Choose bucket' button.

General configuration

AWS Region
US East (N. Virginia) us-east-1

Bucket type [Info](#)

- ☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
- ☐ **Directory - New**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

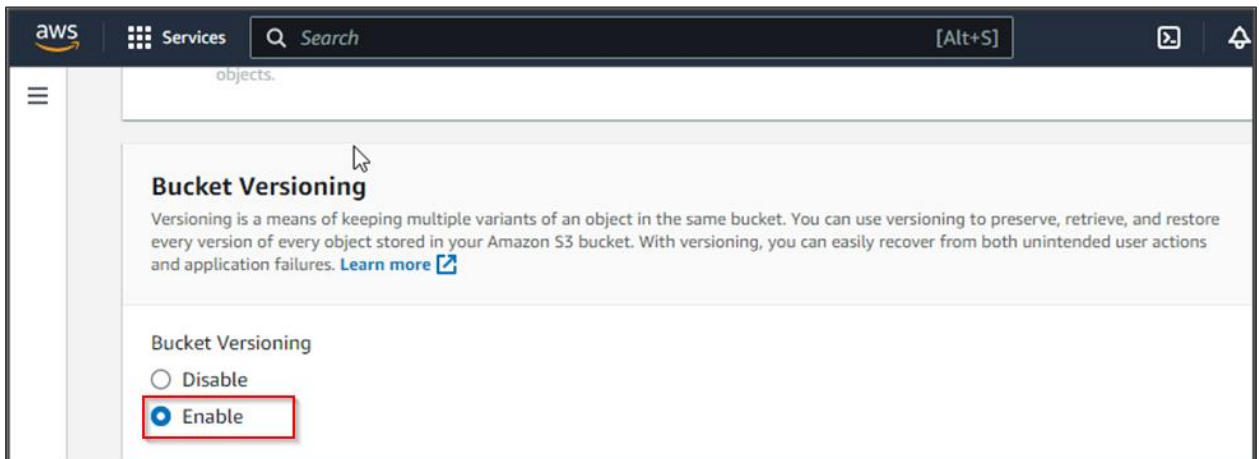
Bucket name [Info](#)
demoversioningsimplilearn

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix



The screenshot shows the 'Bucket Versioning' page in the AWS S3 console. The page title is 'objects.'. The 'Bucket Versioning' section has two options: 'Disable' and 'Enable'. The 'Enable' option is selected and highlighted with a red box.

objects.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

- ☐ Disable
- ☒ **Enable**

3.4 Click on the **Create bucket** button

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

- ☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#).

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- ☐ Disable
- ☒ Enable

► **Advanced settings**

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel **Create bucket**

Successfully created bucket "demoversioningsimplilearn"
To upload files and folders, or to configure additional bucket settings choose [View details](#).

Amazon S3 > Buckets

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

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"/>	config-bucket-554936332221	US East (N. Virginia) us-east-1	Bucket and objects not public	September 6, 2023, 00:44:58 (UTC+05:30)
<input type="radio"/>	demoversioningsimplilearn	US East (N. Virginia) us-east-1	Bucket and objects not public	September 6, 2023, 02:51:15 (UTC+05:30)

The bucket is created successfully.

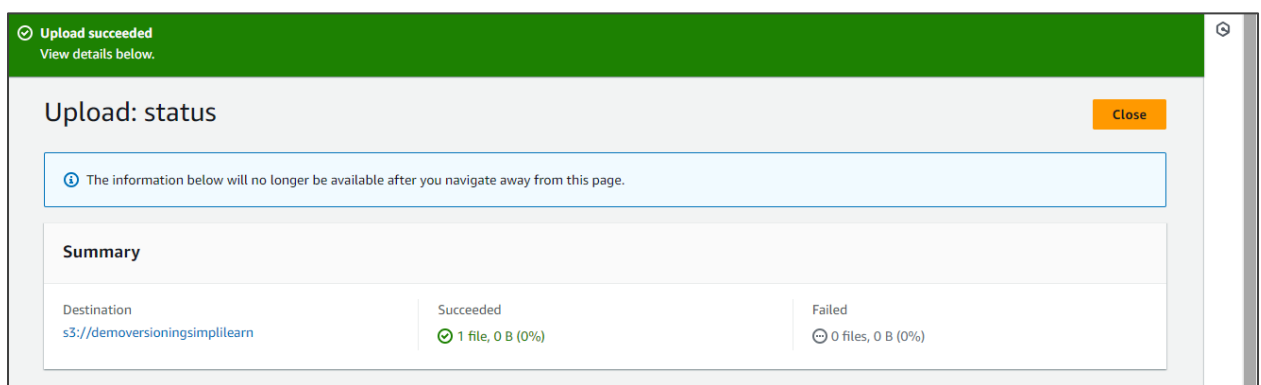
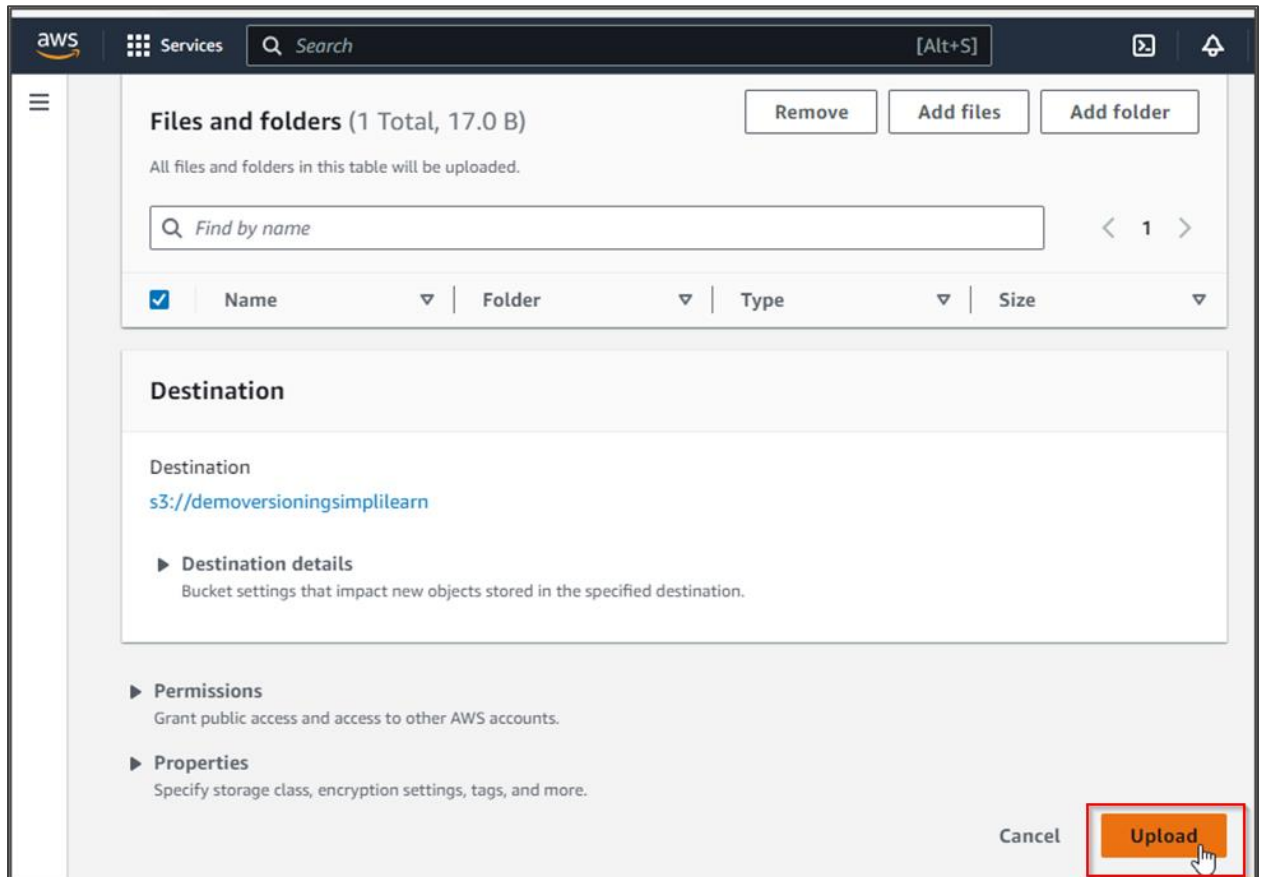
3.5 Click on the bucket that you created and in the Objects section, upload a simple txt file as shown below:

The screenshot shows the Amazon S3 'Upload' page for a bucket named 'demoversioningsimplilearn'. The breadcrumb navigation is 'Amazon S3 > Buckets > demoversioningsimplilearn > Upload'. The main heading is 'Upload' with an 'Info' link. Below this, a message states: 'Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#) '. A dashed box contains the instruction: 'Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.' Below this is a section titled 'Files and folders (1 Total, 0 B)' with 'Remove', 'Add files', and 'Add folder' buttons. A note says 'All files and folders in this table will be uploaded.' There is a search bar with 'Find by name' and a pagination control showing '< 1 >'. A table lists the uploaded file:

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	sample.txt	-	text/plain

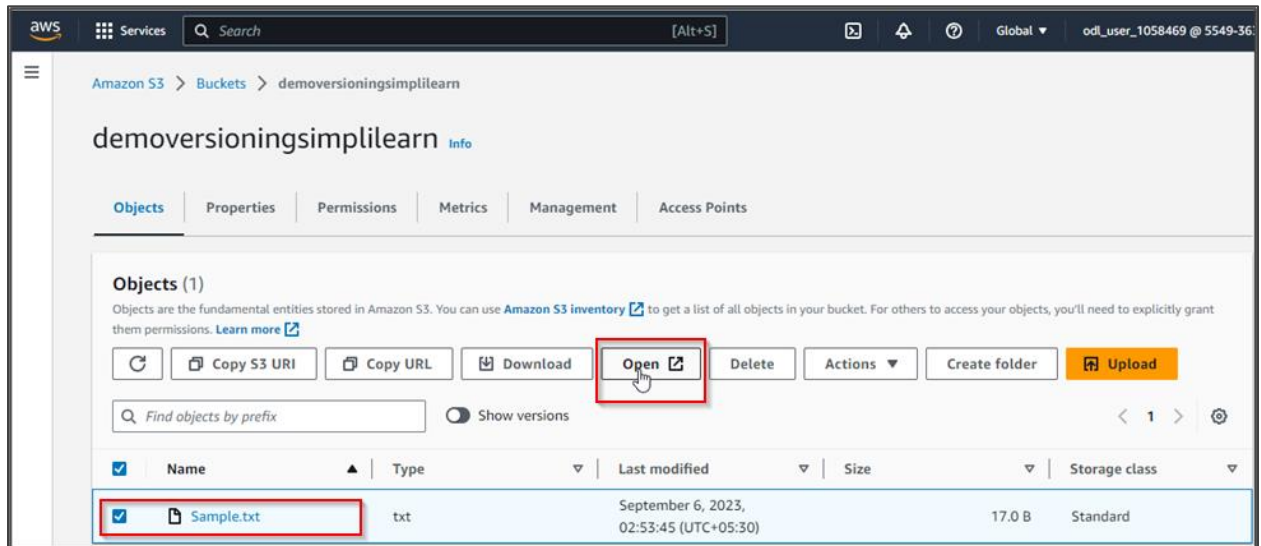
A scrollbar is visible at the bottom of the table.

3.6 Click on the **Upload** button

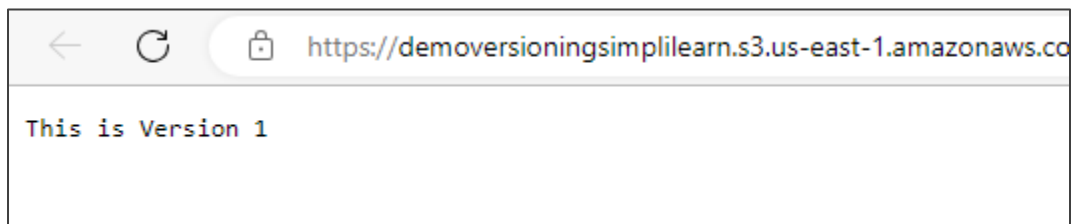


The file is successfully uploaded.

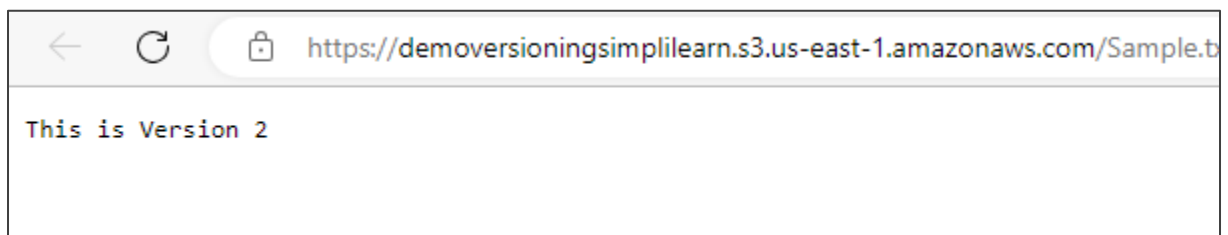
3.7 Select the text file and click on **Open**



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.

