

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

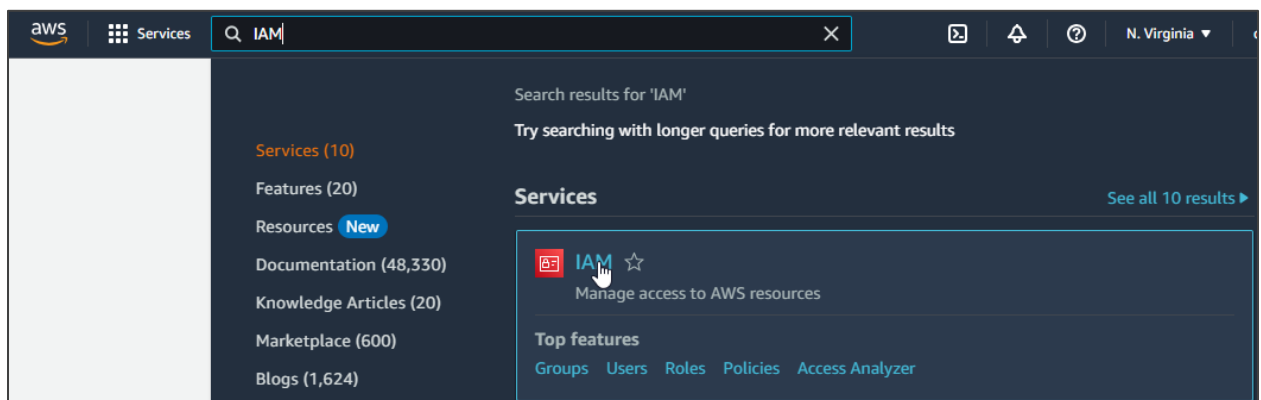
Prerequisites: None

Steps to be followed:

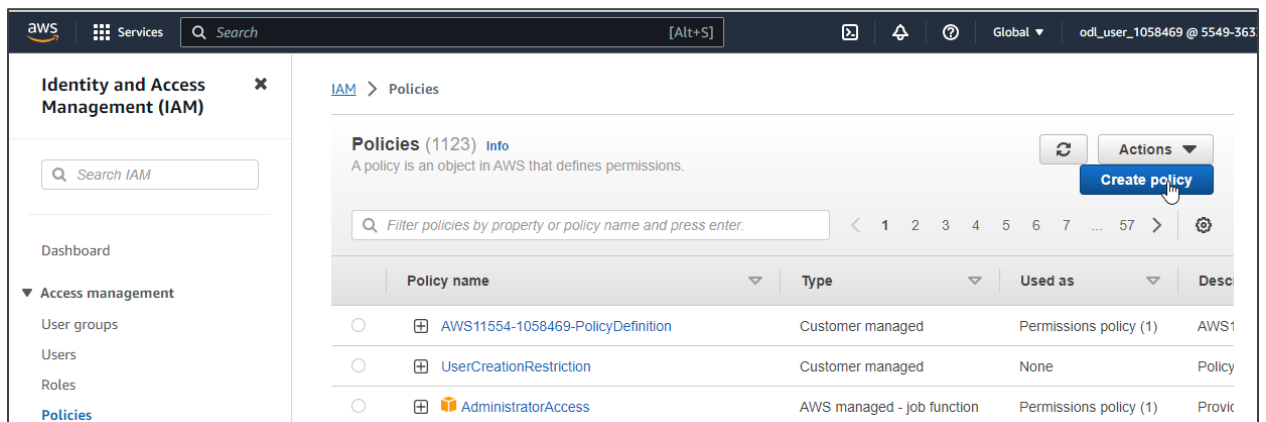
1. Create and manage policy
2. Attach policy and permissions directly to the group using group users
3. Create and manage S3 versioning

Step 1: Create and manage policy

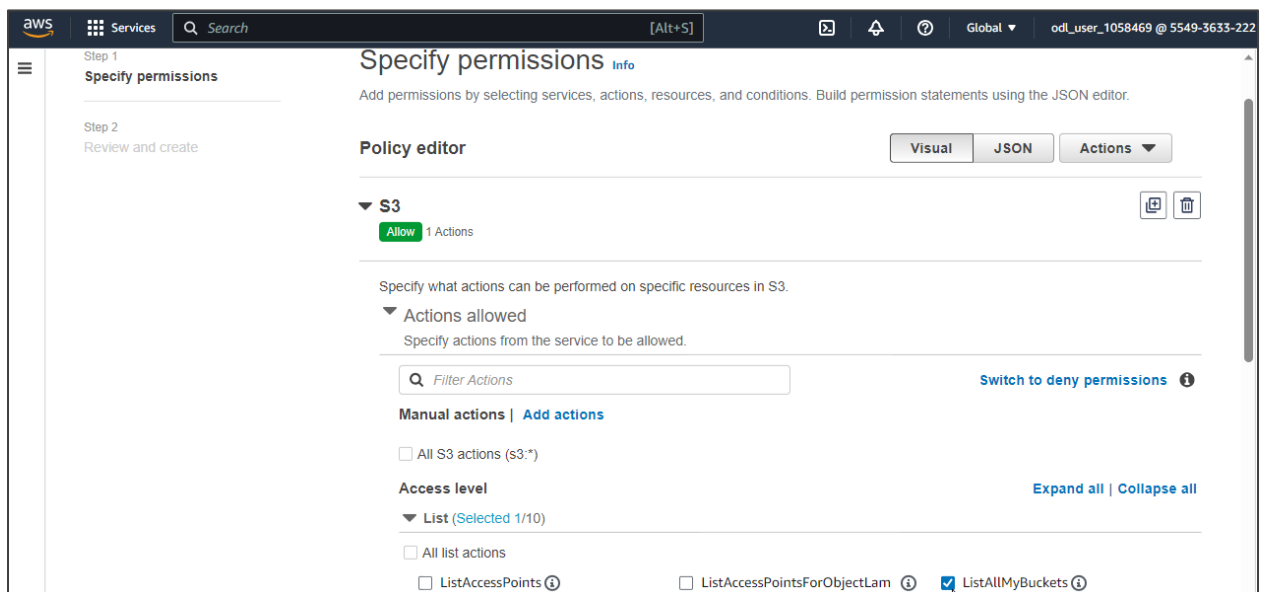
1.1 Go to your Amazon console, search for and select **IAM** in the search bar



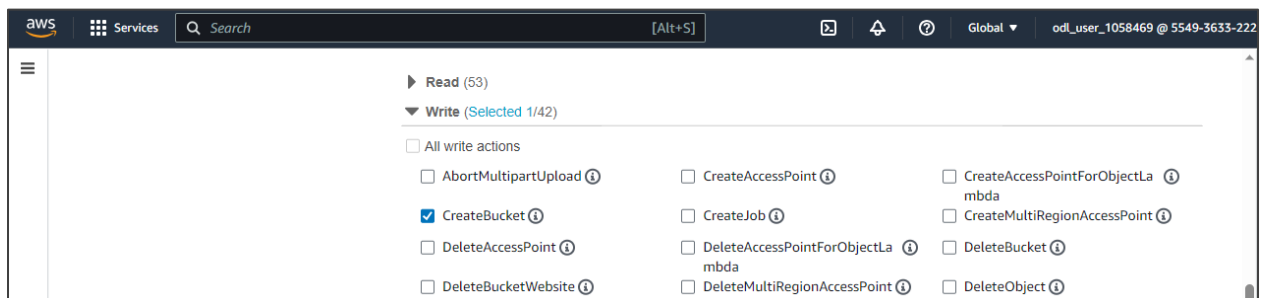
1.2 In the IAM dashboard, select **Policies** and click on **Create policy**



1.3 In the service options, select **S3**, and then choose **ListAllMyBuckets** from the **List** section in the **Access level**



1.4 Now, choose **CreateBucket** from the **Write** section



1.5 In the **Resources** section, select **All**, and then click on **Next**

Resources
Specify resource ARNs for these actions.

☐ Specific
☒ All

⚠ The all wildcard "*" may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

Request conditions - *optional*

Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Cancel Next

1.6 Click on **Create policy**

aws
Services
Search
[Alt+S]
Global
odl_user_1058469 @ 5549-3633

Permissions in the policy document specify which actions are allowed or denied.

Search

Allow (1 of 386 services)
Show remaining 385 services

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

Add tags - *optional*
Info

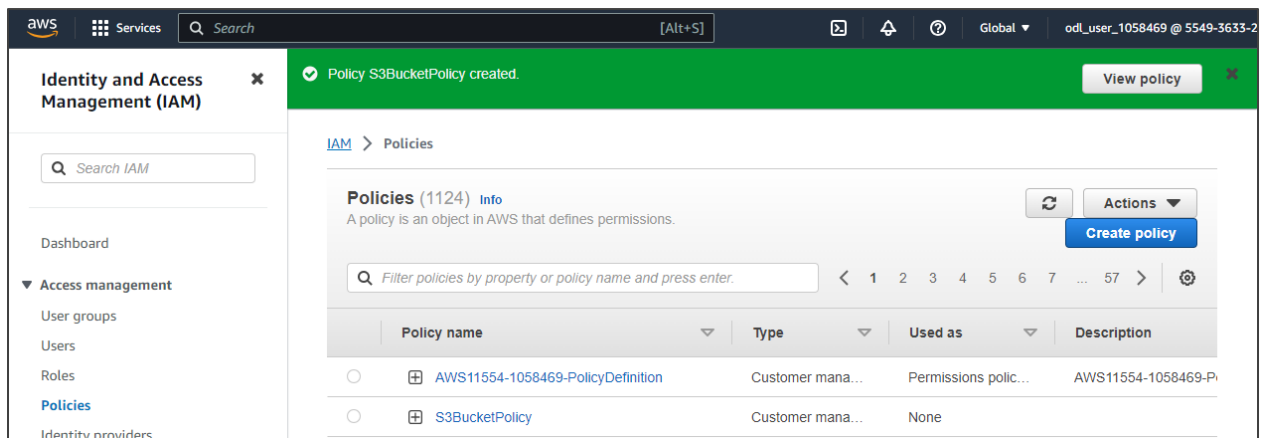
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add tag

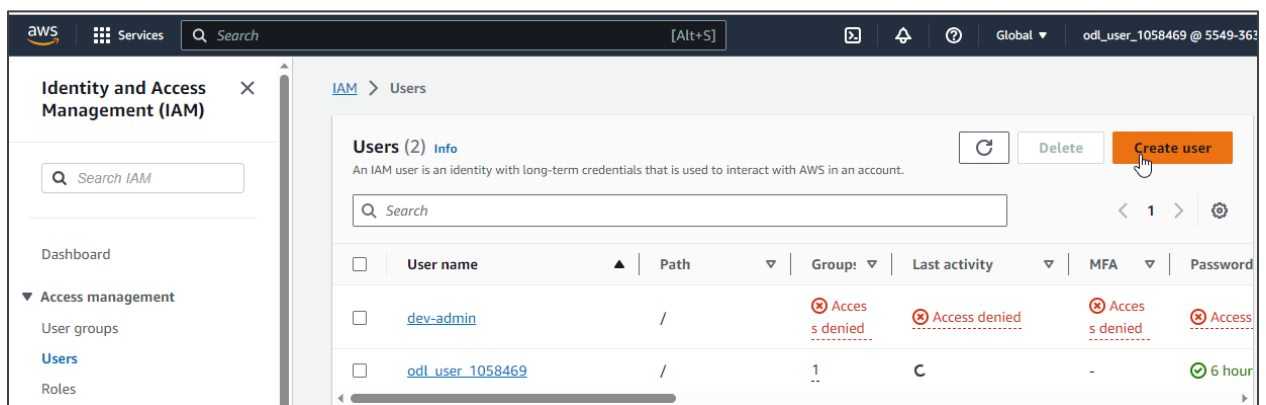
You can add up to 50 more tags.

Cancel Previous Create policy



The policy is created successfully.

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



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

aws Services Search [Alt+S] Global odl_user_1058469 @ 5549-36

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Specify user details

User details

User name

Clouser

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

i If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel **Next**

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

aws Services Search [Alt+S] Global odl_user_1058469 @ 5549-36

IAM > Users > Create user

Step 1
[Specify user details](#)

Step 2
Set permissions

Step 3
Review and create

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☐ 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.

1.10 Select **UserCreationRestriction** policy from the list and then click on **Next**

Permissions policies (1/1126)
Choose one or more policies to attach to your new user.

Filter by Type
UserCrea X All types 1 match

<input checked="" type="checkbox"/>	Policy name	Type	Attached entities
<input checked="" type="checkbox"/>	UserCreationRestriction	Customer managed	0

► Set permissions boundary - optional

Cancel Previous **Next**

1.11 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**

Identity and Access Management (IAM)

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

Users (3) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

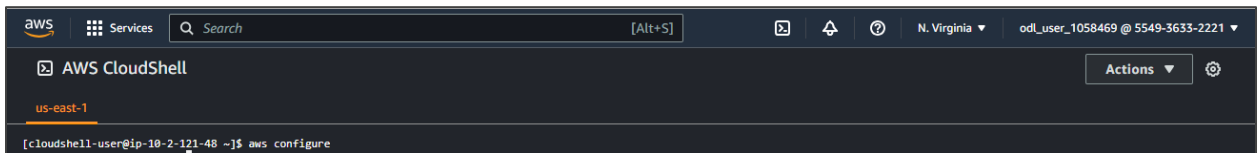
<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password
<input type="checkbox"/>	C1i1user	/	0	.	-	-

Dashboard
Access management
User groups
Users
Roles

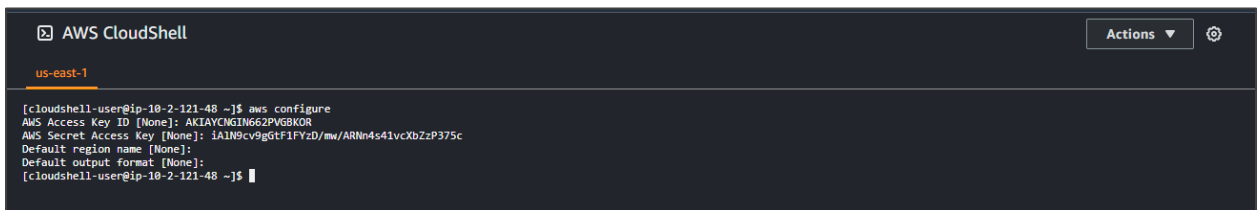
View user
Delete Create user

The user is created successfully.

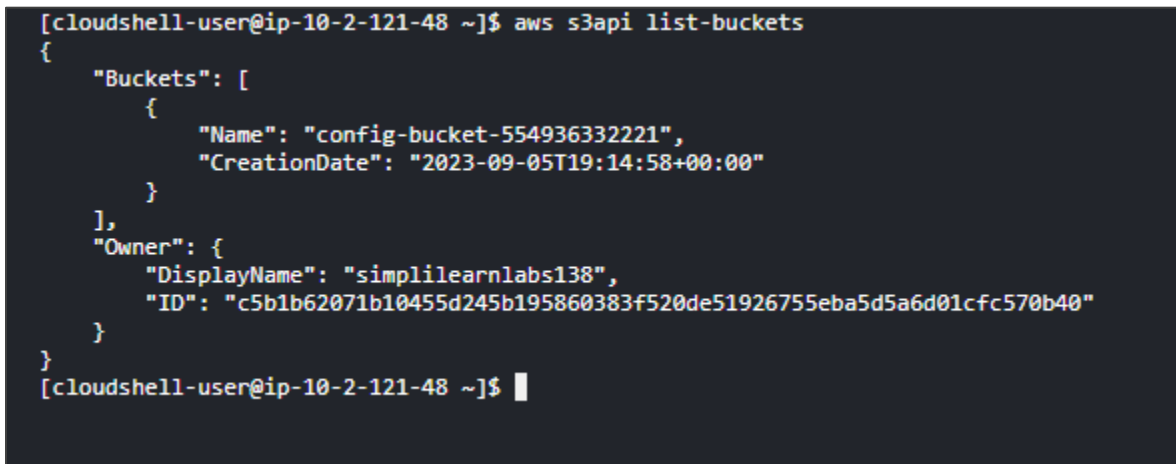
1.12 Now, open **CloudShell** to configure the user



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

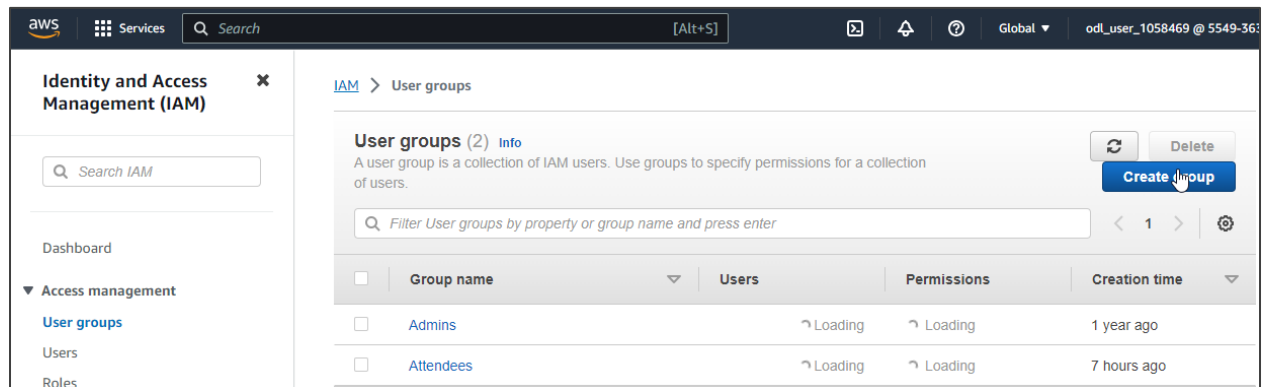


1.14 Now, enter the command **aws s3api list-buckets** to view the buckets in the account

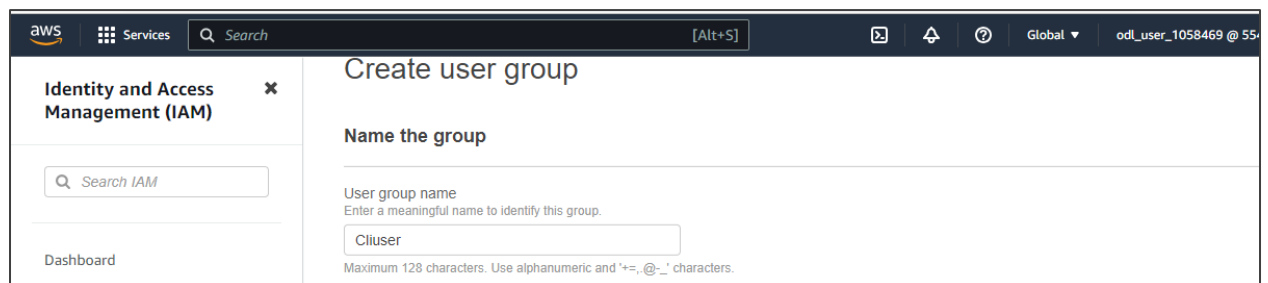


Step 2: Attach policy and permissions directly to the group using group users

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 **UserCreationRestriction** policy, select it, and then click on **Create group**

The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible. The main content area is titled 'Attach permissions policies'. A search bar at the top contains 'UserCreationRestriction'. The search results list several policies, with 'UserCreationRestriction' selected. At the bottom right, the 'Create group' button is highlighted with a mouse cursor.

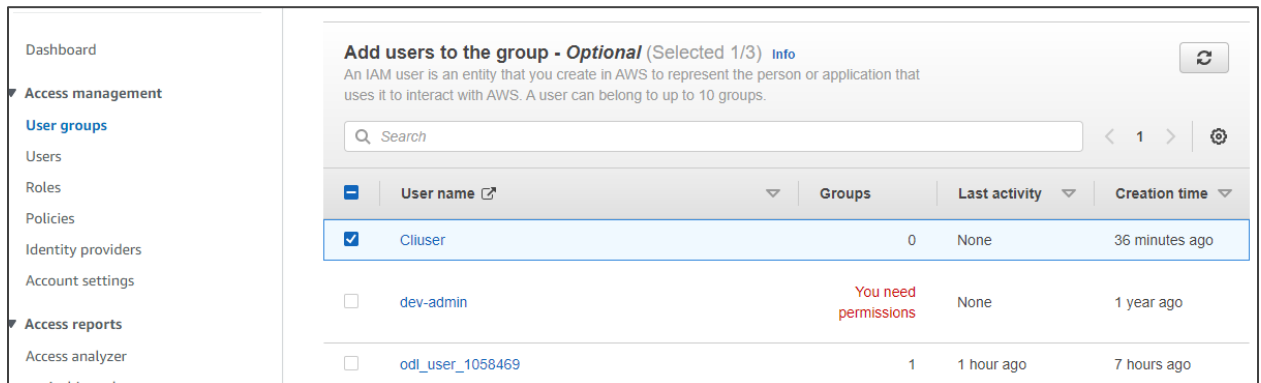
Policy name	Managed by	Description
<input checked="" type="checkbox"/> UserCreationRestriction	Customer managed	Policy for creating i
<input type="checkbox"/> TranslateReadOnly	AWS managed	Provides read-only
<input type="checkbox"/> TranslateFullAccess	AWS managed	Provides full acces
<input type="checkbox"/> SystemAdministrator	AWS managed - job function	Grants full access j
<input type="checkbox"/> SupportUser	AWS managed - job function	This policy grants p
<input type="checkbox"/> SimpleWorkflowFullAccess	AWS managed	Provides full acces
<input type="checkbox"/> ServiceQuotasReadOnlyAccess	AWS managed	Provides read only
<input type="checkbox"/> ServiceQuotasFullAccess	AWS managed	Provides full acces
<input type="checkbox"/> ServerMigration_ServiceRole	AWS managed	Permissions to allo
<input type="checkbox"/> ServerMigrationServiceRoleForInstanceValidation	AWS managed	Permissions to allo
<input type="checkbox"/> ServerMigrationServiceLaunchRole	AWS managed	Permissions to allo
<input type="checkbox"/> ServerMigrationServiceConsoleFullAccess	AWS managed	Required permissio

The screenshot shows the AWS IAM console interface after creating a user group. A green banner at the top indicates 'Ciluser user group created.' with a 'View group' button. The main content area is titled 'User groups (3)'. A table lists the user groups, including 'Ciluser' which is 'Defined'.

Group name	Users	Permissions	Creation time
Admins	↕ Loading	↕ Loading	1 year ago
Attendees	↕ Loading	↕ Loading	7 hours ago
Ciluser	1	✓ Defined	Now

The user group is created successfully.

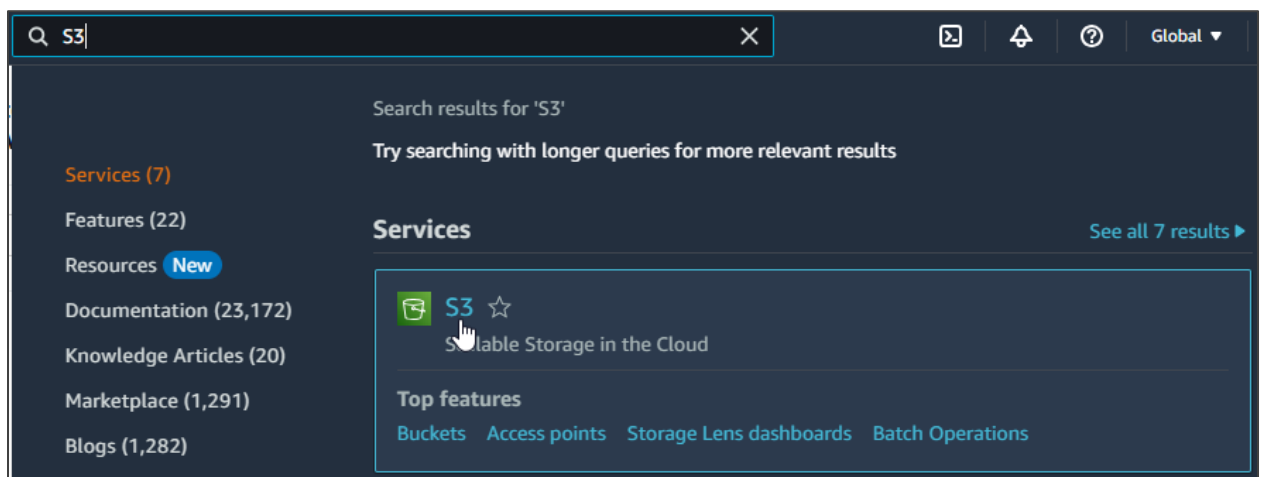
2.4 Under **User groups**, select **Cluser** and click on the **Add users** button



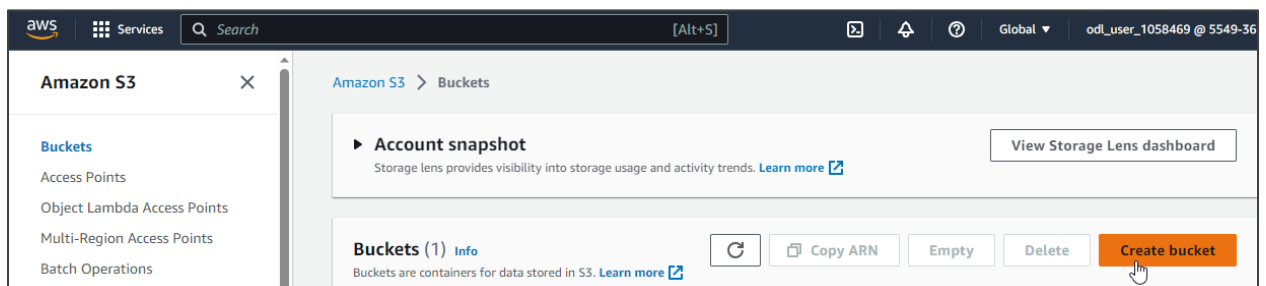
This will add the selected user to the group.

Step 3: Create and manage S3 versioning

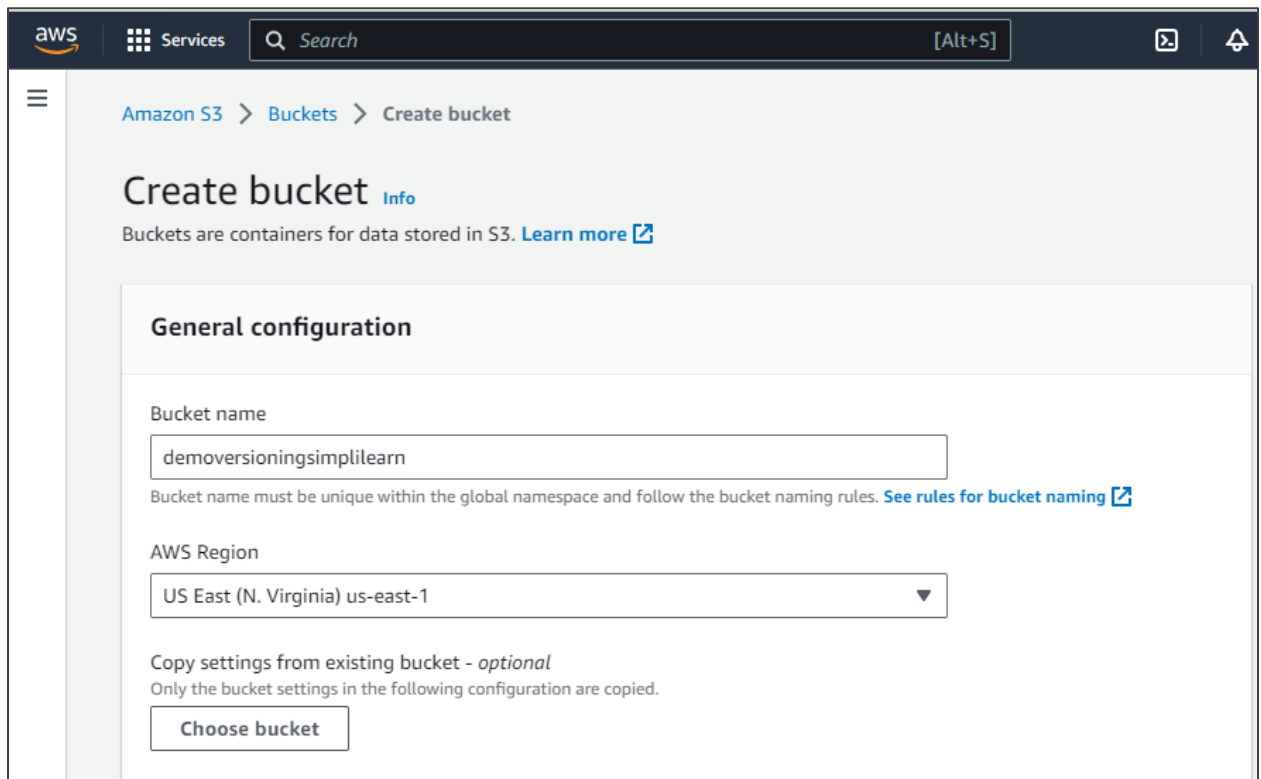
3.1 Search for and select **S3** from the services



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



aws Services Search [Alt+S]

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

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

General configuration

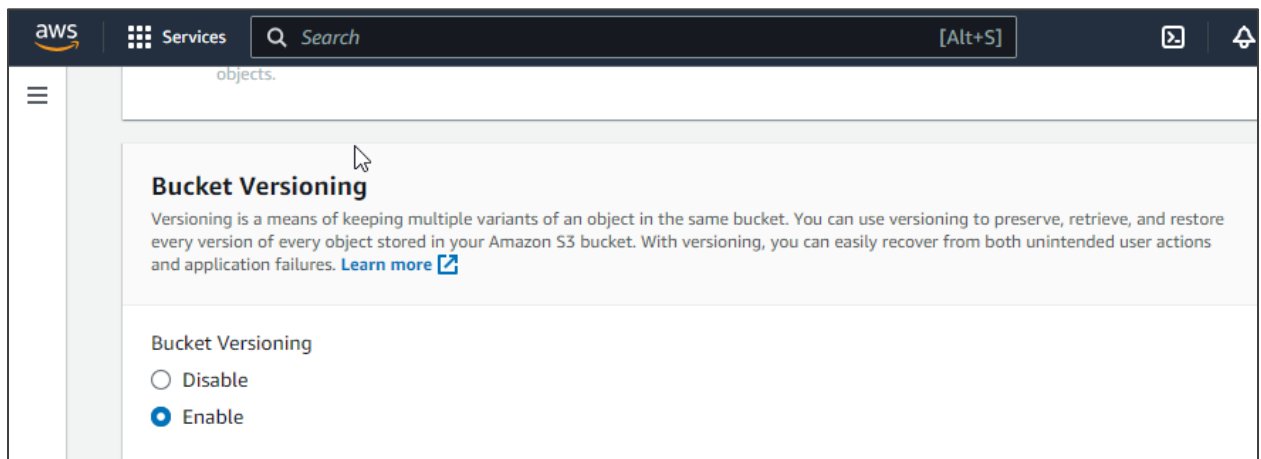
Bucket name

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

AWS Region

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

[Choose bucket](#)



aws Services Search [Alt+S]

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 Now, 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" [View details](#)

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

Amazon S3 > Buckets

► **Account snapshot** [View Storage Lens dashboard](#)

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](#)

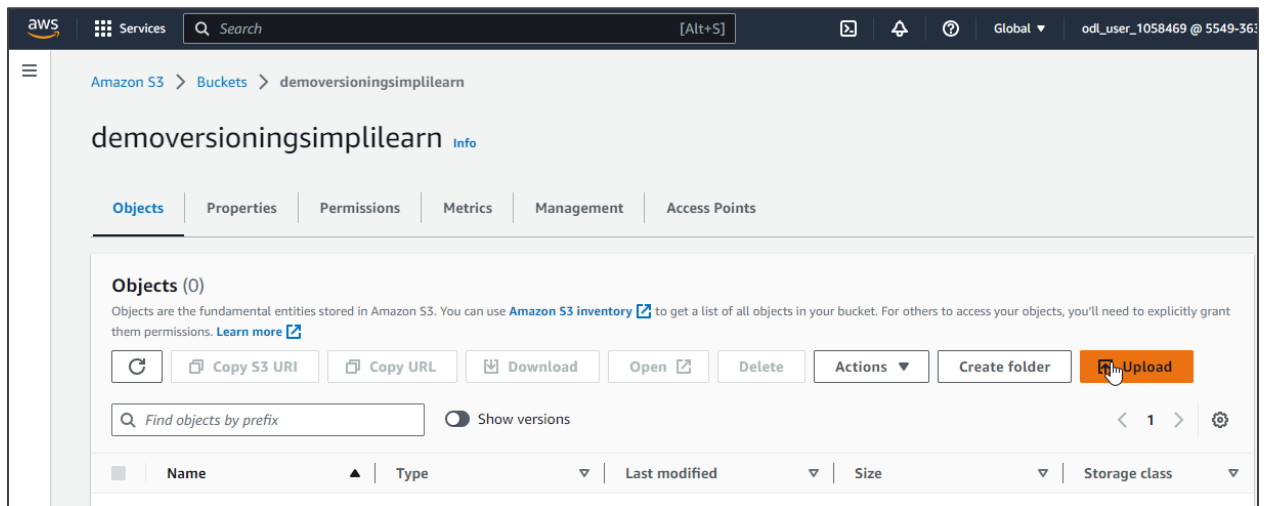
[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) **Create bucket**

Find buckets by name

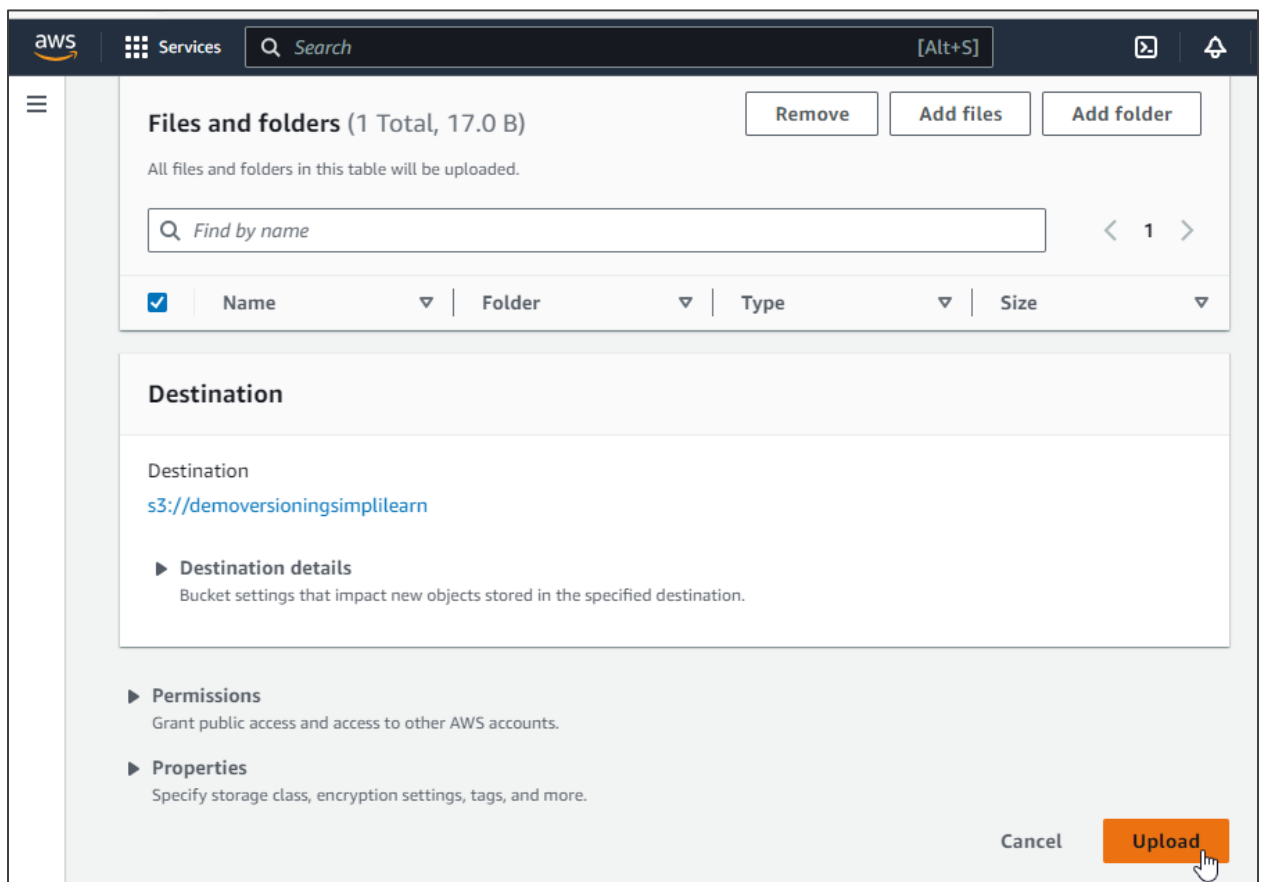
	Name	AWS Region	Access	Creation date
<input type="radio"/>	config-bucket-554936332221	US East (N. Virginia) us-east-1	Bucket and objects not public	September 6, 2023, 00:44:58 (UTC+05:30)
<input type="radio"/>	demoversioningsimplilearn	US East (N. Virginia) us-east-1	Bucket and objects not public	September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

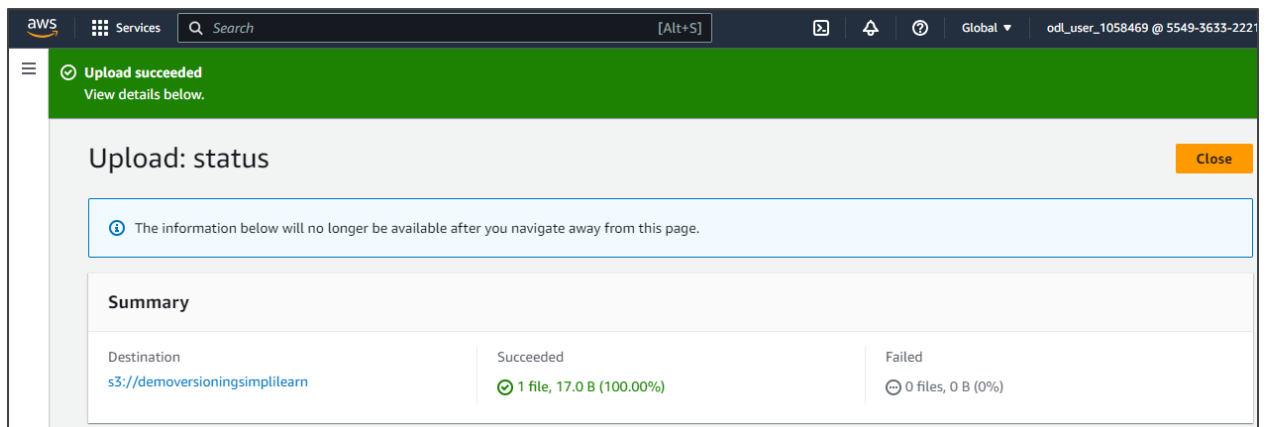
The bucket is created successfully.

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



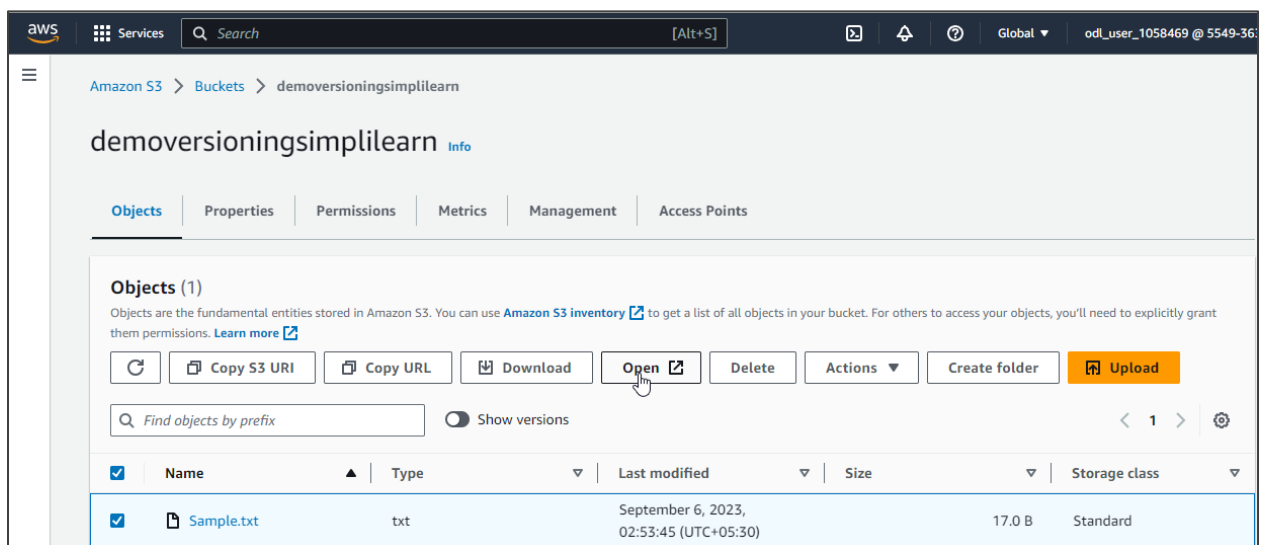
3.6 Click on the **Upload** button



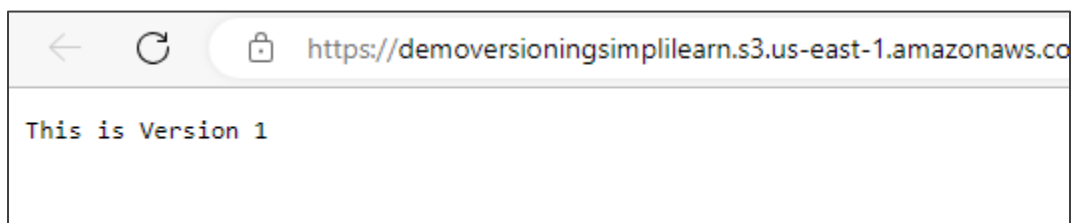


The file is uploaded successfully.

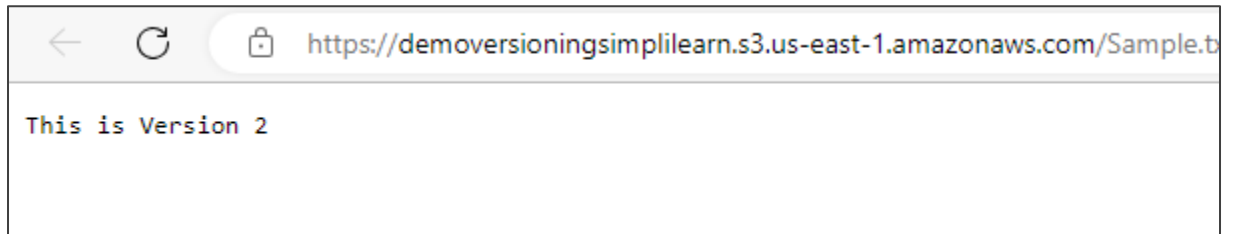
3.7 Now, select the text file and click on **Open**



3.8 The obtained output will be shown like this:



3.9 Now, make changes to the text file, save it, and reupload the same file. The updated output will be shown like this:



By following these steps, you have successfully demonstrated the process of creating and adding policies to groups using a user.