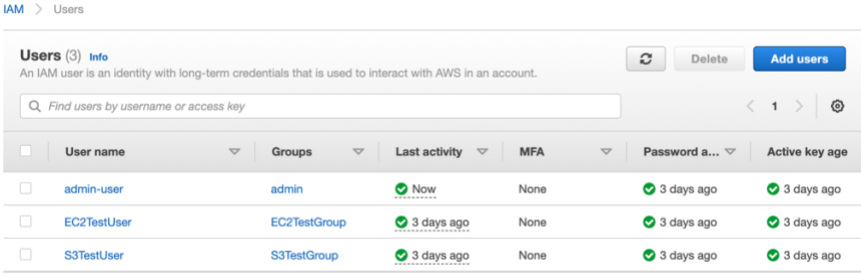



Actions	Snapshots
<ul style="list-style-type: none"> Create 2 users, S3TestUser and EC2TestUser, with strong passwords 	
<ul style="list-style-type: none"> Generate an access key to each user and save them 	
<ul style="list-style-type: none"> Attach AmazonS3FullAccess to S3TestUser 	
<ul style="list-style-type: none"> Create a user group, EC2TestGroup 	
<ul style="list-style-type: none"> Attach AmazonEC2FullAccess to this group 	

- Add EC2TestUser to this group

EC2TestGroup

[Delete](#)

Summary

[Edit](#)

User group name	Creation time	ARN
EC2TestGroup	September 13, 2021, 22:10 (UTC-04:00)	arn:aws:iam::430782206656:group/EC2TestGroup

[Users](#) | [Permissions](#) | [Access advisor](#)

Users in this group (1) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

[Refresh](#) [Remove users](#) [Add users](#)

<input type="checkbox"/>	User name ↗	Groups	Last activity	Creation time
<input type="checkbox"/>	EC2TestUser	1	3 days ago	3 days ago

- Create a role name, EC2Describe, and attach AmazonEC2ReadOnlyAccess to this role

Roles > EC2Describe

[Delete role](#)

Summary

Role ARN	arn:aws:iam::430782206656:role/EC2Describe ↗
Role description	Allows EC2 instances to call AWS services on your behalf. Edit
Instance Profile ARNs	arn:aws:iam::430782206656:instance-profile/EC2Describe ↗
Path	/
Creation time	2021-09-13 22:27 EDT
Last activity	Not accessed in the tracking period
Maximum session duration	1 hour Edit

[Permissions](#) | [Trust relationships](#) | [Tags](#) | [Access Advisor](#) | [Revoke sessions](#)

Permissions policies (1 policy applied)

[Attach policies](#) [Add inline policy](#)

Policy name ↕	Policy type ↕
AmazonEC2ReadOnlyAccess	AWS managed policy

- Test the users and policies by: Login as S3TestUser and try to manipulate EC2 services

Step 1: Choose an Amazon Machine Image (AMI)

[Cancel and Exit](#)

An error occurred describing your selected AMI
You are not authorized to perform this operation.

- Then create a bucket (<classname><yourlastname><yourfirstname>) in the east region, and upload simple file into that bucket

Amazon S3 > cloudcomputing-zhang-sisi

[cloudcomputing-zhang-sisi](#) [Info](#)

[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	sample.txt	txt	September 17, 2021, 01:17:06 (UTC-04:00)	23.0 B	Standard

- Login as EC2TestUser and try to access the file you uploaded before

Amazon S3

[View Storage Lens dashboard](#)

Account snapshot

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

Buckets (0) [Info](#)

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

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

Name	AWS Region	Access	Creation date
------	------------	--------	---------------

You don't have permissions to list buckets
After you or your AWS administrator have updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. [Learn more about identity and access management in Amazon S3](#)

