Name: Shriya Thabe

Roll No: A076

SapId: 86062200070

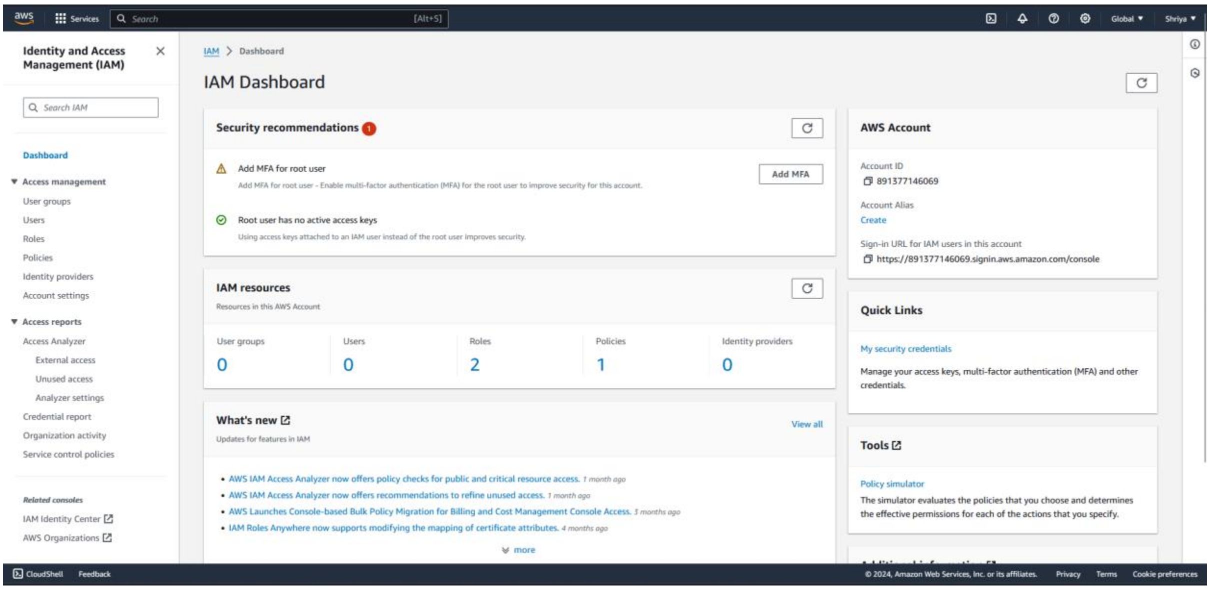
Batch 2

Practical 3 Identity Access Management (IAM)

Step1: Log in to your AWS account and log in.

Step2: On the search bar search IAM.

Step3: Click on IAM.



IAM Dashboard

Security recommendations 1

Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	2	1	0

What's new

Updates for features in IAM

- AWS IAM Access Analyzer now offers policy checks for public and critical resource access. *1 month ago*
- AWS IAM Access Analyzer now offers recommendations to refine unused access. *1 month ago*
- AWS Launches Console-based Bulk Policy Migration for Billing and Cost Management Console Access. *3 months ago*
- IAM Roles Anywhere now supports modifying the mapping of certificate attributes. *4 months ago*

AWS Account

Account ID
891377146069

Account Alias
Create

Sign-in URL for IAM users in this account
https://891377146069.signin.aws.amazon.com/console

Quick Links

My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials.

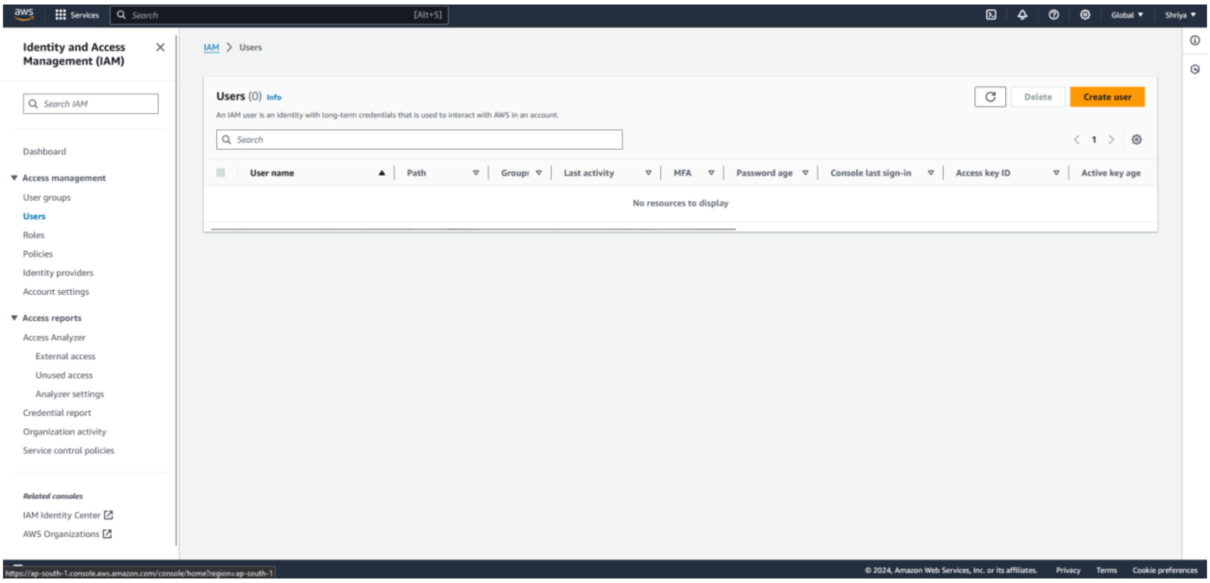
Tools

Policy simulator

The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Step4: Click on user on the left window pane.

Step5: Click on create user option.



Users (0)

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

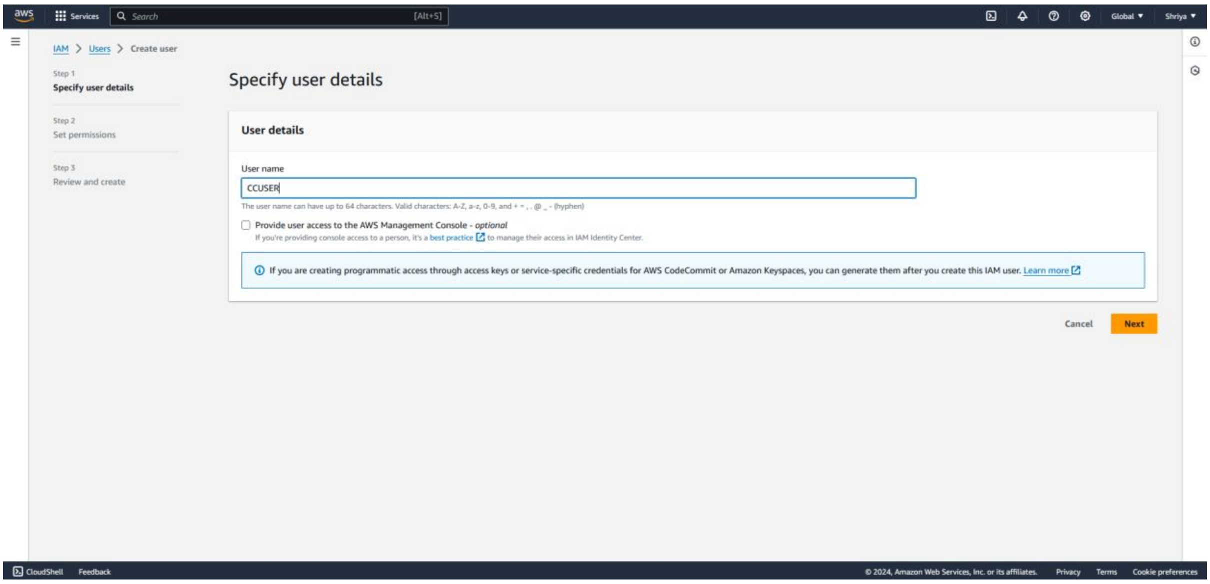
□	User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age

No resources to display

https://ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1

Step6: Give a name to your user and do not select the provide user access to the

AWS Management Console,then click on next.



Specify user details

User details

User name

CCUSER

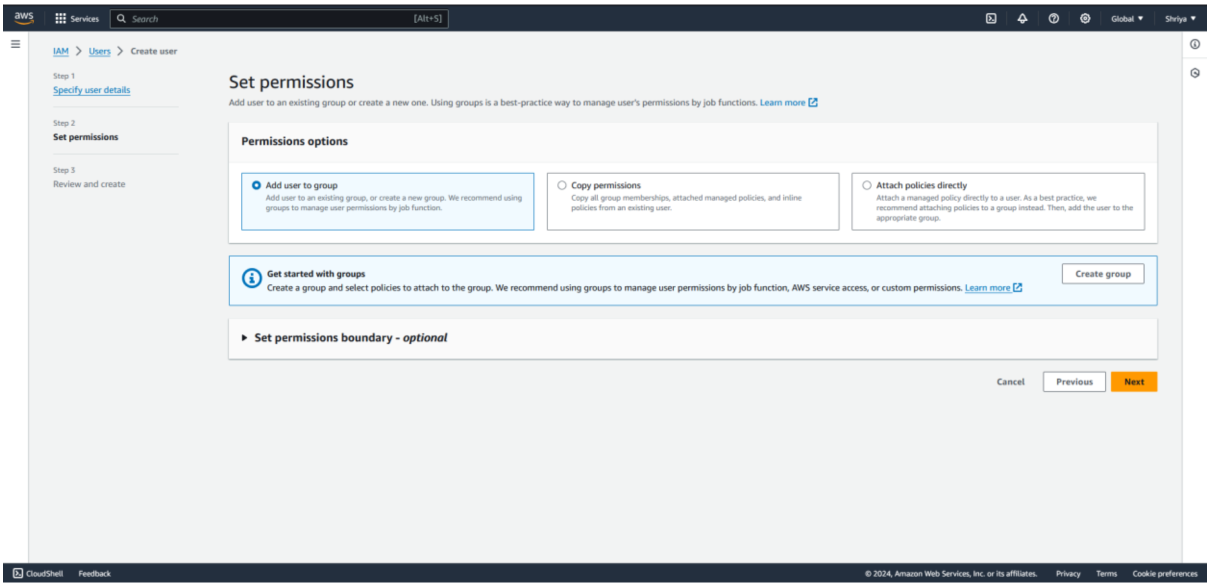
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

□ 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.

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

Step7: Select Add user to group option and click on next.



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

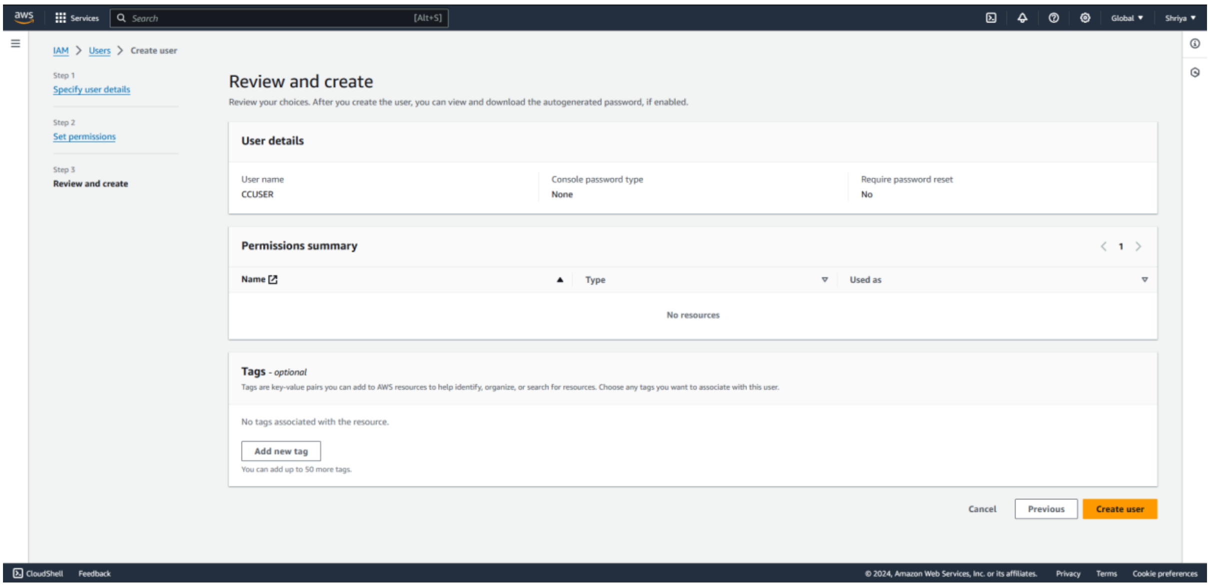
● Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ 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.

Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more

Step8: Click on create user.



Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
CCUSER	None	No

Permissions summary

Name	Type	Used as
No resources		

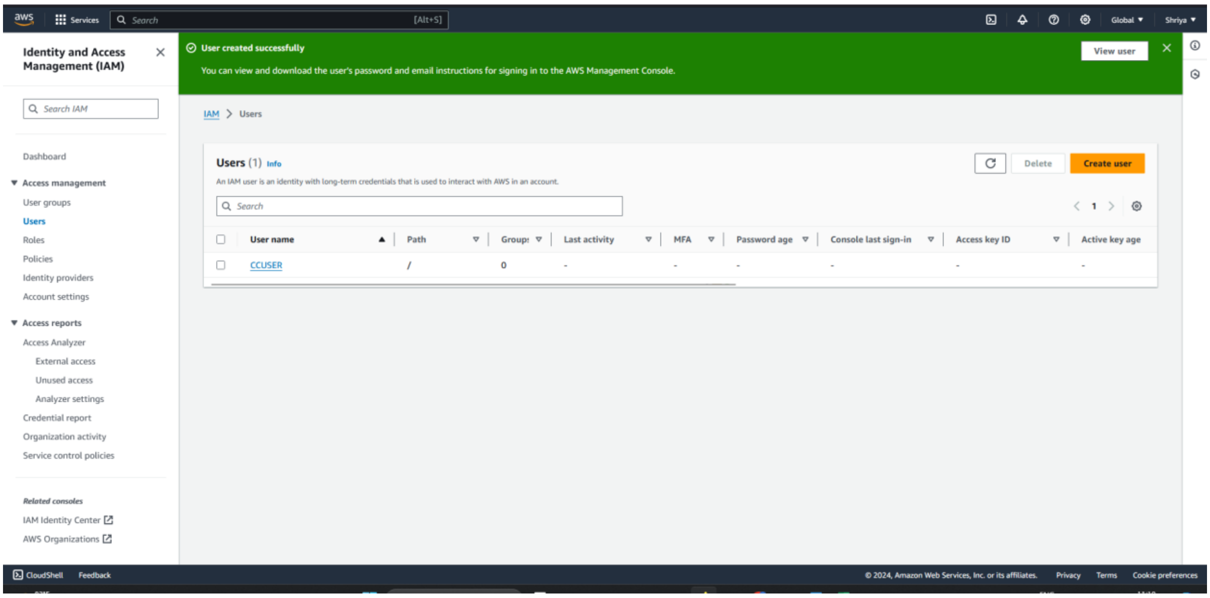
Tags - *optional*

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.

You can add up to 50 more tags.

Step9: On the user name click with a underline in blue colour.



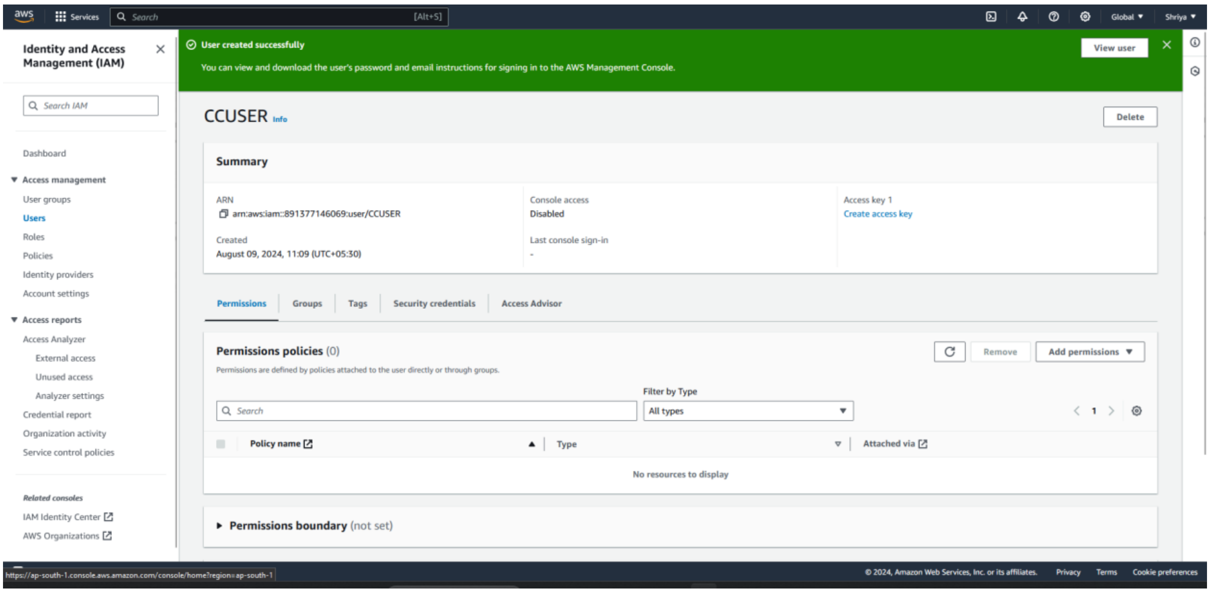
User created successfully

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

Users (1)

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

□	User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age
□	CCUSER	/	0	-	-	-	-	-	-



User created successfully

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

CCUSER Info

Summary

ARN: arn:aws:iam::891377146069:user/CCUSER

Created: August 09, 2024, 11:09 (UTC+05:30)

Console access: Disabled

Last console sign-in: -

Access key 1: Create access key

Permissions policies (0)

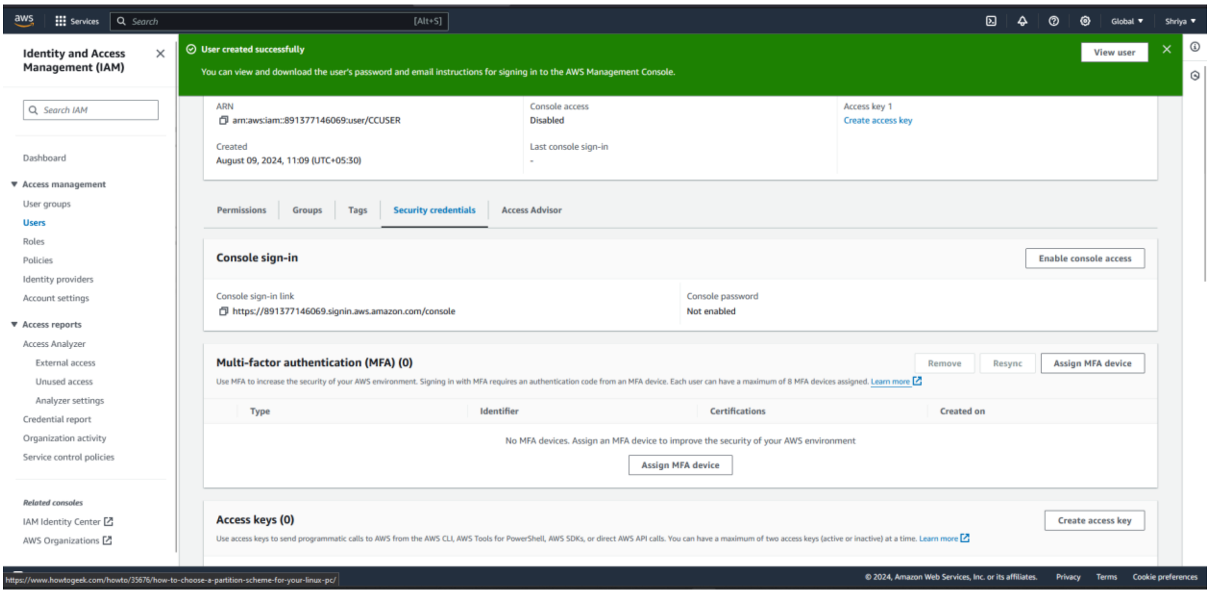
Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

Policy name	Type	Attached via
No resources to display		

Permissions boundary (not set)

Step10: Click on Security Credentials and click on Enable Console Access.



User created successfully

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

ARN: arn:aws:iam::891377146069:user/CCUSER

Created: August 09, 2024, 11:09 (UTC+05:30)

Console access: Disabled

Last console sign-in: -

Access key 1: Create access key

Console sign-in

Console sign-in link: https://891377146069.signin.aws.amazon.com/console

Console password: Not enabled

Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

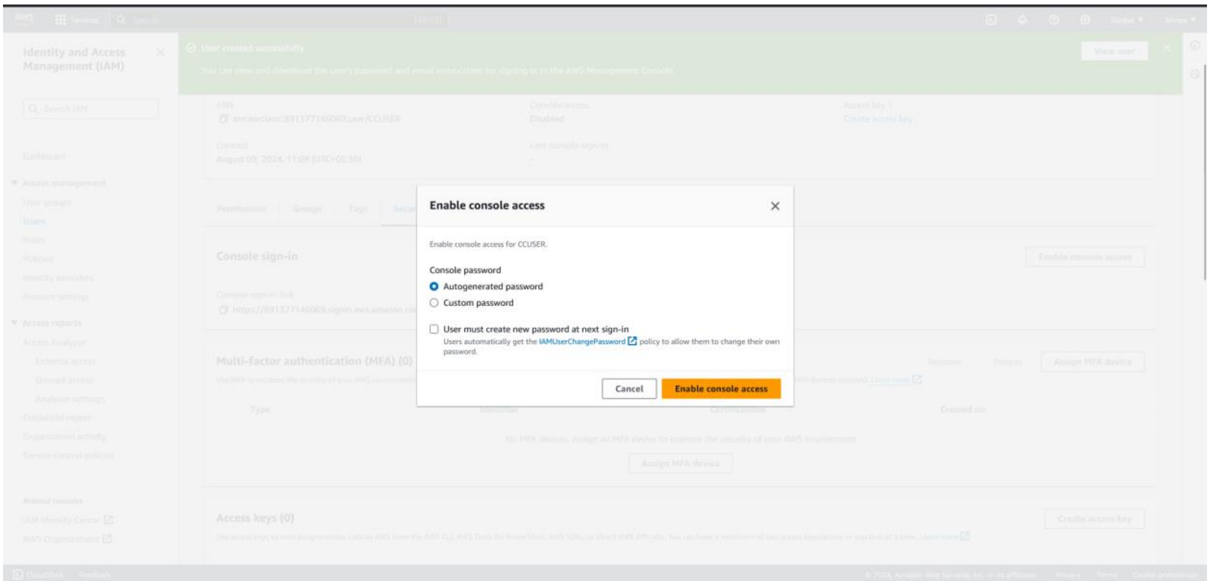
Type	Identifier	Certifications	Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Access keys (0)

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

Step11: Click on autogenerated pass and click on Enable console.



Enable console access ✕

Enable console access for CCUSER.

Console password

● Autogenerated password

○ Custom password

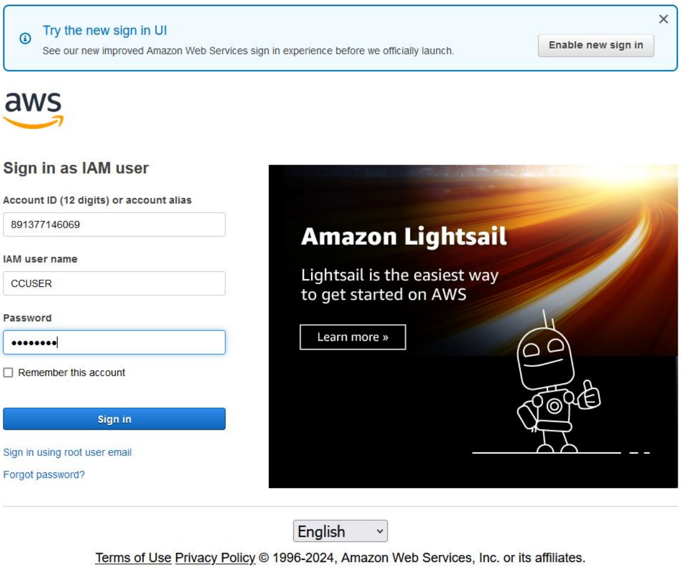
□ User must create new password at next sign-in

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

Step12: Download.csv file.

Step13: Go to incognitive mode and then search AWS and click on AWS

services and login with the user name and password created in Step11



Try the new sign in UI

See our new improved Amazon Web Services sign in experience before we officially launch.

Sign in as IAM user

Account ID (12 digits) or account alias: 891377146069

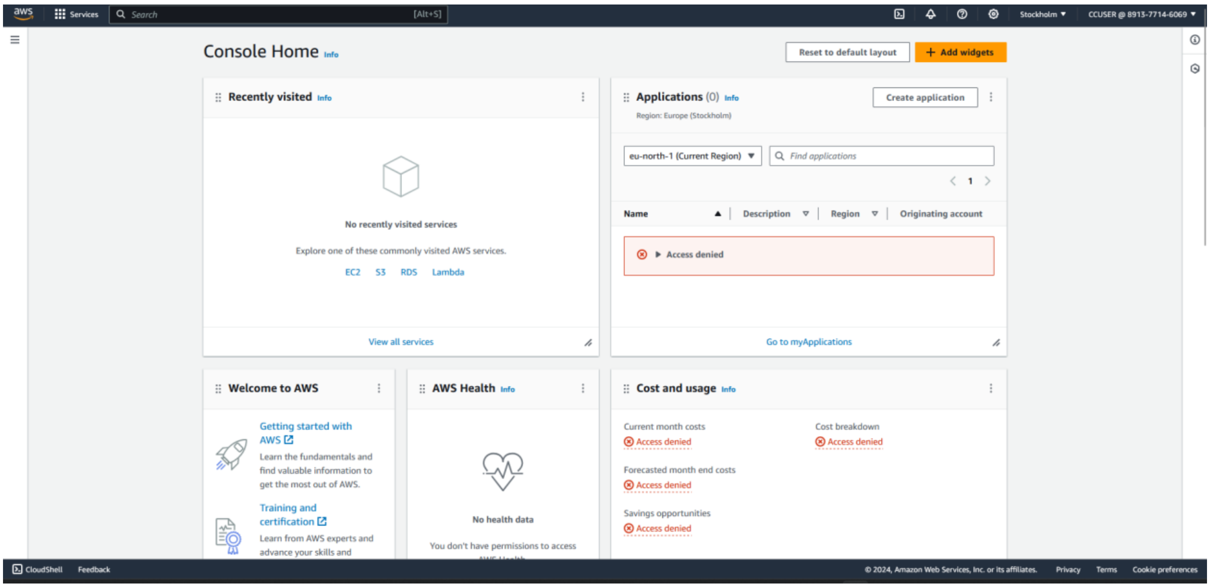
IAM user name: CCUSER

Password: ••••••••

□ Remember this account

Sign in
Sign in using root user email
Forgot password?
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »
English

Terms of Use Privacy Policy © 1996-2024, Amazon Web Services, Inc. or its affiliates.



Console Home Info

Recently visited Info

No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 RDS Lambda

Applications (0) Info

Region: Europe (Stockholm)

eu-north-1 (Current Region)

Find applications

Name	Description	Region	Originating account
Access denied			

Welcome to AWS

Getting started with AWS

Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification

Learn from AWS experts and advance your skills and

AWS Health Info

No health data

You don't have permissions to access

Cost and usage Info

Current month costs: Access denied

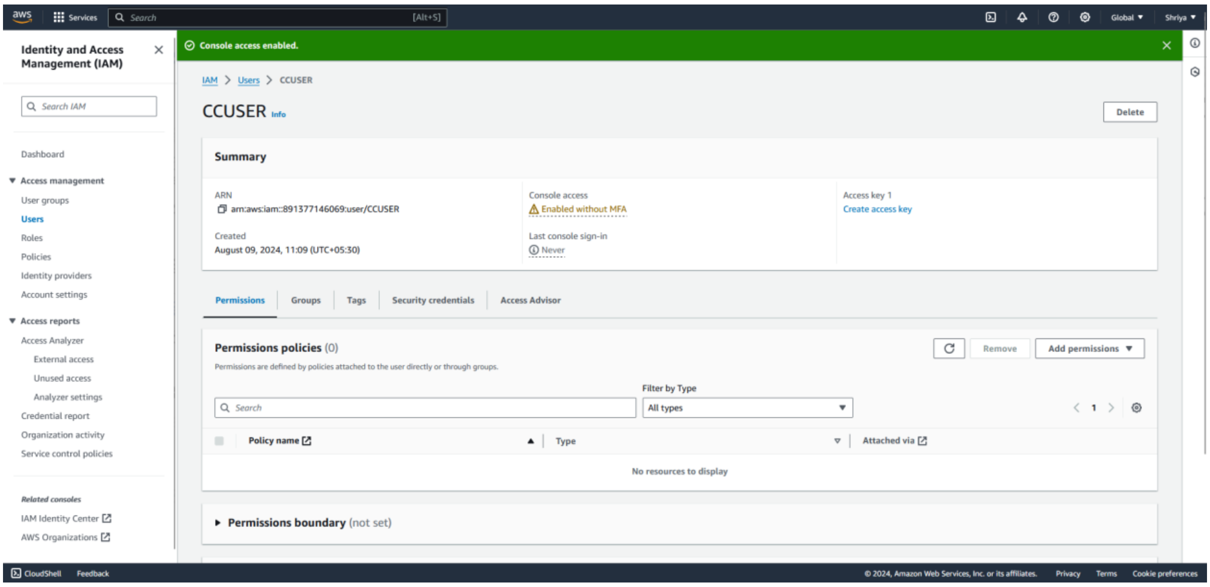
Cost breakdown: Access denied

Forecasted month end costs: Access denied

Savings opportunities: Access denied

© 2024, Amazon Web Services, Inc. or its affiliates.

Step14: Click on Permission to give access to S3



Identity and Access Management (IAM)

Console access enabled.

IAM > Users > CCUSER

CCUSER Info

Summary

ARN: arn:aws:iam::891377146069:user/CCUSER

Created: August 09, 2024, 11:09 (UTC+05:30)

Console access: Enabled without MFA

Last console sign-in: Never

Access key 1: Create access key

Permissions policies (0)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

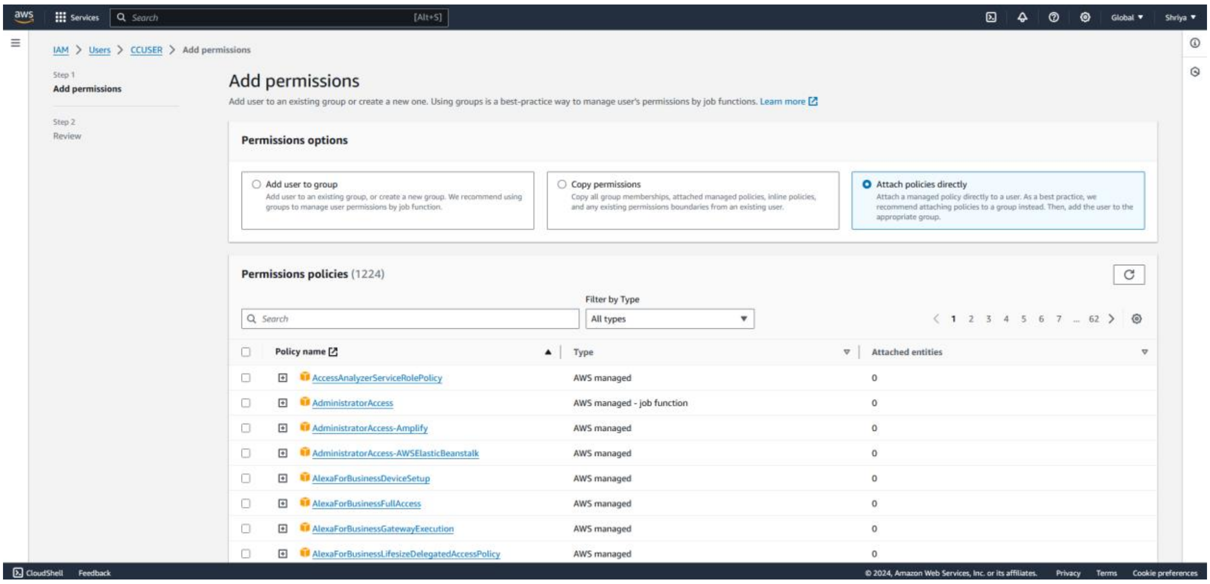
Policy name	Type	Attached via
No resources to display		

Permissions boundary (not set)

© 2024, Amazon Web Services, Inc. or its affiliates.

Step15: Click on Add Permissions and then select Add permissions.

Step16: Click on Attach Policies Directly.



IAM > Users > CCUSER > Add permissions

Step 1
Add permissions

Step 2
Review

Add 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, inline policies, and any existing permissions boundaries 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.

Permissions policies (1224)

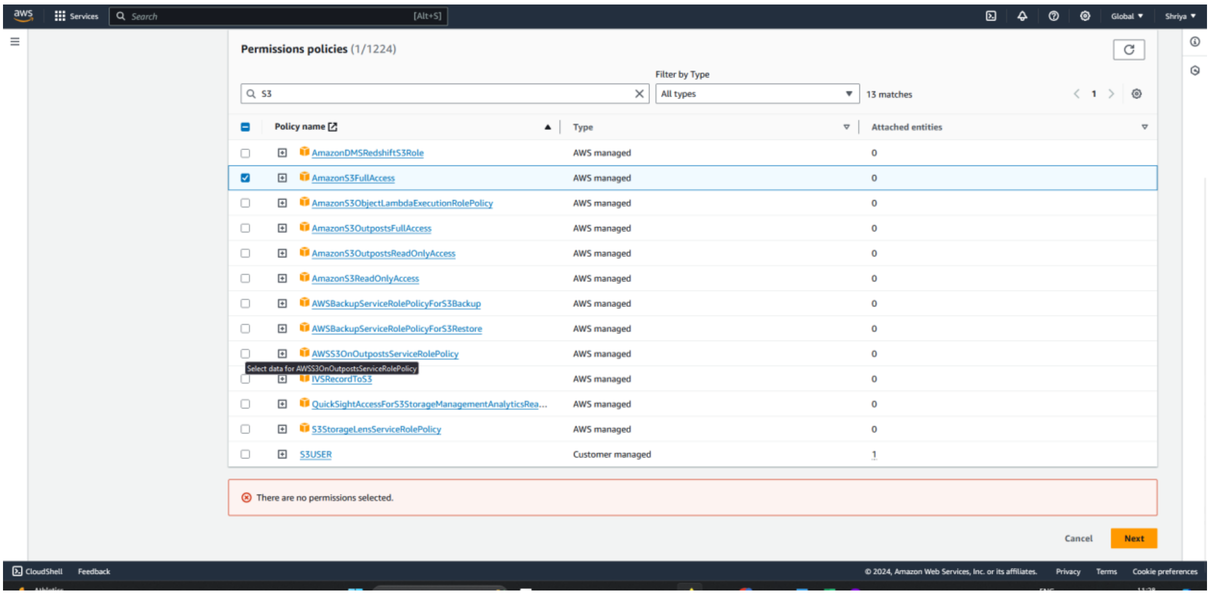
Filter by Type: All types

< 1 2 3 4 5 6 7 ... 62 >

□	Policy name	Type	Attached entities
□	AccessAnalyzerServiceRolePolicy	AWS managed	0
□	AdministratorAccess	AWS managed - job function	0
□	AdministratorAccess-Amplify	AWS managed	0
□	AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
□	AlexaForBusinessDeviceSetup	AWS managed	0
□	AlexaForBusinessFullAccess	AWS managed	0
□	AlexaForBusinessGatewayExecution	AWS managed	0
□	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	0

Step17: Search S3 and then select S3 give full access.

Step18: Click on next.



Permissions policies (1/1224)

Filter by Type: All types

Search: S3

13 matches

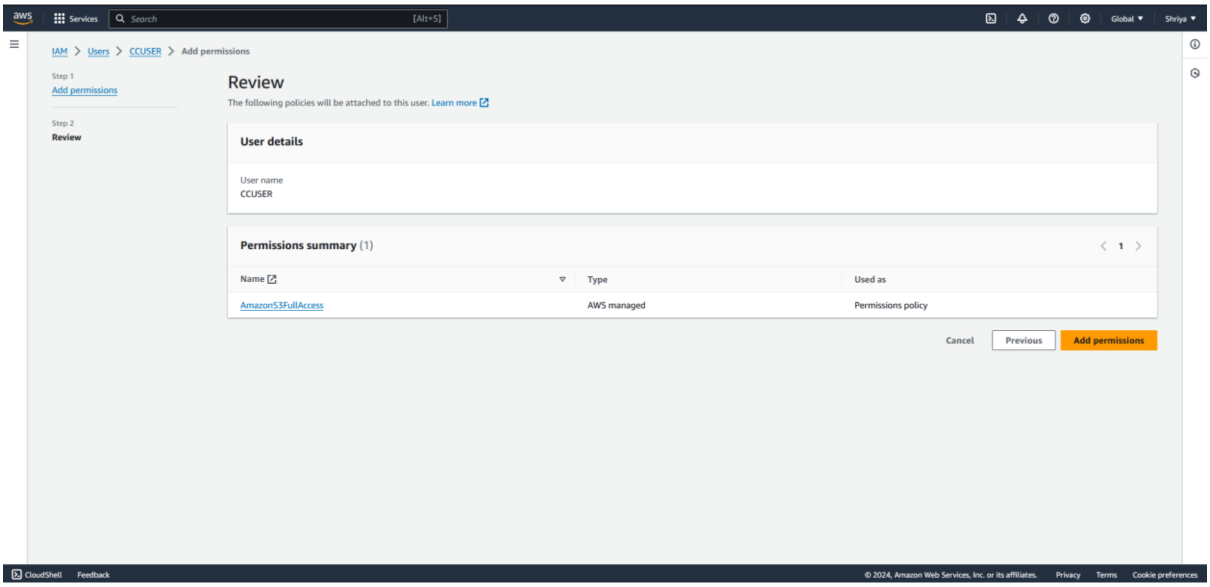
< 1 >

☐	Policy name	Type	Attached entities
□	AmazonDMSRedshiftS3Role	AWS managed	0
☑	AmazonS3FullAccess	AWS managed	0
□	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	0
□	AmazonS3OutpostsFullAccess	AWS managed	0
□	AmazonS3OutpostsReadOnlyAccess	AWS managed	0
□	AmazonS3ReadOnlyAccess	AWS managed	0
□	AWSBackupServiceRolePolicyForS3Backup	AWS managed	0
□	AWSBackupServiceRolePolicyForS3Restore	AWS managed	0
□	AWSS3OnOutpostsServiceRolePolicy	AWS managed	0
□	IVSRecordToS3	AWS managed	0
□	QuickSightAccessForS3StorageManagementAnalyticsRea...	AWS managed	0
□	S3StorageLensServiceRolePolicy	AWS managed	0
□	S3USER	Customer managed	1

Select data for AWSS3OnOutpostsServiceRolePolicy

There are no permissions selected.

Step19: Click on Add Permissions.



Review

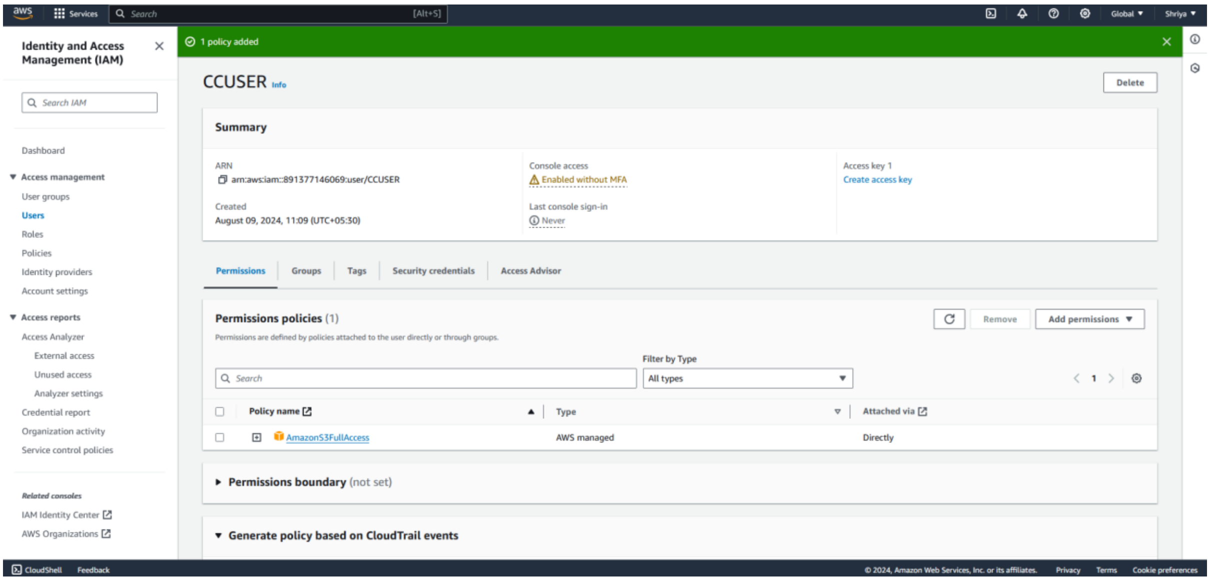
The following policies will be attached to this user. Learn more

User details

User name
CCUSER

Permissions summary (1)

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy



1 policy added

CCUSER

Summary

ARN
arn:aws:iam::891377146069:user/CCUSER

Created
August 09, 2024, 11:09 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Never

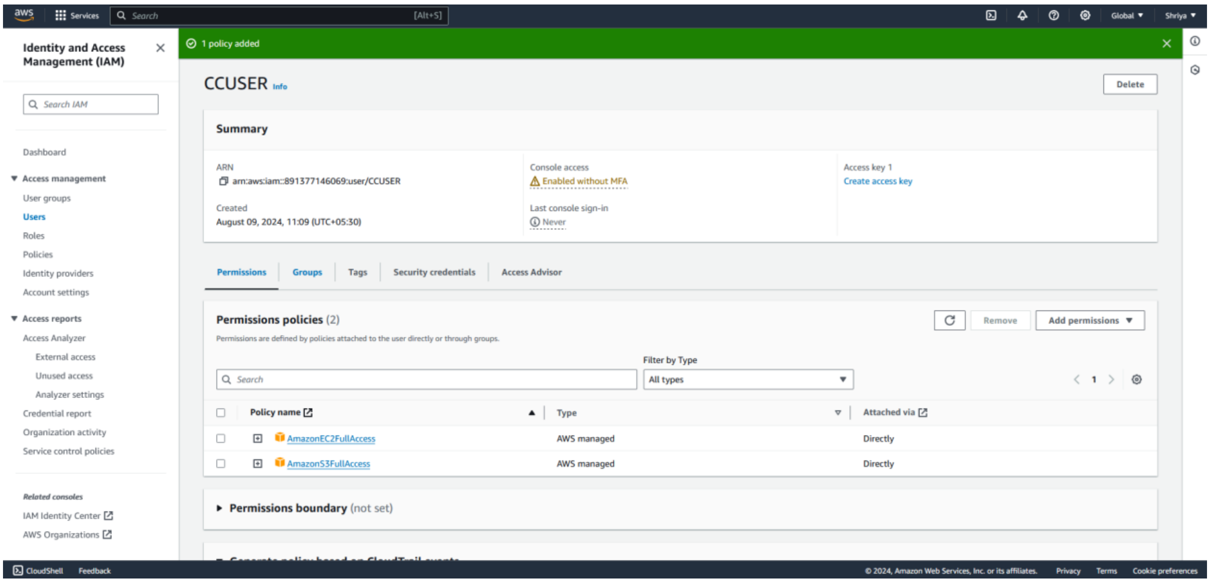
Access key 1
Create access key

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

□	Policy name	Type	Attached via
□	AmazonS3FullAccess	AWS managed	Directly

Step20: Follow similar method to add EC2.



1 policy added

CCUSER Info

Summary

ARN
arn:aws:iam::891377146069:user/CCUSER

Created
August 09, 2024, 11:09 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type
All types

□	Policy name	Type	Attached via
□	AmazonEC2FullAccess	AWS managed	Directly
□	AmazonS3FullAccess	AWS managed	Directly

Permissions boundary (not set)

Generate policy based on CloudTrail events

© 2024, Amazon Web Services, Inc. or its affiliates.

Step20: Now go on incognitive mode and then login into aws using the ashish user name and password you have created then you can see that ashish will have full access to S3 and EC2.