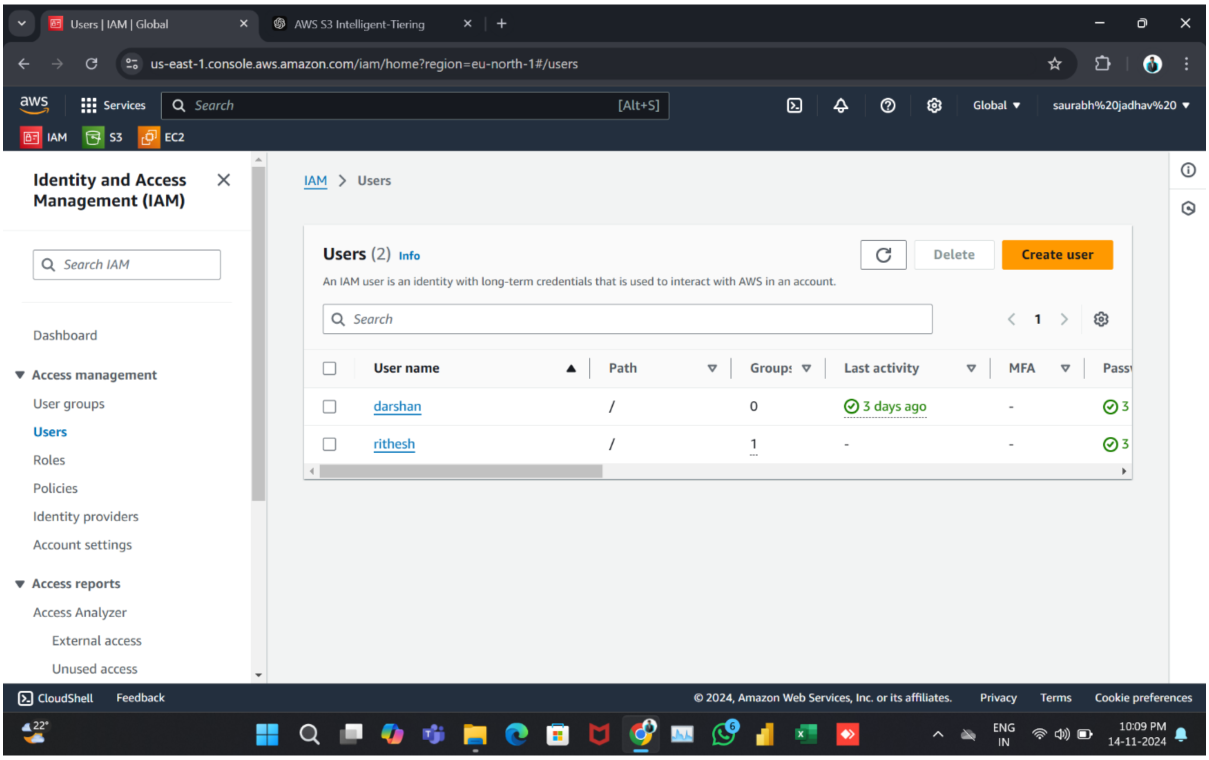
Saurabh Sanjiv Jadhav

AWS Tasks Submission

1. Task : Create User And Apply the S3 Permission For One Hours .

1 . Create a User in iam service



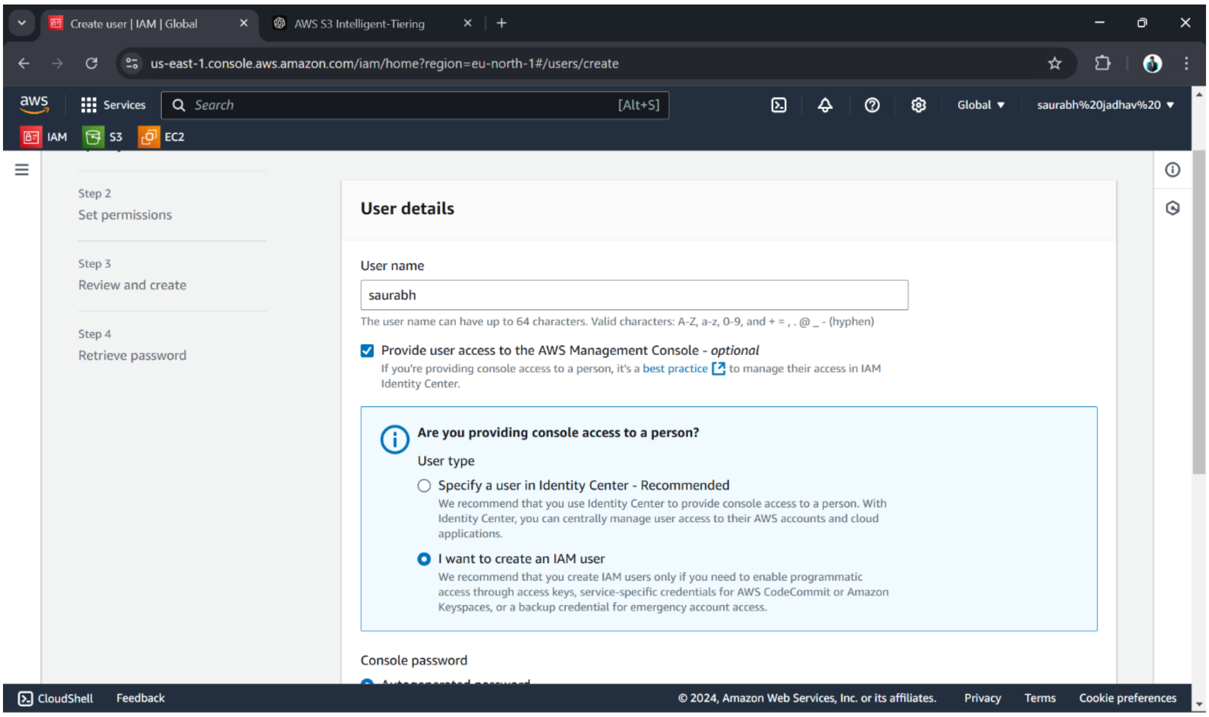
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users

Users (2) Info

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

User name	Path	Groups	Last activity	MFA	Pass
darshan	/	0	3 days ago	-	3
rithesh	/	1	-	-	3

2 . Enter New User Name



us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create

User details

User name: saurabh

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.

Are you providing console access to a person?

User type

○ Specify a user in Identity Center - Recommended

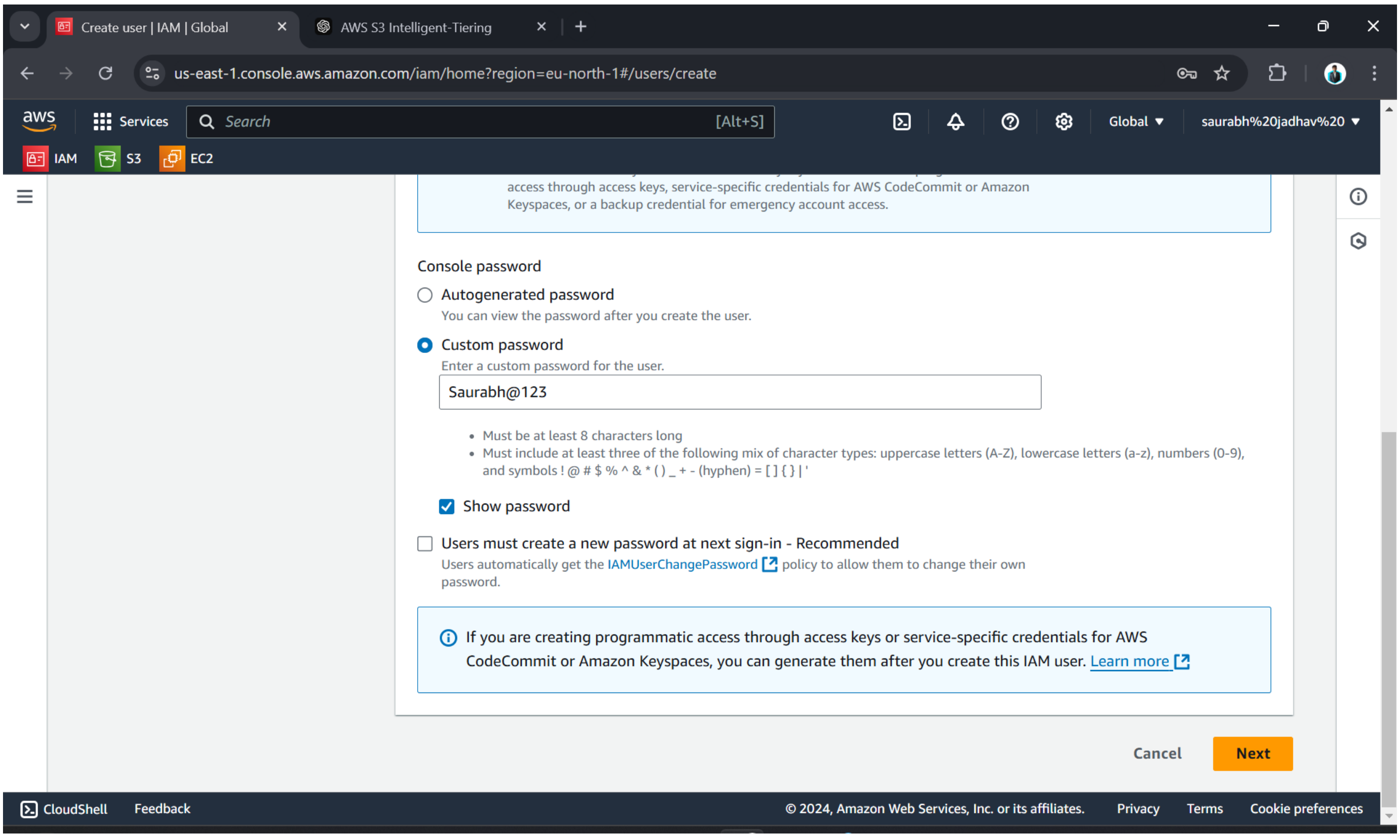
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

3.Enter the Password.



access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

○ Autogenerated password
You can view the password after you create the user.

● Custom password
Enter a custom password for the user.

Saurabh@123

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

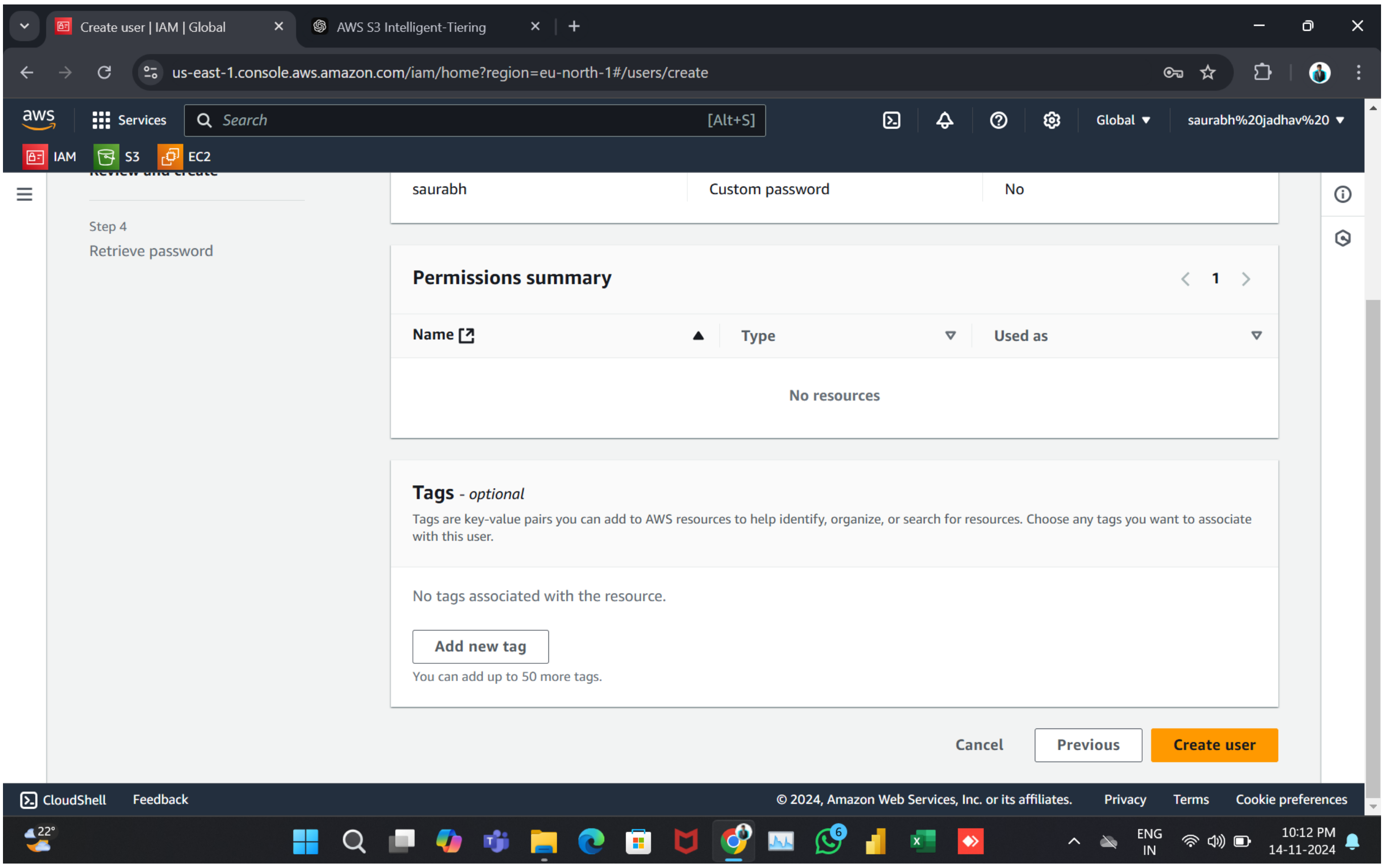
☑ Show password

□ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

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

Create user | IAM | Global
AWS S3 Intelligent-Tiering
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create
Services
Search
[Alt+S]
Global
saurabh%20jadhav%20
IAM
S3
EC2
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

4. Click to Create User



saurabh	Custom password	No

Step 4
Retrieve password

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.

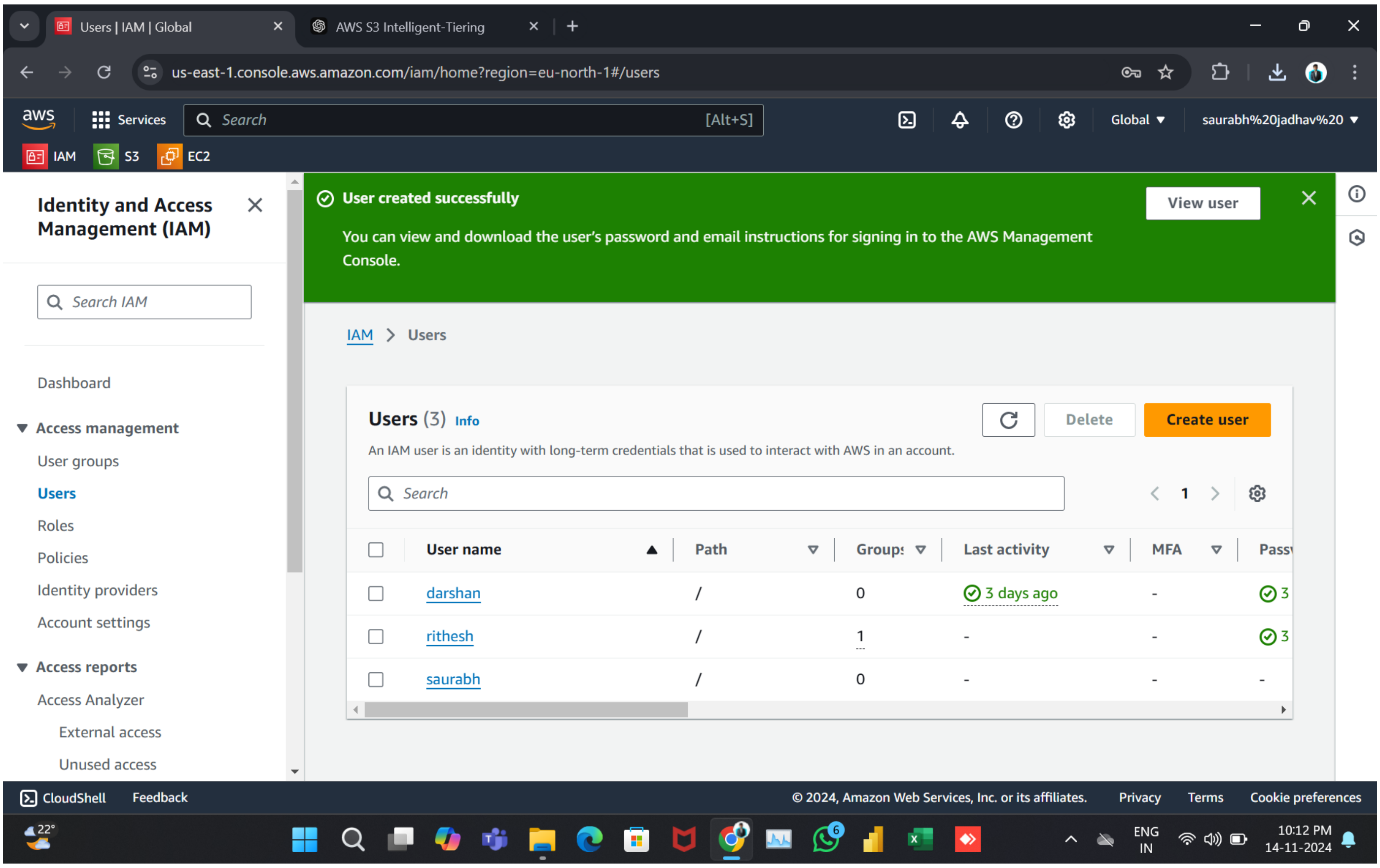
No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Create user | IAM | Global
AWS S3 Intelligent-Tiering
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create
Services
Search
[Alt+S]
Global
saurabh%20jadhav%20
IAM
S3
EC2
1
Cancel
Previous
Create user
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
22°
ENG
IN
10:12 PM
14-11-2024

5.Your User Is Successfully Created .



User created successfully

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

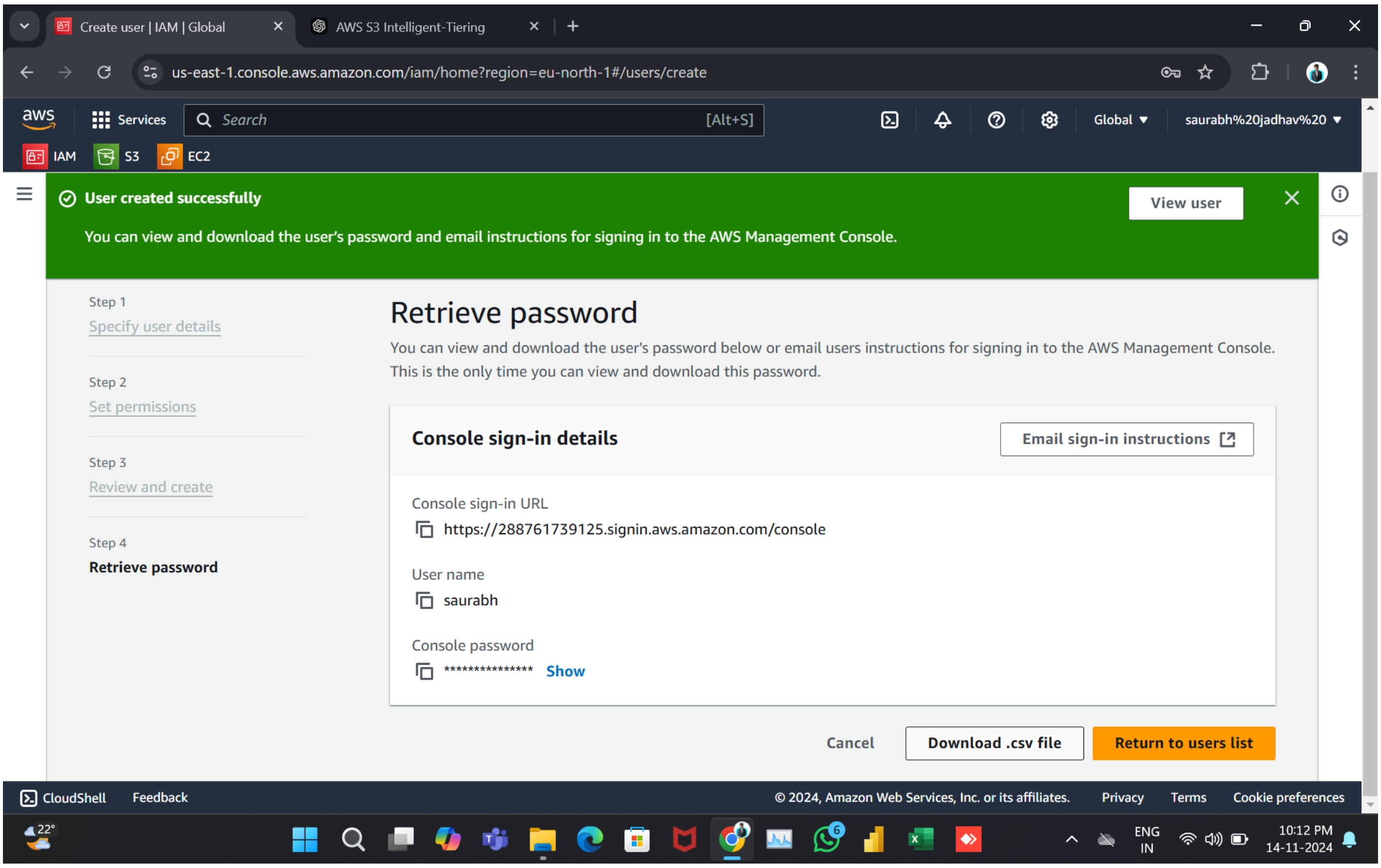
IAM > Users

Users (3) Info

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

	User name	Path	Groups	Last activity	MFA	Pass
□	darshan	/	0	✓ 3 days ago	-	✓ 3
□	rithesh	/	1	-	-	✓ 3
□	saurabh	/	0	-	-	-

6. Download .csv File



User created successfully

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

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

Step 4 Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

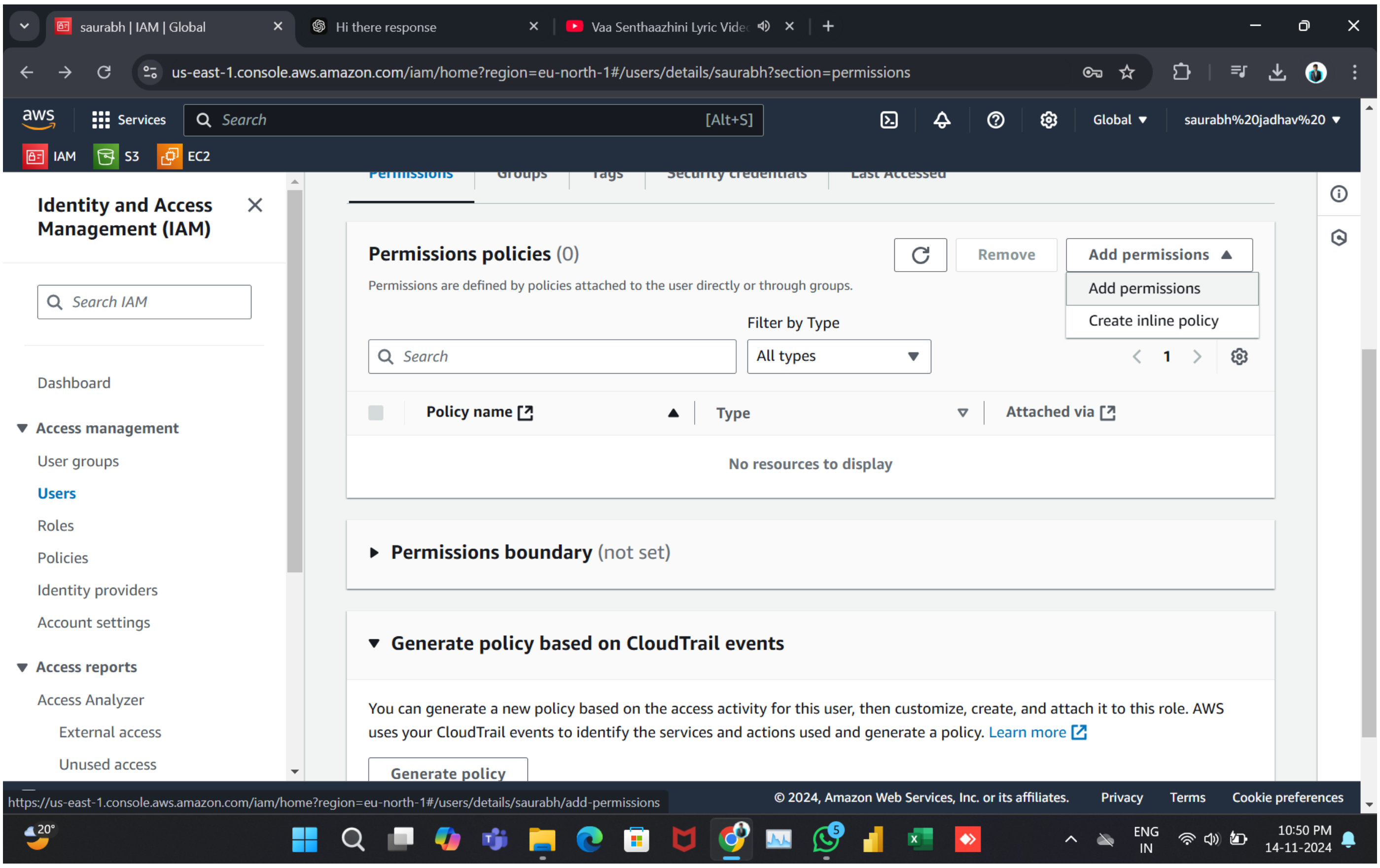
Console sign-in URL: https://288761739125.signin.aws.amazon.com/console

User name: saurabh

Console password: *************** Show

Create user | IAM | Global
AWS S3 Intelligent-Tiering
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create
Services
Search
[Alt+S]
Global
saurabh%20jadhav%20
IAM
S3
EC2
View user
Email sign-in instructions
Cancel
Download .csv file
Return to users list
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
22°
ENG IN
10:12 PM
14-11-2024

7. Add Permission To User



us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/saurabh?section=permissions

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management
- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports
- Access Analyzer
  - External access
  - Unused access

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)

Generate policy based on CloudTrail events

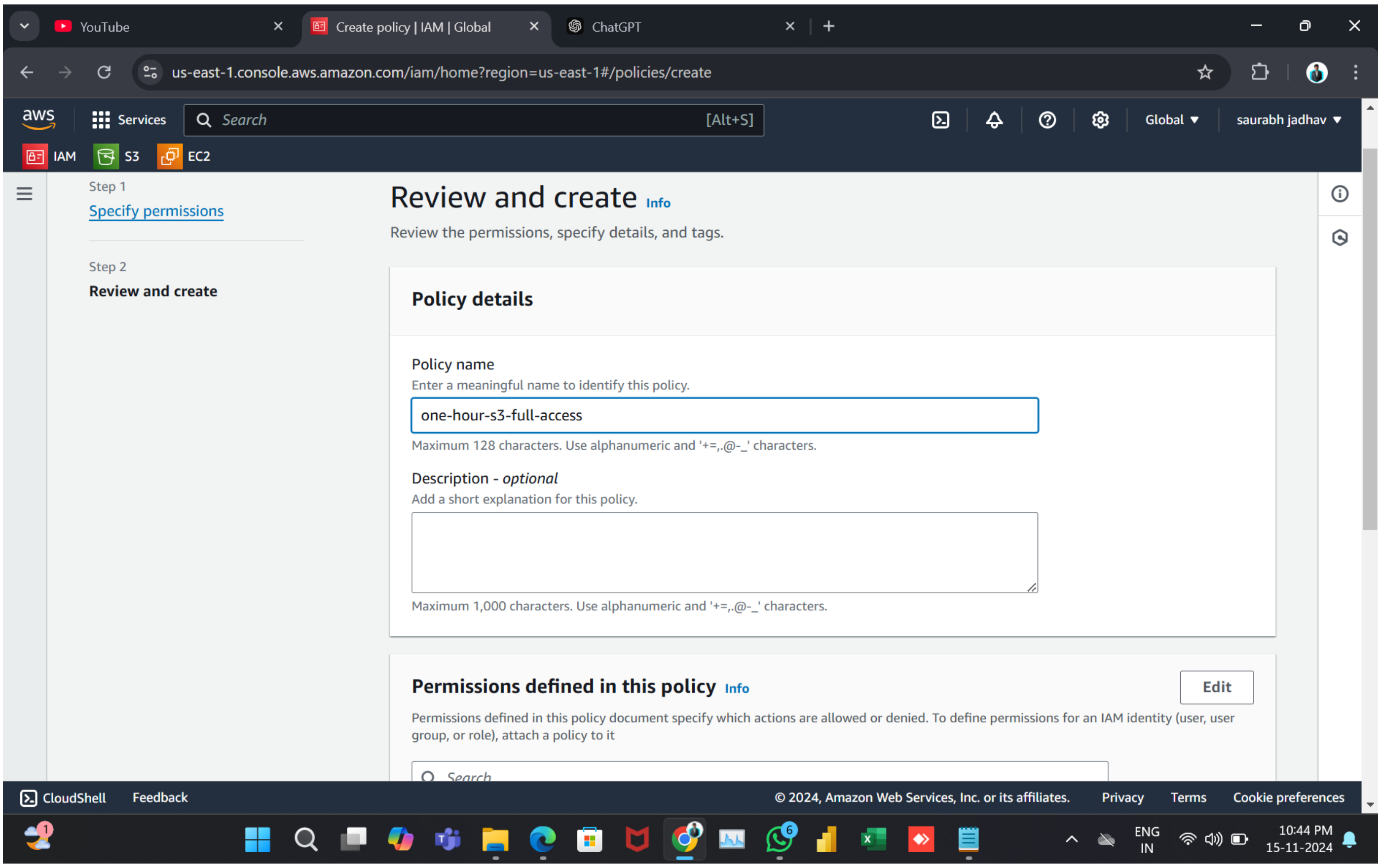
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

https://us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/saurabh/add-permissions

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

20° ENG IN 10:50 PM 14-11-2024

8. Create a AWS customer managed policy and Enter the Policy Name



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create

Step 1
Specify permissions

Step 2
Review and create

Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.
one-hour-s3-full-access
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

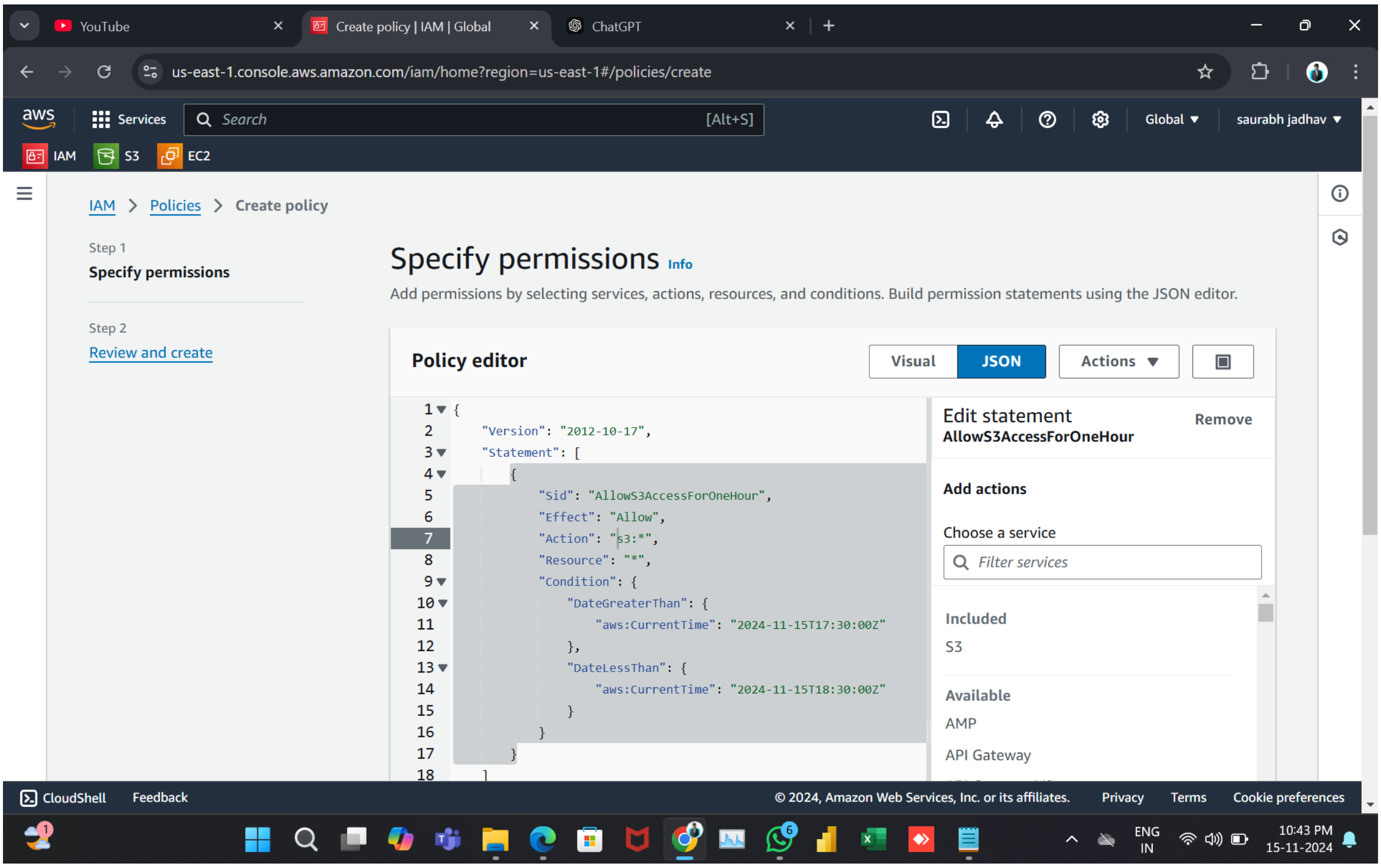
Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

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

ENG IN 10:44 PM 15-11-2024

9. Create or generator the 1 Hour S3 Full Acces Permission code in json format



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3AccessForOneHour",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2024-11-15T17:30:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2024-11-15T18:30:00Z"
                }
            }
        }
    ]
```

Edit statement
AllowS3AccessForOneHour

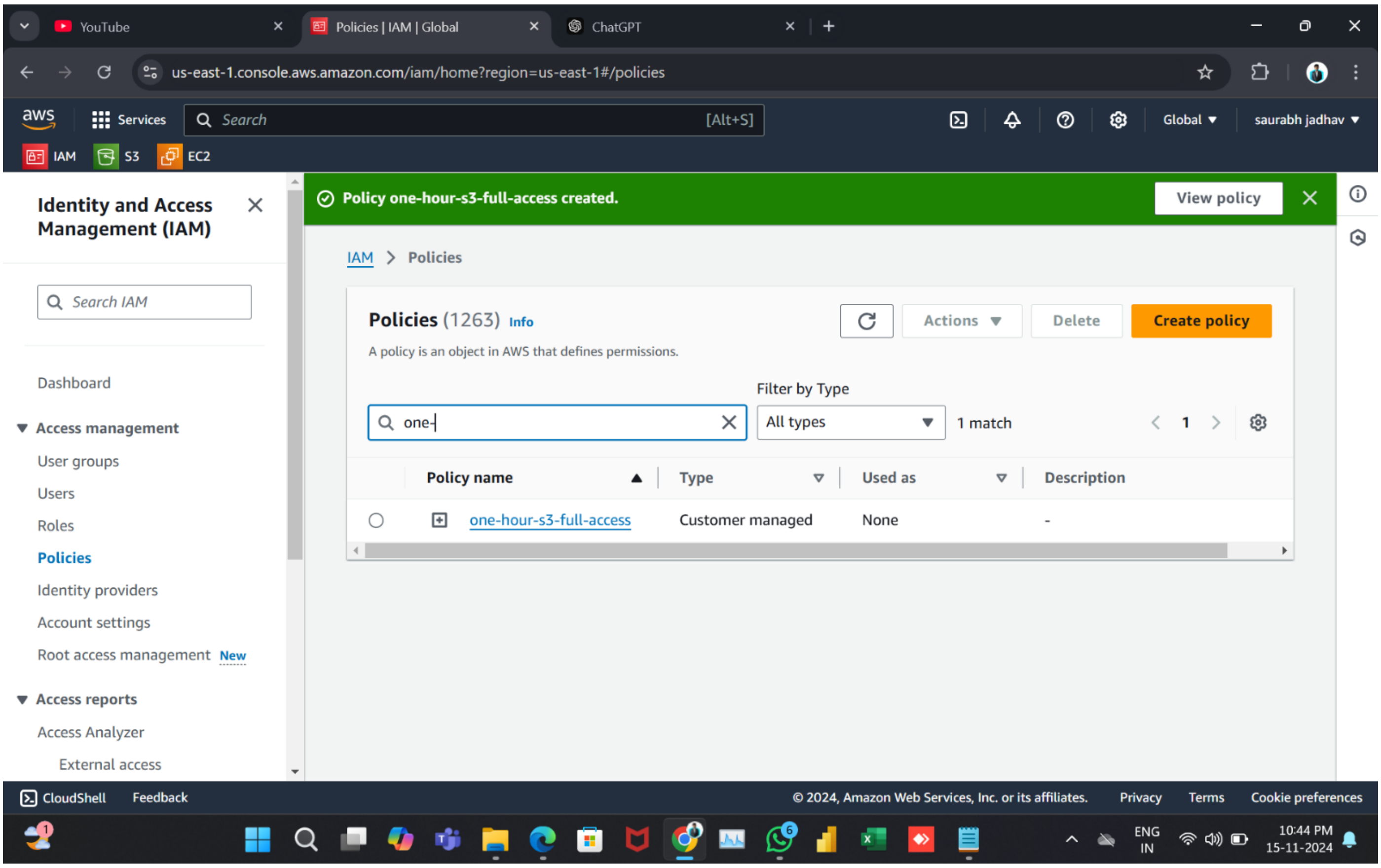
Add actions

Choose a service

Included
S3

Available
AMP
API Gateway

10. Successfully Created the policy.



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies

Policy one-hour-s3-full-access created.

IAM > Policies

Policies (1263) Info

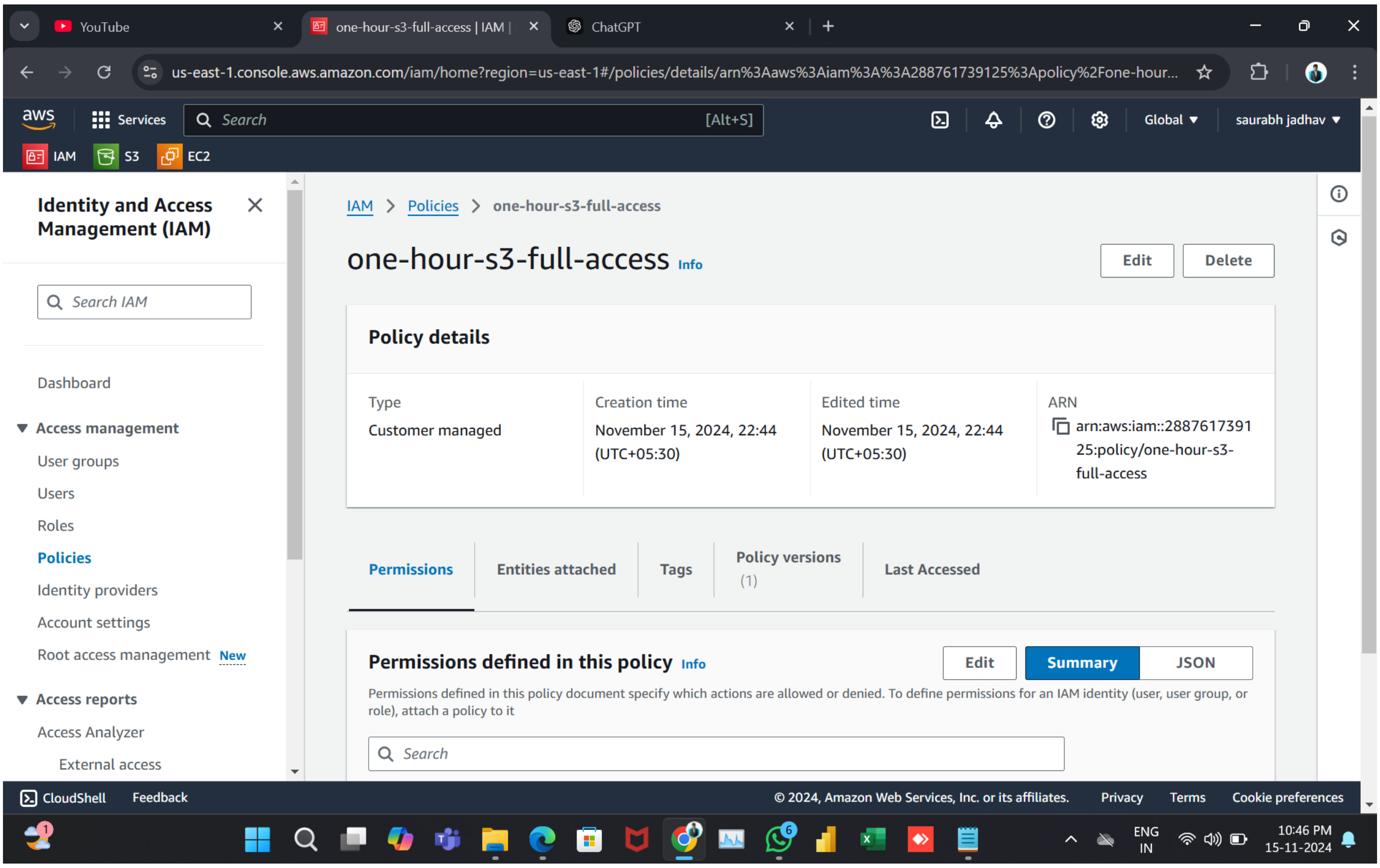
A policy is an object in AWS that defines permissions.

Filter by Type

Search: one | All types | 1 match

	Policy name ▲	Type	Used as	Description
○	one-hour-s3-full-access	Customer managed	None	-

11. Policy Details .



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3A288761739125%3Apolicy%2Fone-hour...

IAM > Policies > one-hour-s3-full-access

one-hour-s3-full-access Info

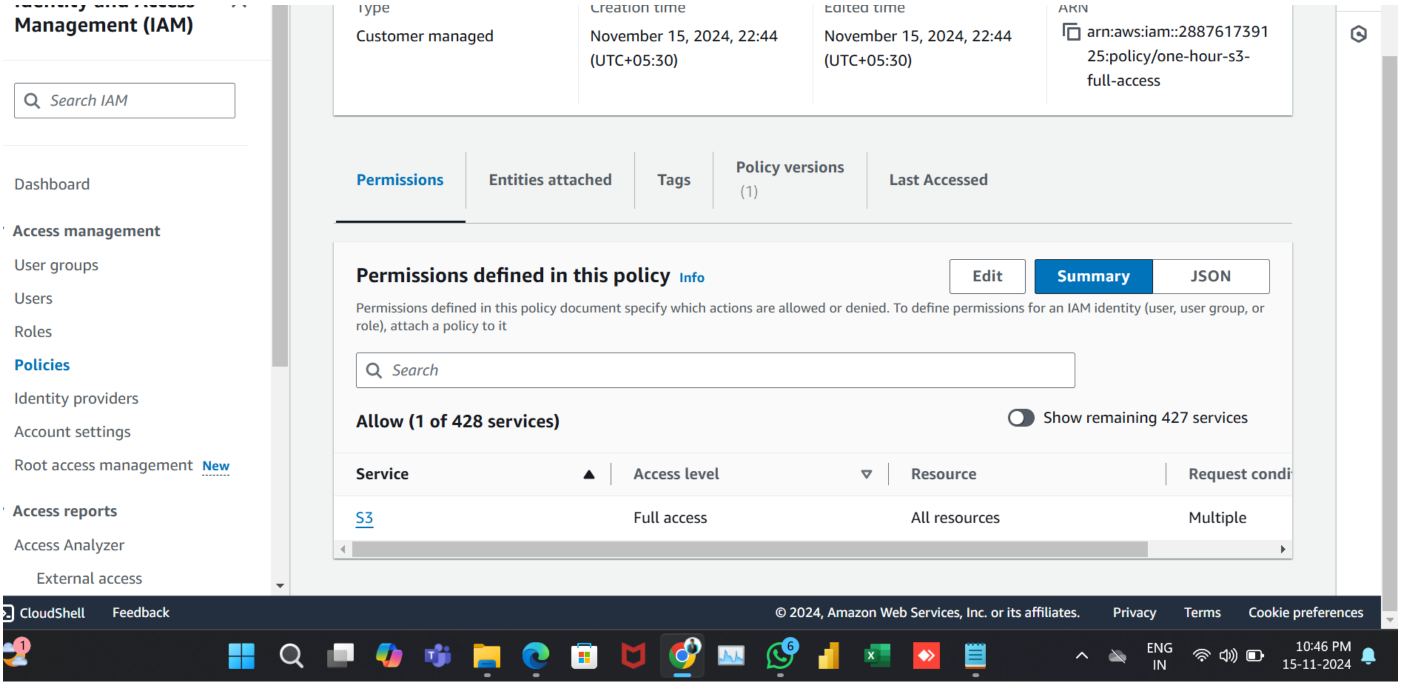
Policy details

Type	Creation time	Edited time	ARN
Customer managed	November 15, 2024, 22:44 (UTC+05:30)	November 15, 2024, 22:44 (UTC+05:30)	arn:aws:iam::288761739125:policy/one-hour-s3-full-access

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

12. S3 Full Access Successfully Allocated .



Type	Creation time	Edited time	ARN
Customer managed	November 15, 2024, 22:44 (UTC+05:30)	November 15, 2024, 22:44 (UTC+05:30)	arn:aws:iam::288761739125:policy/one-hour-s3-full-access

Permissions defined in this policy Info

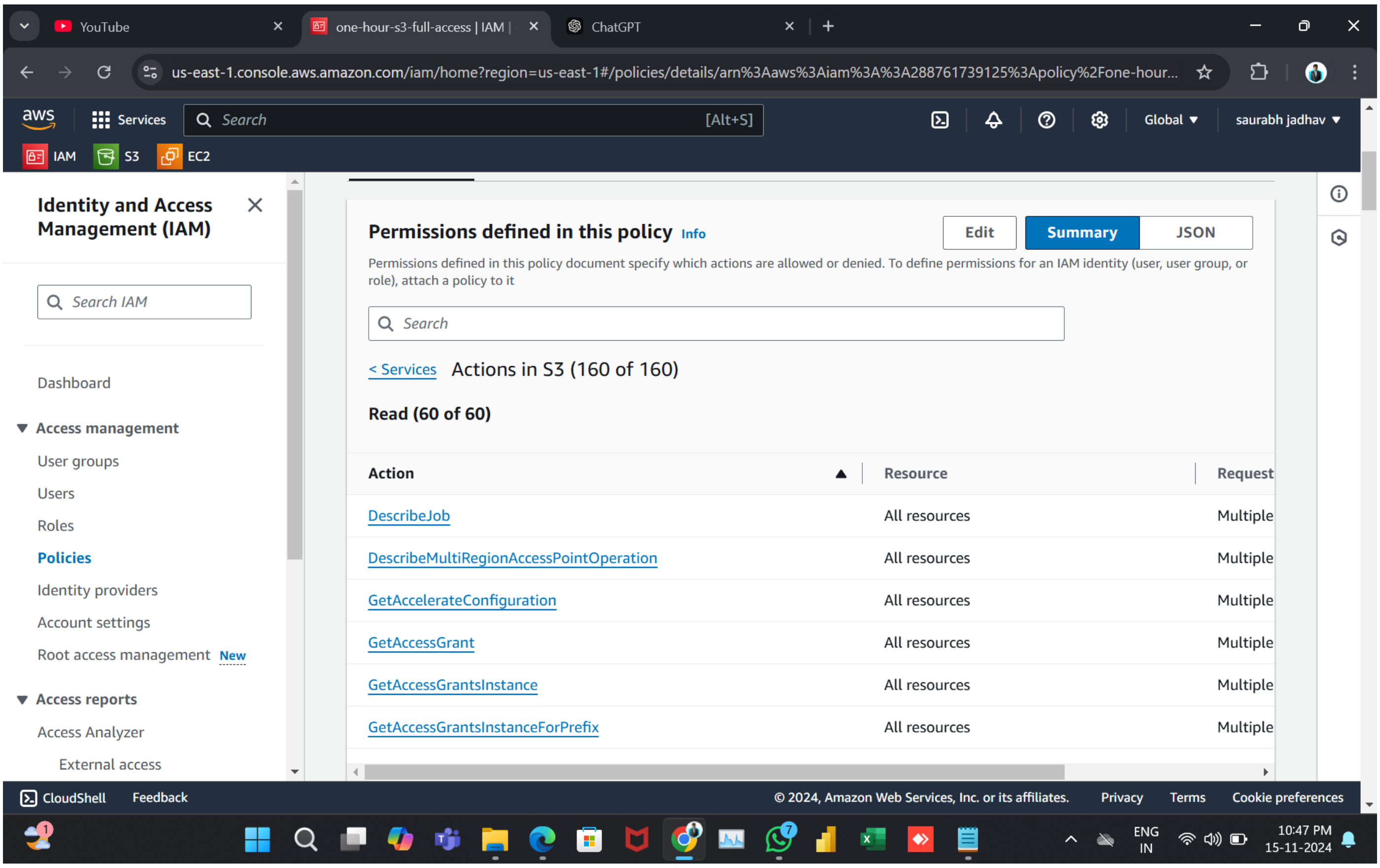
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 428 services)

Show remaining 427 services

Service	Access level	Resource	Request condi
S3	Full access	All resources	Multiple

13. View All Actions in S3



Permissions defined in this policy Info

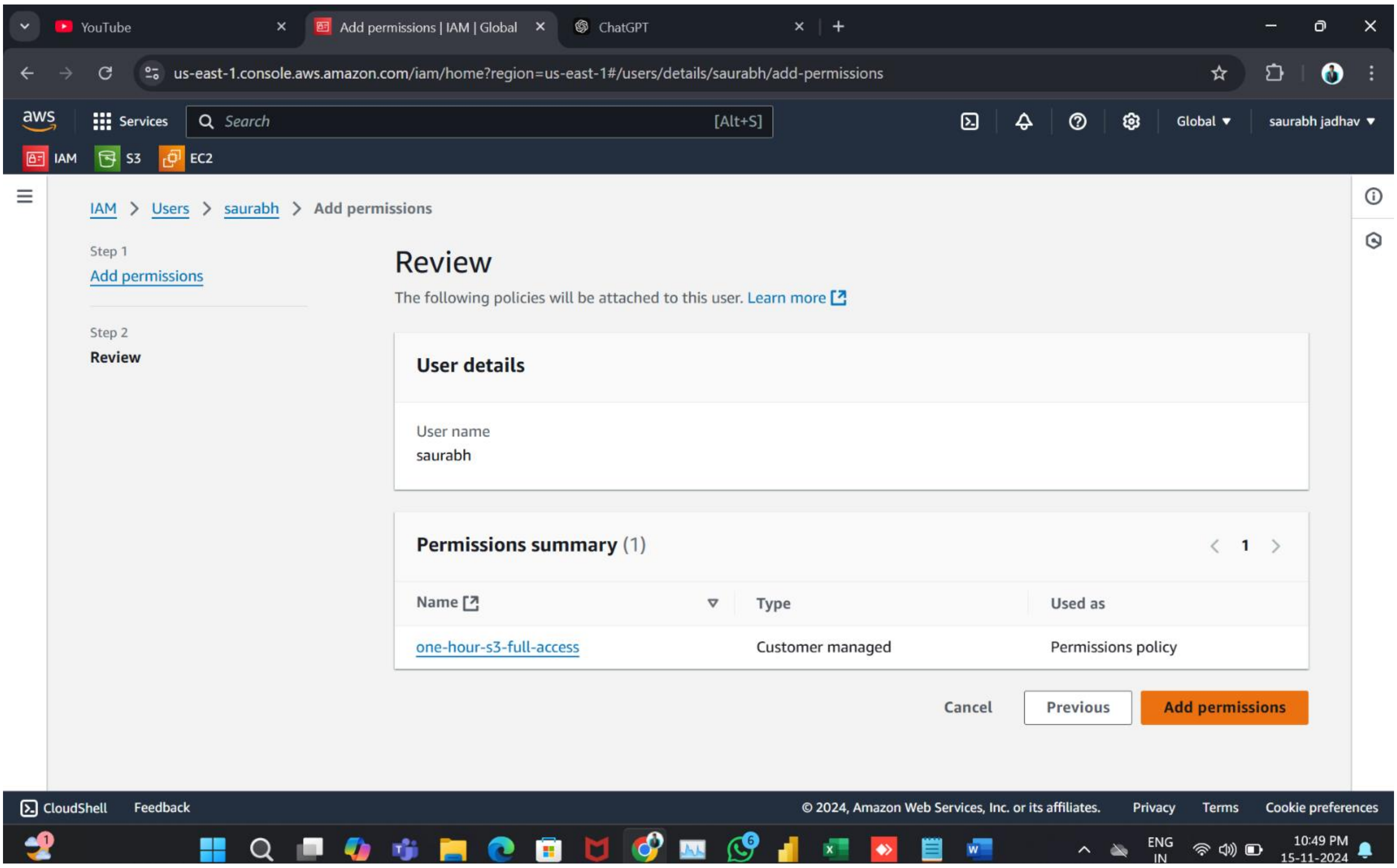
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

< Services Actions in S3 (160 of 160)

Read (60 of 60)

Action	Resource	Request
DescribeJob	All resources	Multiple
DescribeMultiRegionAccessPointOperation	All resources	Multiple
GetAccelerateConfiguration	All resources	Multiple
GetAccessGrant	All resources	Multiple
GetAccessGrantsInstance	All resources	Multiple
GetAccessGrantsInstanceForPrefix	All resources	Multiple

14. Add Permission to User


YouTube
Add permissions | IAM | Global
ChatGPT
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/saurabh/add-permissions
aws
Services
Search
[Alt+S]
Global
saurabh jadhav
IAM
S3
EC2
IAM > Users > saurabh > Add permissions
Step 1
Add permissions
Step 2
Review
Cancel
Previous
Add permissions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG IN
10:49 PM
15-11-2024

Review

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

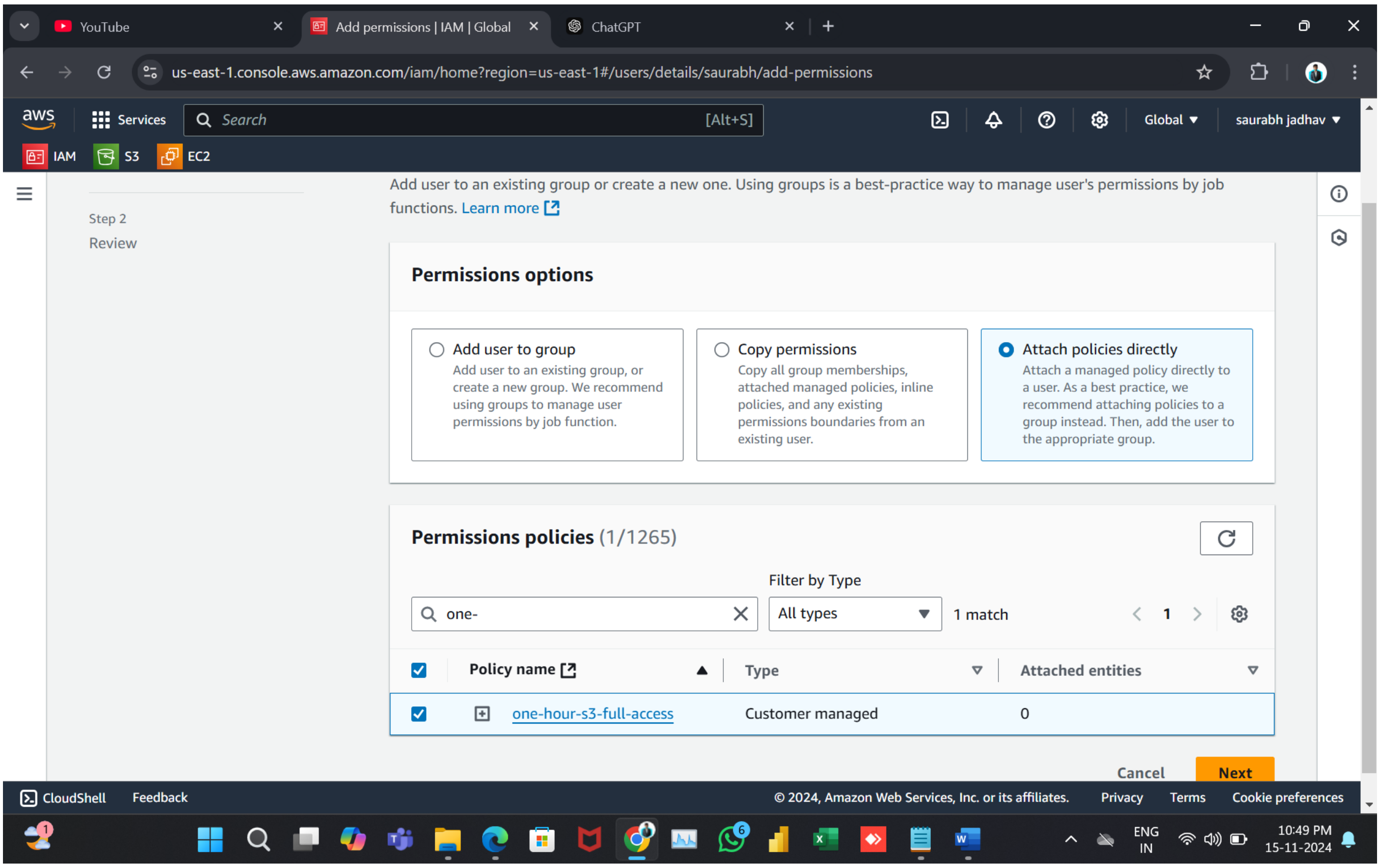
User details

User name
saurabh

Permissions summary (1)

Name	Type	Used as
one-hour-s3-full-access	Customer managed	Permissions policy

15. Attach Policies Directly And Select the Policy .



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/saurabh/add-permissions

Step 2
Review

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 (1/1265)

Filter by Type

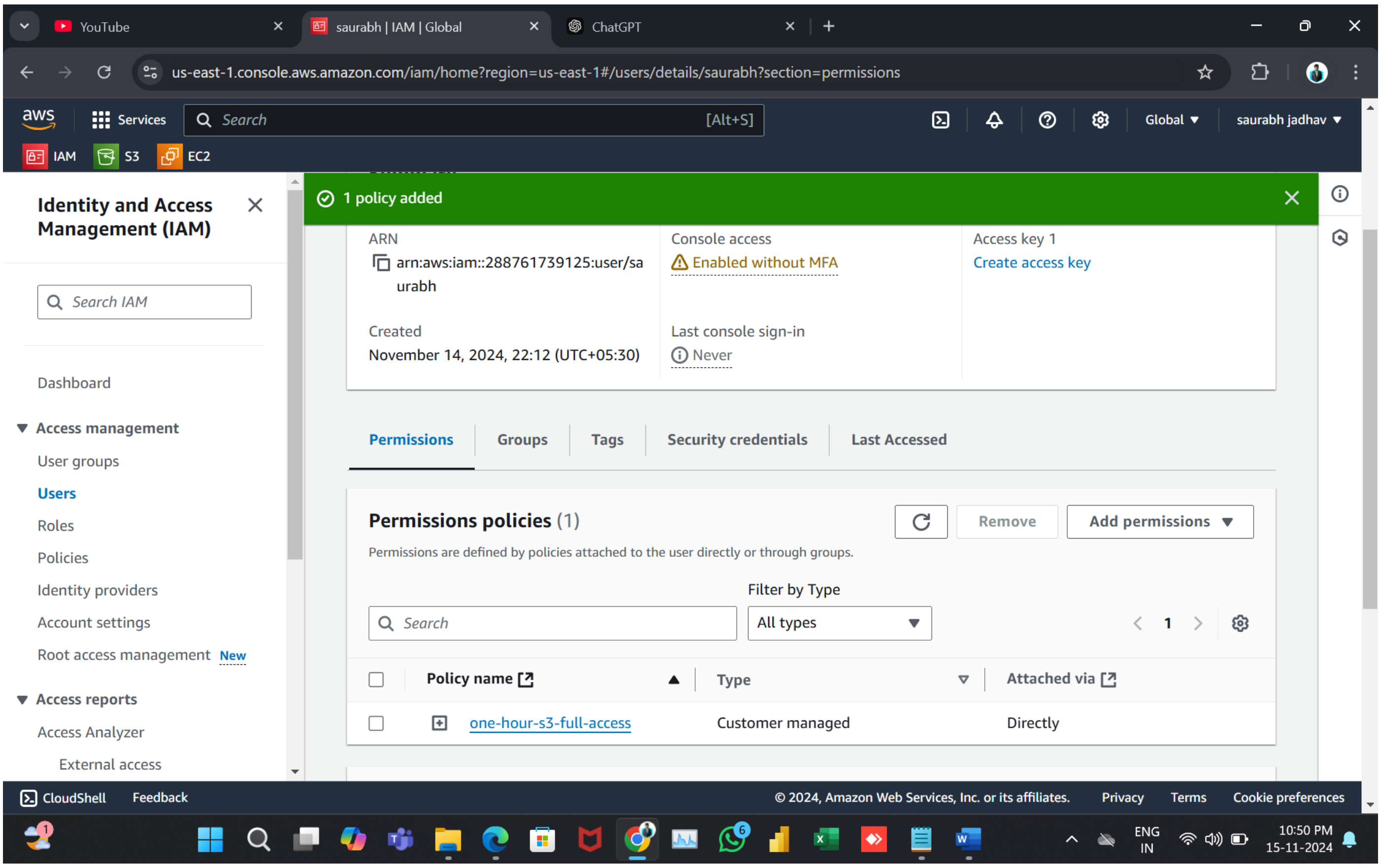
one- | All types | 1 match

☑	Policy name	Type	Attached entities
☑	one-hour-s3-full-access	Customer managed	0

Cancel Next

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

16. Successfully Attached the Policy to User .



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/saurabh?section=permissions

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management
- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports
- Access Analyzer
- External access

1 policy added

ARN
arn:aws:iam::288761739125:user/saurabh

Console access
Enabled without MFA

Access key 1
Create access key

Created
November 14, 2024, 22:12 (UTC+05:30)

Last console sign-in
Never

Permissions | Groups | Tags | Security credentials | Last Accessed

Permissions policies (1)

Remove Add permissions

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

Filter by Type

Search | All types

□	Policy name	Type	Attached via
□	one-hour-s3-full-access	Customer managed	Directly

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