

Cloud Computing

PRACTICAL 3

Identity Access Management

[Login as root user

Search iam (manage access to aws services)

Go to users write name create user

Giving access:- go to ARN(auto enable console ; what you want to show the user first page

Custom password you can set

Auto by computer

Then after copying the link sign in to I am user

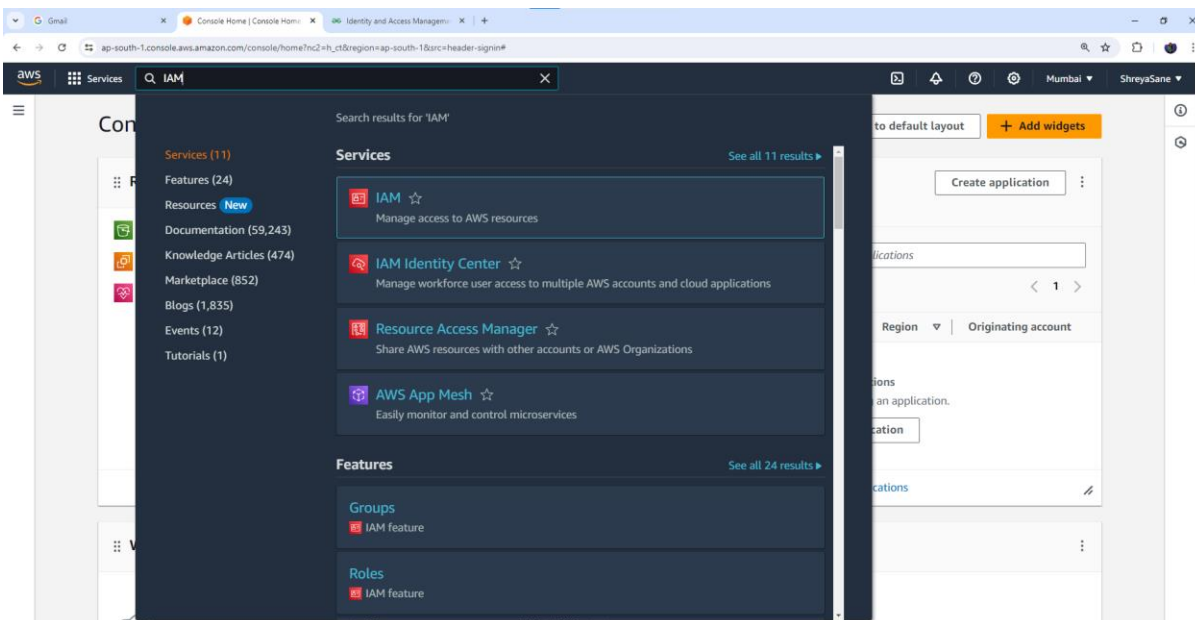
Create policies select service –S3 effect=allow sid name of root user create

go to json

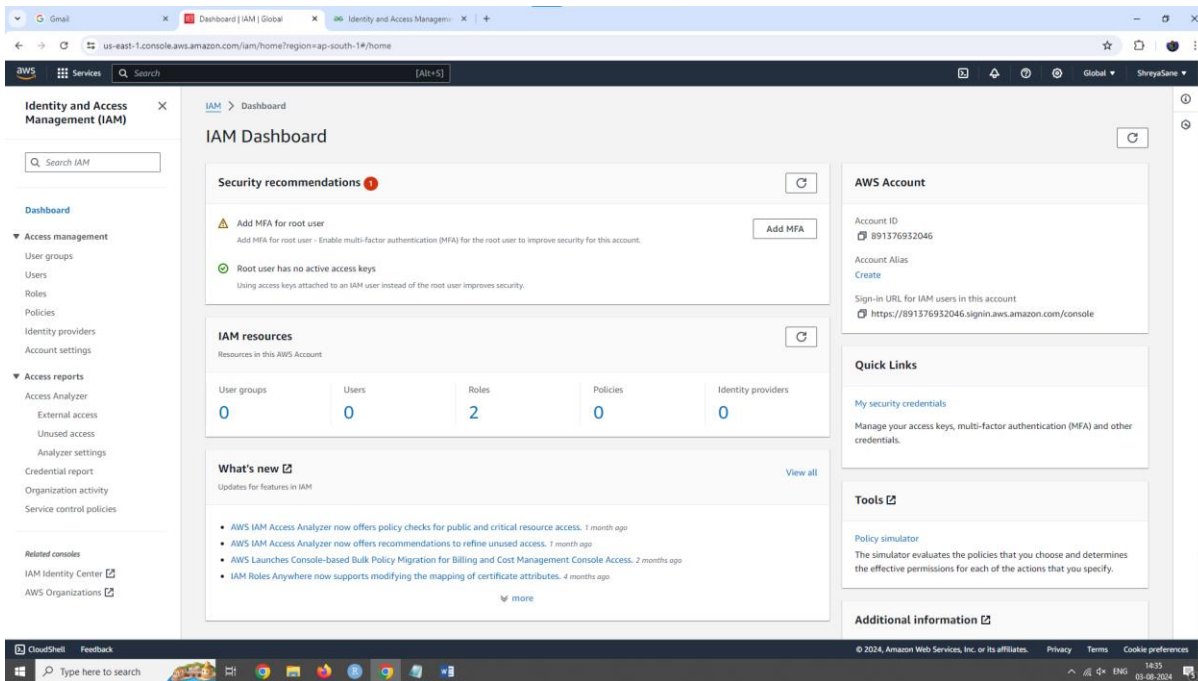
visualise : graphical access select s3 allow all options(*)

root user add permission attach policy search and add permission]

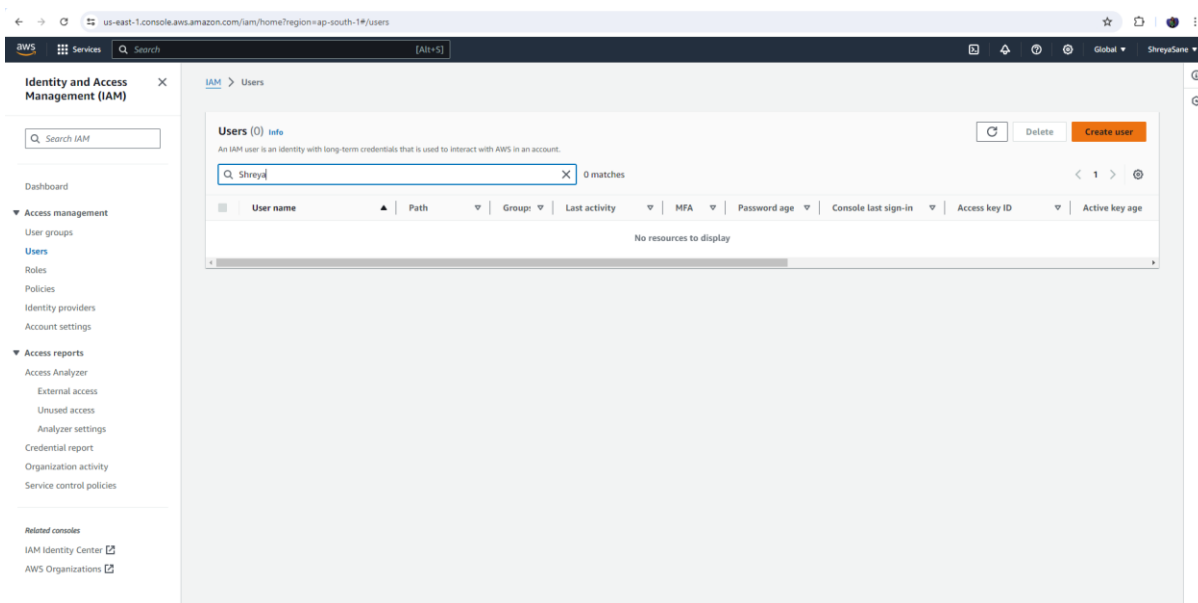
1: Search IAM Identify and manage access on AWS services)



Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science



2: Go to users ----> write name--> create user



3: Once the user is created we can create password by two method a) autogenerated b) custom
Tap on the user name that you created. Go into the Security credentials and enable console access.

Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science

This screenshot shows the 'Specify user details' step in the AWS IAM console. The user name 'Shreya_Sane' is entered in the 'User name' field. Below the field, a note states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, -, @, _ - (Pinyin)'. There is an unchecked checkbox for 'Provide user access to the AWS Management Console - optional' with a note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' A blue information box contains the text: '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'. At the bottom right are 'Cancel' and 'Next' buttons.

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

Specify user details

User details

User name
Shreya_Sane

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

☐ 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](#)

Cancel Next

This screenshot shows the 'Set permissions' step in the AWS IAM console. It includes three radio button options: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. The 'Add user to group' option has a sub-note: 'Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.' The 'Copy permissions' option has a sub-note: 'Copy all group memberships, attached managed policies, and inline policies from an existing user.' The 'Attach policies directly' option has a sub-note: '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.' Below these is a blue information box titled 'Get started with groups' with the text: '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' and a 'Create group' button. At the bottom is a section for 'Set permissions boundary - optional'. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons.

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

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](#)

Create group

Set permissions boundary - optional

Cancel Previous Next

Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science

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

Services Search [Alt+S]

Global ShreyaSane

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

IAM > Users > Create user

Step 1
[Specify user details](#)

Step 2
[Set permissions](#)

Step 3
Review and create

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 Shreya_Sane	Console password type None	Require password reset No
--------------------------	-------------------------------	------------------------------

Permissions summary

< 1 >

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.

Cancel Previous **Create user**

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

Services Search [Alt+S]

Global ShreyaSane

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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
- Analyzer settings
- Credential report
- Organization activity
- Service control policies

Related consoles

- [IAM Identity Center](#)
- [AWS Organizations](#)

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](#)

IAM > Users

Users (1) Info

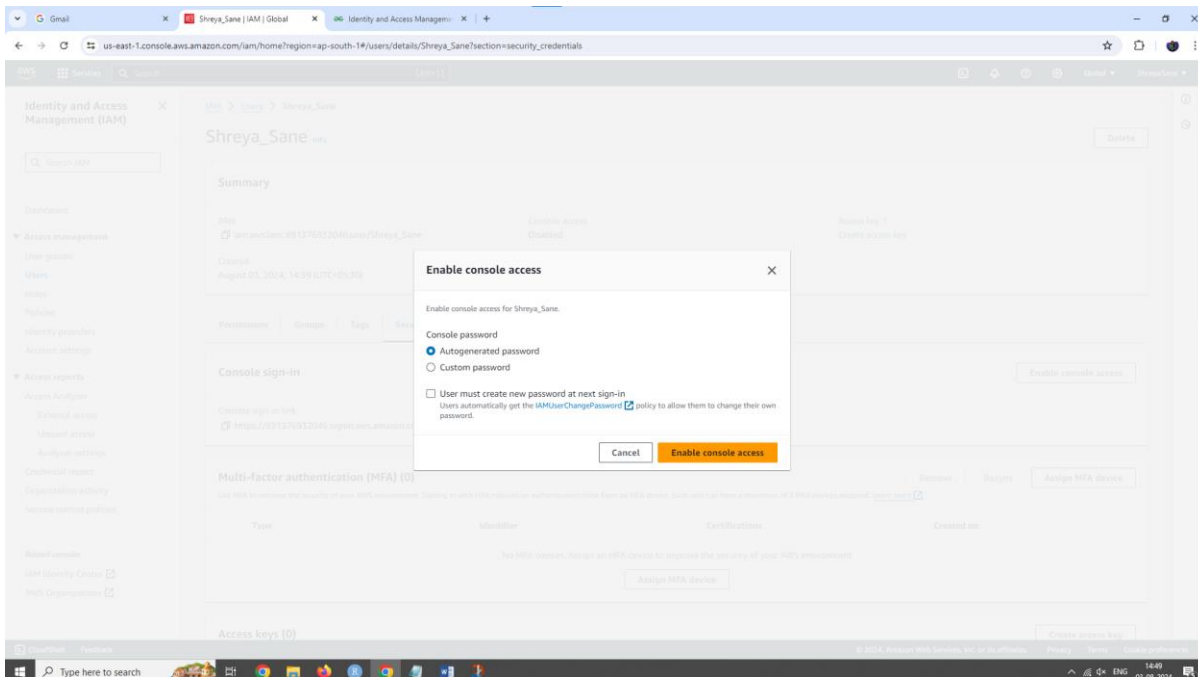
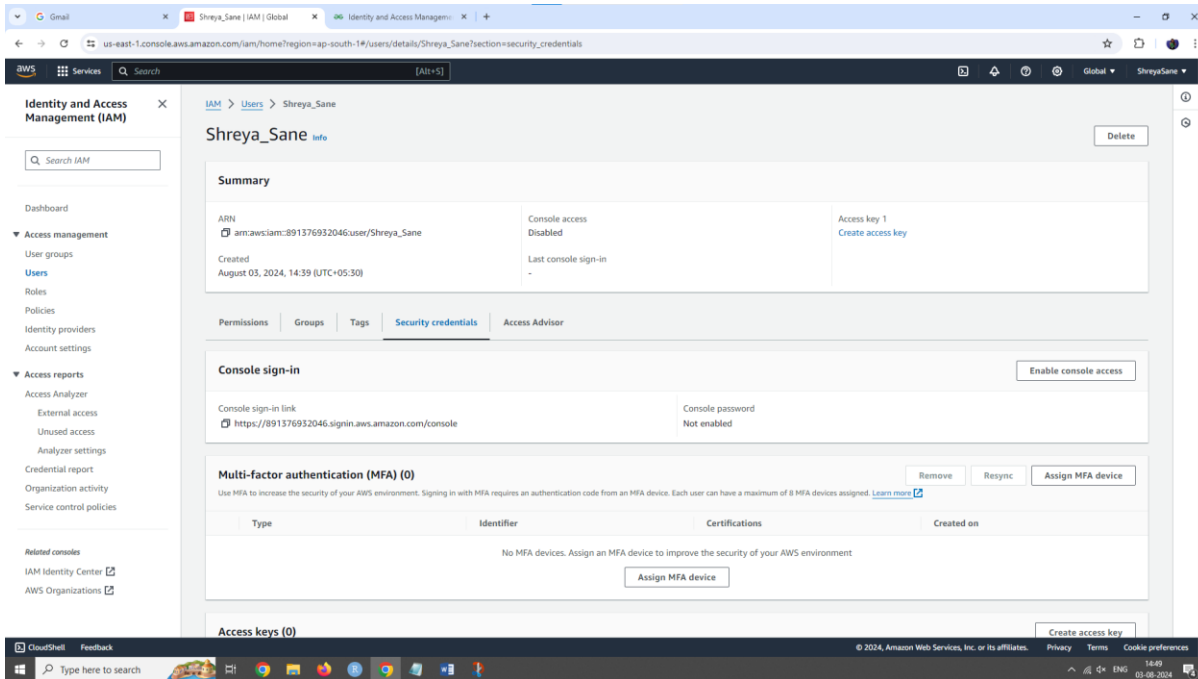
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

[Refresh](#) [Delete](#) [Create user](#)

Search

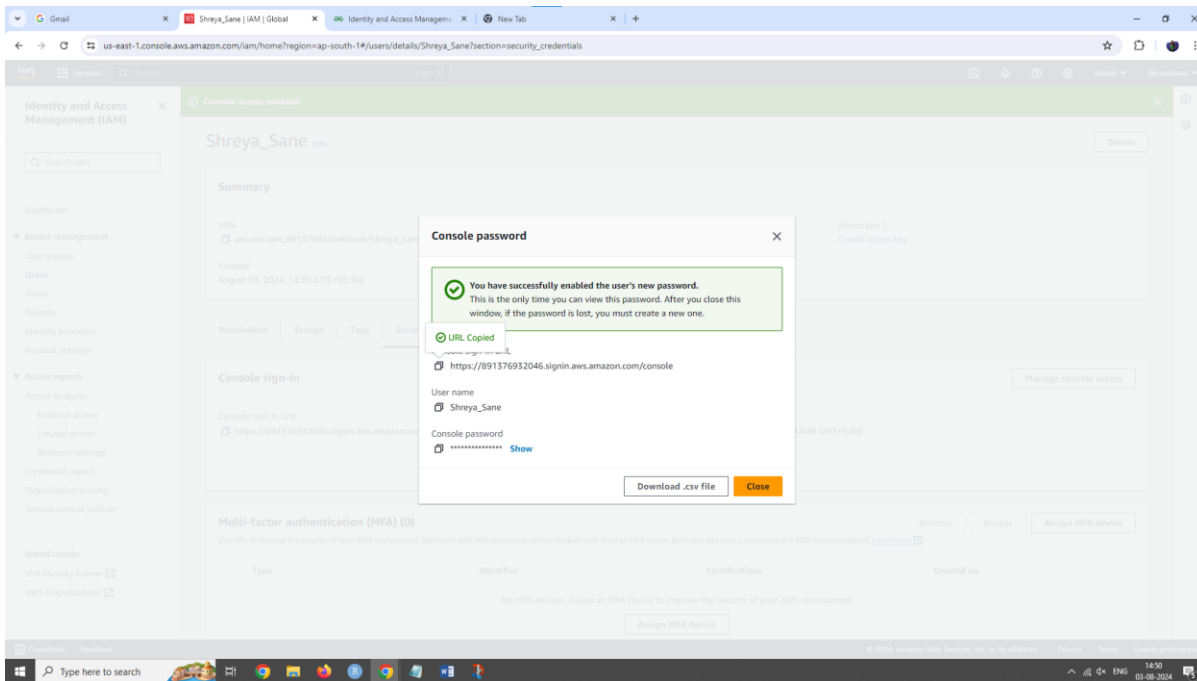
<input type="checkbox"/>	User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age
<input type="checkbox"/>	Shreya_Sane	/	0	-	-	-	-	-	-

Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science

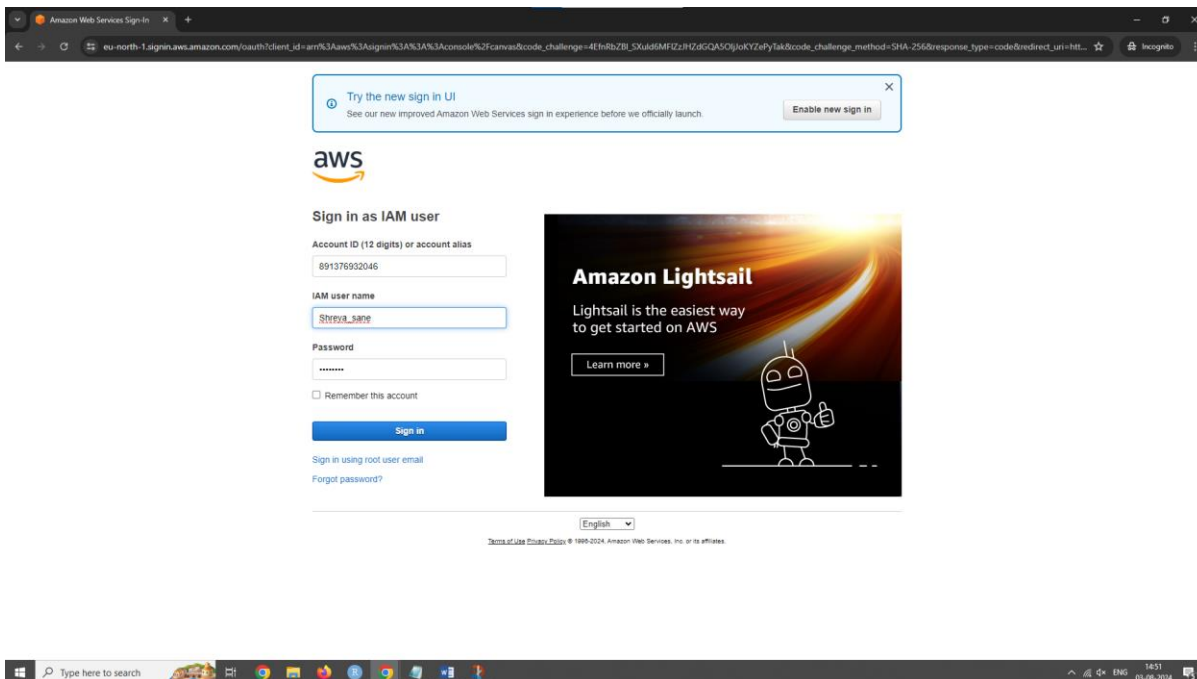


4: this is what will appear after enabling the console access. The ARN link is the link from which other i.e IAM user can access the account .

Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science

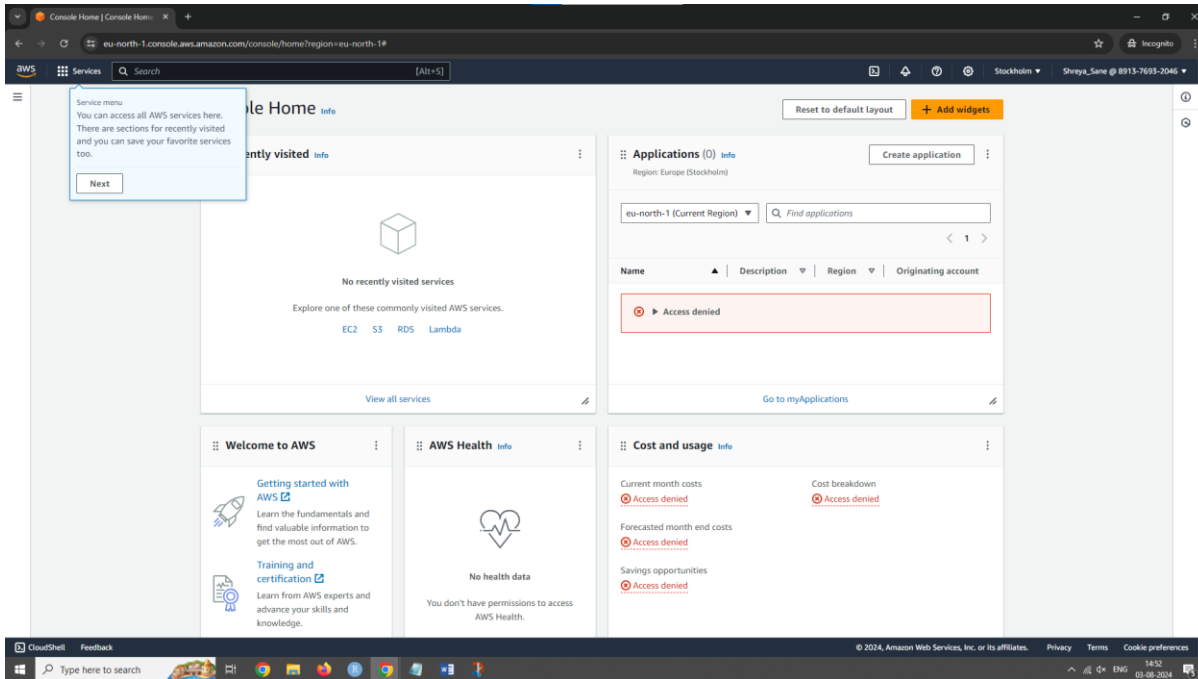


5: Copying the ARN and logging with I AM user



6: Unless and until the access to delete or update or create the buckets, EC2 is granted the IAM user can't perform those tasks the access is denied.

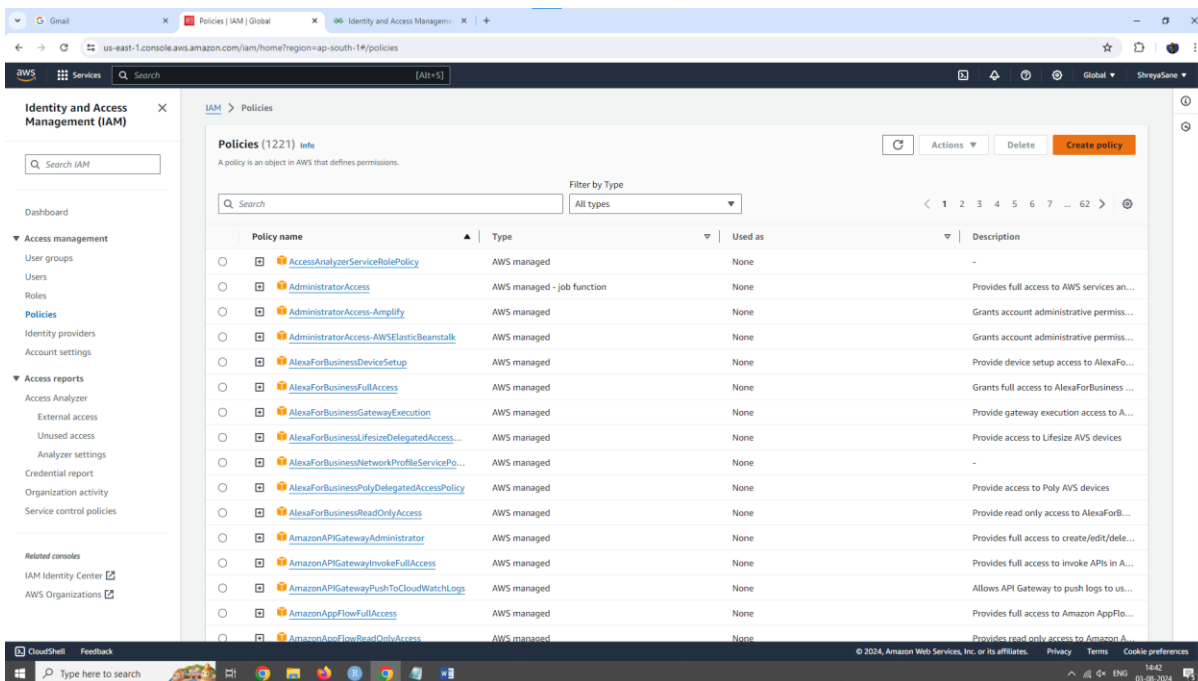
Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science



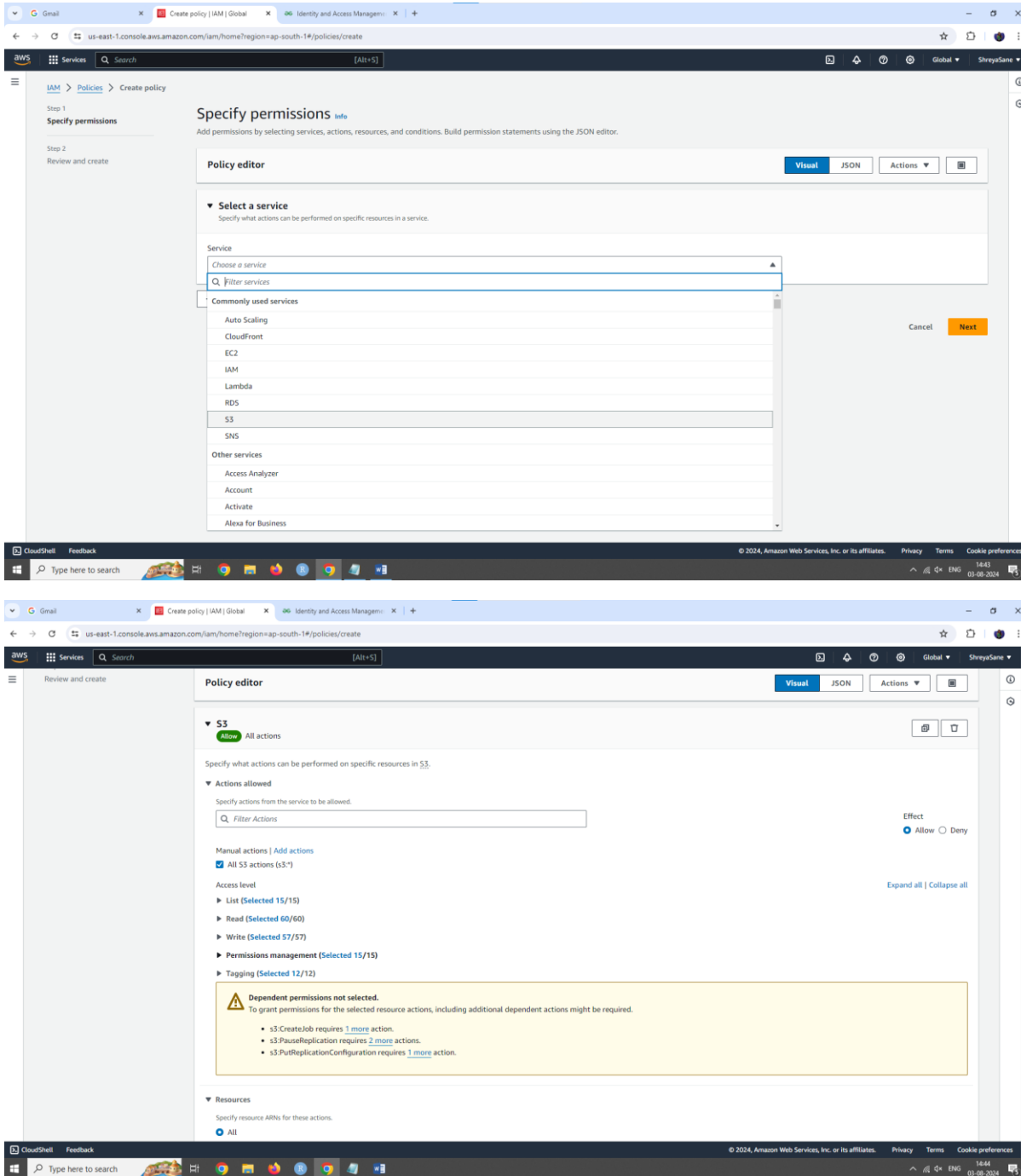
7: To enable those access we need to create a policy for the same .

Left side of the window comprises of the option policy then create policy .

Once the policy is created attach it to the user name.



8: Granting permission .change the sid to the user name .



9: Now, the IAM user can successfully create a S3 bucket .

Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science

The screenshot shows the 'Review and create' step in the AWS IAM console. The left sidebar indicates 'Step 1: Specify permissions' and 'Step 2: Review and create'. The main content area is titled 'Review and create' and includes a 'Policy details' section with fields for 'Policy name' (empty) and 'Description - optional' (empty). Below this is the 'Permissions defined in this policy' section, which shows a table with one entry: 'S3' with 'Full access' and 'All resources'. The 'Add tags - optional' section is also visible, showing no tags are currently associated with the resource.

Review and create [Info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

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](#) [Edit](#)

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 420 services) [Show remaining 419 services](#)

Service	Access level	Resource	Request condition
S3	Full access	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 new tag](#)

This screenshot shows the same 'Review and create' step, but with the 'Policy name' field filled with 'admin_shreya' and the 'Description - optional' field filled with 'policies for shreya'. The 'Permissions defined in this policy' section remains the same, showing 'S3' with 'Full access' and 'All resources'. The 'Add tags - optional' section is still empty, with an 'Add new tag' button visible.

Review and create [Info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

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](#) [Edit](#)

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 420 services) [Show remaining 419 services](#)

Service	Access level	Resource	Request condition
S3	Full access	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 new tag](#)

Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science

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

Policy admin_shreya created.

View policy

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
- Analyzer settings
- Credential report
- Organization activity
- Service control policies

Related consoles

- IAM Identity Center
- AWS Organizations

Policies (1222)

A policy is an object in AWS that defines permissions.

Filter by Type

Search

Policy name	Type	Used as	Description
<input type="radio"/> AccessAnalyzerServiceRolePolicy	AWS managed	None	-
<input type="radio"/> admin_shreya	Customer managed	None	policies for shreya
<input type="radio"/> AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
<input type="radio"/> AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permis...
<input type="radio"/> AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permis...
<input type="radio"/> AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
<input type="radio"/> AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
<input type="radio"/> AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to A...
<input type="radio"/> AlexaForBusinessLifesizeDelegatedAccess...	AWS managed	None	Provide access to Lifesize AVS devices
<input type="radio"/> AlexaForBusinessNetworkProfileServicePo...	AWS managed	None	-
<input type="radio"/> AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
<input type="radio"/> AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForB...
<input type="radio"/> AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/dele...
<input type="radio"/> AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in A...

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Shreya_Sane?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
- Analyzer settings
- Credential report
- Organization activity
- Service control policies

Related consoles

- IAM Identity Center
- AWS Organizations

Shreya_Sane

Summary

ARN
arn:aws:iam::891376932046:user/Shreya_Sane

Console access
Enabled without MFA

Access key 1
Create access key

Created
August 05, 2024, 14:39 (UTC+05:30)

Last console sign-in
Never

Permissions | Groups | Tags | Security credentials | Access Advisor

Permissions policies (0)

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

Filter by Type

Search

Policy name	Type	Attached via
No resources to display		

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can create a permissions boundary for this user. This permissions boundary will attach to the user and any AWS managed CloudTrail event filters that are associated with the user.

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Shreya_Sane?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
- Analyzer settings
- Credential report
- Organization activity
- Service control policies

Related consoles

- IAM Identity Center
- AWS Organizations

Shreya_Sane

Info

Summary

ARN
arn:aws:iam::891376932046:user/Shreya_Sane

Console access
Enabled without MFA

Access key 1
Create access key

Created
August 05, 2024, 14:39 (UTC+05:30)

Last console sign-in
Never

Permissions | Groups | Tags | Security credentials | Access Advisor

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

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

Add permissions

Step 1
Add permissions

Step 2
Review

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.

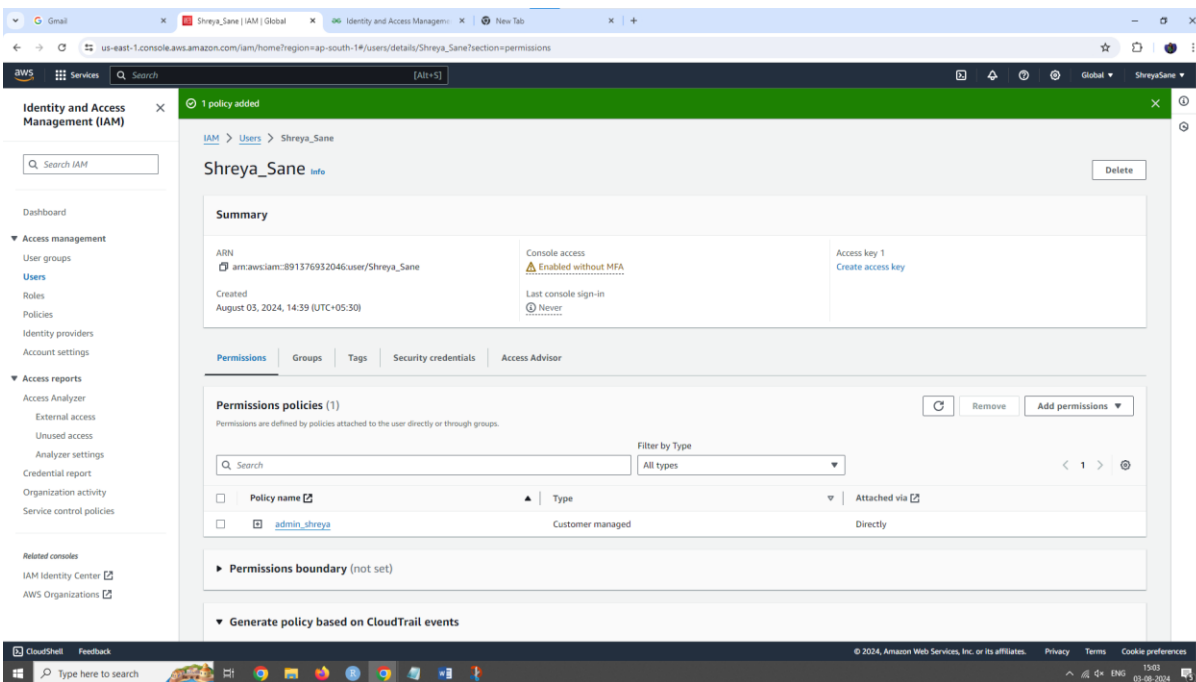
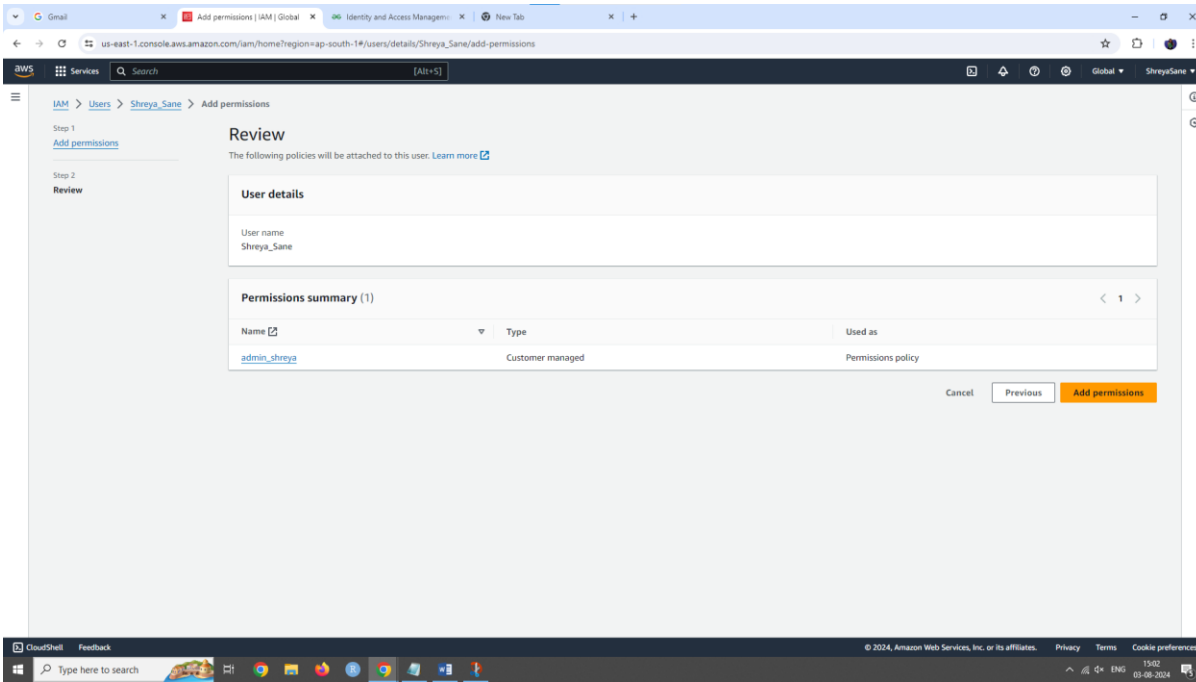
☒ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1224)

Filter by Type
All types

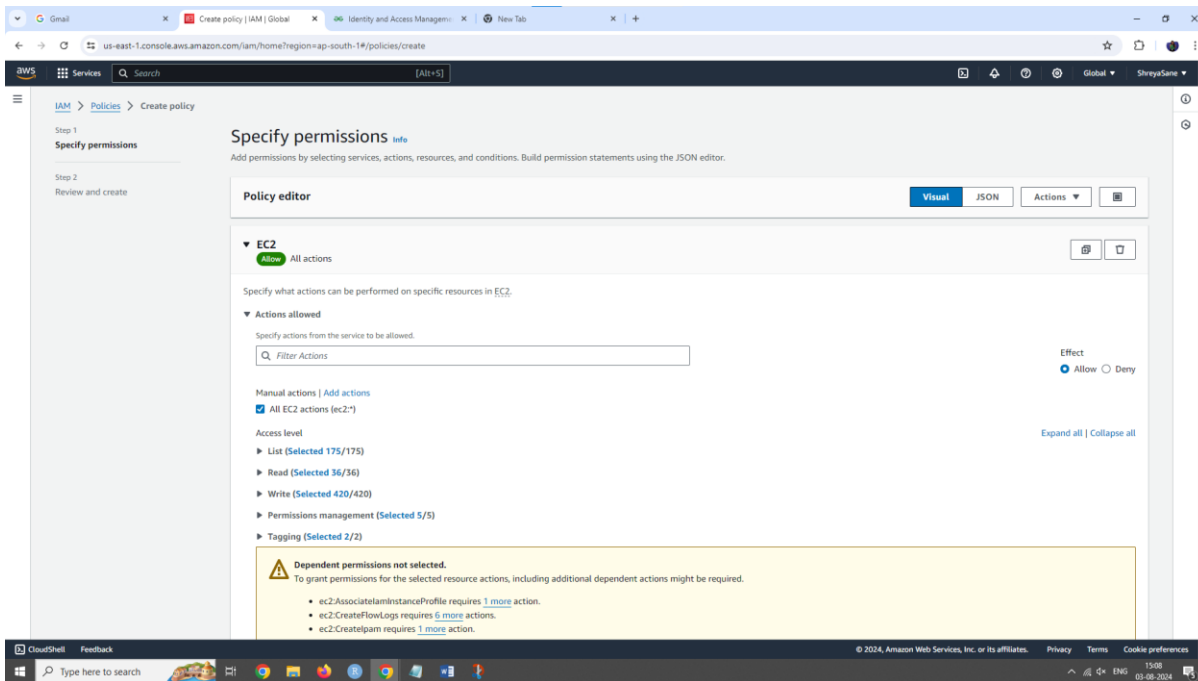
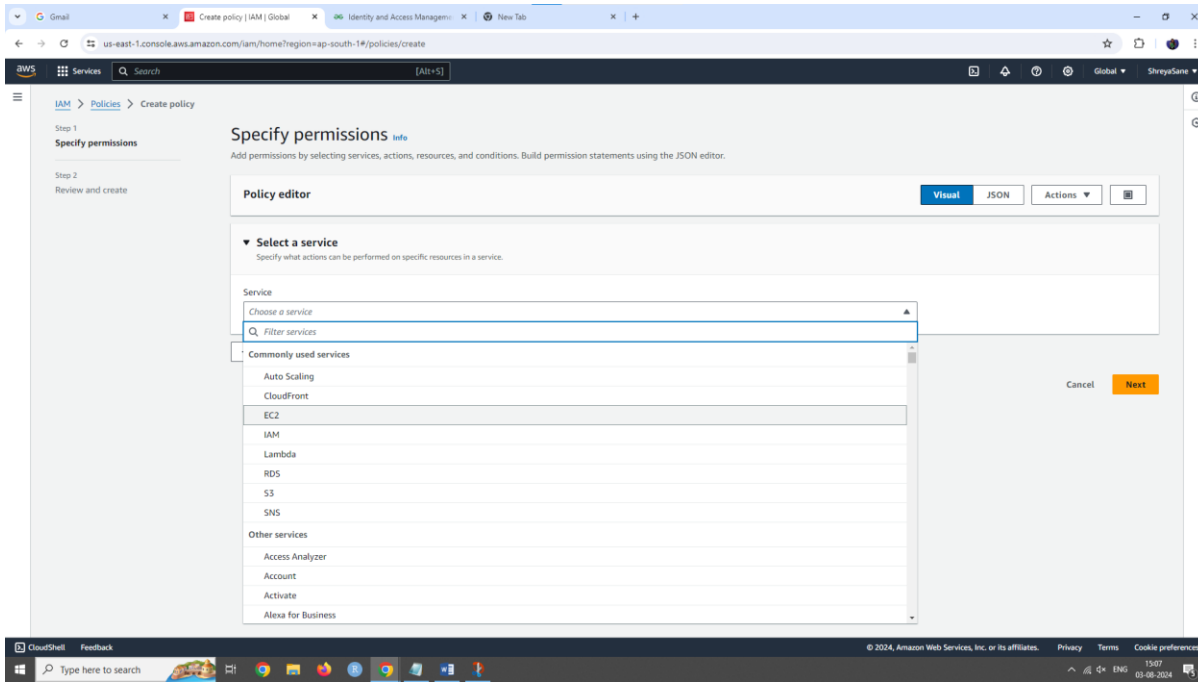
Policy name	Type	Attached entities
<input type="checkbox"/> AccessAnalyzerServiceRolePolicy	AWS managed	0
<input checked="" type="checkbox"/> admin_shreya	Customer managed	0
<input type="checkbox"/> AdministratorAccess	AWS managed - job function	0
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	0
<input type="checkbox"/> AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
<input type="checkbox"/> AlexaForBusinessDeviceSetup	AWS managed	0
<input type="checkbox"/> AlexaForBusinessFullAccess	AWS managed	0
<input type="checkbox"/> AlexaForBusinessGatewayExecution	AWS managed	0
<input type="checkbox"/> AlexaForBusinessIframeDelegatedAccessPolicy	AWS managed	0

Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science

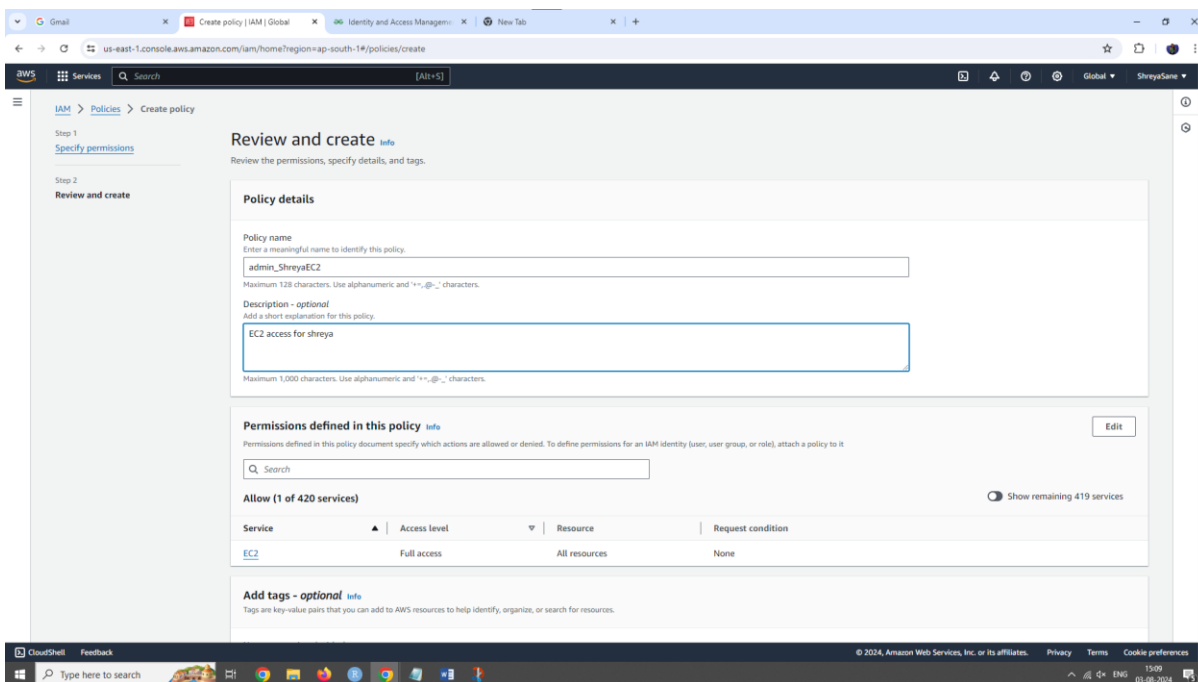
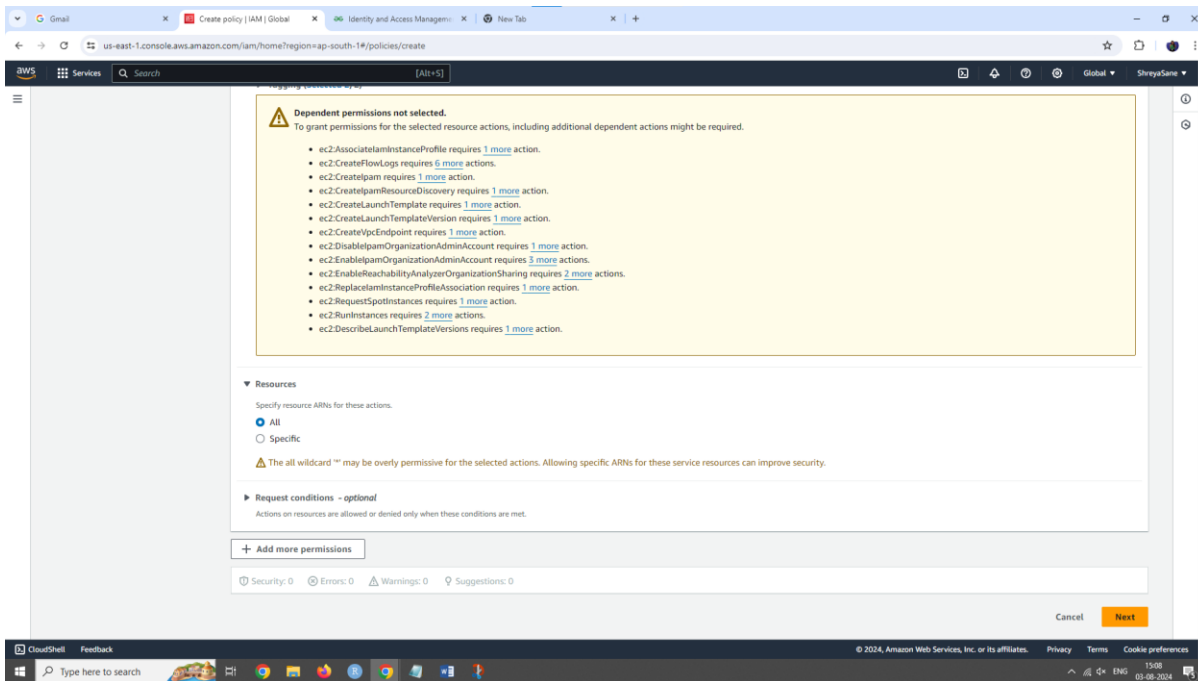


EC2 Permissions

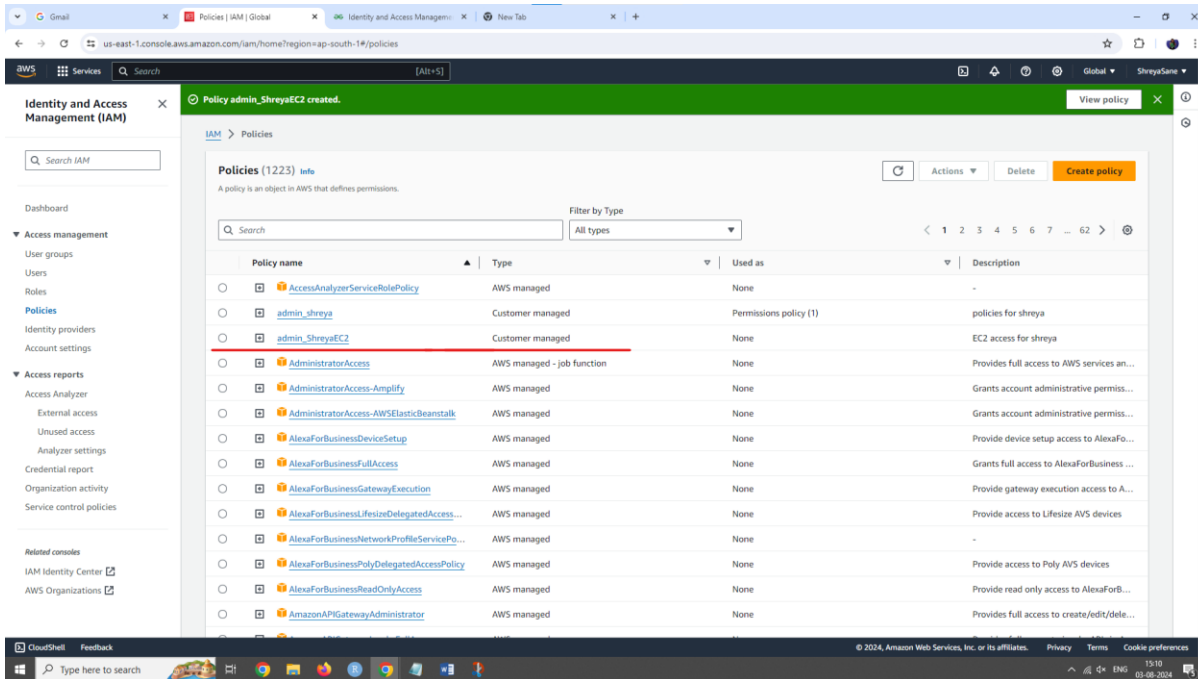
Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science



Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science

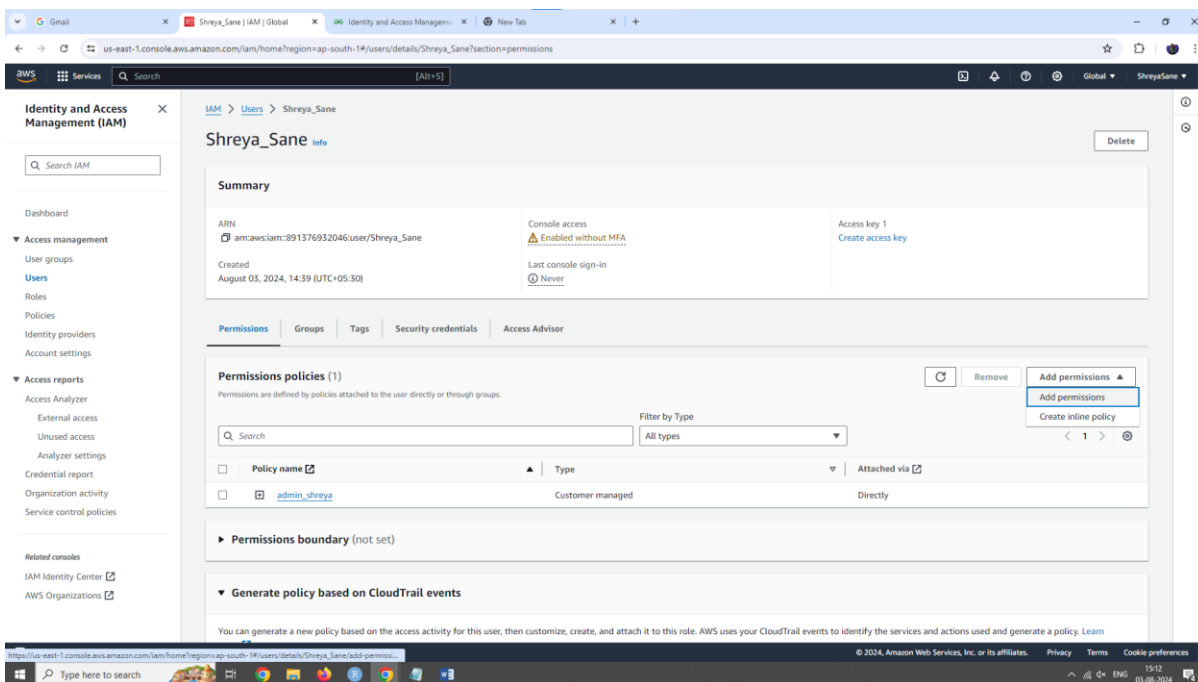


Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science



This screenshot shows the AWS IAM console's 'Policies' page. The left sidebar contains navigation links for Identity and Access Management (IAM), including Dashboard, Access management, User groups, Roles, Policies, Identity providers, and Account settings. The main content area displays a list of 1223 policies. A table lists various policies, including 'admin_shreya' and 'admin_shreyaEC2', which are highlighted with a red border. The table columns are Policy name, Type, Used as, and Description. The 'admin_shreyaEC2' policy is a Customer managed policy used as a Permissions policy (1) for 'shreya', providing EC2 access.

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	-
admin_shreya	Customer managed	Permissions policy (1)	policies for shreya
admin_shreyaEC2	Customer managed	None	EC2 access for shreya
AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permis...
AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permis...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to A...
AlexaForBusinessLifeSizeDelegatedAccess...	AWS managed	None	Provide access to Lifesize AVS devices
AlexaForBusinessNetworkProfileServicePo...	AWS managed	None	-
AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForB...
AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/dele...



This screenshot shows the AWS IAM console's 'Users' page for the user 'Shreya_Sane'. The left sidebar is the same as the previous screenshot. The main content area displays the user's details, including their ARN (arn:aws:iam::891376932046:user/Shreya_Sane), creation date (August 03, 2024, 14:39 UTC+05:30), and console access status (Enabled without MFA). The 'Permissions' tab is selected, showing a list of permissions policies attached to the user. The table lists the 'admin_shreya' policy, which is a Customer managed policy attached directly. Below the table, there are sections for 'Permissions boundary' (not set) and 'Generate policy based on CloudTrail events'.

Policy name	Type	Attached via
admin_shreya	Customer managed	Directly

Name: Shreya Sameer Sane
SAP ID: 86062300009
Roll No: A054
M.Sc. Statistics & Data Science

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

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 (1/1224)

Filter by Type: All types

Policy name	Type	Attached entities
<input type="checkbox"/> AccessAnalyzerServiceRolePolicy	AWS managed	0
<input checked="" type="checkbox"/> admin_ShreyaEC2	Customer managed	0
<input type="checkbox"/> AdministratorAccess	AWS managed - job function	0
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	0
<input type="checkbox"/> AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
<input type="checkbox"/> AlexaForBusinessDeviceSetup	AWS managed	0
<input type="checkbox"/> AlexaForBusinessFullAccess	AWS managed	0
<input type="checkbox"/> AlexaForBusinessGatewayExecution	AWS managed	0
<input type="checkbox"/> AlexaForBusinessIIFSizeDelegatedAccessPolicy	AWS managed	0

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

Review

The following policies will be attached to this user. [Learn more](#)

User details

User name: Shreya_Sane

Permissions summary (1)

Name	Type	Used as
admin_ShreyaEC2	Customer managed	Permissions policy

[Cancel](#) [Previous](#) [Add permissions](#)

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Shreya_Sane

Shreya_Sane

[Delete](#)

Summary

ARN: [arn:aws:iam::891376932046:user/Shreya_Sane](#)

Created: August 03, 2024, 14:39 (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
<input type="checkbox"/> admin_shreya	Customer managed	Directly
<input type="checkbox"/> admin_ShreyaEC2	Customer managed	Directly