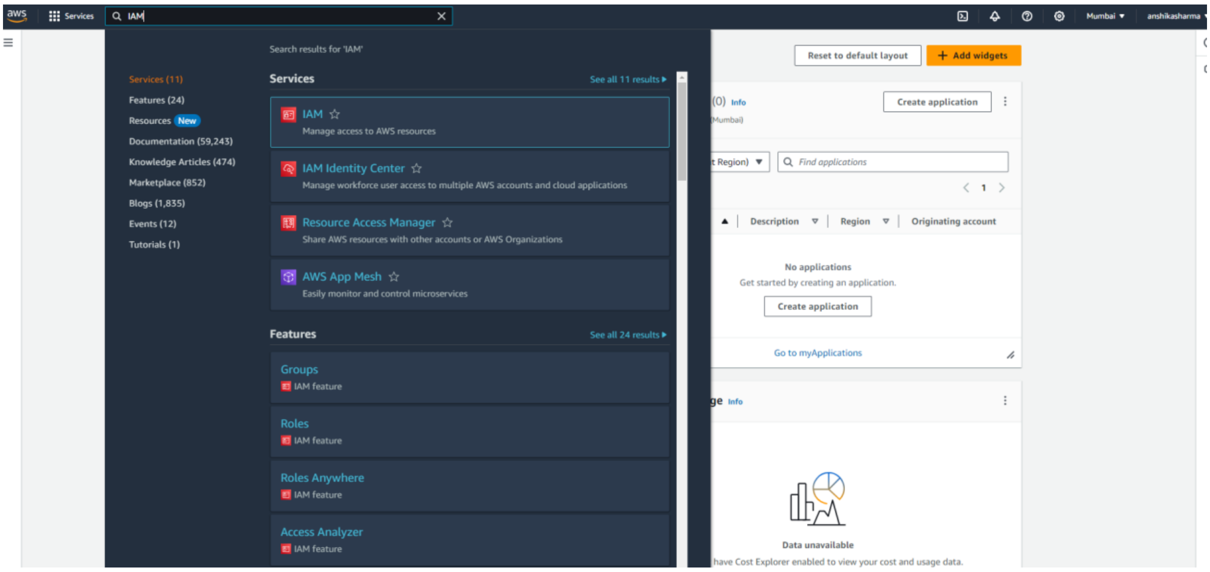
Practical-3 Identity Access Management

Name: Anshika Sharma

SAP ID: 86062300034

Roll No: A061

1.Navigate to the search bar and search for "IAM."



Search results for 'IAM'

- Services (11)
- Features (24)
- Resources New
- Documentation (59,243)
- Knowledge Articles (474)
- Marketplace (852)
- Blogs (1,835)
- Events (12)
- Tutorials (1)

Services — See all 11 results ▸

IAM ☆
Manage access to AWS resources

IAM Identity Center ☆
Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager ☆
Share AWS resources with other accounts or AWS Organizations

AWS App Mesh ☆
Easily monitor and control microservices

Features — See all 24 results ▸

Groups
IAM feature

Roles
IAM feature

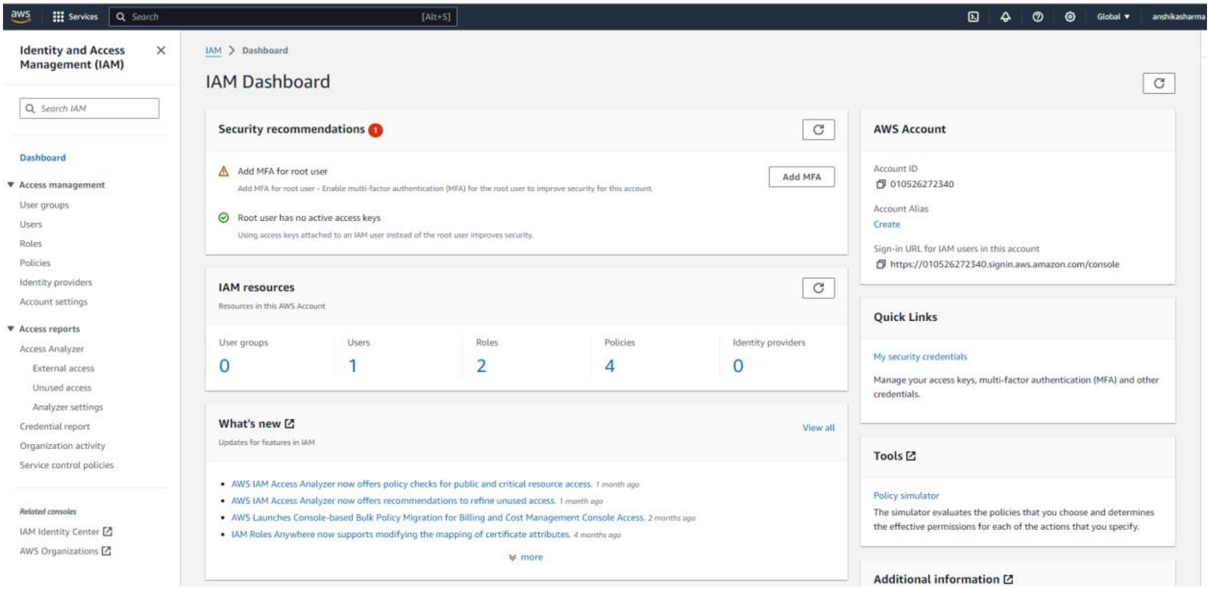
Roles Anywhere
IAM feature

Access Analyzer
IAM feature

No applications
Get started by creating an application.

Data unavailable
have Cost Explorer enabled to view your cost and usage data.

2.The IAM dashboard will appear.



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	1	2	4	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. 2 months ago
- IAM Roles Anywhere now supports modifying the mapping of certificate attributes. 4 months ago

AWS Account

Account ID
010526272340

Account Alias
Create

Sign-in URL for IAM users in this account
https://010526272340.signin.aws.amazon.com/console

Quick Links

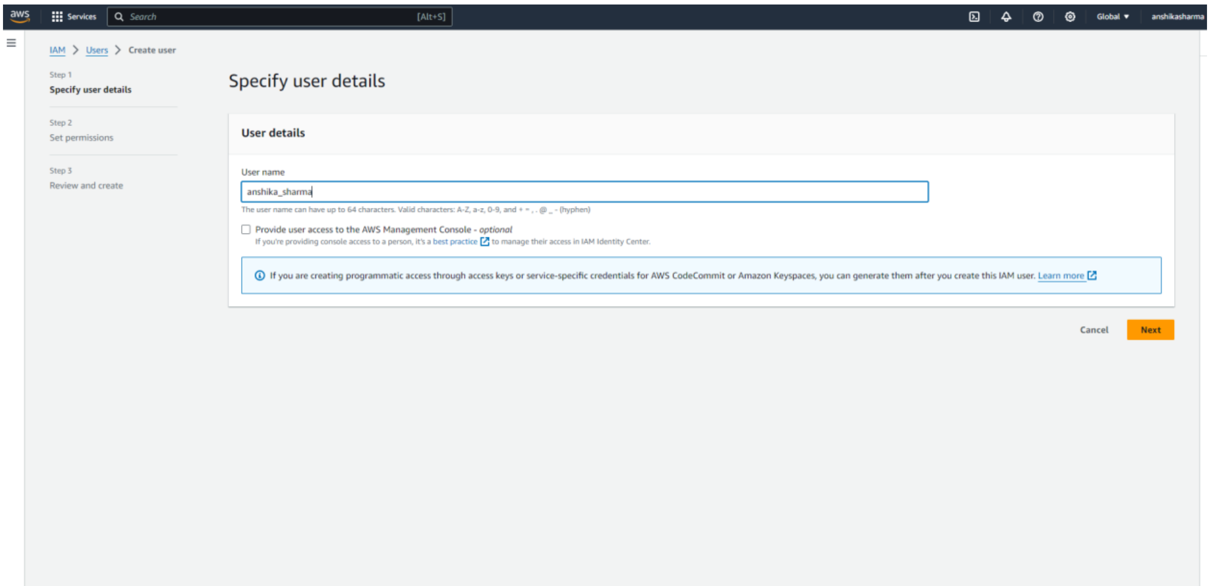
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

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

Additional information

3.Select "Users" from the left pane. Enter the user details and click "Next."



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Specify user details

User details

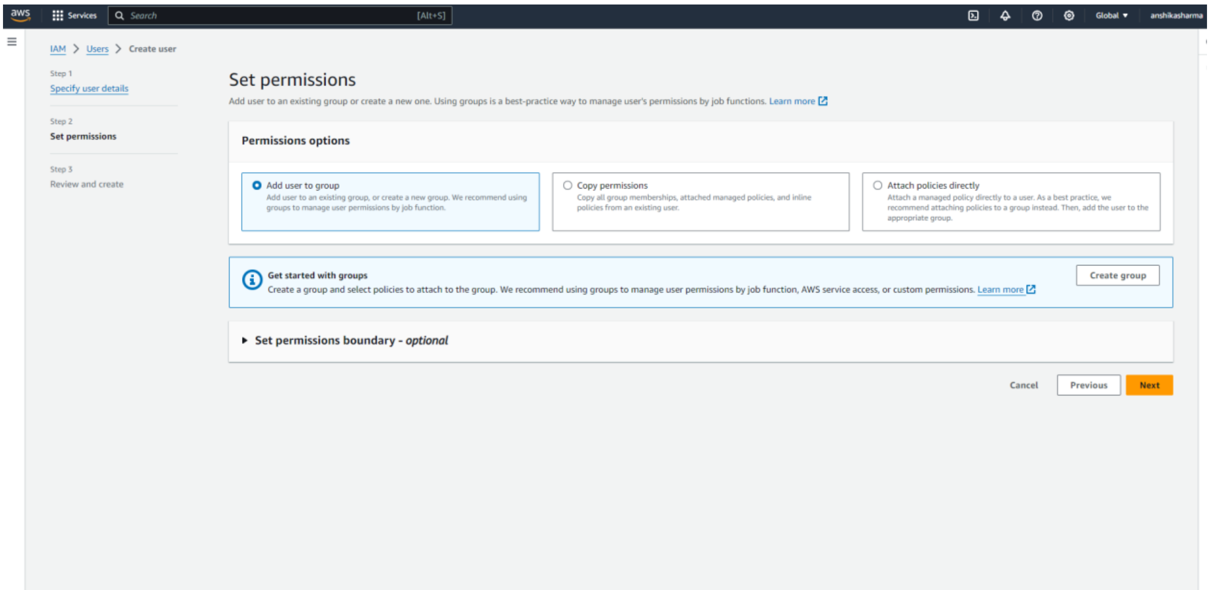
User name
anshika_sharma

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

4.Set permissions by selecting "Add user to group."



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.

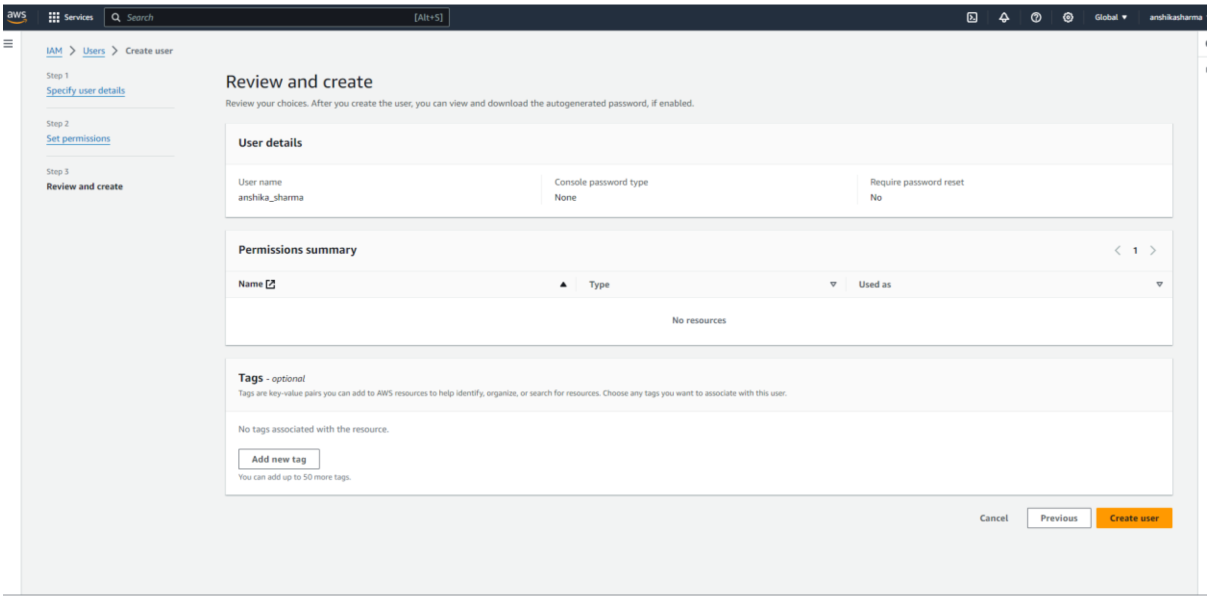
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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.

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

▸ **Set permissions boundary - *optional***

5.Review the details and click "Create user."



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	Console password type	Require password reset
anshika_sharma	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.

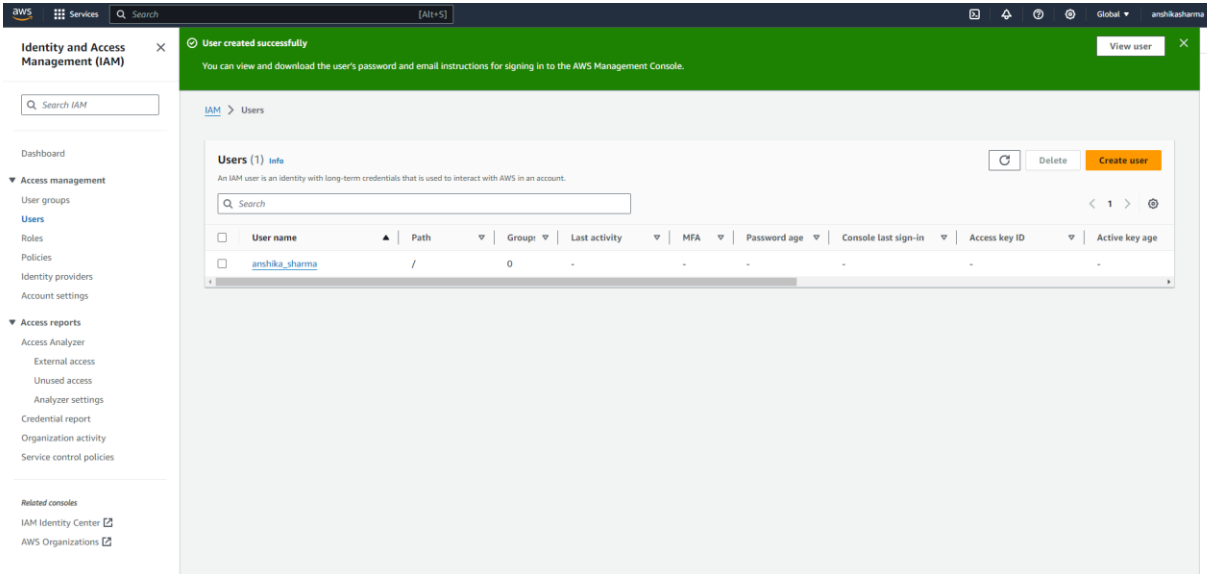
No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous Create user

6.The 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.

View user

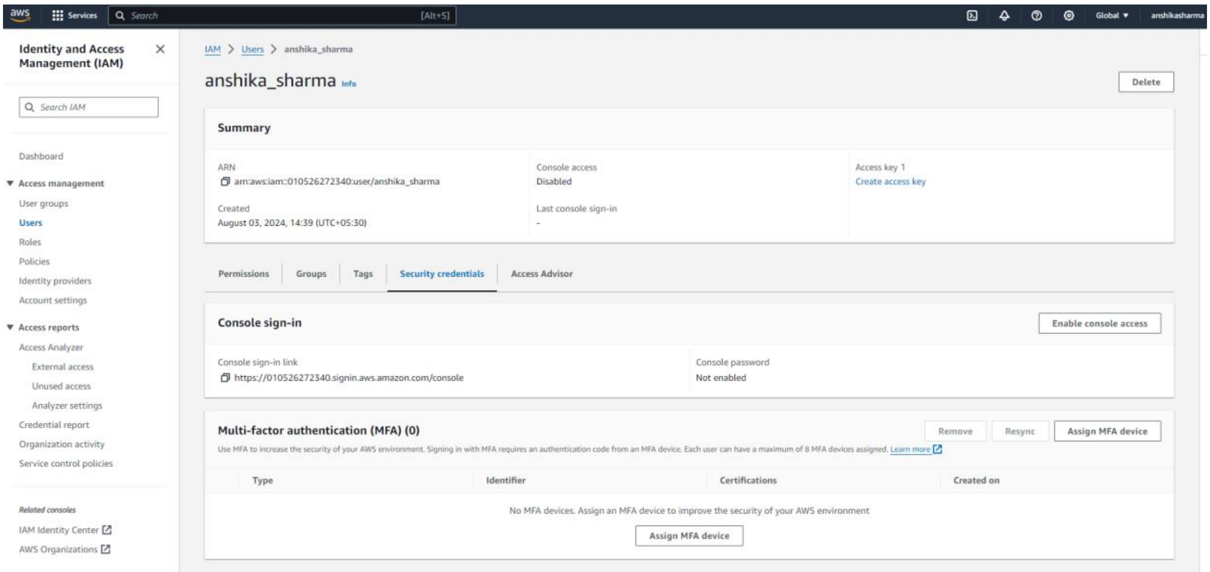
IAM > Users

Users (1) Info

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

☐	User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age
☐	anshika_sharma	/	0	-	-	-	-	-	-

7.Click on the newly created user named "anshika_sharma." Navigate to Security Credentials and click on "Enable Console Access."



anshika_sharma

Summary

ARN: arn:aws:iam::010526272340:user/anshika_sharma

Created: August 03, 2024, 14:39 (UTC+05:30)

Console access: Disabled

Last console sign-in: -

Access key 1: Create access key

Console sign-in

Console sign-in link: https://010526272340.signin.aws.amazon.com/console

Console password: Not enabled

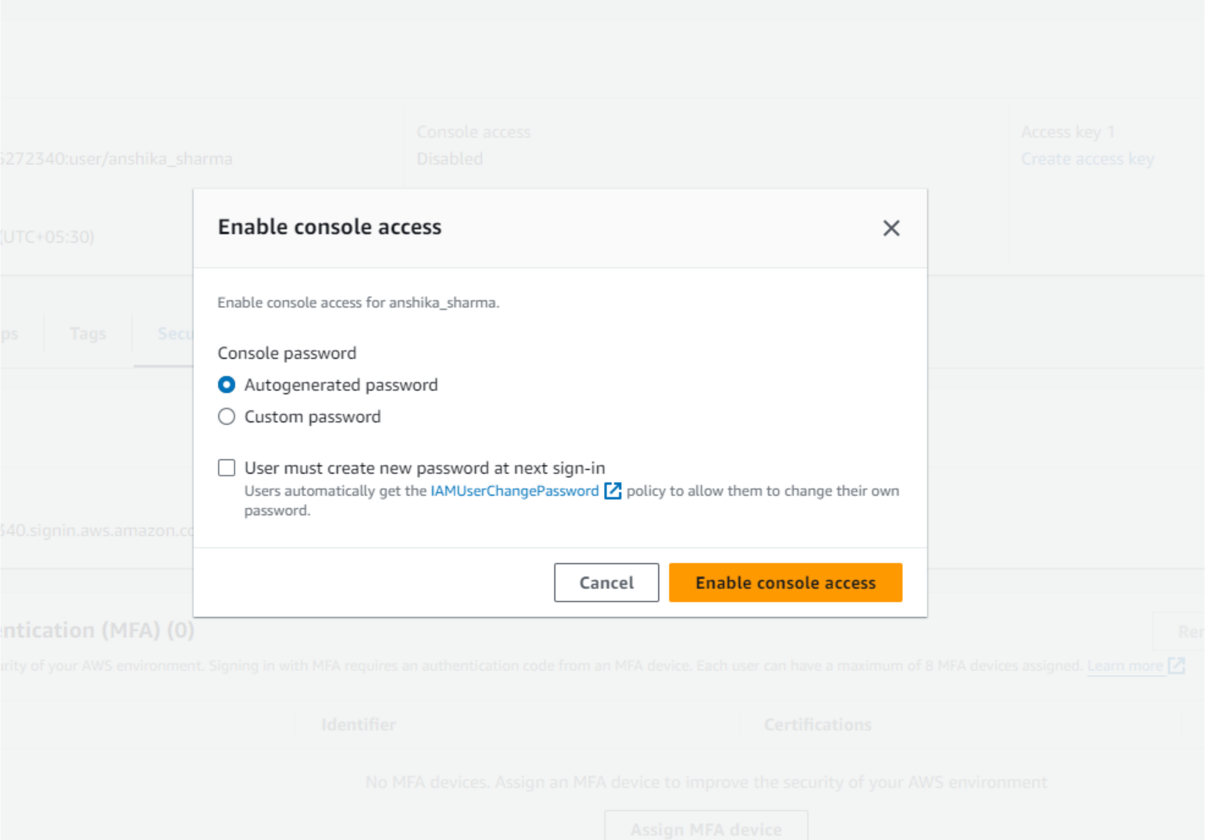
Multi-factor authentication (MFA) (0)

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

8.Customize the password and then click on "Enable Console Access."



Enable console access

Enable console access for anshika_sharma.

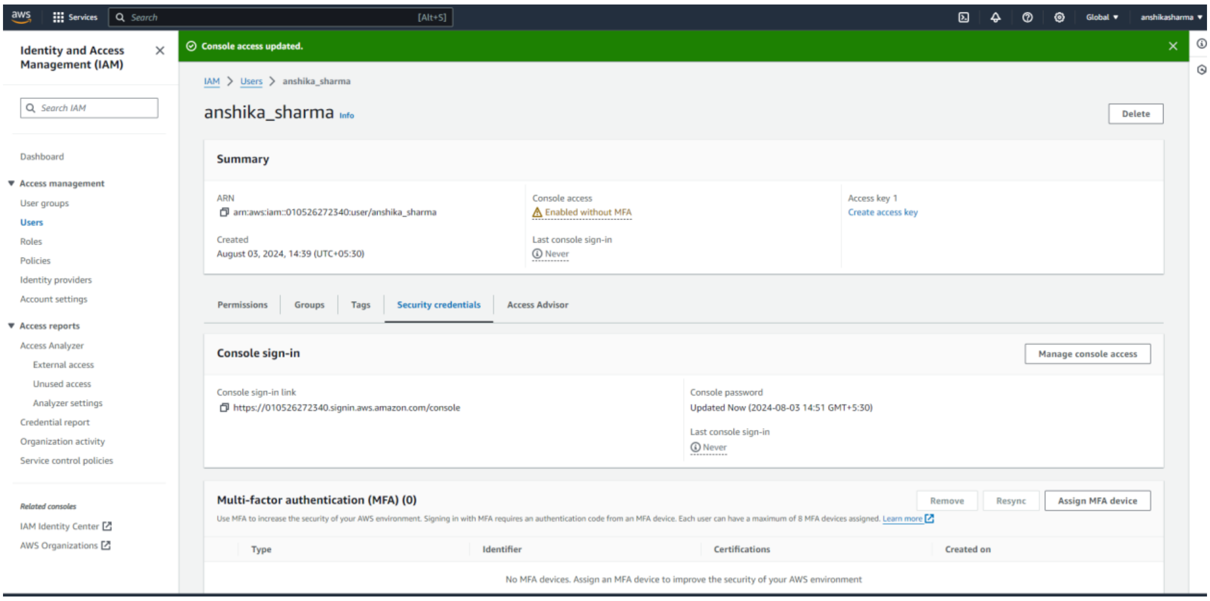
Console password

● 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.



Console access updated.

anshika_sharma

Summary

ARN
arn:aws:iam::010526272340:user/anshika_sharma

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

Console sign-in

Console sign-in link
https://010526272340.signin.aws.amazon.com/console

Console password
Updated Now (2024-08-03 14:51 GMT+5:30)

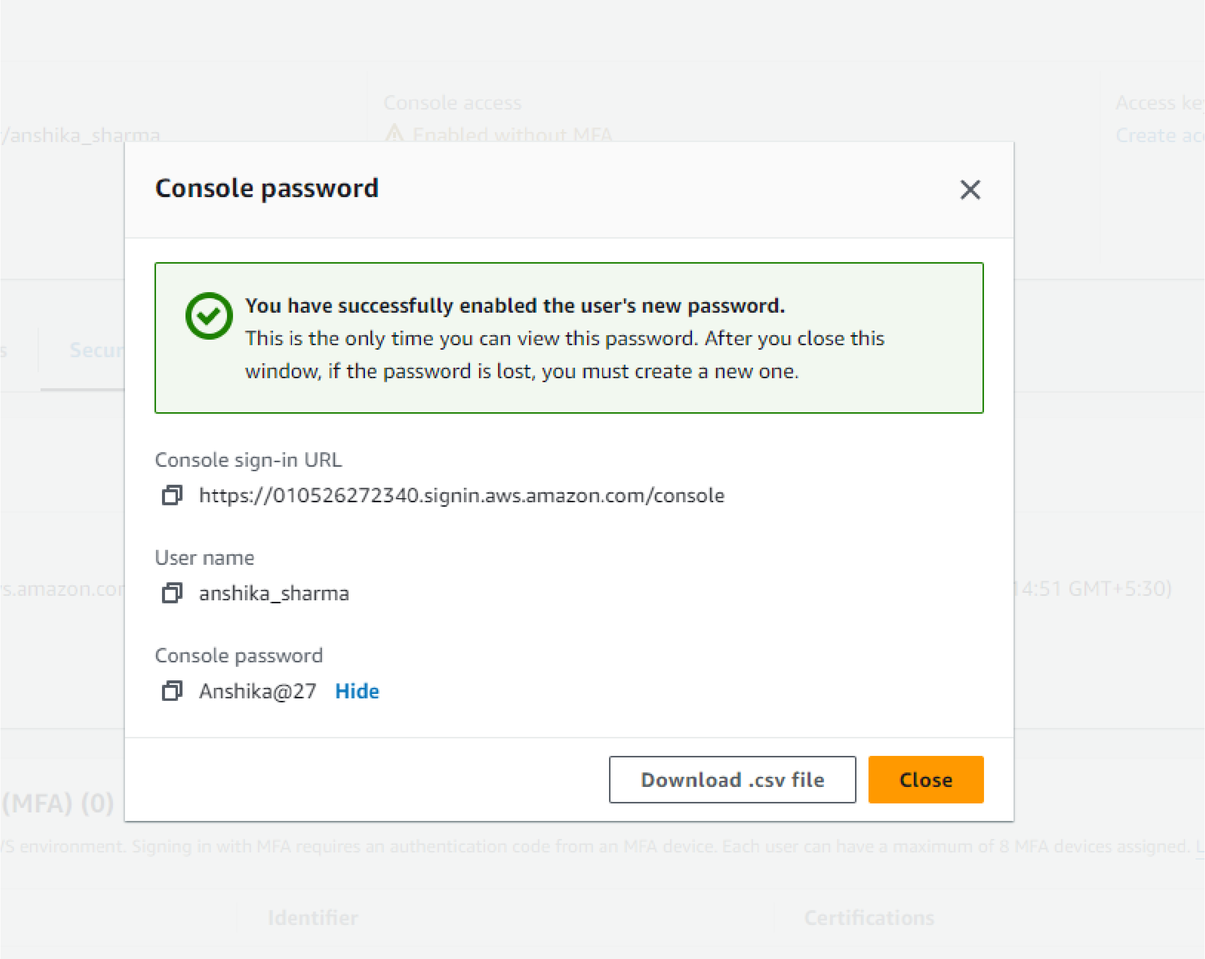
Last console sign-in
Never

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

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

9.Console access has been successfully enabled with the new password.



Console password

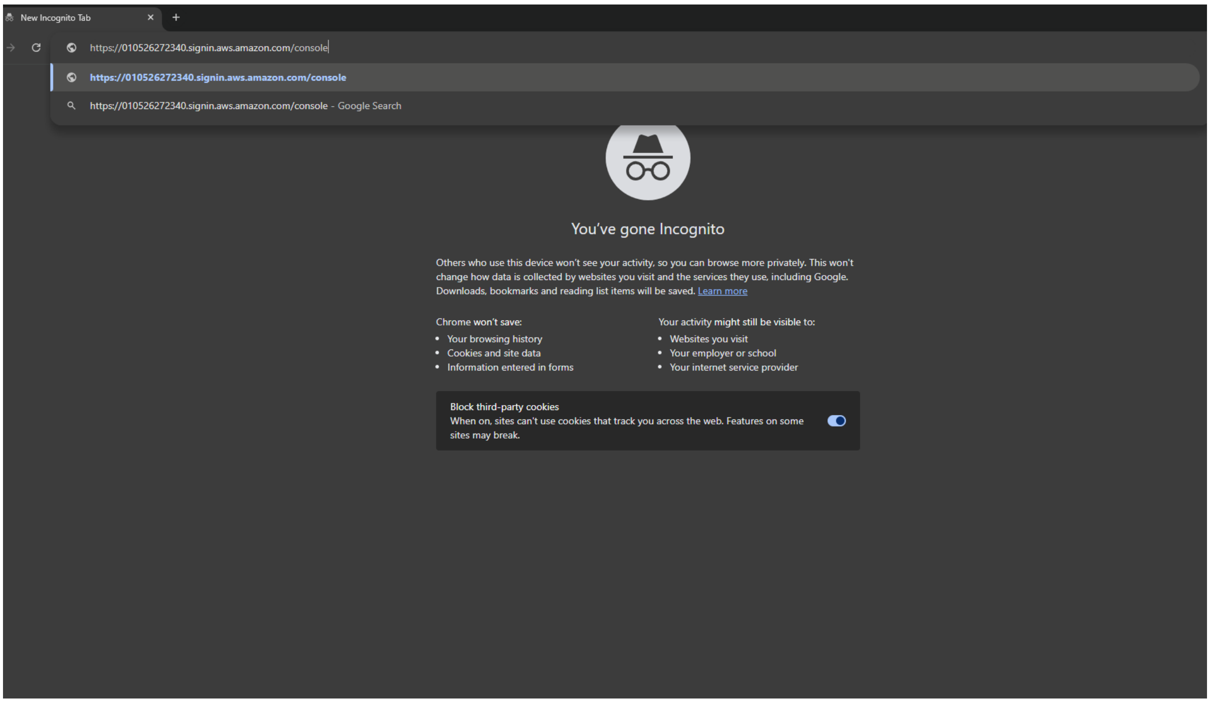
You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

Console sign-in URL
https://010526272340.signin.aws.amazon.com/console

User name
anshika_sharma

Console password
Anshika@27

10.Copy the Console sign-in URL and paste it into an incognito window.


New Incognito Tab
https://010526272340.signin.aws.amazon.com/console
https://010526272340.signin.aws.amazon.com/console
https://010526272340.signin.aws.amazon.com/console - Google Search

You've gone Incognito

Others who use this device won't see your activity, so you can browse more privately. This won't change how data is collected by websites you visit and the services they use, including Google. Downloads, bookmarks and reading list items will be saved. Learn more

Chrome won't save:

- Your browsing history
- Cookies and site data
- Information entered in forms

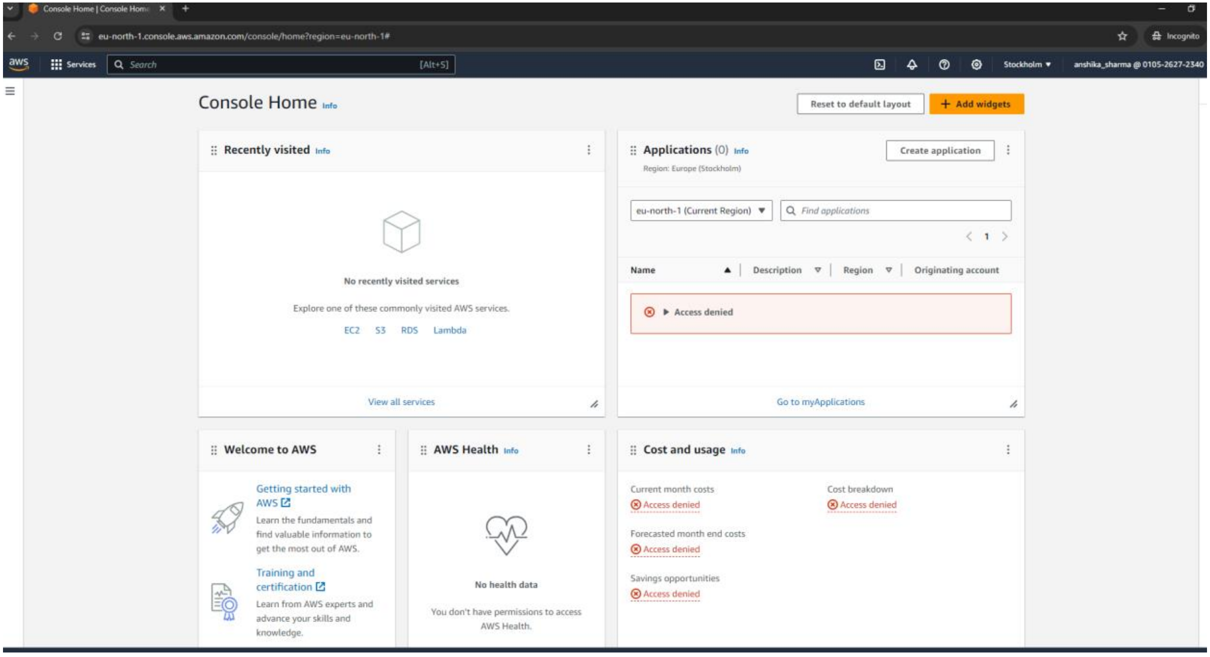
Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies

When on, sites can't use cookies that track you across the web. Features on some sites may break.

11.Using the customised login id and password you login to console home. The Console Home will appear, but you'll see that access is denied for the current user.



No recently visited services

Explore one of these commonly visited AWS services.

Access denied

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 knowledge.

No health data

You don't have permissions to access AWS Health.

Current month costs: Access denied

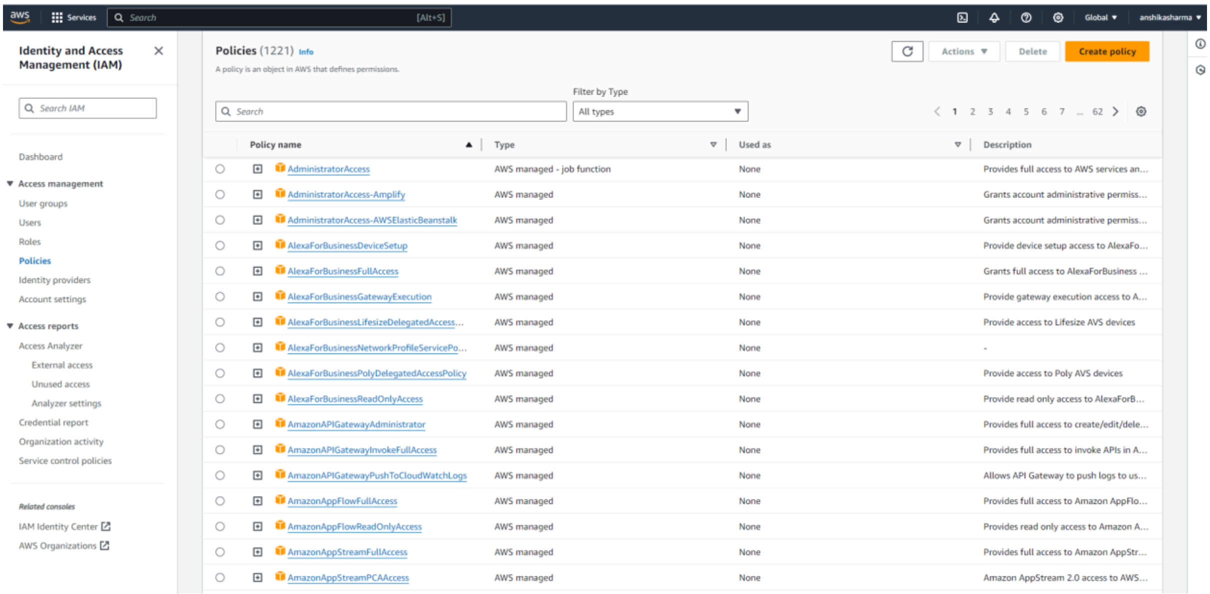
Cost breakdown: Access denied

Forecasted month end costs: Access denied

Savings opportunities: Access denied

12.To grant access to the newly created user, create policies:

- Go to your account.
- From the left pane, select "Policies."
- Click on "Create Policies."



Policies (1221)

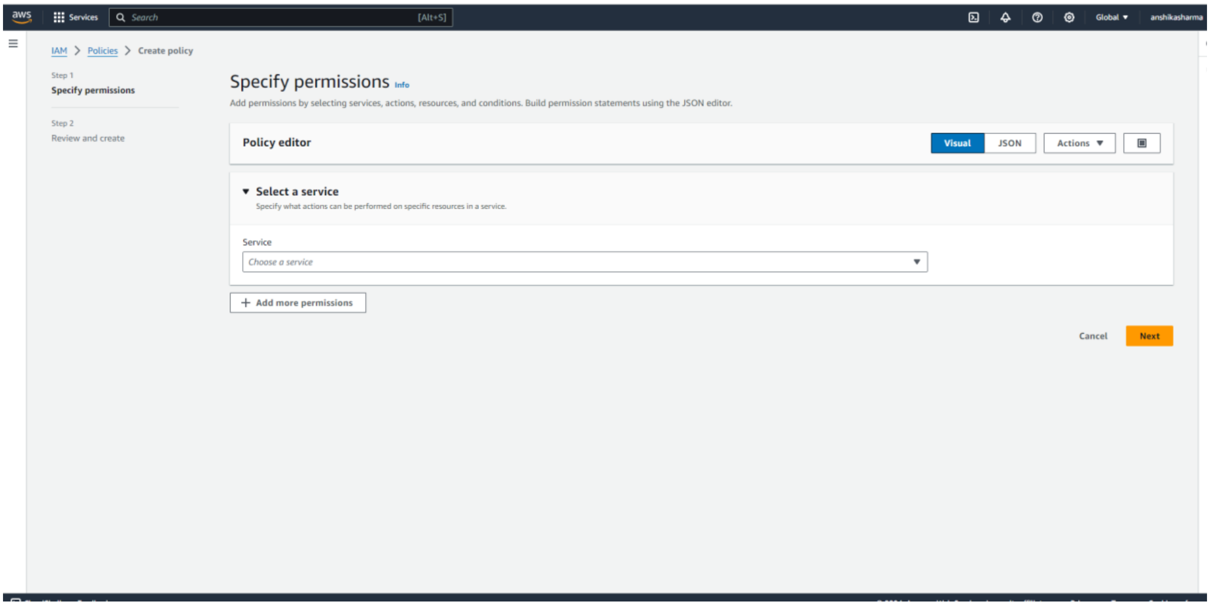
A policy is an object in AWS that defines permissions.

Filter by Type: All types

‹ 1 2 3 4 5 6 7 ... 62 ›

Policy name	Type	Used as	Description
AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permiss...
AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permiss...
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...
AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in A...
AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None	Allows API Gateway to push logs to us...
AmazonAppFlowFullAccess	AWS managed	None	Provides full access to Amazon AppFlo...
AmazonAppFlowReadOnlyAccess	AWS managed	None	Provides read only access to Amazon A...
AmazonAppStreamFullAccess	AWS managed	None	Provides full access to Amazon AppStr...
AmazonAppStreamPCAAccess	AWS managed	None	Amazon AppStream 2.0 access to AWS...

13.Specify permissions for the user.



Specify permissions

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

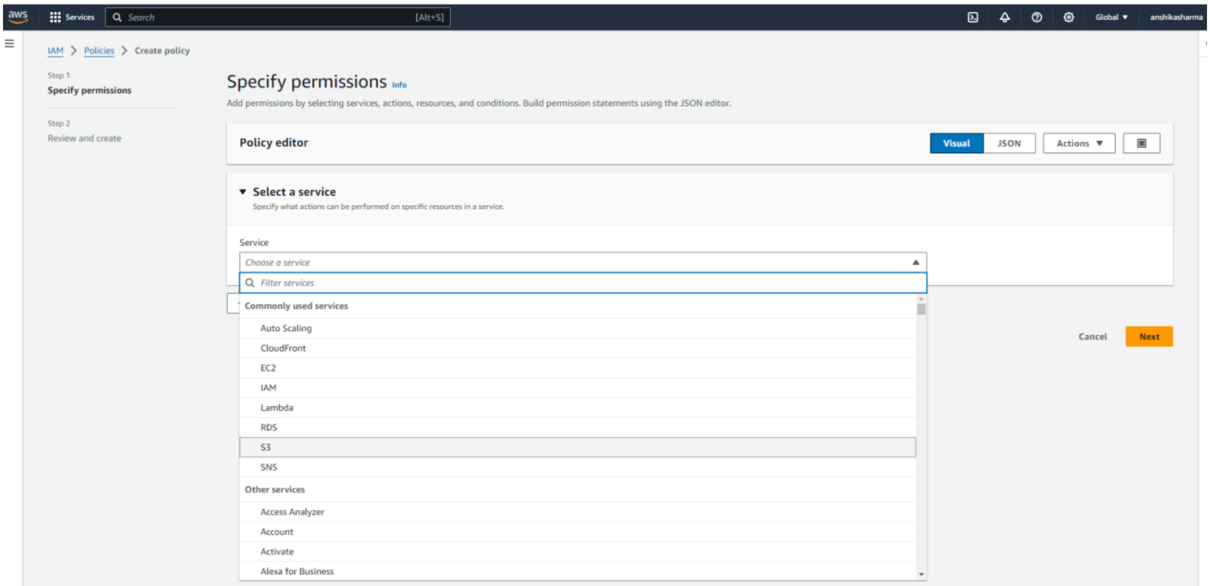
Policy editor

▼ Select a service

Specify what actions can be performed on specific resources in a service.

Service: Choose a service

14.Under the Service option, select S3 to grant access for bucket creation.



Specify permissions

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

Policy editor

▼ Select a service

Specify what actions can be performed on specific resources in a service.

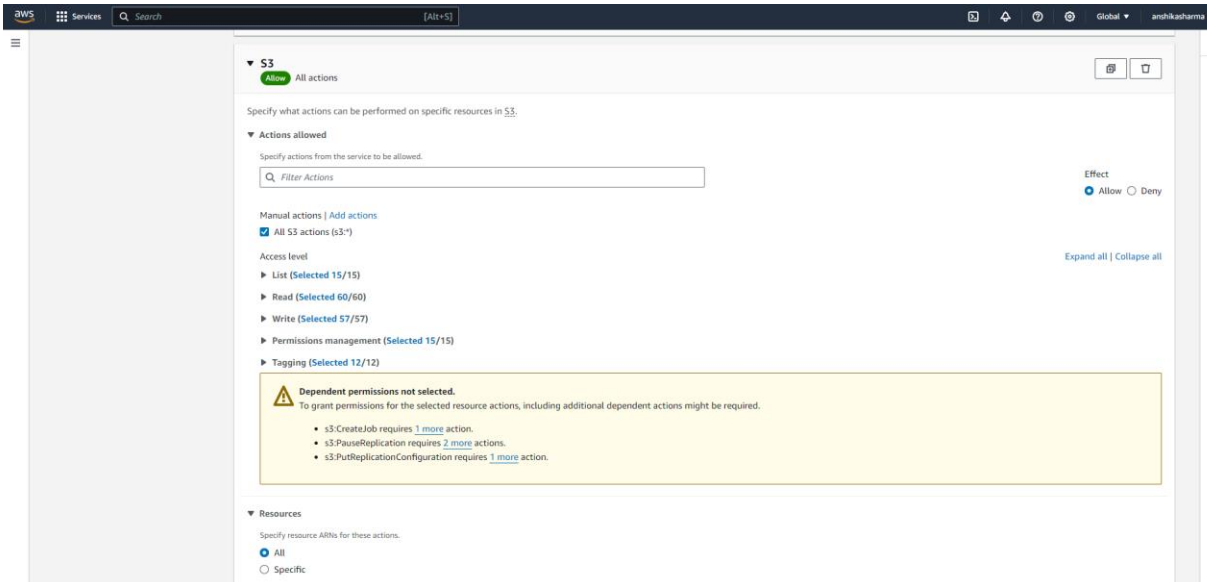
Service: Choose a service

Filter services

Commonly used services
- Auto Scaling
- CloudFront
- EC2
- IAM
- Lambda
- RDS
- S3
- SNS

Other services
- Access Analyzer
- Account
- Activate
- Alexa for Business

15.Next, select "All S3 actions" and “All” under the Resources section.



▼ S3

Allow All actions

Specify what actions can be performed on specific resources in S3.

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect

● Allow ○ Deny

Manual actions | Add actions

☑ All S3 actions (s3:*)

Access level

Expand all | Collapse all

- List (Selected 15/15)
- Read (Selected 60/60)
- Write (Selected 57/57)
- Permissions management (Selected 15/15)
- Tagging (Selected 12/12)

Dependent permissions not selected.
To grant permissions for the selected resource actions, including additional dependent actions might be required.

- s3:CreateJob requires 1 more action.
- s3:PauseReplication requires 2 more actions.
- s3:PutReplicationConfiguration requires 1 more action.

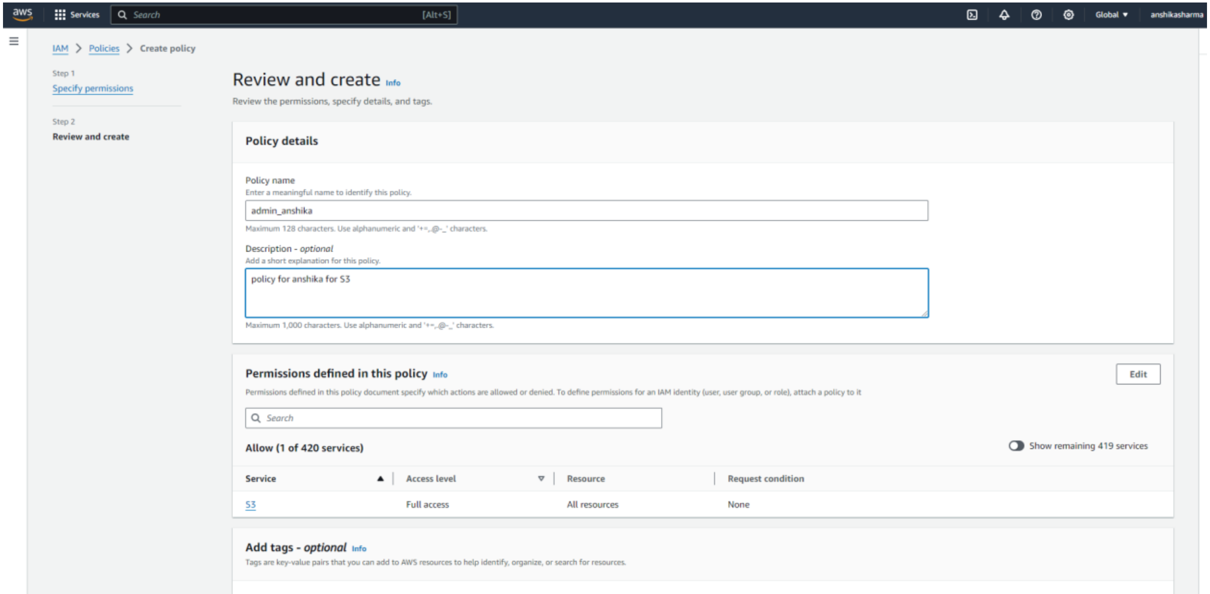
▼ Resources

Specify resource ARNs for these actions.

● All

○ Specific

16.Proceed to the Review and Create pane, where you'll need to specify the policy name and provide a short description for the policy.



IAM > Policies > Create policy

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.
admin_anshika
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.
policy for anshika for S3
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

Search

Allow (1 of 420 services)

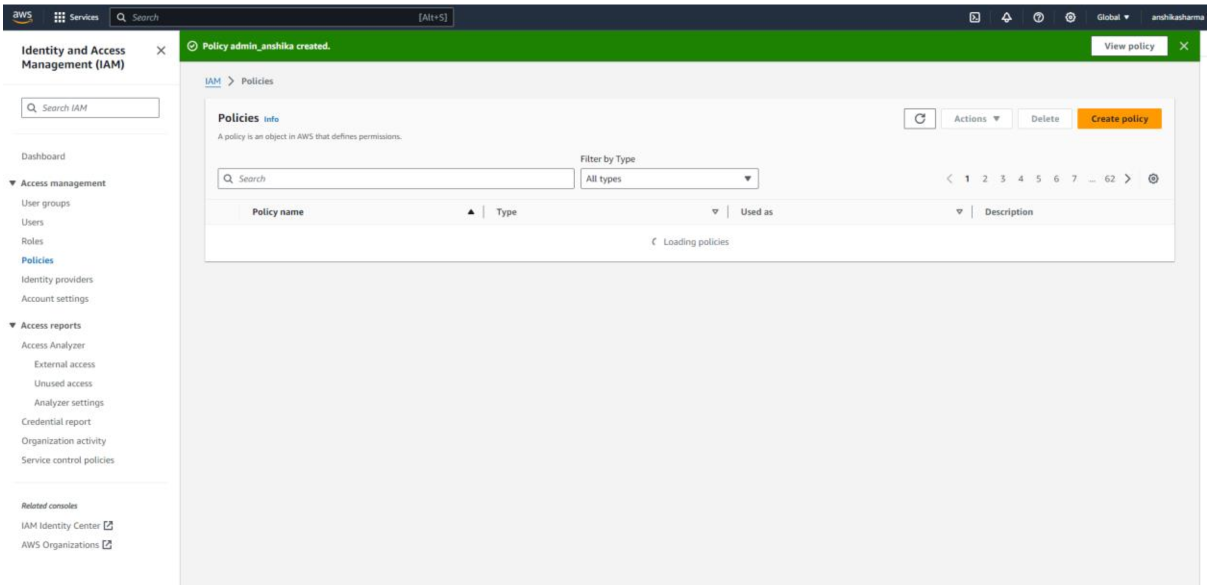
Show remaining 419 services

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.

17.Click on Create Policy, and the policy will be created successfully.



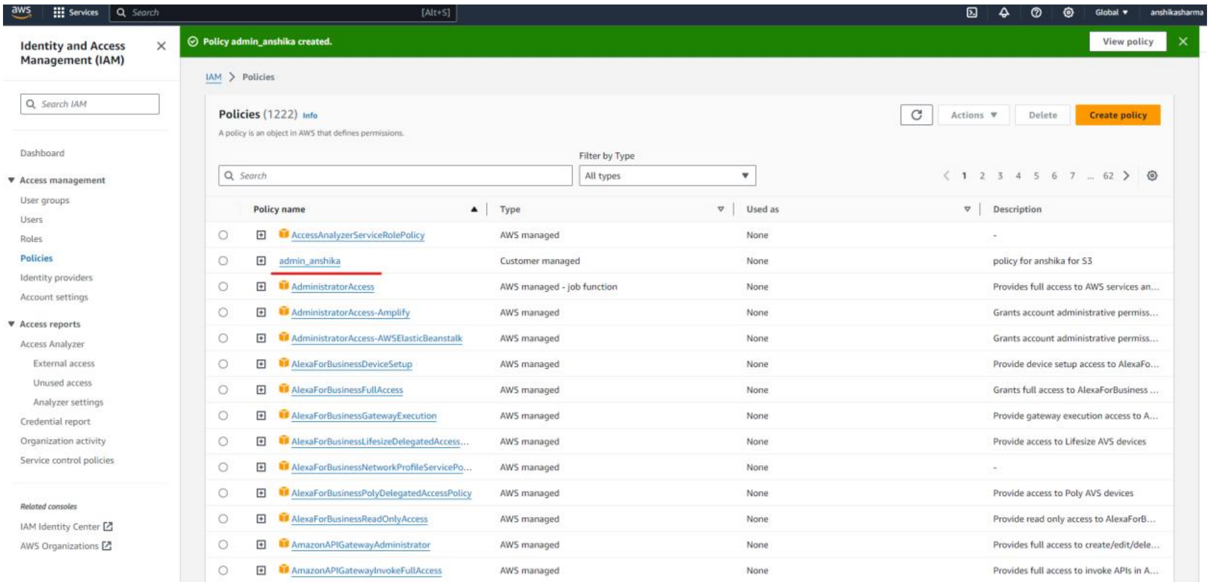
Policy admin_anshika created.

Policies

A policy is an object in AWS that defines permissions.

Loading policies

18.Your policy named admin_anshika, underlined in red, now appears in the policy list.



Policy admin_anshika created.

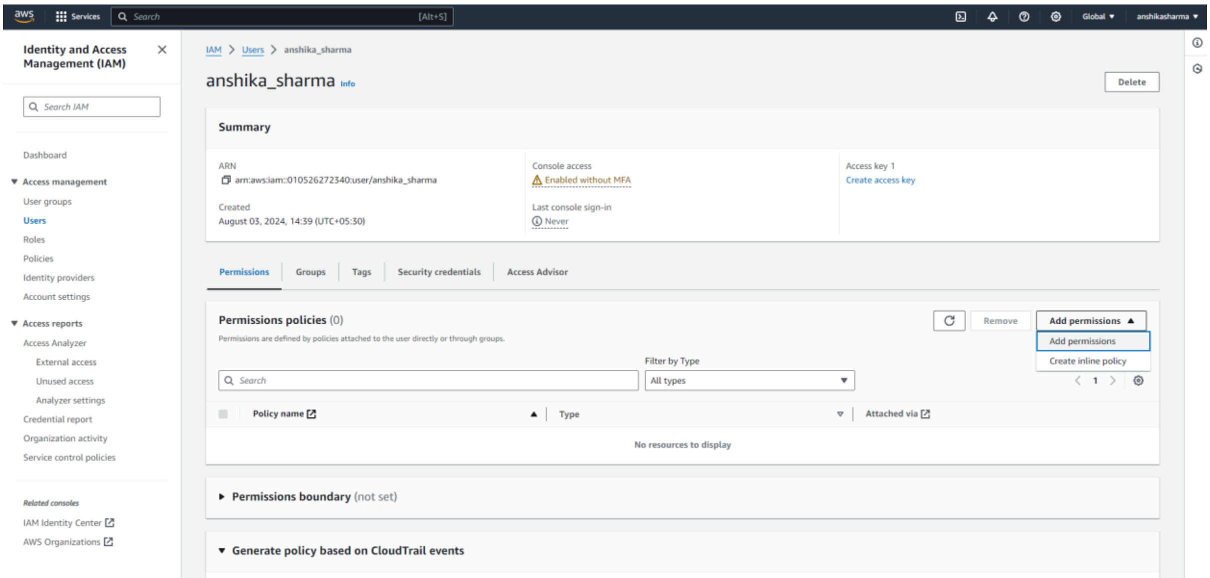
Policies (1222)

A policy is an object in AWS that defines permissions.

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	-
admin_anshika	Customer managed	None	policy for anshika for S3
AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permiss...
AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permiss...
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...
AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in A...

19.Next, you need to add this permission:

- Click on Users from the left pane.
- Select the Permissions tab.
- On the right side, click on Add Permissions.



anshika_sharma Info

Summary

ARN
arn:aws:iam::010526272340:user/anshika_sharma

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 (0)

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

Filter by Type: All types

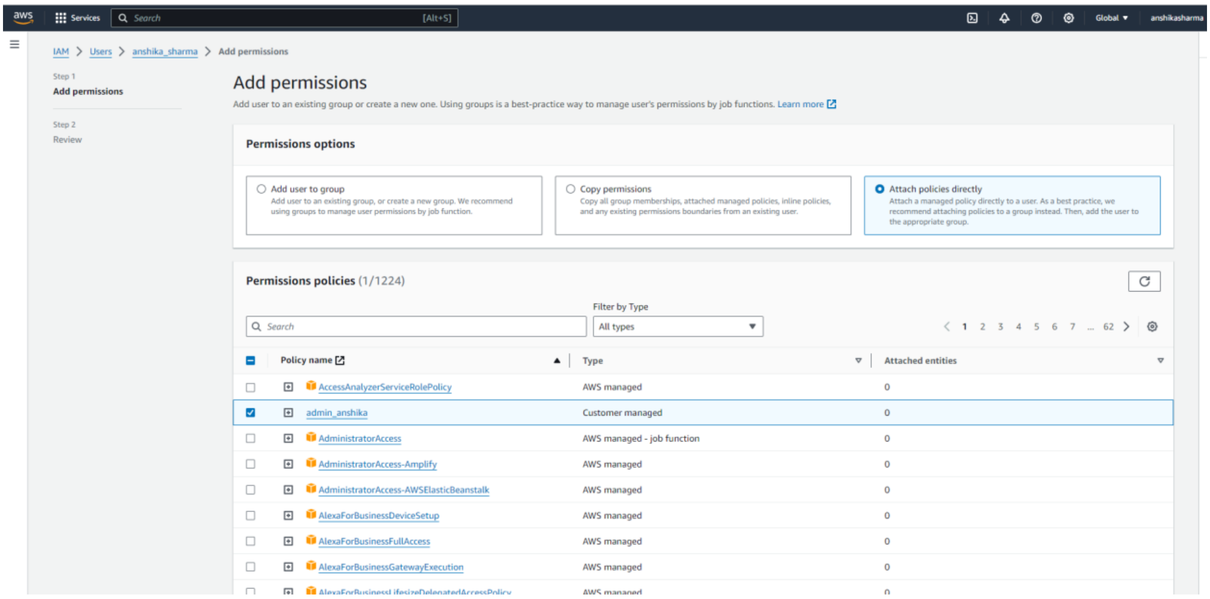
Policy name	Type	Attached via

No resources to display

▸ Permissions boundary (not set)

▾ Generate policy based on CloudTrail events

20.Select the policy you created under the "Add Permissions" section and click on “Attach Policy Directly”.



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.

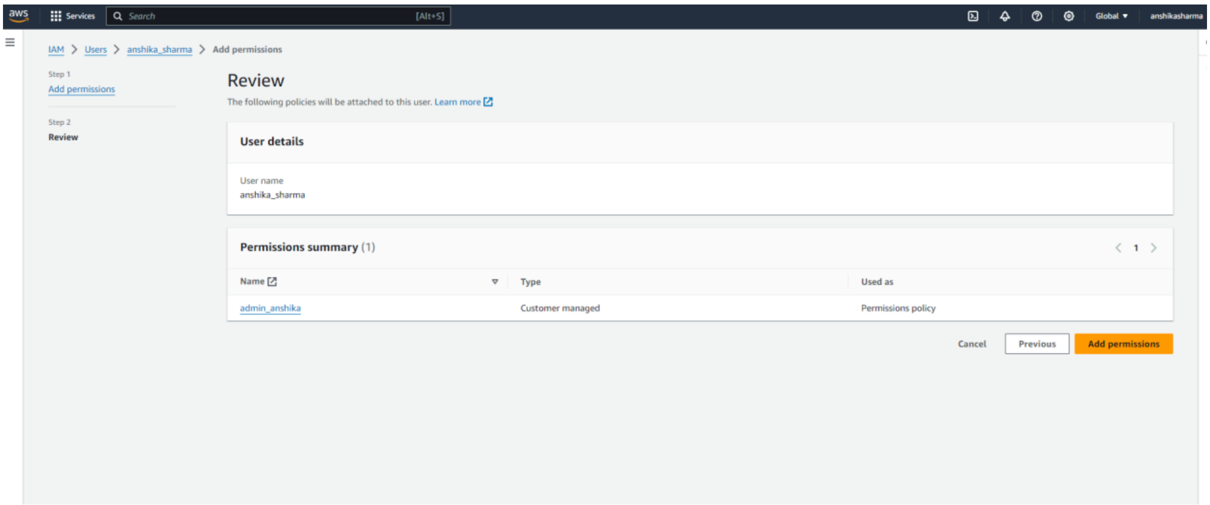
Permissions policies (1/1224)

Filter by Type: All types

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

	Policy name	Type	Attached entities
□	AccessAnalyzerServiceRolePolicy	AWS managed	0
☑	admin_anshika	Customer 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

21.Review the details and click on Add Permissions.



Review

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

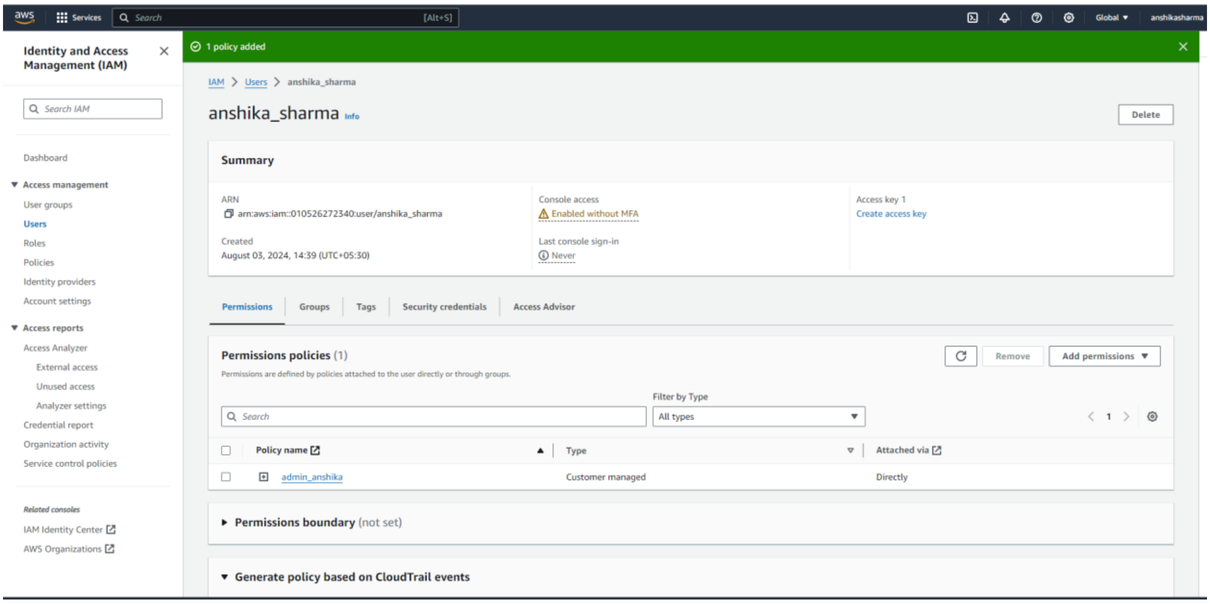
User details

User name
anshika_sharma

Permissions summary (1)

Name	Type	Used as
admin_anshika	Customer managed	Permissions policy

22.Your policy has now been successfully added.



1 policy added

anshika_sharma

Summary

ARN: arn:aws:iam::010526272340:user/anshika_sharma

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 (1)

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

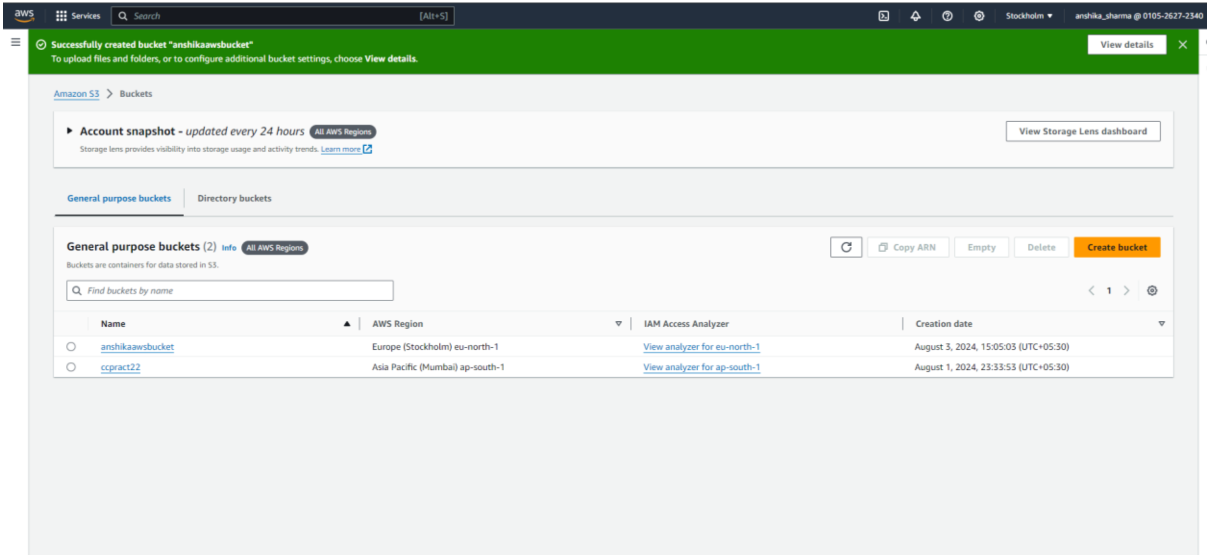
Filter by Type: All types

Policy name	Type	Attached via
admin_anshika	Customer managed	Directly

Permissions boundary (not set)

Generate policy based on CloudTrail events

23.Return to the incognito window where you logged in as the new user and try to create a bucket. You'll see the bucket is created successfully, because of the granted access for S3.



Successfully created bucket "anshikaawsbucket"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

Account snapshot - *updated every 24 hours* All AWS Regions

Storage lens provides visibility into storage usage and activity trends. Learn more

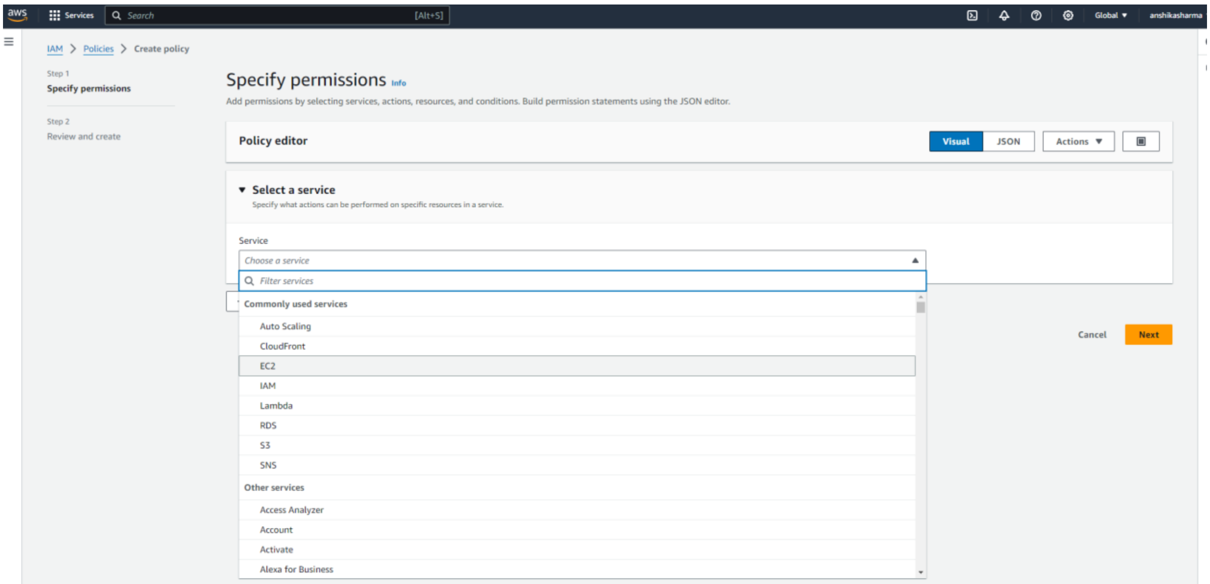
General purpose buckets (2)

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
anshikaawsbucket	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	August 3, 2024, 15:05:03 (UTC+05:30)
ccpract22	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	August 1, 2024, 23:33:53 (UTC+05:30)

24.Repeat the same process for EC2: Just as you did for S3.

Under Specify Permissions service option select EC2.


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

▼ Select a service

Specify what actions can be performed on specific resources in a service.

Service

Choose a service

Filter services

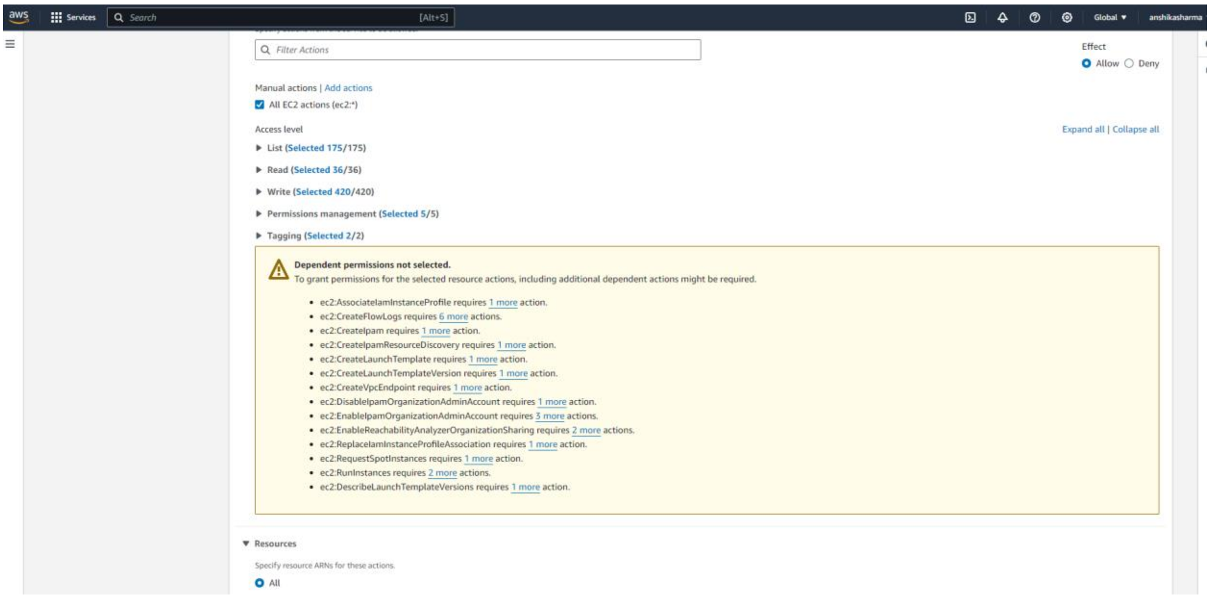
Commonly used services

- Auto Scaling
- CloudFront
- EC2
- IAM
- Lambda
- RDS
- S3
- SNS

Other services

- Access Analyzer
- Account
- Activate
- Alexa for Business

25.Select "All EC2 actions" and “All” under the Resources section


Filter Actions

Effect

● Allow ○ Deny

Manual actions | Add actions

☑ All EC2 actions (ec2:*)

Access level

- ▶ List (Selected 175/175)
- ▶ Read (Selected 36/36)
- ▶ Write (Selected 420/420)
- ▶ Permissions management (Selected 5/5)
- ▶ Tagging (Selected 2/2)

Dependent permissions not selected.
To grant permissions for the selected resource actions, including additional dependent actions might be required.

- ec2:AssociateIamInstanceProfile requires 1 more action.
- ec2:CreateFlowLogs requires 6 more actions.
- ec2:CreateIpam requires 1 more action.
- ec2:CreateIpamResourceDiscovery requires 1 more action.
- ec2:CreateLaunchTemplate requires 1 more action.
- ec2:CreateLaunchTemplateVersion requires 1 more action.
- ec2:CreateVpcEndpoint requires 1 more action.
- ec2:DisableIpamOrganizationAdminAccount requires 1 more action.
- ec2:EnableIpamOrganizationAdminAccount requires 3 more actions.
- ec2:EnableReachabilityAnalyzerOrganizationSharing requires 2 more actions.
- ec2:ReplaceIamInstanceProfileAssociation requires 1 more action.
- ec2:RequestSpotInstances requires 1 more action.
- ec2:RunInstances requires 2 more actions.
- ec2:DescribeLaunchTemplateVersions requires 1 more action.

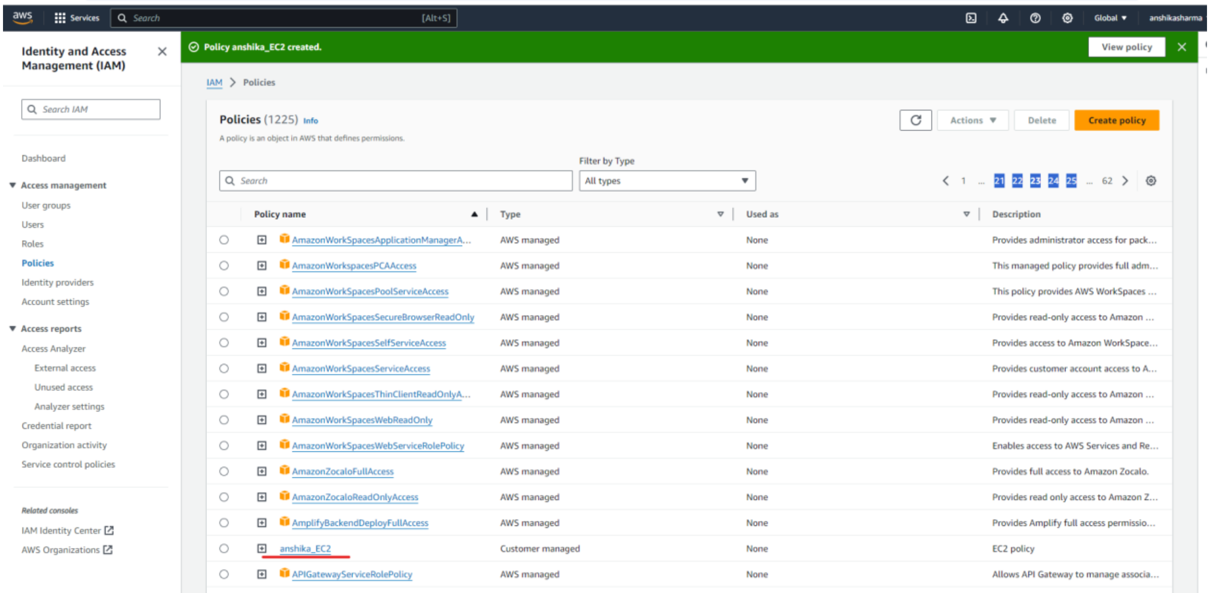
▼ Resources

Specify resource ARNs for these actions.

● All

26. Proceed to the Review and Create pane, where you'll need to specify the policy name and provide a short description for the policy. Click on Create Policy, and the policy will be created successfully.

Your policy named Anshika_EC2, underlined in red, now appears in the policy list.



Policy anshika_EC2 created.

Policies (1225)

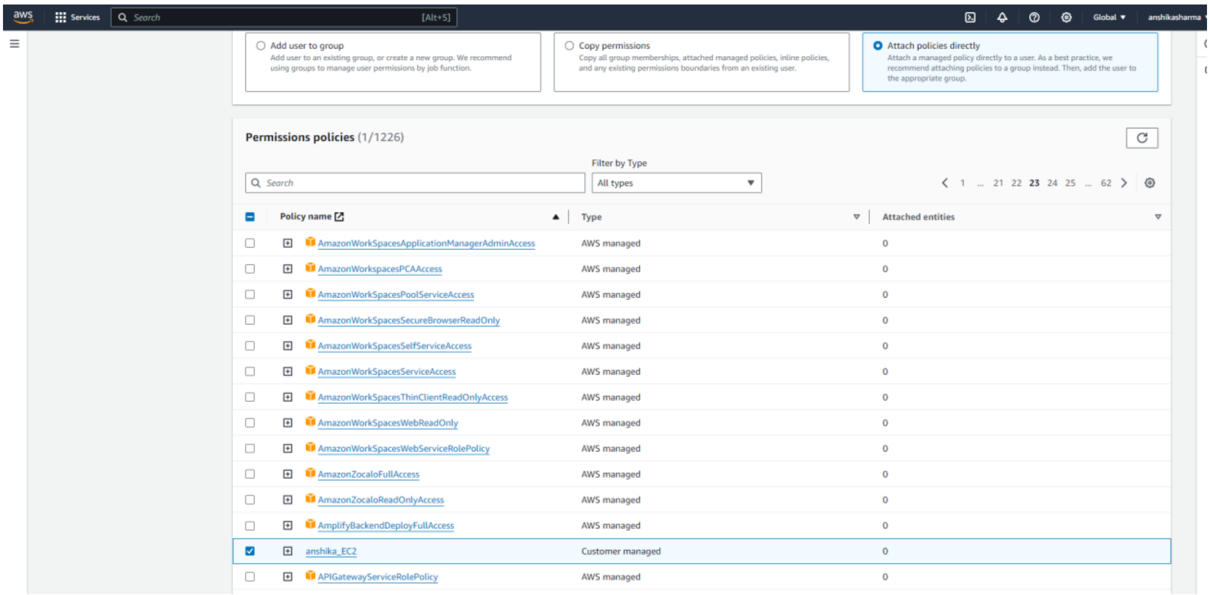
A policy is an object in AWS that defines permissions.

	Policy name	Type	Used as	Description
○	AmazonWorkSpacesApplicationManagerA...	AWS managed	None	Provides administrator access for pack...
○	AmazonWorkspacesPCAAccess	AWS managed	None	This managed policy provides full adm...
○	AmazonWorkSpacesPoolServiceAccess	AWS managed	None	This policy provides AWS WorkSpaces ...
○	AmazonWorkSpacesSecureBrowserReadOnly	AWS managed	None	Provides read-only access to Amazon ...
○	AmazonWorkSpacesSelfServiceAccess	AWS managed	None	Provides access to Amazon WorkSpace...
○	AmazonWorkSpacesServiceAccess	AWS managed	None	Provides customer account access to A...
○	AmazonWorkSpacesThinClientReadOnlyA...	AWS managed	None	Provides read-only access to Amazon ...
○	AmazonWorkSpacesWebReadOnly	AWS managed	None	Provides read-only access to Amazon ...
○	AmazonWorkSpacesWebServiceRolePolicy	AWS managed	None	Enables access to AWS Services and Re...
○	AmazonZocaloFullAccess	AWS managed	None	Provides full access to Amazon Zocalo.
○	AmazonZocaloReadOnlyAccess	AWS managed	None	Provides read only access to Amazon Z...
○	AmplifyBackendDeployFullAccess	AWS managed	None	Provides Amplify full access permissio...
○	anshika_EC2	Customer managed	None	EC2 policy
○	APIGatewayServiceRolePolicy	AWS managed	None	Allows API Gateway to manage associa...

27. Next , you need to add this permission:

- Click on Users from the left pane.
- Select the Permissions tab.
- On the right side, click on Add Permissions

Select the policy you created under the "Add Permissions" section and click on “Attach Policy Directly”



○ 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.

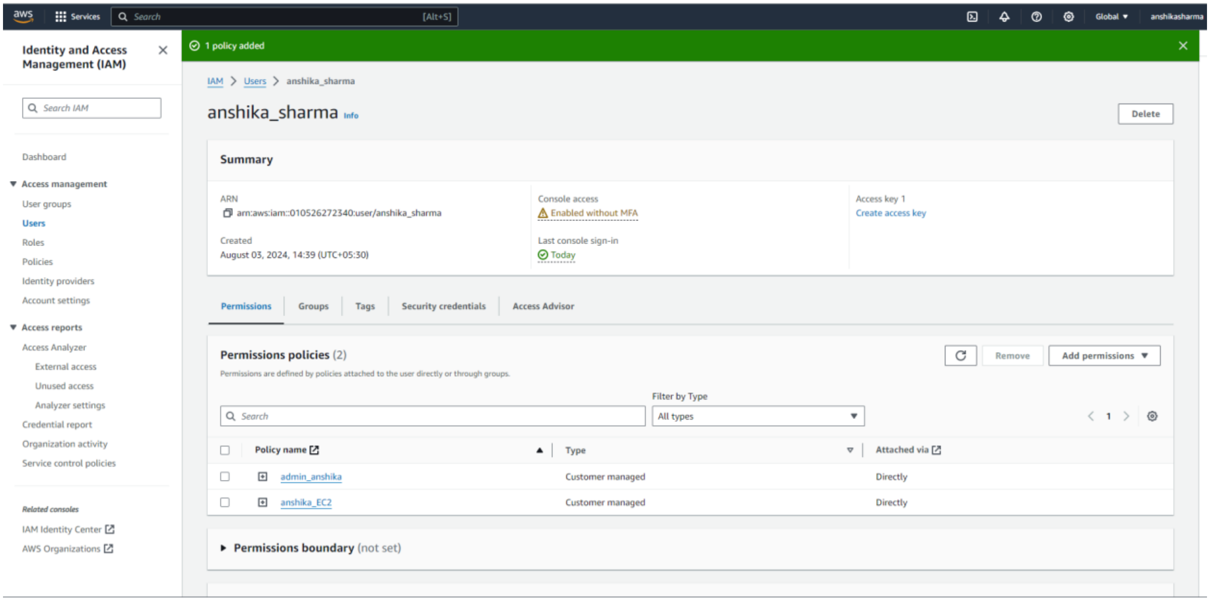
● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1226)

	Policy name	Type	Attached entities
□	AmazonWorkSpacesApplicationManagerAdminAccess	AWS managed	0
□	AmazonWorkspacesPCAAccess	AWS managed	0
□	AmazonWorkSpacesPoolServiceAccess	AWS managed	0
□	AmazonWorkSpacesSecureBrowserReadOnly	AWS managed	0
□	AmazonWorkSpacesSelfServiceAccess	AWS managed	0
□	AmazonWorkSpacesServiceAccess	AWS managed	0
□	AmazonWorkSpacesThinClientReadOnlyAccess	AWS managed	0
□	AmazonWorkSpacesWebReadOnly	AWS managed	0
□	AmazonWorkSpacesWebServiceRolePolicy	AWS managed	0
□	AmazonZocaloFullAccess	AWS managed	0
□	AmazonZocaloReadOnlyAccess	AWS managed	0
□	AmplifyBackendDeployFullAccess	AWS managed	0
☑	anshika_EC2	Customer managed	0
□	APIGatewayServiceRolePolicy	AWS managed	0

28.Review the details and click on Add Permissions.

29.Your policy has now been successfully added.



1 policy added

IAM > Users > anshika_sharma

anshika_sharma Info

Summary

ARN: arn:aws:iam::010526272340:user/anshika_sharma

Created: August 03, 2024, 14:39 (UTC+05:30)

Console access: Enabled without MFA

Last console sign-in: Today

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
admin_anshika	Customer managed	Directly
anshika_EC2	Customer managed	Directly

Permissions boundary (not set)

30. Return to the incognito window where you logged in as the new user and try to launch an instance. You'll see instance is launched successfully, because of the granted access for EC2.