CLOUD COMPUTING PRACTICAL 3

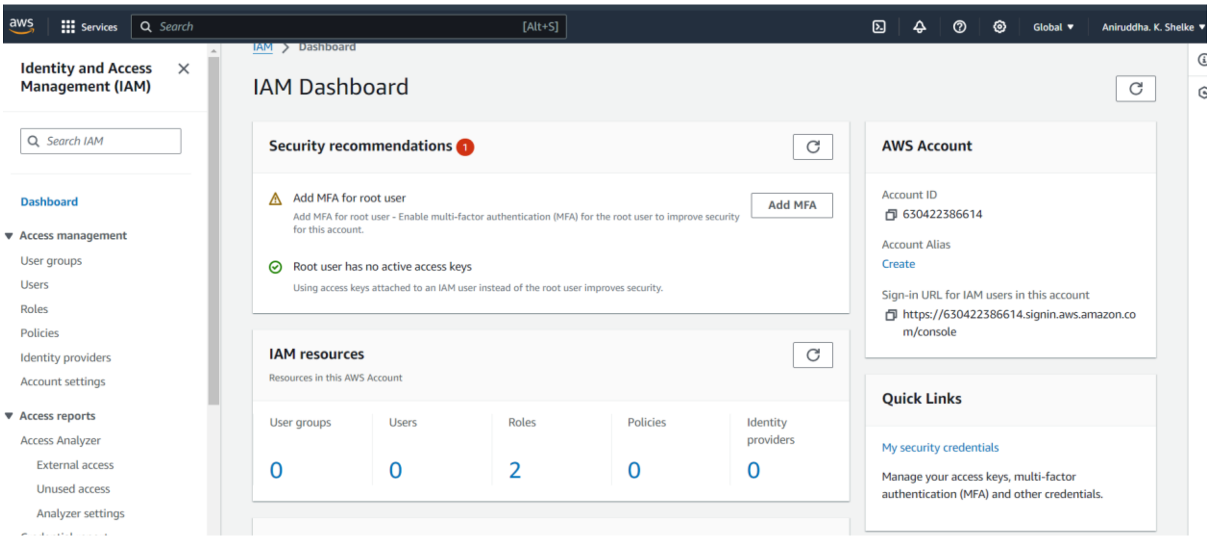
NAME: ANIRUDDHA.K.SHELKE

SAP ID: 86062300008

ROLL NO: A062

DATE: 03/08/2024

Step 1: Sign in into your AWS account, search for 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	0	0

AWS Account

Account ID
630422386614

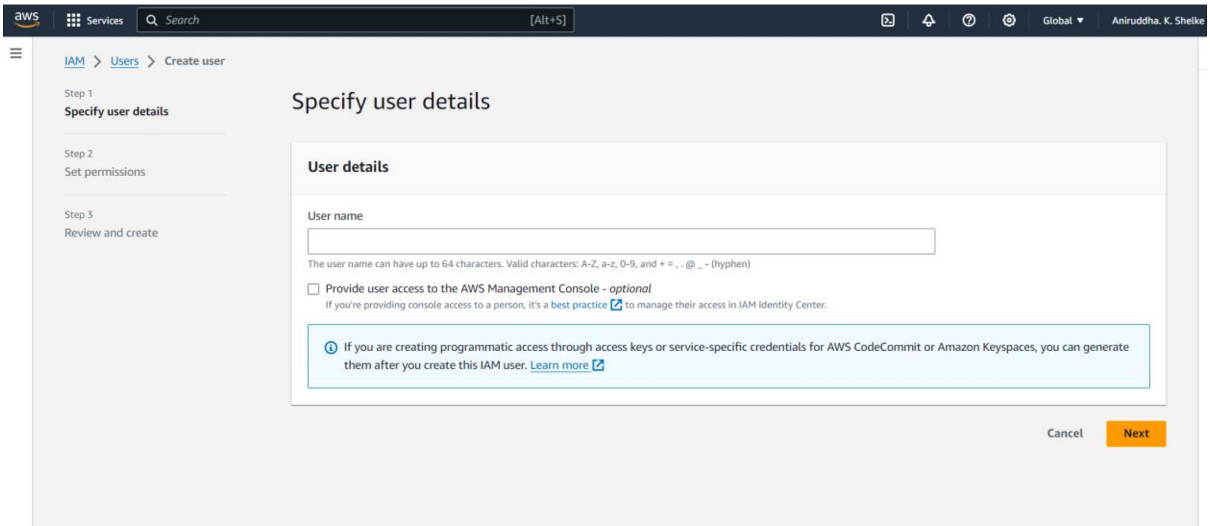
Account Alias

Sign-in URL for IAM users in this account
https://630422386614.signin.aws.amazon.com/console

Quick Links

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

Step 2: Click on Users option and Create users



Specify user details

User details

User name

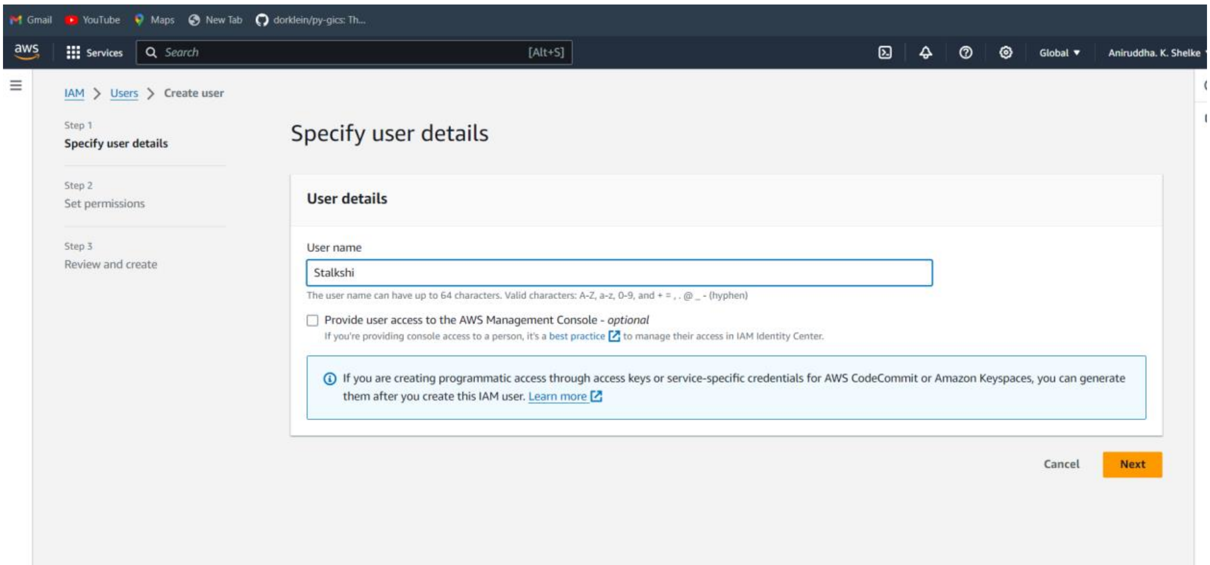
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ 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

Step 3: Give your user a name



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

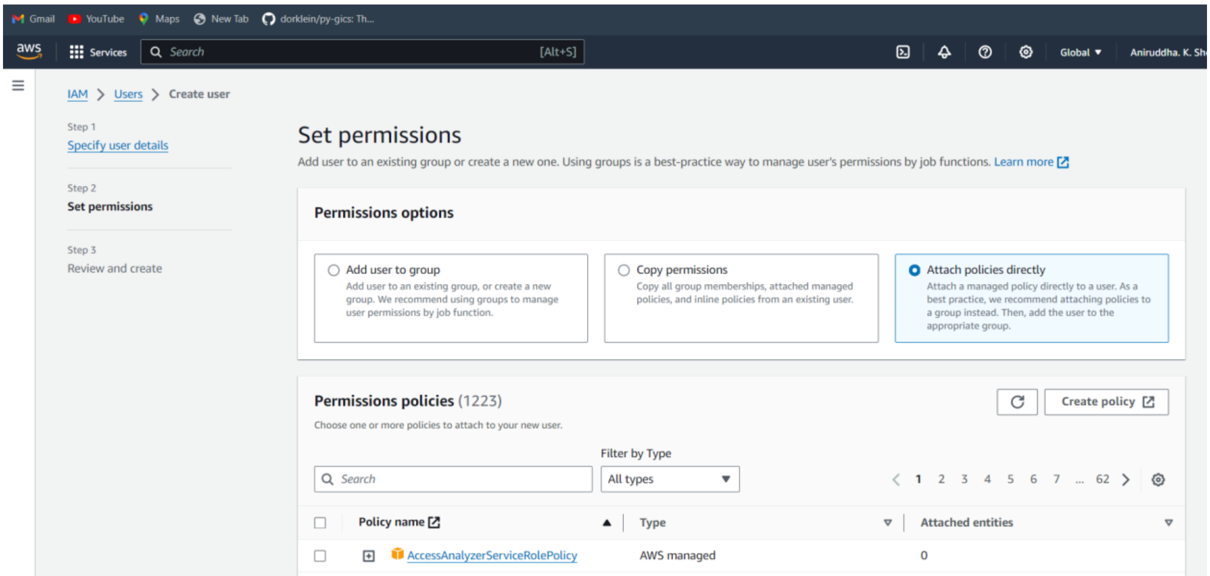
Stalkshi

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

Step 4: In Permissions status select attach policies



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.

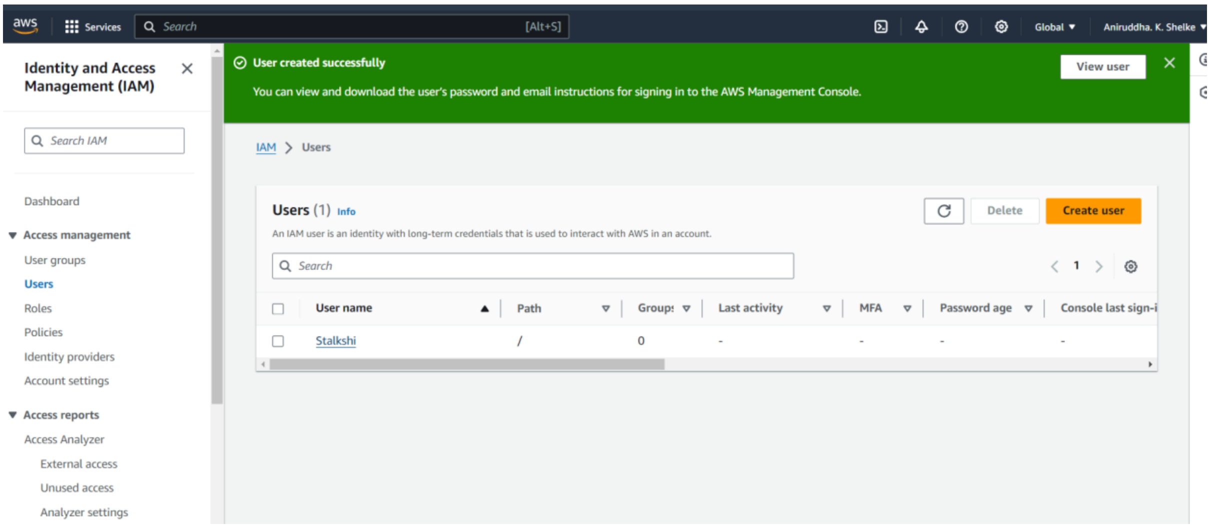
● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1223)

Choose one or more policies to attach to your new user.

□	Policy name ▲	Type	Attached entities
□	⊞ AccessAnalyzerServiceRolePolicy	AWS managed	0

Step 5: You can see that user has been created successfully



User created successfully

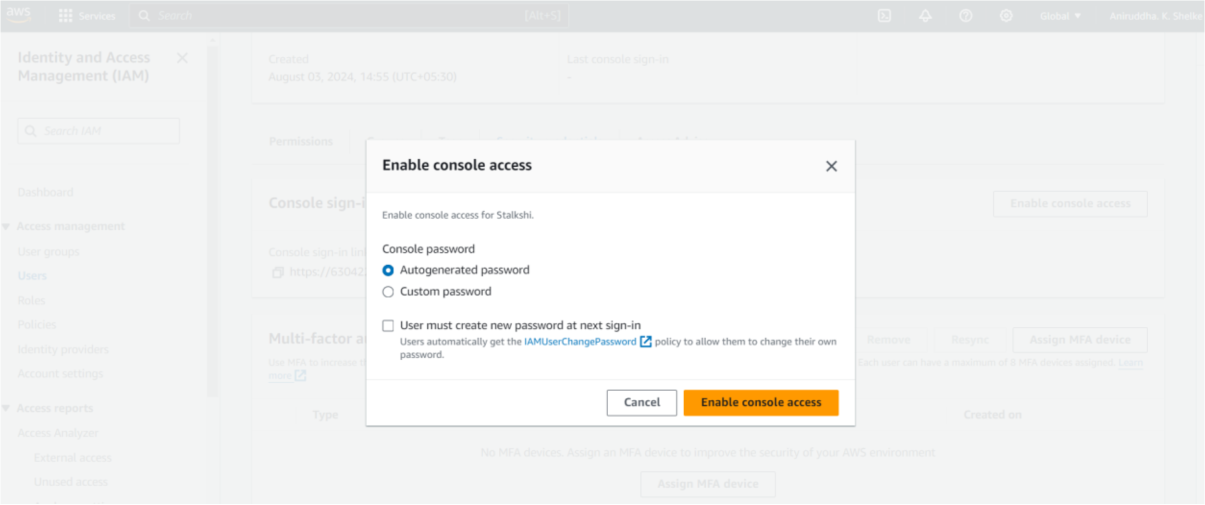
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

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	Groups	Last activity	MFA	Password age	Console last sign-i
□	Stalkshi	/	0	-	-	-	-

Step 6: On Security Credentials tab Enable Console access



Created
August 03, 2024, 14:55 (UTC+05:30)

Last console sign-in
-

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

Enable console access

Enable console access for Stalkshi.

Console password

● Autogenerated password

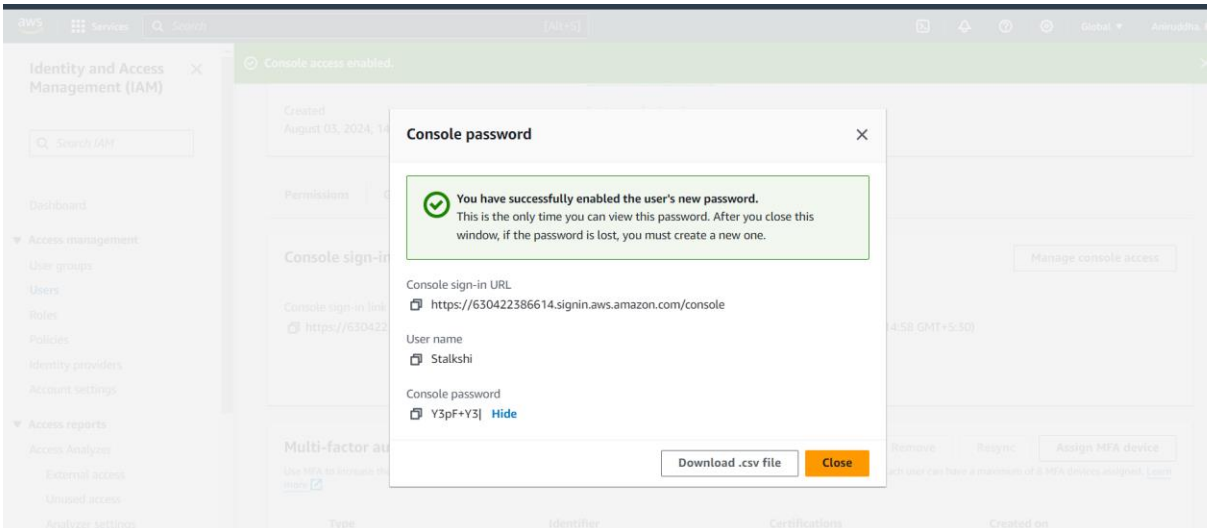
○ Custom password

□ User must create new password at next sign-in

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

Cancel | Enable console access

Step 7: You can see this



Console password

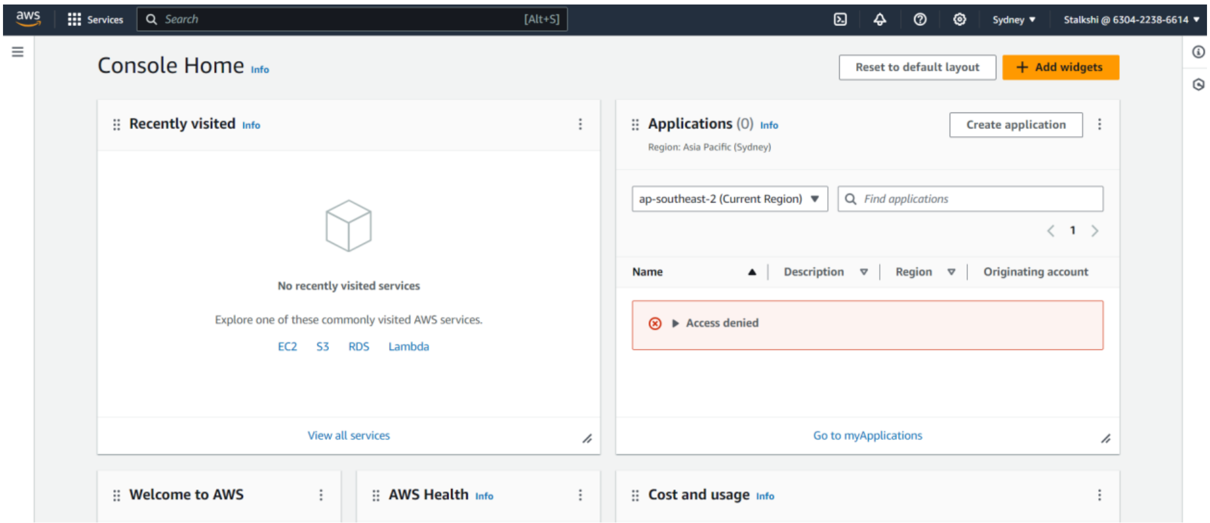
You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

Console sign-in URL
https://630422386614.signin.aws.amazon.com/console

User name
Stalkshi

Console password
Y3pF+Y3| Hide

Step 8: Open the incognito tab and paste the link it will direct you to the Sign in page now Sign in with your User name “Stalkshi” and password.

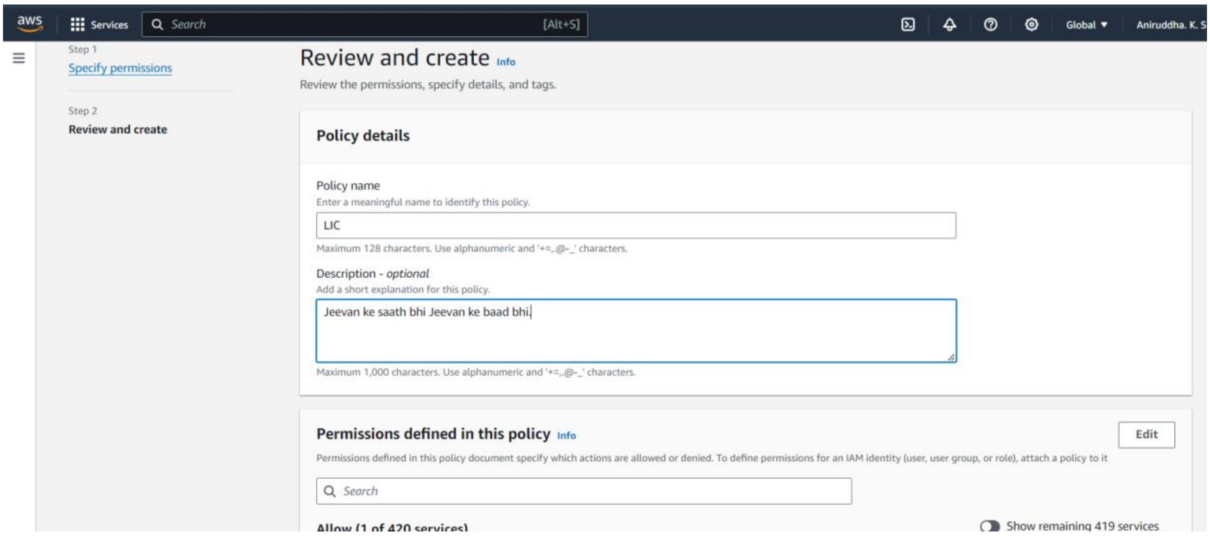


No recently visited services

Explore one of these commonly visited AWS services.

Access denied

Step 9: Go back to your main account and Create a policy for “Stalkshi”, select json and enable all, select service as S3



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

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

Permissions defined in this policy Info

Edit

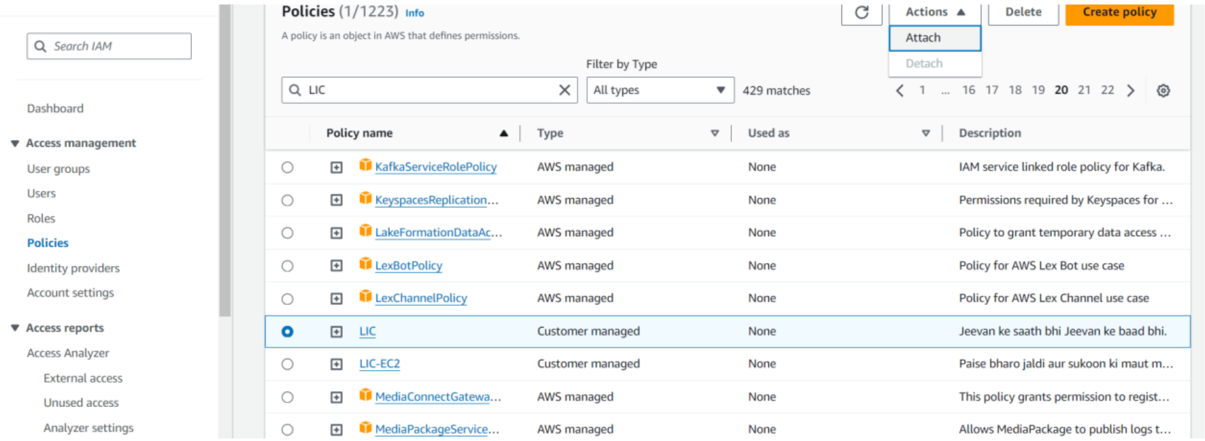
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (1 of 420 services)

Show remaining 419 services

Step 10: Attach ploicy



Policies (1/1223) Info

A policy is an object in AWS that defines permissions.

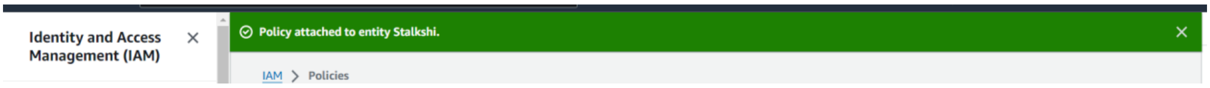
Filter by Type

LIC | All types | 429 matches

< 1 ... 16 17 18 19 20 21 22 >

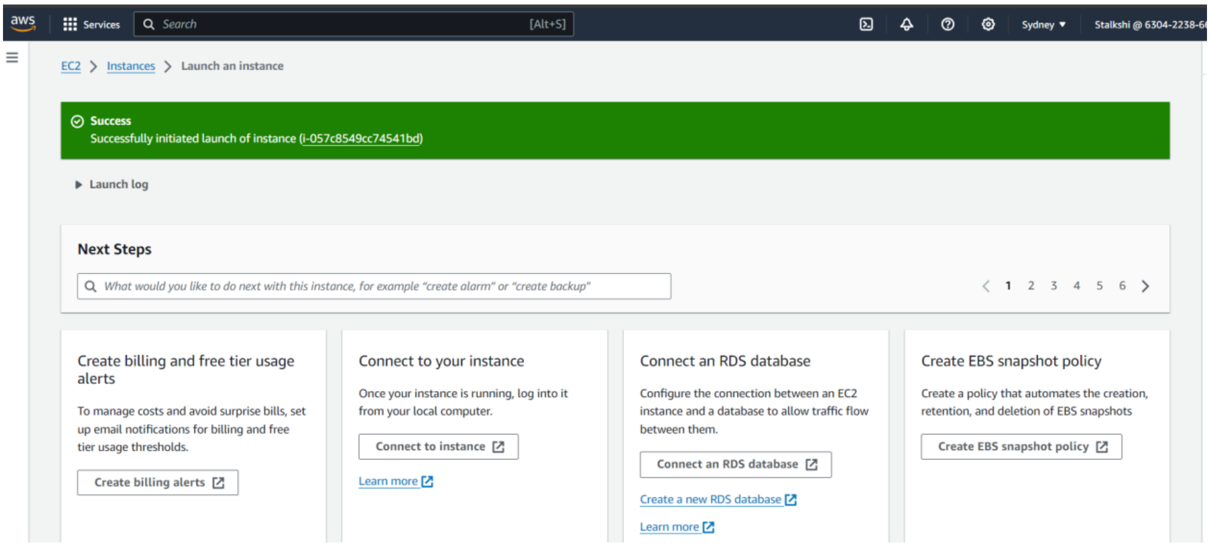
		Policy name	Type	Used as	Description
○	⊞	KafkaServiceRolePolicy	AWS managed	None	IAM service linked role policy for Kafka.
○	⊞	KeyspacesReplication...	AWS managed	None	Permissions required by Keyspaces for ...
○	⊞	LakeFormationDataAc...	AWS managed	None	Policy to grant temporary data access ...
○	⊞	LexBotPolicy	AWS managed	None	Policy for AWS Lex Bot use case
○	⊞	LexChannelPolicy	AWS managed	None	Policy for AWS Lex Channel use case
●	⊞	LIC	Customer managed	None	Jeevan ke saath bhi Jeevan ke baad bhi.
○	⊞	LIC-EC2	Customer managed	None	Paise bharo jaldi aur sukoon ki maut m...
○	⊞	MediaConnectGatewa...	AWS managed	None	This policy grants permission to regist...
○	⊞	MediaPackageService...	AWS managed	None	Allows MediaPackage to publish logs t...

Step 11: Policy has been attached to the user



Policy attached to entity Stalkshi.

Step 12: Create an EC2 policy and attach it to the user, now the user has the access for S3 and EC2 instance, create any one of the instance for the user.



Success
Successfully initiated launch of instance (i-057c8549cc74541bd)

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Connect to your instance

Once your instance is running, log into it from your local computer.

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots