rajendra0968jangid

IAM & AWS CLI (Identity and Access Management)

SAA-C03

IAM

In AWS, IAM (Identity and Access Management) is the service used to securely manage access to AWS resources. Two core components of IAM are Users and Groups.

IAM User

- An IAM User is an entity that represents a single person or application that interacts with AWS services.

Feature	Description
Credentials	Can have **username** + **password** (for AWS Management Console access) and/or **access keys** (for API/CLI access).
Permissions	Permissions are assigned directly or via **groups**.
Use Case	Ideal for **individual users** such as admins, developers, or applications.
Limits	Default limit is **5,000 IAM users** per AWS account.

IAM Group

- An IAM Group is a collection of IAM users. Groups allow you to manage permissions collectively rather than individually.

Feature	Description
No credentials	Groups don't have credentials themselves.
Permission control	Policies attached to the group apply to **all users** in that group.
Use Case	Useful for managing users with similar roles (e.g., Admins, Developers).
Nesting	Groups **cannot contain other groups.**

Best Practices

- Usegroups to assign permissions wherever possible. Avoid root user for everyday tasks—create IAM users instead.
- Enable MFA (Multi-Factor Authentication) for additional security.
- Use least privilege principle—only give the access needed.

Example Scenario

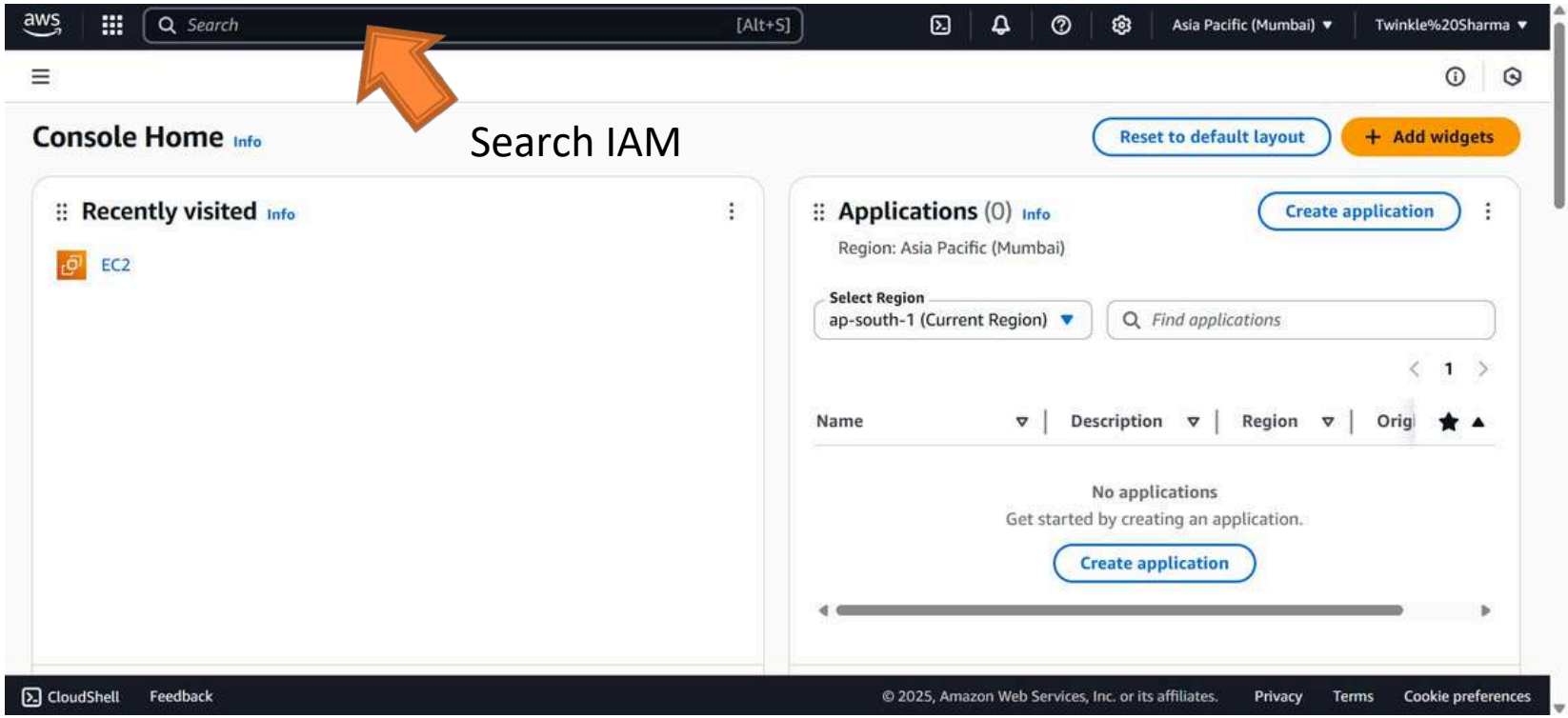
- Let's say you have a team of developers.
- You create an IAM Group called Developers.
- Attach policies like AmazonEC2ReadOnlyAccess to the group.
- Create IAM Users like alice, bob, and charlie.

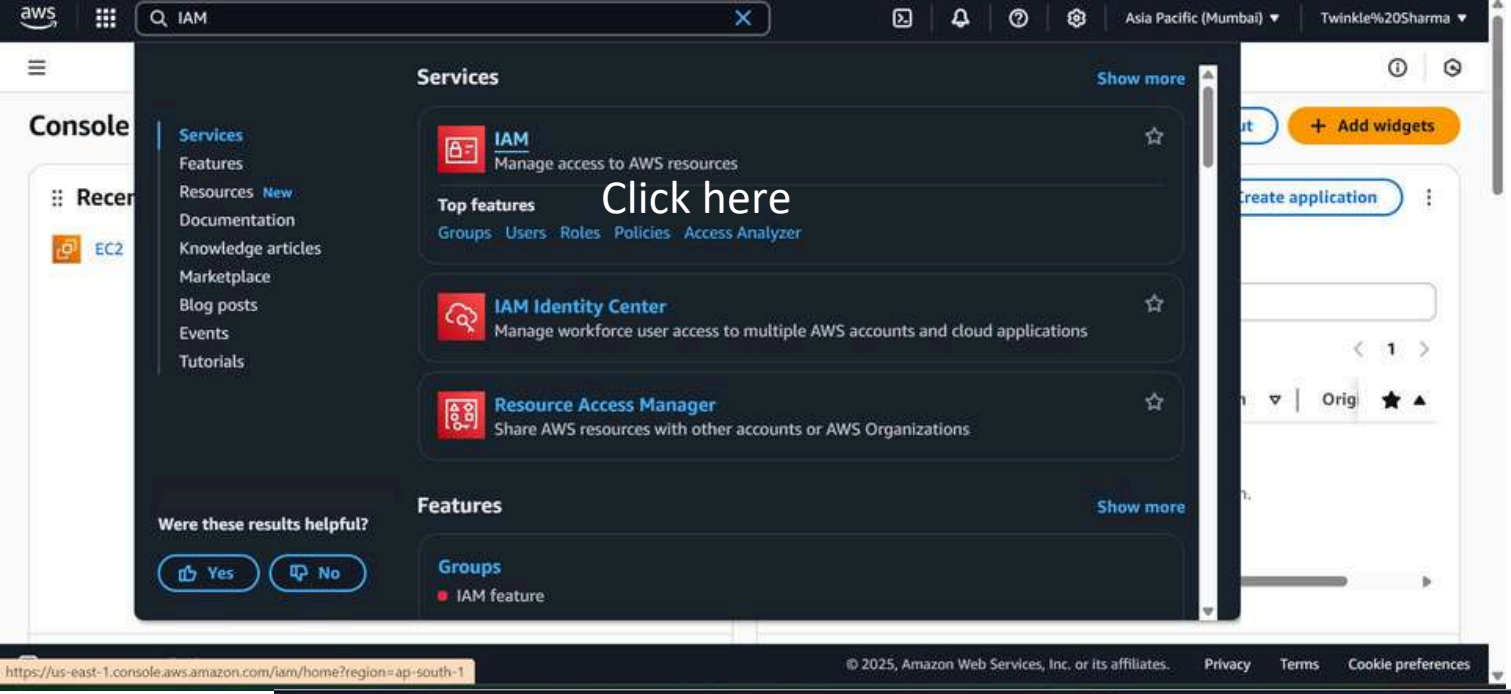
Addthem to the Developers group.

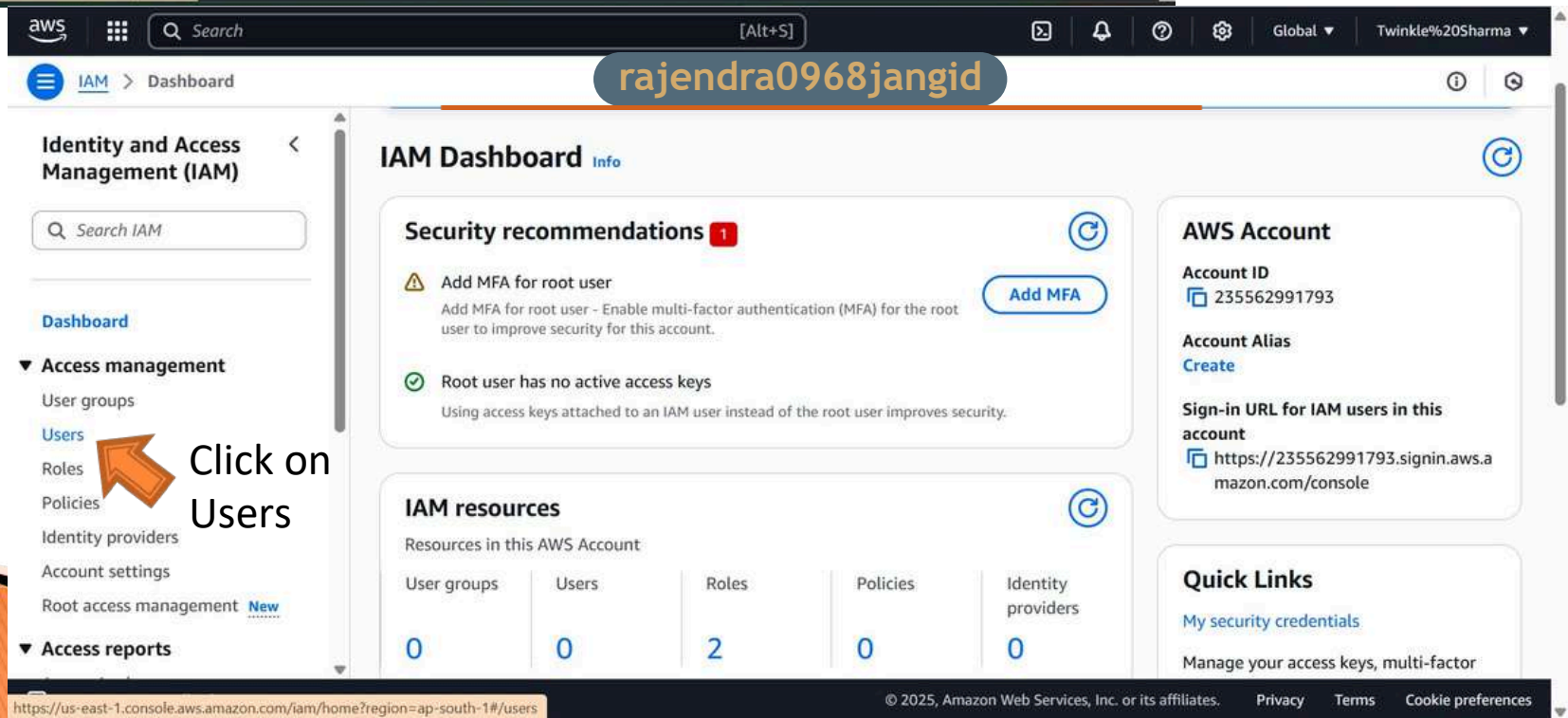
- All three now inherit the same EC2 read-only permissions.

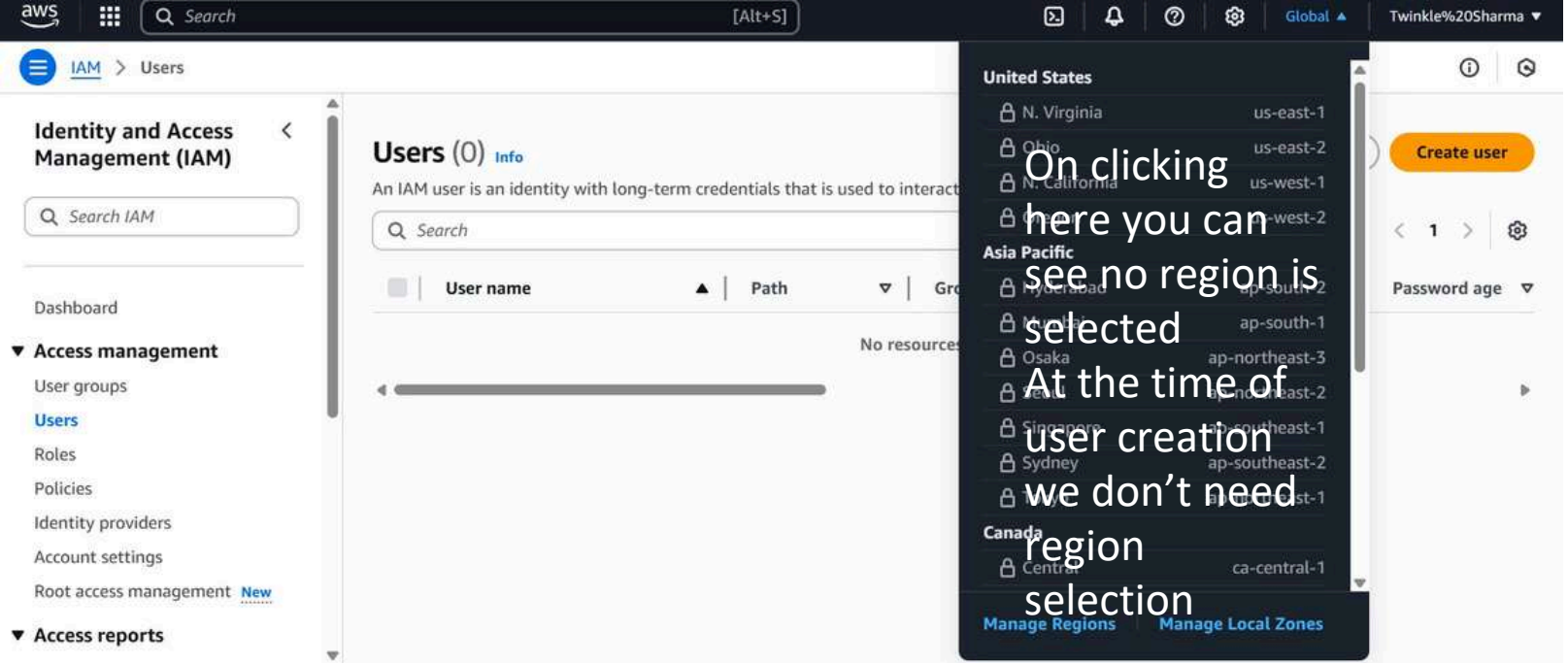
IAM Users & Groups Hands On

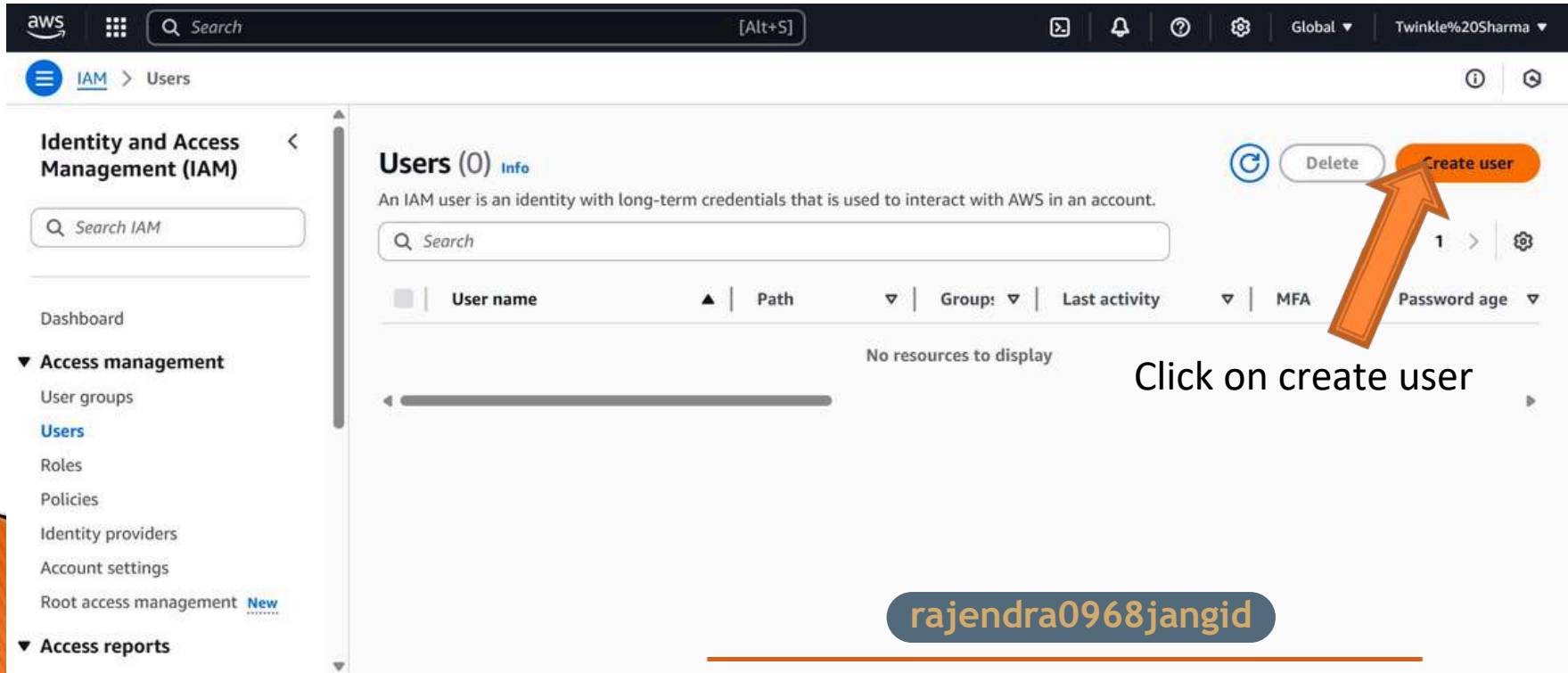
- Go to https://aws.amazon.com/console/
- Sign in your account

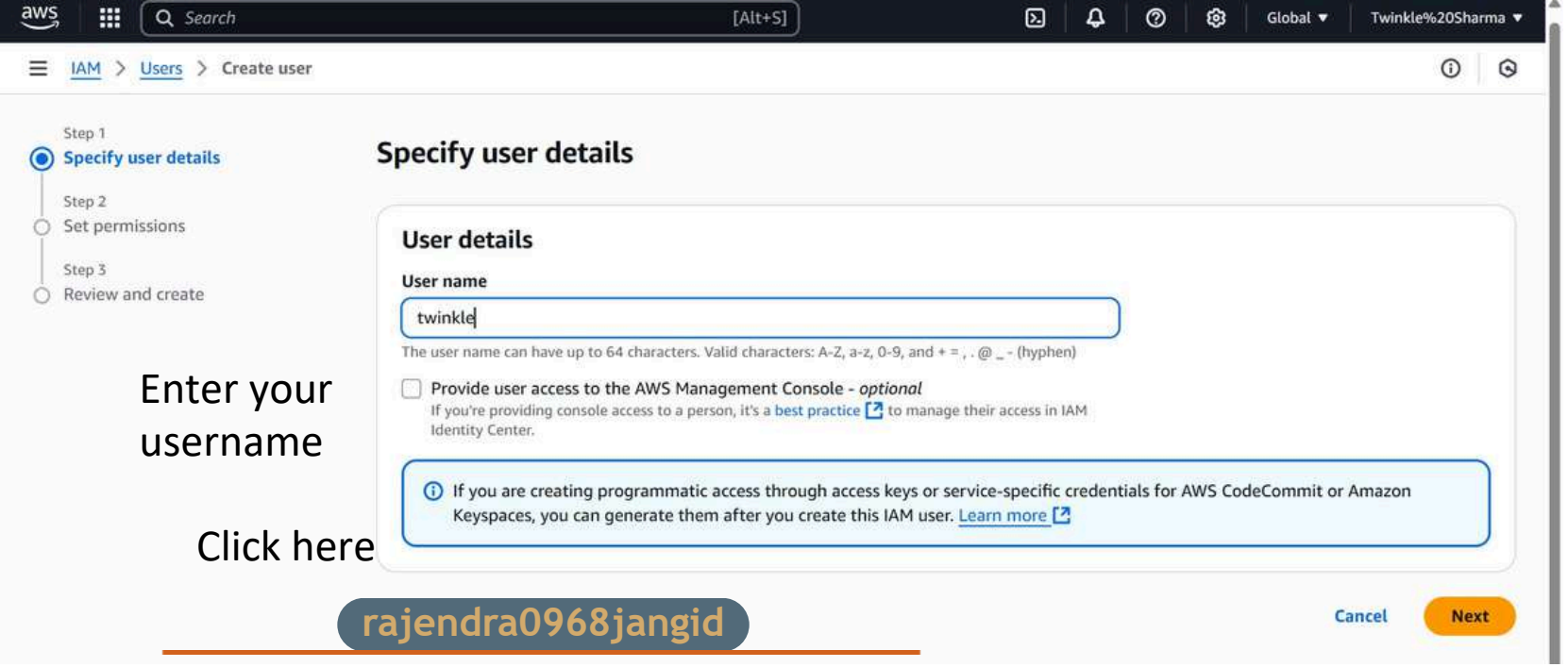



IAM
Asia Pacific (Mumbai)
Twinkle%20Sharma
Console
Services
Features
Resources New
Documentation
Knowledge articles
Marketplace
Blog posts
Events
Tutorials
Show more
IAM
Manage access to AWS resources
Top features
Groups Users Roles Policies Access Analyzer
Click here
IAM Identity Center
Manage workforce user access to multiple AWS accounts and cloud applications
Resource Access Manager
Share AWS resources with other accounts or AWS Organizations
Features
Show more
Groups
IAM feature
Were these results helpful?
Yes
No
Add widgets
Create application
EC2
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
Global
Twinkle%20Sharma
IAM > Dashboard
rajendra0968jangid
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
Click on Users
IAM Dashboard Info
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.
Add MFA
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 0
Users 0
Roles 2
Policies 0
Identity providers 0
AWS Account
Account ID
235562991793
Account Alias
Create
Sign-in URL for IAM users in this account
https://235562991793.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



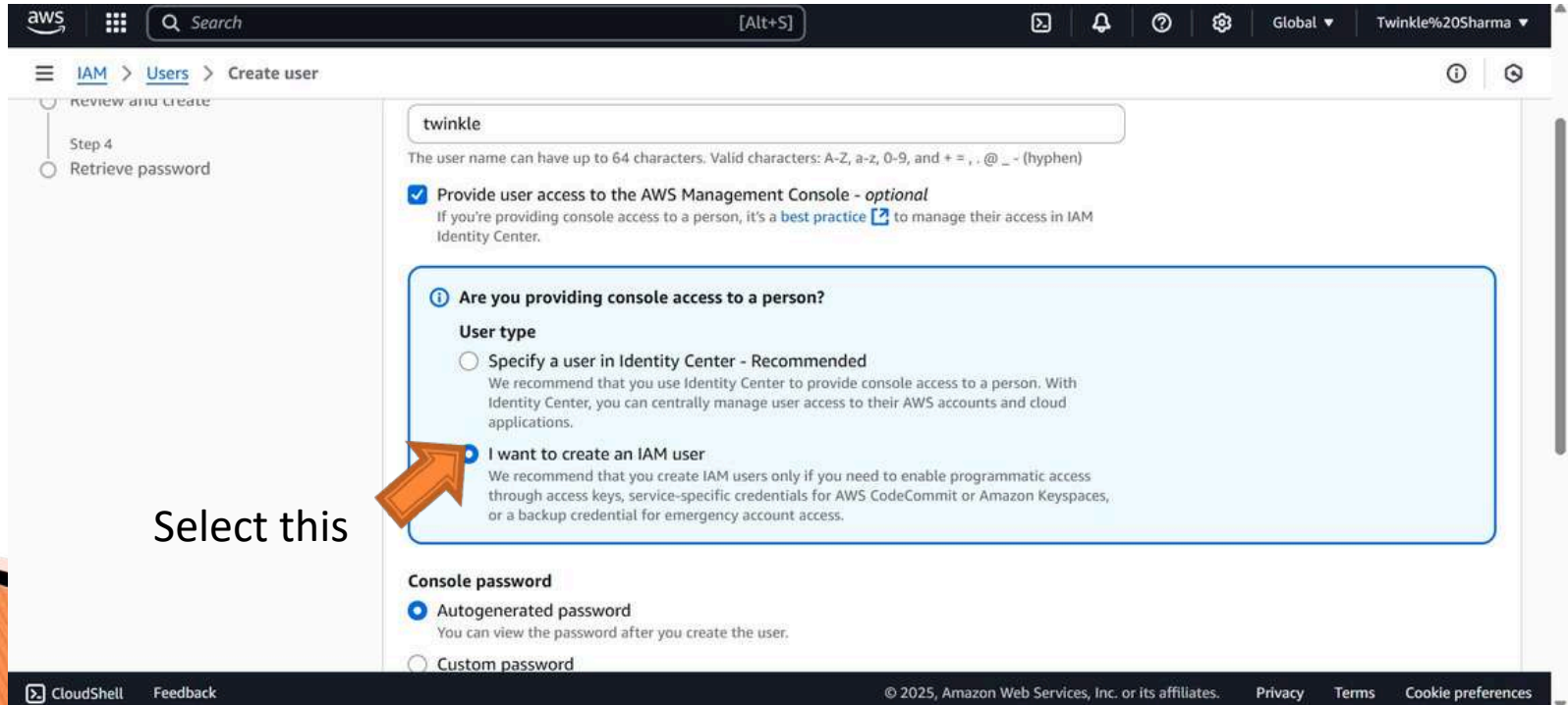




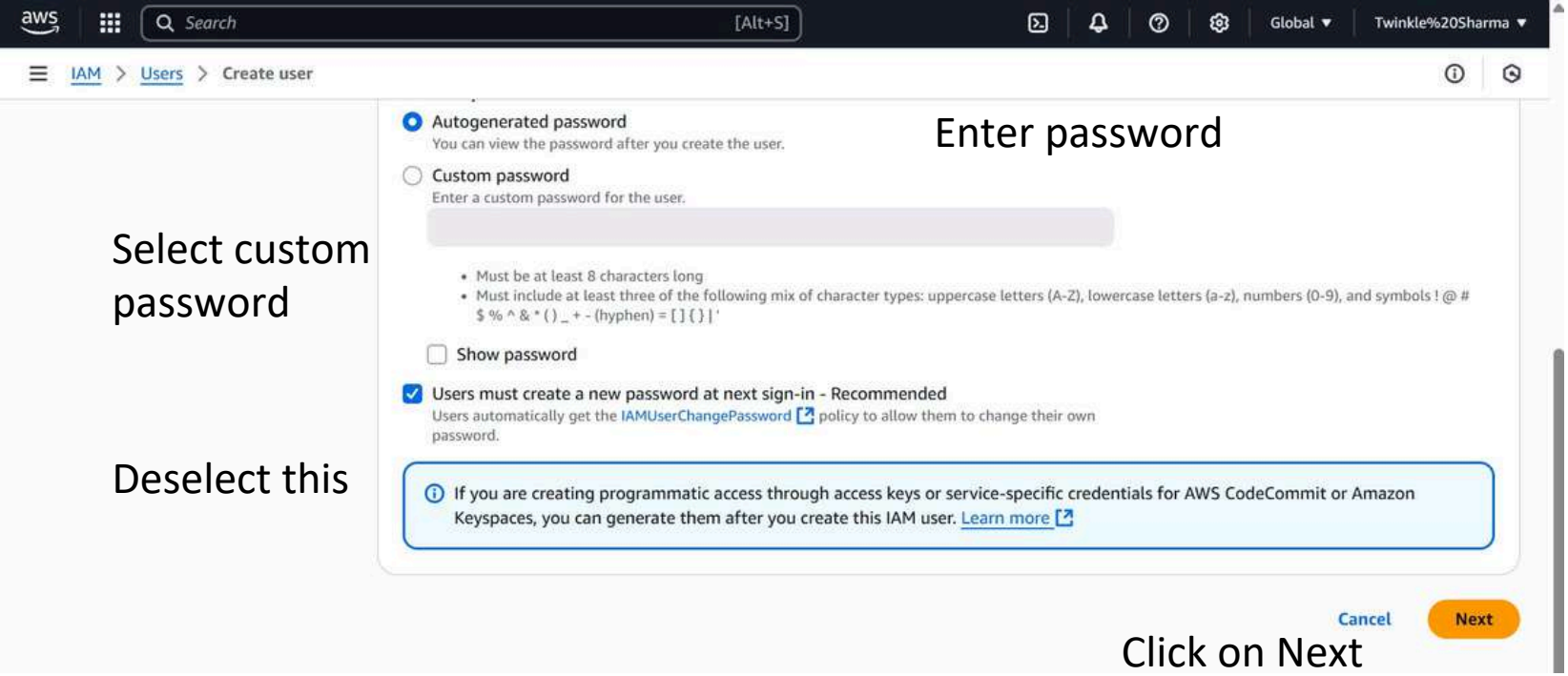
Enter your username

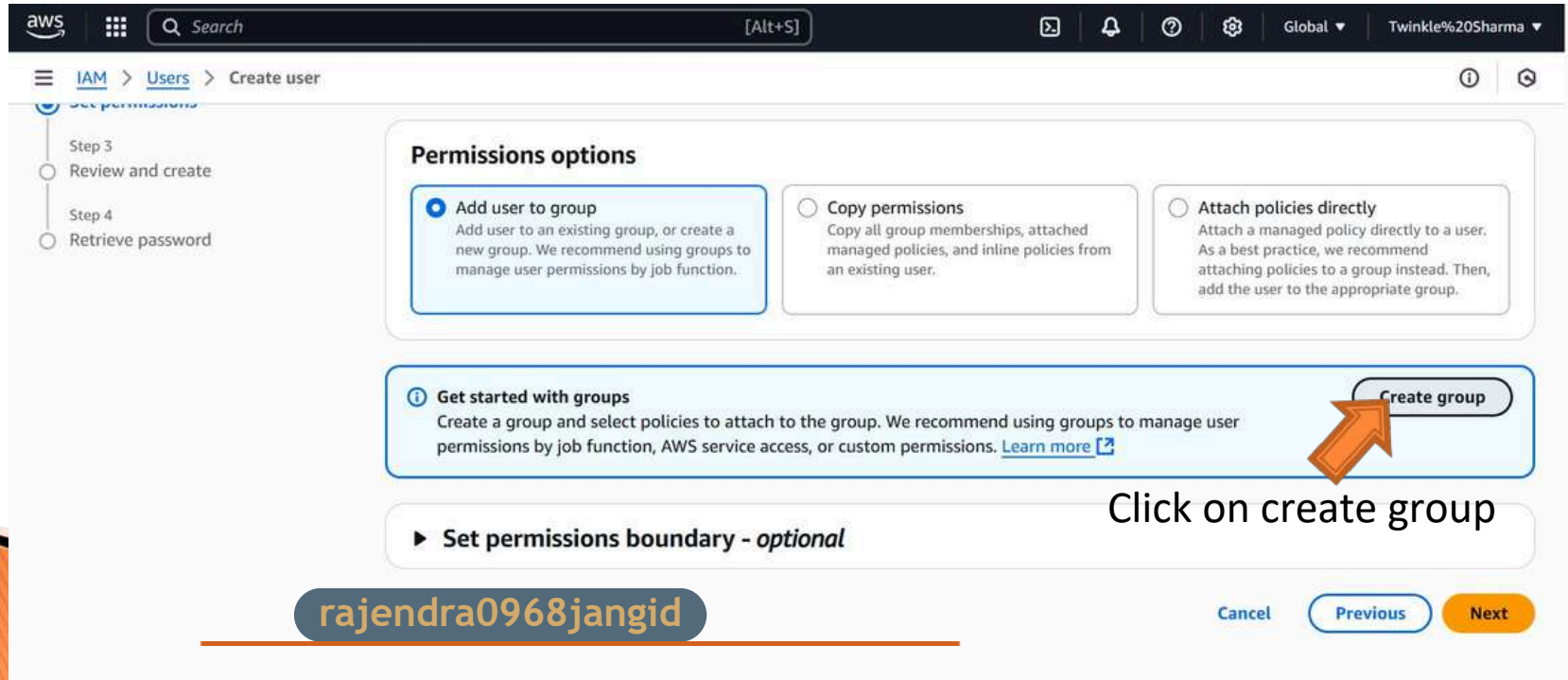
Click here

rajendra0968jangid



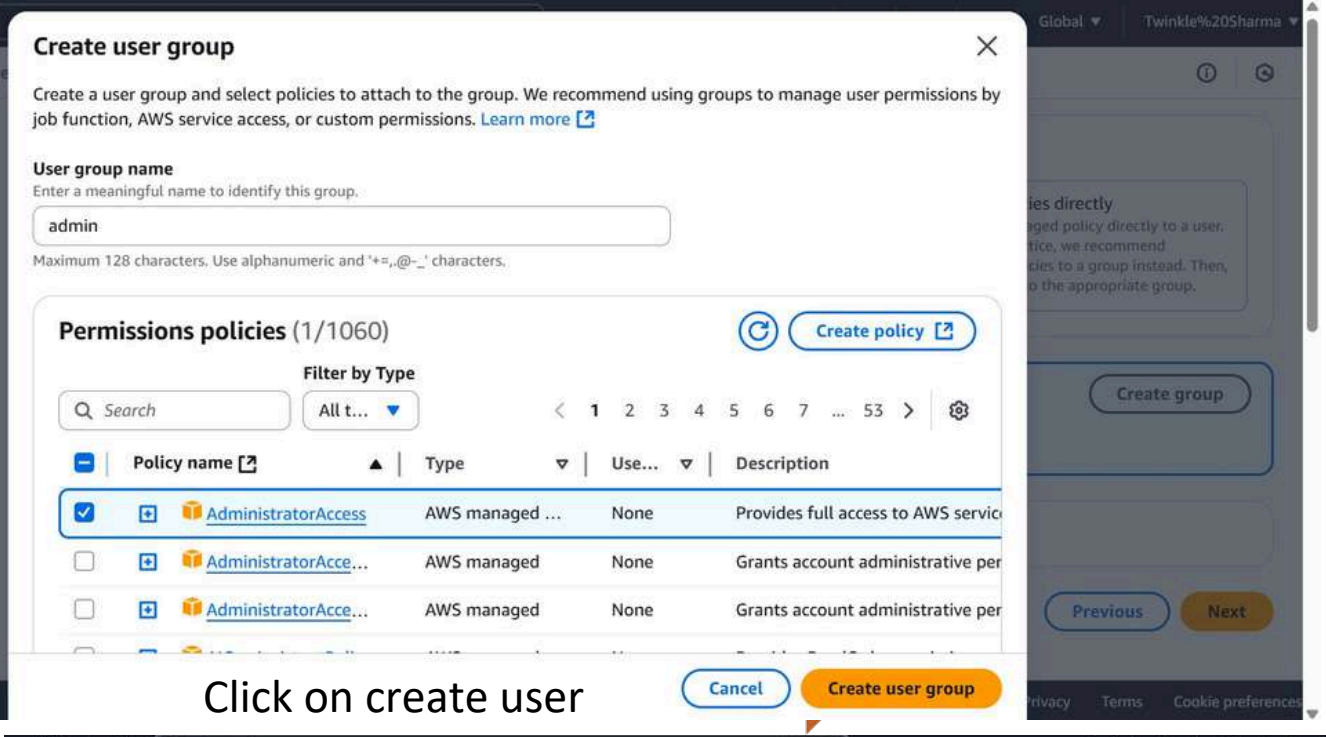
Select this



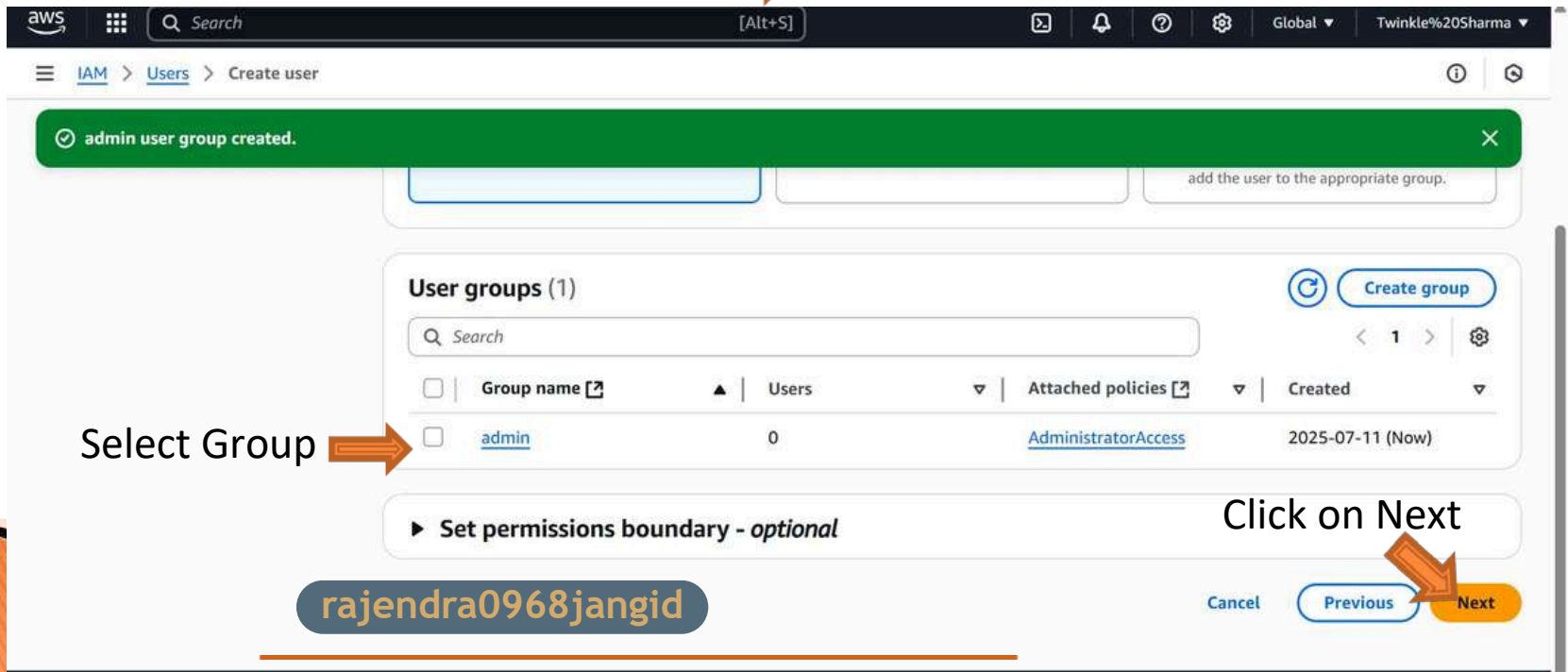


Enter user group name

Select Policy

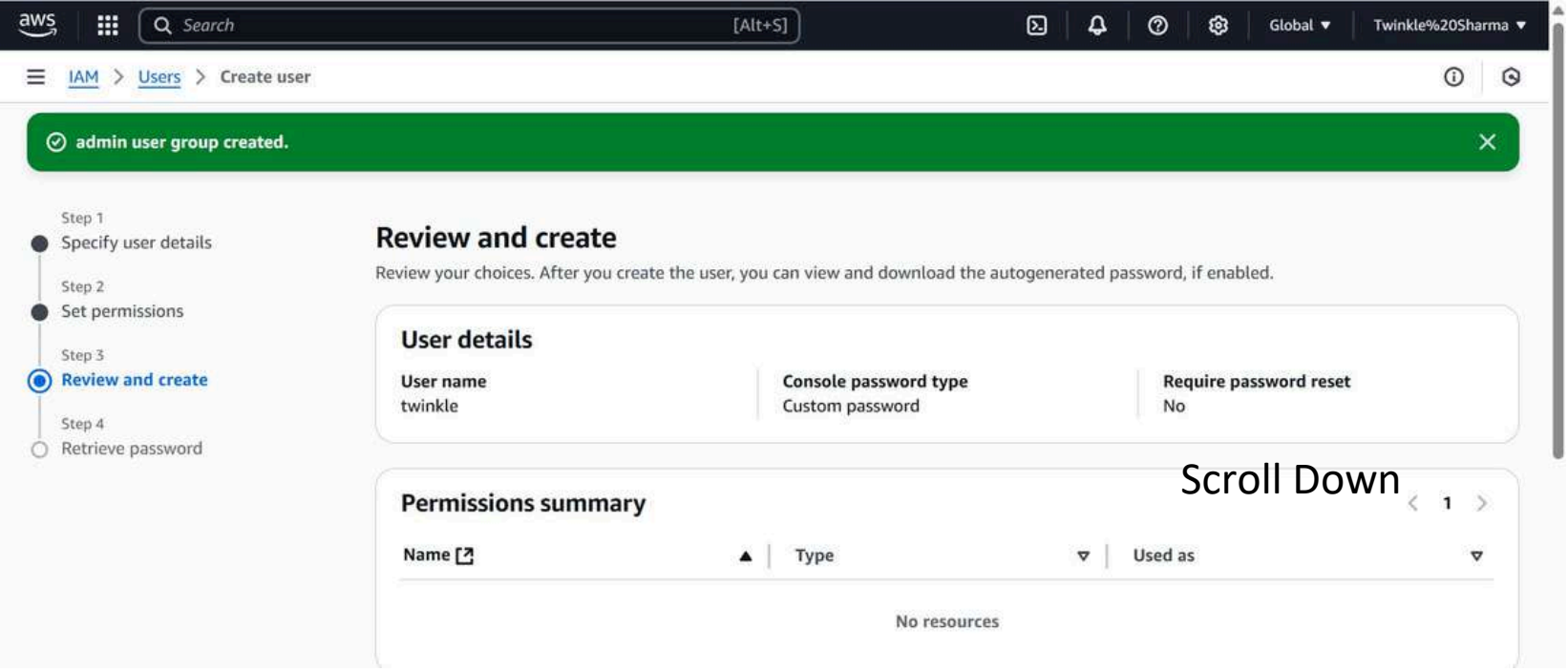


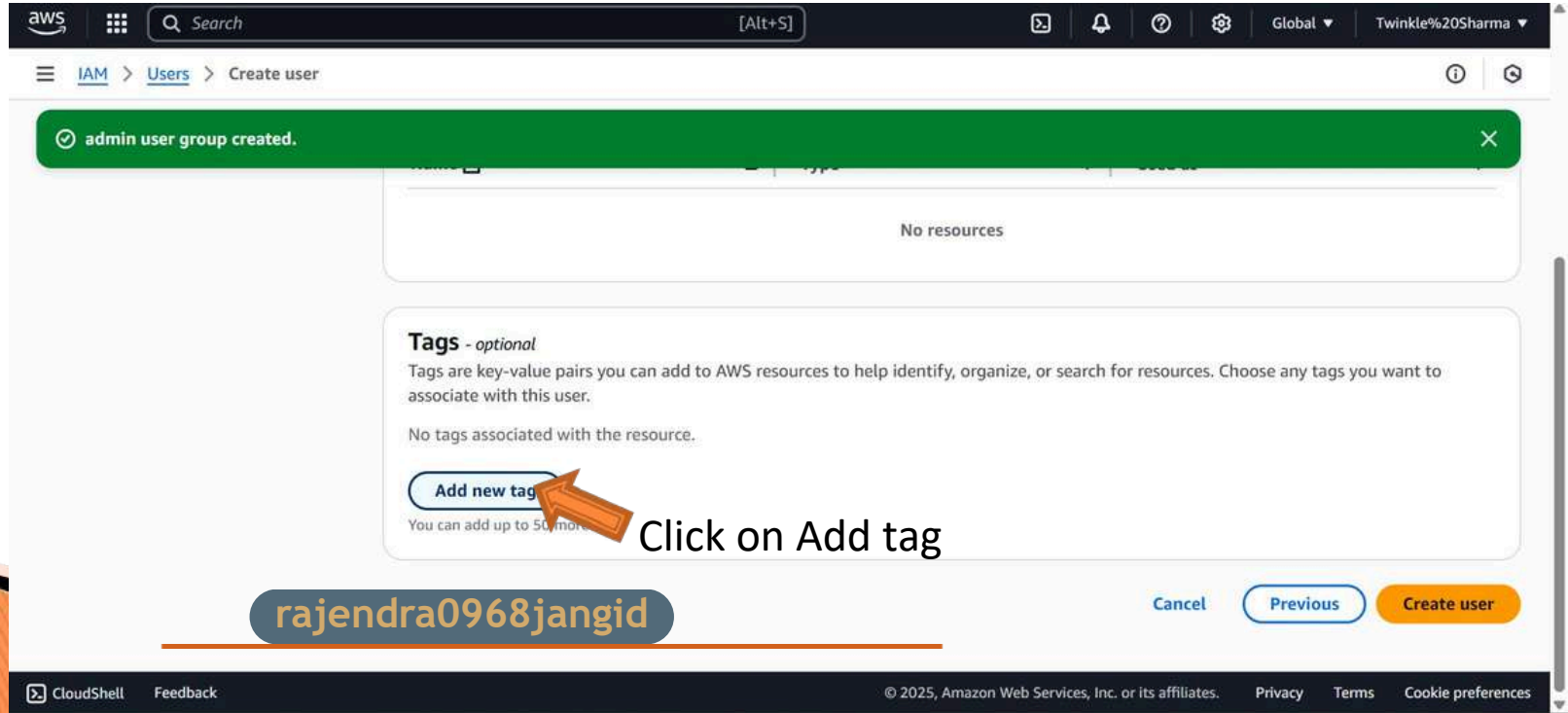
Click on create user



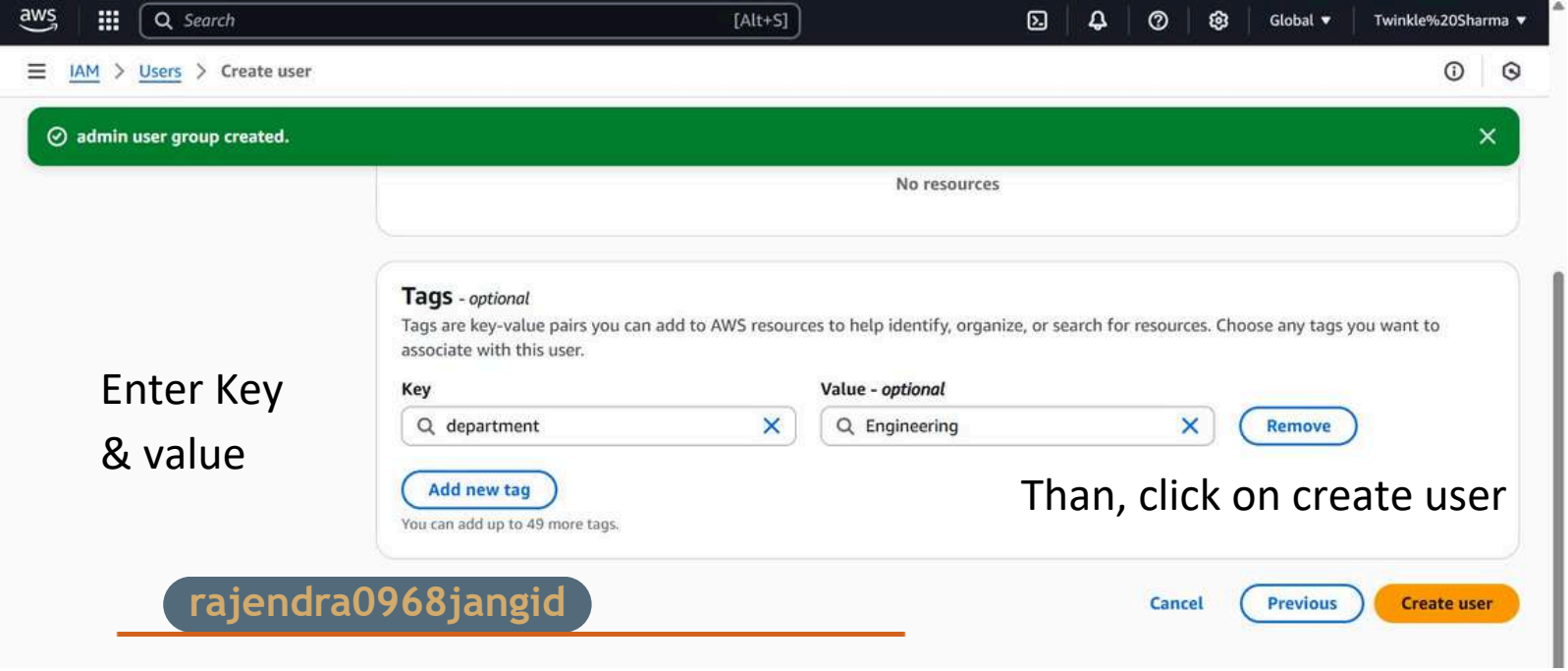
Select Group

Click on Next





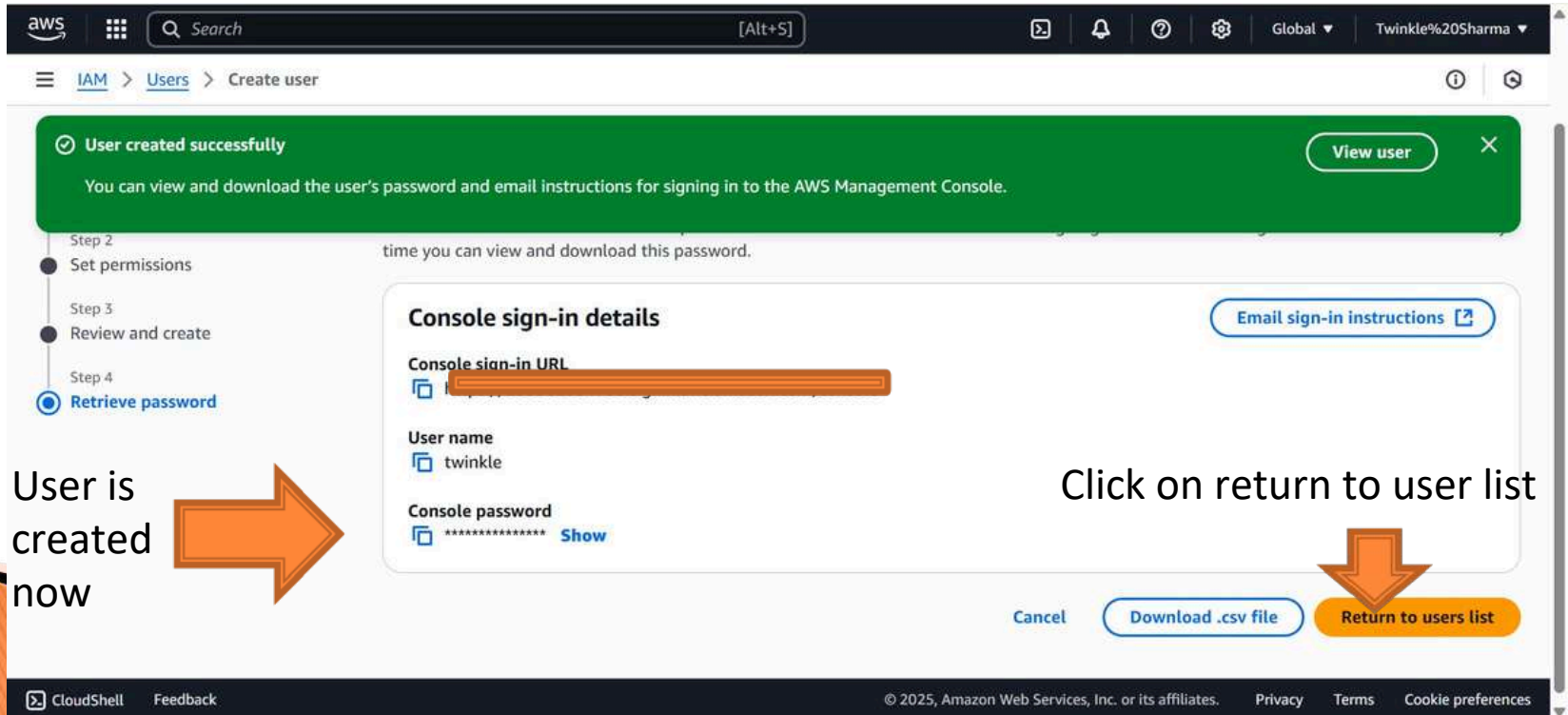
rajendra0968jangid



Enter Key & value

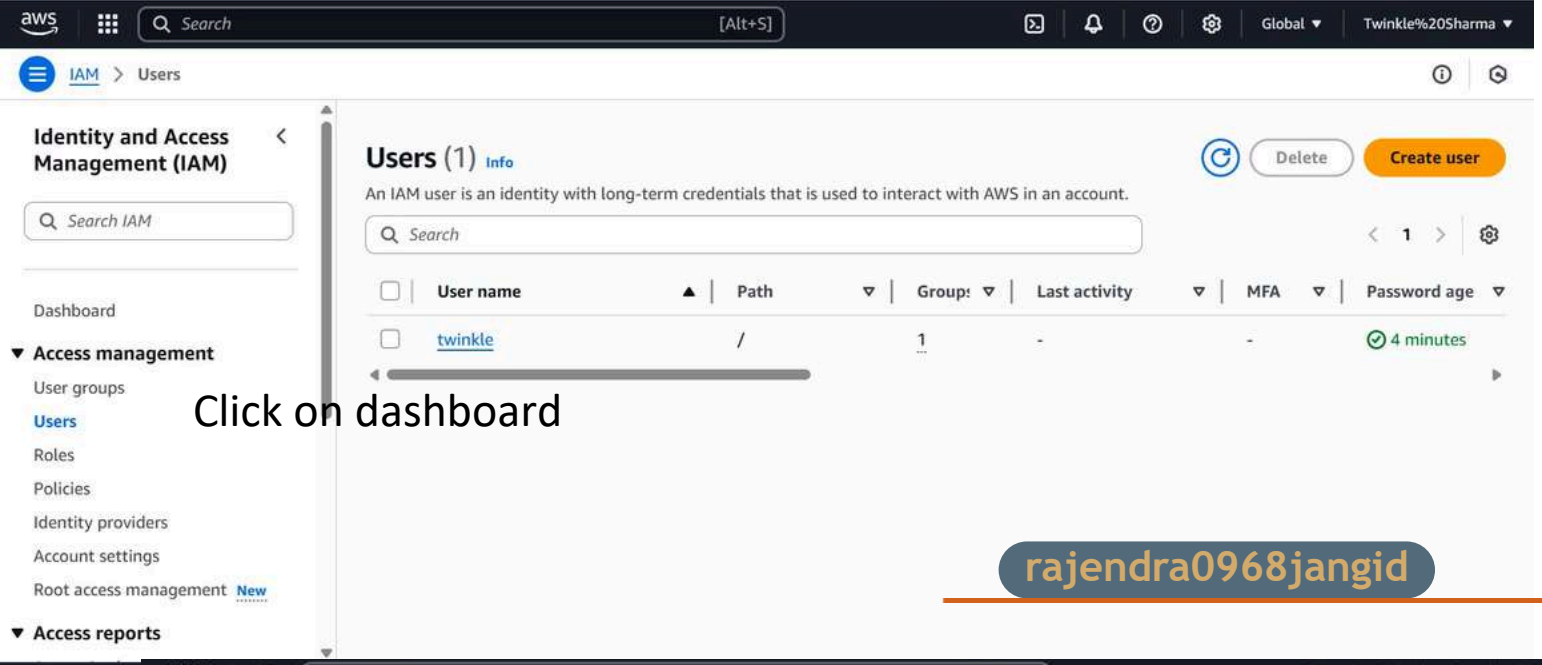
Than, click on create user

rajendra0968jangid



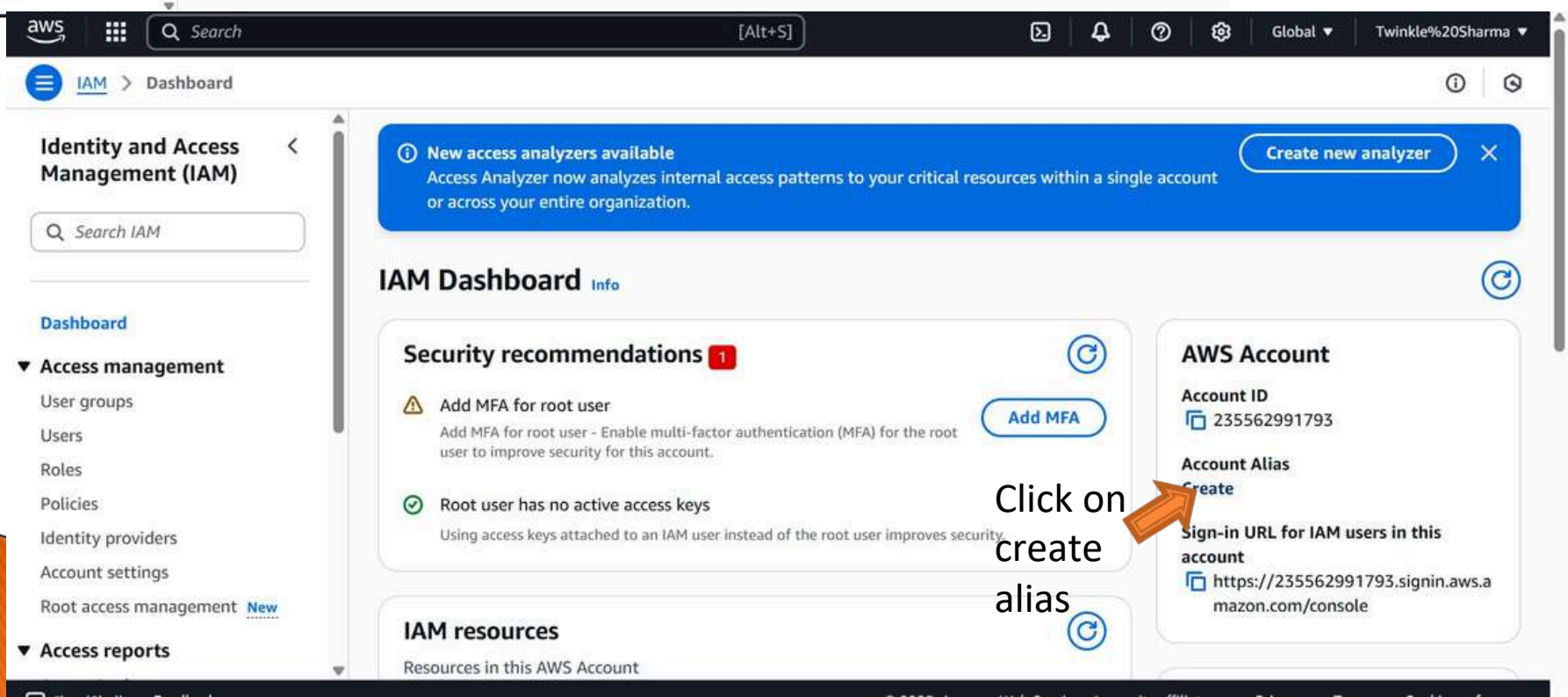
User is created now

Click on return to user list

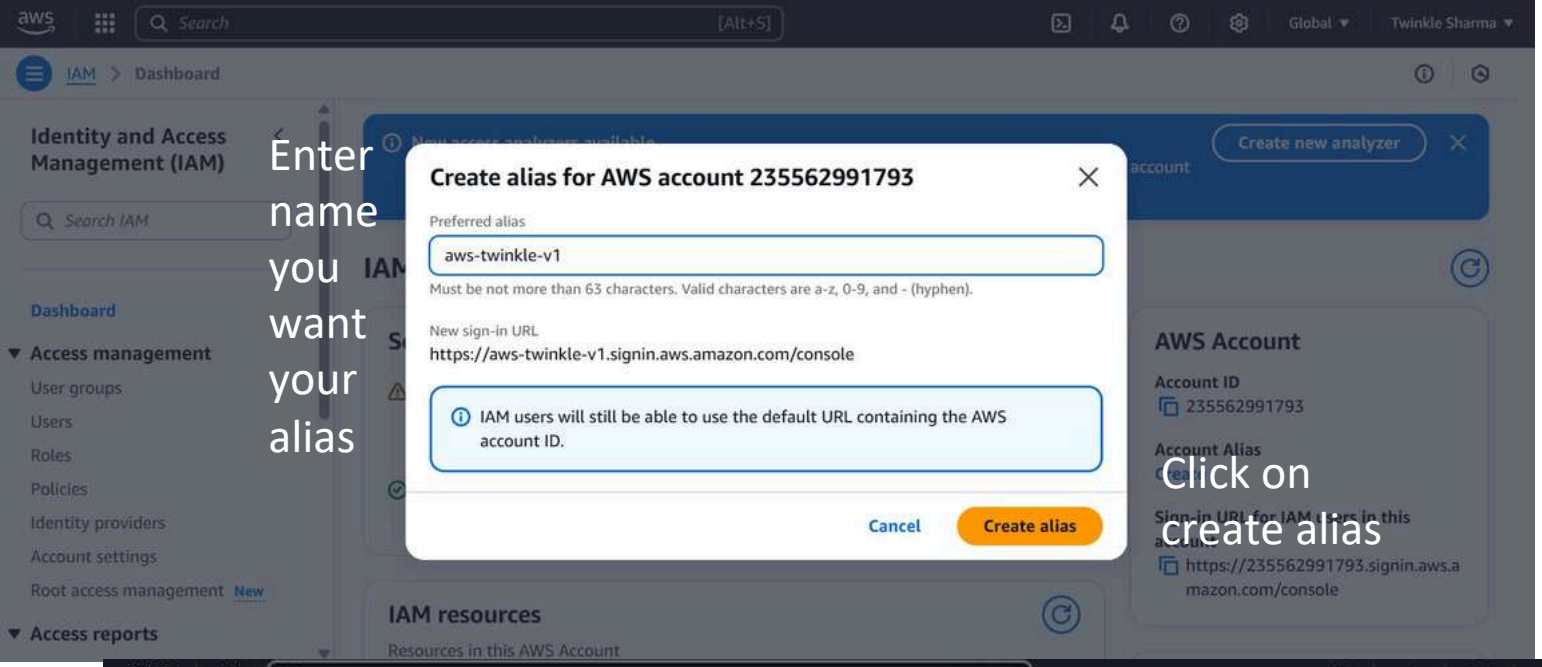


Click on dashboard

rajendra0968jangid



Click on create alias

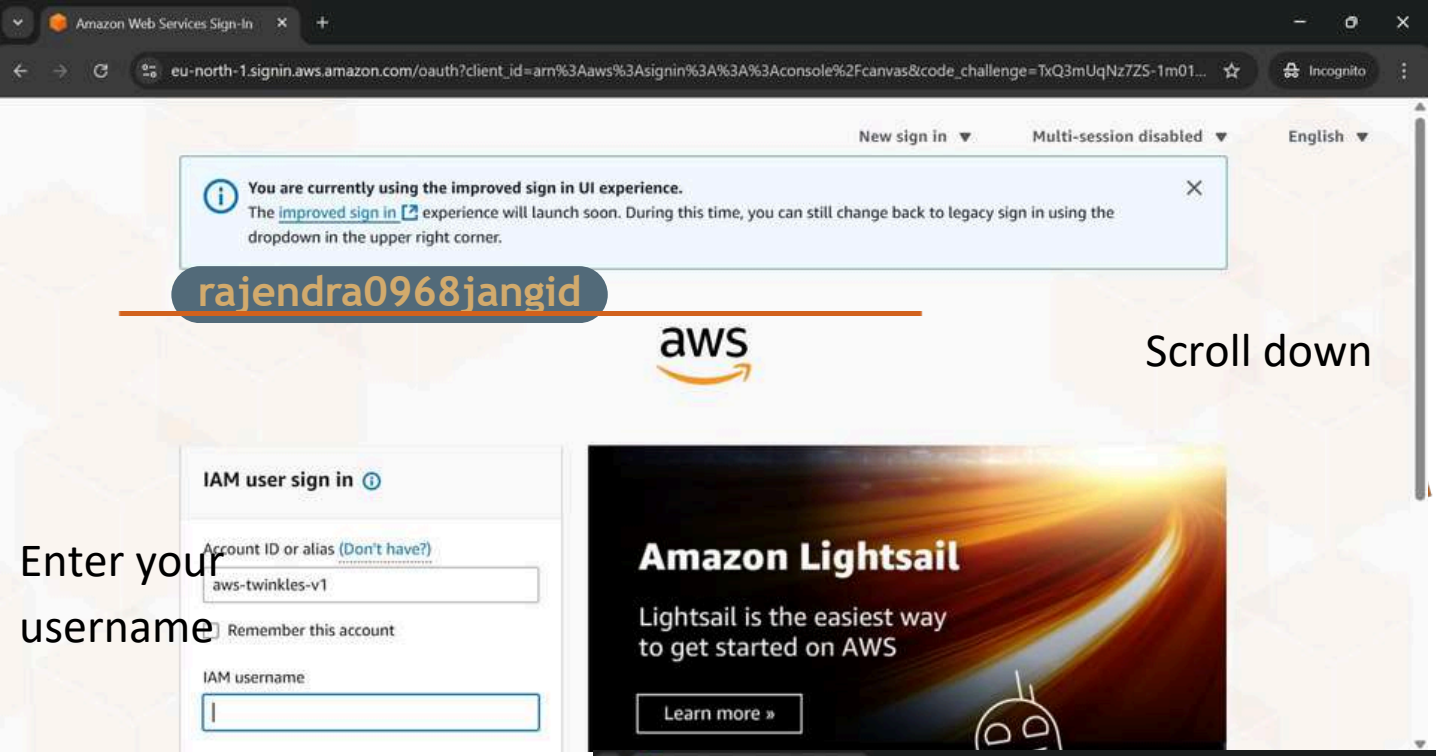


Alias aws-twinkles-v1 created for this account.

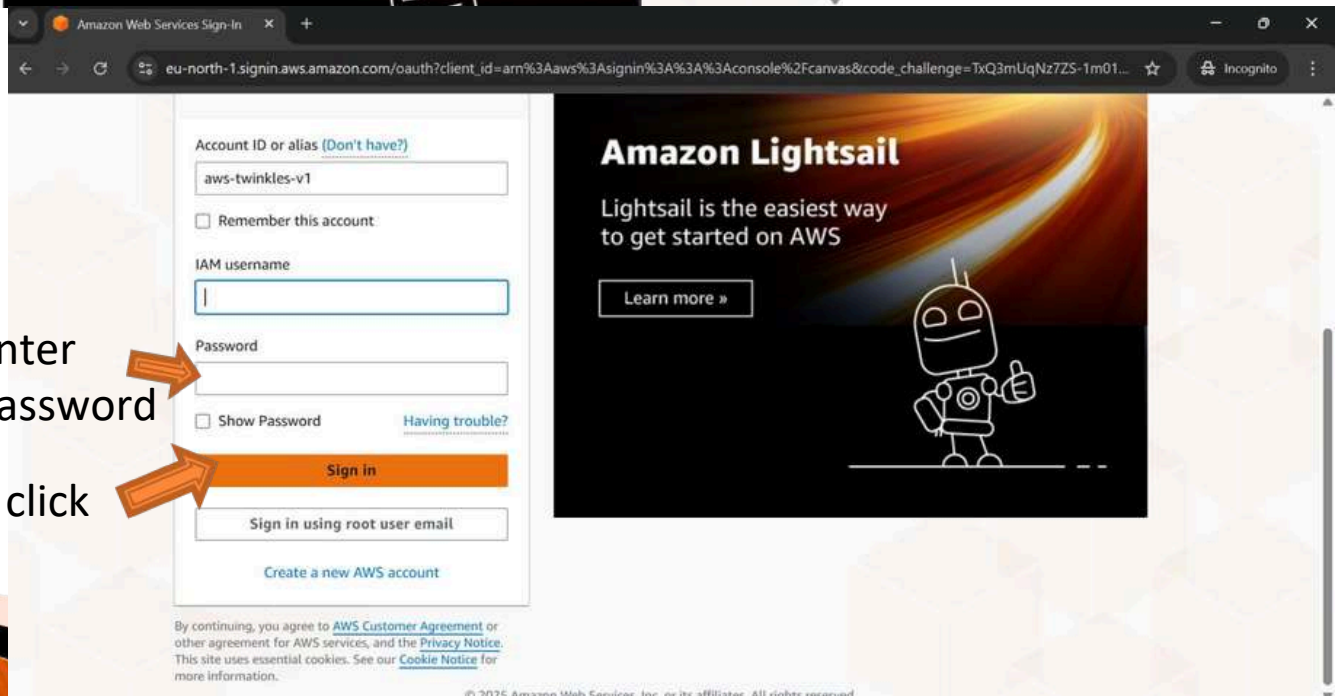
IAM Dashboard Info

Our account alias is created

Copy this URL & paste it in incognite browser for login user

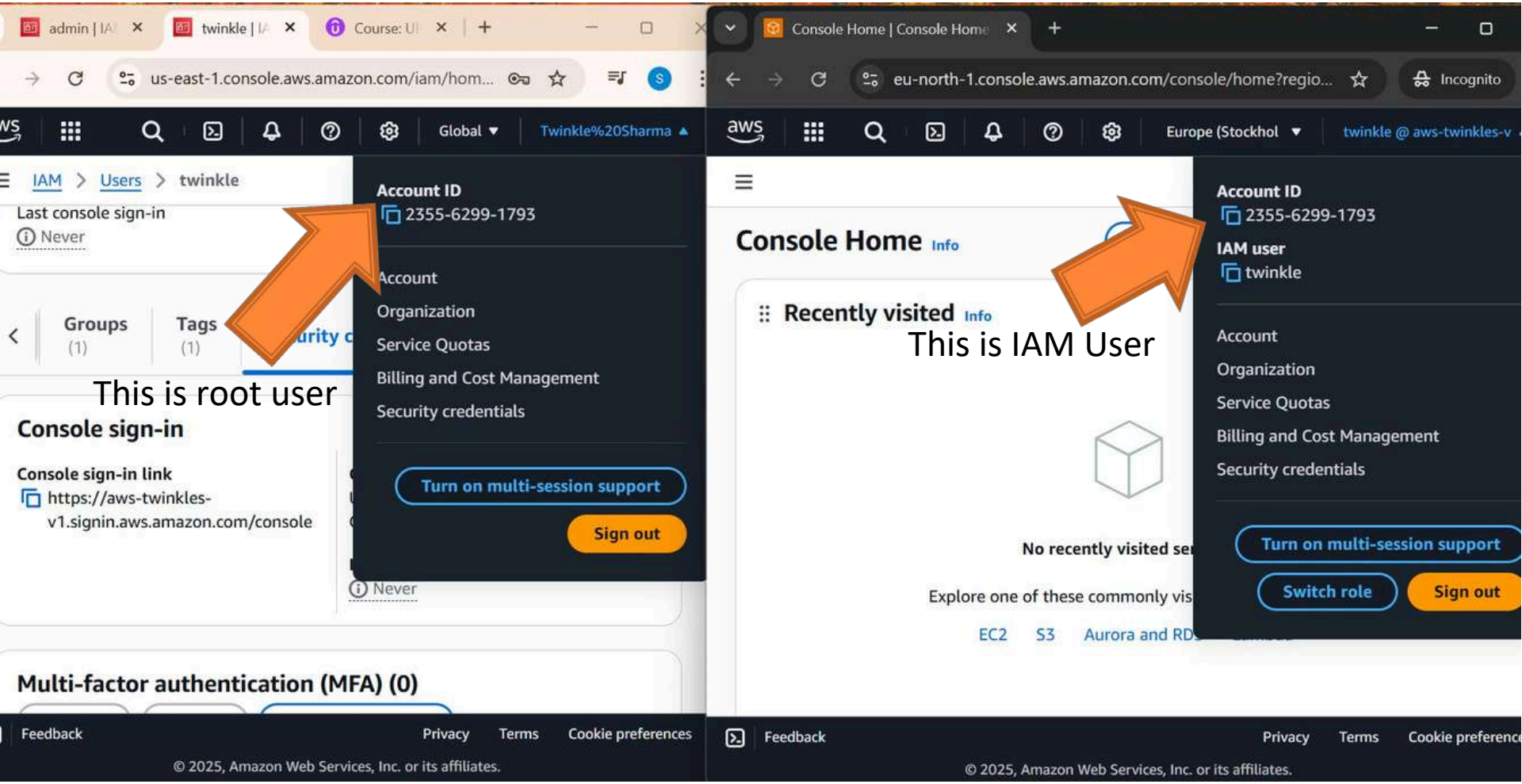


Enter your username



Enter Password

After that click on sign-in


admin | IA
twinkle | IA
Course: UI
us-east-1.console.aws.amazon.com/iam/hom...
Global
Twinkle%20Sharma
IAM > Users > twinkle
Last console sign-in
Never
Groups (1)
Tags (1)
Account ID
2355-6299-1793
Account
Organization
Service Quotas
Billing and Cost Management
Security credentials
Turn on multi-session support
Sign out
This is root user
Console sign-in
Console sign-in link
https://aws-twinkles-v1.signin.aws.amazon.com/console
Never
Multi-factor authentication (MFA) (0)
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.
Console Home | Console Home
eu-north-1.console.aws.amazon.com/console/home?regio...
Incognito
Europe (Stockhol
twinkle @ aws-twinkles-v
Console Home Info
Recently visited Info
No recently visited ser
Explore one of these commonly vis
EC2
S3
Aurora and RD
Account ID
2355-6299-1793
IAM user
twinkle
Account
Organization
Service Quotas
Billing and Cost Management
Security credentials
Turn on multi-session support
Switch role
Sign out
This is IAM User
Feedback
Privacy
Terms
Cookie preference
© 2025, Amazon Web Services, Inc. or its affiliates.

IAM Policy

An IAM policy is a set of rules written in JSON format that determines whether a request is allowed or denied. It controls access to AWS services and resources.

Types of IAM Policies

Type	Description	Example
Identity-based policies	Attached to **users, groups, or roles** to grant permissions.	"Allow EC2 start for developers"
Resource-based policies	Attached directly to **resources** (like S3 buckets or SNS topics).	"Allow another account to access my bucket"
Permissions boundaries	Set **limits** on the maximum permissions an identity-based policy can grant.	"User can't delete EC2 even if a policy says yes"
Organizations SCPs	Service Control Policies applied at AWS Organization level.	"Deny root account from disabling CloudTrail"
Session policies	Passed when assuming a role (temporary permissions).	"Allow temporary upload to S3 during session"

Structure of an IAM Policy

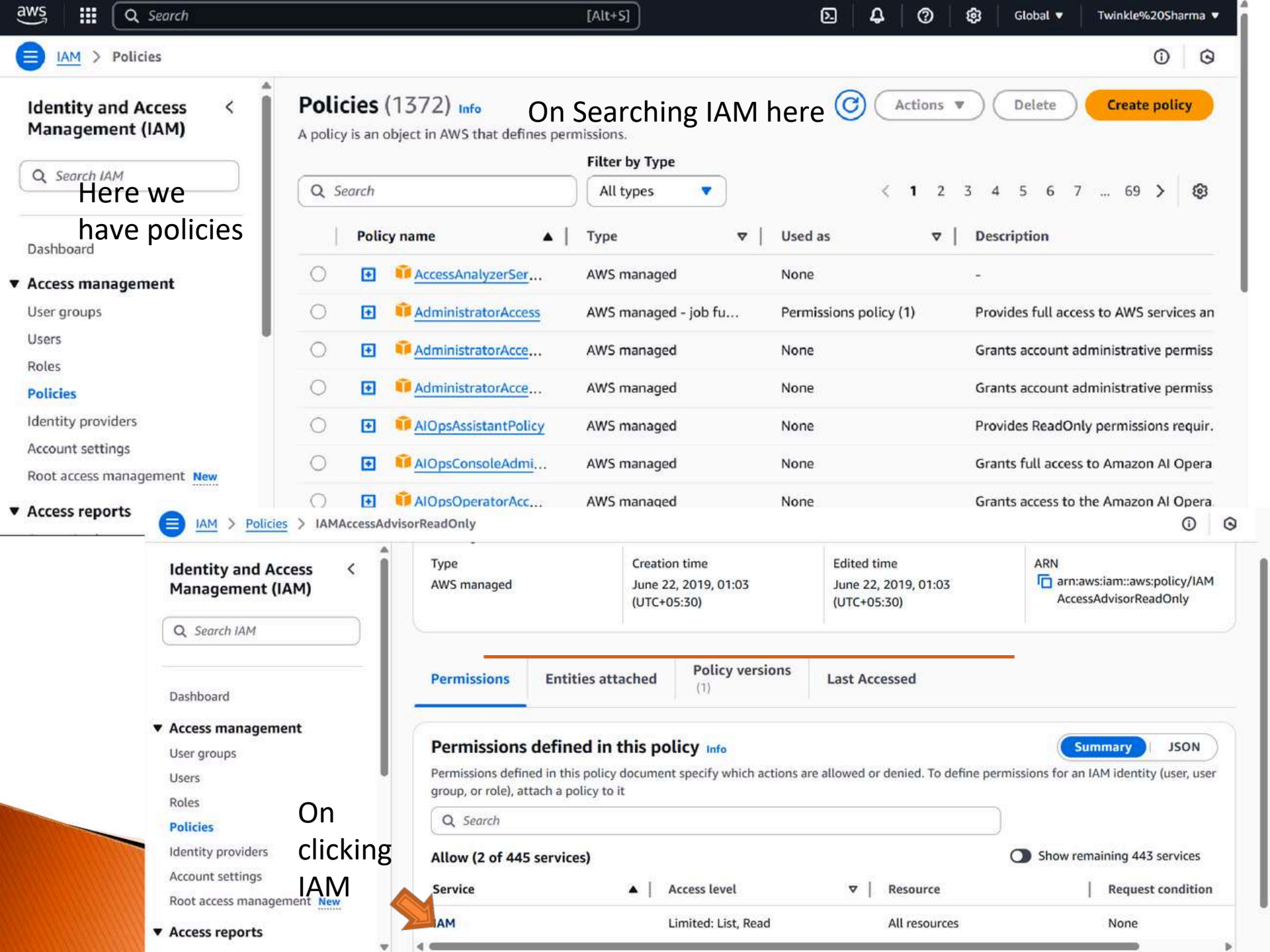
Abasic IAM policy contains the following key elements:

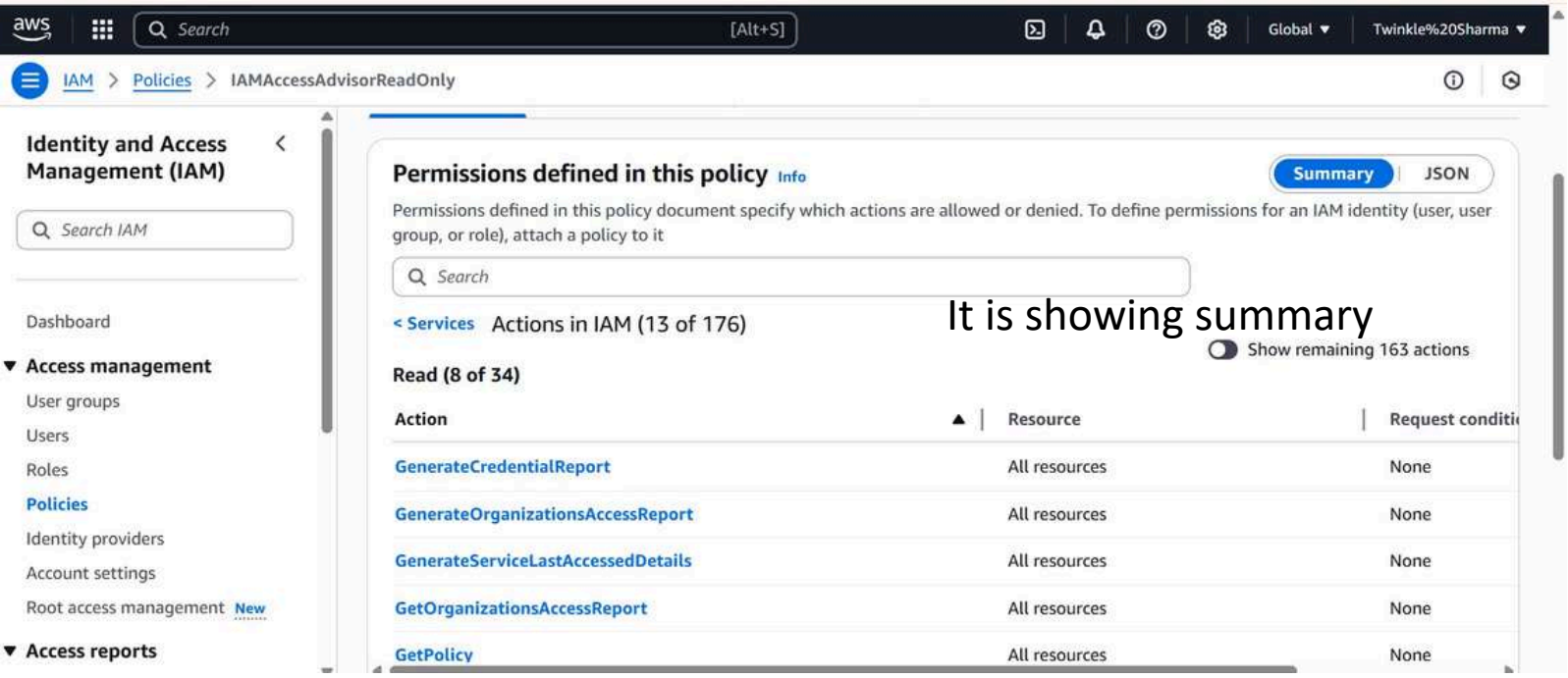
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-bucket/*"
    }
  ]
}
```

Breakdown of the Policy Structure:

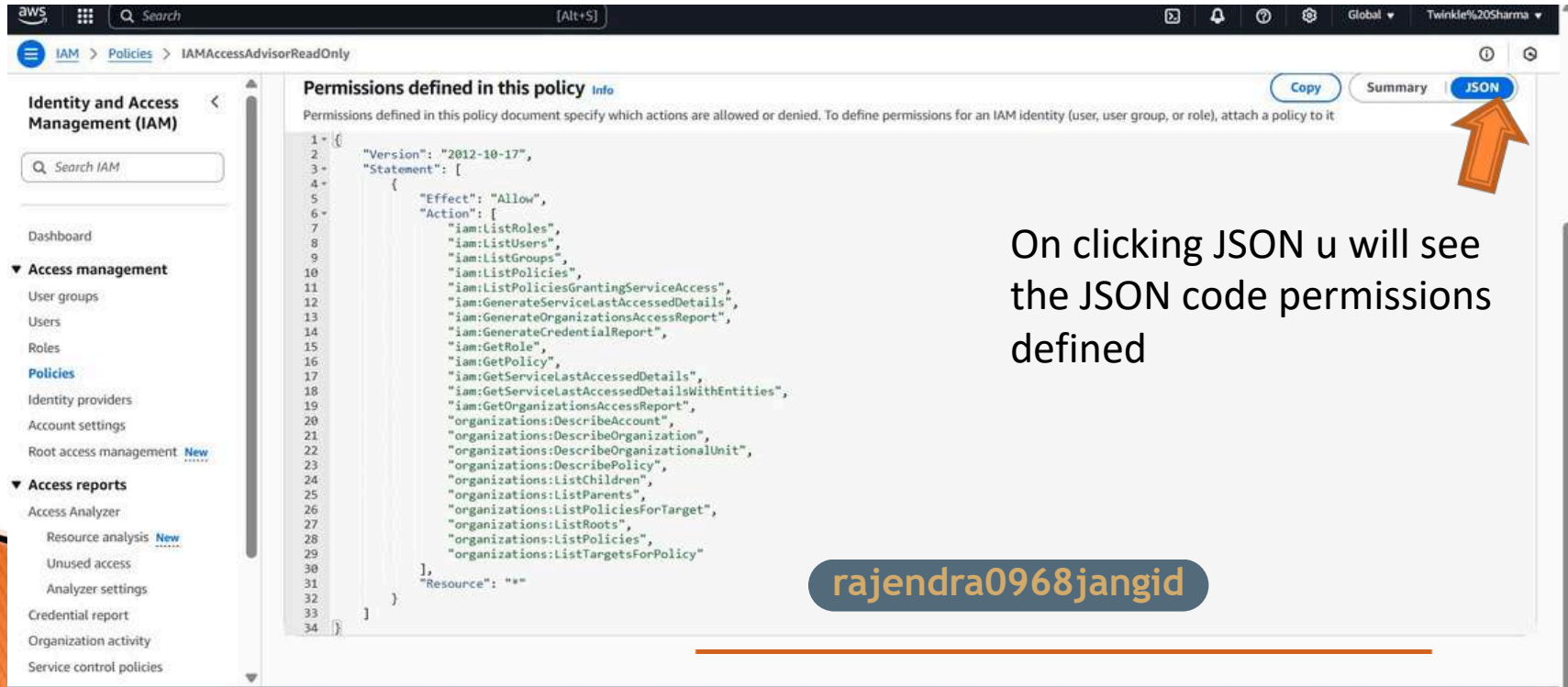
```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-bucket/*"
    }
  ]
}
```

Element	Description
`"Version"`	Specifies the policy language version. Always use `"2012-10-17"` (latest version).
`"Statement"`	One or more individual permission blocks.
`"Effect"`	Either `"Allow"` or `"Deny"` — determines if the action is permitted or blocked.
`"Action"`	Specifies the AWS service actions (like `s3:GetObject`, `ec2:StartInstances`).
`"Resource"`	Specifies the ARN of the resource the action applies to.
`"Condition"` *(Optional)*	Adds conditions to when the policy is in effect (e.g., based on IP address, time, MFA).


aws
Search
[Alt+S]
Global
Twinkle%20Sharma
IAM > Policies
Identity and Access Management (IAM)
Search IAM
Here we have policies
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Policies (1372) Info
A policy is an object in AWS that defines permissions.
On Searching IAM here
Actions
Delete
Create policy
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 69
Policy name
Type
Used as
Description
AccessAnalyzerSer...
AWS managed
None
AdministratorAccess
AWS managed - job fu...
Permissions policy (1)
Provides full access to AWS services an
AdministratorAcce...
AWS managed
None
Grants account administrative permiss
AdministratorAcce...
AWS managed
None
Grants account administrative permiss
AIOpsAssistantPolicy
AWS managed
None
Provides ReadOnly permissions requir.
AIOpsConsoleAdmi...
AWS managed
None
Grants full access to Amazon AI Opera
AIOpsOperatorAcc...
AWS managed
None
Grants access to the Amazon AI Opera
IAM > Policies > IAMAccessAdvisorReadOnly
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
On clicking IAM
Type
AWS managed
Creation time
June 22, 2019, 01:03 (UTC+05:30)
Edited time
June 22, 2019, 01:03 (UTC+05:30)
ARN
arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly
Permissions
Entities attached
Policy versions (1)
Last Accessed
Permissions defined in this policy Info
Summary
JSON
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 (2 of 445 services)
Show remaining 443 services
Service
Access level
Resource
Request condition
IAM
Limited: List, Read
All resources
None



It is showing summary

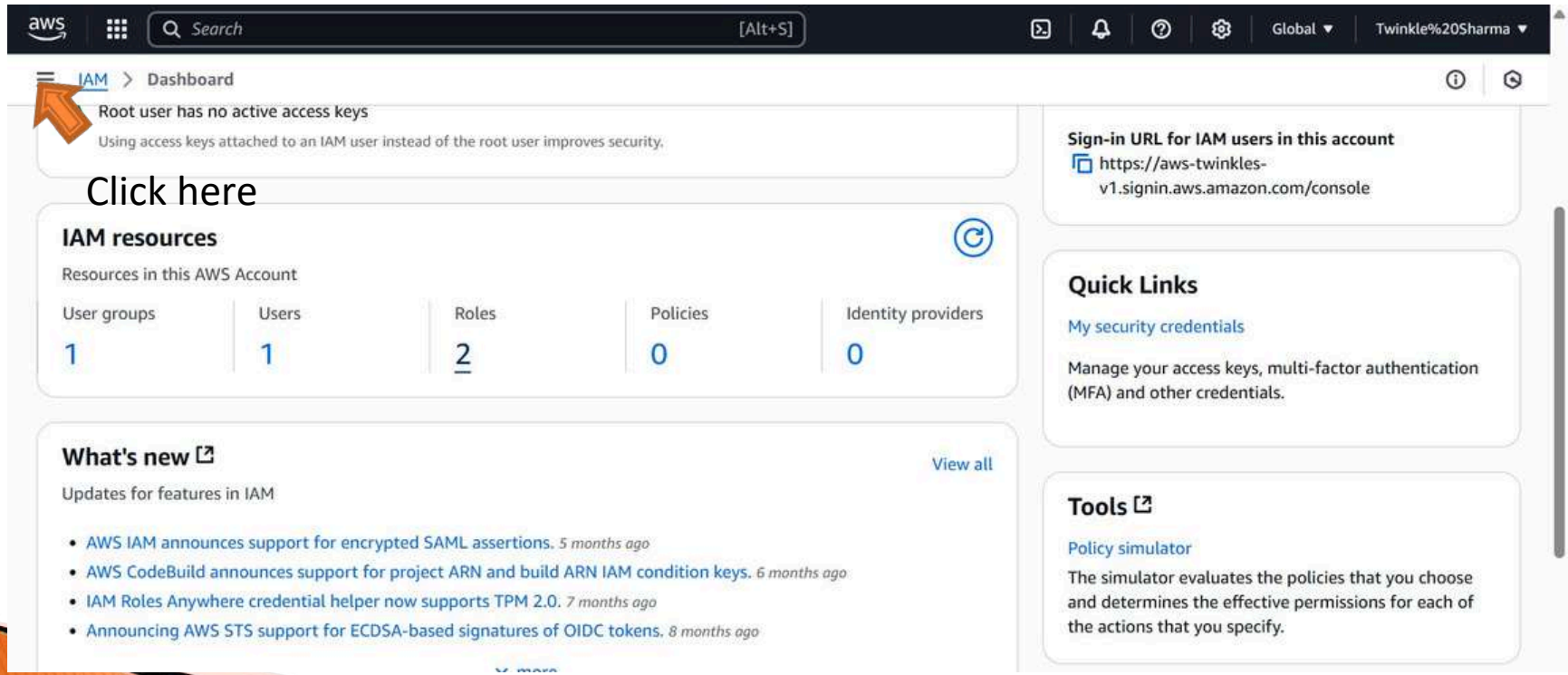


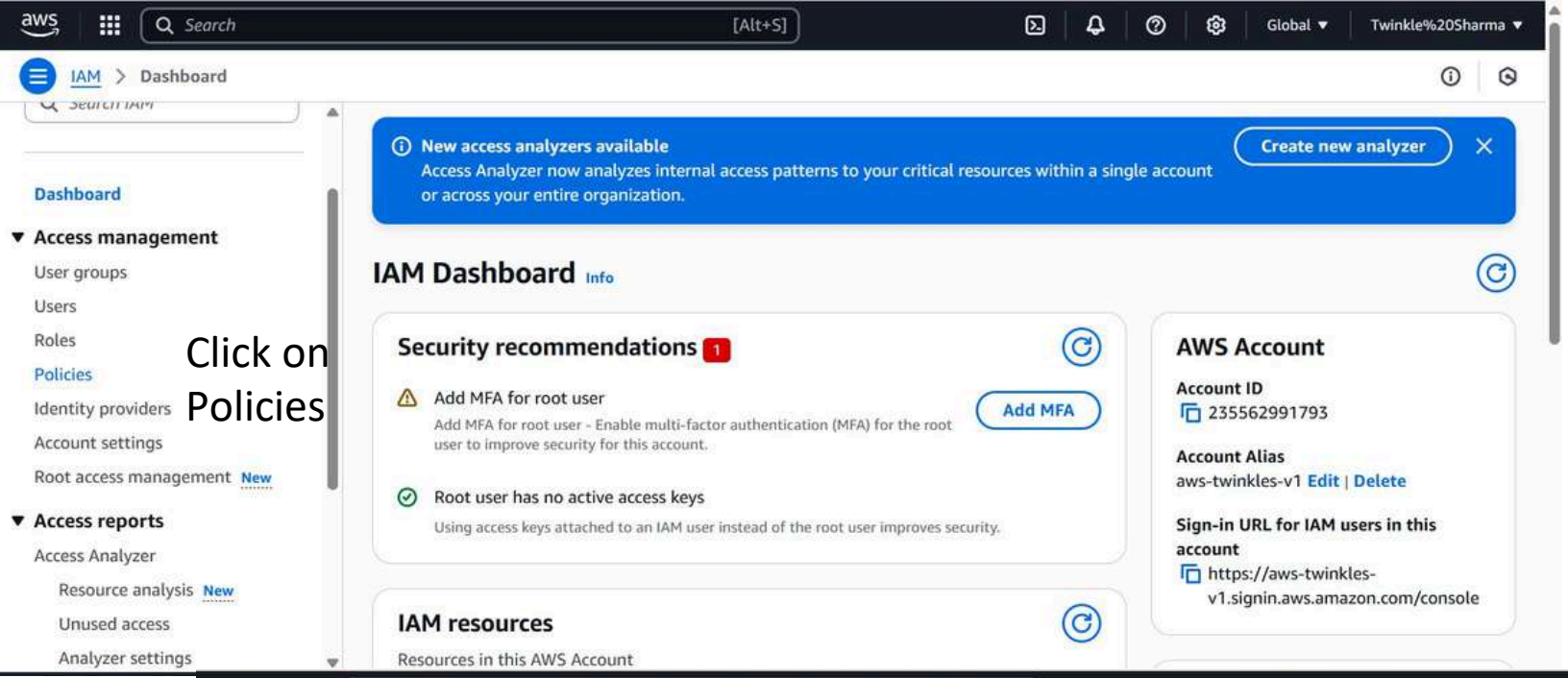
On clicking JSON u will see the JSON code permissions defined

rajendra0968jangid

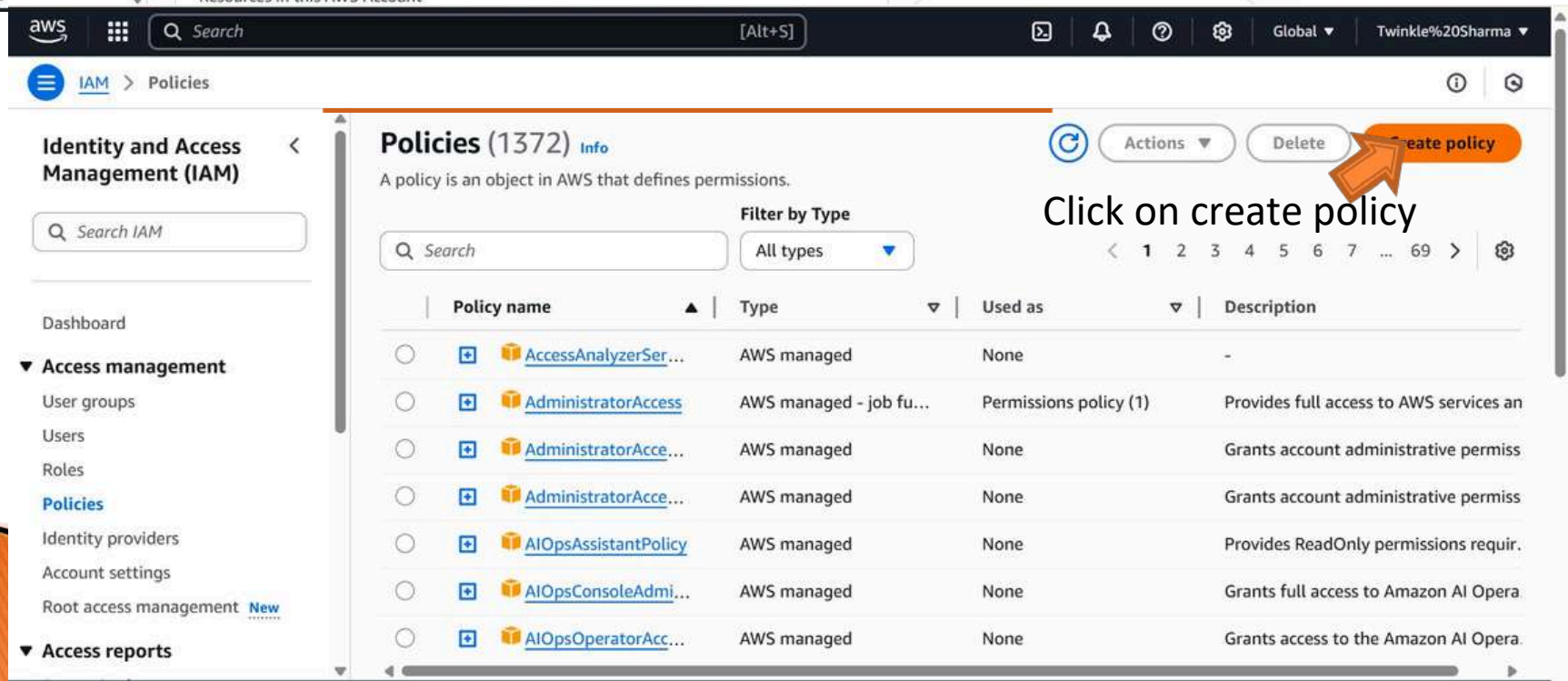
IAM Policies Hand On

- Go to portal login root user
- Go to IAM

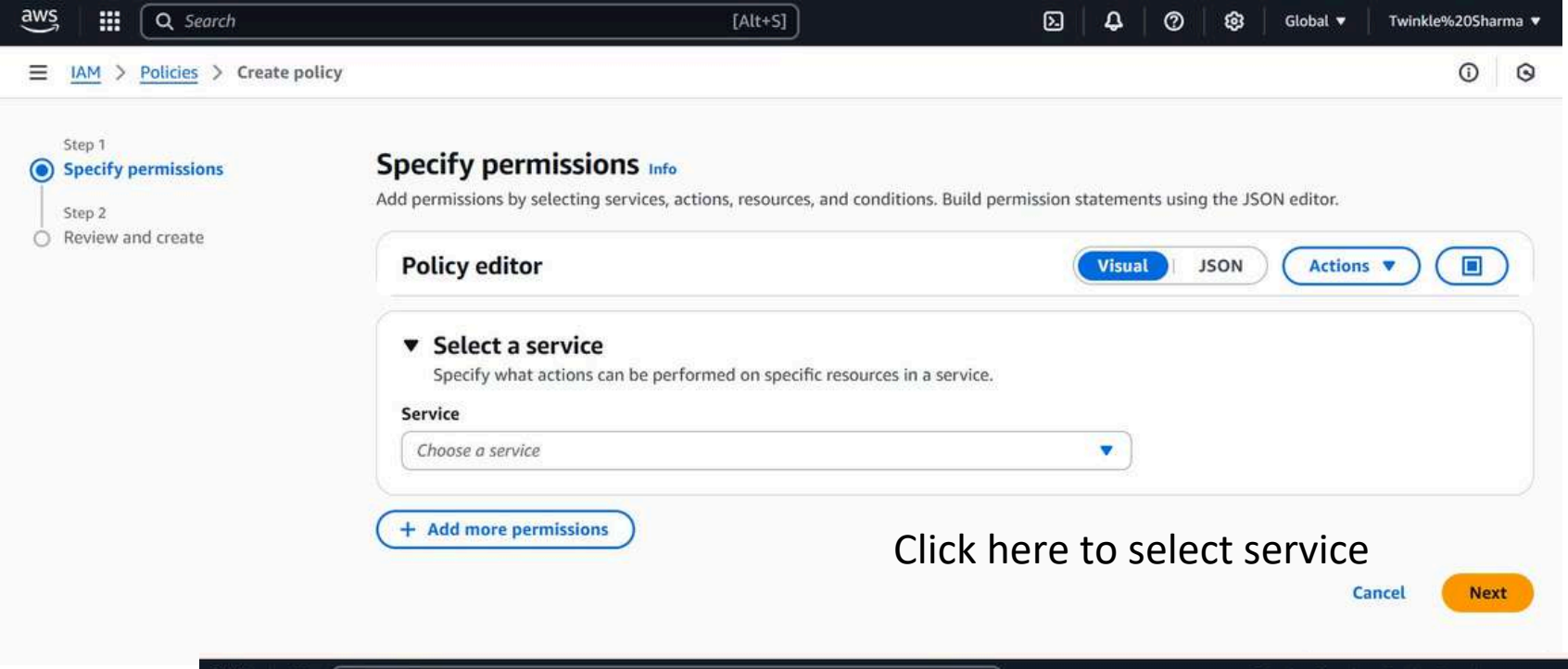


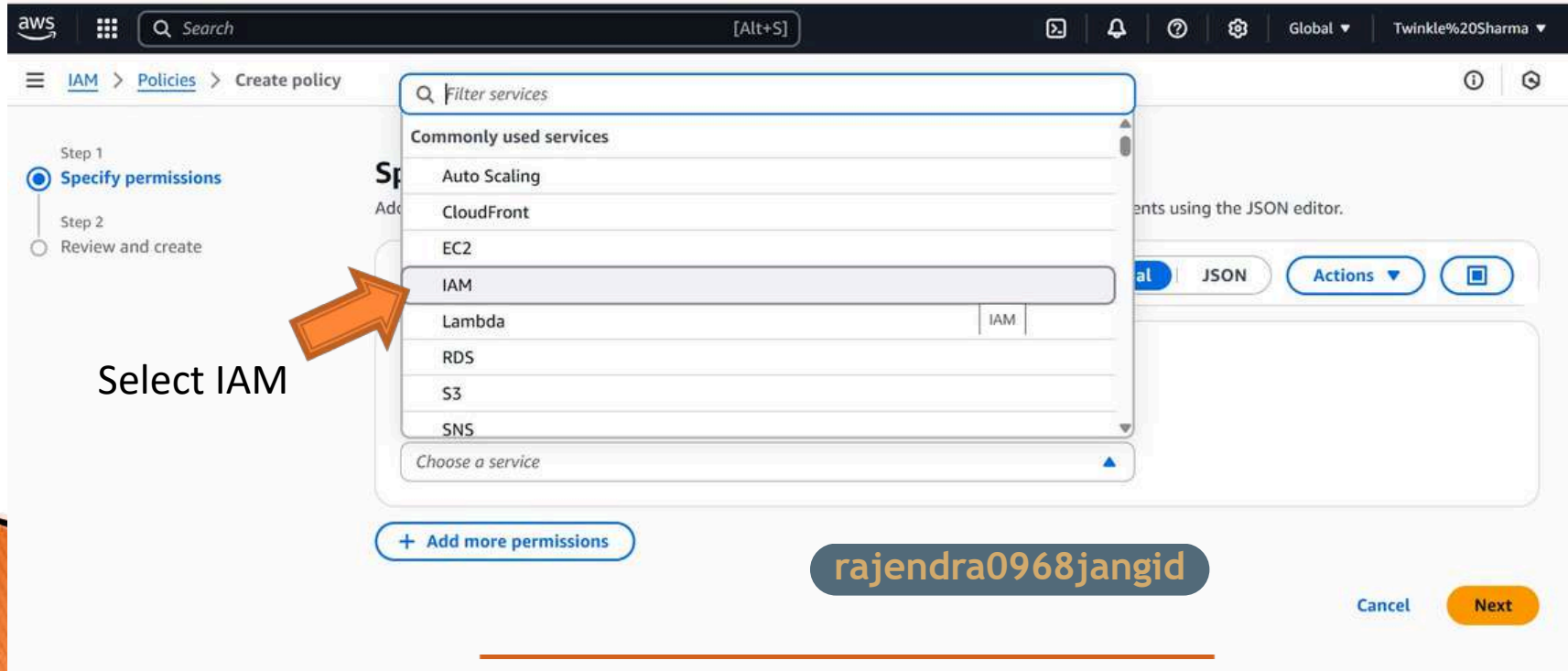


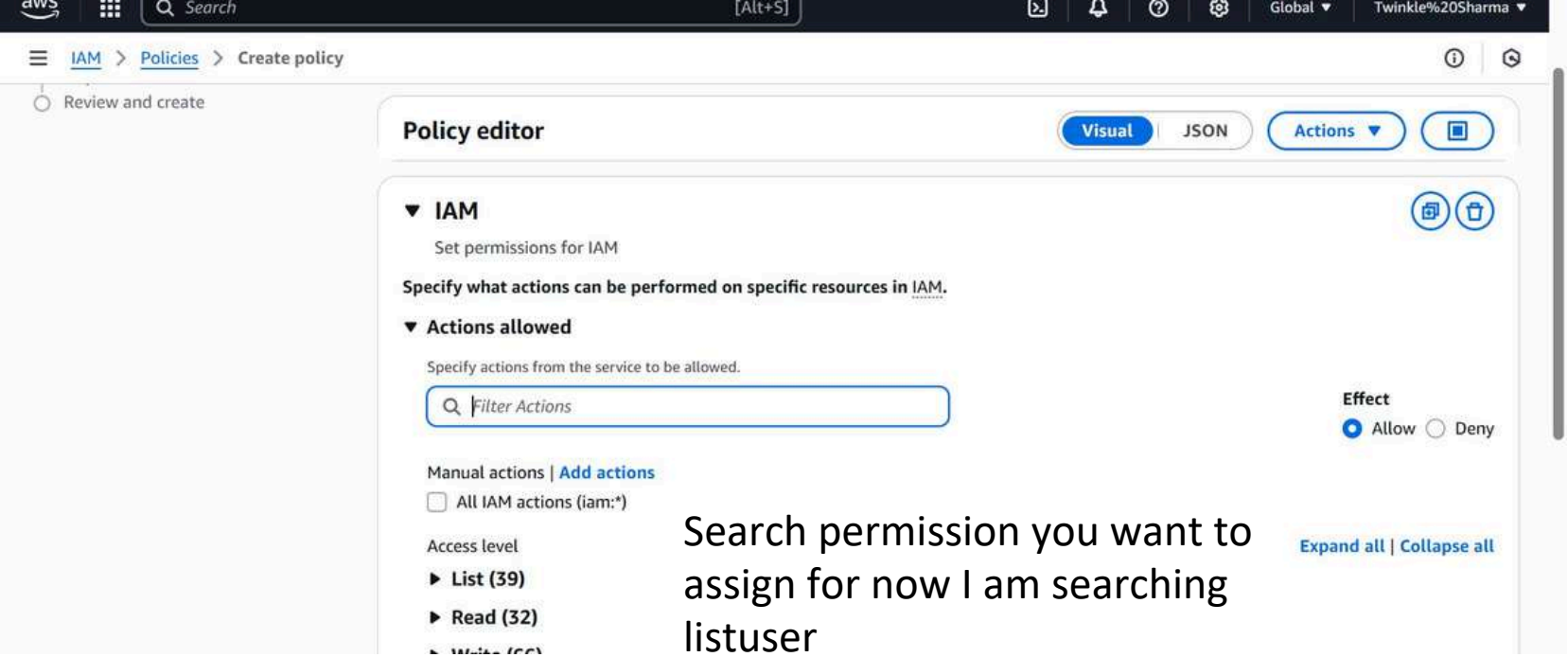
Click on Policies



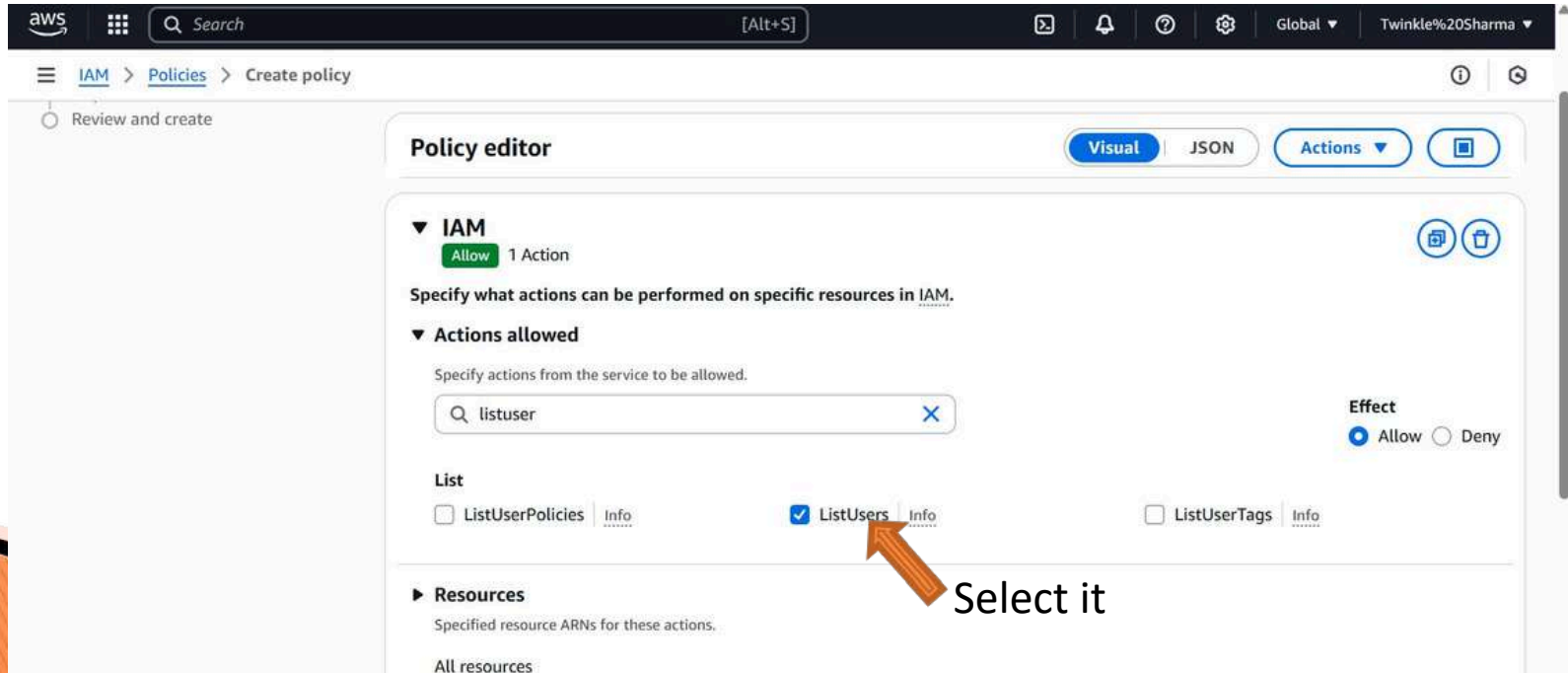
Click on create policy


aws
Search
[Alt+S]
Global
Twinkle%20Sharma
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
Visual
JSON
Actions
Select a service
Specify what actions can be performed on specific resources in a service.
Service
Choose a service
+ Add more permissions
Click here to select service
Cancel
Next

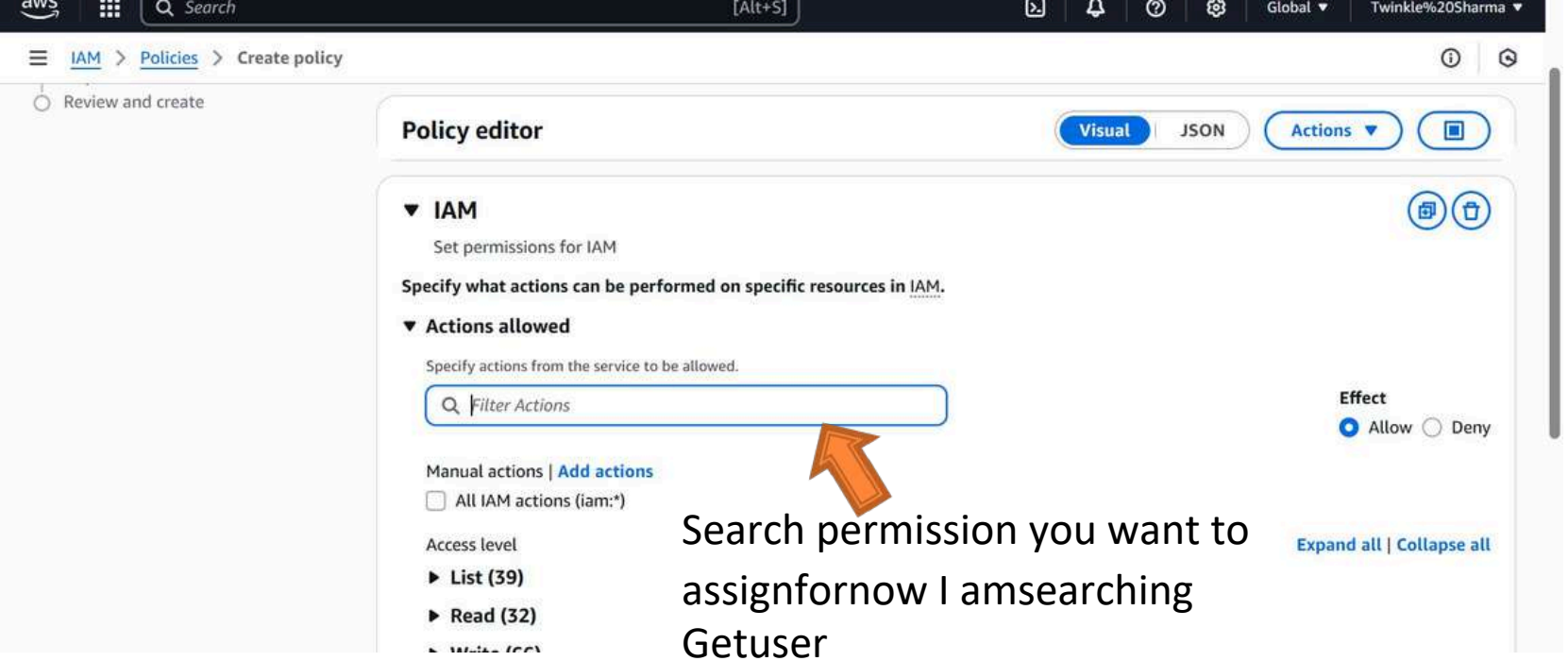

aws
Search
[Alt+S]
Global
Twinkle%20Sharma
IAM > Policies > Create policy
Filter services
Commonly used services
Auto Scaling
CloudFront
EC2
IAM
Lambda
IAM
RDS
S3
SNS
Step 1
Specify permissions
Step 2
Review and create
JSON
Actions
Choose a service
+ Add more permissions
Select IAM
rajendra0968jangid
Cancel
Next



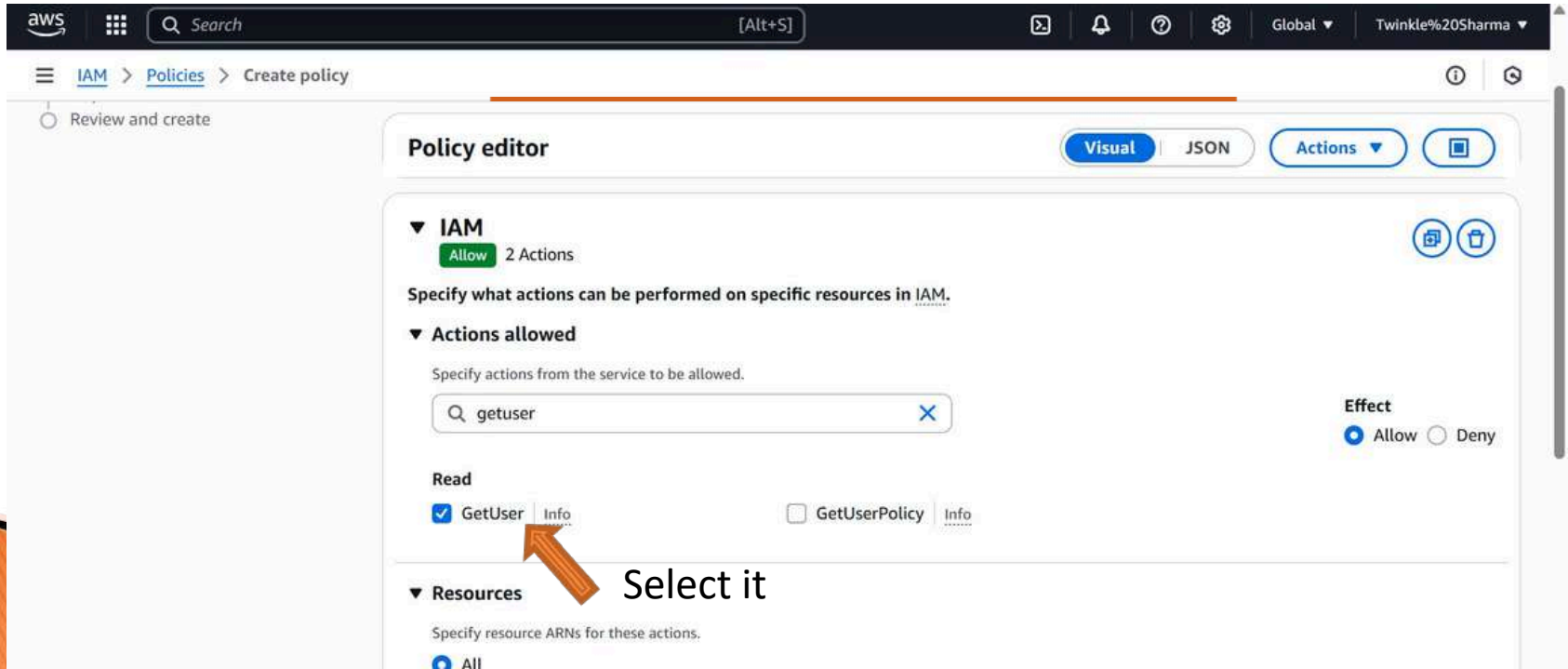
Search permission you want to assign for now I am searching listuser



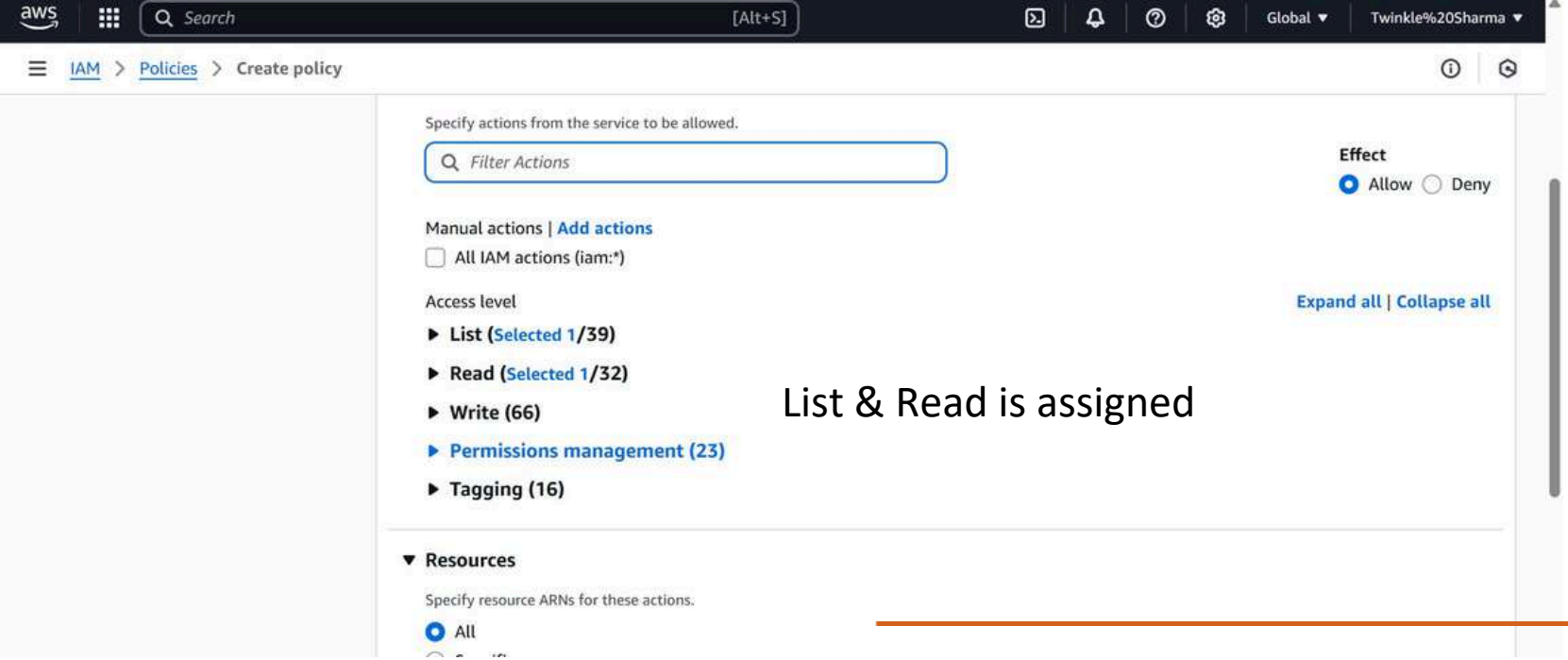
Select it



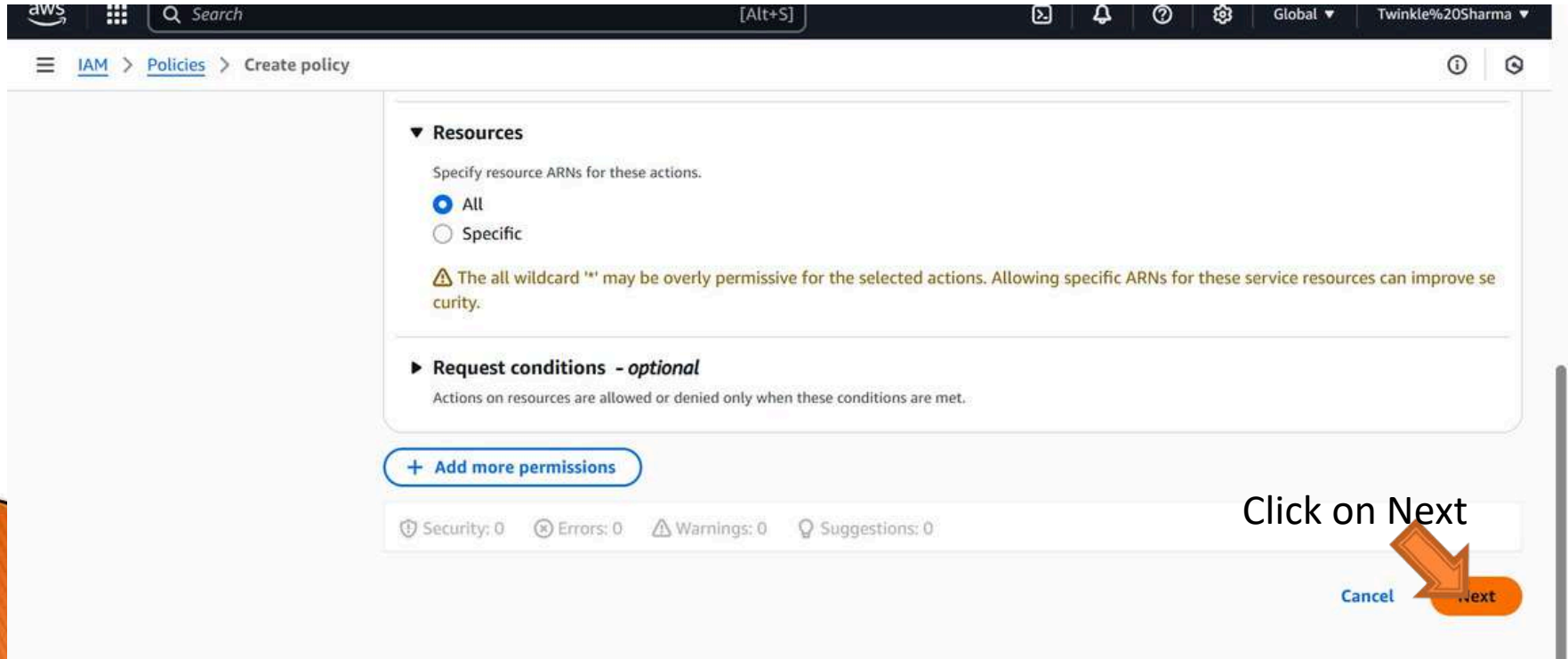
Search permission you want to assignfornow I amsearching Getuser



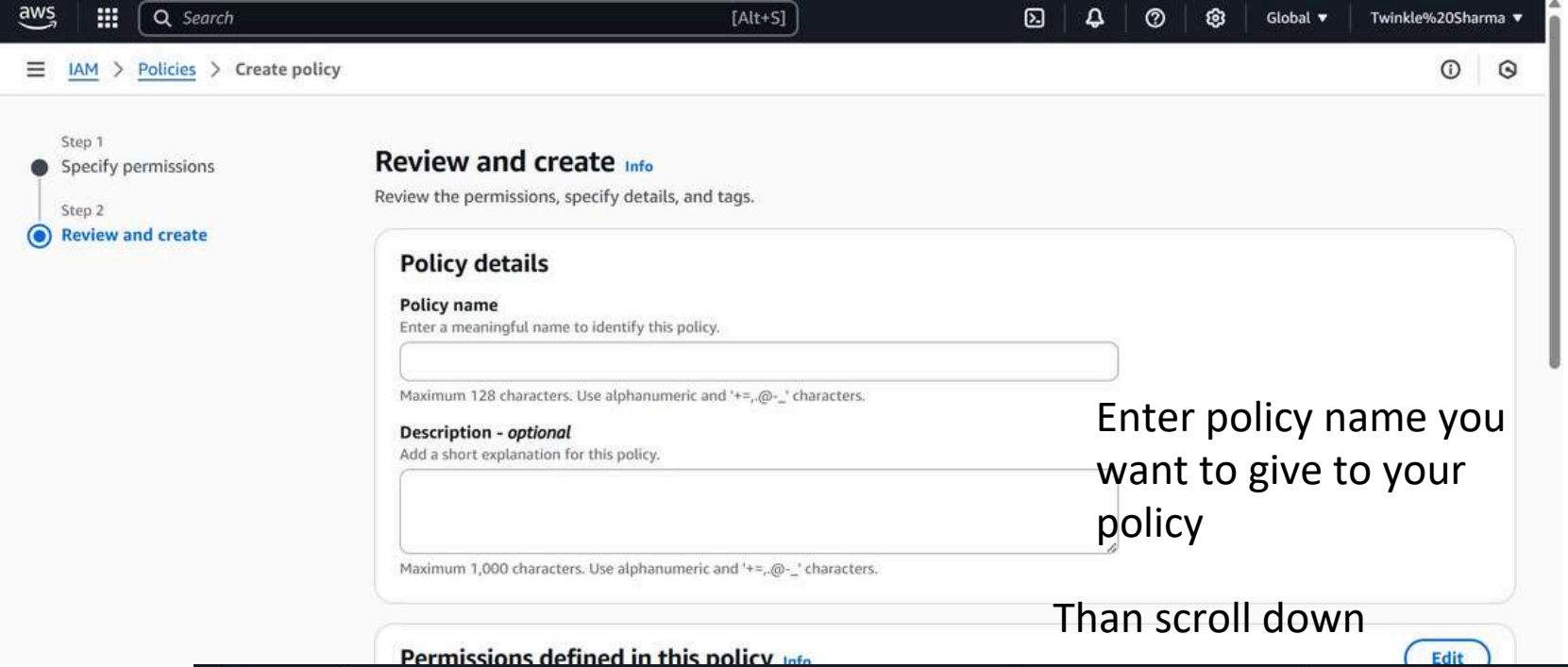
Select it



List & Read is assigned

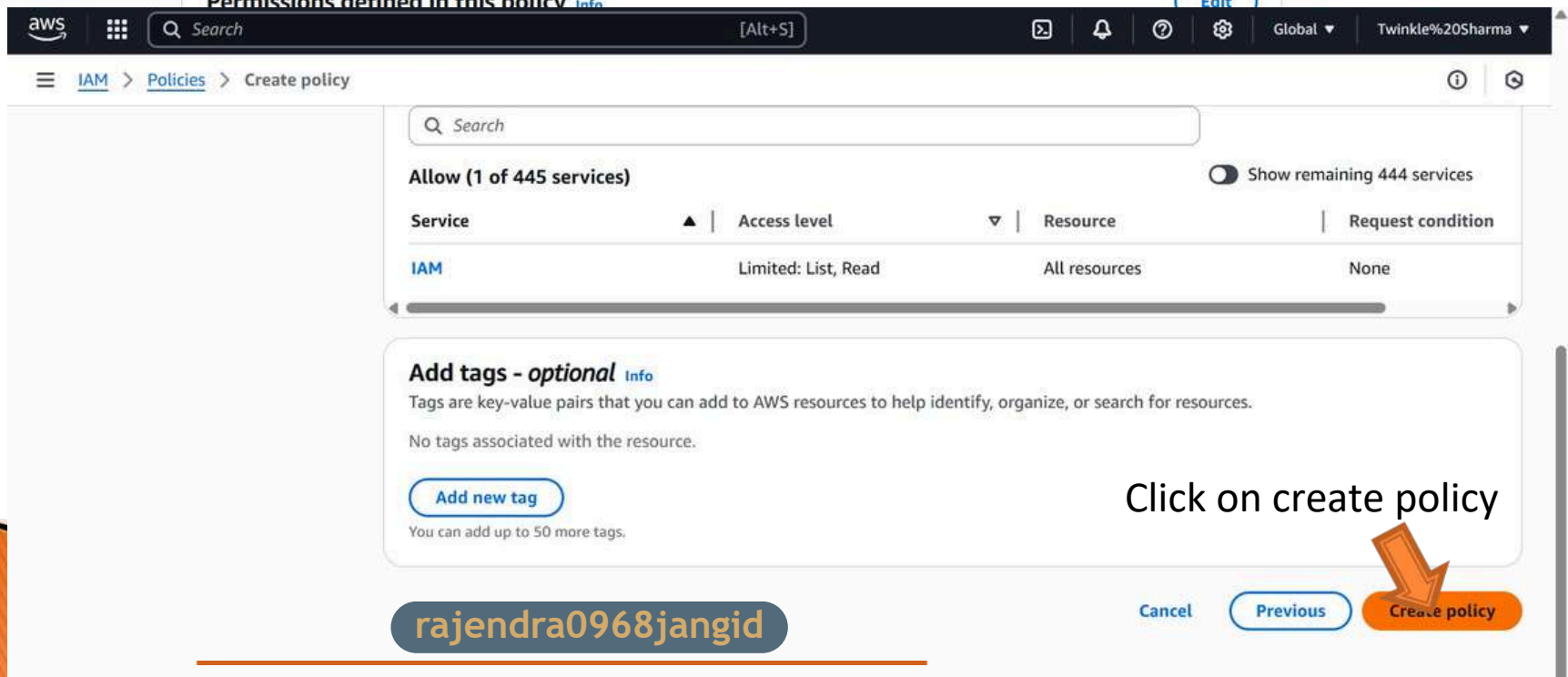


Click on Next

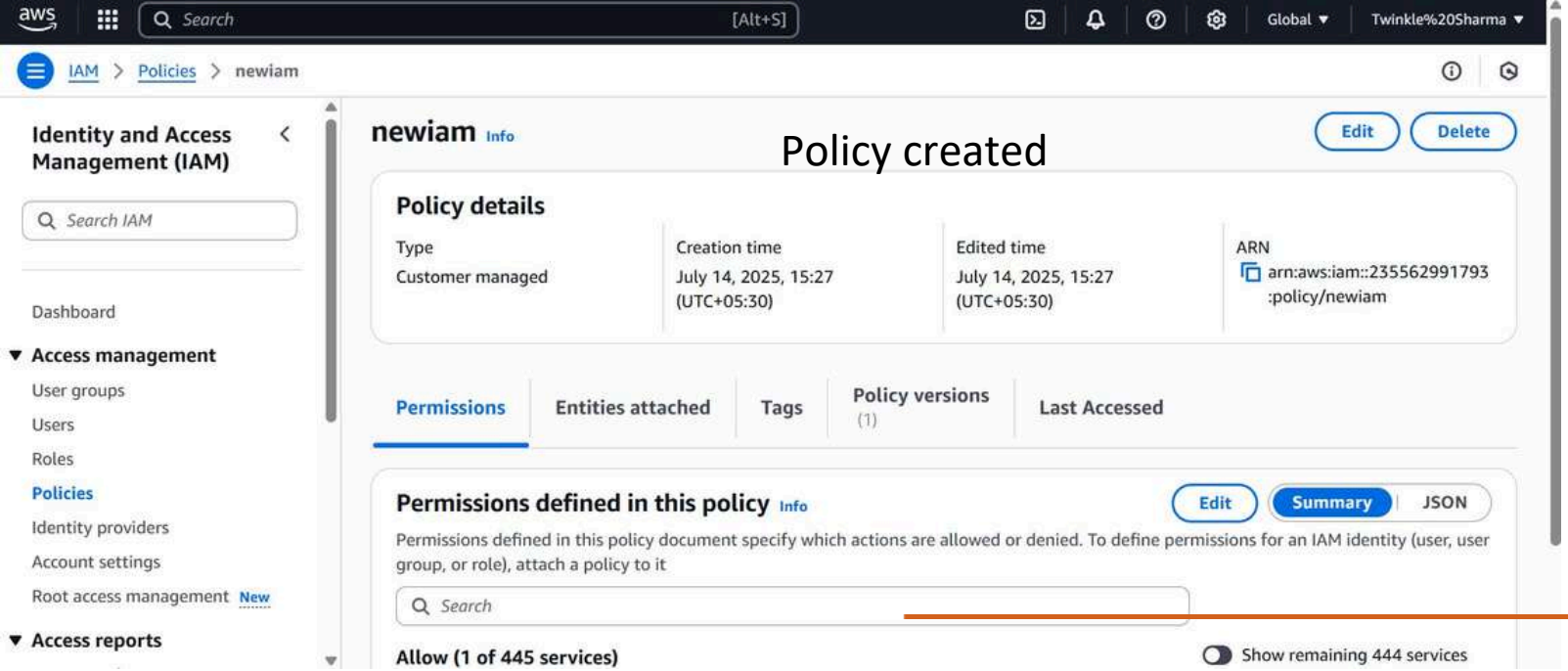


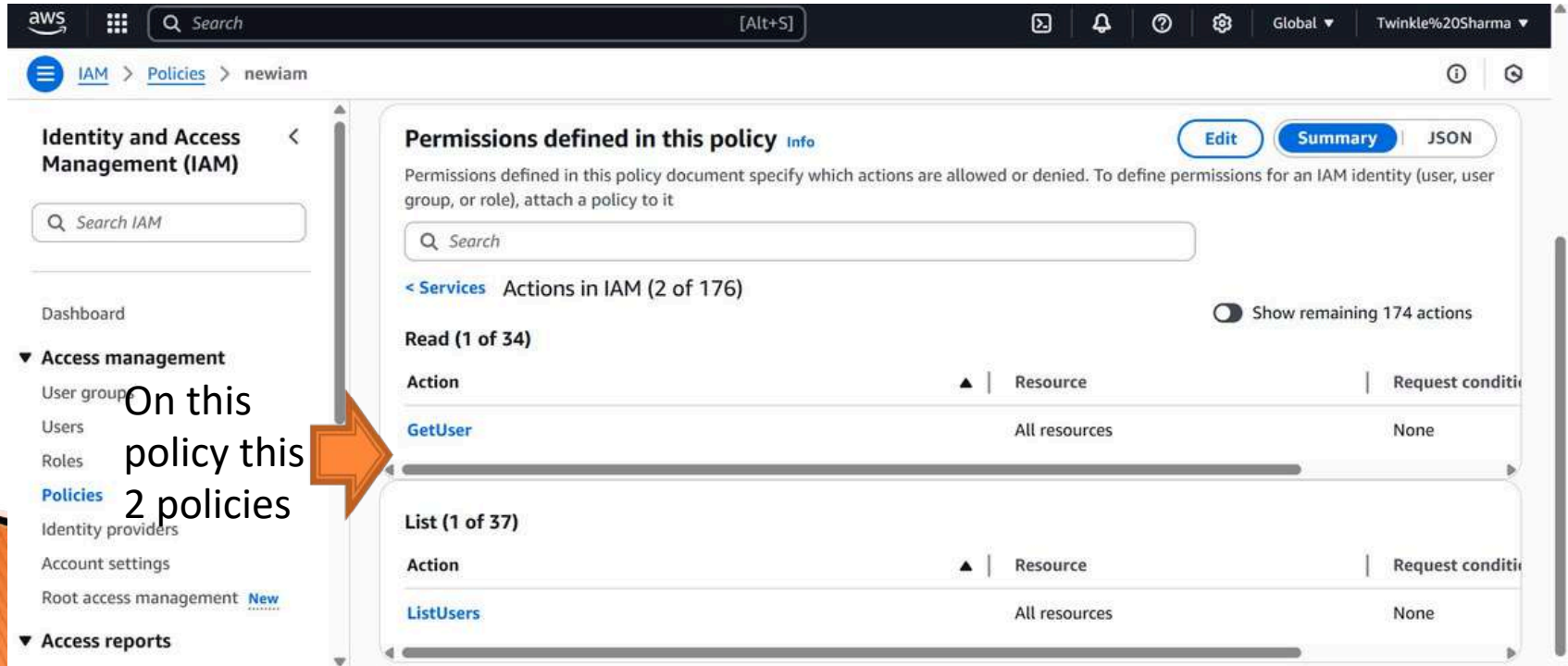
Enter policy name you want to give to your policy

Than scroll down



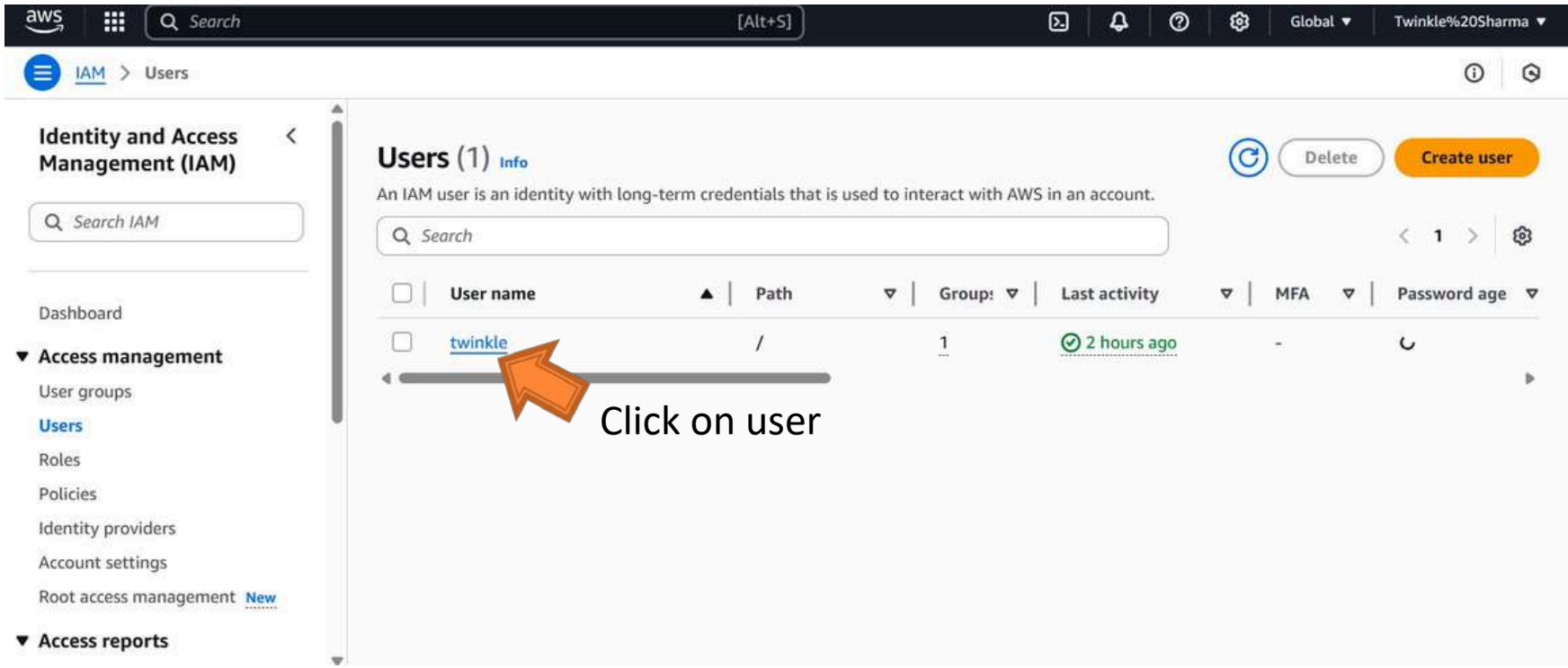
Click on create policy

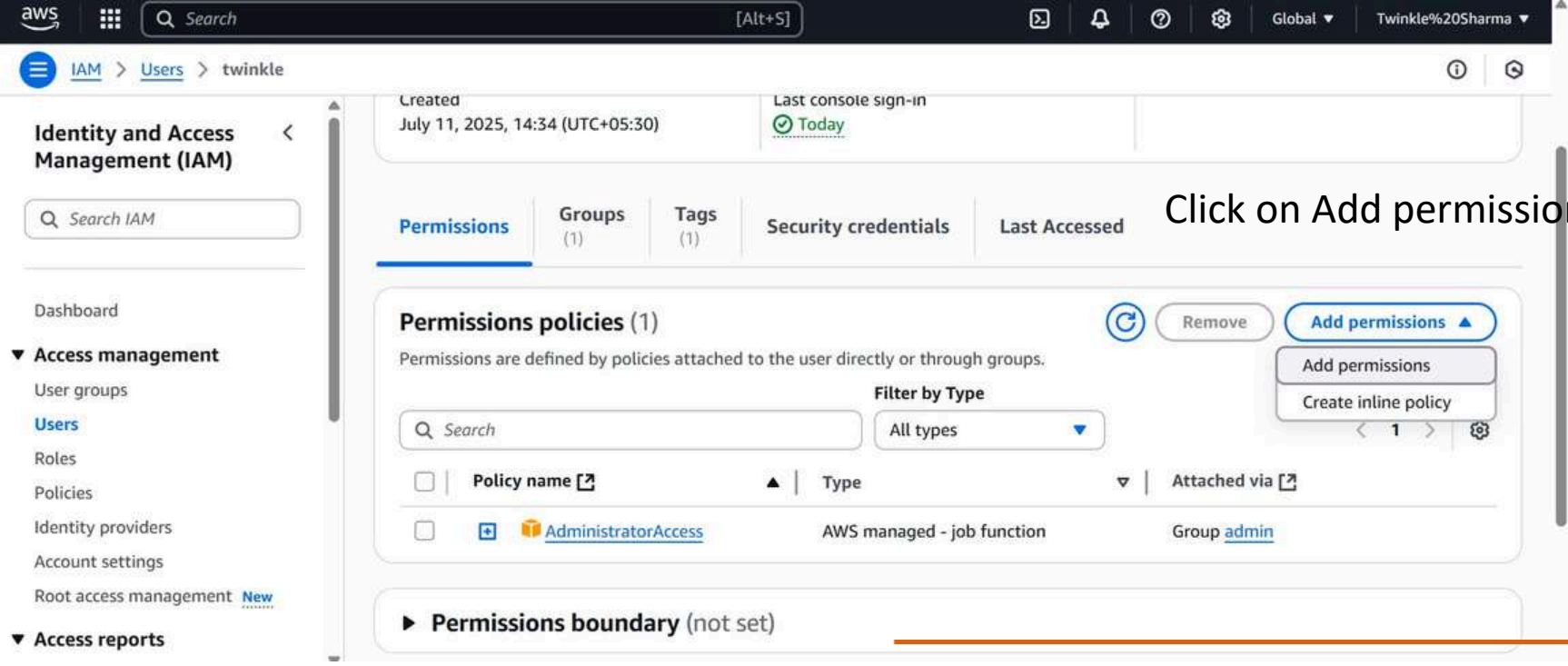

aws
Search
[Alt+S]
Global
Twinkle%20Sharma
IAM > Policies > newiam
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
newiam Info
Edit
Delete
Policy created
Policy details
Type
Customer managed
Creation time
July 14, 2025, 15:27 (UTC+05:30)
Edited time
July 14, 2025, 15:27 (UTC+05:30)
ARN
arn:aws:iam::235562991793 :policy/newiam
Permissions
Entities attached
Tags
Policy versions (1)
Last Accessed
Permissions defined in this policy Info
Edit
Summary
JSON
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 445 services)
Show remaining 444 services


aws
Search
[Alt+S]
Global
Twinkle%20Sharma
IAM > Policies > newiam
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
On this policy this 2 policies
Permissions defined in this policy Info
Edit
Summary
JSON
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
< Services
Actions in IAM (2 of 176)
Show remaining 174 actions
Read (1 of 34)
Action
Resource
Request conditi
GetUser
All resources
None
List (1 of 37)
Action
Resource
Request conditi
ListUsers
All resources
None

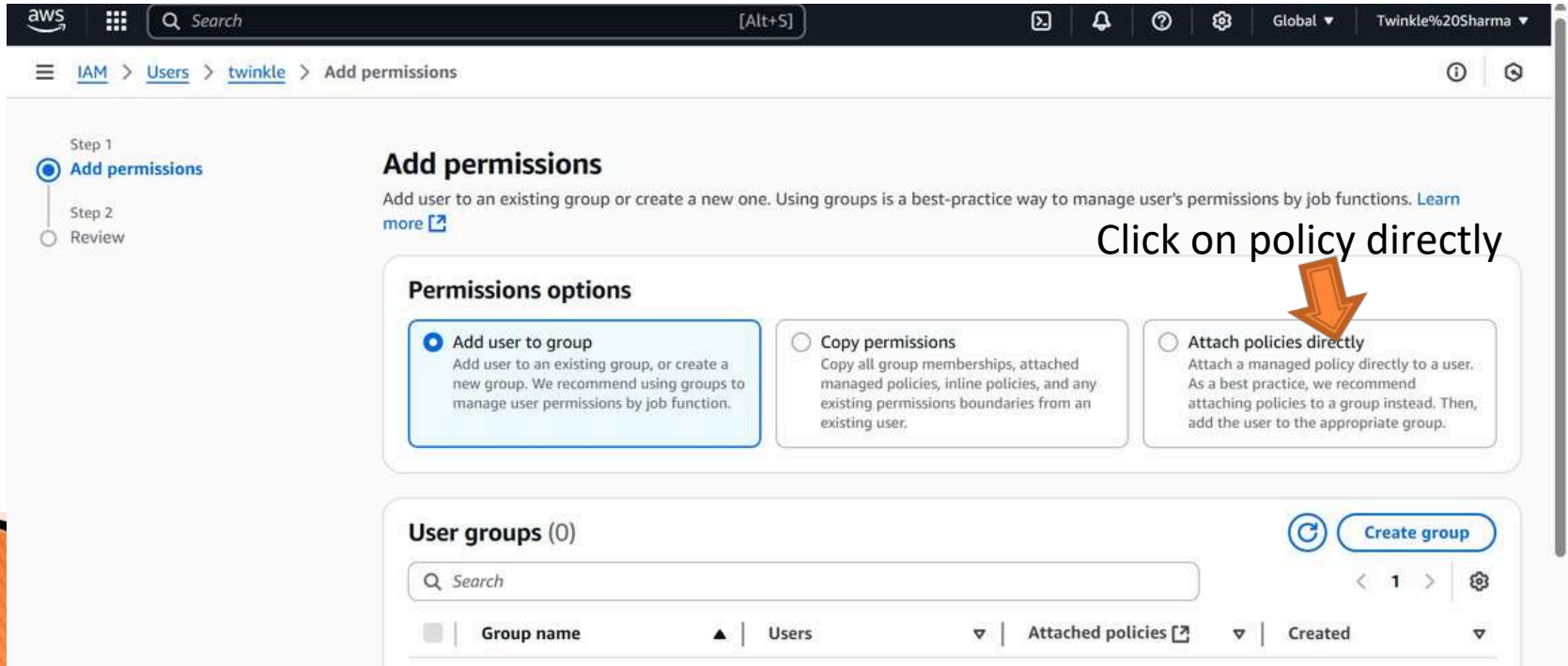
Assign Direct policy to user

- Go to IAM
- Go to user



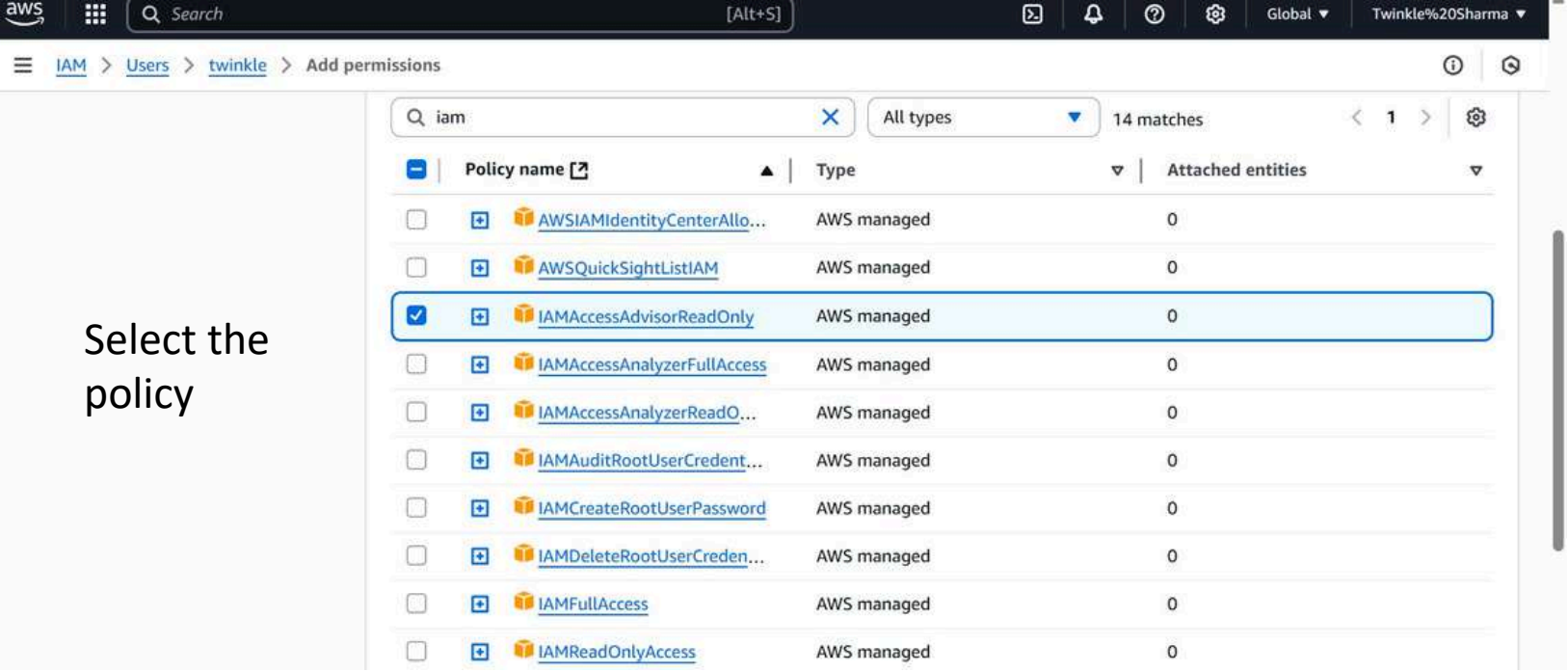


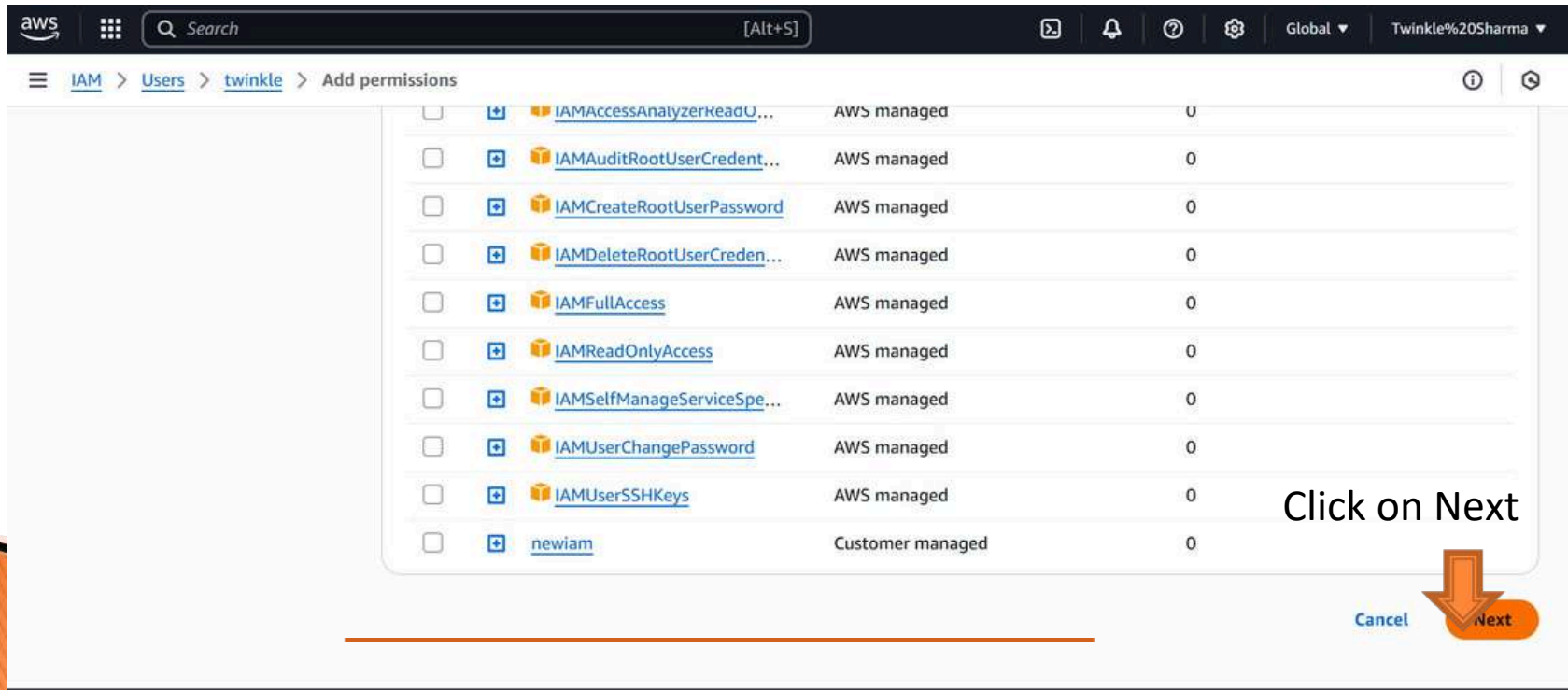
Click on Add permissions



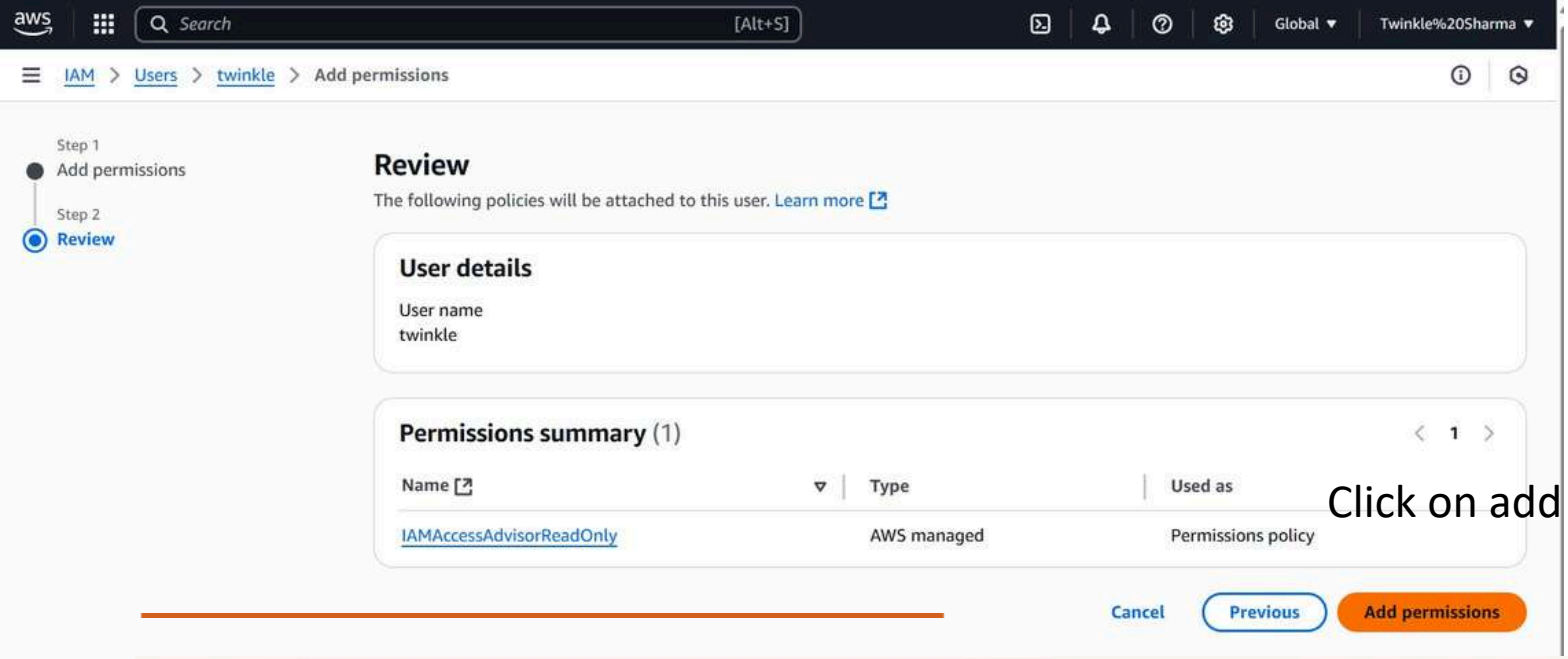
Click on policy directly

Select the policy

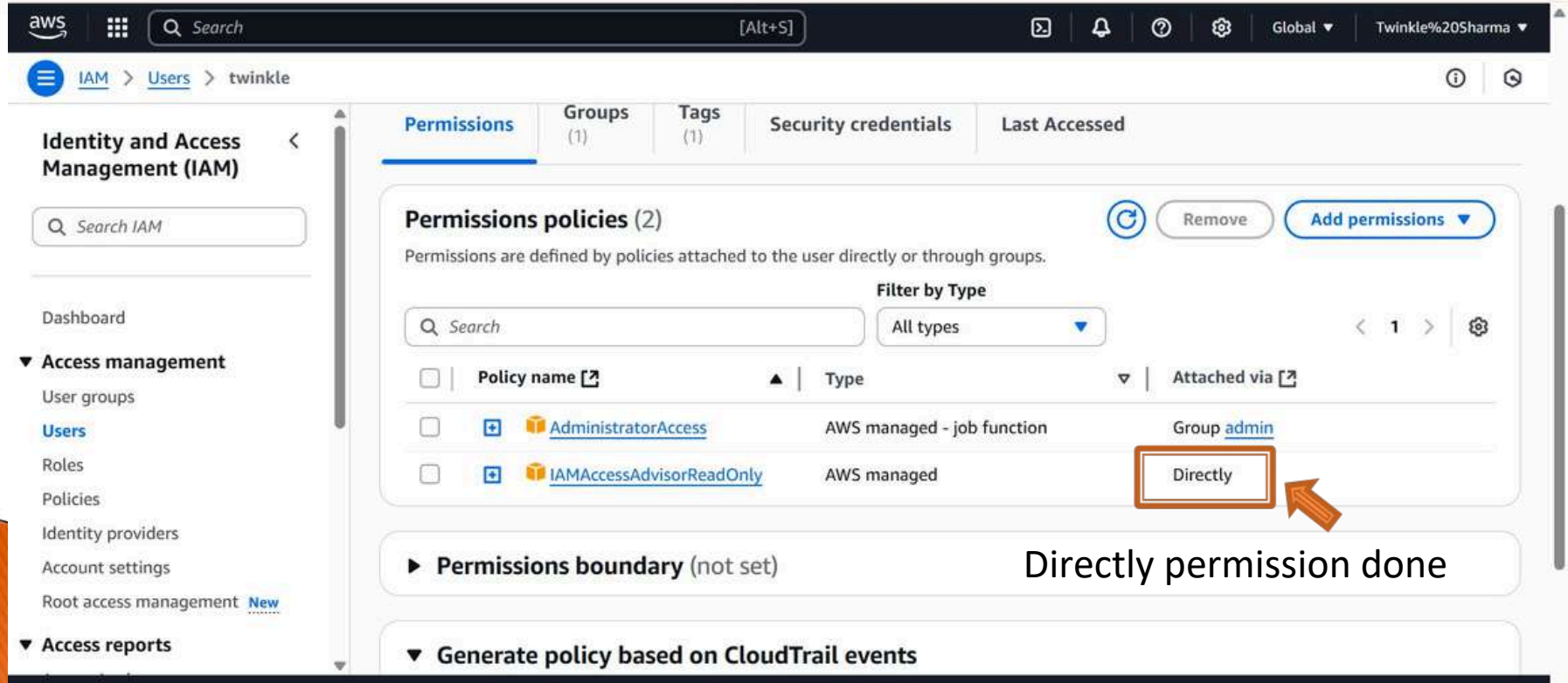




Click on Next



Click on add permissions



Directly permission done

IAM – Password Policy

An IAM Password Policy in AWS defines the rules for creating and managing console passwords for IAM users. It helps ensure users create strong, secure passwords.

IAM Password Policy Options

Policy Setting	Description
☑ **Minimum password length**	Set a length from **6 to 128** characters
☑ **Require uppercase letters**	Must include at least one **A–Z**
☑ **Require lowercase letters**	Must include at least one **a–z**
☑ **Require numbers**	Must include at least one **0–9**
☑ **Require non-alphanumeric characters**	Must include symbols like `!@#$%`
☑ **Allow users to change their own password**	Users can update their passwords
☑ **Enable password expiration**	Force password change after **X days** (up to 1,095 days)
☑ **Prevent password reuse**	Remember and block reuse of last **N passwords** (1–24)
☑ **Require password reset on next sign-in**	When manually creating or updating a password

IAM – MFA (Multi-Factor Authentication)

- MFA requires users to enter:
- Username + Password (first factor)
- One-time code from a virtual/hardware device (second factor)
- Best practice: Enable MFA for all users who log in to the AWS Management Console—especially the root account.

Why Use MFA in IAM?

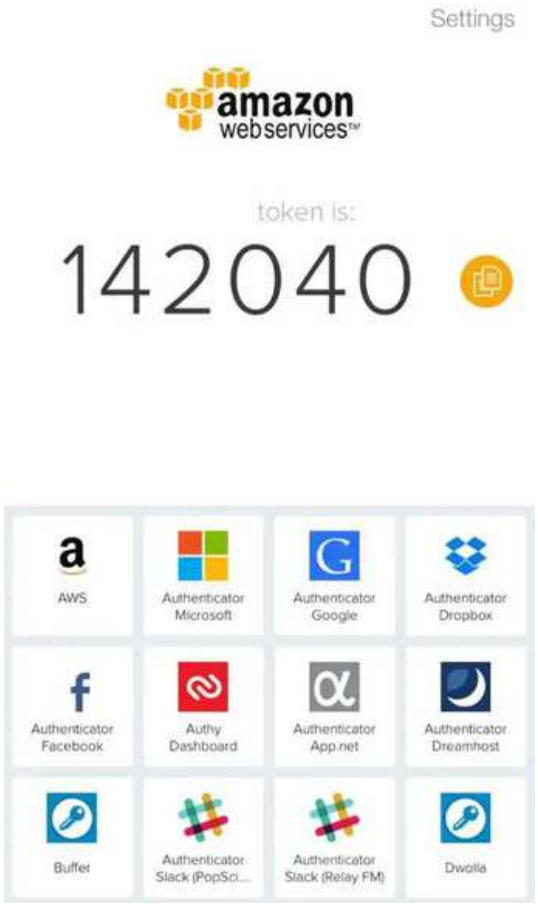
- Adds an extra security layer
- Prevents unauthorized access

ProtectssensitiveAWSresourcesandmanagementactions

MFA Devices Options in AWS

VIRTUAL MFA Device

Google Authenticator
(phoneonly)



Authy
(phone only)

MFA Devices Options in AWS

Universal 2 nd Factor (U2F) Security Key

Yubikey by Yubico (3rd Party)

MFA Devices Options in AWS

Hardware Key FOB MFA Device

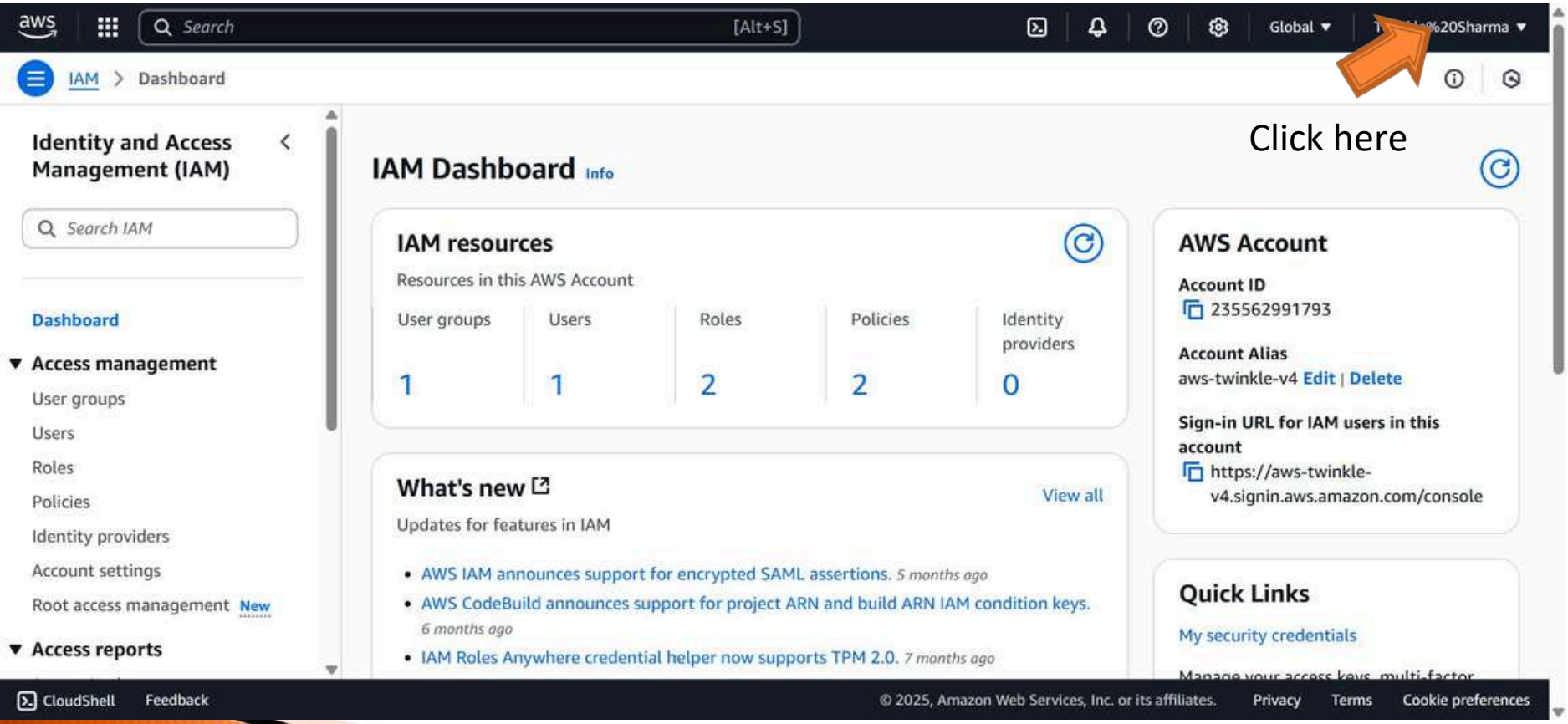
Provided by Gemalto (3rd Party)

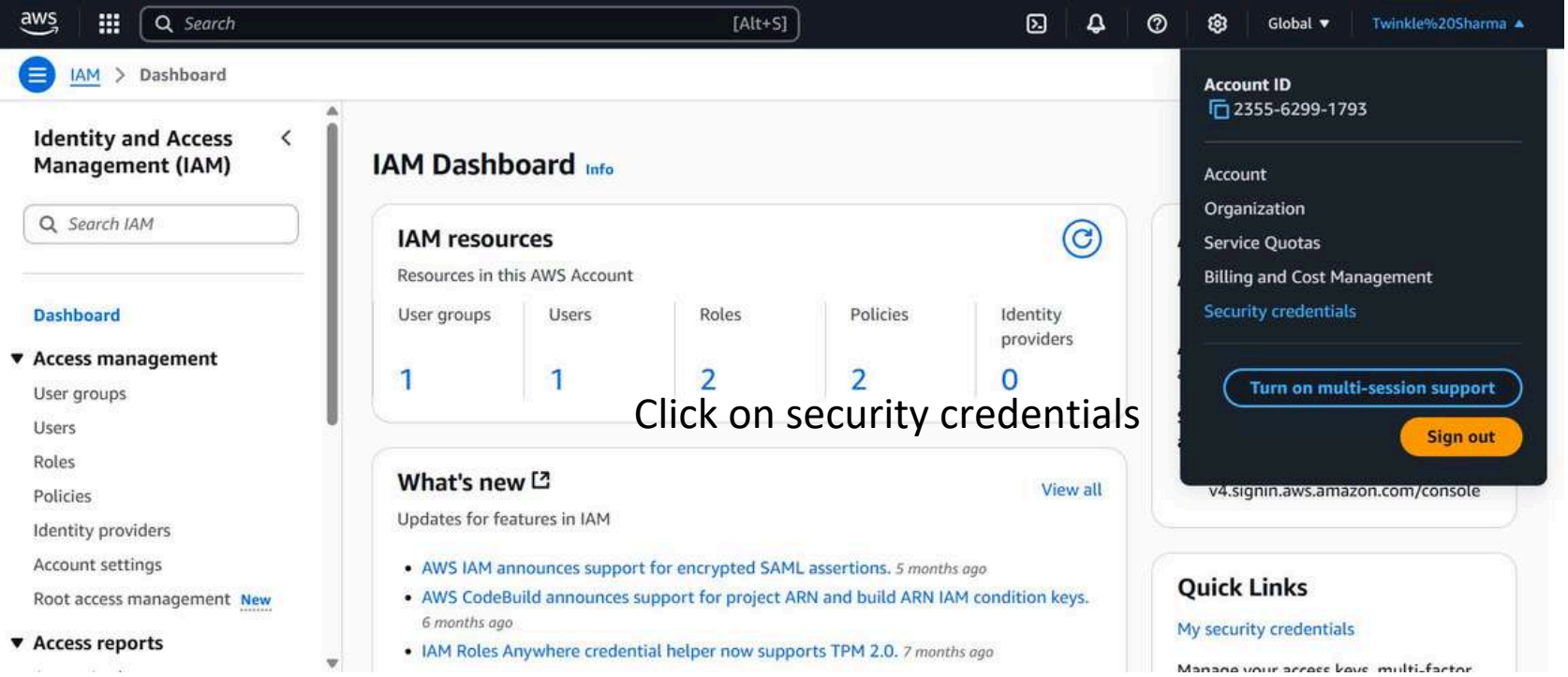
Hardware Key FOB MFA Device for AWS Gov Cloud (US)

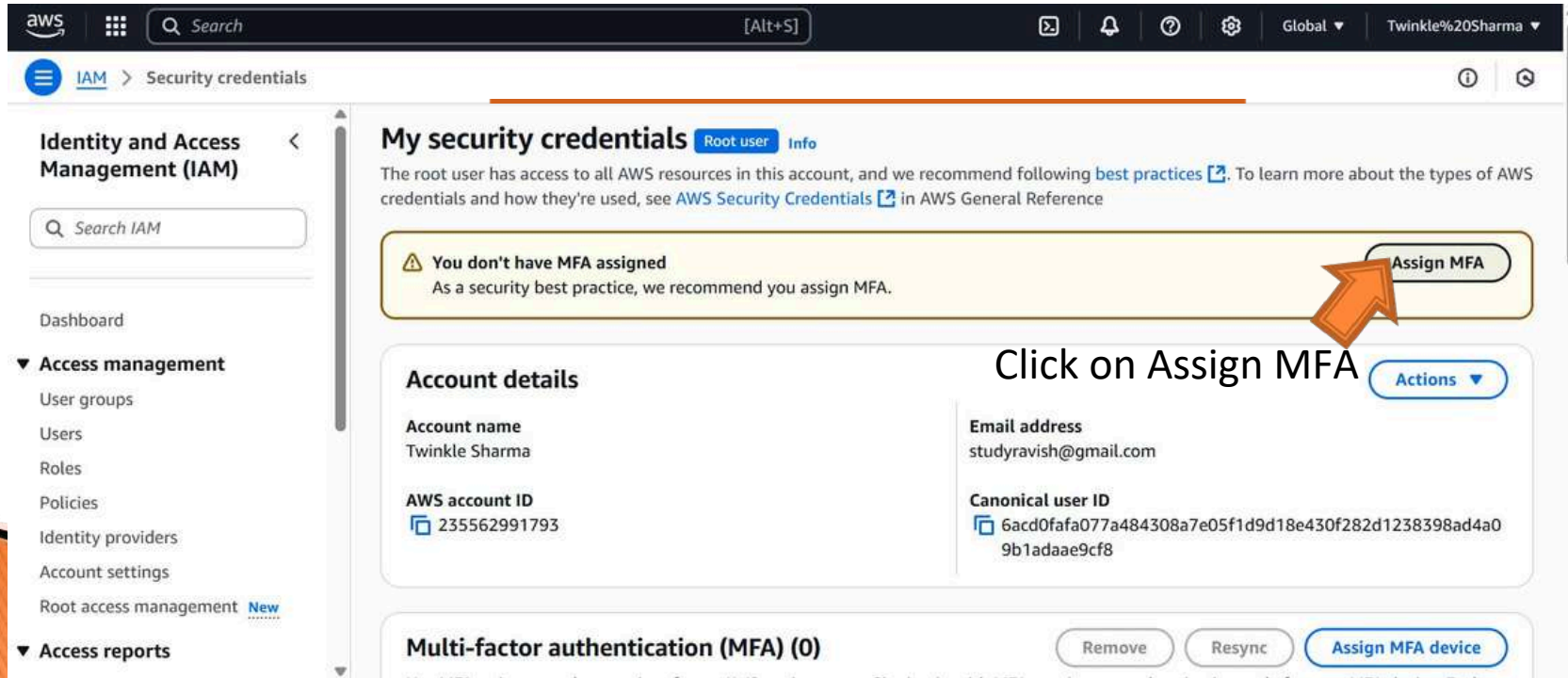
Provided by SurePassID (3rd Party)

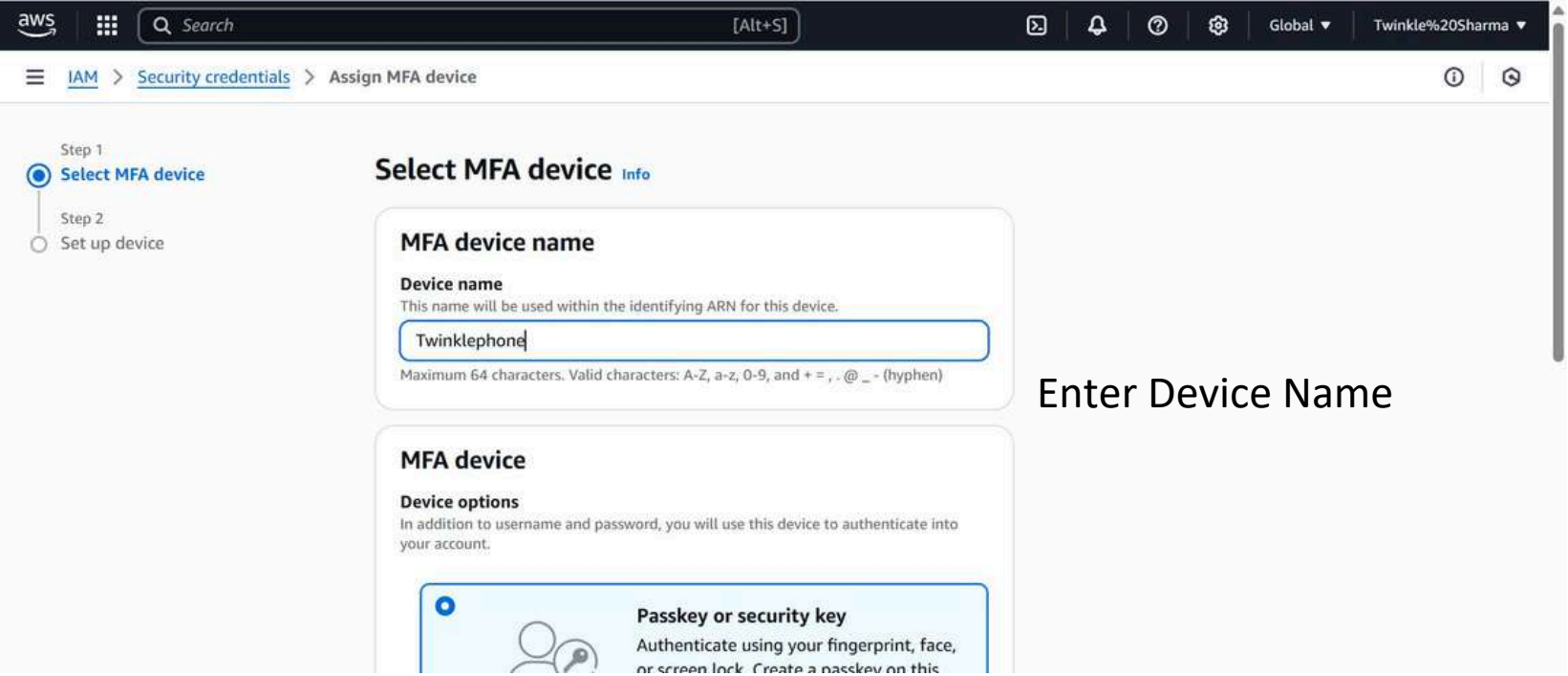
MFA – Hands ON

- Login to AWS Console Portal



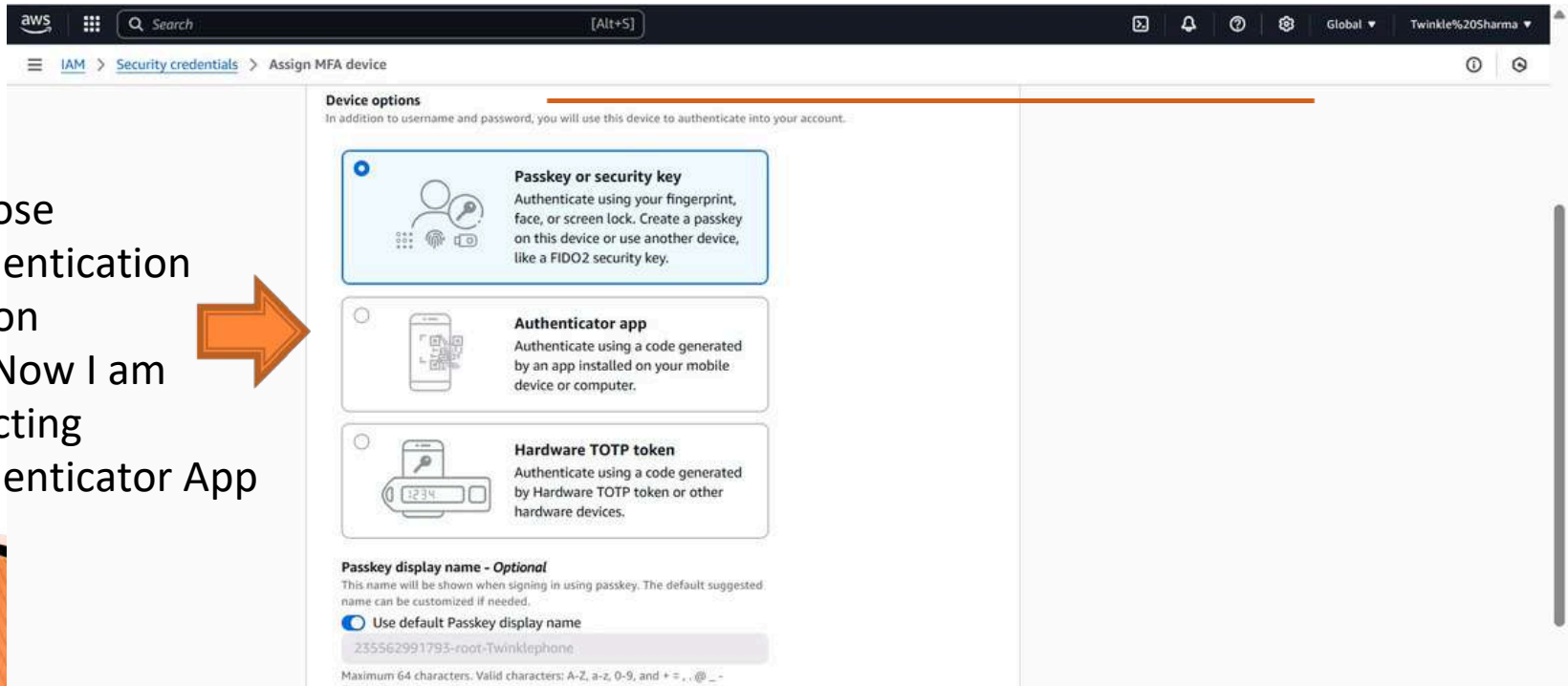

aws
Search
[Alt+S]
Global
Twinkle%20Sharma
IAM > Dashboard
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
IAM Dashboard Info
IAM resources
Resources in this AWS Account
User groups 1
Users 1
Roles 2
Policies 2
Identity providers 0
What's new
View all
Updates for features in IAM
AWS IAM announces support for encrypted SAML assertions. 5 months ago
AWS CodeBuild announces support for project ARN and build ARN IAM condition keys. 6 months ago
IAM Roles Anywhere credential helper now supports TPM 2.0. 7 months ago
Account ID
2355-6299-1793
Account
Organization
Service Quotas
Billing and Cost Management
Security credentials
Turn on multi-session support
Sign out
v4.signin.aws.amazon.com/console
Quick Links
My security credentials
Click on security credentials

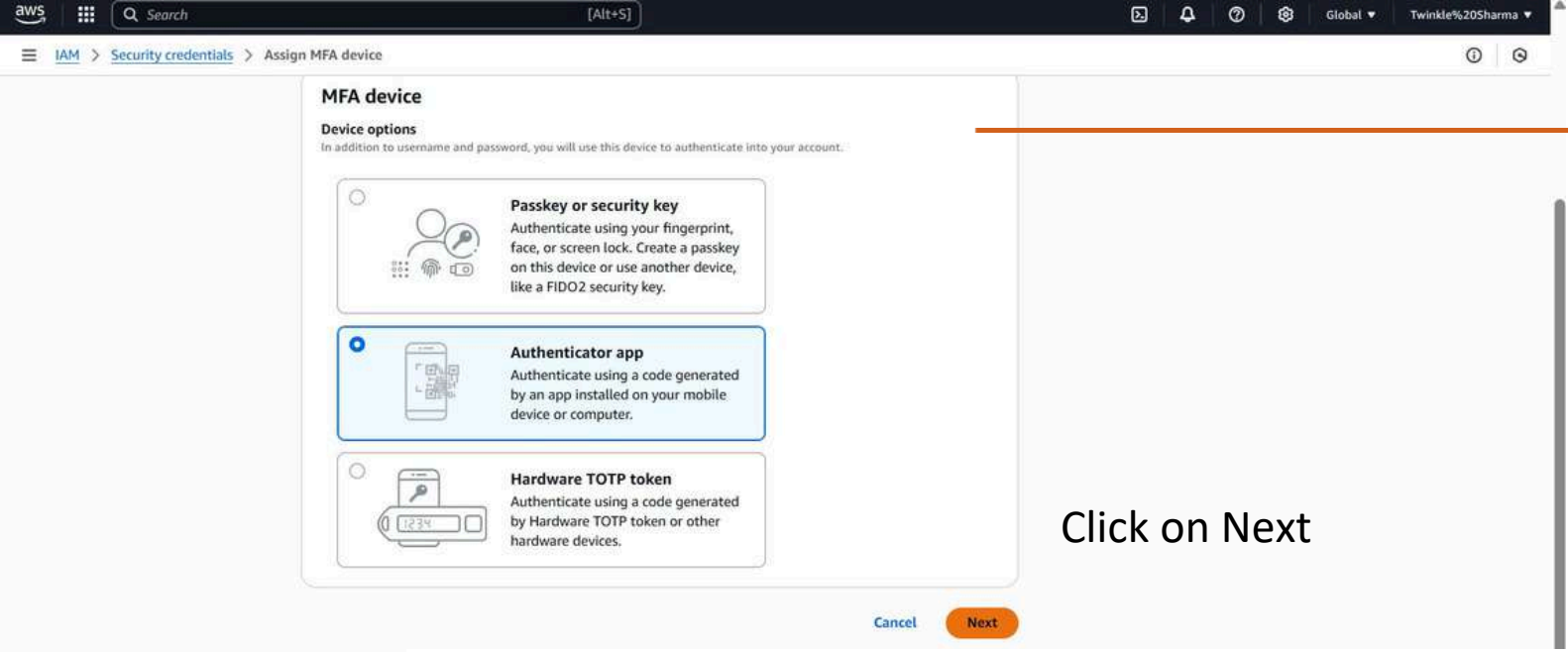

aws
Search
[Alt+S]
Global
Twinkle%20Sharma
IAM > Security credentials
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
My security credentials Root user Info
The root user has access to all AWS resources in this account, and we recommend following best practices. To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference
You don't have MFA assigned
As a security best practice, we recommend you assign MFA.
Assign MFA
Click on Assign MFA
Account details
Actions
Account name
Twinkle Sharma
AWS account ID
235562991793
Email address
studyravish@gmail.com
Canonical user ID
6acd0fafa077a484308a7e05f1d9d18e430f282d1238398ad4a09b1adaae9cf8
Multi-factor authentication (MFA) (0)
Remove
Resync
Assign MFA device



Enter Device Name

Choose authentication option
For Now I am selecting authenticator App





Click on Next

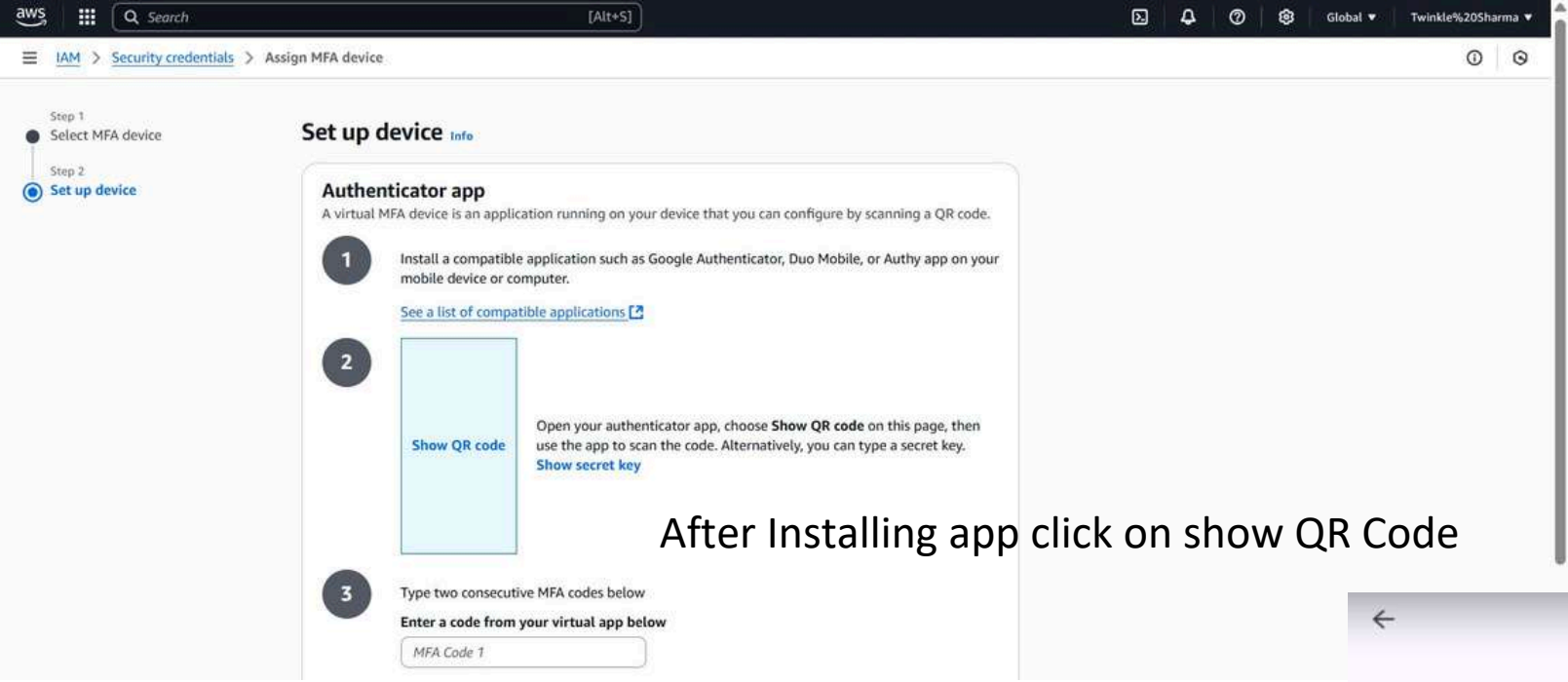
Install any App in your mobile Phone As I Have Android I am installing google authenticator

You can install apps for your smartphone from the app store that is specific to your type of smartphone. Some app providers also have web and desktop applications available. See the following table for examples.

You can choose according to your device

Android: Twilio Authy Authenticator, Duo Mobile, Microsoft Authenticator, Google Authenticator, Symantec VIP

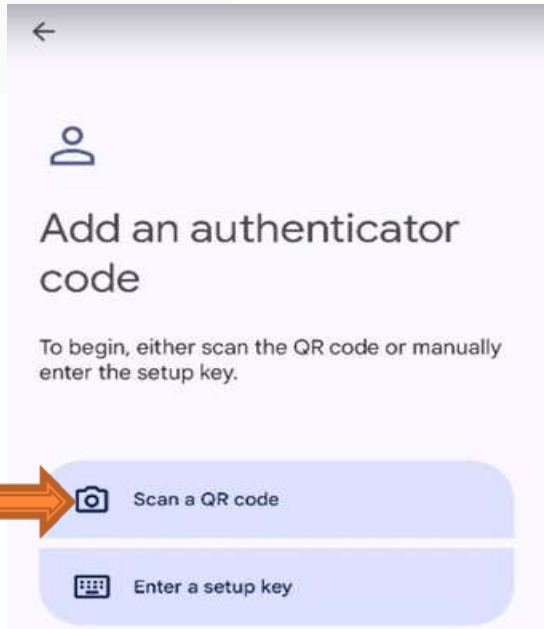
IOS: Twilio Authy Authenticator, Duo Mobile, Microsoft Authenticator, Google Authenticator, Symantec VIP



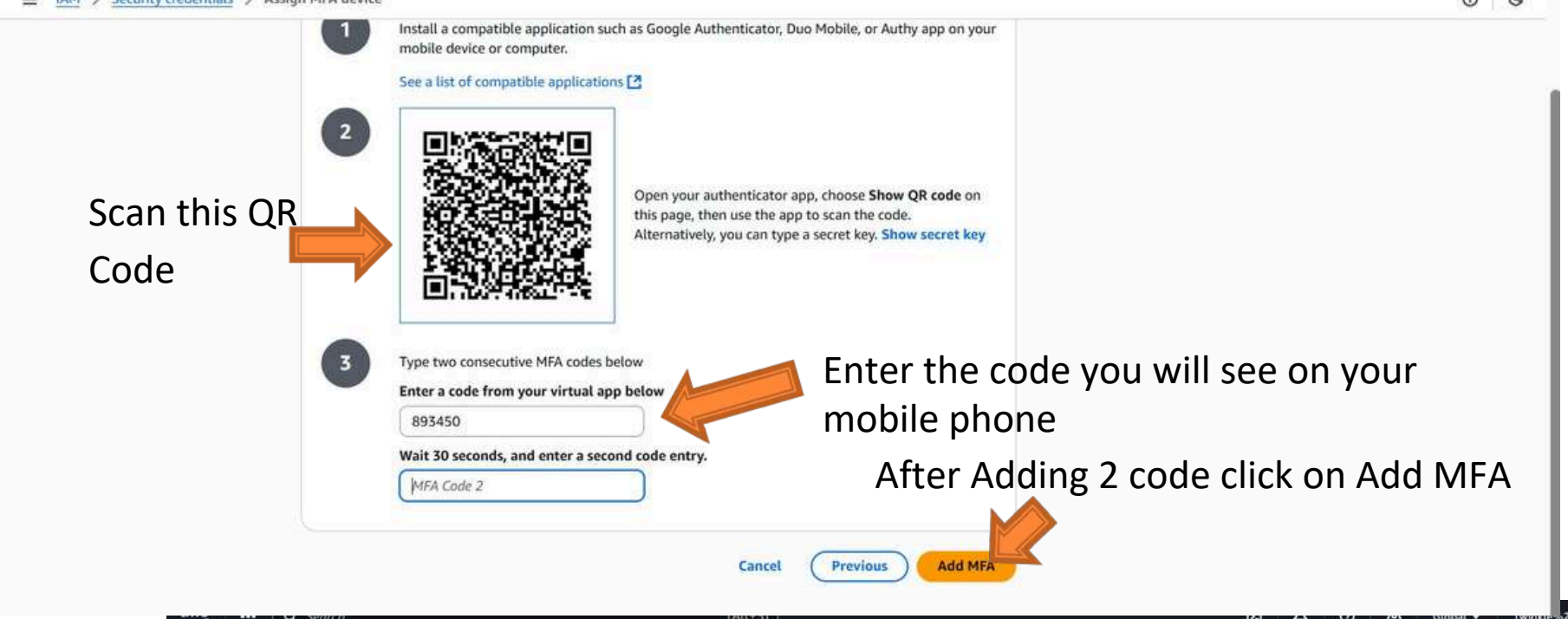
After Installing app click on show QR Code

Open google Authenticator App inmobilephone

Touch on scan a QR Code

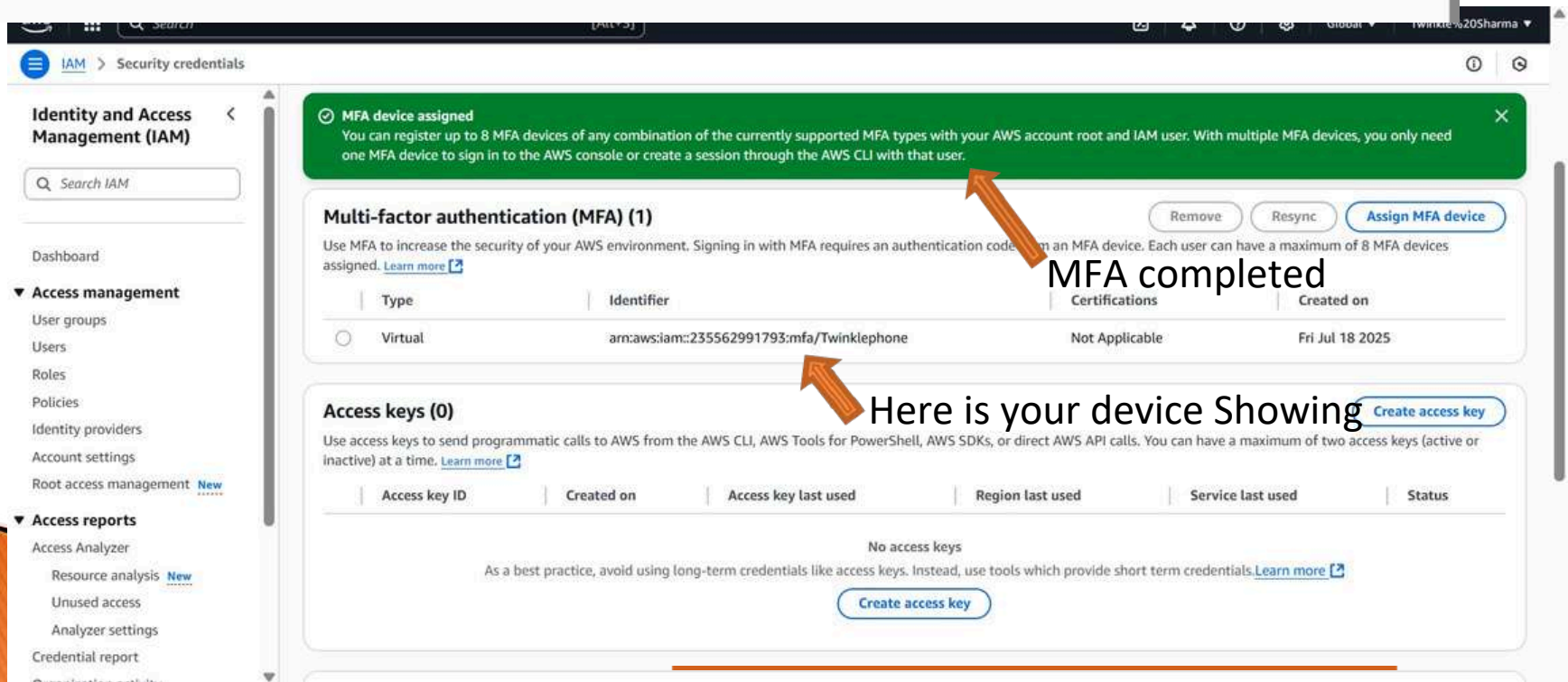


Scan this QR Code



Enter the code you will see on your mobile phone

After Adding 2 code click on Add MFA



MFA completed

Here is your device Showing

What is access key in AWS?

- An AWS Access Key is a pair of security credentials that allow programmatic access to your AWS account using tools like the AWS CLI, SDKs, or API calls.

What Is an AWS Access Key?

It consists of two parts:

Component	Example Format
Access Key ID	`AKIAIOSFODNN7EXAMPLE`
Secret Access Key	`wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Together, these are used to **authenticate** your application/script to AWS.

AWS CLI (Command Line Interface)

- The AWS CLI is a unified tool that provides a consistent interface for interacting with AWS services using commands in your shell (PowerShell, Bash, etc.).

What is the AWS SDK (Software Development Kit)?

The AWS SDK allows you to:

CallAWSservicesprogrammatically(likeEC2,S3,DynamoDB)

Sign requests, handle retries, parse responses

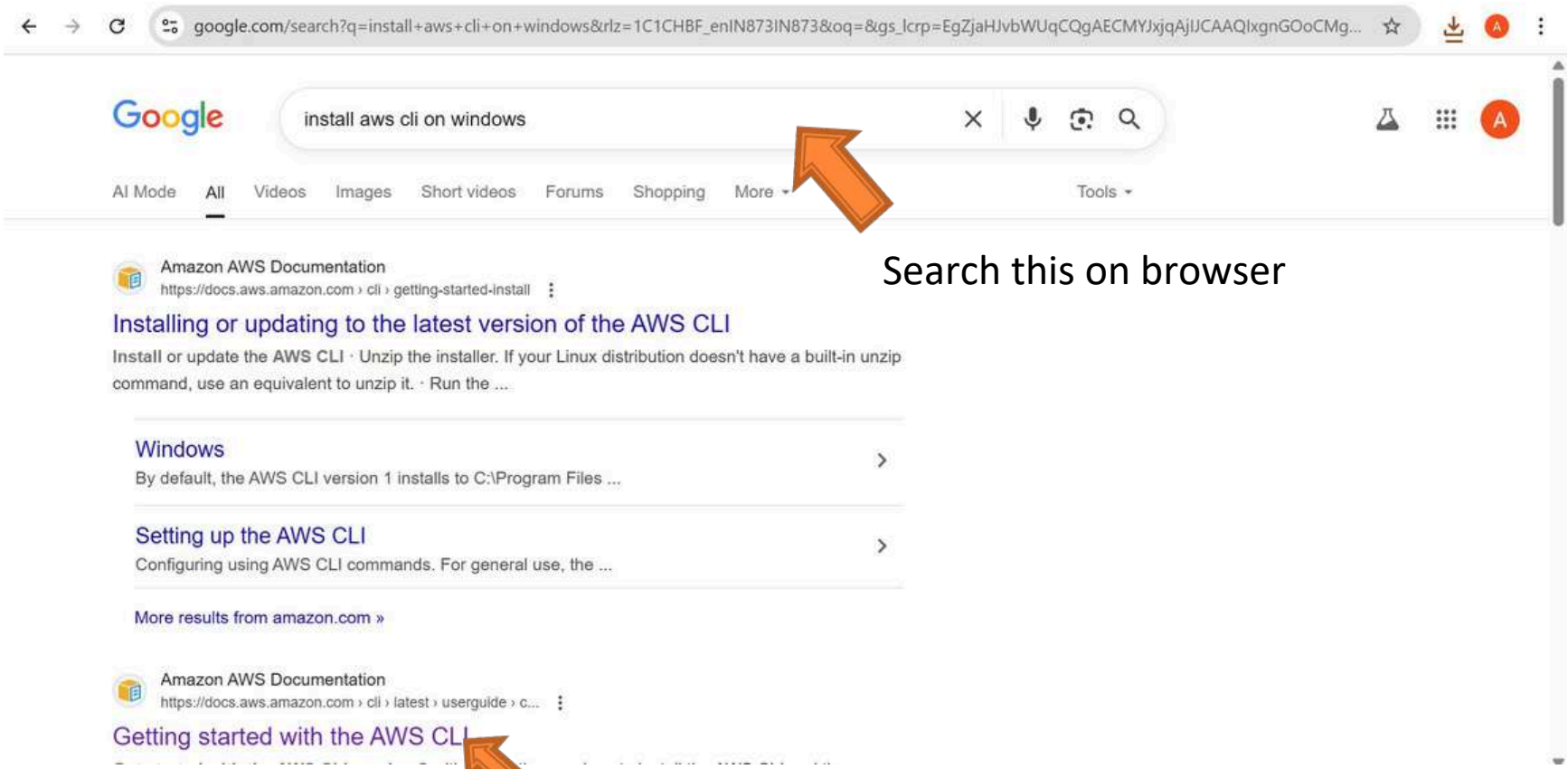
Integrate AWS into mobile, web, and backend applications
Use temporary credentials, MFA, and roles

It simplifies using AWS APIs in your language of choice.

Popular AWS SDKs by Language

Language	SDK Name	Package Manager
Python	**boto3**	`pip install boto3`
JavaScript/Node.js	**aws-sdk / @aws-sdk/client-s3**	`npm install`
Java	AWS SDK for Java	Maven/Gradle
C#/.NET	AWS SDK for .NET	NuGet
Go	AWS SDK for Go	`go get`
PHP	AWS SDK for PHP	Composer
Ruby	AWS SDK for Ruby	`gem install`

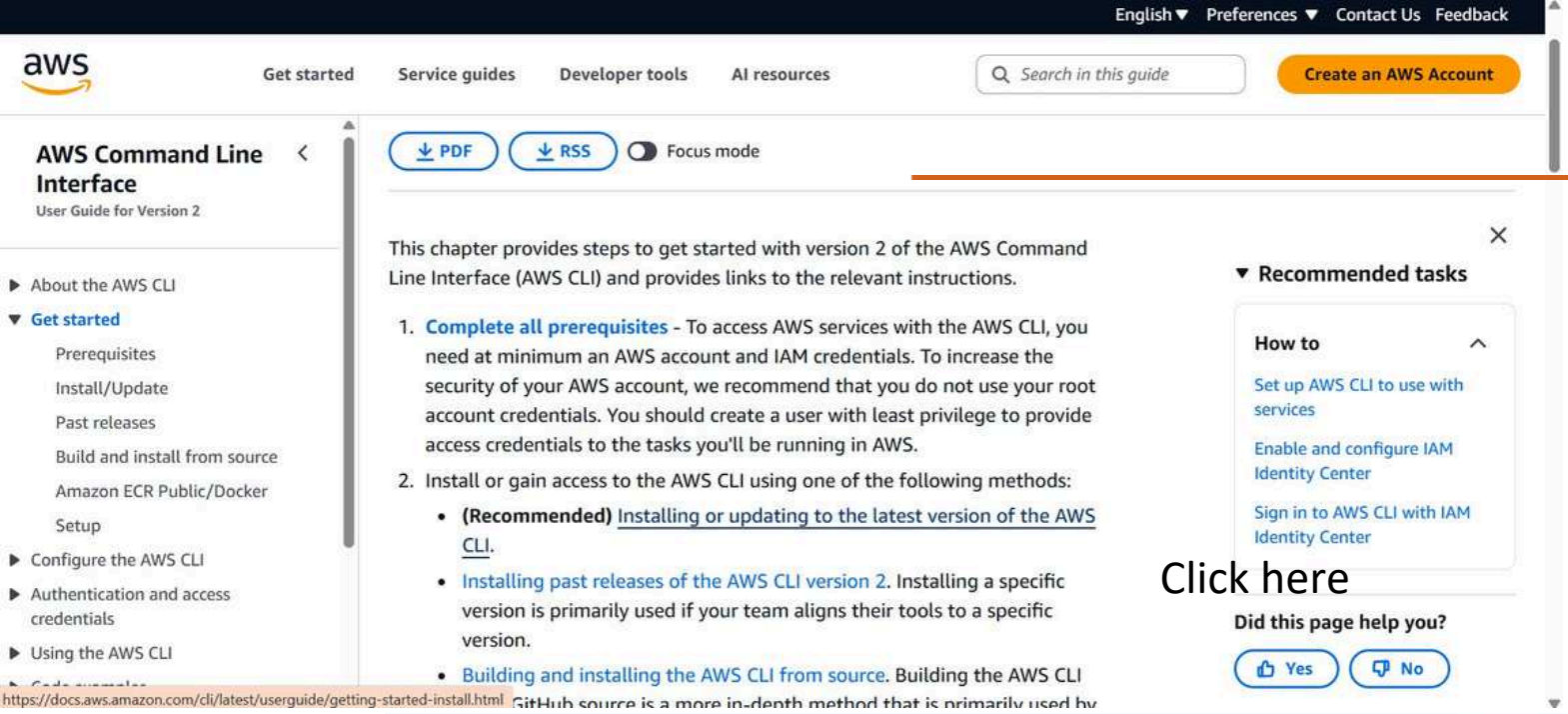
AWS CLI Setup on windows

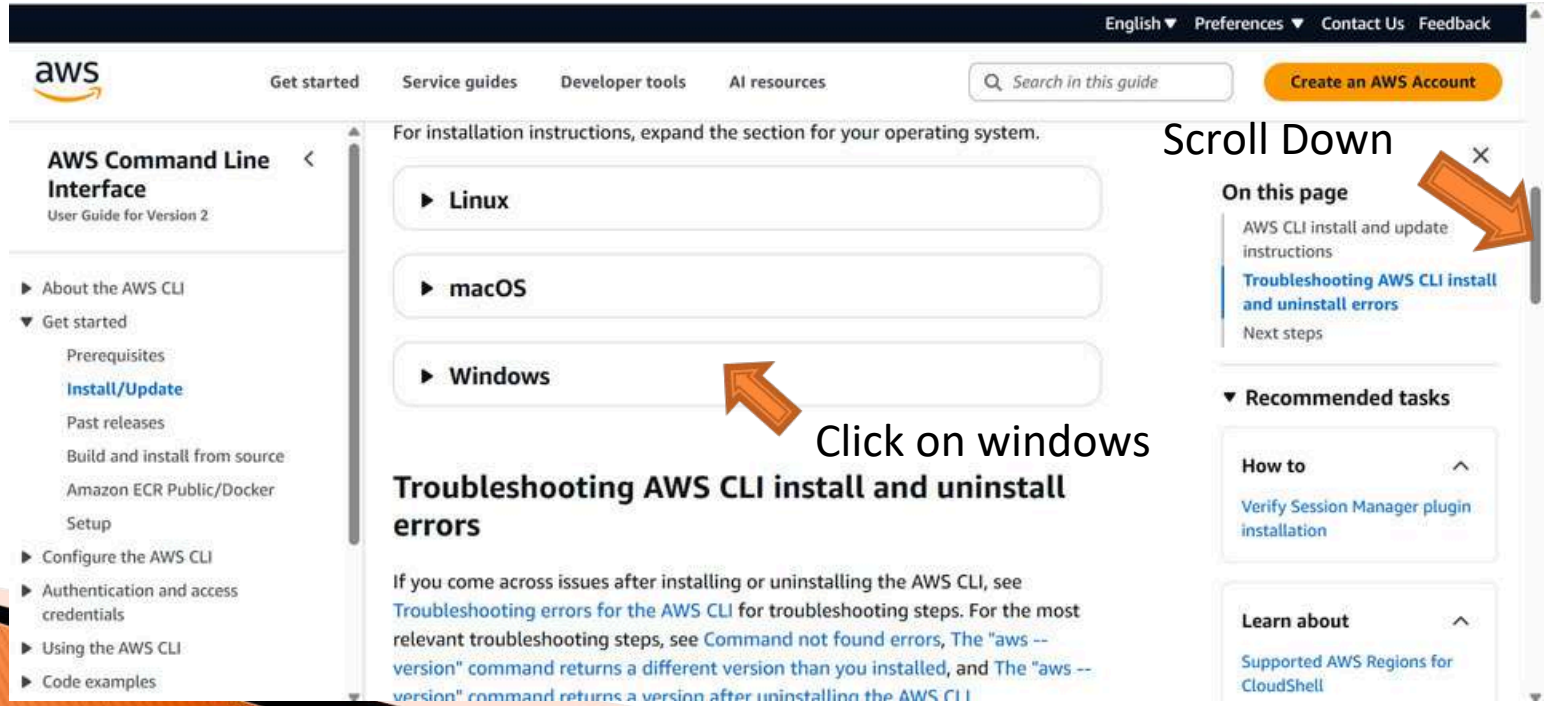


Search this on browser

After that, click here

rajendra0968jangid


English Preferences Contact Us Feedback
aws
Get started
Service guides
Developer tools
AI resources
Search in this guide
Create an AWS Account
AWS Command Line Interface
User Guide for Version 2
About the AWS CLI
Get started
Prerequisites
Install/Update
Past releases
Build and install from source
Amazon ECR Public/Docker
Setup
Configure the AWS CLI
Authentication and access credentials
Using the AWS CLI
PDF
RSS
Focus mode
This chapter provides steps to get started with version 2 of the AWS Command Line Interface (AWS CLI) and provides links to the relevant instructions.
1. Complete all prerequisites - To access AWS services with the AWS CLI, you need at minimum an AWS account and IAM credentials. To increase the security of your AWS account, we recommend that you do not use your root account credentials. You should create a user with least privilege to provide access credentials to the tasks you'll be running in AWS.
2. Install or gain access to the AWS CLI using one of the following methods:
• (Recommended) Installing or updating to the latest version of the AWS CLI.
• Installing past releases of the AWS CLI version 2. Installing a specific version is primarily used if your team aligns their tools to a specific version.
• Building and installing the AWS CLI from source. Building the AWS CLI
Recommended tasks
How to
Set up AWS CLI to use with services
Enable and configure IAM Identity Center
Sign in to AWS CLI with IAM Identity Center
Click here
Did this page help you?
Yes
No
https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html


English Preferences Contact Us Feedback
aws
Get started
Service guides
Developer tools
AI resources
Search in this guide
Create an AWS Account
AWS Command Line Interface
User Guide for Version 2
About the AWS CLI
Get started
Prerequisites
Install/Update
Past releases
Build and install from source
Amazon ECR Public/Docker
Setup
Configure the AWS CLI
Authentication and access credentials
Using the AWS CLI
Code examples
For installation instructions, expand the section for your operating system.
Linux
macOS
Windows
Scroll Down
Click on windows
Troubleshooting AWS CLI install and uninstall errors
If you come across issues after installing or uninstalling the AWS CLI, see Troubleshooting errors for the AWS CLI for troubleshooting steps. For the most relevant troubleshooting steps, see Command not found errors, The "aws --version" command returns a different version than you installed, and The "aws --
On this page
AWS CLI install and update instructions
Troubleshooting AWS CLI install and uninstall errors
Next steps
Recommended tasks
How to
Verify Session Manager plugin installation
Learn about
Supported AWS Regions for CloudShell

- We support the AWS CLI on Microsoft-supported versions of 64-bit Windows.
- Admin rights to install software

Install or update the AWS CLI

To update your current installation of AWS CLI on Windows, download a new installer each time you update to overwrite previous versions. AWS CLI is updated regularly. To see when the latest version was released, see the AWS CLI version 2 Changelog on *GitHub*.

1. Download and run the AWS CLI MSI installer for Windows (64-bit):
   https://awscli.amazonaws.com/AWSCLIV2.msi
   Alternatively, you can run the `msiexec` command to run the MSI installer.

```
C:\> msiexec.exe /i https://awscli.amazonaws.com/AWSC
```

For various parameters that can be used with `msiexec`, see msiexec

Recommended tasks

How to
Verify Session Manager plugin installation

Learn about
Supported AWS Regions for CloudShell

Click here

aws Get started Service guides Developer tools AI resources

AWS Command Line Interface
User Guide for Version 2

- About the AWS CLI
- Get started
  - Prerequisites
  - Install/Update
  - Past releases
  - Build and install from source
  - Amazon ECR Public/Docker
  - Setup
- Configure the AWS CLI
- Authentication and access credentials
- Using the AWS CLI
- Code examples

- We support the AWS CLI on Microsoft-supported versions of 64-bit Windows.
- Admin rights to install software

Install or update the AWS CLI

To update your current installation of AWS CLI on Windows, download a new installer each time you update to overwrite previous versions. AWS CLI is updated regularly. To see when the latest version was released, see the AWS CLI version 2 Changelog on *GitHub*.

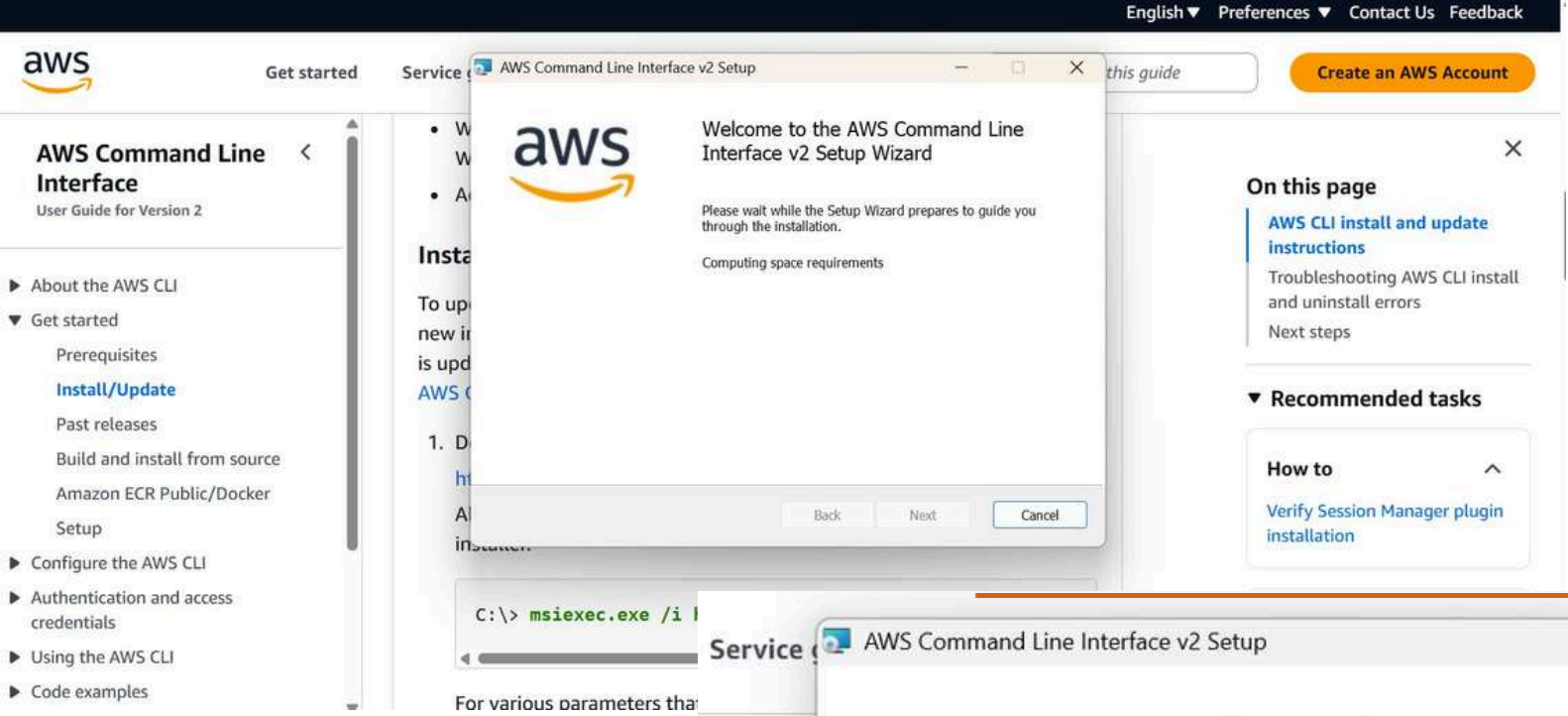
1. Download and run the AWS CLI MSI installer for Windows (64-bit):
   https://awscli.amazonaws.com/AWSCLIV2.msi
   Alternatively, you can run the `msiexec` command to run the MSI installer.

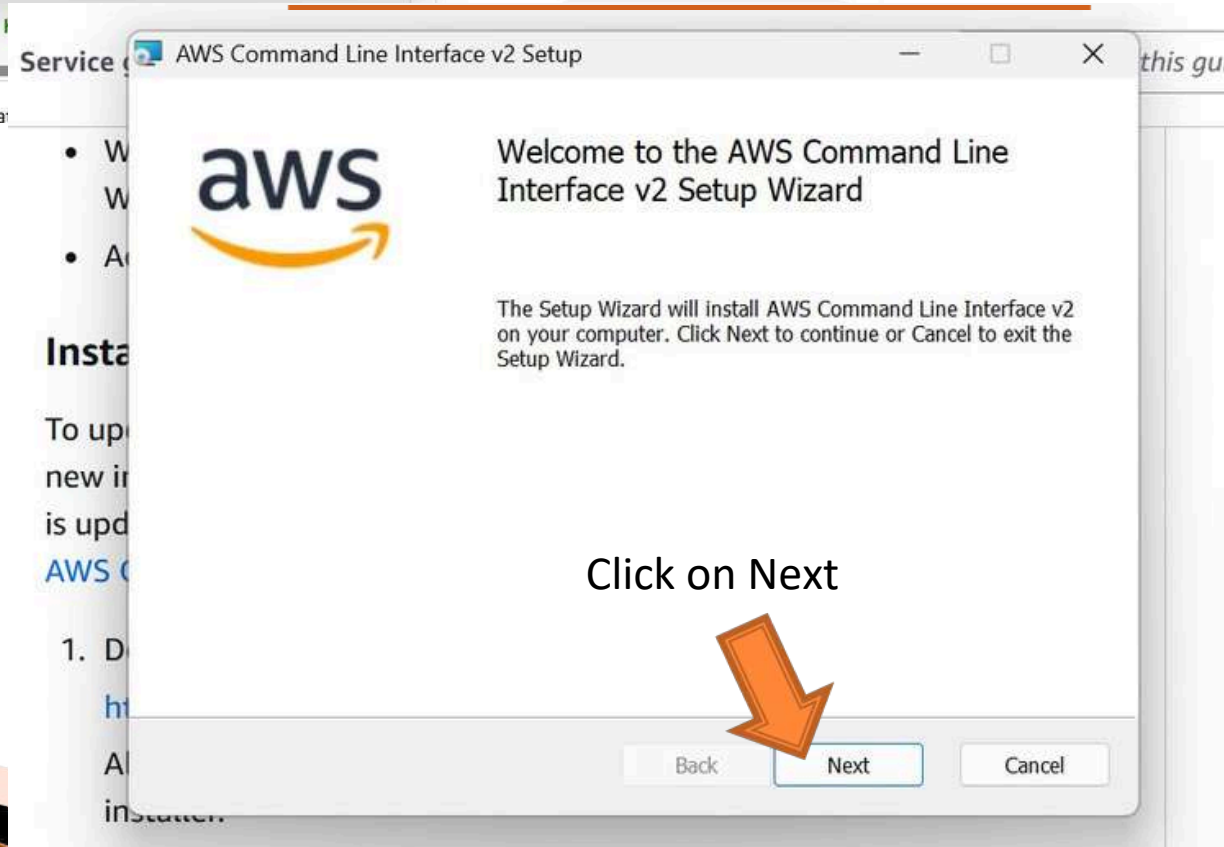
```
C:\> msiexec.exe /i https://awscli.amazonaws.com/AWSC
```

For various parameters that can be used with `msiexec`, see msiexec

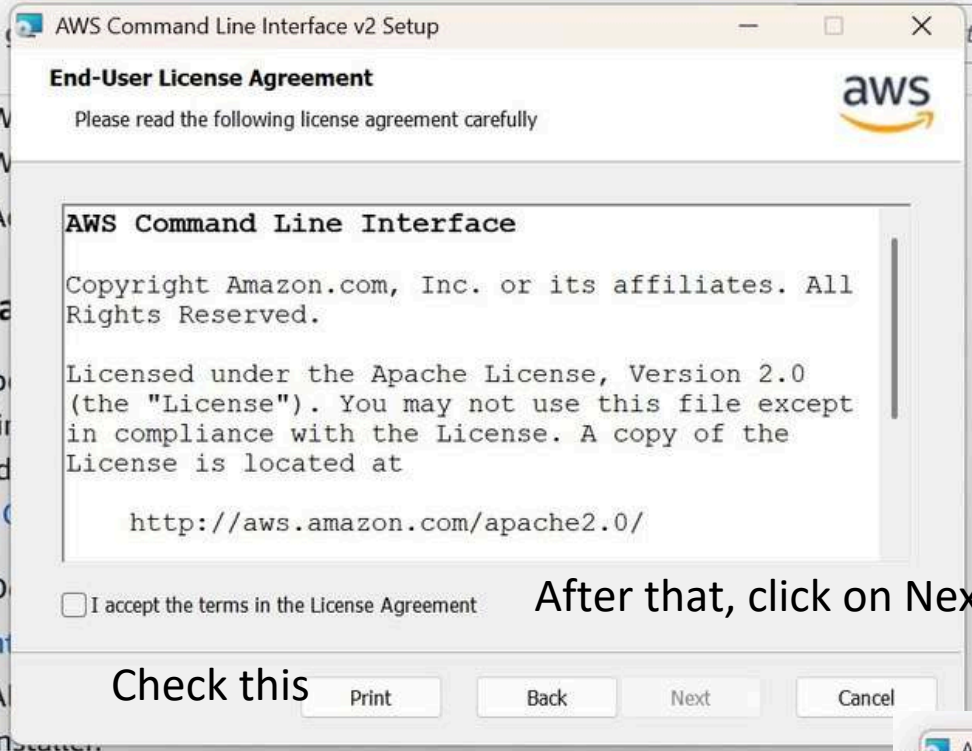
Recent download history
AWSCLIV2.msi
39.2 MB • Done
Full download history

Click on downloaded File



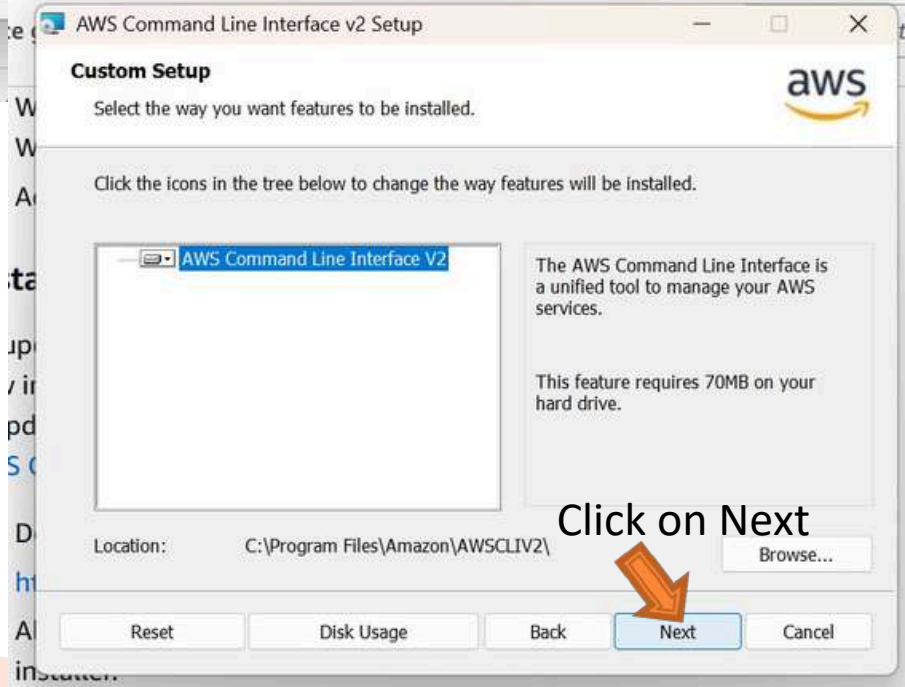


Click on Next

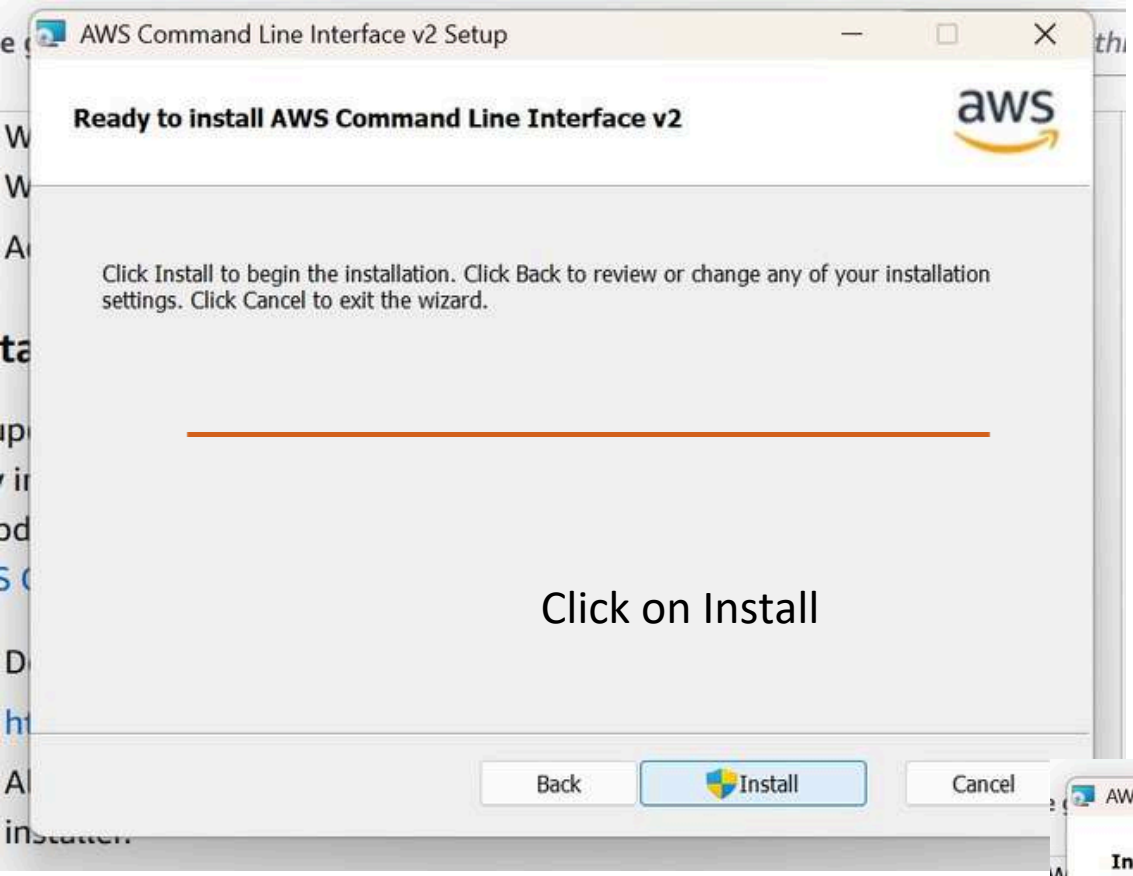


After that, click on Next

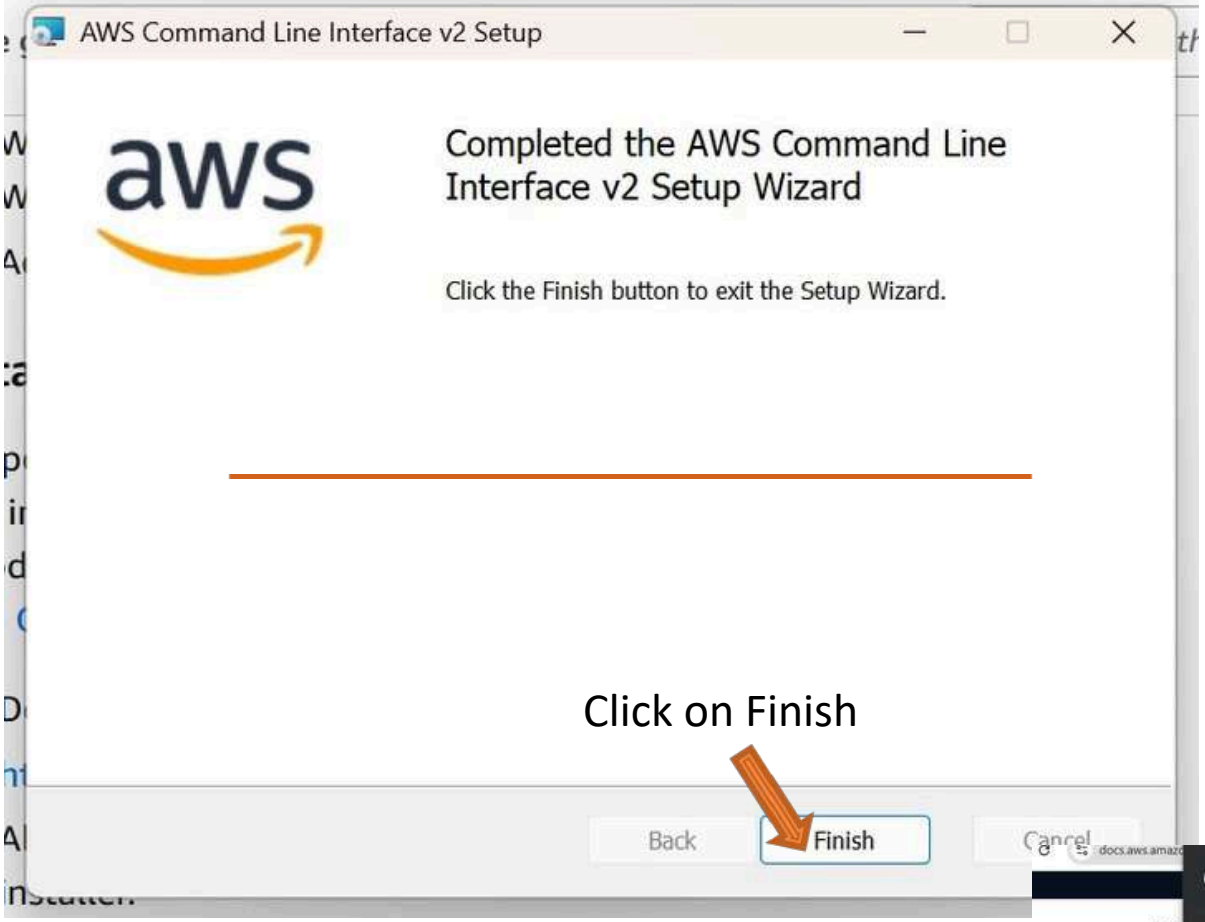
Check this



Click on Next

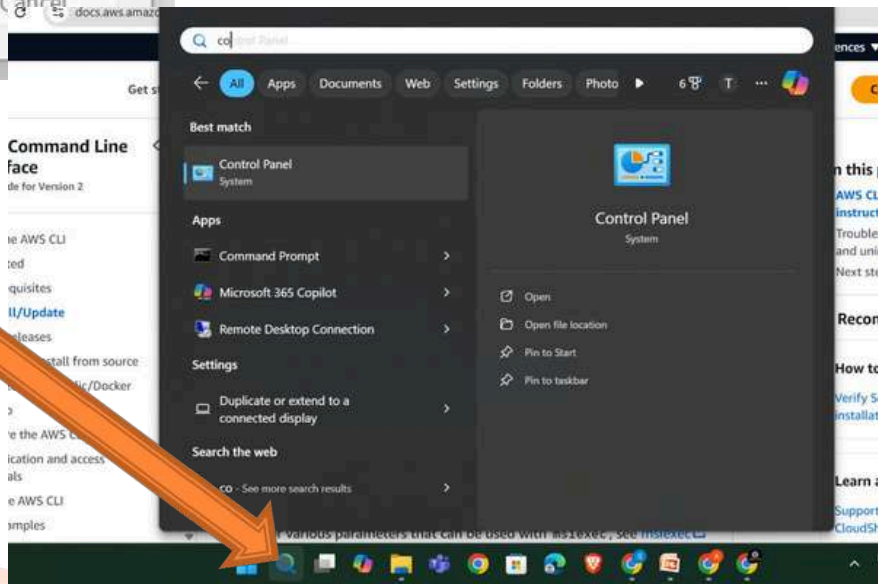


Click on Install



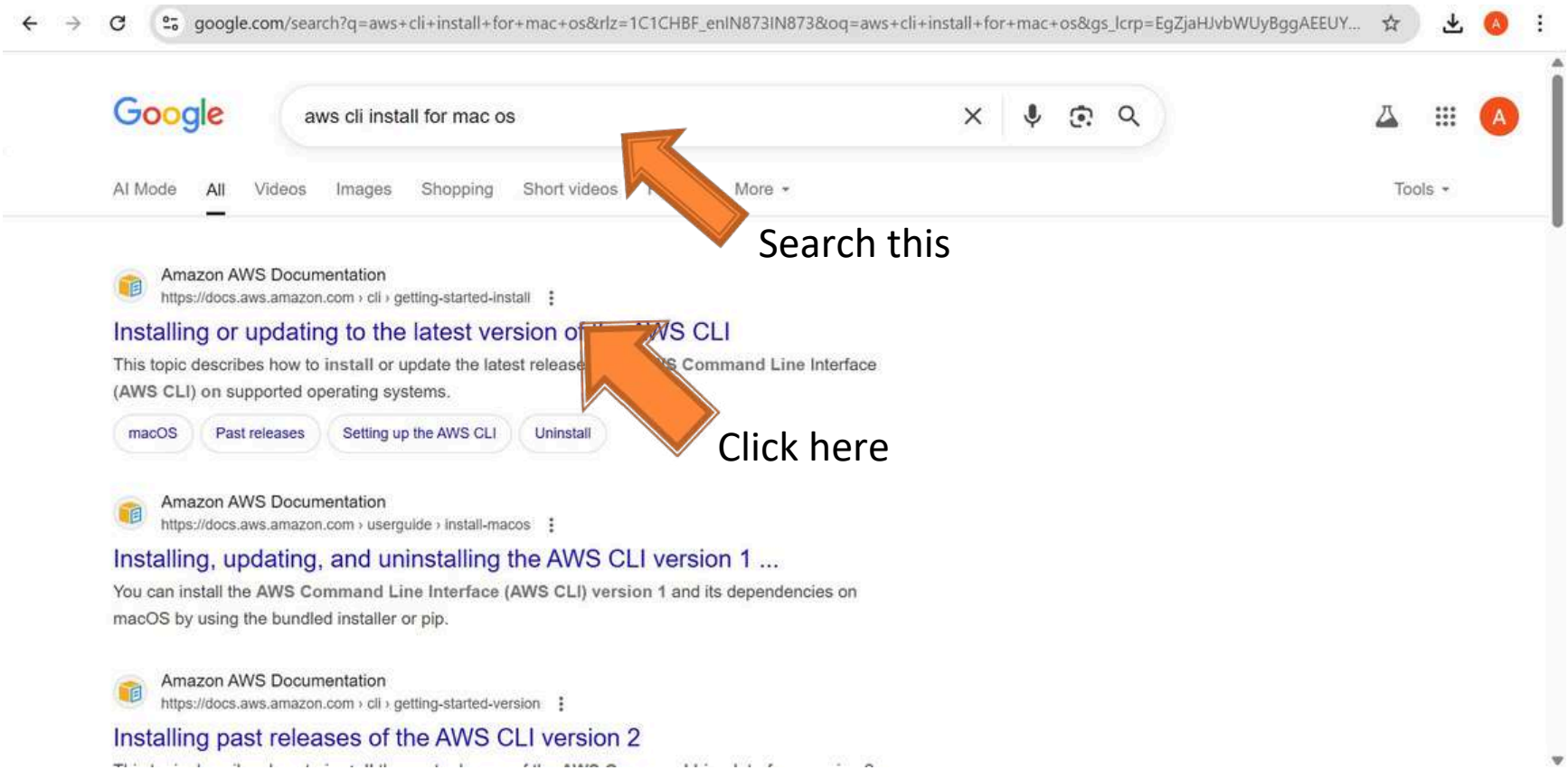
Click on Finish

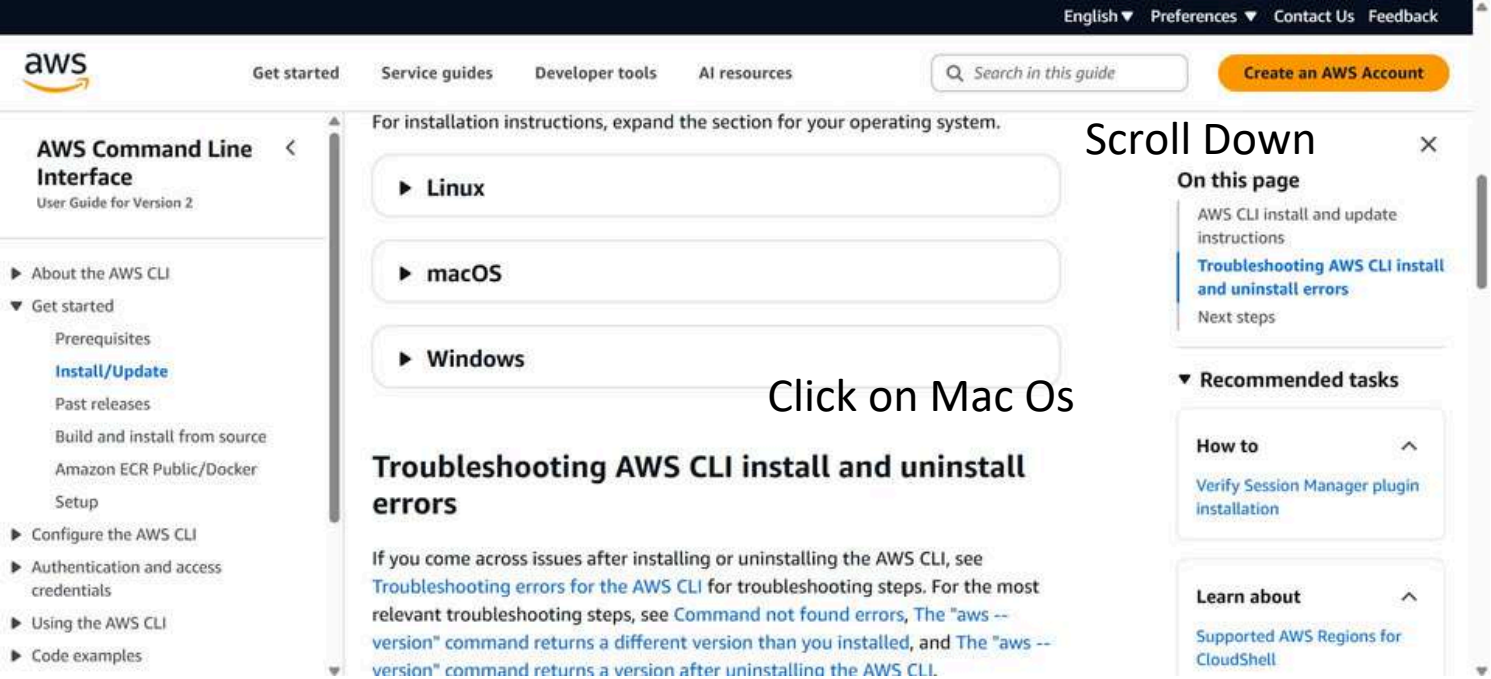
Click on search, command Prompt

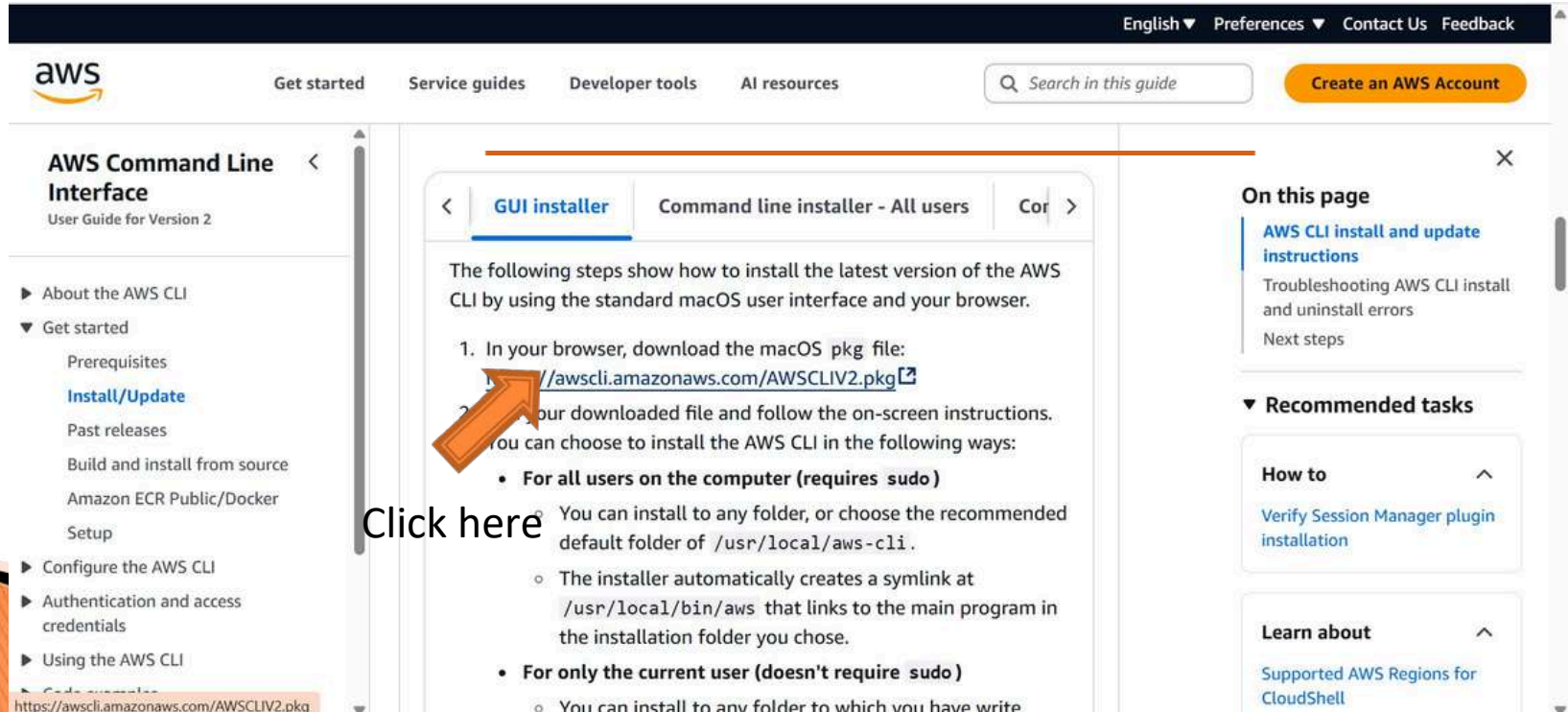


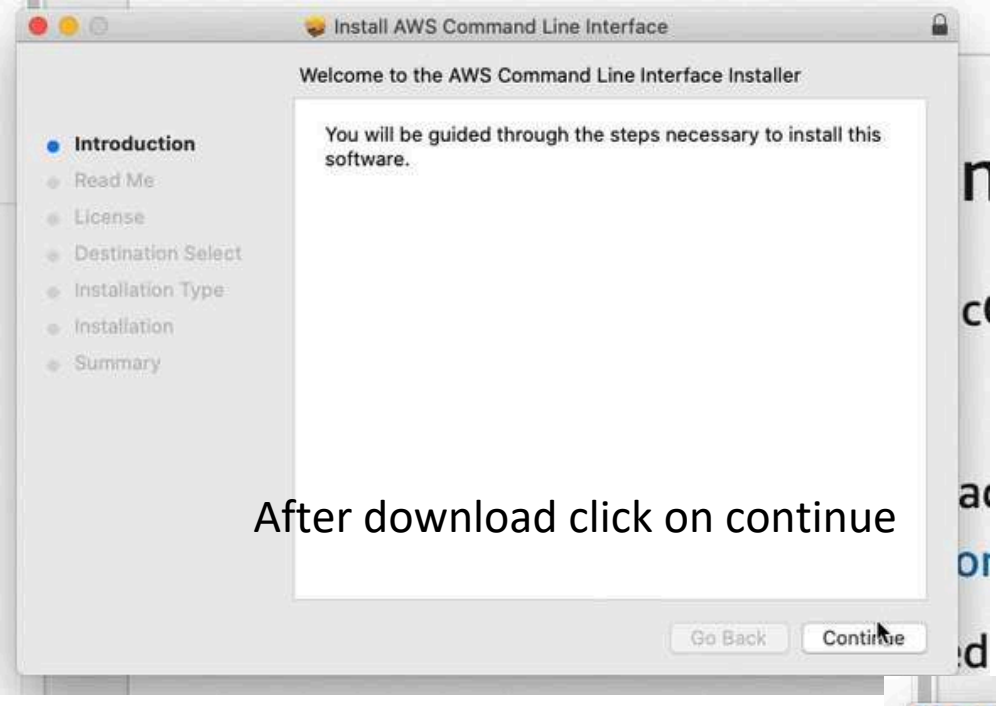

C:\Users\[redacted]s>aws --version
aws-cli/2.27.54 Python/3.13.[redacted]dows/11 exe/AMD64
C:\Users\t[redacted]>
You will see this
Type this & press enter

AWS CLI Setup on Mac OS X

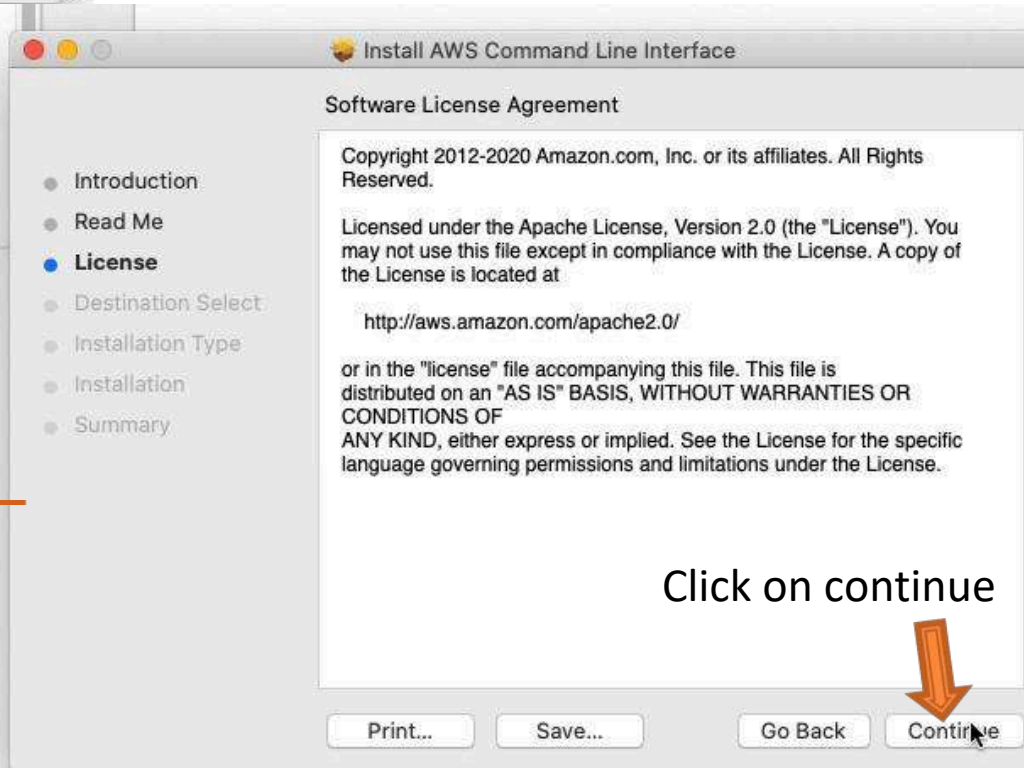



English Preferences Contact Us Feedback
aws
Get started
Service guides
Developer tools
AI resources
Search in this guide
Create an AWS Account
AWS Command Line Interface
User Guide for Version 2
About the AWS CLI
Get started
Prerequisites
Install/Update
Past releases
Build and install from source
Amazon ECR Public/Docker
Setup
Configure the AWS CLI
Authentication and access credentials
Using the AWS CLI
Code examples
For installation instructions, expand the section for your operating system.
Linux
macOS
Windows
Troubleshooting AWS CLI install and uninstall errors
If you come across issues after installing or uninstalling the AWS CLI, see Troubleshooting errors for the AWS CLI for troubleshooting steps. For the most relevant troubleshooting steps, see Command not found errors, The "aws --version" command returns a different version than you installed, and The "aws --version" command returns a version after uninstalling the AWS CLI.
Scroll Down
On this page
AWS CLI install and update instructions
Troubleshooting AWS CLI install and uninstall errors
Next steps
Recommended tasks
How to
Verify Session Manager plugin installation
Learn about
Supported AWS Regions for CloudShell
Click on Mac Os

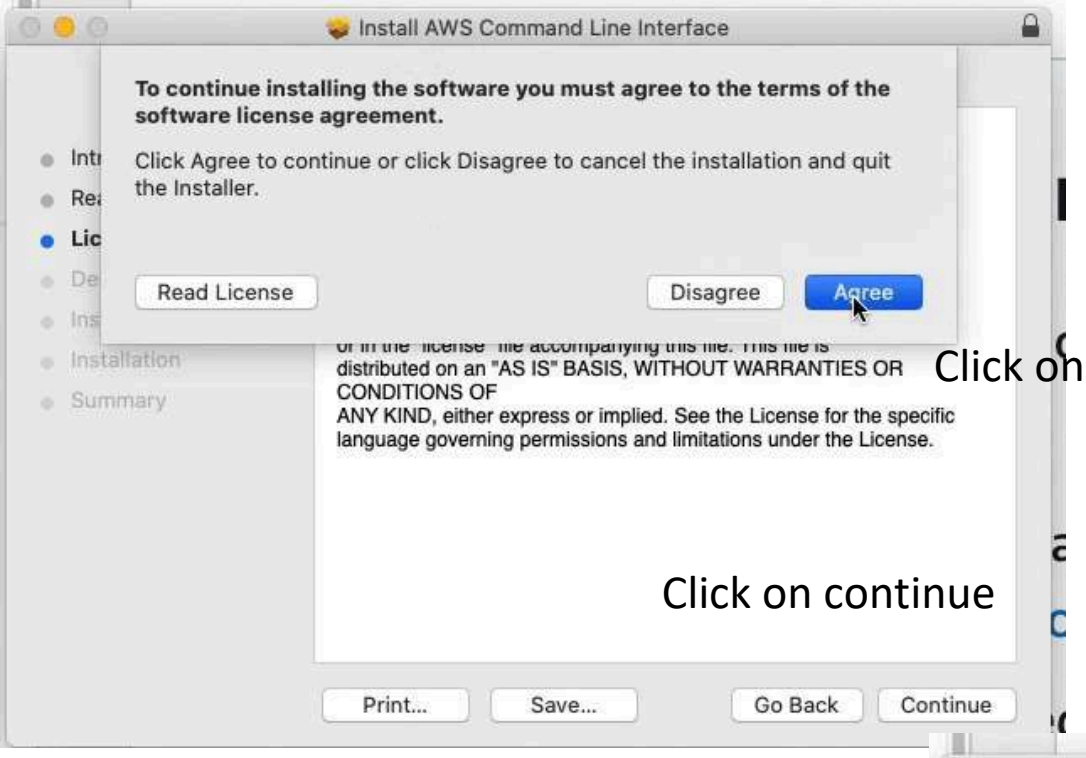

English Preferences Contact Us Feedback
aws
Get started
Service guides
Developer tools
AI resources
Search in this guide
Create an AWS Account
AWS Command Line Interface
User Guide for Version 2
About the AWS CLI
Get started
Prerequisites
Install/Update
Past releases
Build and install from source
Amazon ECR Public/Docker
Setup
Configure the AWS CLI
Authentication and access credentials
Using the AWS CLI
GUI installer
Command line installer - All users
The following steps show how to install the latest version of the AWS CLI by using the standard macOS user interface and your browser.
1. In your browser, download the macOS pkg file:
//awscli.amazonaws.com/AWSCLIV2.pkg
ur downloaded file and follow the on-screen instructions.
ou can choose to install the AWS CLI in the following ways:
For all users on the computer (requires sudo)
You can install to any folder, or choose the recommended default folder of /usr/local/aws-cli.
The installer automatically creates a symlink at /usr/local/bin/aws that links to the main program in the installation folder you chose.
For only the current user (doesn't require sudo)
You can install to any folder to which you have write
Click here
On this page
AWS CLI install and update instructions
Troubleshooting AWS CLI install and uninstall errors
Next steps
Recommended tasks
How to
Verify Session Manager plugin installation
Learn about
Supported AWS Regions for CloudShell
https://awscli.amazonaws.com/AWSCLIV2.pkg



After download click on continue



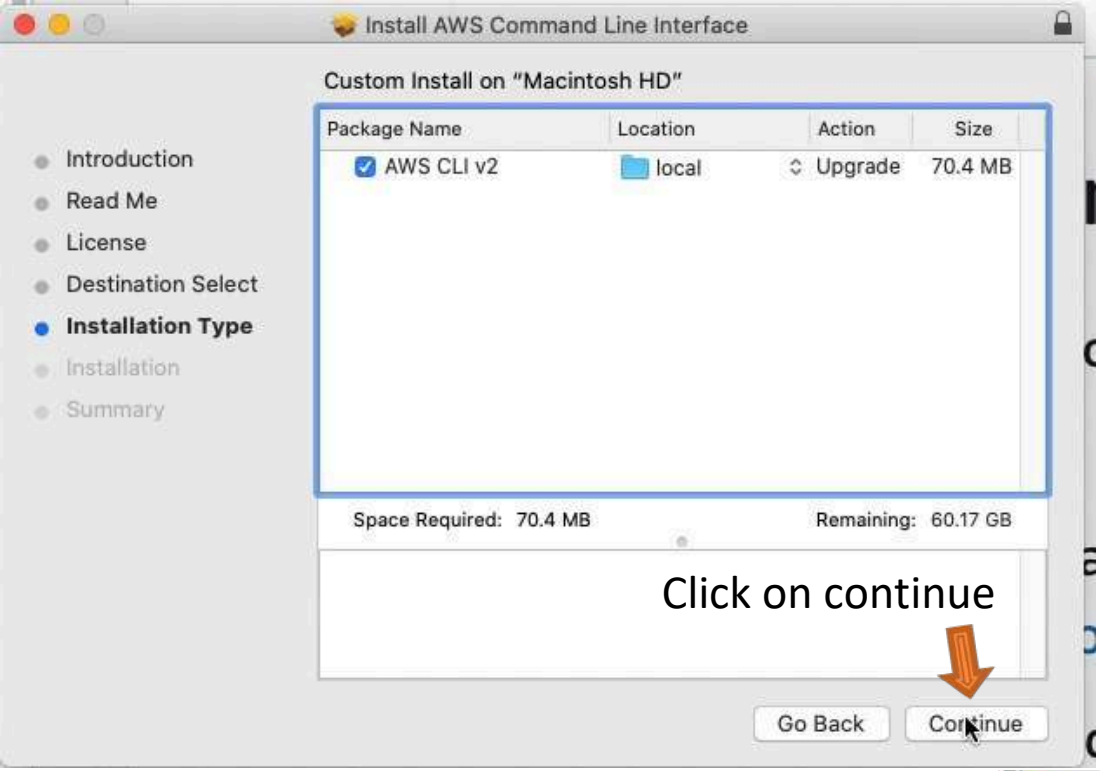
Click on continue



Click on agree

Click on continue

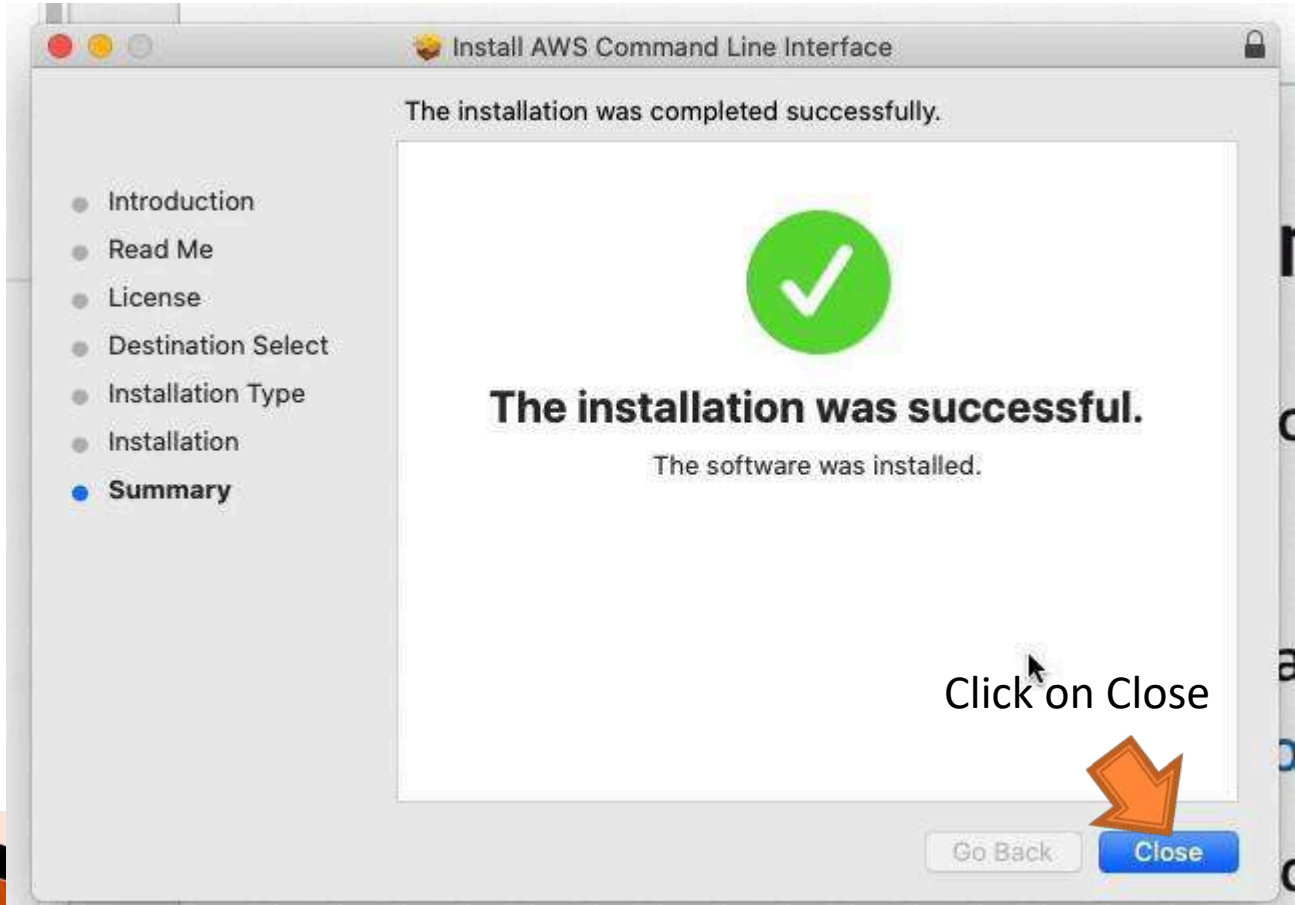
Click on continue


Install AWS Command Line Interface
Custom Install on "Macintosh HD"
Introduction
Read Me
License
Destination Select
Installation Type
Installation
Summary
Package Name
Location
Action
Size
AWS CLI v2
local
Upgrade
70.4 MB
Space Required: 70.4 MB
Remaining: 60.17 GB
Click on continue
Go Back
Continue


Install AWS Command Line Interface
Standard Install on "Macintosh HD"
Introduction
Read Me
License
Destination Select
Installation Type
Installation
Summary
This will take 70.4 MB of space on your computer.
Click Install to perform a standard installation of this software for all users of this computer. All users of this computer will be able to use this software.
Click on Install
Go Back

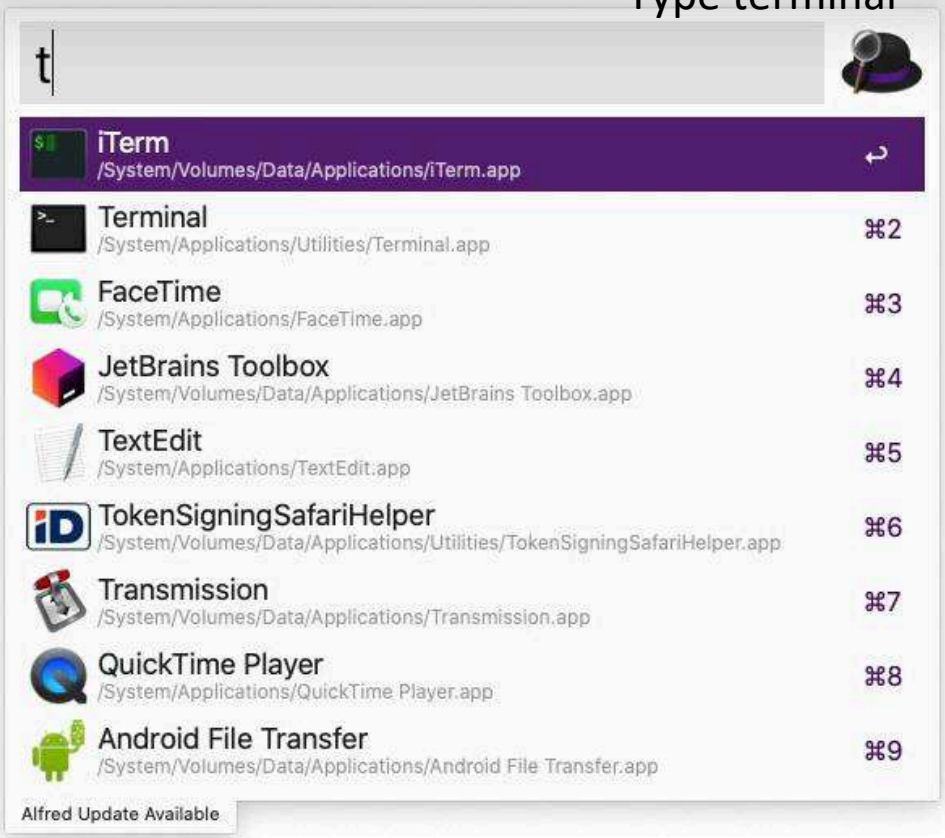
Enter password

Click on install software



Click on Close

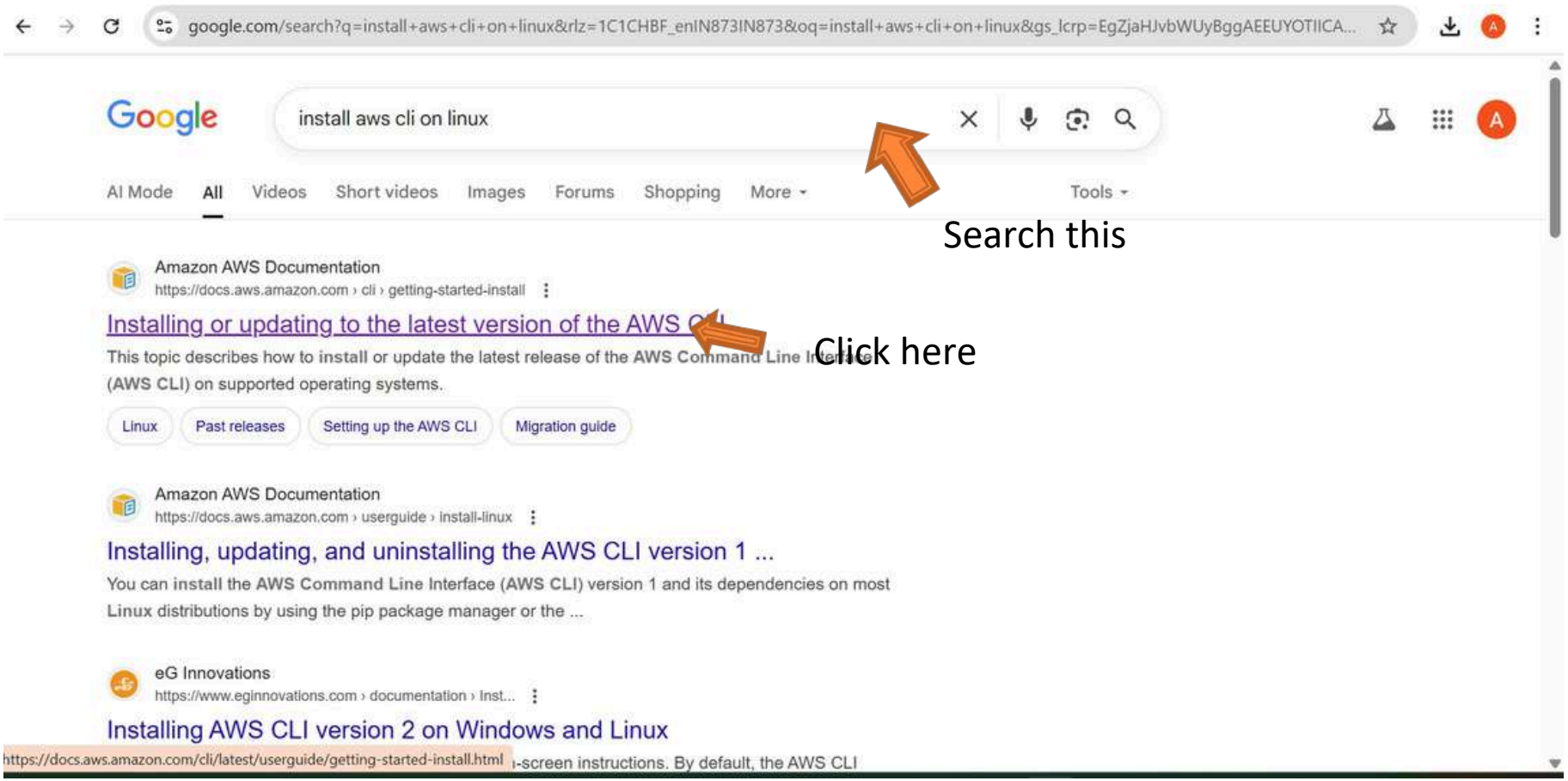
Type terminal

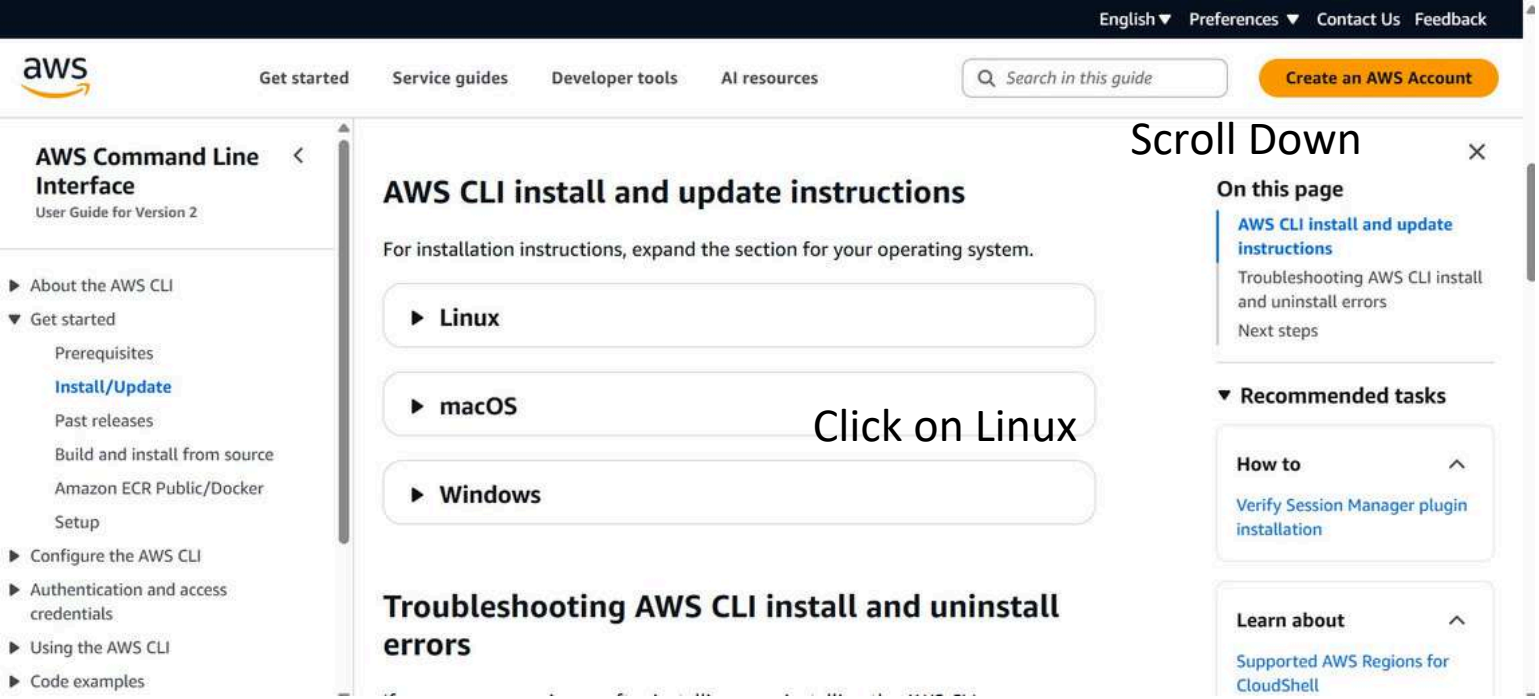


Type this & press enter

It will show this when cli is installed

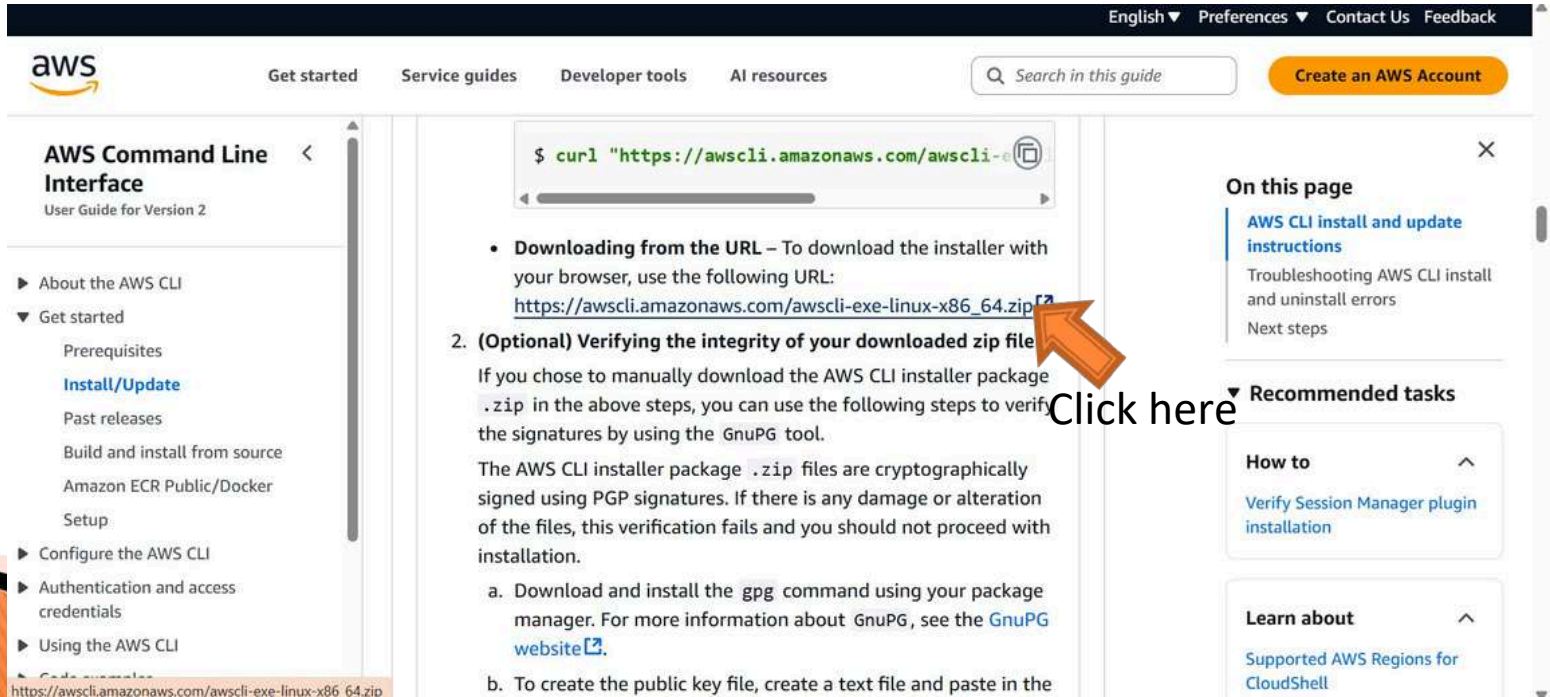
AWS CLI Setup on Linux





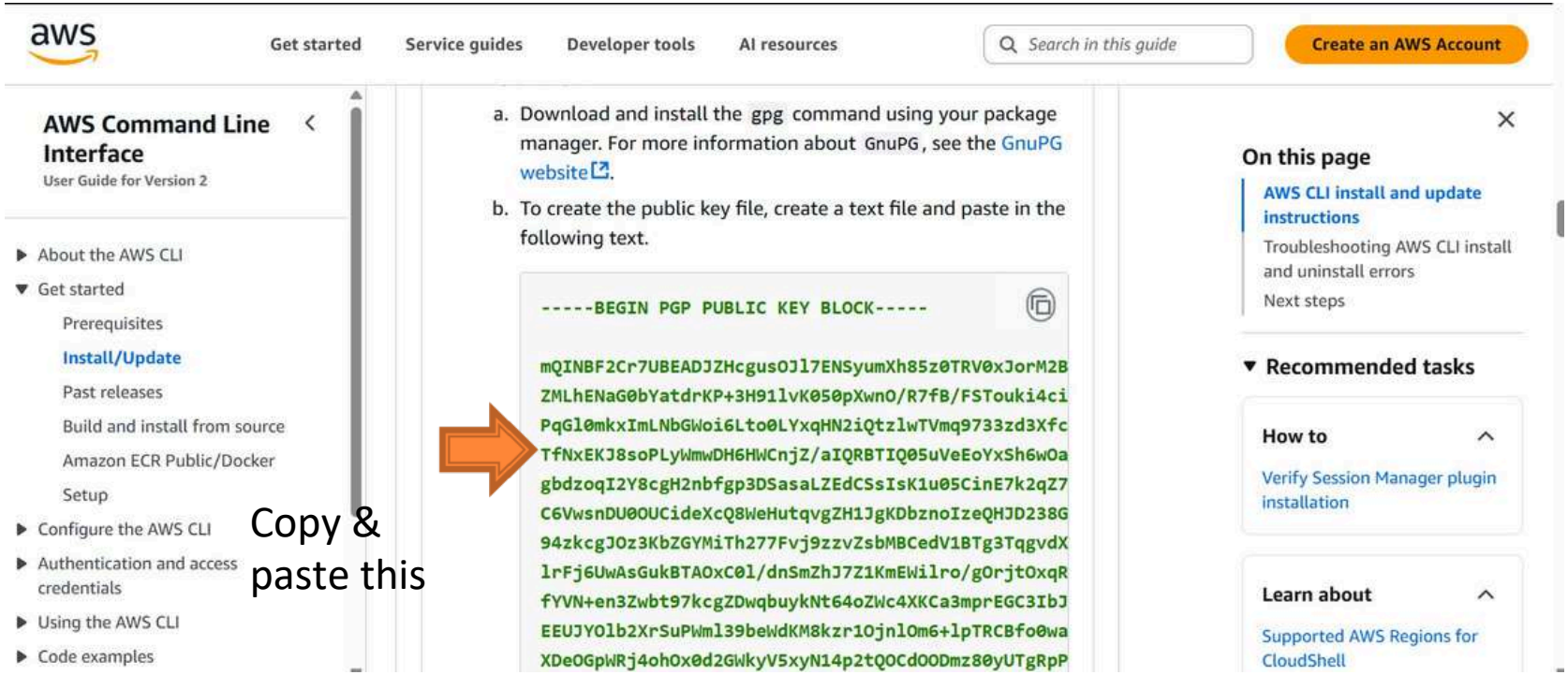
Scroll Down

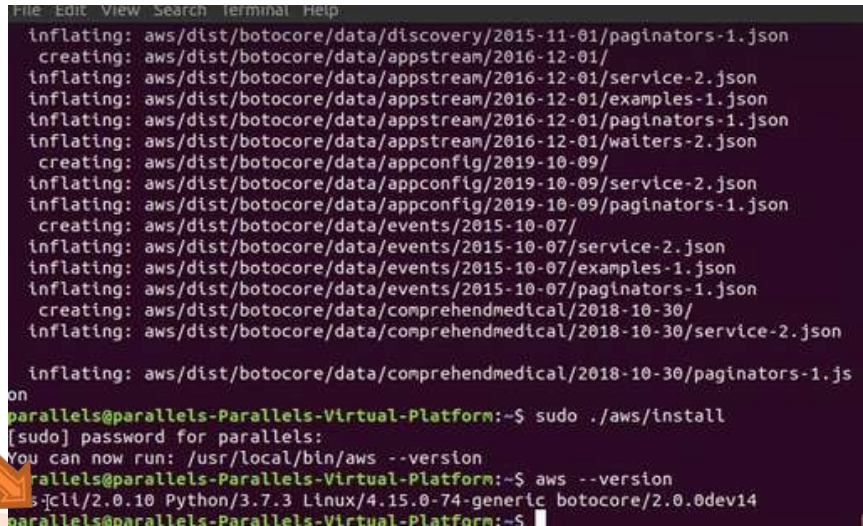
Click on Linux



Click here

Do whole process

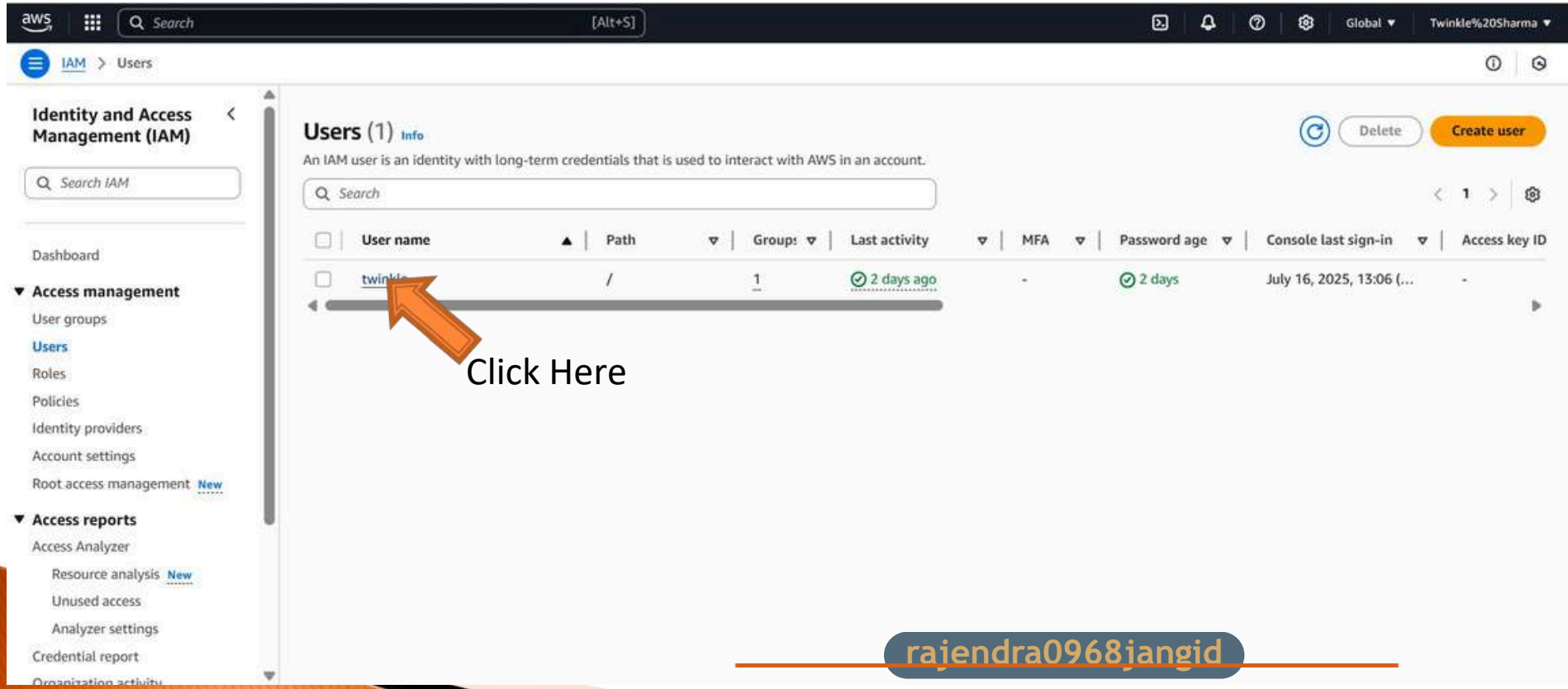


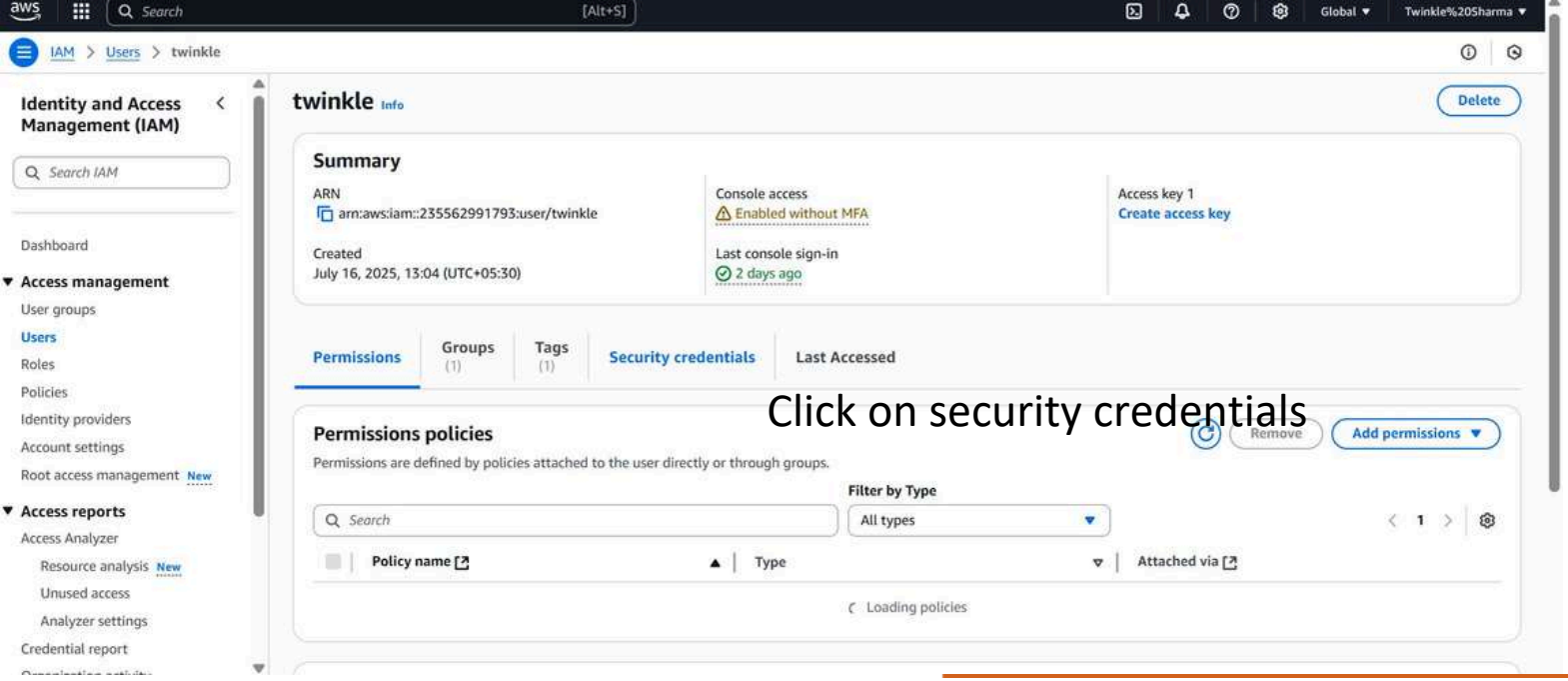


At last type this you will get the version of CLI

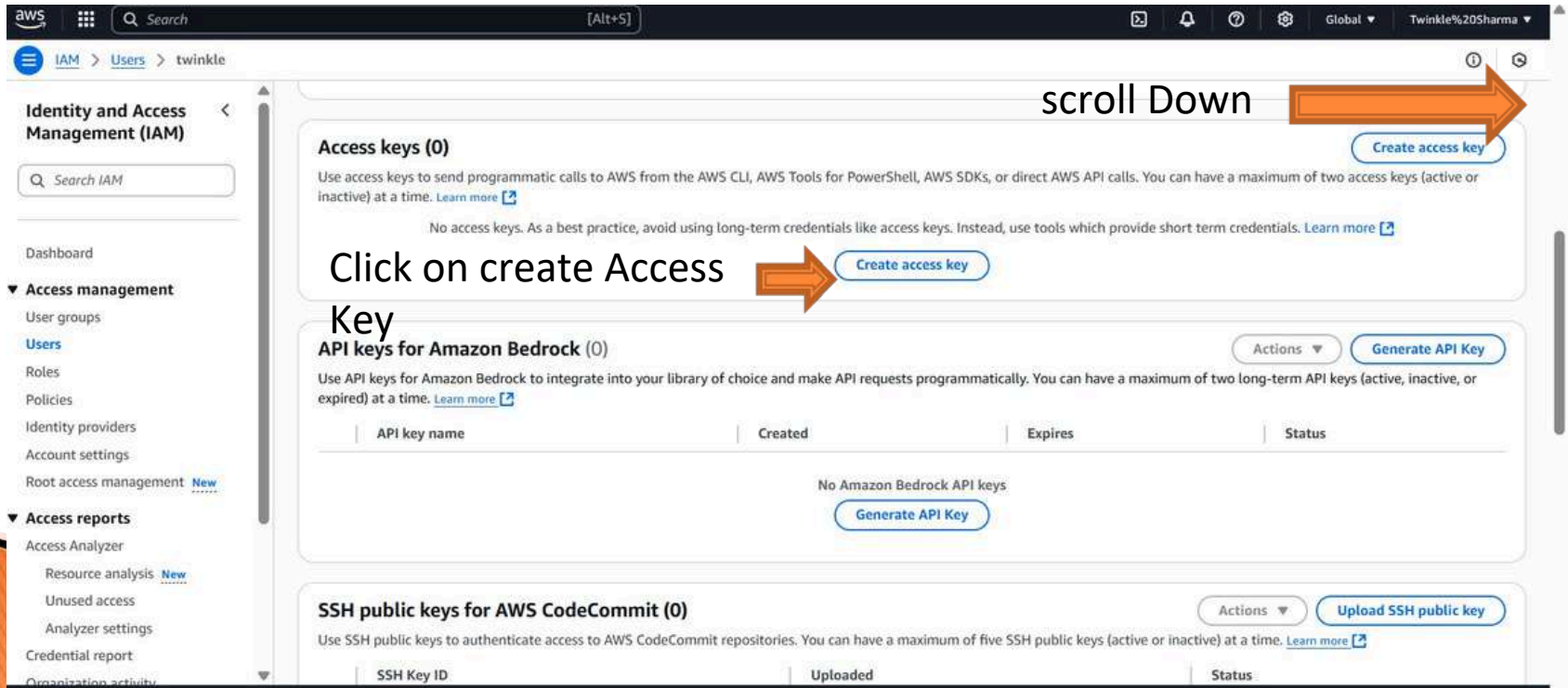
AWS CLI – Hands On

- Go to aws console
- Go to IAM than to Users

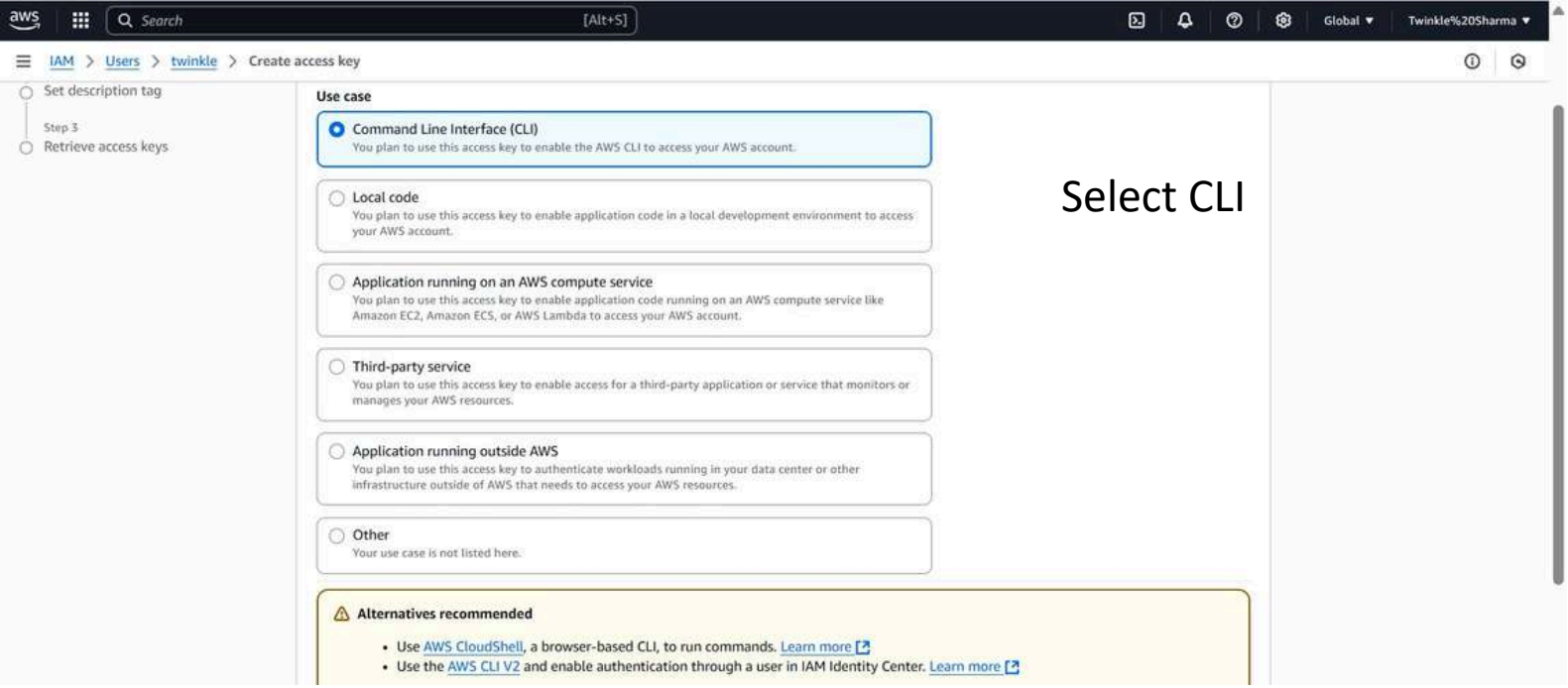




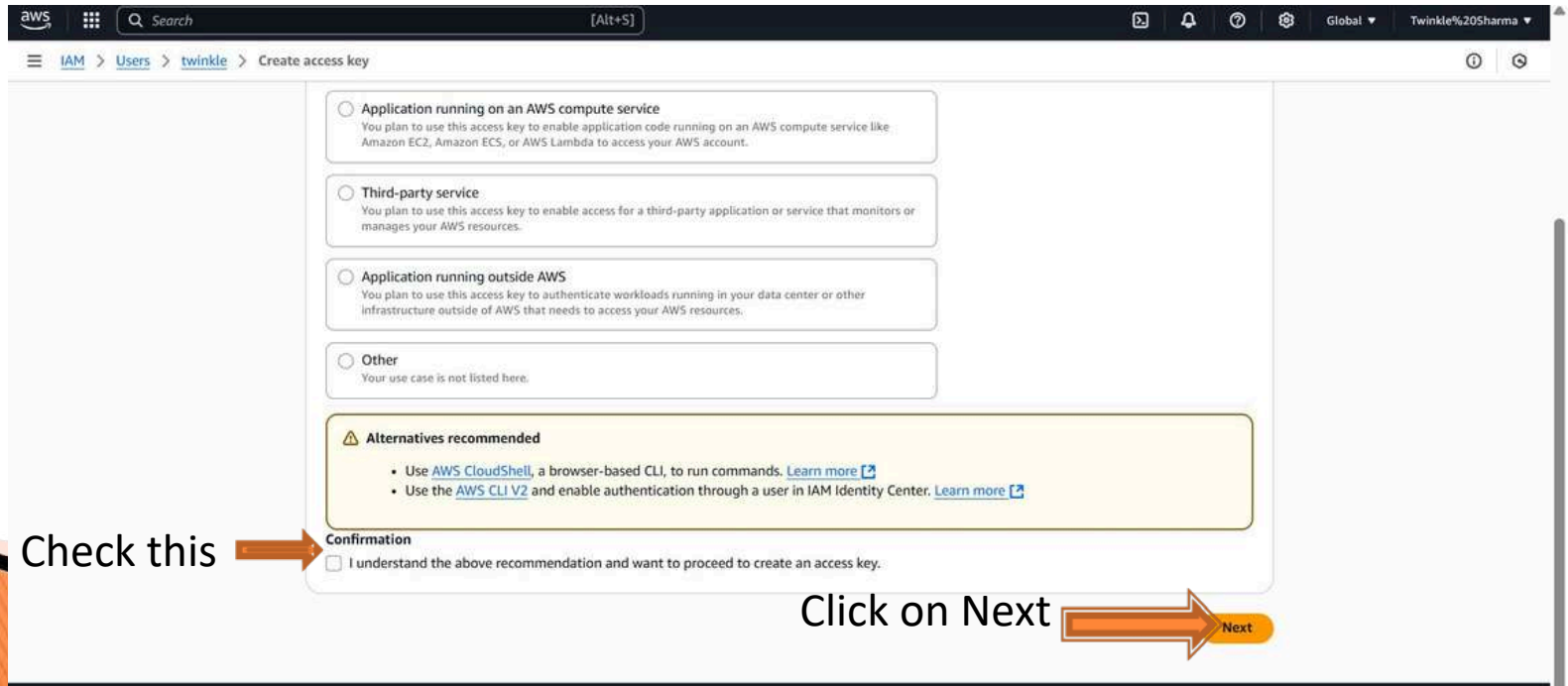
Click on security credentials



Click on create Access Key

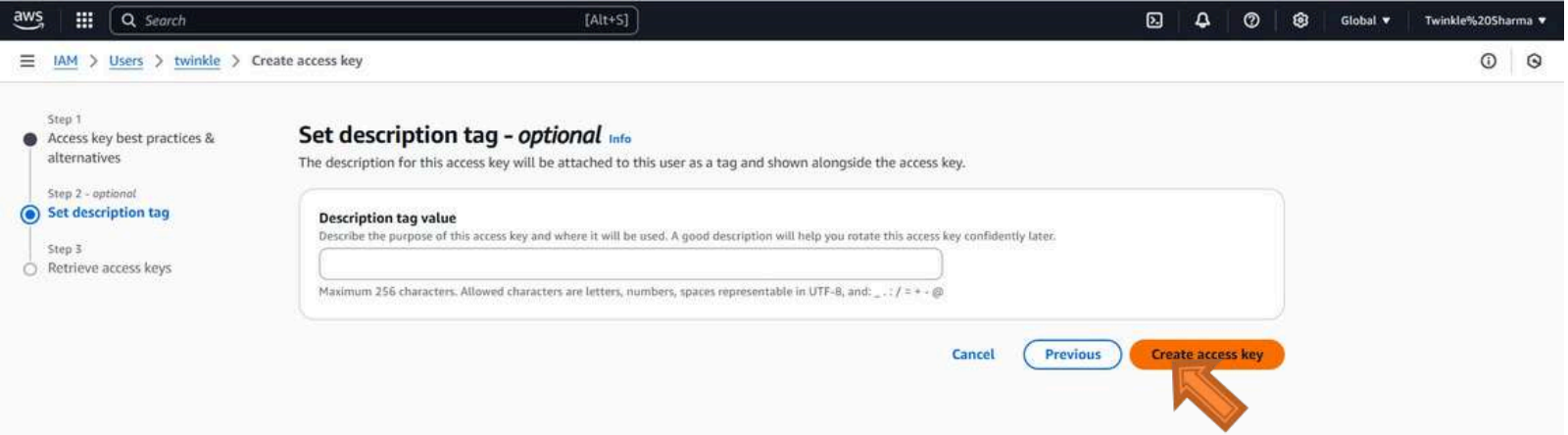


Select CLI



Check this

Click on Next



Click on create access key

Aftercreatingaccesskeycopy&pasteyouraccesskeyinnotepad- go to command prompt

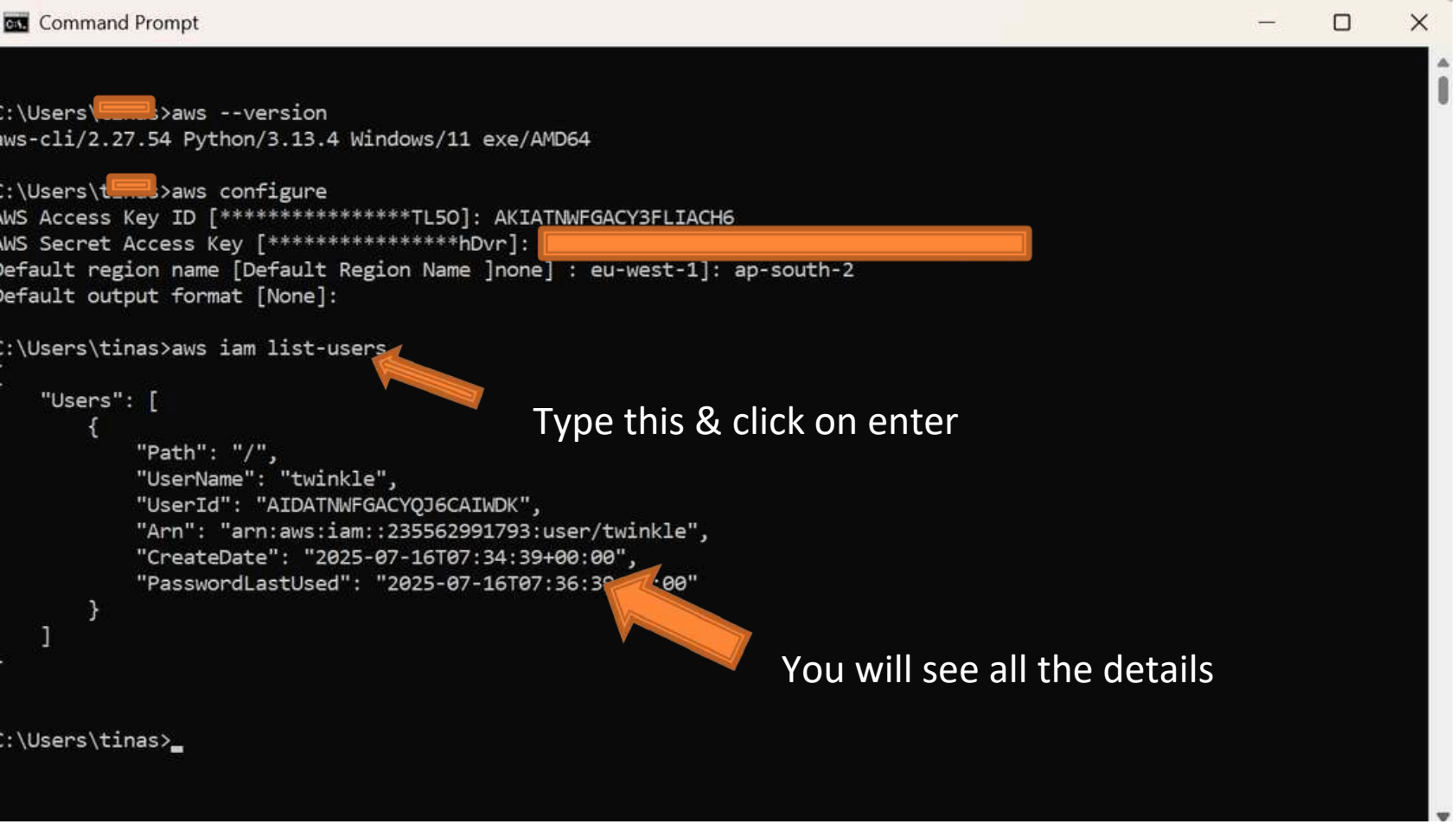
Type AWS Configure

```
C:\Users\tinas>aws --version
aws-cli/2.27.54 Python/3.13.4 Windows/11 exe/AMD64

C:\Users\tinas>aws configure
AWS Access Key ID [****************TL5O]: AKIATNWFGACY3FLIACH6
AWS Secret Access Key [****************hDvr]: [redacted]
```

Paste your access key ID & access secret key

```
C:\Users\t[redacted]>aws --version
aws-cli/2.27.54 Python/3.13.4 Windows/11 exe/AMD64

C:\Users\t[redacted]>aws configure
AWS Access Key ID [****************TL5O]: AKIATNWFGACY3FLIACH6
AWS Secret Access Key [****************hDvr]: [redacted]
Default region name [Default Region Name ]none] : eu-west-1]: ap-south-2
Default output format [None]:
```

Enter region



rajendra0968jangid

AWS Cloudshell

- It’s a pre-authenticated shell environment provided by AWS, accessible through the console, with built-in tools like the AWS CLI, Python, Node.js, Git, and more.
- KeyFeaturesof CloudShell

Feature	Description
✅ **Pre-authenticated**	No need to configure credentials — uses the IAM role of your console user
✅ **Built-in CLI & SDKs**	AWS CLI v2, Python, Node.js, and more pre-installed
✅ **Persistent storage**	1 GB of persistent home directory (`~/`) storage per region
✅ **Runs in browser**	No software installation needed
✅ **Multi-region support**	Each region has its own shell environment
✅ **Free to use**	No cost for usage (within limits)

AWS Cloudshell – Region Availability

https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html

Find this list here

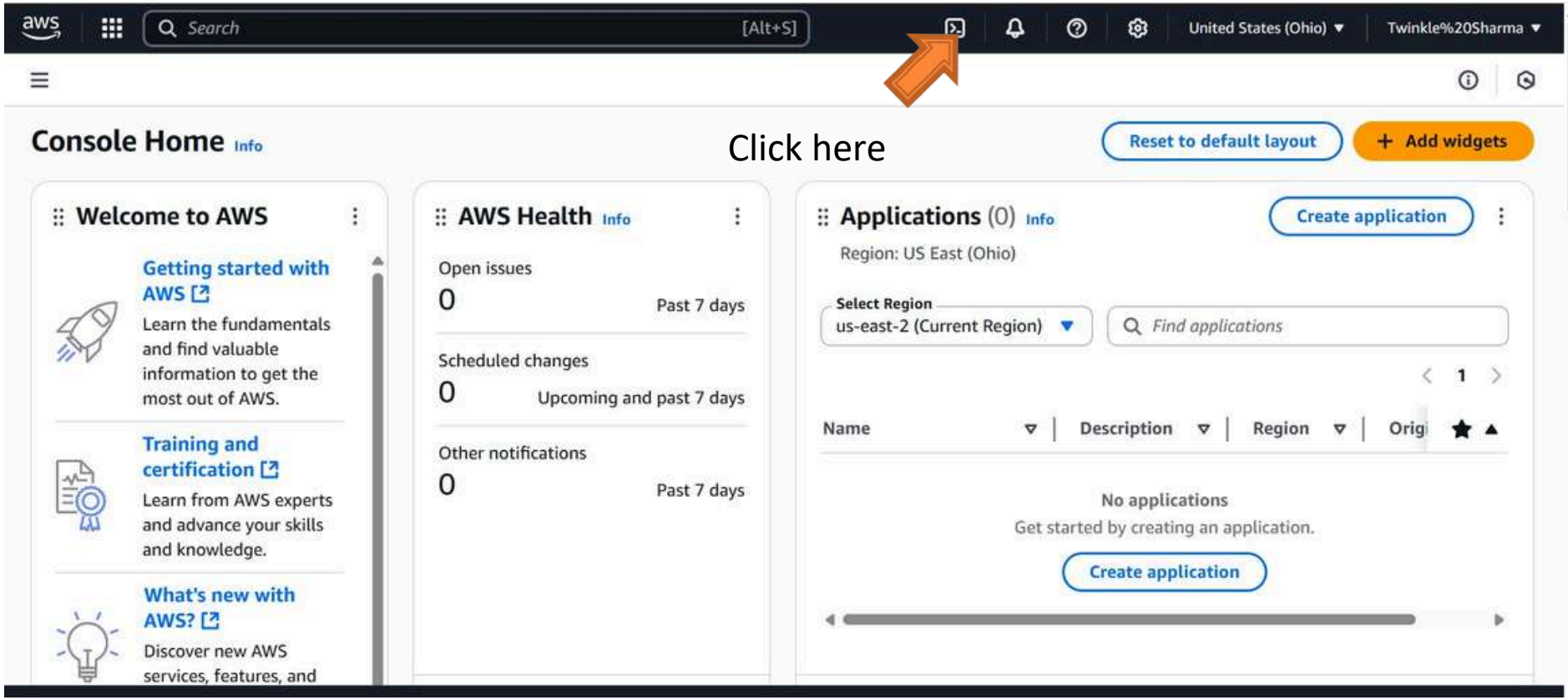
It is not yet available in all regions, and you can find the region list

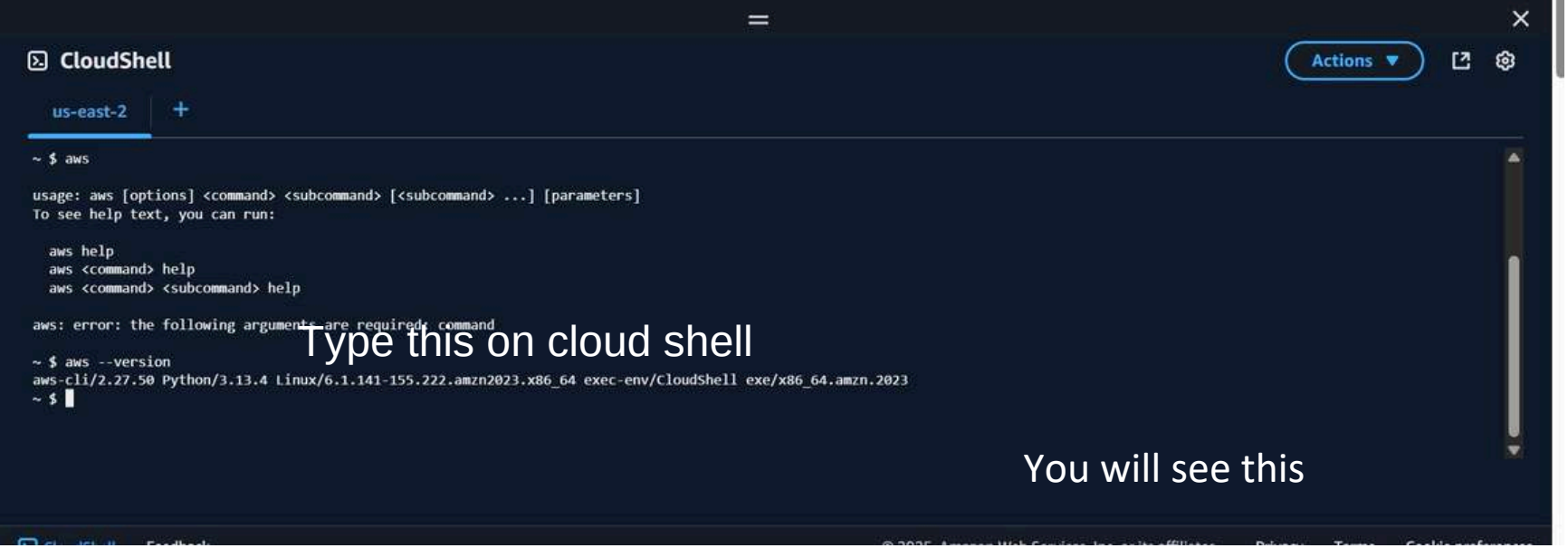
The following are the supported AWS Regions for CloudShell, Docker, and CloudShell VPC environment:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Jakarta)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Milan)
- Europe (Paris)
- Europe (Stockholm)
- Middle East (Bahrain)
- Middle East (UAE)
- South America (São Paulo)

Please switch to one of these regions if you want to do the next (optional) hands-on.

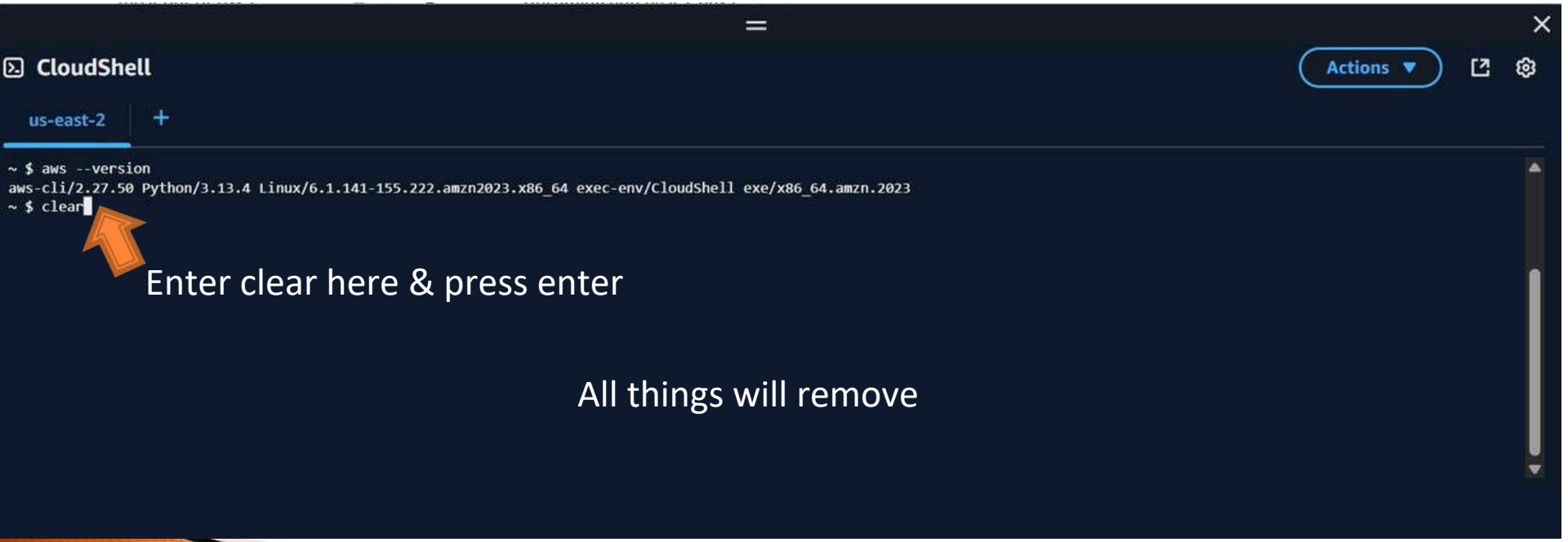
AWS Cloudshell





Type this on cloud shell

You will see this



Enter clear here & press enter

All things will remove

CloudShell

Actions

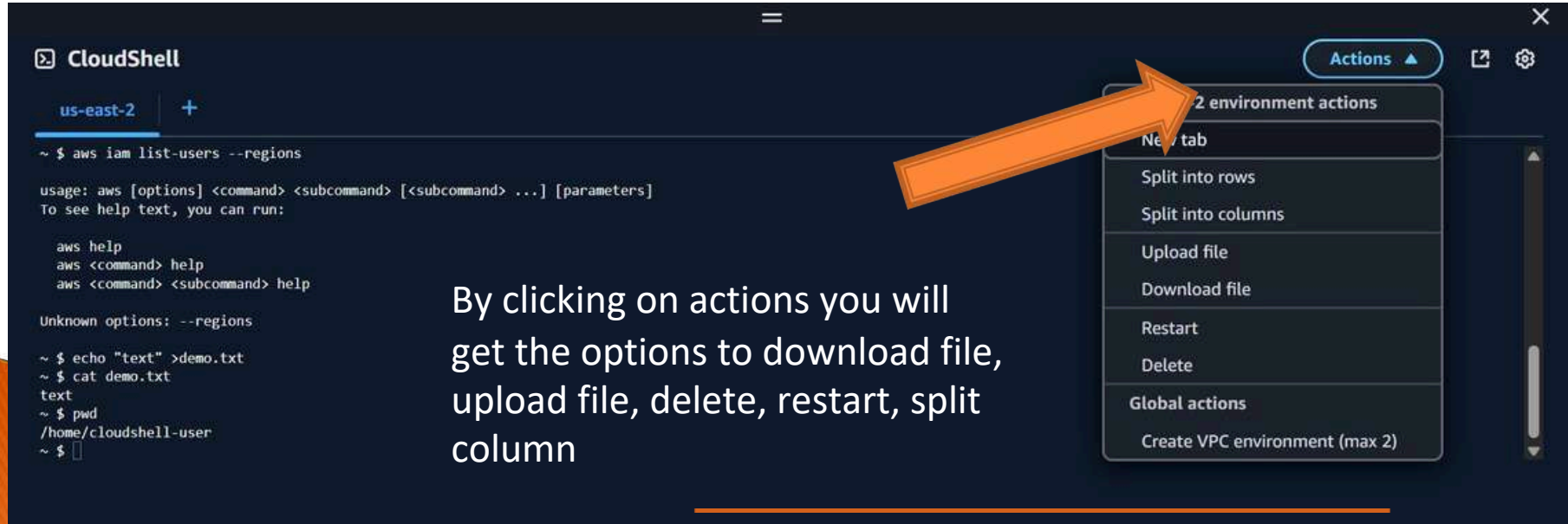
us-east-2

```
~ $ aws iam list-users
{
    "Users": [
        {
            "Path": "/",
            "UserName": "twinkle",
            "UserId": "AIDATNWFGACYQJ6CAIWDK",
            "Arn": "arn:aws:iam::235562991793:user/twinkle",
            "CreateDate": "2025-07-16T07:34:39+00:00",
            "PasswordLastUsed": "2025-07-16T07:36:39+00:00"
        }
    ]
}
```

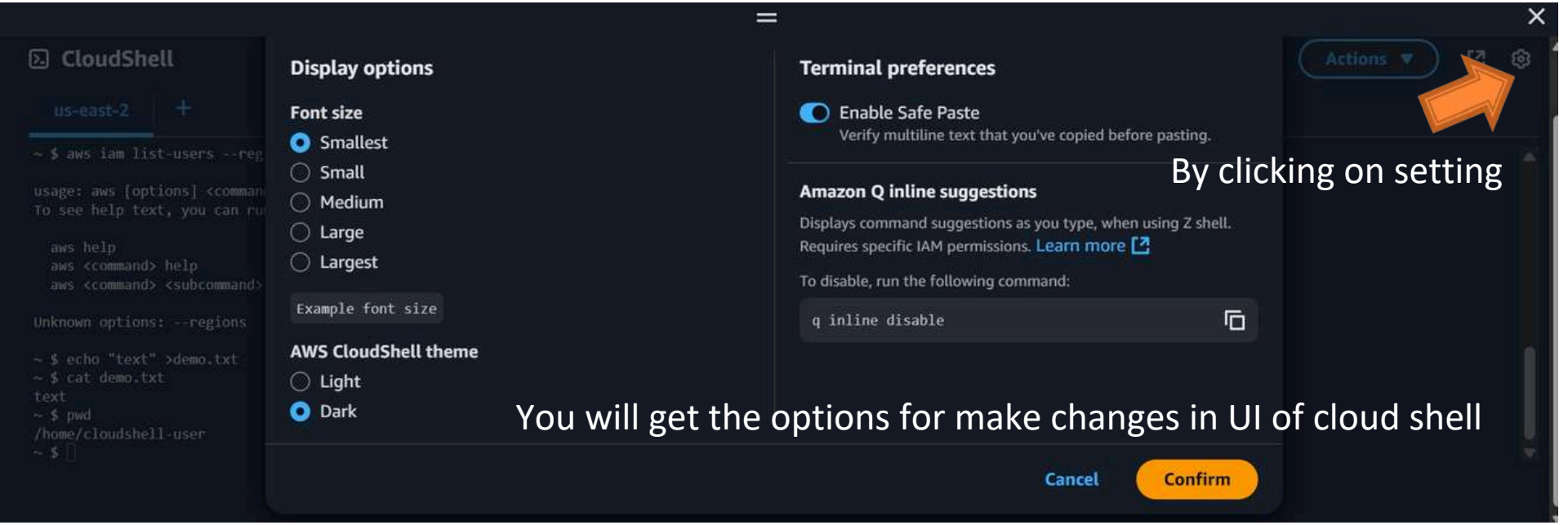
By typing this you will get the user details as in commandprompt

```
~ $ echo "text" >demo.txt
~ $ cat demo.txt
text
~ $ pwd
/home/cloudshell-user
~ $
```

By this tags it is going to create text file



By clicking on actions you will get the options to download file, upload file, delete, restart, split column



By clicking on setting

You will get the options for make changes in UI of cloud shell

IAM Roles For AWS Services

- IAM Roles in AWS are temporary permission sets that allow AWS services, applications, or users to access resources securely without using long-term credentials (like access keys).

They are essential when:

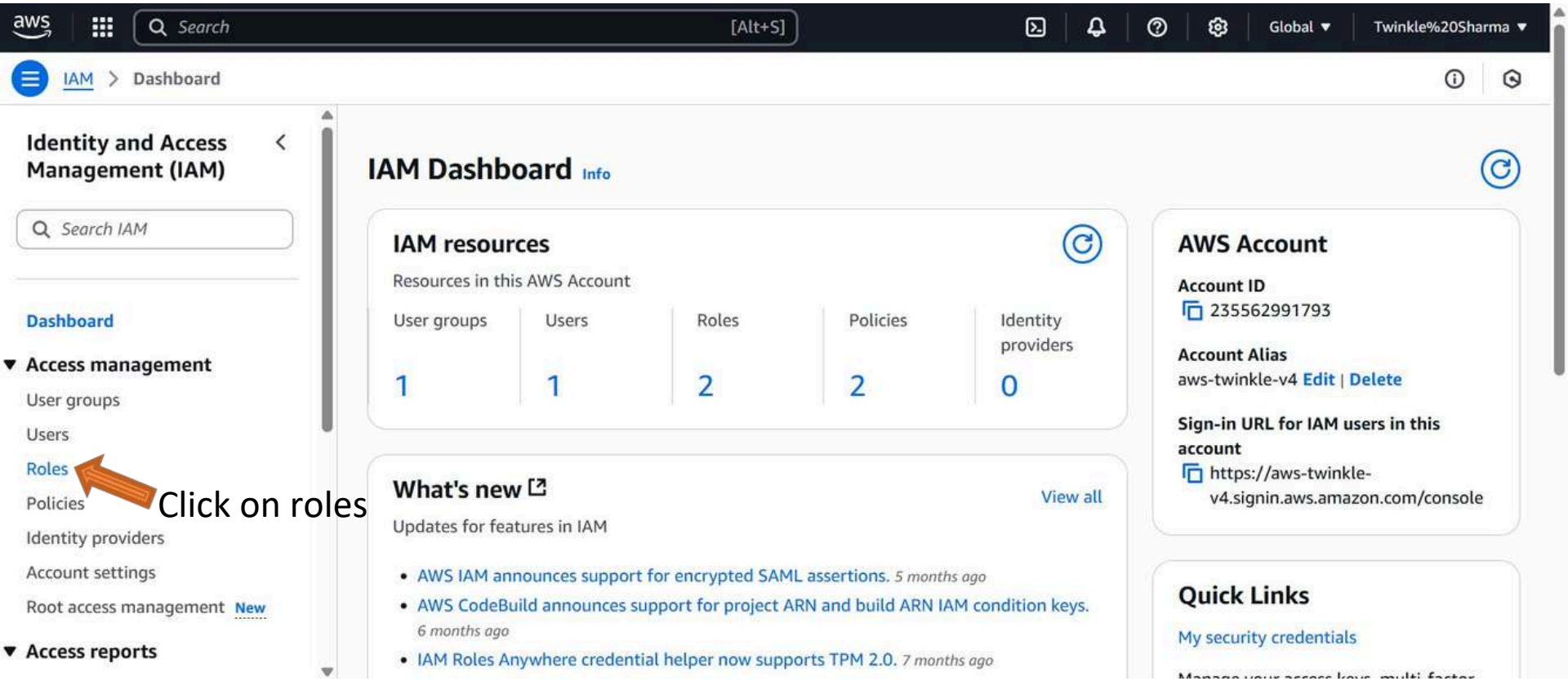
- An EC2 instance needs to access S3 or DynamoDB
- A Lambda function needs to read from a database
- An ECS task or Glue job needs access to other AWS resources

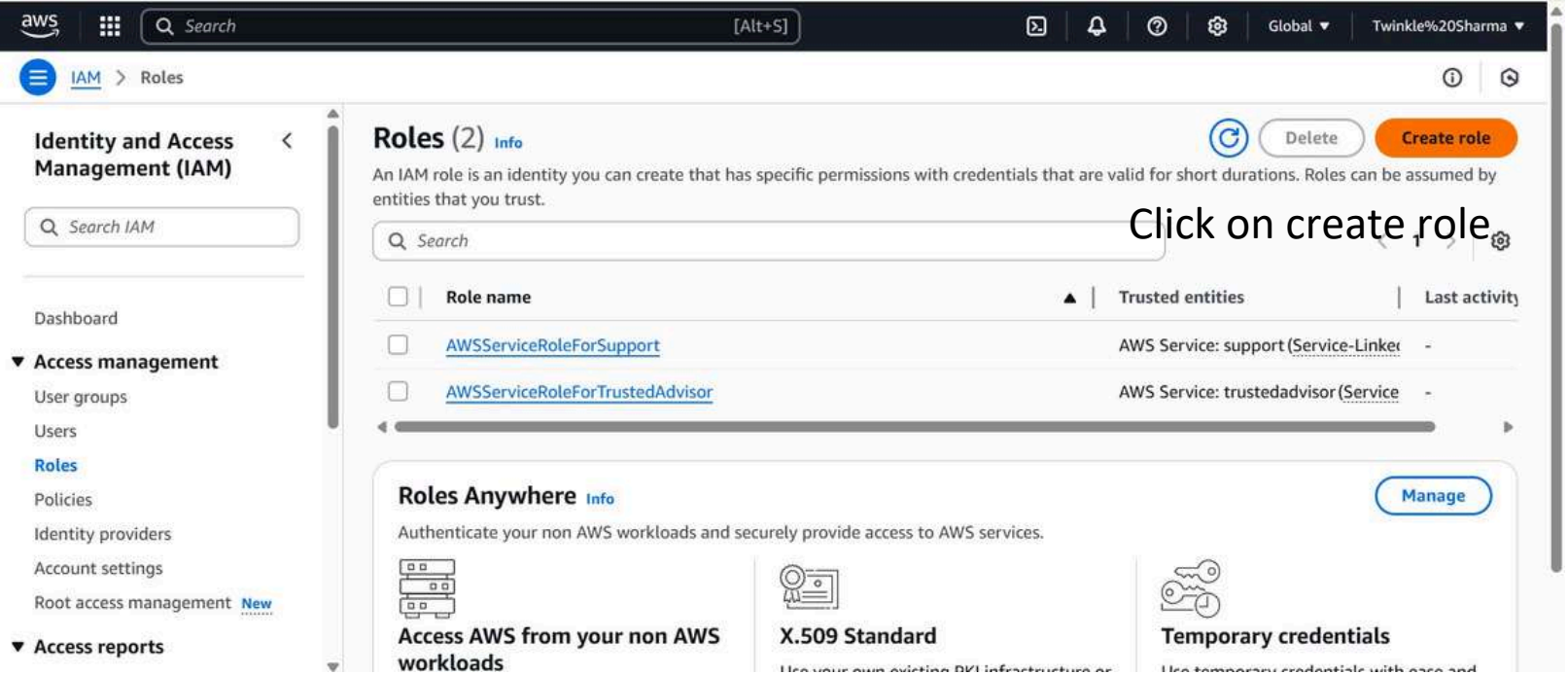
How AWS Services Use IAM Roles

Here's how some common AWS services use IAM roles:

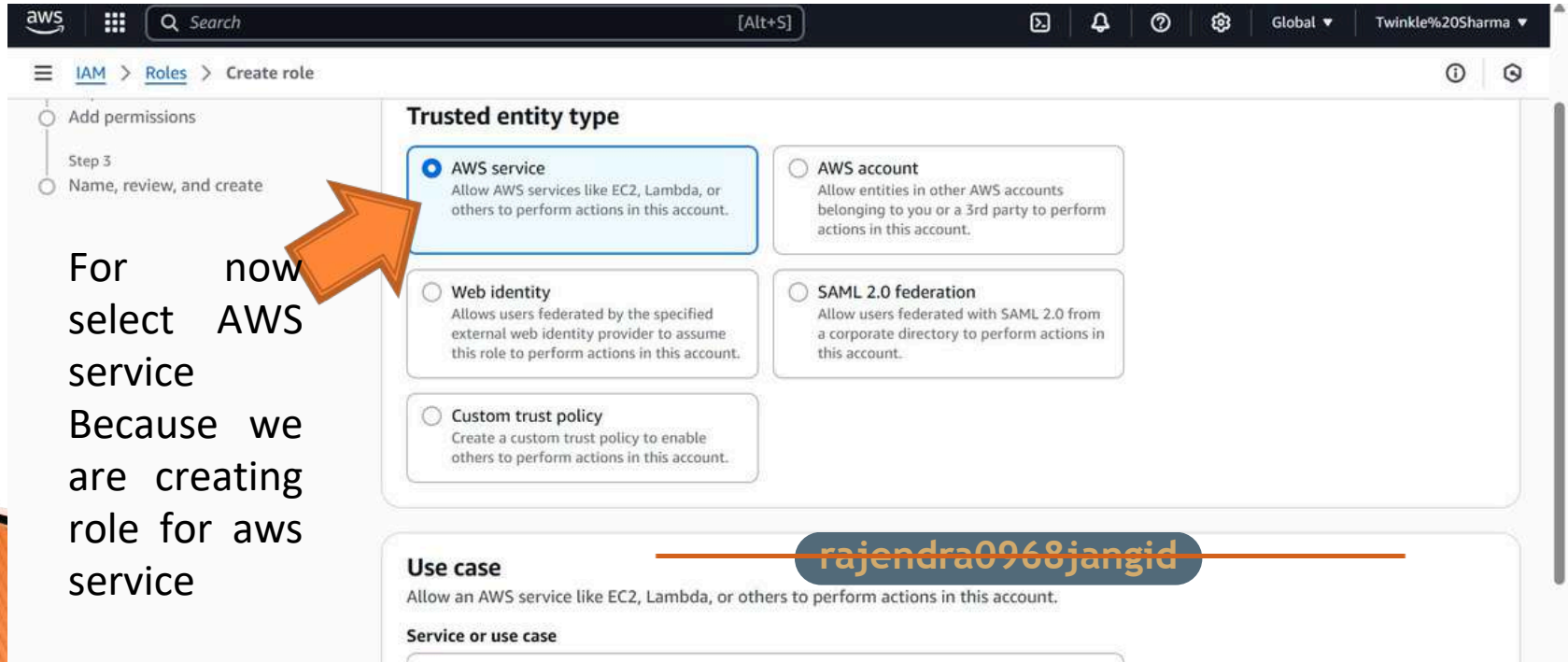
AWS Service	Role Used For	Example Action
EC2	EC2 instance profile (instance role)	Read/write S3, access secrets
Lambda	Execution role	Access DynamoDB or SNS
ECS Tasks	Task execution role	Pull container images, logs
Glue	Job role	Read from S3, write to Redshift
CodeBuild	Build role	Access S3, CodeCommit, ECR
SageMaker	Execution role	Access training data in S3
Step Functions	State machine role	Invoke Lambda, access DynamoDB
CloudFormation	Service role	Create/delete AWS resources

IAM Roles Hands On

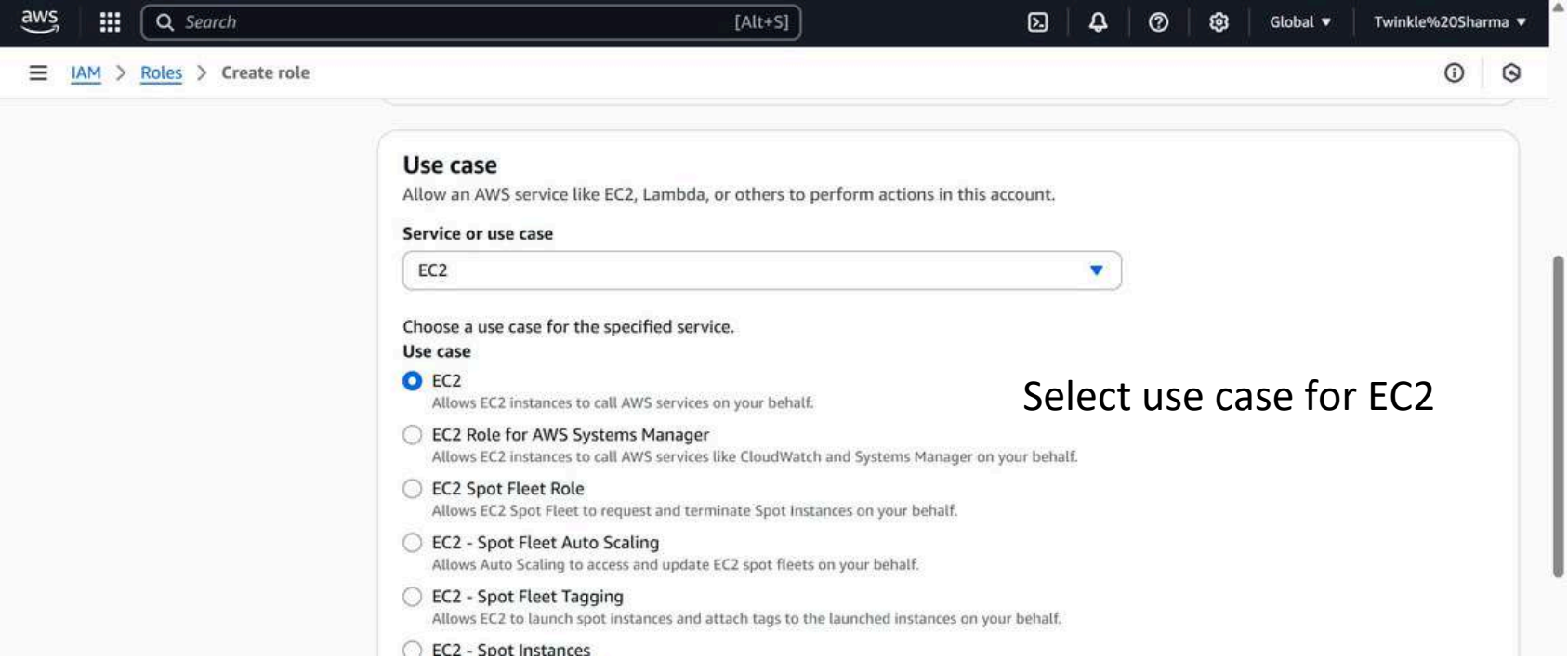




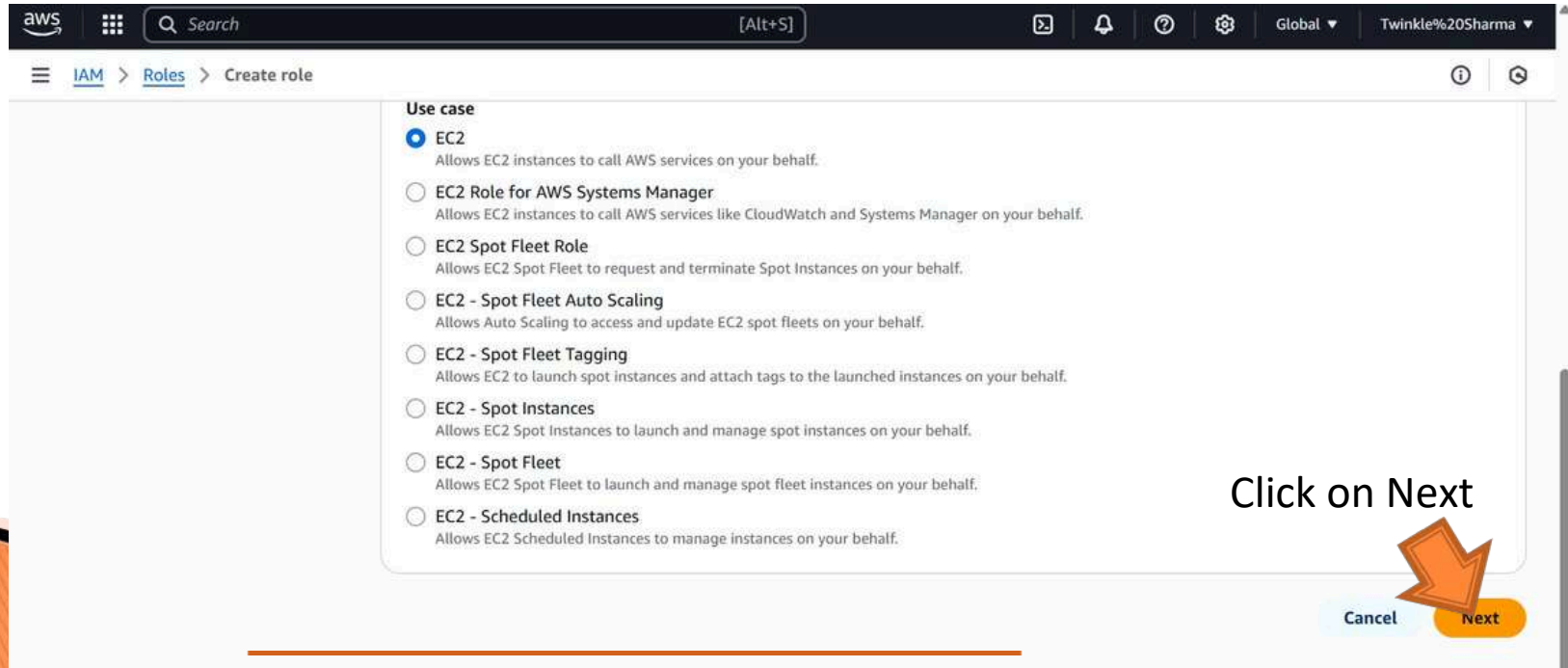
Click on create role



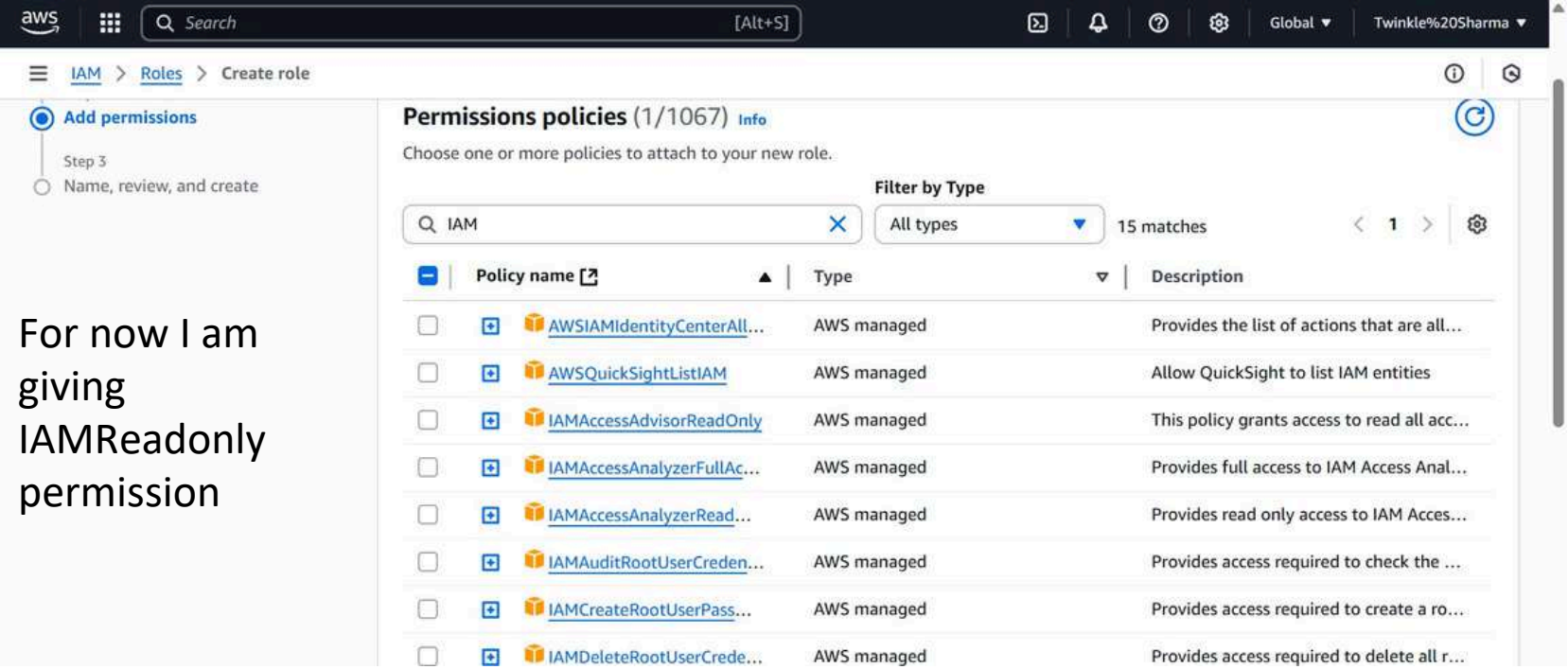
For now select AWS service Because we are creating role for aws service



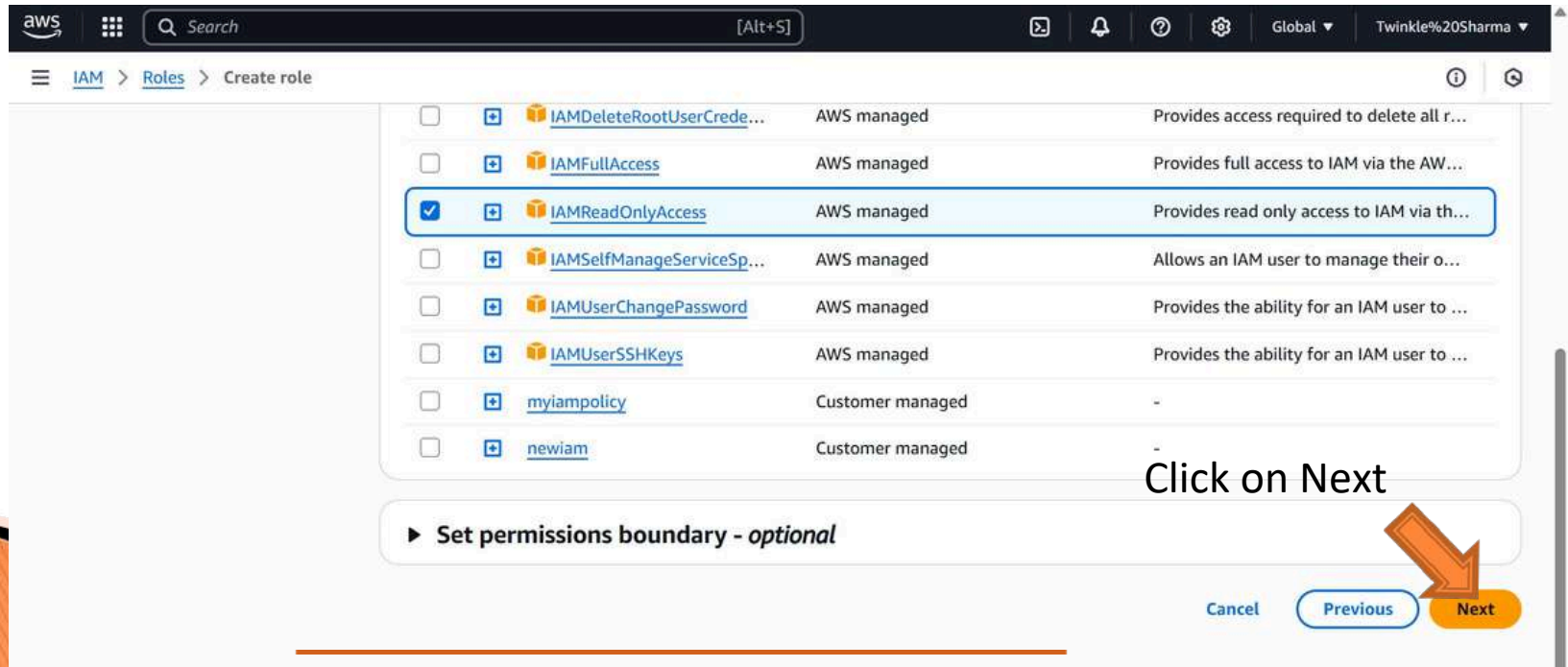
Select use case for EC2



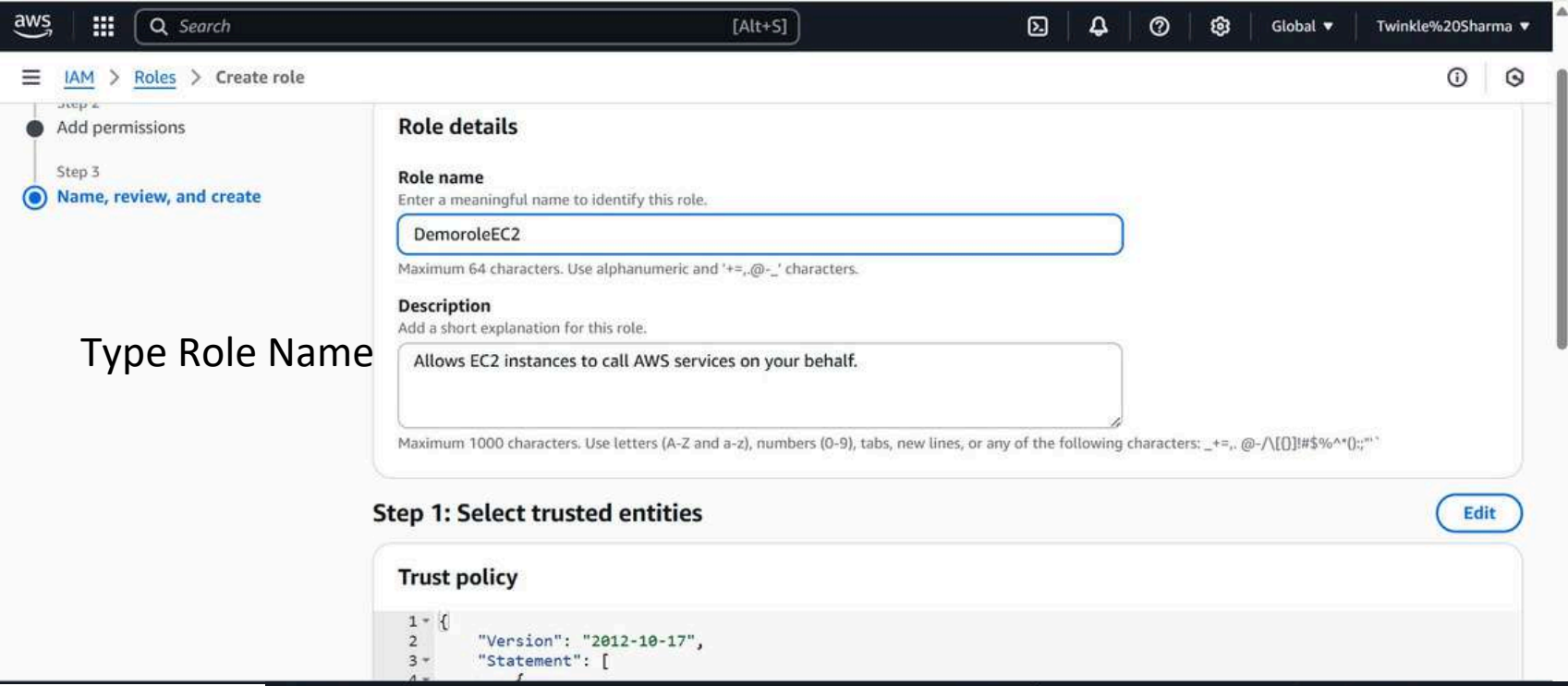
Click on Next



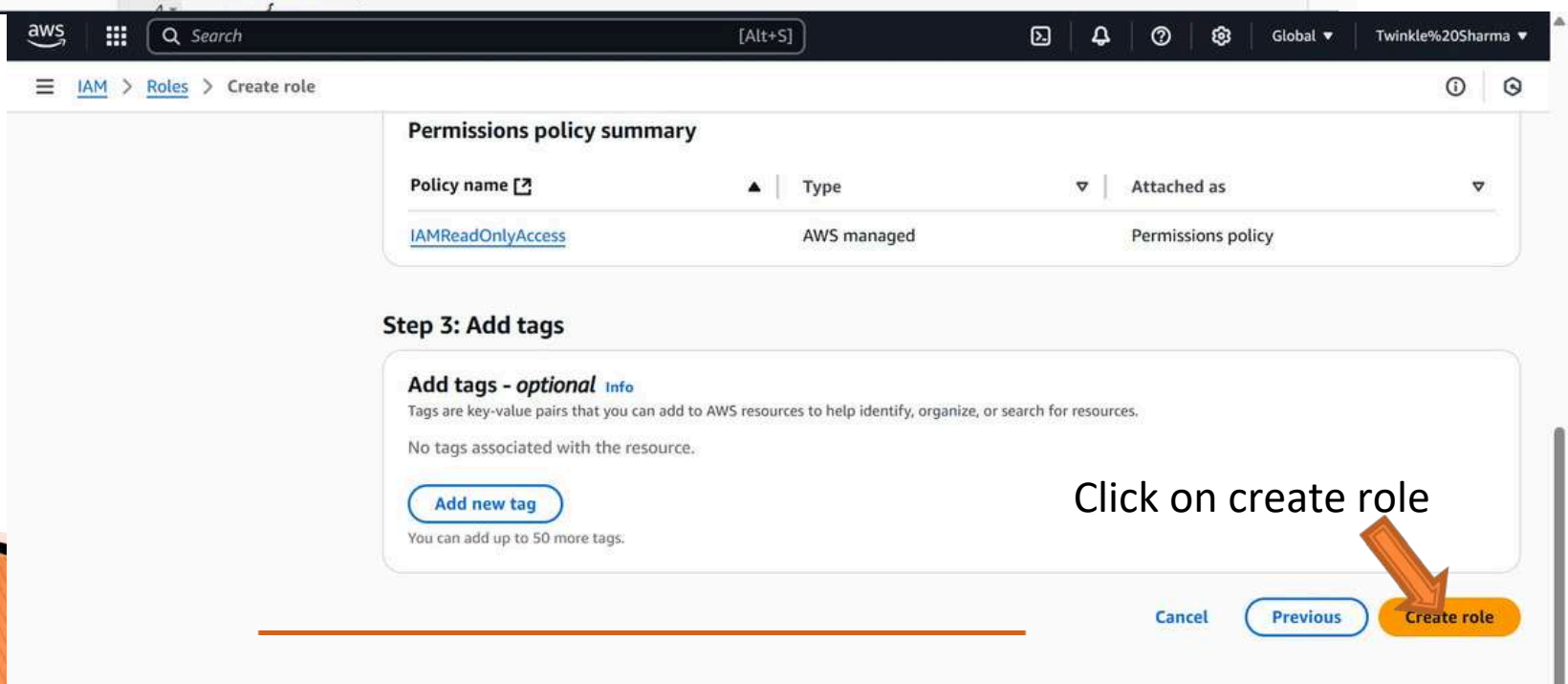
For now I am giving IAMReadonly permission



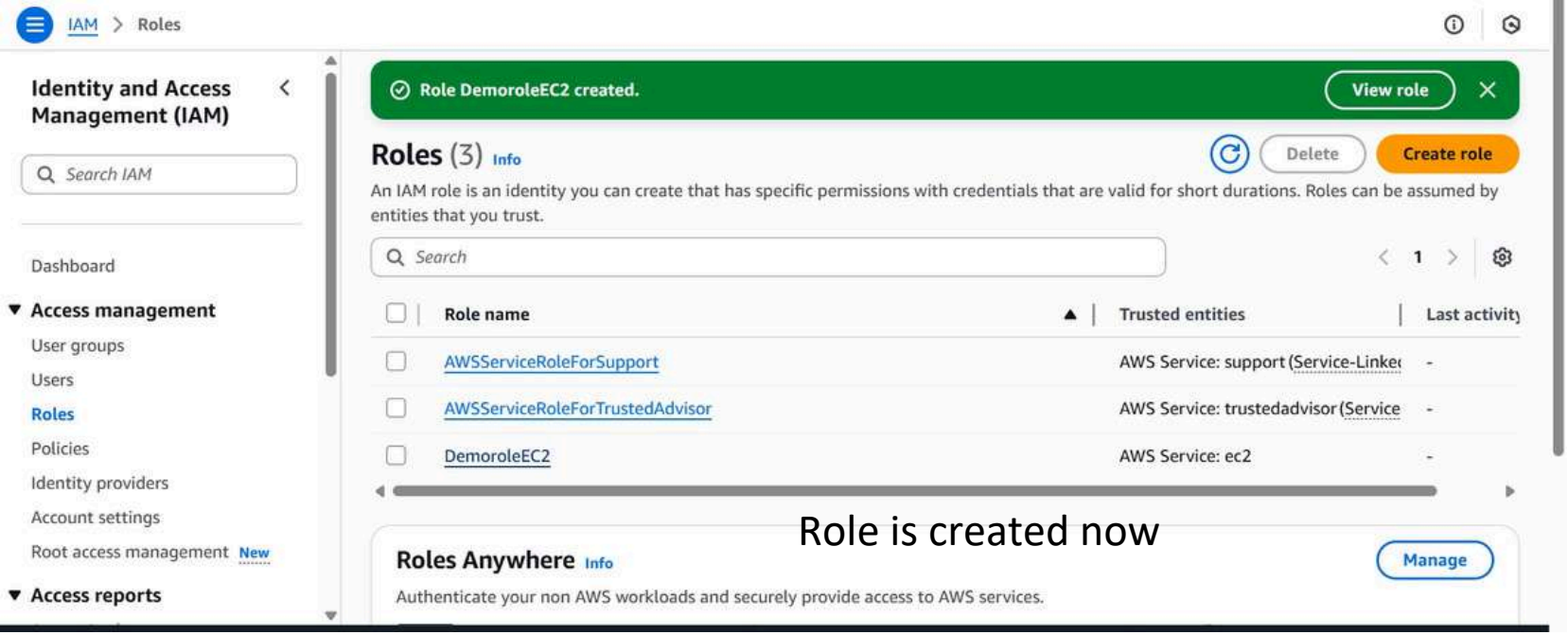
Click on Next



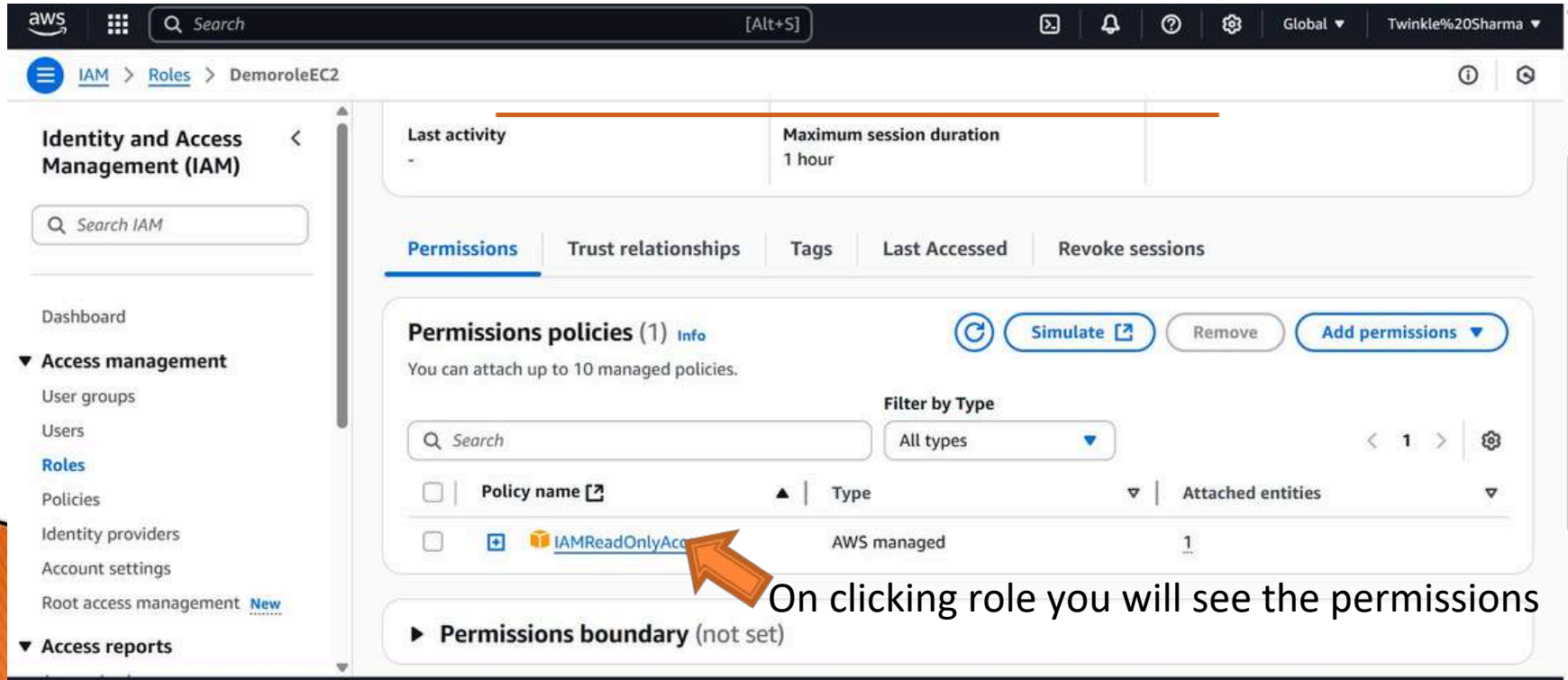
Type Role Name



Click on create role



Role is created now

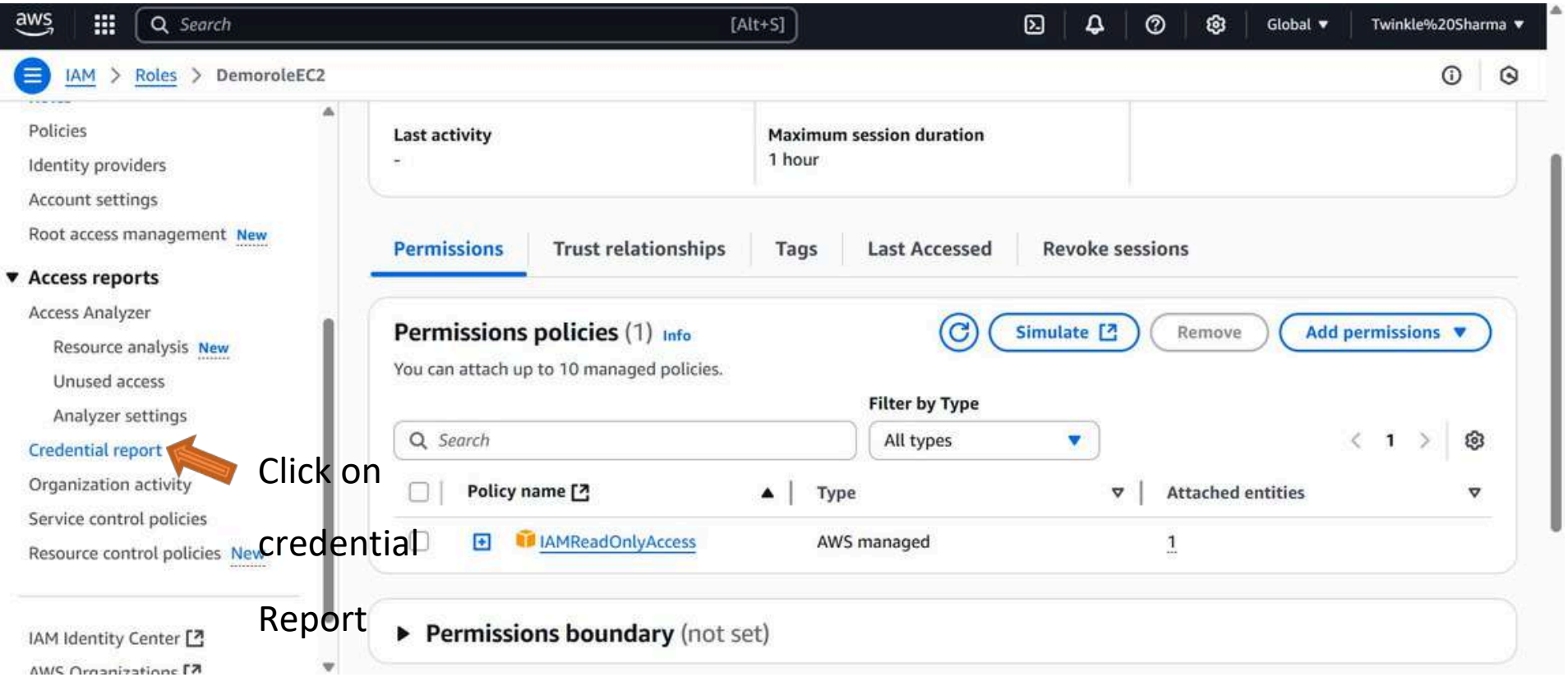


On clicking role you will see the permissions

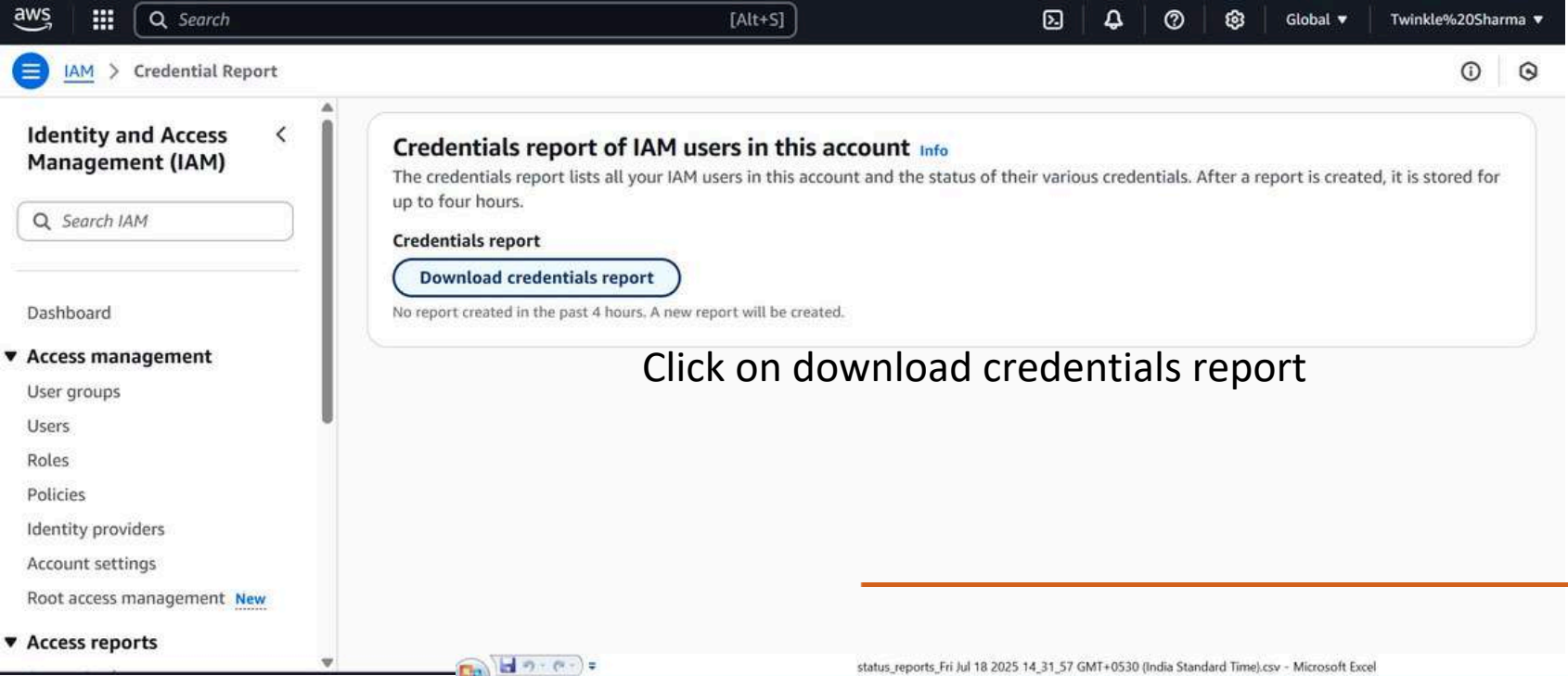
IAM Security Tools in AWS

Tool	Purpose
IAM Access Analyzer	🔍 Detects unused or publicly shared resources
IAM Policy Simulator	🧪 Test and simulate IAM policy behavior before applying
Credential Reports	📊 View the age/status of passwords, access keys, and MFA for users
Access Advisor	📉 Shows services used by users/roles to help reduce over-permissioning
AWS Organizations SCPs	🔒 Apply service control policies to limit actions across accounts
AWS Config Rules	📋 Detect non-compliance with IAM rules (e.g., missing MFA)
CloudTrail	🕵️ Logs all IAM and user activity for auditing
GuardDuty	⚠️ Threat detection (e.g., unusual credential use)
AWS Security Hub	🧩 Centralized security findings from IAM and other tools

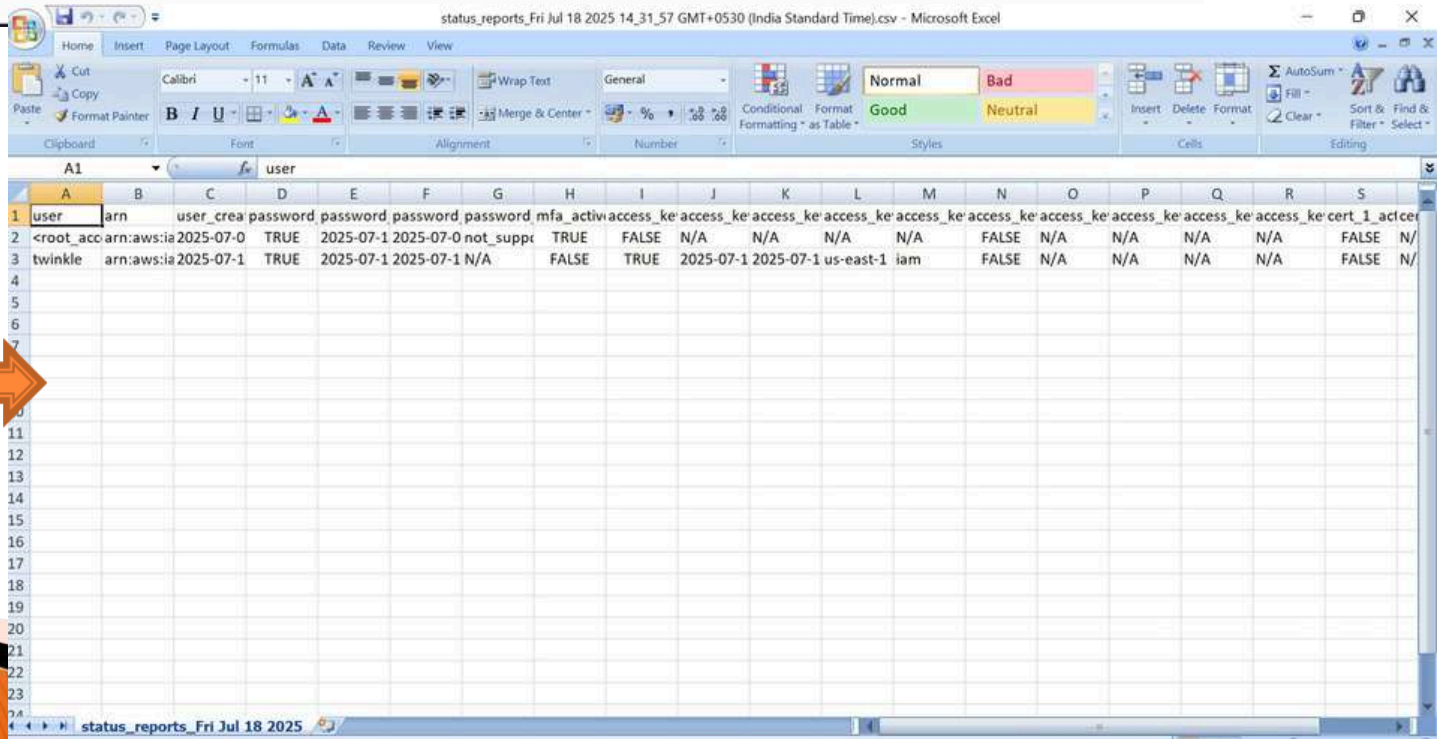
IAM Security Tools Hands On



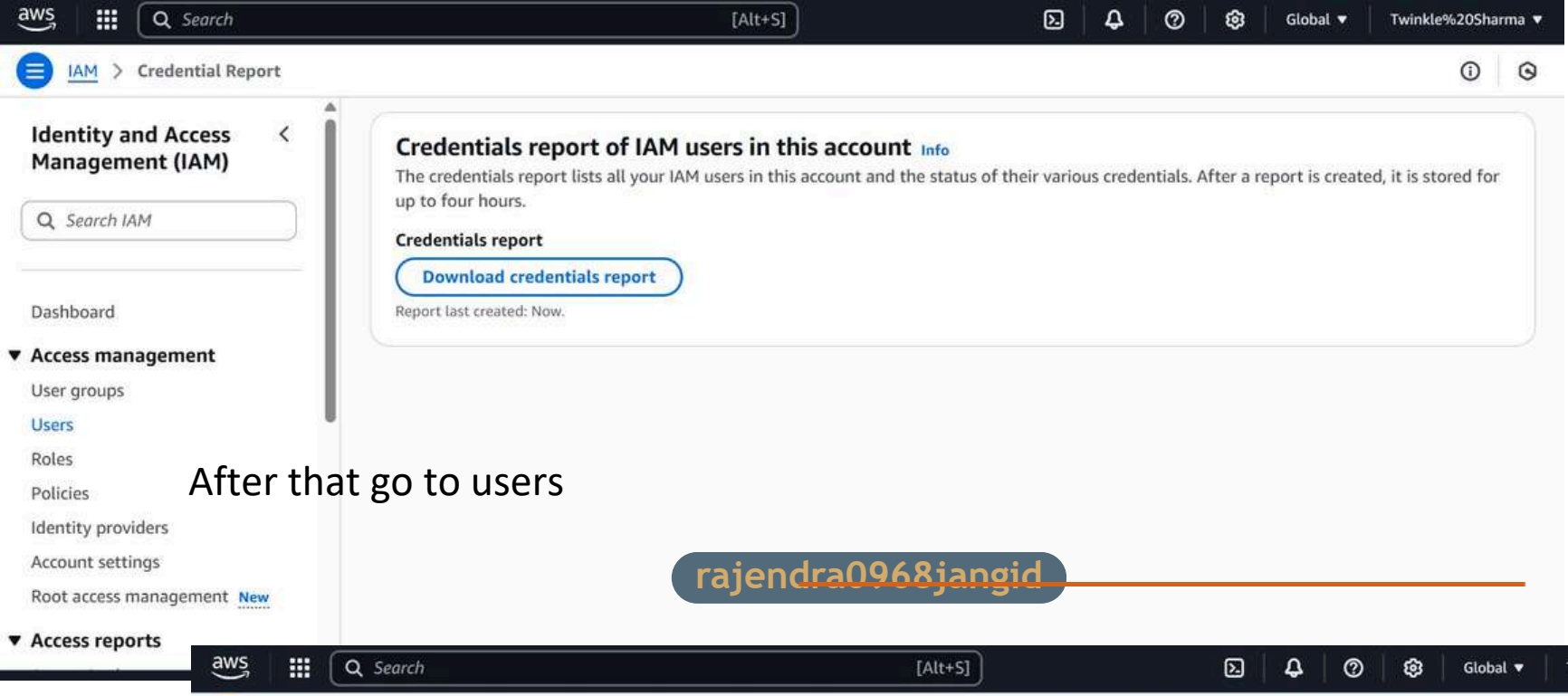
Click on credential Report



Click on download credentials report

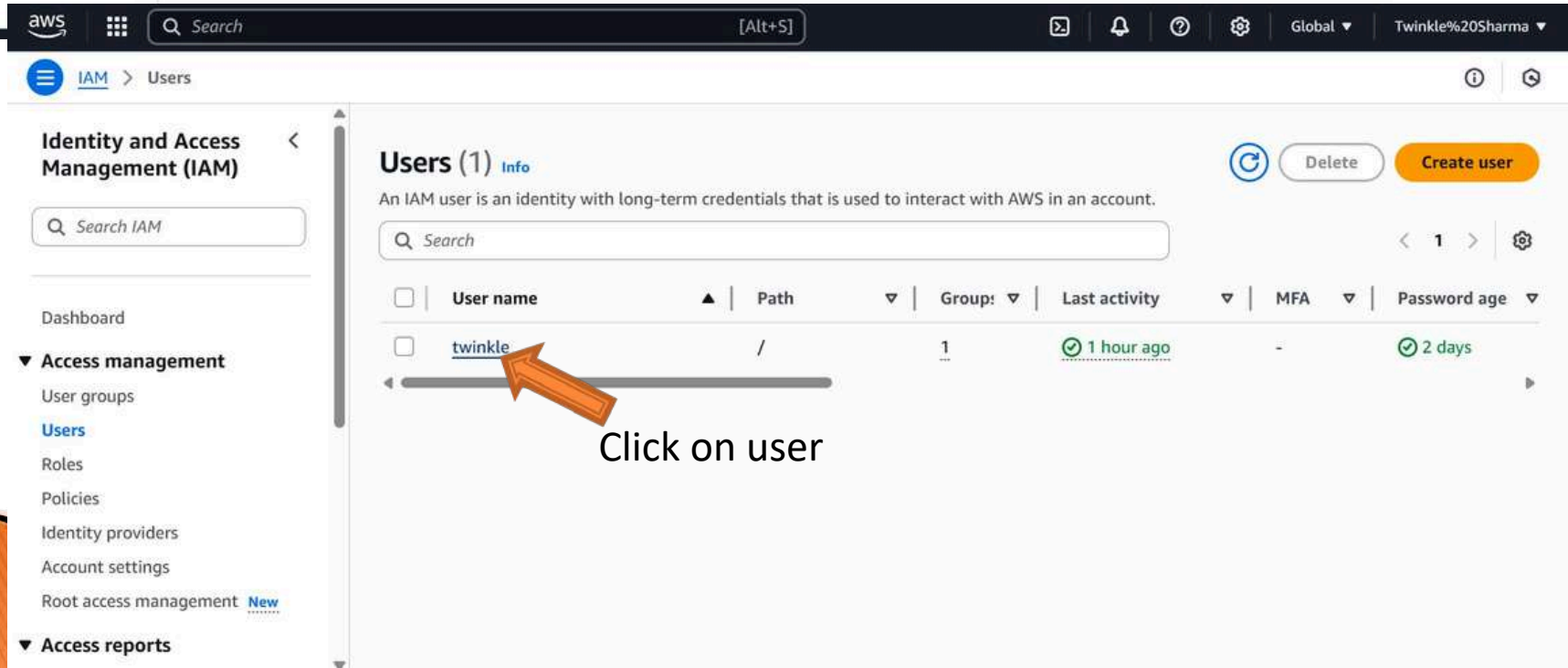


In this Sheet you will get all the details of users

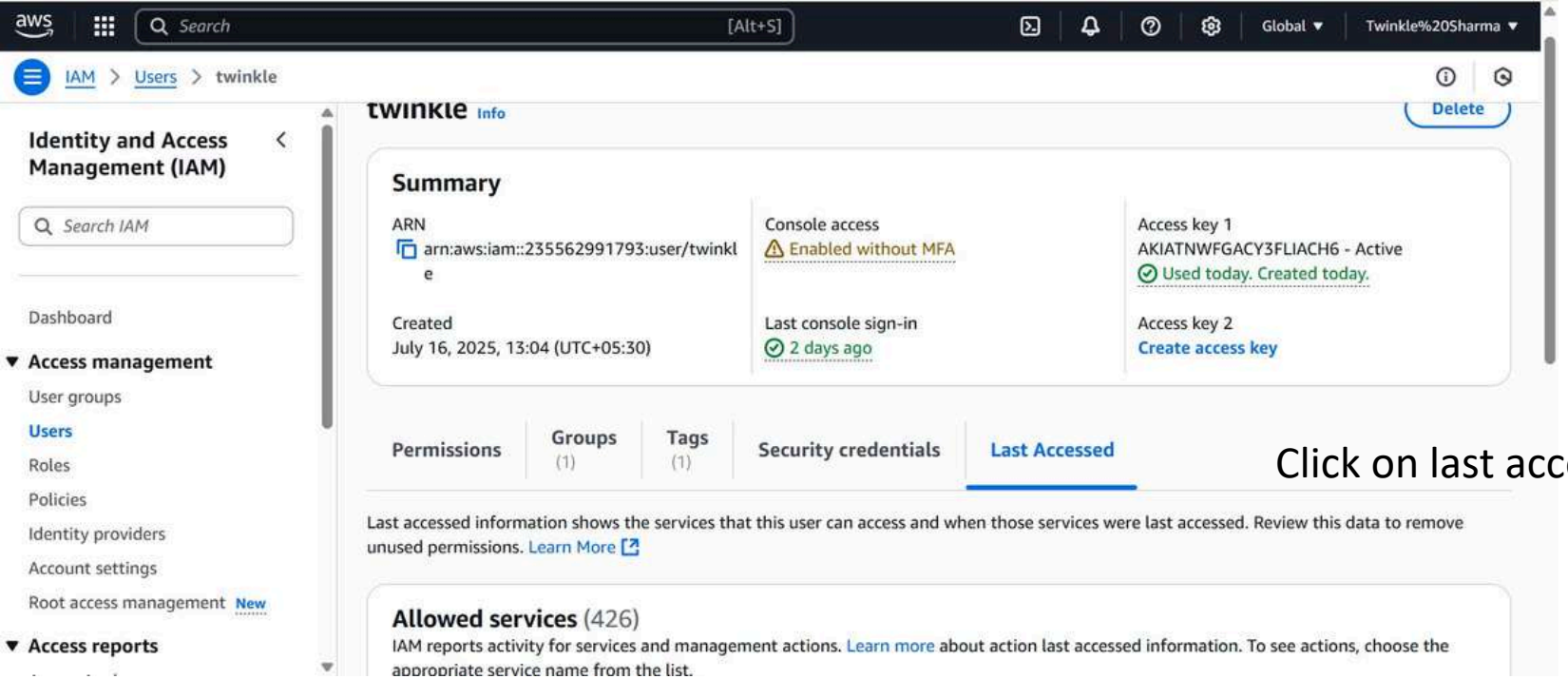


After that go to users

rajendra0968jangid

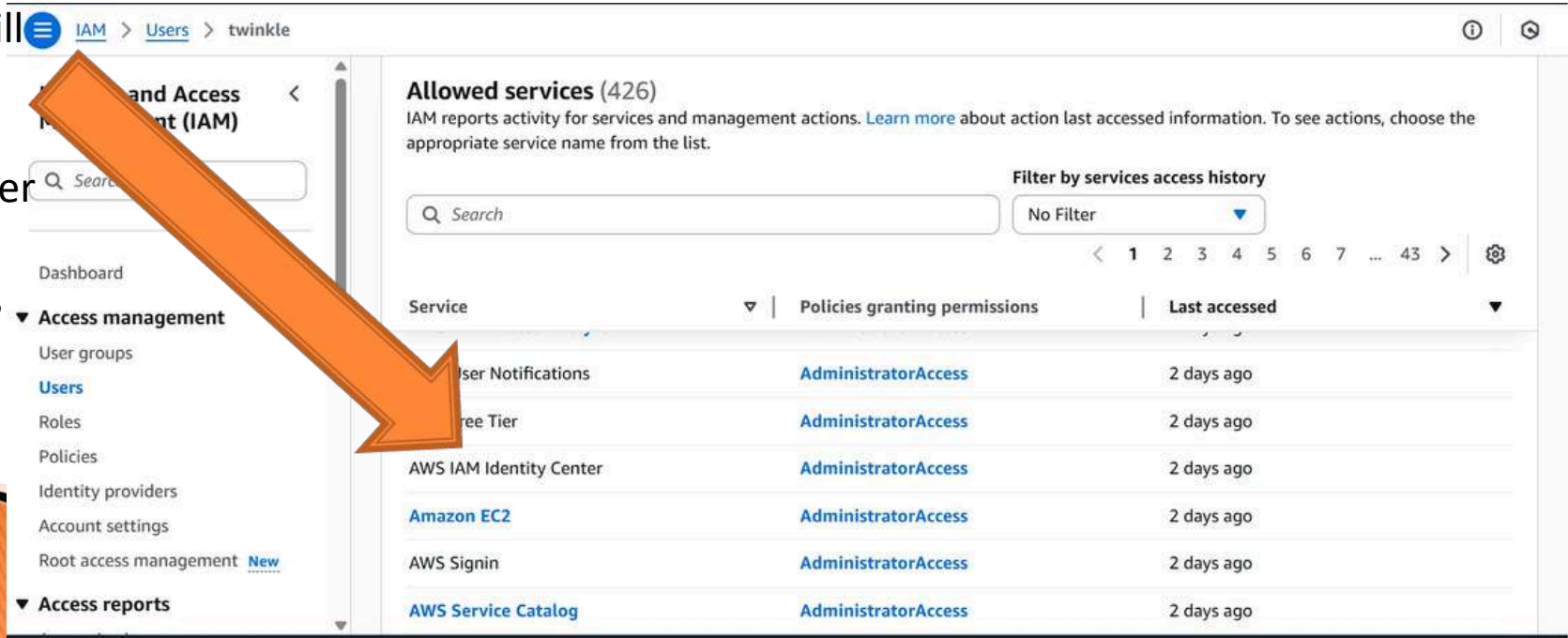


Click on user



Click on last accessed

Here you will see the last accessed servicebyuser & also the permissions granted



IAM Guidelines & Best Practices

- Don't use the root account except for AWS account setup
- One physical user = One AWS user
- Assign users to groups and assign permissions to groups
  Create a strong password policy
- Use and enforce the use of Multi Factor Authentication (MFA)
- Create and use Roles for giving permissions to AWS services
- Use Access Keys for Programmatic Access (CLI / SDK)
- Audit permissions of your account using IAM Credentials Report & IAM Access Advisor
  Never share IAM users & Access Keys
-