THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

EXPERIMENT NO. 7

Aim :- To study and implement Identity and Access Management (IAM) practices on AWS.

Theory :-

Access management : Access management in cloud computing refers to practice of controlling and regulating access to resources, data and services within a cloud environment. It involves managing and enforcing authentication, authorization ; and permissions for users, applications, and permissions for users, applications, only authorized entities can interact with specific resources.

Need of access management :
1) Data Protection
2) Compliance and Regulatory Requirements
3) Operational Efficiency
4) SSO capabilities

Identity Access Management (IAM) : It is security discipline that enables the right individuals to access right resources at right time for right reasons. Identity management looks to confirm that an accessing user is who they are, by examining information presented during access request against a database. Access management, on the other hand, uses info regarding user's identity to determine which resources they are entitled to access.

Components:

1) Authentication: It is module through which a user provides sufficient credentials to gain initial access to a system of a particular resource.

2) Authorization: It determines whether a user is permitted to access a particular resource.

3) User Management: It consists of set of administrating functions such as identity creation, propagation, and maintenance of user identity and privileges.

4) Central User Repository: It stores and delivers identity information to other services, and provides service to verify credentials submitted from clients.

Root users	IAM users
It is the account created when you create first an AWS account. Full administrative access to all AWS services and resources. Can create and manage IAM users, change billing info. Not used for any sort of routine tasks and set up tasks.	IAM users are entities created within an AWS account. Specific permissions assigned to them based on policies. Are created and managed by the account administrator. Is generally used for day to day activities, and their permissions should be carefully configured.

Roles	Policies
These are entities that define a set of permissions for making AWS requests.	These are JSON-formated documents defining policies determining what actions are all allowed or denied.
Roles are often used to grant temporary permissions to an AWS resource or user.	Policies can be broadly scoped, allowing permissions across multiple services.
Roles have a trust policy that defines which entities are allowed to assume role.	Policies can be attached to IAM users, groups or roles, and can be in line, i.e, directly embedded in a user, group or managed.

Inline Policies: These are policies that are directly embedded within a specific IAM user, group or role. Inline policies are scoped to a particular IAM entity and cannot be reused elsewhere.

Custom Policies: These are standalone policies that are created and managed separately from IAM users, groups, or roles.

MFA: AWS Multi-factor Authentication (MFA) is an AWS identity and access managed (IAM) best practice that requires a second authentication factor.

Conclusion :- Thus we understood the implementation of IAM practices on AWS.

A+
15/3/24

Rishab Mandal
2103110
C23

Cloud Computing Experiment 7

Aim: To study and implement Identity and Access Management (IAM) practices on AWS.

Theory:

Introduction:

In the realm of cloud computing, maintaining secure access to resources is paramount. Identity and Access Management (IAM) is the cornerstone of ensuring that only authorized individuals and services can interact with cloud resources. This write-up delves into the concept of access management, the components of AWS IAM, a comparison between root users and IAM users, roles and policies, types of policies, and Multi-Factor Authentication (MFA) on AWS.

Concept and Need of Access Management:

Access management refers to the practice of controlling and monitoring access to resources within a system. In cloud environments like AWS, where resources are abstracted and accessed remotely, ensuring secure access is crucial. The need arises from the requirement to safeguard sensitive data, prevent unauthorized usage of resources, and comply with regulatory standards.

IAM and Its Components:

IAM in AWS is a service that enables you to manage access to AWS services and resources securely. Its components include:

Users: Represent individuals or services interacting with AWS resources. Each user has unique security credentials.

Groups: A collection of users, simplifying the management of permissions by applying policies to groups rather than individual users.

Roles: Similar to users, but intended for services or entities outside of AWS, allowing them temporary access to AWS resources.

Policies: JSON documents defining permissions. These can be attached to users, groups, or roles to specify the actions they are allowed or denied.

Root Users vs. IAM Users:

Root Users: When an AWS account is created, the email address and password used become the root user credentials. Root users have complete access to all resources and services in the account. However, it's recommended to avoid using root credentials for day-to-day activities due to security risks.

IAM Users: These are users created within AWS IAM. IAM users have specific permissions assigned to them through policies. They don't have inherent access to all resources like root users, but their permissions can be finely tuned.

Roles and Policies:

Roles: IAM roles are meant to be assumed by entities within or outside of AWS, such as AWS services, applications, or users. Roles define a set of permissions, and temporary security credentials are provided when a role is assumed.

Policies: IAM policies are documents that define permissions. They can be attached to users, groups, or roles. Policies specify what actions are allowed or denied, and on which resources.

Inline and Custom Policies in AWS:

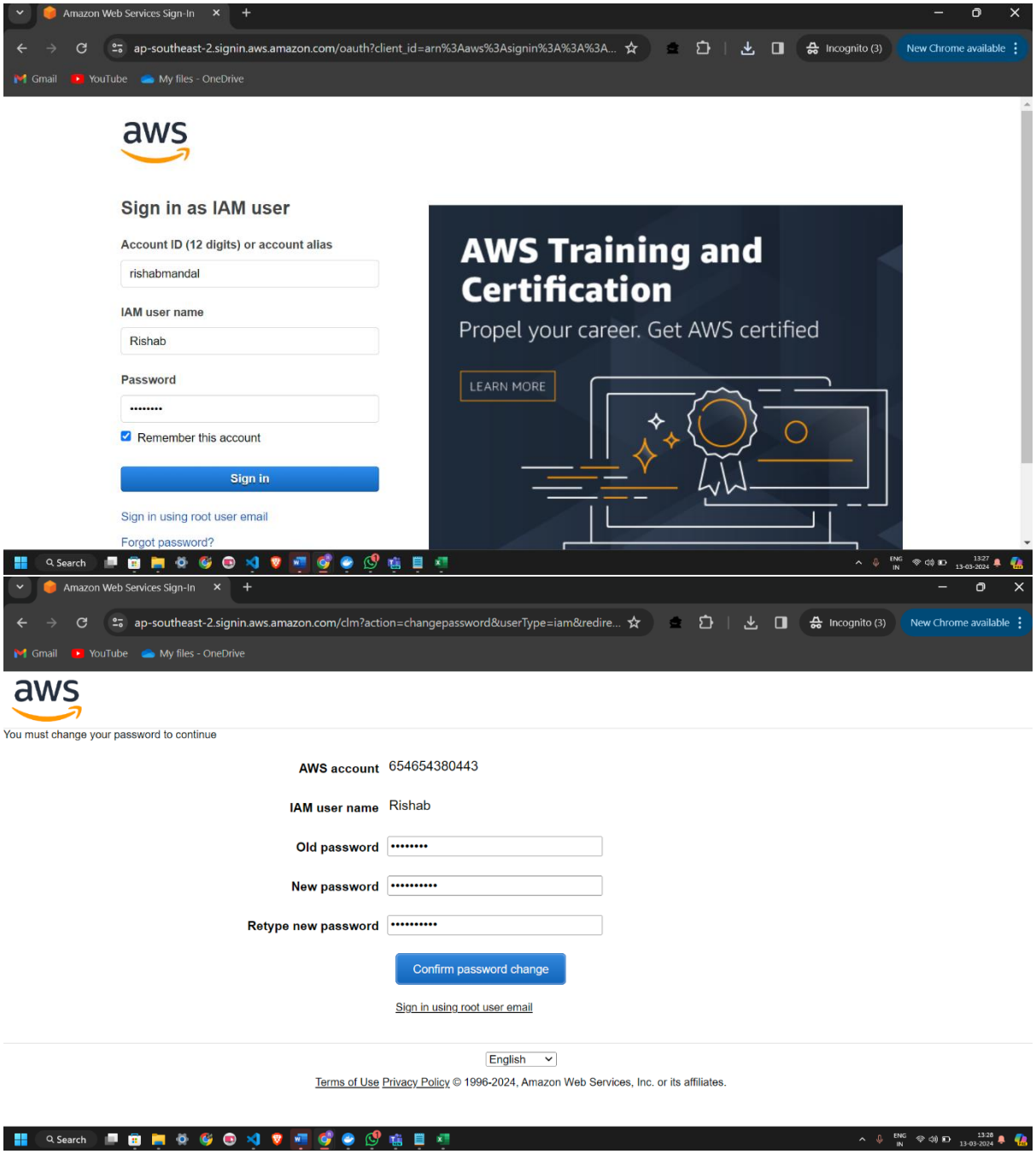
Inline Policies: These are policies that are embedded directly into a single user, group, or role. Inline policies are tightly coupled with the entity to which they are attached and cannot be reused across multiple entities.

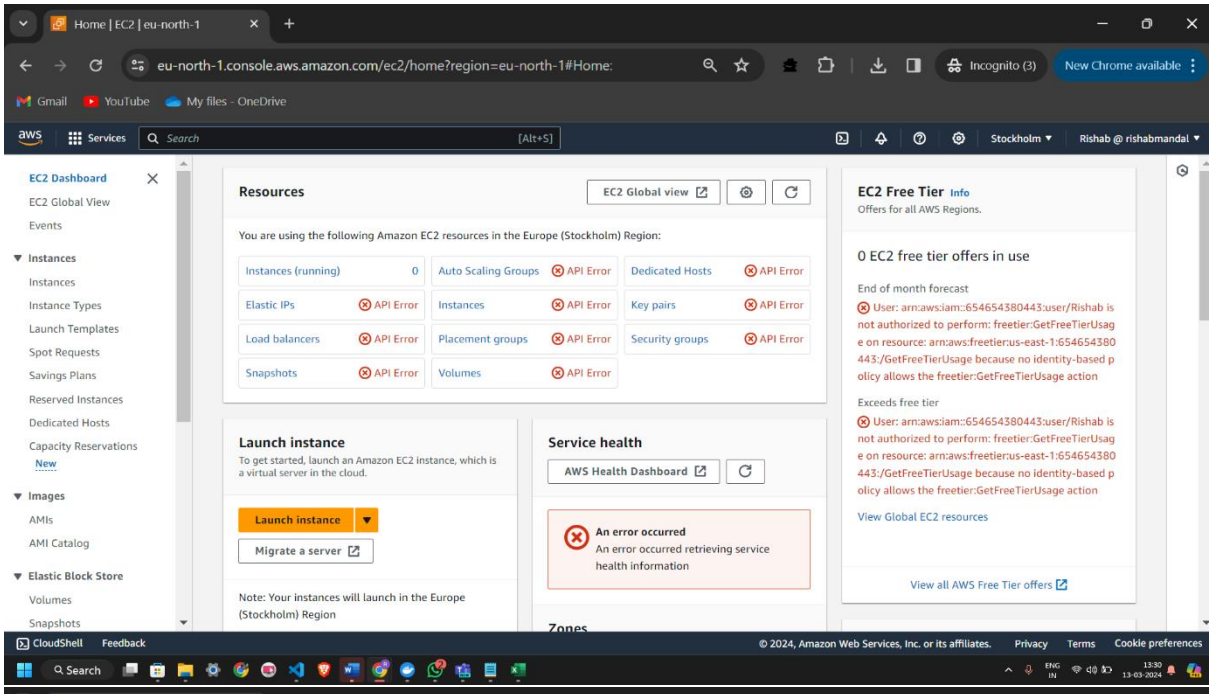
Custom Policies: Custom policies are standalone documents that can be attached to multiple users, groups, or roles. They offer more flexibility and reusability compared to inline policies.

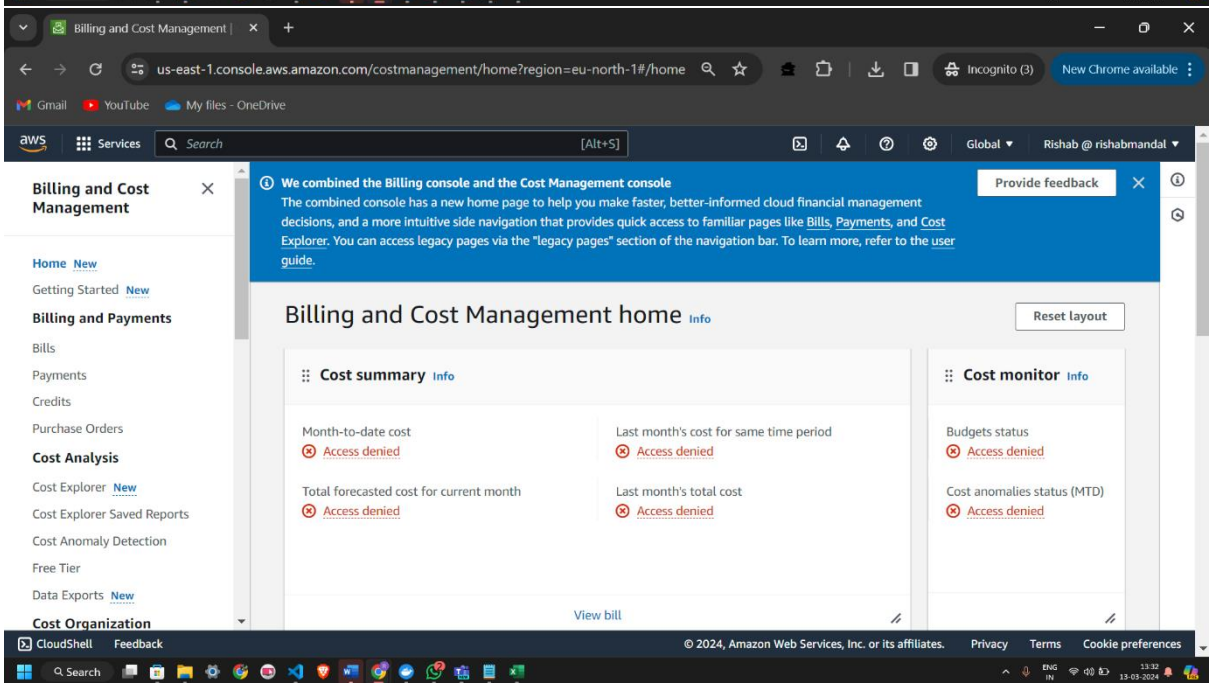
Multi-Factor Authentication (MFA) in AWS:

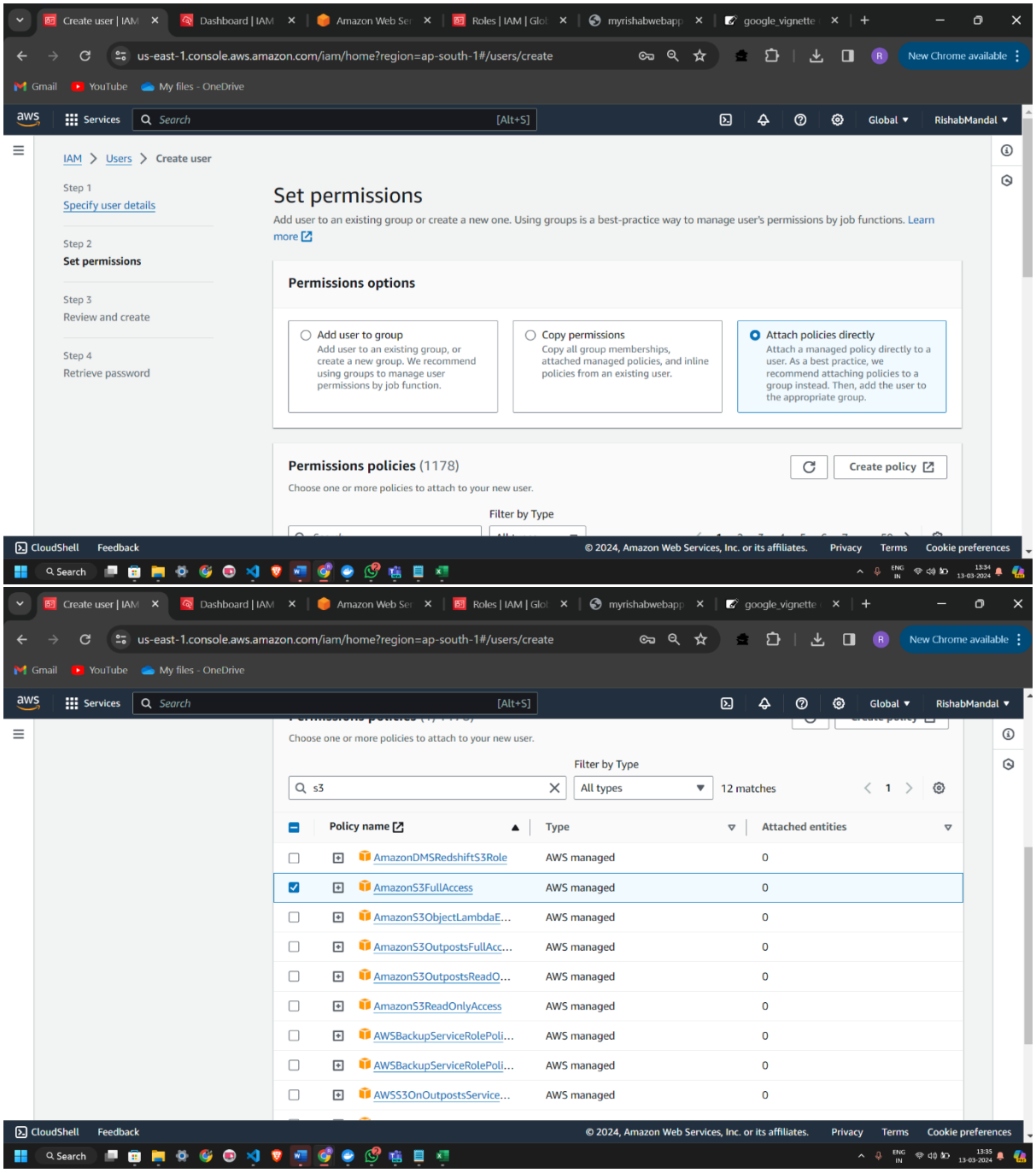
MFA adds an extra layer of security to AWS accounts by requiring users to present two or more forms of verification before granting access. This typically involves something the user knows (like a password) and something they possess (like a mobile device or hardware token). MFA can be enabled for IAM users and can be enforced for specific actions or console logins, enhancing security by mitigating the risks associated with compromised passwords.

Screenshots:

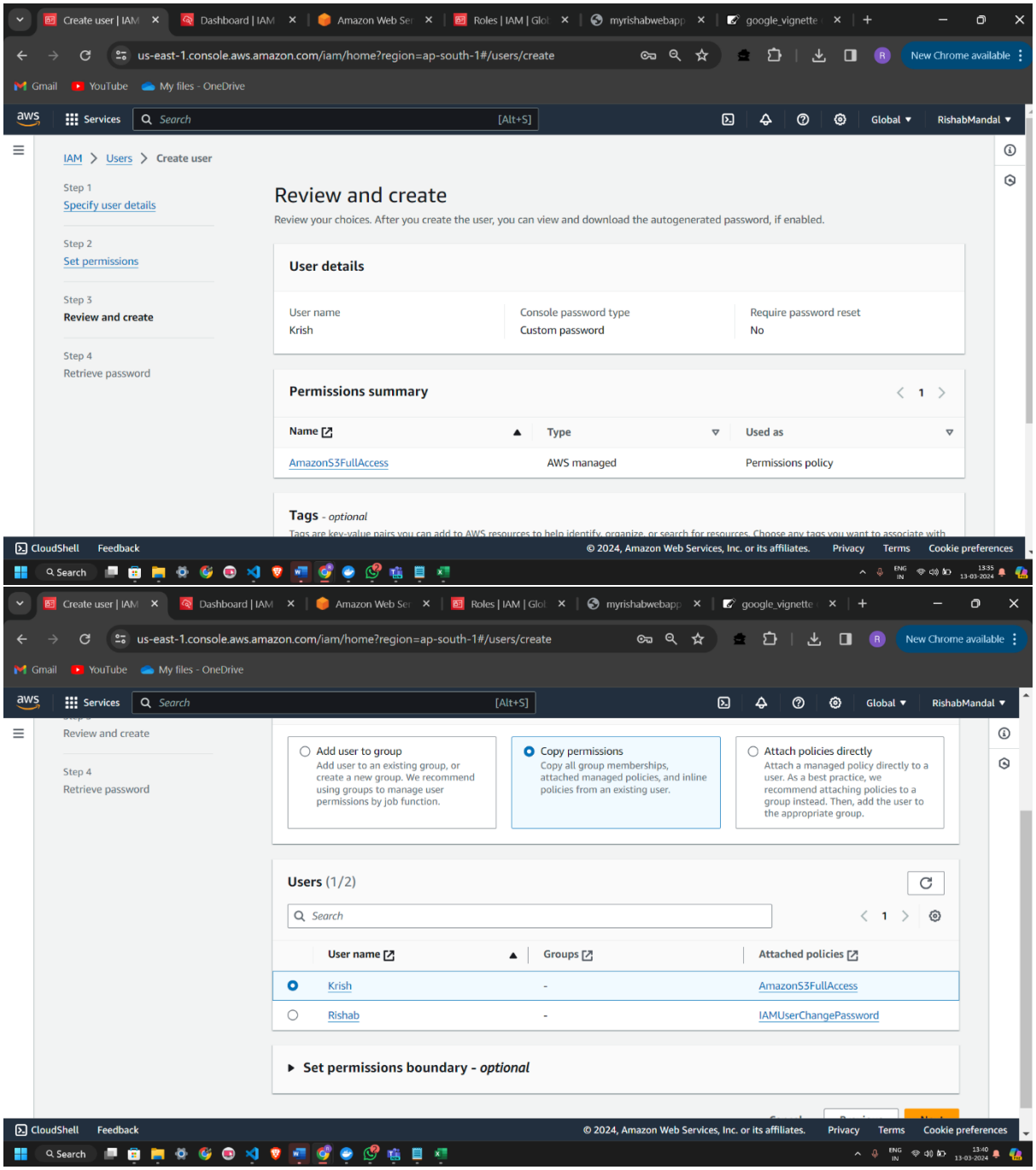


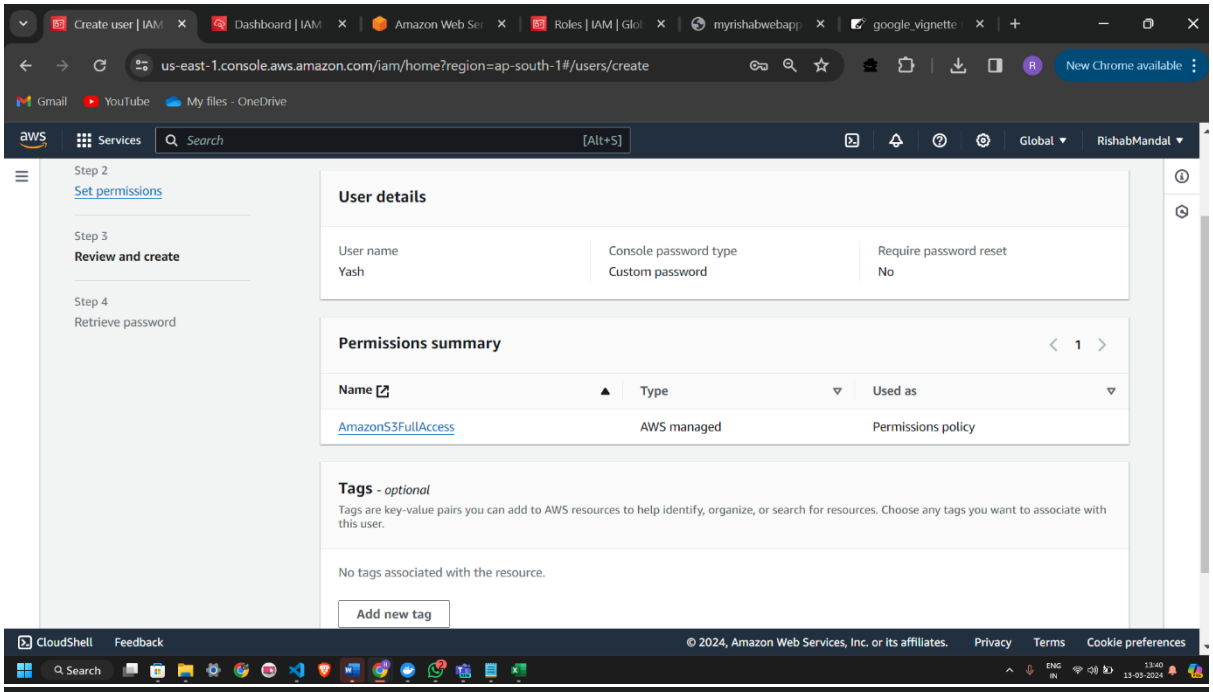

Home | EC2 | eu-north-1
eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#Home:
Incognito (3)
New Chrome available
Gmail
YouTube
My files - OneDrive
Services
Search
[Alt+S]
Stockholm
Rishab @ rishabmandal
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Resources
EC2 Global view
You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:
Instances (running) 0
Auto Scaling Groups API Error
Dedicated Hosts API Error
Elastic IPs API Error
Instances API Error
Key pairs API Error
Load balancers API Error
Placement groups API Error
Security groups API Error
Snapshots API Error
Volumes API Error
EC2 Free Tier Info
Offers for all AWS Regions.
0 EC2 free tier offers in use
End of month forecast
User: arn:aws:iam::654654380443:user/Rishab is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:654654380443:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action
Exceeds free tier
User: arn:aws:iam::654654380443:user/Rishab is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:654654380443:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action
View Global EC2 resources
View all AWS Free Tier offers
Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.
Launch instance
Migrate a server
Note: Your instances will launch in the Europe (Stockholm) Region
Service health
AWS Health Dashboard
An error occurred
An error occurred retrieving service health information
Zones
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

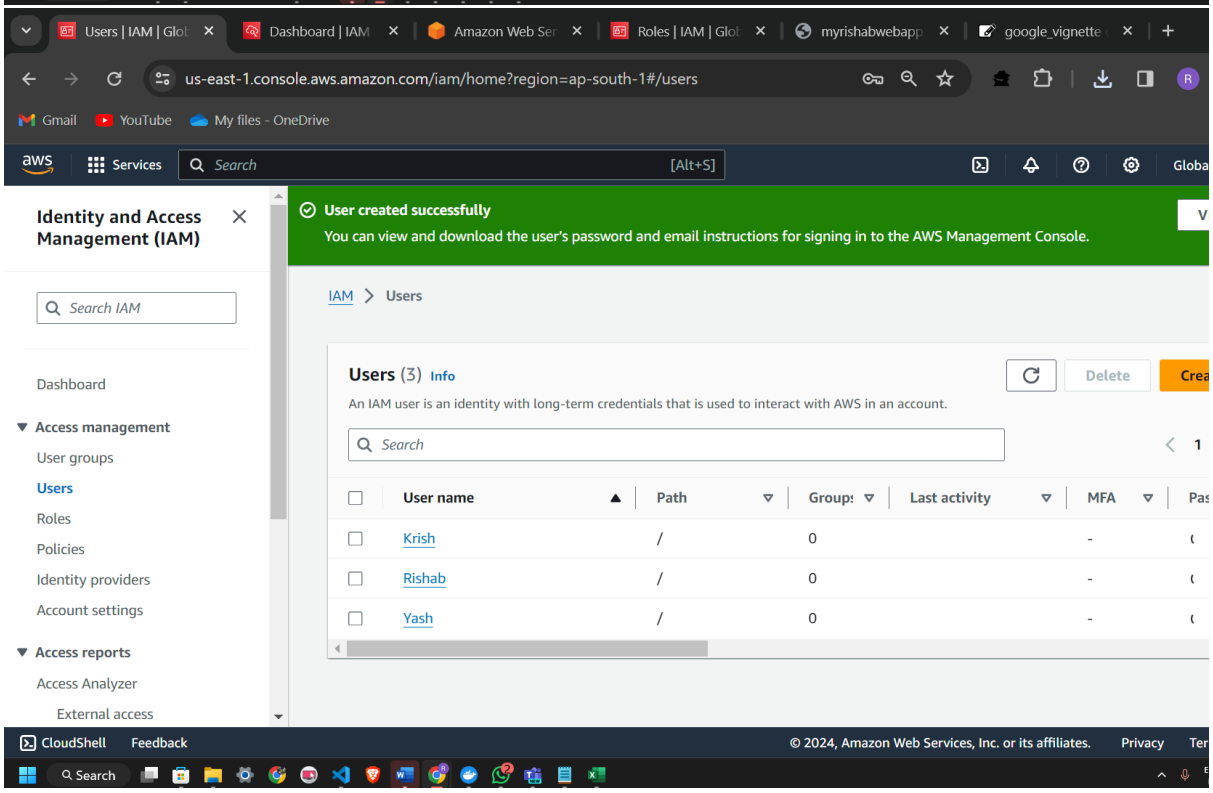

Billing and Cost Management |
us-east-1.console.aws.amazon.com/costmanagement/home?region=eu-north-1#/home
Incognito (3)
New Chrome available
Gmail
YouTube
My files - OneDrive
Services
Search
[Alt+S]
Global
Rishab @ rishabmandal
Billing and Cost Management
Home New
Getting Started New
Billing and Payments
Bills
Payments
Credits
Purchase Orders
Cost Analysis
Cost Explorer New
Cost Explorer Saved Reports
Cost Anomaly Detection
Free Tier
Data Exports New
Cost Organization
We combined the Billing console and the Cost Management console
The combined console has a new home page to help you make faster, better-informed cloud financial management decisions, and a more intuitive side navigation that provides quick access to familiar pages like Bills, Payments, and Cost Explorer. You can access legacy pages via the "legacy pages" section of the navigation bar. To learn more, refer to the user guide.
Provide feedback
Billing and Cost Management home Info
Reset layout
Cost summary Info
Month-to-date cost
Access denied
Last month's cost for same time period
Access denied
Total forecasted cost for current month
Access denied
Last month's total cost
Access denied
Cost monitor Info
Budgets status
Access denied
Cost anomalies status (MTD)
Access denied
View bill
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

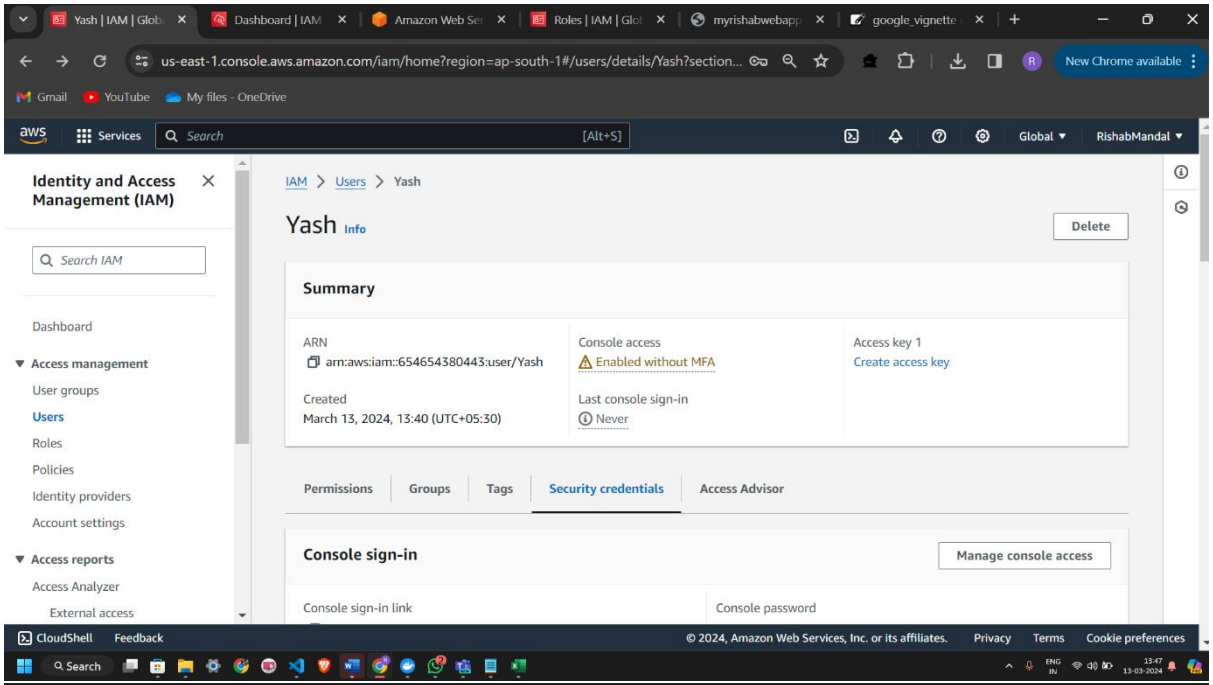

Create user | IAM
Dashboard | IAM
Amazon Web Ser
Roles | IAM | Glob
myrishabwebapp
google_vignette
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
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 (1178)
Choose one or more policies to attach to your new user.
Create policy
Filter by Type
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search

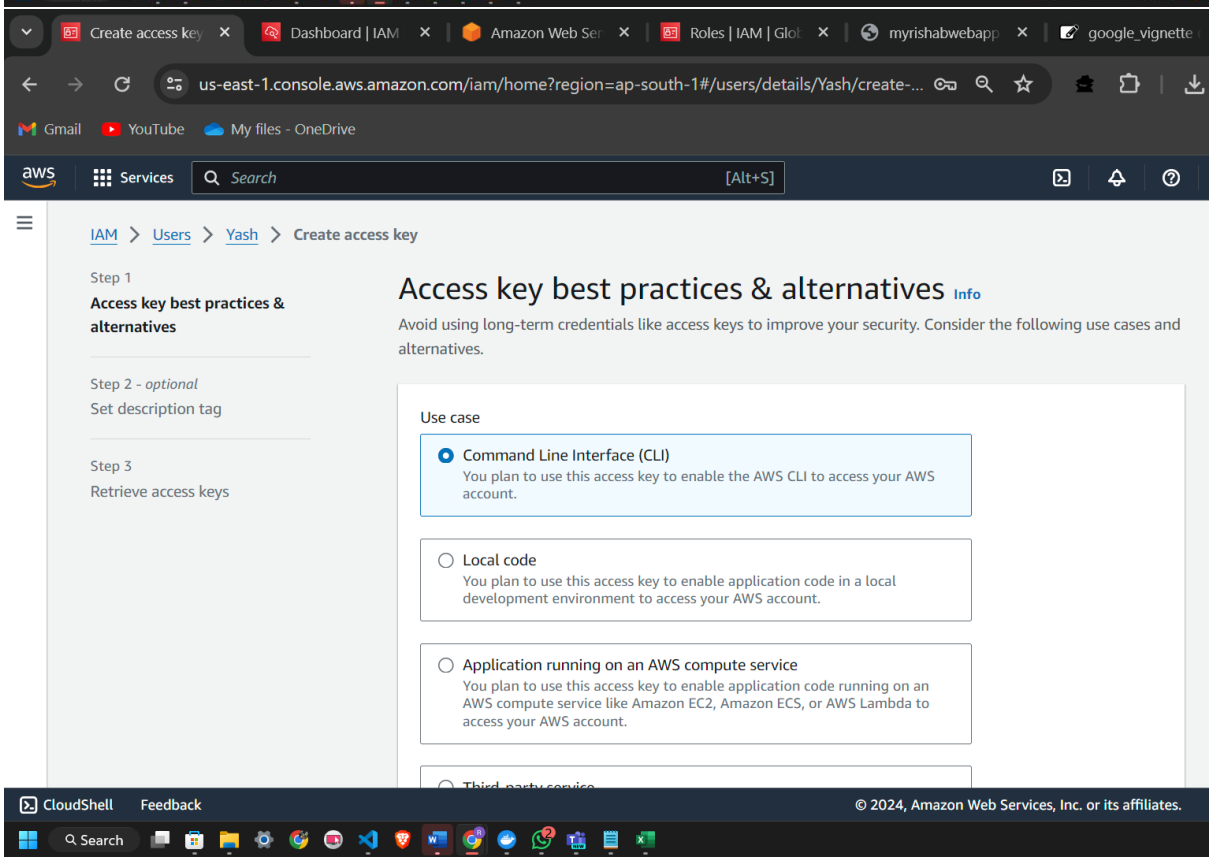
Create user | IAM
Dashboard | IAM
Amazon Web Ser
Roles | IAM | Glob
myrishabwebapp
google_vignette
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
Choose one or more policies to attach to your new user.
Filter by Type
s3
All types
12 matches
1
Policy name
Type
Attached entities
AmazonDMSRedshiftS3Role
AWS managed
0
AmazonS3FullAccess
AWS managed
0
AmazonS3ObjectLambdaE...
AWS managed
0
AmazonS3OutpostsFullAcc...
AWS managed
0
AmazonS3OutpostsReadO...
AWS managed
0
AmazonS3ReadOnlyAccess
AWS managed
0
AWSBackupServiceRolePoli...
AWS managed
0
AWSBackupServiceRolePoli...
AWS managed
0
AWSS3OnOutpostsService...
AWS managed
0
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search

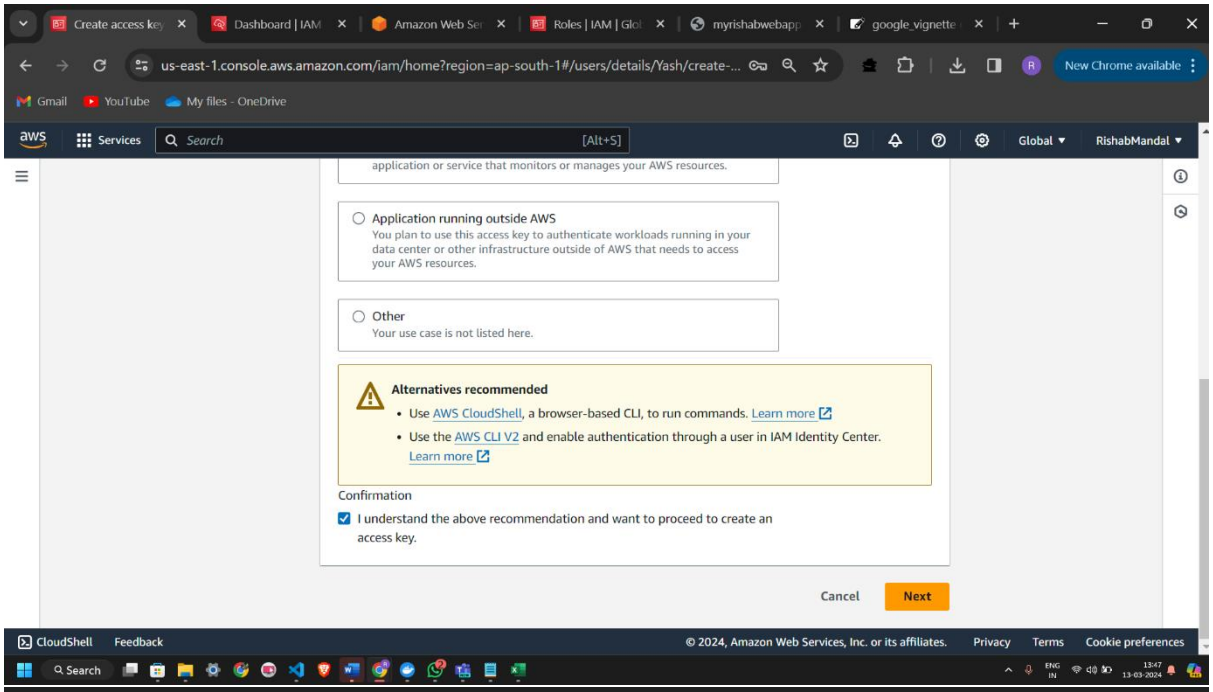

Create user | IAM
Dashboard | IAM
Amazon Web Ser
Roles | IAM | Glot
myrishabwebapp
google_vignette
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
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
Krish
Console password type
Custom password
Require password reset
No
Permissions summary
Name
Type
Used as
AmazonS3FullAccess
AWS managed
Permissions policy
Tags - optional
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
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.
Users (1/2)
Search
User name
Groups
Attached policies
Krish
-
AmazonS3FullAccess
Rishab
-
IAMUserChangePassword
Set permissions boundary - optional

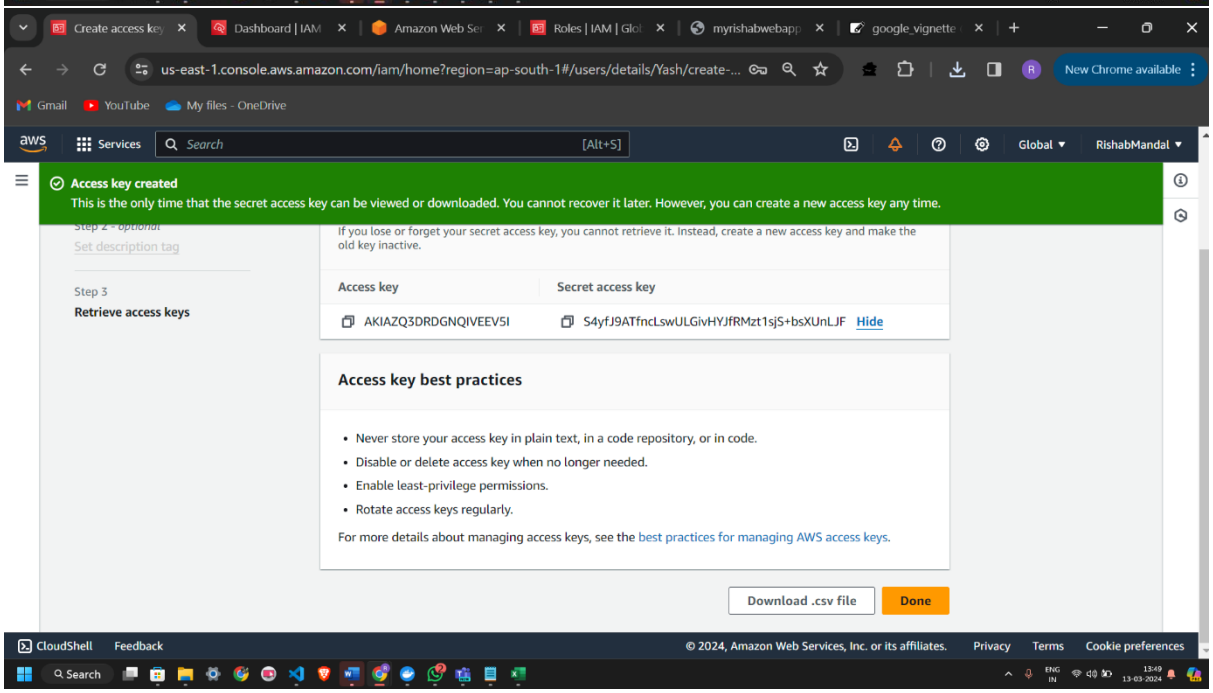

Create user | IAM
Dashboard | IAM
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
New Chrome available
Gmail
YouTube
My files - OneDrive
Services
Search
[Alt+S]
Global
RishabMandal
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
User details
User name
Yash
Console password type
Custom password
Require password reset
No
Permissions summary
Name
Type
Used as
AmazonS3FullAccess
AWS managed
Permissions policy
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

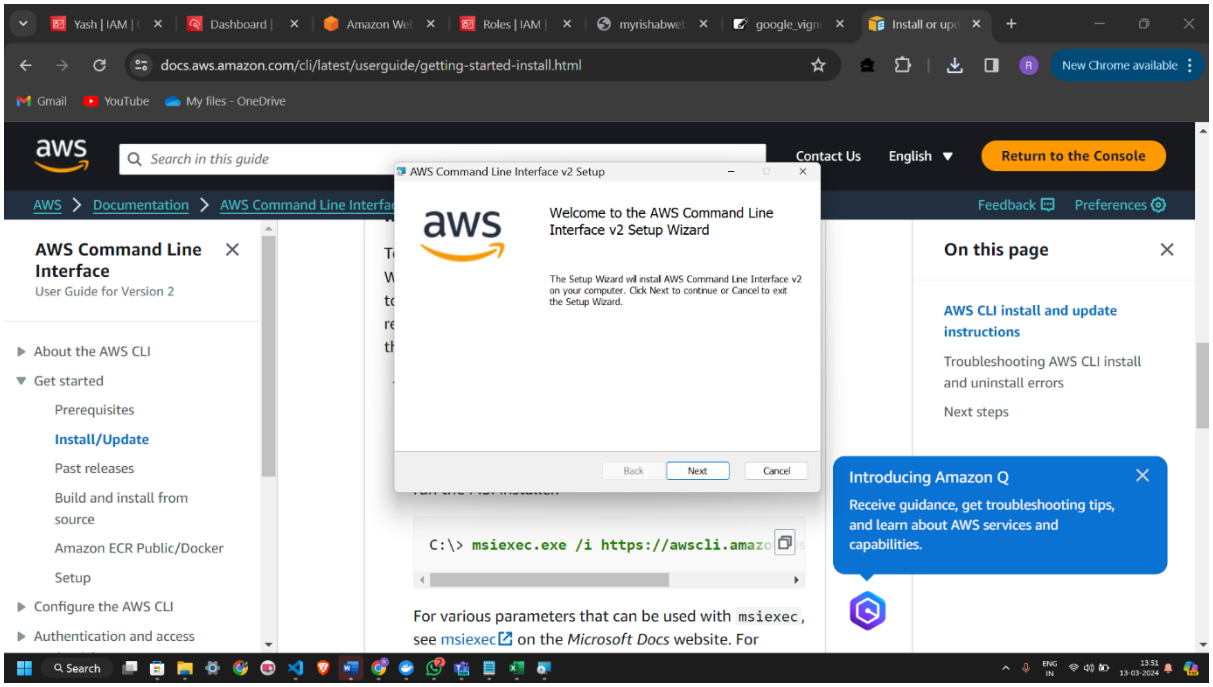

Users | IAM | Glob
Dashboard | IAM
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users
Gmail
YouTube
My files - OneDrive
Services
Search
[Alt+S]
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
IAM
Users
Users (3) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Search
User name
Path
Groups
Last activity
MFA
Krish
/
0
Rishab
/
0
Yash
/
0
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy

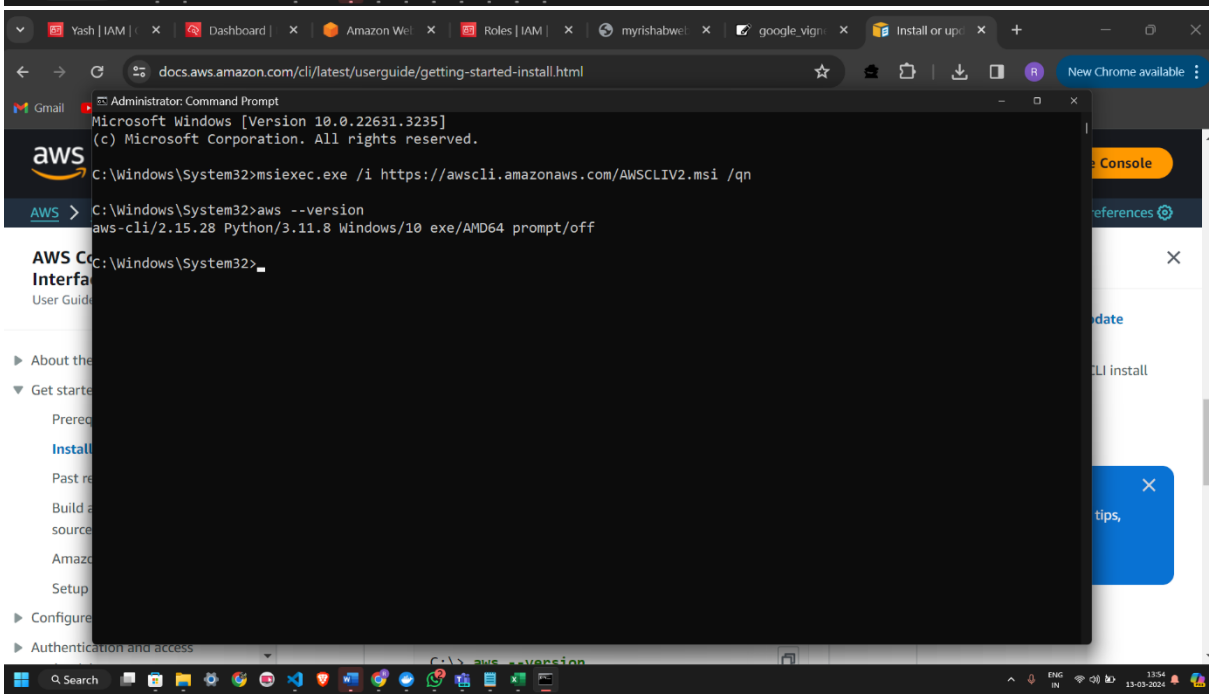

Yash | IAM | Glob
Dashboard | IAM
Amazon Web Ser
Roles | IAM | Glo
myrishabwebapp
google_vignette
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Yash?section...
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
IAM > Users > Yash
Yash Info
Delete
Summary
ARN
arn:aws:iam::654654380443:user/Yash
Console access
Enabled without MFA
Access key 1
Create access key
Created
March 13, 2024, 13:40 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Access Advisor
Console sign-in
Manage console access
Console sign-in link
Console password
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search

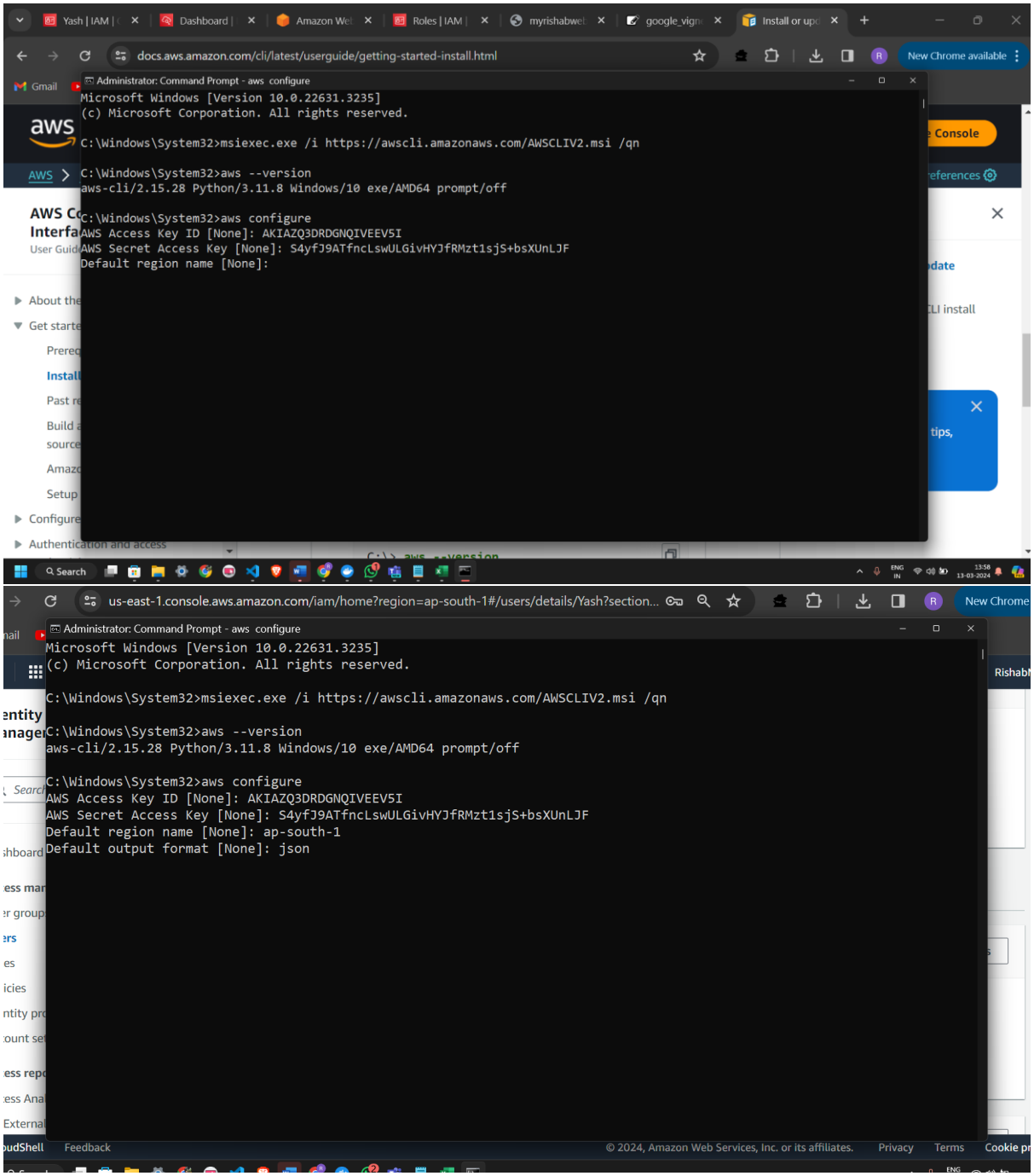

Create access key
Dashboard | IAM
Amazon Web Ser
Roles | IAM | Glo
myrishabwebapp
google_vignette
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Yash/create-...
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
IAM > Users > Yash > Create access key
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Access key best practices & alternatives Info
Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.
Use case
Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.
Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.
Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Search

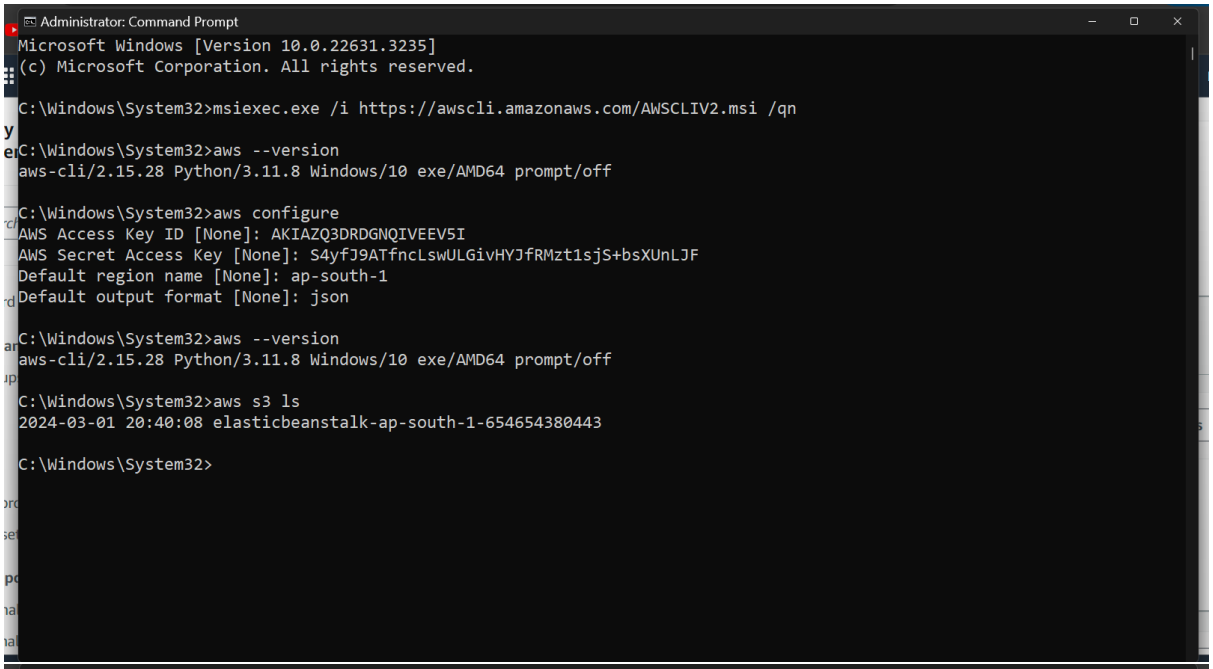

Create access key
Dashboard | IAM
Amazon Web Ser
Roles | IAM | Glob
myrishabwebapp
google_vignette
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Yash/create-...
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
application or service that monitors or manages your AWS resources.
Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.
Other
Your use case is not listed here.
Alternatives recommended
Use AWS CloudShell, a browser-based CLI, to run commands. Learn more
Use the AWS CLI V2 and enable authentication through a user in IAM Identity Center. Learn more
Confirmation
I understand the above recommendation and want to proceed to create an access key.
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search

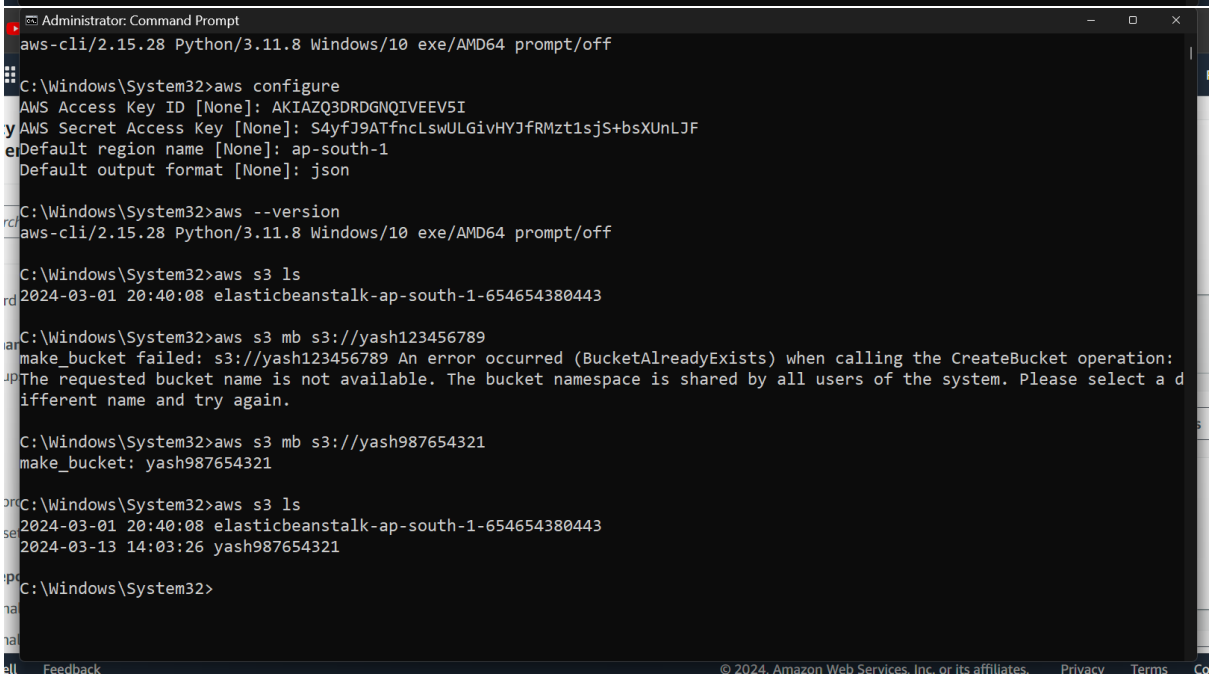

Create access key
Dashboard | IAM
Amazon Web Ser
Roles | IAM | Glob
myrishabwebapp
google_vignette
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Yash/create-...
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.
Set description tag
Step 3
Retrieve access keys
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.
Access key
Secret access key
AKIAZQ3DRDGNQIVEEV5I
S4yfJ9ATfncLswULGivHYJfRMzt1sjS+bsXUnLJF
Hide
Access key best practices
Never store your access key in plain text, in a code repository, or in code.
Disable or delete access key when no longer needed.
Enable least-privilege permissions.
Rotate access keys regularly.
For more details about managing access keys, see the best practices for managing AWS access keys.
Download .csv file
Done
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search


docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html
Search in this guide
Contact Us
English
Return to the Console
AWS Command Line Interface v2 Setup
Welcome to the AWS Command Line Interface v2 Setup Wizard
The Setup Wizard will install AWS Command Line Interface v2 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel
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
On this page
AWS CLI install and update instructions
Troubleshooting AWS CLI install and uninstall errors
Next steps
Introducing Amazon Q
Receive guidance, get troubleshooting tips, and learn about AWS services and capabilities.
C:\> msiexec.exe /i https://awscli.amazo
For various parameters that can be used with msiexec, see msiexec on the Microsoft Docs website. For

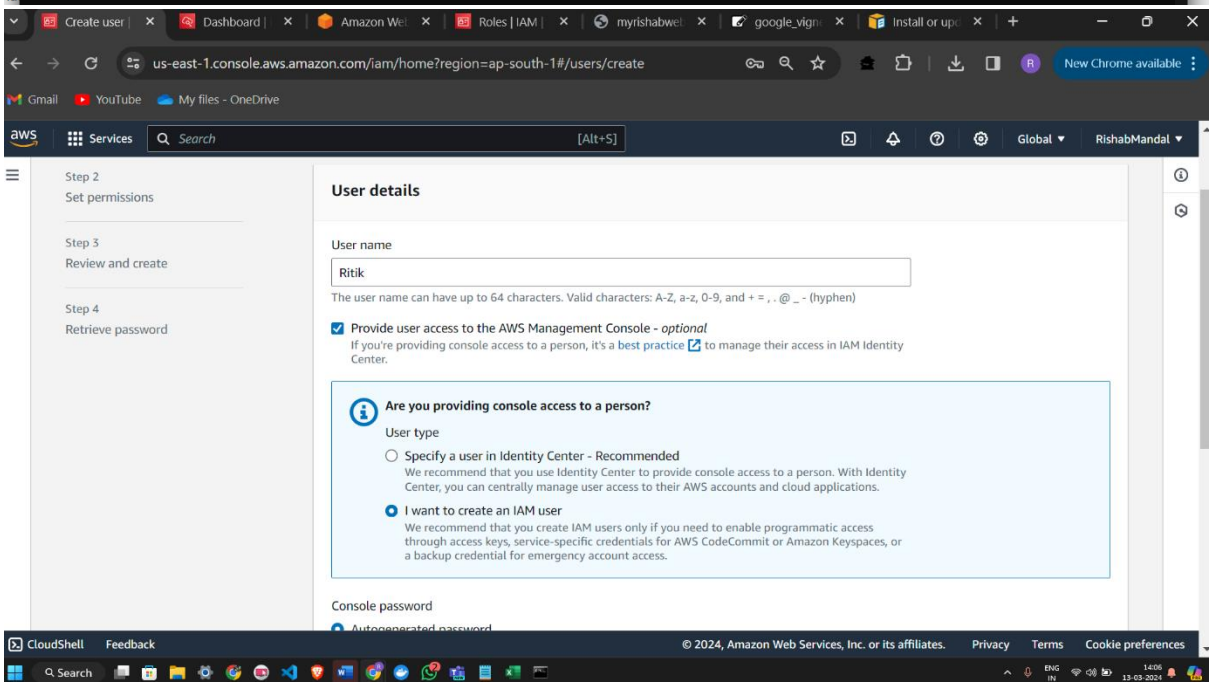

Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.3235]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\System32>msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi /qn
C:\Windows\System32>aws --version
aws-cli/2.15.28 Python/3.11.8 Windows/10 exe/AMD64 prompt/off
C:\Windows\System32>

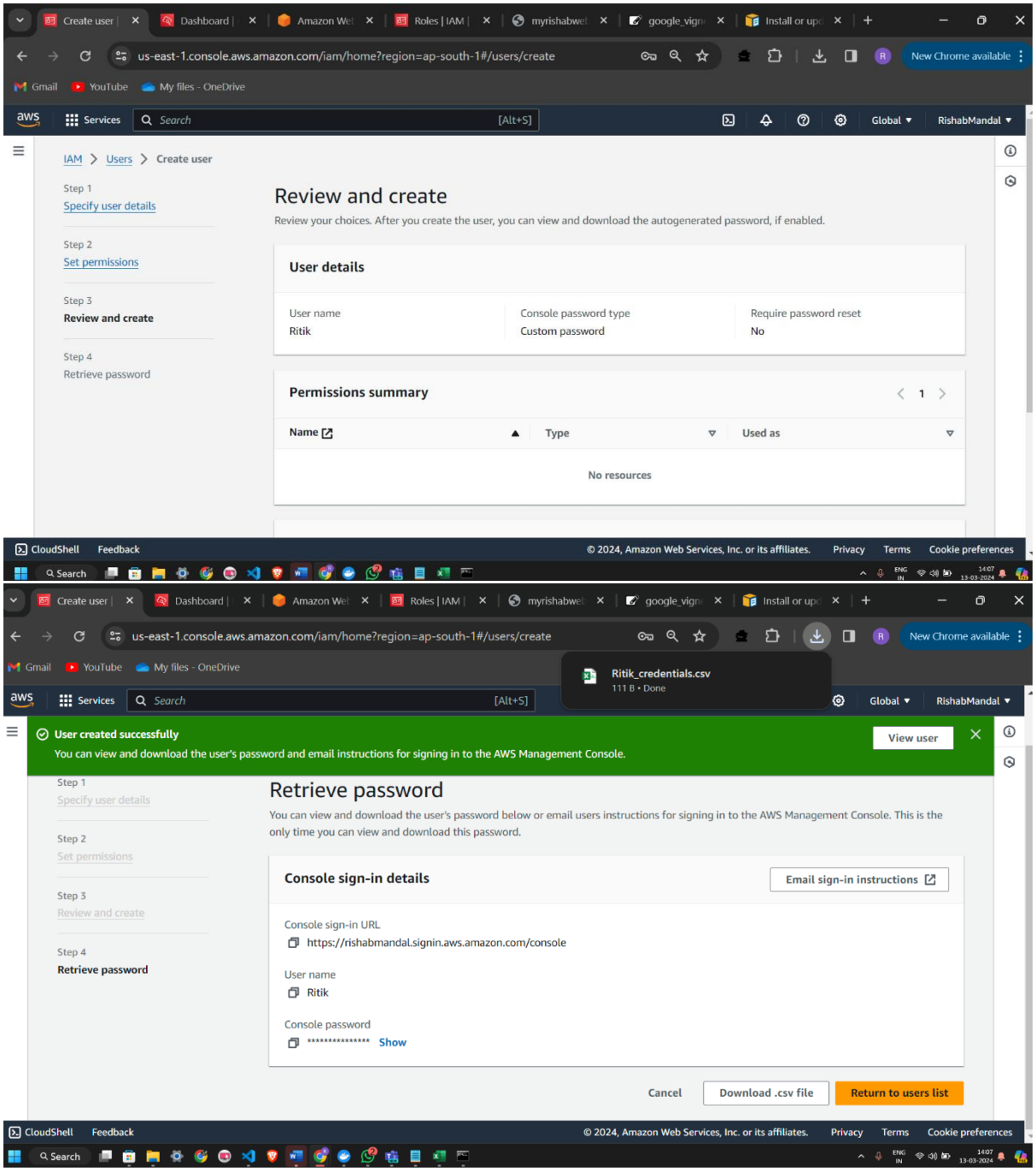

Administrator: Command Prompt - aws configure
Microsoft Windows [Version 10.0.22631.3235]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\System32>msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi /qn
C:\Windows\System32>aws --version
aws-cli/2.15.28 Python/3.11.8 Windows/10 exe/AMD64 prompt/off
C:\Windows\System32>aws configure
AWS Access Key ID [None]: AKIAZQ3DRDGNQIVEEV5I
AWS Secret Access Key [None]: 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
Default region name [None]:
Administrator: Command Prompt - aws configure
Microsoft Windows [Version 10.0.22631.3235]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\System32>msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi /qn
C:\Windows\System32>aws --version
aws-cli/2.15.28 Python/3.11.8 Windows/10 exe/AMD64 prompt/off
C:\Windows\System32>aws configure
AWS Access Key ID [None]: AKIAZQ3DRDGNQIVEEV5I
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: json

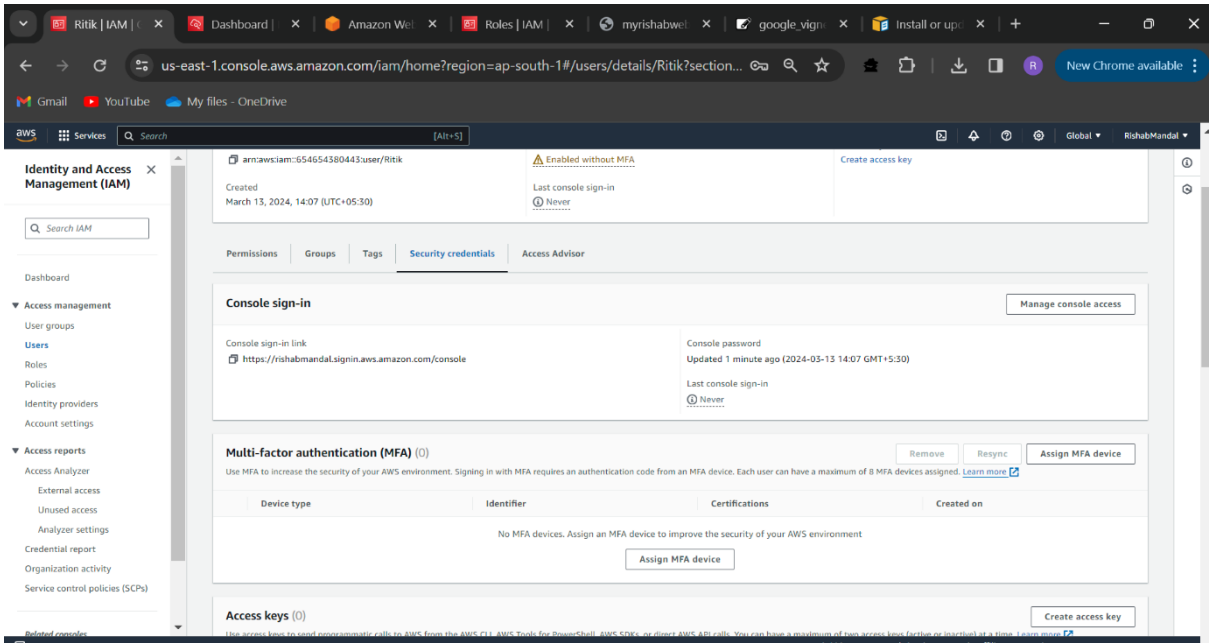

Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.3235]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\System32>msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi /qn
C:\Windows\System32>aws --version
aws-cli/2.15.28 Python/3.11.8 Windows/10 exe/AMD64 prompt/off
C:\Windows\System32>aws configure
AWS Access Key ID [None]: AKIAZQ3DRDGNQIVEEV5I
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: json
C:\Windows\System32>aws --version
aws-cli/2.15.28 Python/3.11.8 Windows/10 exe/AMD64 prompt/off
C:\Windows\System32>aws s3 ls
2024-03-01 20:40:08 elasticbeanstalk-ap-south-1-654654380443
C:\Windows\System32>

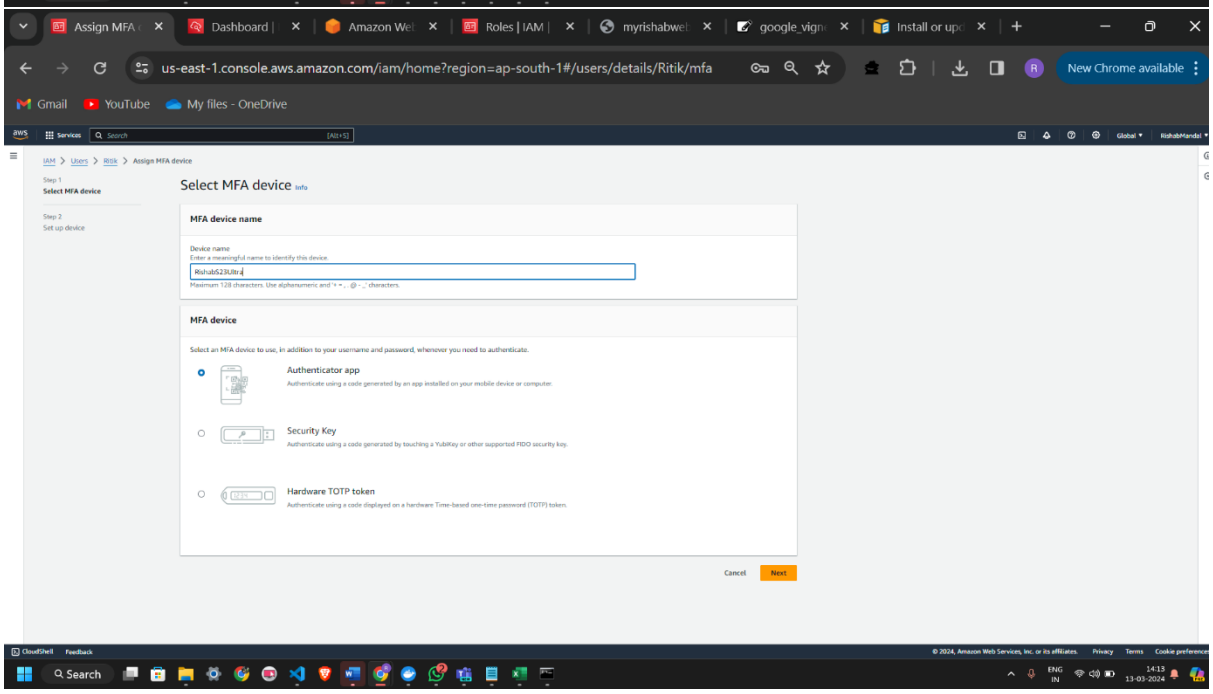

Administrator: Command Prompt
aws-cli/2.15.28 Python/3.11.8 Windows/10 exe/AMD64 prompt/off
C:\Windows\System32>aws configure
AWS Access Key ID [None]: AKIAZQ3DRDGNQIVEEV5I
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: json
C:\Windows\System32>aws --version
aws-cli/2.15.28 Python/3.11.8 Windows/10 exe/AMD64 prompt/off
C:\Windows\System32>aws s3 ls
2024-03-01 20:40:08 elasticbeanstalk-ap-south-1-654654380443
C:\Windows\System32>aws s3 mb s3://yash123456789
make_bucket failed: s3://yash123456789 An error occurred (BucketAlreadyExists) when calling the CreateBucket operation:
The requested bucket name is not available. The bucket namespace is shared by all users of the system. Please select a d
ifferent name and try again.
C:\Windows\System32>aws s3 mb s3://yash987654321
make_bucket: yash987654321
C:\Windows\System32>aws s3 ls
2024-03-01 20:40:08 elasticbeanstalk-ap-south-1-654654380443
2024-03-13 14:03:26 yash987654321
C:\Windows\System32>
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms

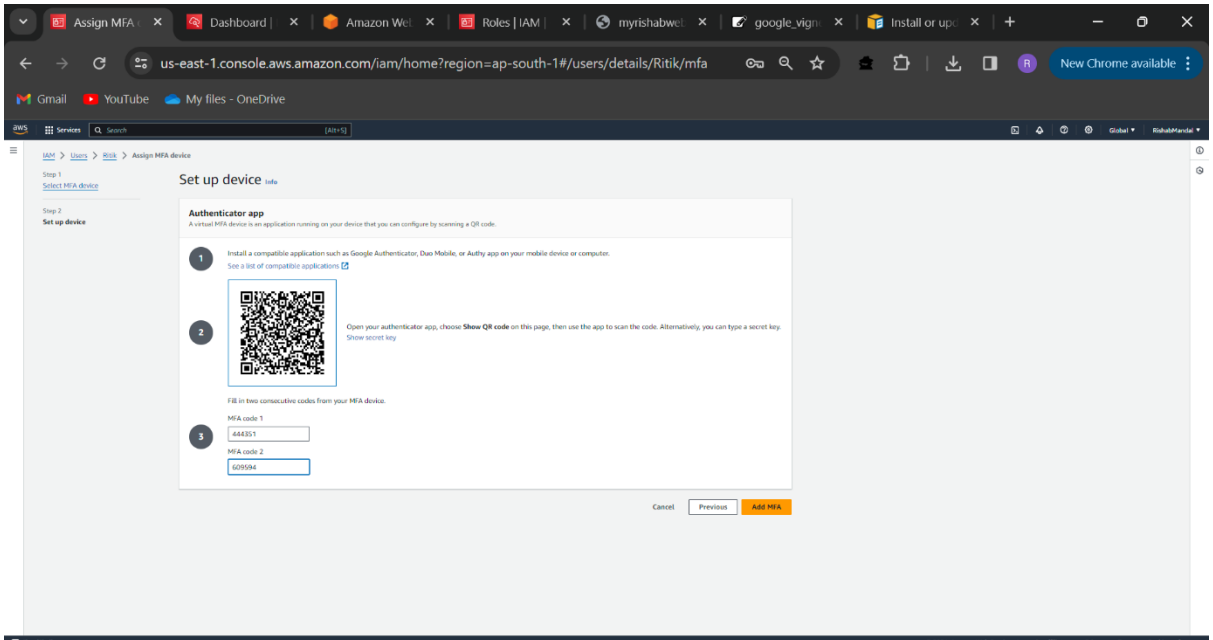
```
make_bucket failed: s3://yash123456789 An error occurred (BucketAlreadyExists) when calling the CreateBucket operation:
The requested bucket name is not available. The bucket namespace is shared by all users of the system. Please select a d
ifferent name and try again.

C:\Windows\System32>aws s3 mb s3://yash987654321
make_bucket: yash987654321

C:\Windows\System32>aws s3 ls
2024-03-01 20:40:08 elasticbeanstalk-ap-south-1-654654380443
2024-03-13 14:03:26 yash987654321

C:\Windows\System32>aws s3 rb s3://yash987654321
remove_bucket: yash987654321

C:\Windows\System32>aws s3 ls
2024-03-01 20:40:08 elasticbeanstalk-ap-south-1-654654380443

C:\Windows\System32>
```

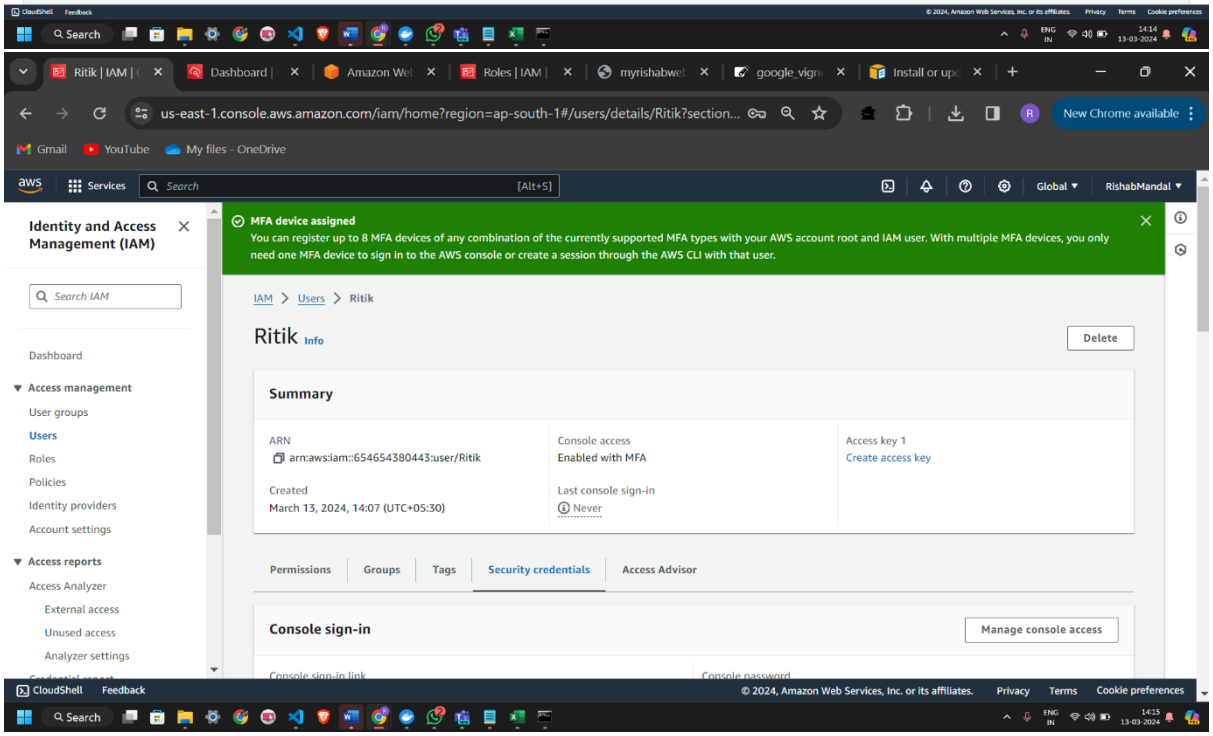


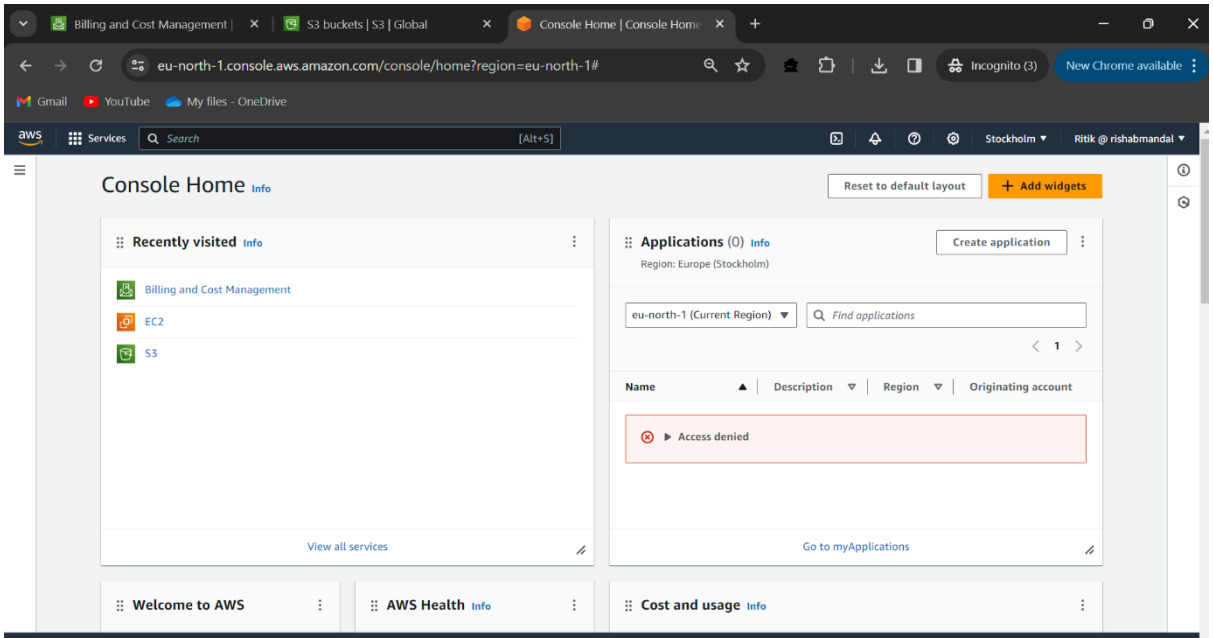

Create user
Dashboard
Amazon Web
Roles | IAM
myrishabwel
google_vigne
Install or upd
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
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
Ritik
Console password type
Custom password
Require password reset
No
Permissions summary
1
Name
Type
Used as
No resources
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
14:07
13-03-2024
Ritik_credentials.csv
111 B • Done
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
Retrieve password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.
Console sign-in details
Email sign-in instructions
Console sign-in URL
https://rishabmandal.signin.aws.amazon.com/console
User name
Ritik
Console password
********** Show
Cancel
Download .csv file
Return to users list

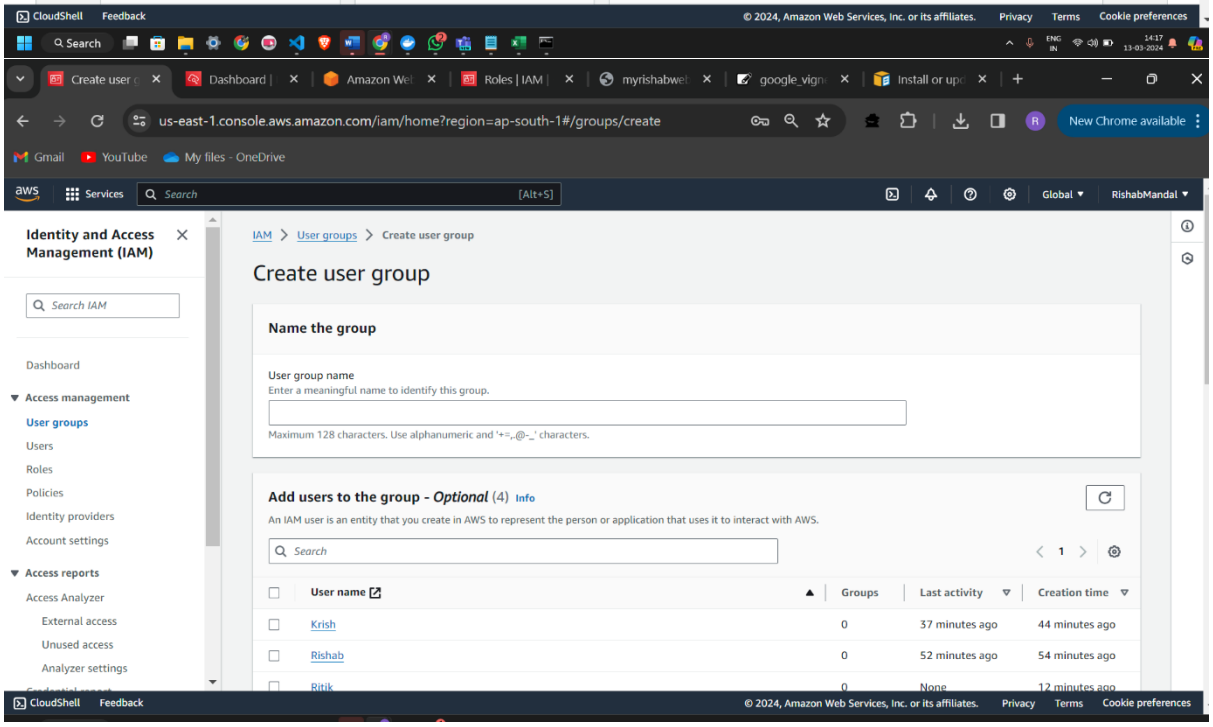

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies (SCPs)
arn:aws:iam::654654380443:user/Ritik
Enabled without MFA
Create access key
Created
March 13, 2024, 14:07 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Access Advisor
Console sign-in
Manage console access
Console sign-in link
https://rishabmandal.signin.aws.amazon.com/console
Console password
Updated 1 minute ago (2024-03-13 14:07 GMT+5:30)
Last console sign-in
Never
Multi-factor authentication (MFA) (0)
Remove
Resync
Assign MFA device
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
Device type
Identifier
Certifications
Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device
Access keys (0)
Create access key
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

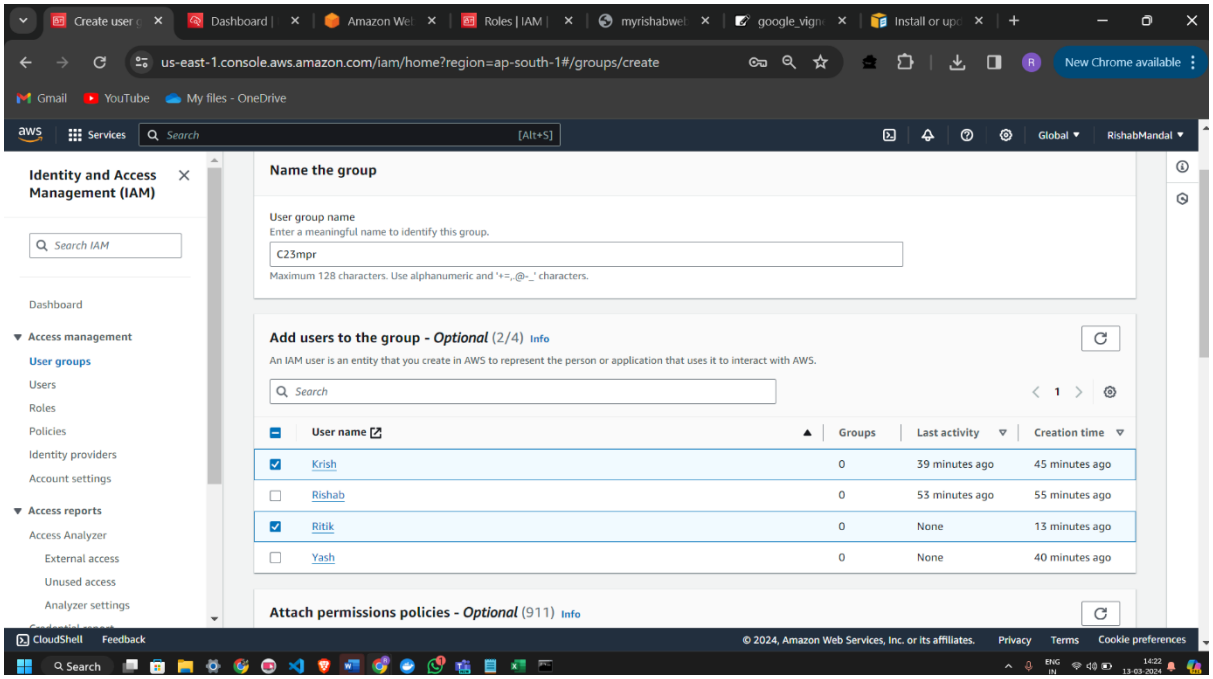

IAM > Users > Ritik > Assign MFA device
Step 1
Select MFA device
Step 2
Set up device
Select MFA device Info
MFA device name
Device name
Enter a meaningful name to identify this device.
RishabS23Ultra
Maximum 128 characters. Use alphanumeric and '+ = , . @ - _' characters.
MFA device
Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.
Authenticator app
Authenticate using a code generated by an app installed on your mobile device or computer.
Security Key
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.
Hardware TOTP token
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.
Cancel
Next

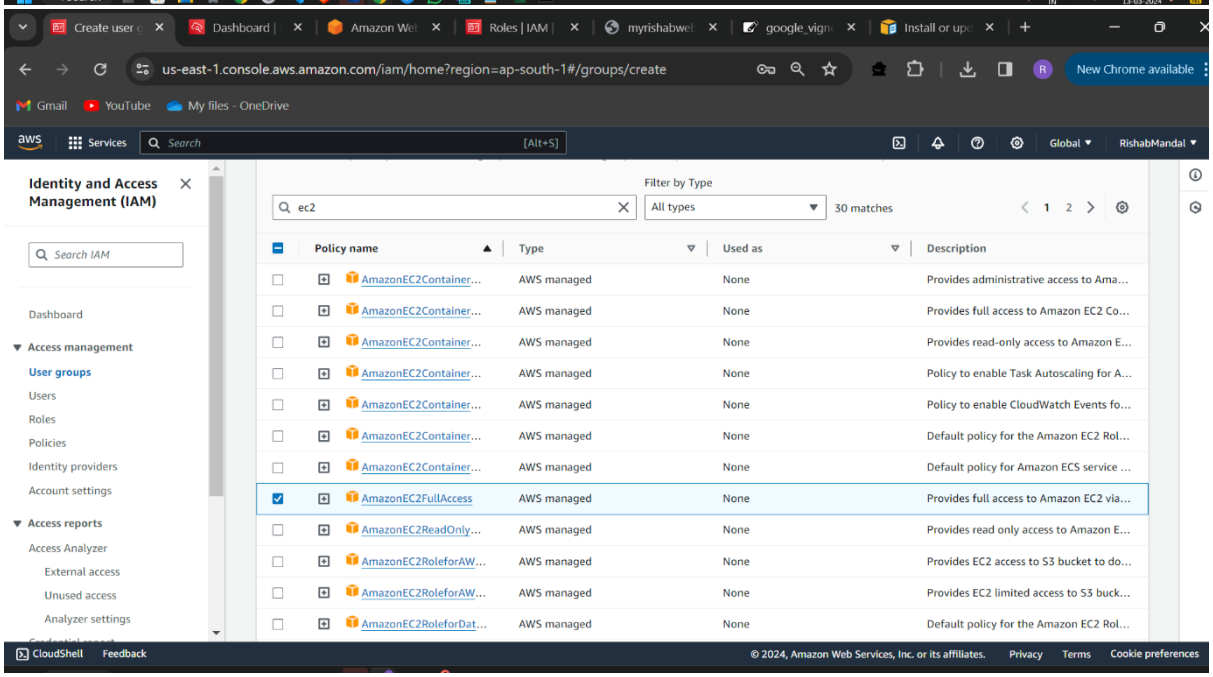

Assign MFA
Dashboard
Amazon Web
Roles | IAM
myrishabwet
google_vign
Install or upd
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Ritik/mfa
New Chrome available
Gmail
YouTube
My files - OneDrive
Services
Search
[Alt+S]
Global
RishabMandal
IAM > Users > Ritik > Assign MFA device
Step 1
Select MFA device
Step 2
Set up device
Set up device Info
Authenticator app
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.
1
Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
See a list of compatible applications
2
Open your authenticator app, choose Show QR code on this page, then use the app to scan the code. Alternatively, you can type a secret key.
Show secret key
Fill in two consecutive codes from your MFA device.
3
MFA code 1
444351
MFA code 2
609594
Cancel
Previous
Add MFA

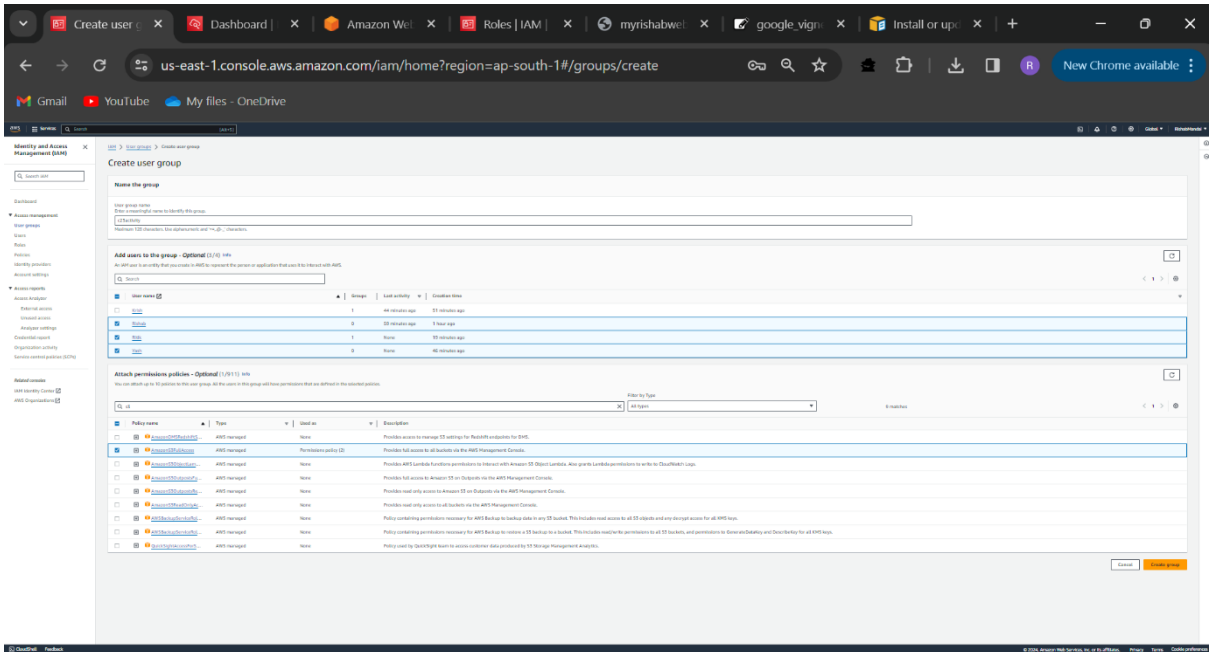

Ritik | IAM
Dashboard
Amazon Web
Roles | IAM
myrishabwet
google_vign
Install or upd
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Ritik?section...
New Chrome available
Gmail
YouTube
My files - OneDrive
Services
Search
[Alt+S]
Global
RishabMandal
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
MFA device assigned
You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.
IAM > Users > Ritik
Ritik Info
Delete
Summary
ARN
arn:aws:iam::654654380443:user/Ritik
Console access
Enabled with MFA
Access key 1
Create access key
Created
March 13, 2024, 14:07 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Access Advisor
Console sign-in
Manage console access
Console sign-in link
Console password
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

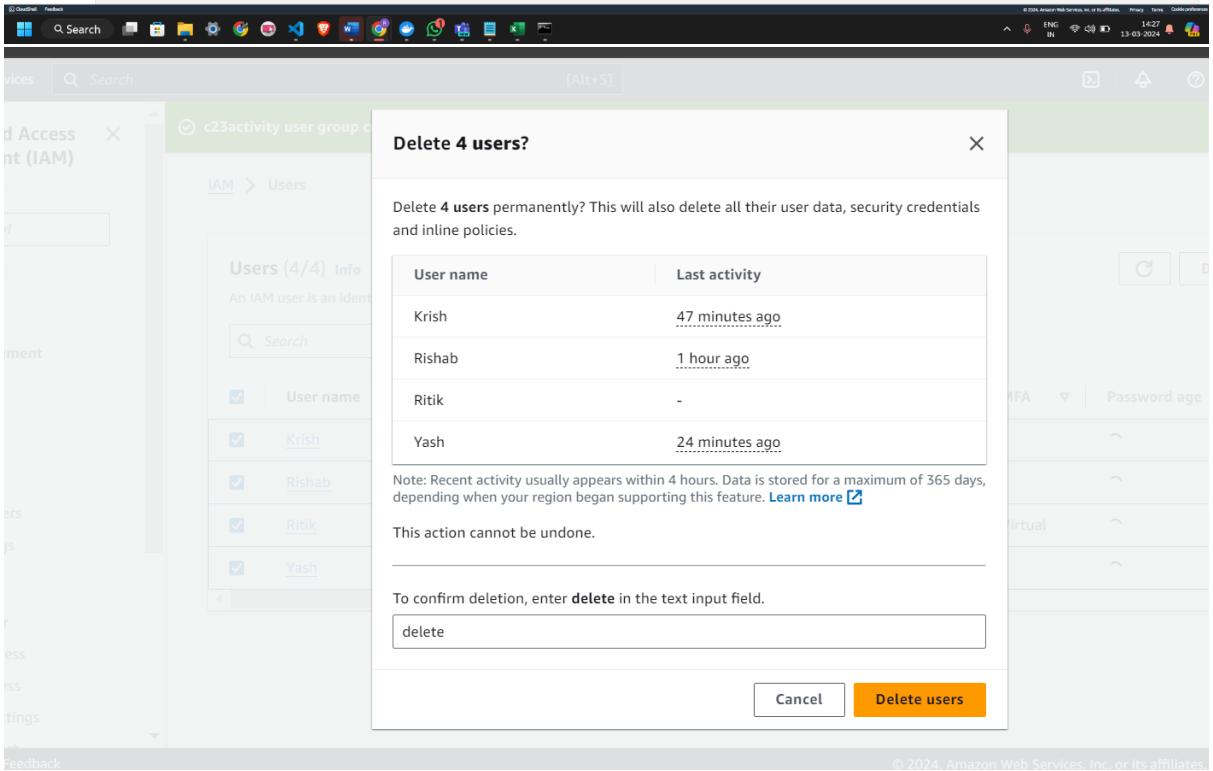

Billing and Cost Management
S3 buckets | S3 | Global
Console Home | Console Home
eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1#
Incognito (3)
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Stockholm
Ritik @ rishabmandal
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
Billing and Cost Management
EC2
S3
View all services
Applications (0) Info
Region: Europe (Stockholm)
Create application
eu-north-1 (Current Region)
Find applications
Name
Description
Region
Originating account
Access denied
Go to myApplications
Welcome to AWS
AWS Health Info
Cost and usage Info
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

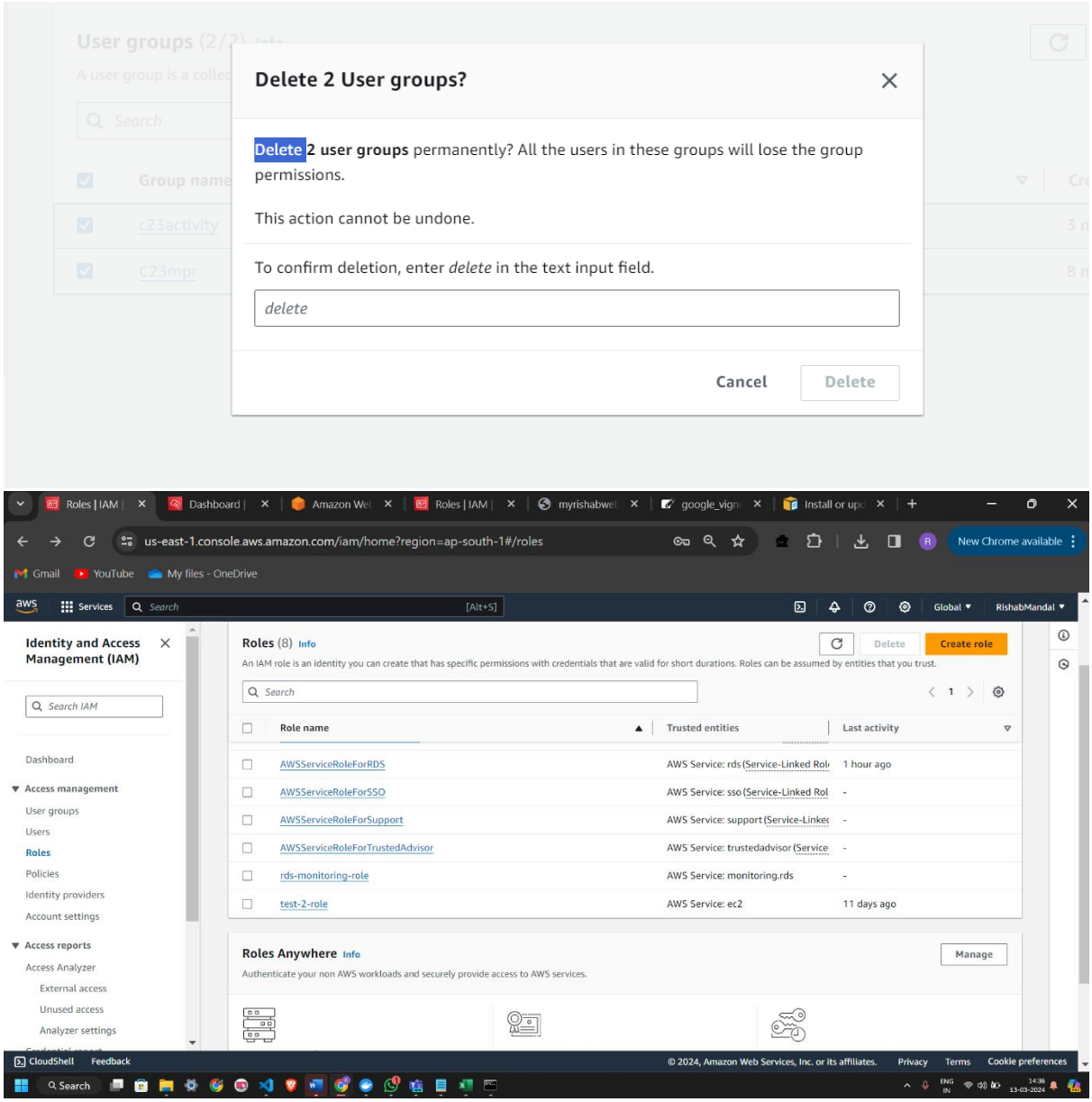

Create user
Dashboard
Amazon Web
Roles | IAM
myrishabweb
google_vign
Install or upd
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/create
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
IAM > User groups > Create user group
Create user group
Name the group
User group name
Enter a meaningful name to identify this group.
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Add users to the group - Optional (4) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Search
User name
Groups
Last activity
Creation time
Krish
0
37 minutes ago
44 minutes ago
Rishab
0
52 minutes ago
54 minutes ago
Ritik
0
None
12 minutes ago
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Create user
Dashboard
Amazon Wel
Roles | IAM
myrishabwel
google_vign
Install or upd
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/create
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Name the group
User group name
Enter a meaningful name to identify this group.
C23mpr
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Add users to the group - Optional (2/4) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Search
1
User name
Groups
Last activity
Creation time
Krish
0
39 minutes ago
45 minutes ago
Rishab
0
53 minutes ago
55 minutes ago
Ritik
0
None
13 minutes ago
Yash
0
None
40 minutes ago
Attach permissions policies - Optional (911) Info
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

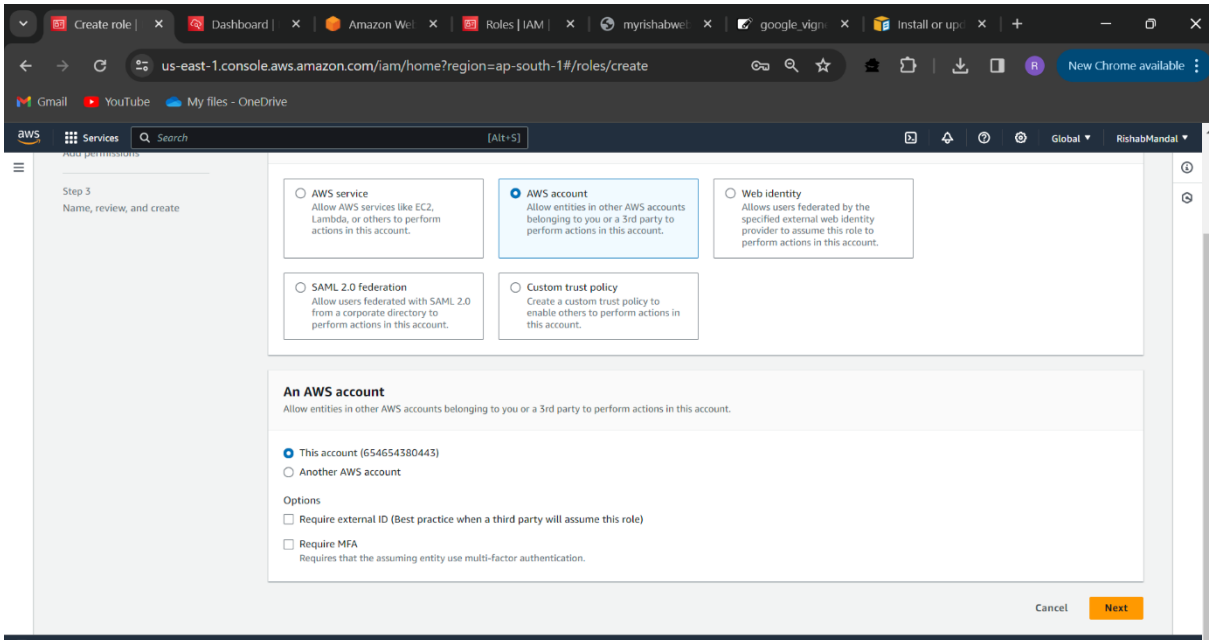

Create user
Dashboard
Amazon Wel
Roles | IAM
myrishabwel
google_vign
Install or upd
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/create
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Filter by Type
ec2
All types
30 matches
1
2
Policy name
Type
Used as
Description
AmazonEC2Container...
AWS managed
None
Provides administrative access to Ama...
AmazonEC2Container...
AWS managed
None
Provides full access to Amazon EC2 Co...
AmazonEC2Container...
AWS managed
None
Provides read-only access to Amazon E...
AmazonEC2Container...
AWS managed
None
Policy to enable Task Autoscaling for A...
AmazonEC2Container...
AWS managed
None
Policy to enable CloudWatch Events fo...
AmazonEC2Container...
AWS managed
None
Default policy for the Amazon EC2 Rol...
AmazonEC2Container...
AWS managed
None
Default policy for Amazon ECS service ...
AmazonEC2FullAccess
AWS managed
None
Provides full access to Amazon EC2 via...
AmazonEC2ReadOnly...
AWS managed
None
Provides read only access to Amazon E...
AmazonEC2RoleforAW...
AWS managed
None
Provides EC2 access to S3 bucket to do...
AmazonEC2RoleforAW...
AWS managed
None
Provides EC2 limited access to S3 buck...
AmazonEC2RoleforDat...
AWS managed
None
Default policy for the Amazon EC2 Rol...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

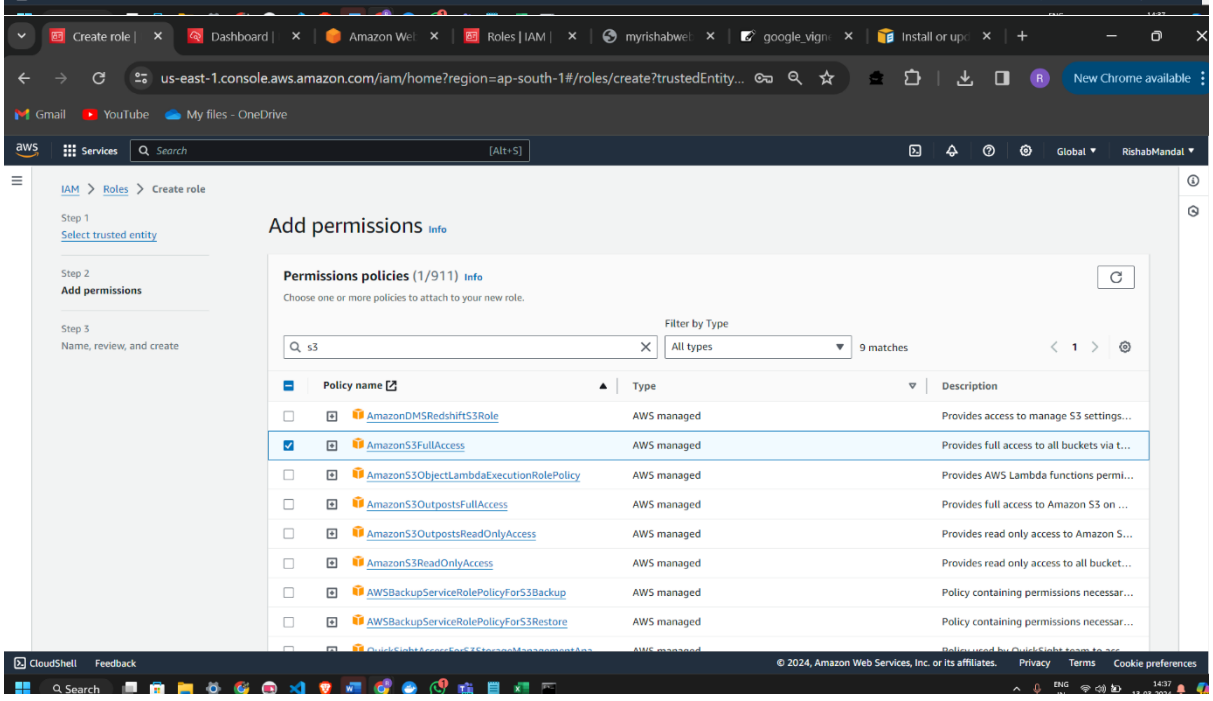

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/create
Create user group

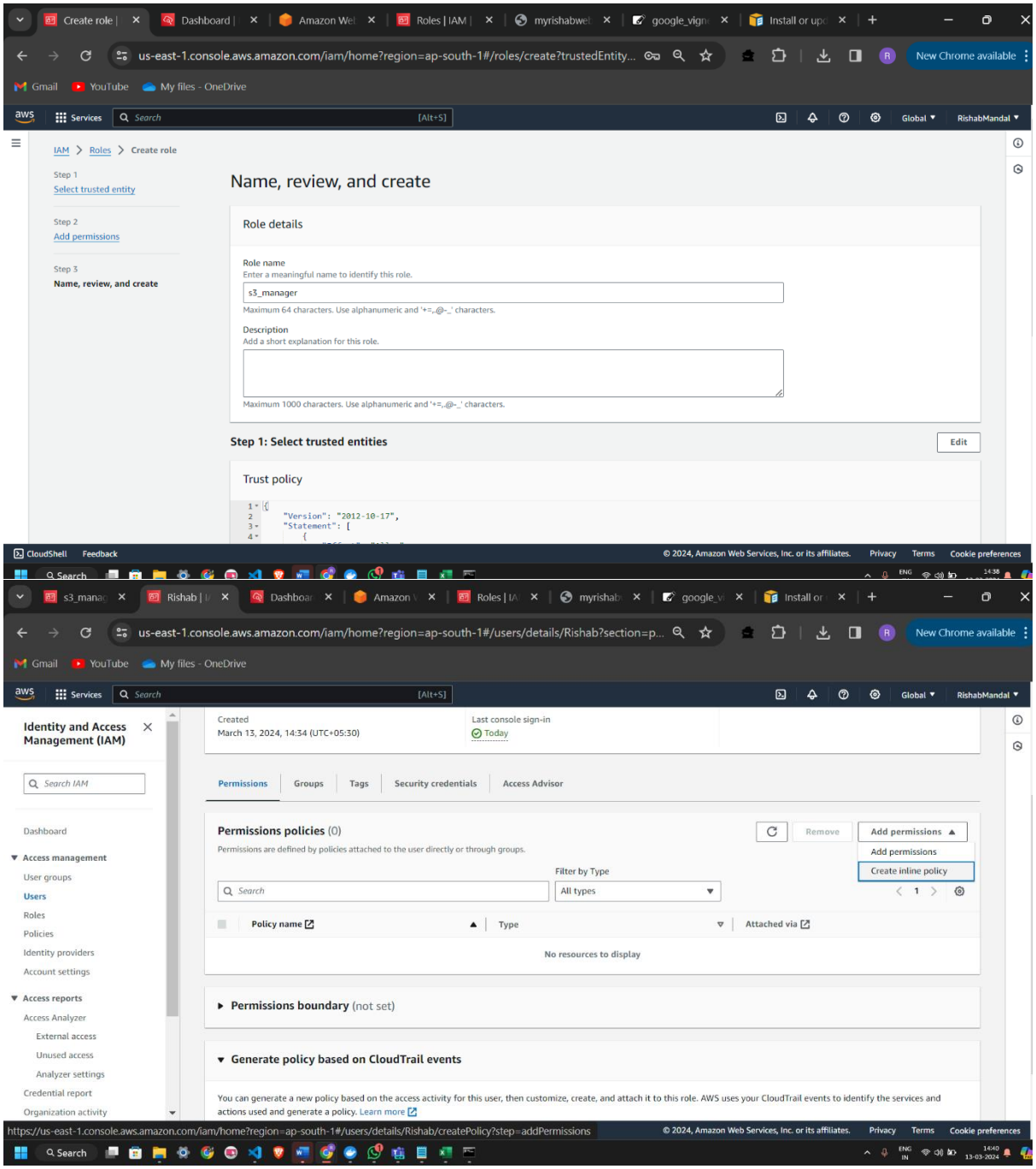

Delete 4 users?
Delete 4 users permanently? This will also delete all their user data, security credentials and inline policies.
User name
Last activity
Krish
47 minutes ago
Rishab
1 hour ago
Ritik
-
Yash
24 minutes ago
Note: Recent activity usually appears within 4 hours. Data is stored for a maximum of 365 days, depending when your region began supporting this feature. Learn more
This action cannot be undone.
To confirm deletion, enter delete in the text input field.
delete
Cancel
Delete users


User groups (2/2) Info
A user group is a collec
Search
Group name
c23activity
C23mpr
Delete 2 User groups?
Delete 2 user groups permanently? All the users in these groups will lose the group permissions.
This action cannot be undone.
To confirm deletion, enter delete in the text input field.
delete
Cancel
Delete

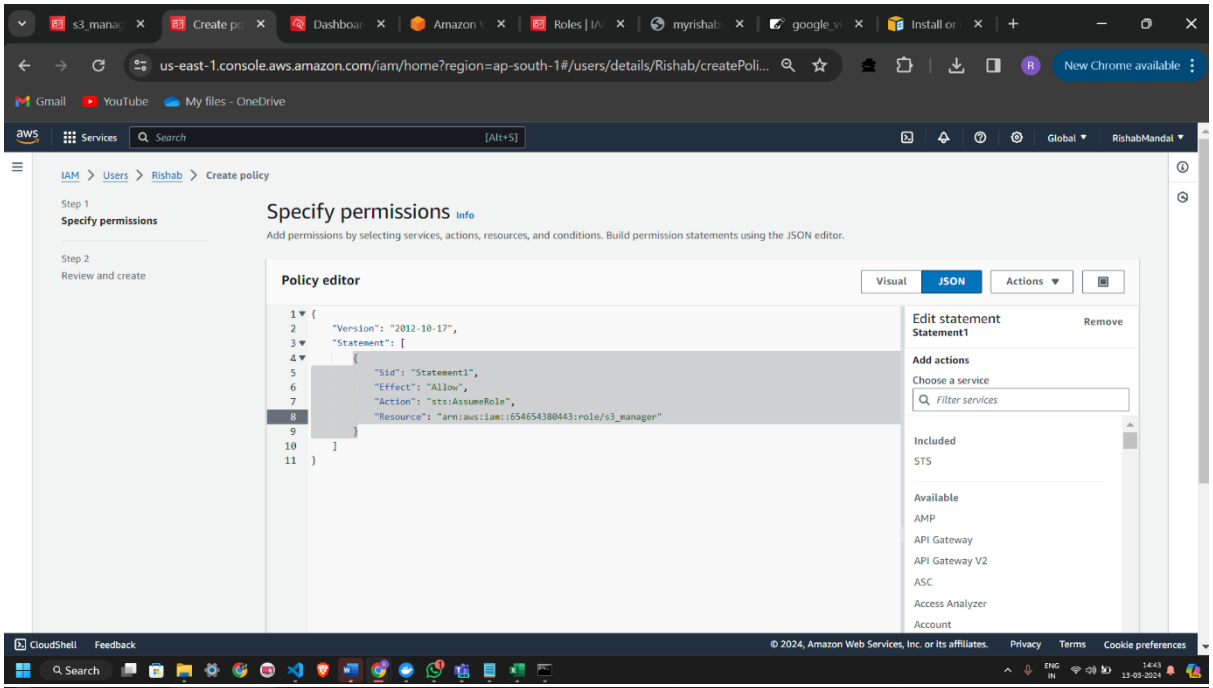
Roles | IAM
Dashboard
Amazon We
Roles | IAM
myrishabwe
google_vign
Install or up
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Roles (8) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Delete
Create role
Search
Role name
Trusted entities
Last activity
AWSServiceRoleForRDS
AWS Service: rds (Service-Linked Rol
1 hour ago
AWSServiceRoleForSSO
AWS Service: sso (Service-Linked Rol
-
AWSServiceRoleForSupport
AWS Service: support (Service-Linkec
-
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service
-
rds-monitoring-role
AWS Service: monitoring.rds
-
test-2-role
AWS Service: ec2
11 days ago
Roles Anywhere Info
Authenticate your non AWS workloads and securely provide access to AWS services.
Manage
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
14:36
13-03-2024

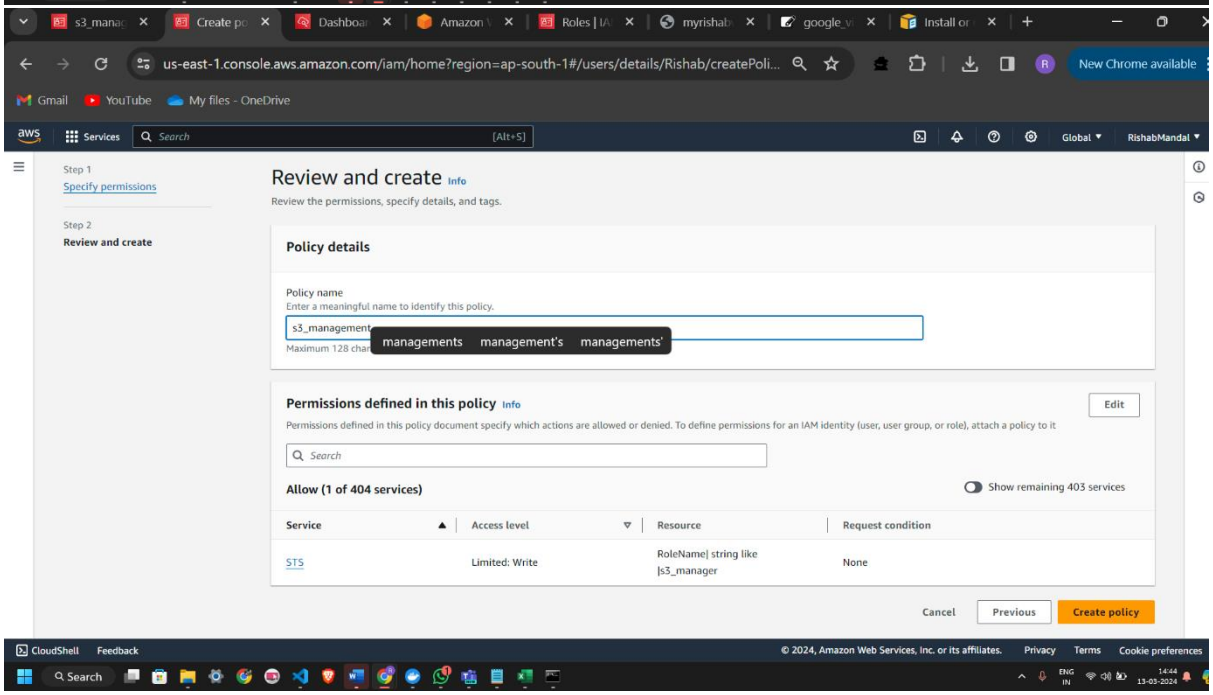

Create role
Dashboard
Amazon Web
Roles | IAM
myrishabwel
google_vign
Install or upd
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
Step 3
Name, review, and create
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
This account (654654380443)
Another AWS account
Options
Require external ID (Best practice when a third party will assume this role)
Require MFA
Requires that the assuming entity use multi-factor authentication.
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

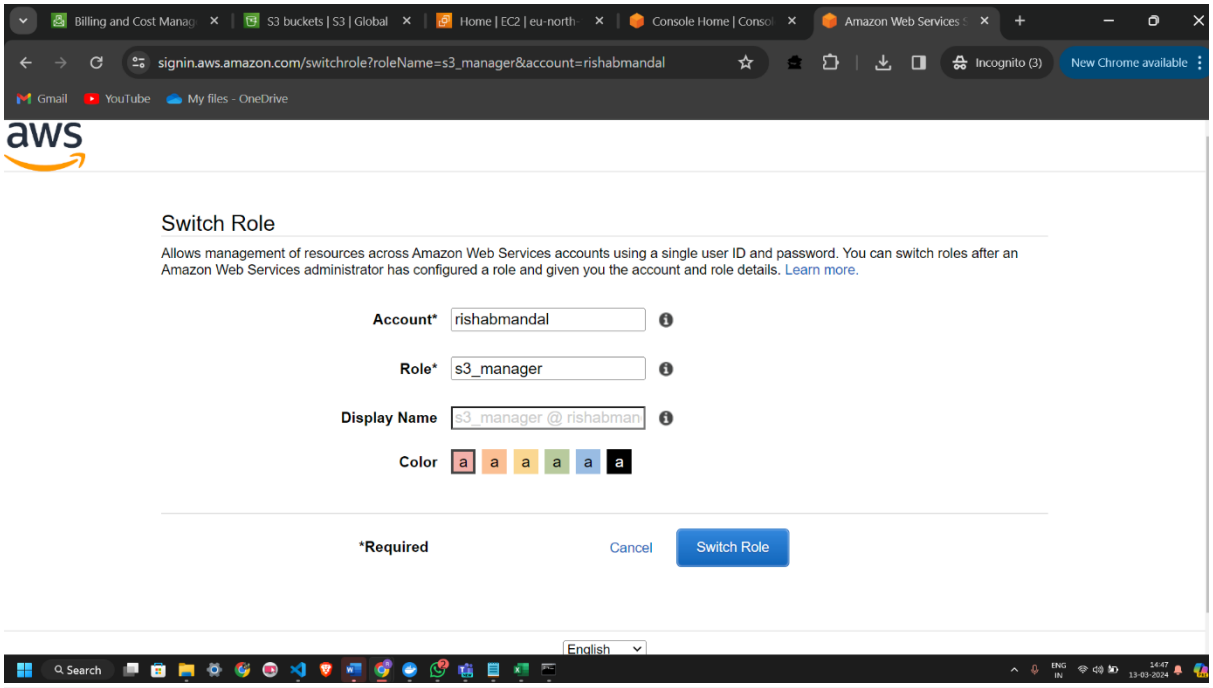

Create role
Dashboard
Amazon Web
Roles | IAM
myrishabwel
google_vign
Install or upd
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntity...
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1/911) Info
Choose one or more policies to attach to your new role.
Filter by Type
s3
All types
9 matches
1
Policy name
Type
Description
AmazonDMSRedshiftS3Role
AWS managed
Provides access to manage S3 settings...
AmazonS3FullAccess
AWS managed
Provides full access to all buckets via t...
AmazonS3ObjectLambdaExecutionRolePolicy
AWS managed
Provides AWS Lambda functions permi...
AmazonS3OutpostsFullAccess
AWS managed
Provides full access to Amazon S3 on ...
AmazonS3OutpostsReadOnlyAccess
AWS managed
Provides read only access to Amazon S...
AmazonS3ReadOnlyAccess
AWS managed
Provides read only access to all bucket...
AWSBackupServiceRolePolicyForS3Backup
AWS managed
Policy containing permissions necessar...
AWSBackupServiceRolePolicyForS3Restore
AWS managed
Policy containing permissions necessar...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search

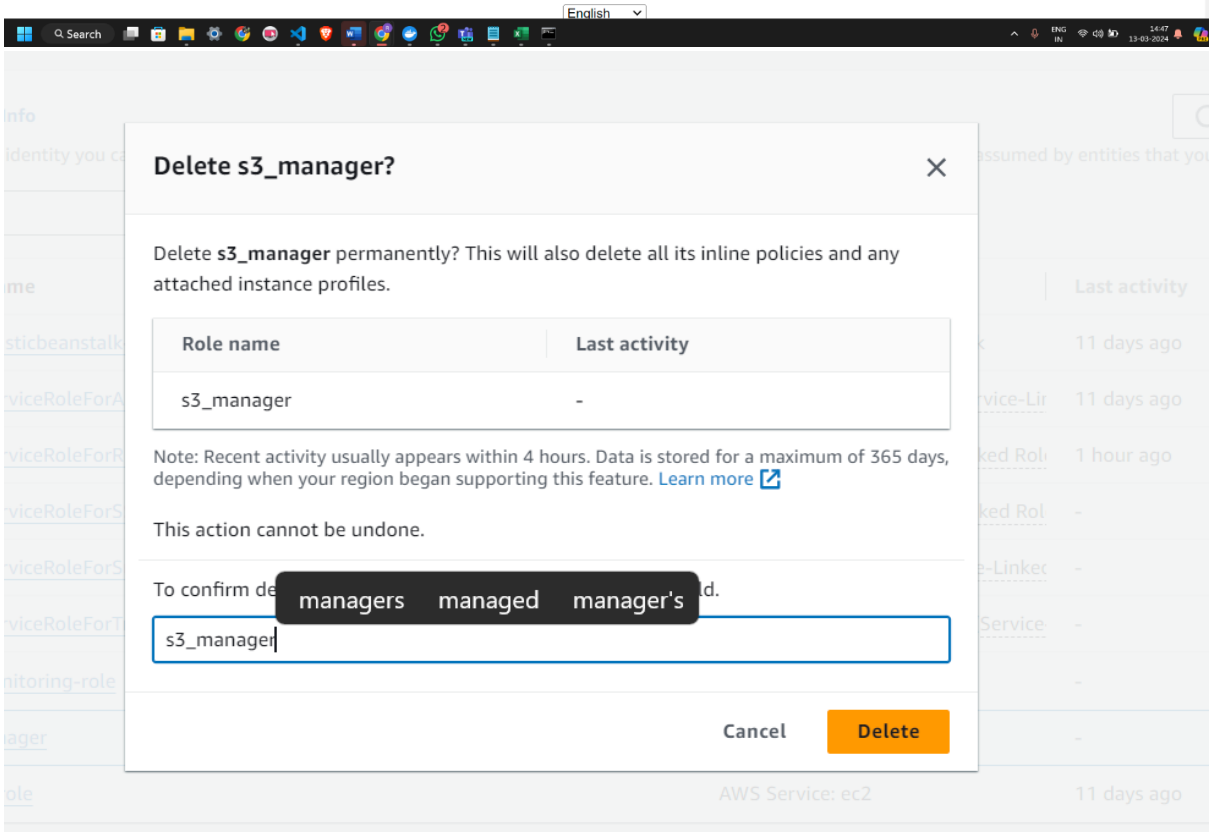

Create role
Dashboard
Amazon Web
Roles | IAM
myrishabweb
google_vignan
Install or update
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntity...
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
s3_manager
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{

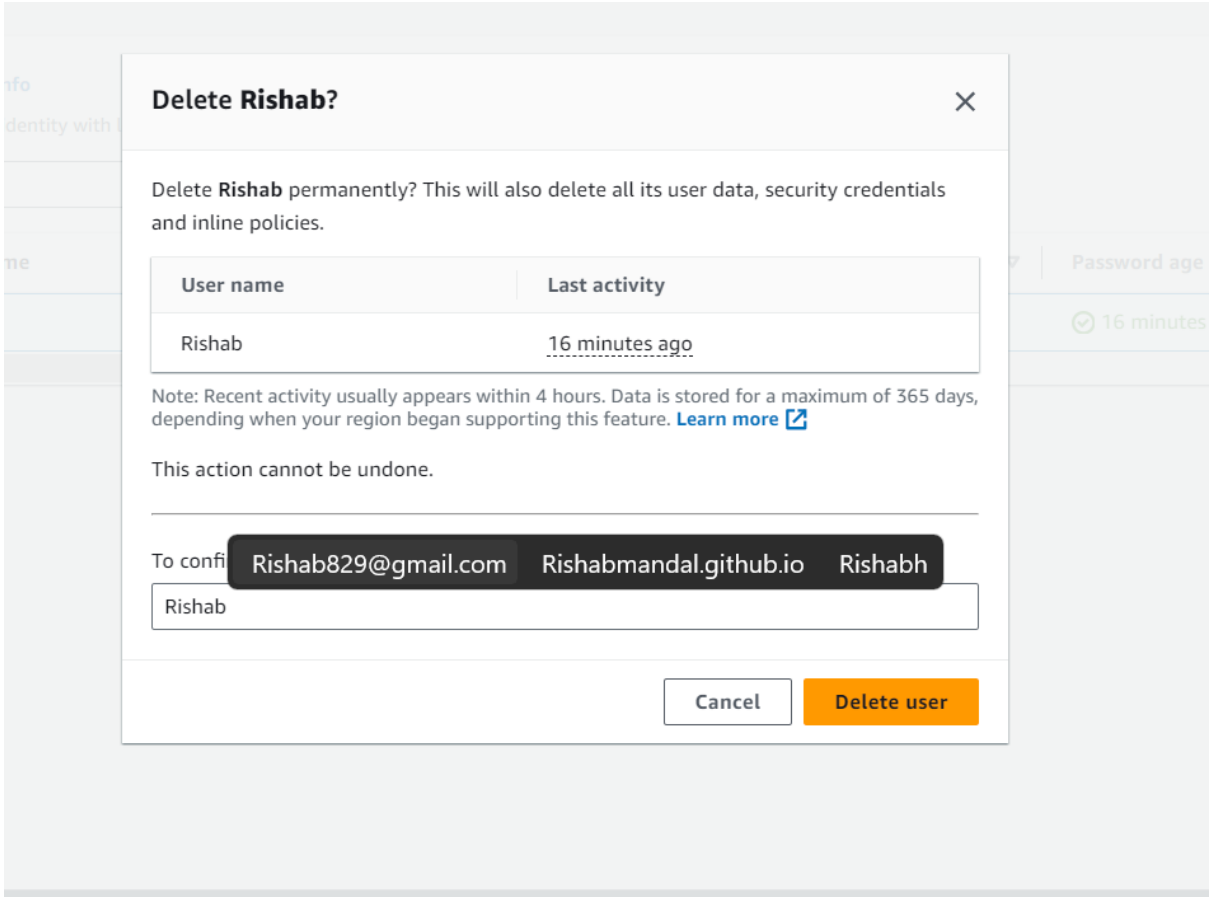
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
s3_manag
Rishab | I
Dashboar
Amazon
Roles | IA
myrishab
google_v
Install or
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Rishab?section=p...
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Services
Search
[Alt+S]
Global
RishabMandal
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Created
March 13, 2024, 14:34 (UTC+05:30)
Last console sign-in
Today
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (0)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Add permissions
Create inline policy
Filter by Type
Search
All types
Policy name
Type
Attached via
No resources to display
Permissions boundary (not set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Rishab/createPolicy?step=addPermissions
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search


us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Rishab/createPoli...
New Chrome available
Gmail
YouTube
My files - OneDrive
Services
Search
[Alt+S]
Global
RishabMandal
IAM > Users > Rishab > 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
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Statement1",
"Effect": "Allow",
"Action": "sts:AssumeRole",
"Resource": "arn:aws:iam::654654380443:role/s3_manager"
}
]
}
Edit statement
Statement1
Remove
Add actions
Choose a service
Filter services
Included
STS
Available
AMP
API Gateway
API Gateway V2
ASC
Access Analyzer
Account
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Rishab/createPoli...
New Chrome available
Gmail
YouTube
My files - OneDrive
Services
Search
[Alt+S]
Global
RishabMandal
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.
s3_management
managements
management's
managements'
Maximum 128 char
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 404 services)
Show remaining 403 services
Service
Access level
Resource
Request condition
STS
Limited: Write
RoleName| string like |s3_manager
None
Cancel
Previous
Create policy
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Billing and Cost Manag
S3 buckets | S3 | Global
Home | EC2 | eu-north
Console Home | Consol
Amazon Web Services
signin.aws.amazon.com/switchrole?roleName=s3_manager&account=rishabmandal
Incognito (3)
New Chrome available
Gmail
YouTube
My files - OneDrive
aws
Switch Role
Allows management of resources across Amazon Web Services accounts using a single user ID and password. You can switch roles after an Amazon Web Services administrator has configured a role and given you the account and role details. Learn more.
Account*
rishabmandal
Role*
s3_manager
Display Name
s3_manager @ rishabman
Color
*Required
Cancel
Switch Role
English


Search
Delete s3_manager?
Delete s3_manager permanently? This will also delete all its inline policies and any attached instance profiles.
Role name
Last activity
s3_manager
-
Note: Recent activity usually appears within 4 hours. Data is stored for a maximum of 365 days, depending when your region began supporting this feature. Learn more
This action cannot be undone.
To confirm de
managers
managed
manager's
s3_manager
Cancel
Delete



Conclusion:

In conclusion, mastering IAM practices on AWS is crucial for maintaining a secure and compliant cloud environment. Understanding the differences between root users and IAM users, roles and policies, and implementing MFA adds layers of security necessary for protecting valuable resources and data in the cloud.