Name: Ruchika
SAP ID: 86062300062

PRACTICAL-3

USERS and GROUPS

USERS:

→ In cloud computing, users are individuals entities that require access to ~~some~~ cloud resource and services. Users can be human individuals or non-human entities (such as applications or services).

→ Each user has a unique identity and is authenticated through credentials like usernames, passwords, API keys or certificates.

→ Users are assigned permissions that define what actions they can perform within the cloud environment.

Key aspects of Users:

→ Identity Management: Ensures each user has a unique identity.

→ Authentication: Verifies user identity through methods like passwords or multi factor authentication.

→ Authorization: Determines what actions a user can perform based on permissions.

→ Types: End users, service accounts, administrators and external users.

GROUPS :

→ Groups in cloud computing are collections of users who share similar roles or access needs.

→ Groups simplify permission management by allowing administrators to assign permissions and policies collectively rather than individually.

→ This approach especially useful & is large organisations, where managing individual user permissions can be complex.

Key aspects of groups :

- Role-based access control (RBAC) : Assigns permissions based on roles to enhance security and reduce administrative tasks.
- Policy enforcement : Ensures consistent application of security process across all groups members.
- Scalability : Facilitates management of permissions for large members of users.
- Types : Security groups, resource groups and user groups.

(2) IDENTITY and ACCESS MANAGEMENT (IAM)?

→ Identity and Access management (IAM) is a combination of policies of technologies that allows organizations to identify users and provide the right form of access as and when required.

→ There has been a burst in the market with new applications and the requirements for an organization to use these applications has increased drastically.

→ The services and resources you want to access can be specified in IAM. IAM doesn't provide any replica or backups. IAM can be used for many purpose such as if one wants to control access of individual groups access for your AWS resources.

→ With IAM policies, managing permissions to your workforce and system to ensure least privilge permissions becomes easier.

→ Components of Identity and Access Management (IAM)

1. Roles
2. Groups
3. Policies

→ IAM identifies classified as

1. IAM users
2. IAM Groups
3. IAM Roles.

3. IAM ROLES

→ A role is a set of permissions that grant access to actions and resources in AWS.

→ These permissions are attached to the role, not to an IAM user or a group.

→ An IAM user can use a role in the same AWS account or a different account.

→ An IAM user is similar to a IAM user ; role is also an AWS identity with permission policies that determine what the identity can & cannot do in AWS.

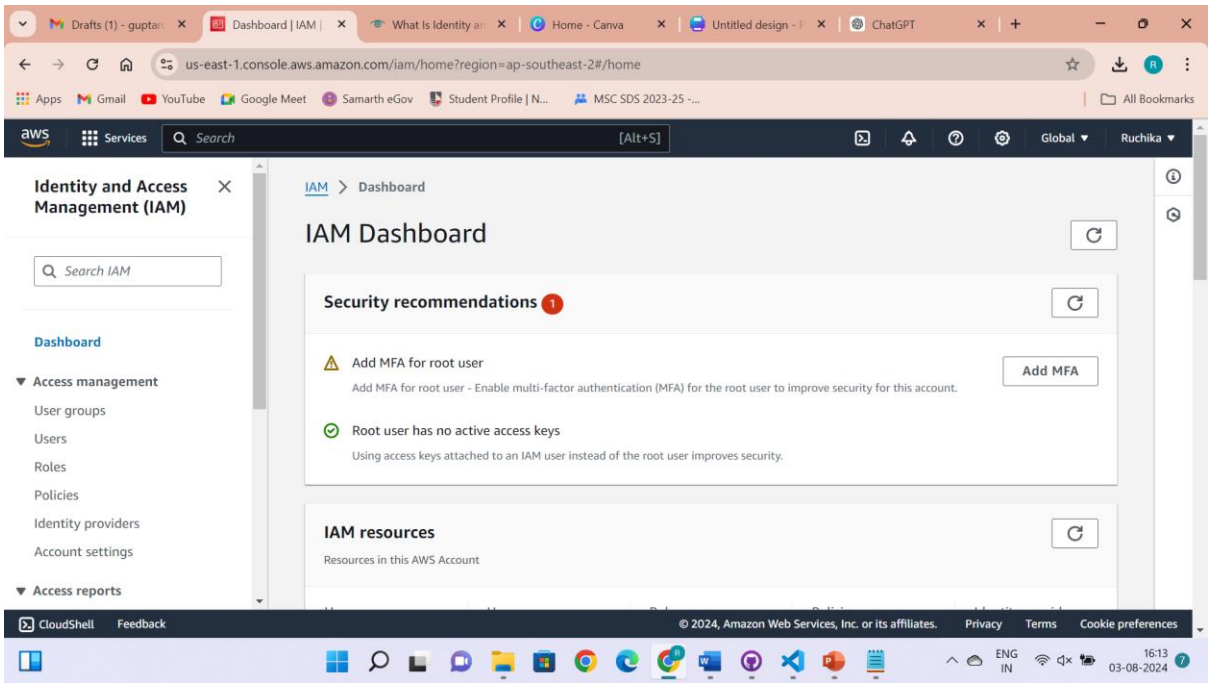
→ A role is a not uniquely associated with a single person, it can be used by anyone who needs it.

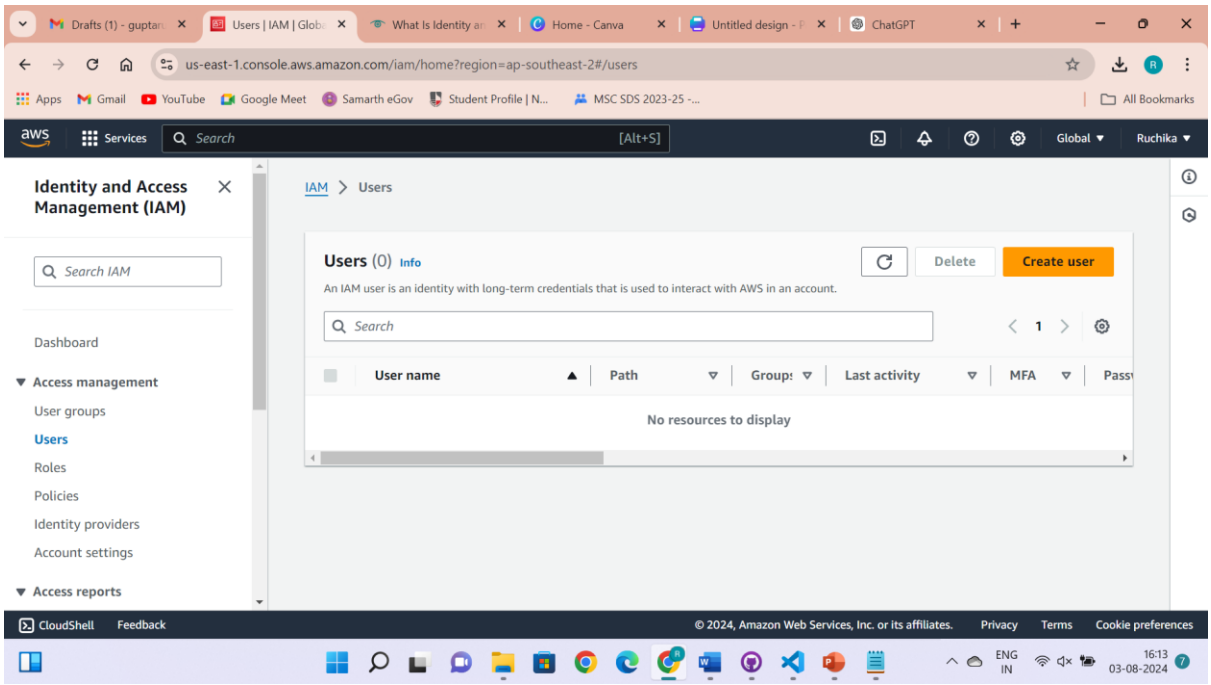
→ A role is does not have long term security credential i.e. password or security by instead if the user uses a role, temporarily security credentials are instead created and provided to the user.

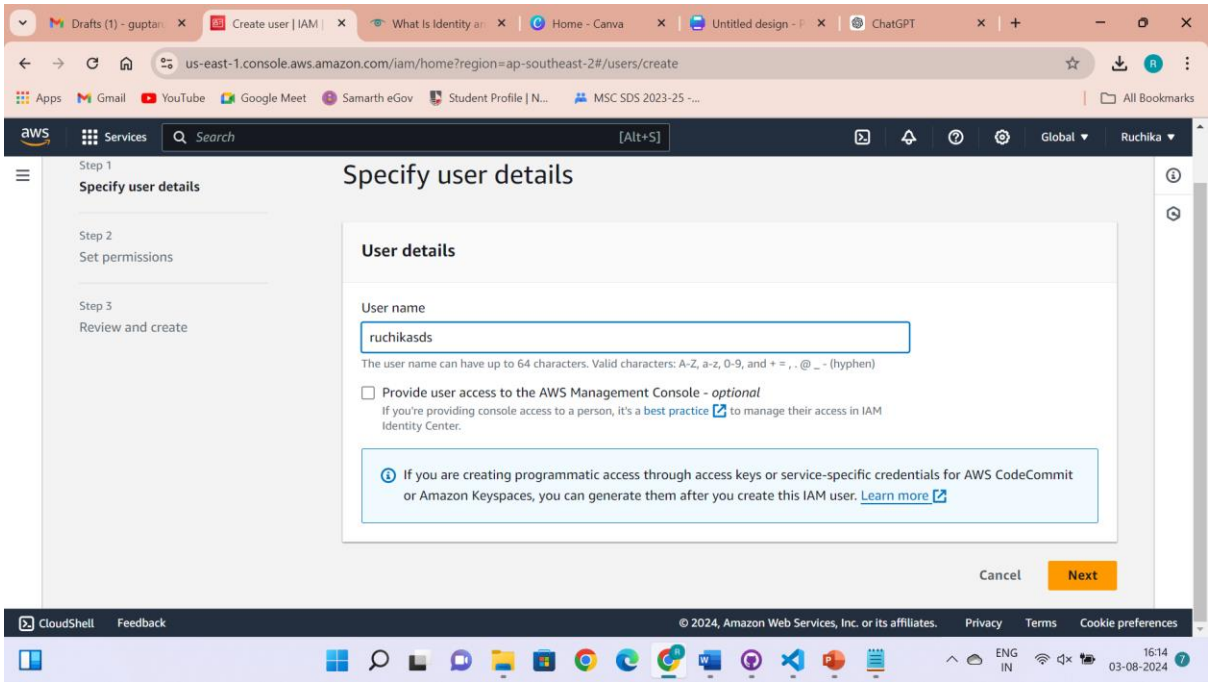
→ You can use the roles to delegate access to users, application or services that generally do not have access to your AWS account/resources.

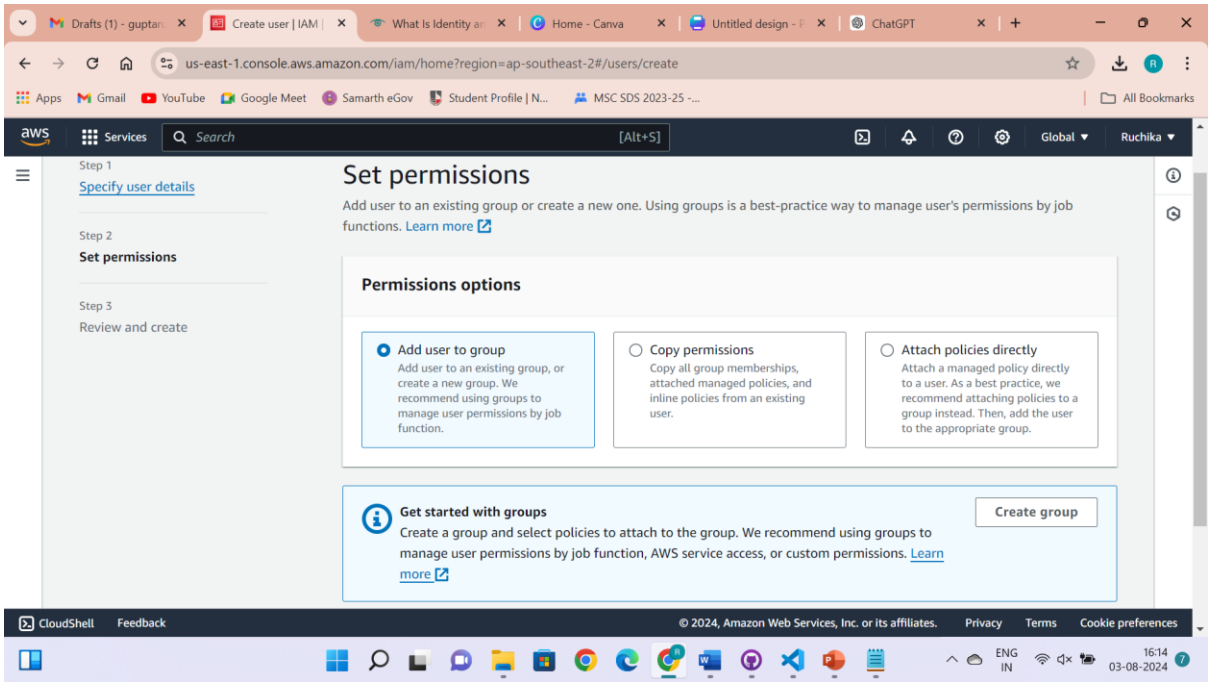
CLOUD COMPUTING
PRACTICAL-3

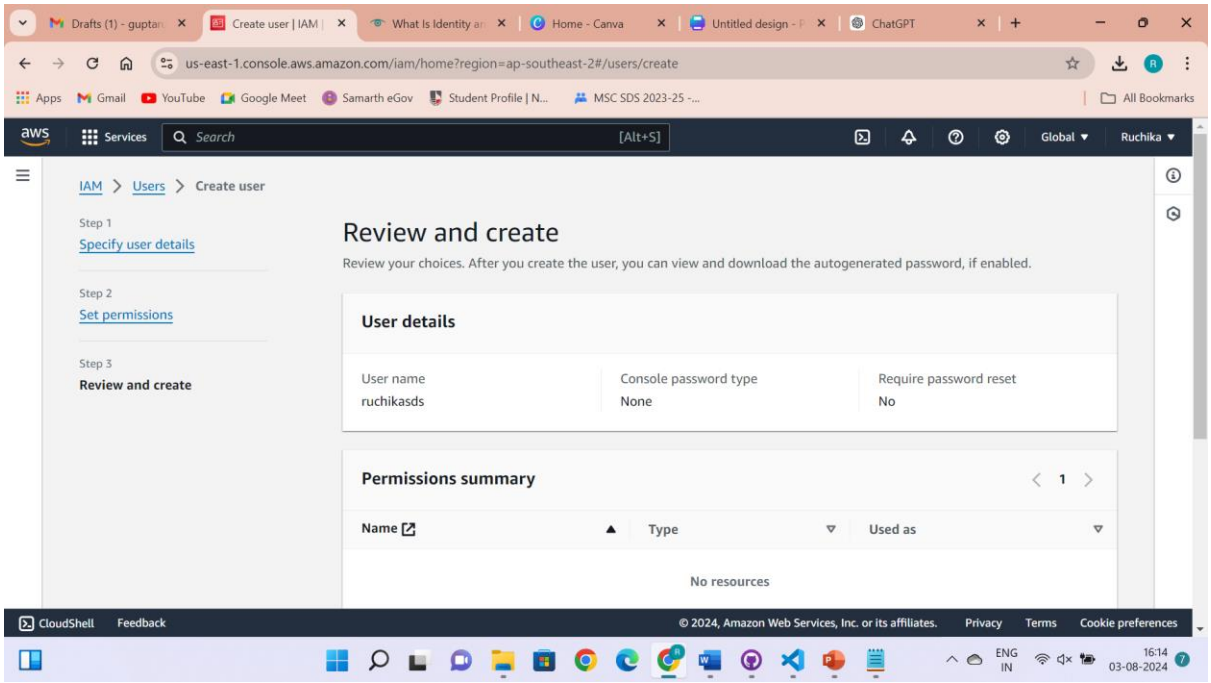
Ruchika (RollNo-19)
86062300062
Msc. Statistics and Data Science

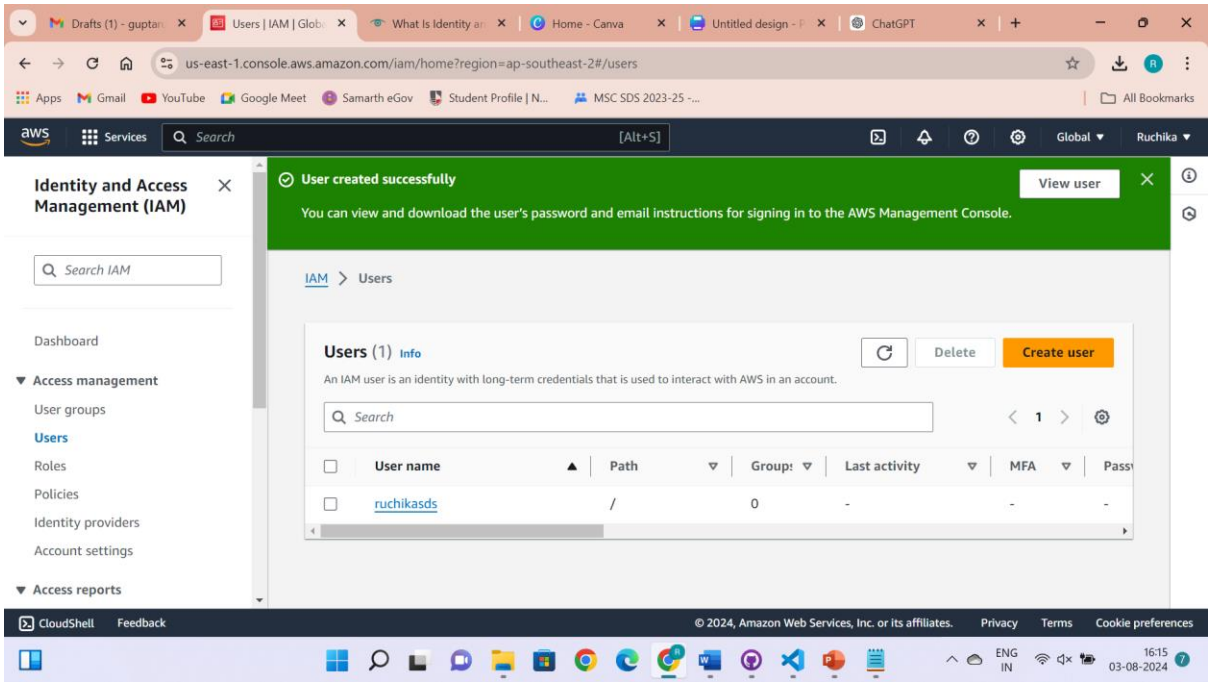


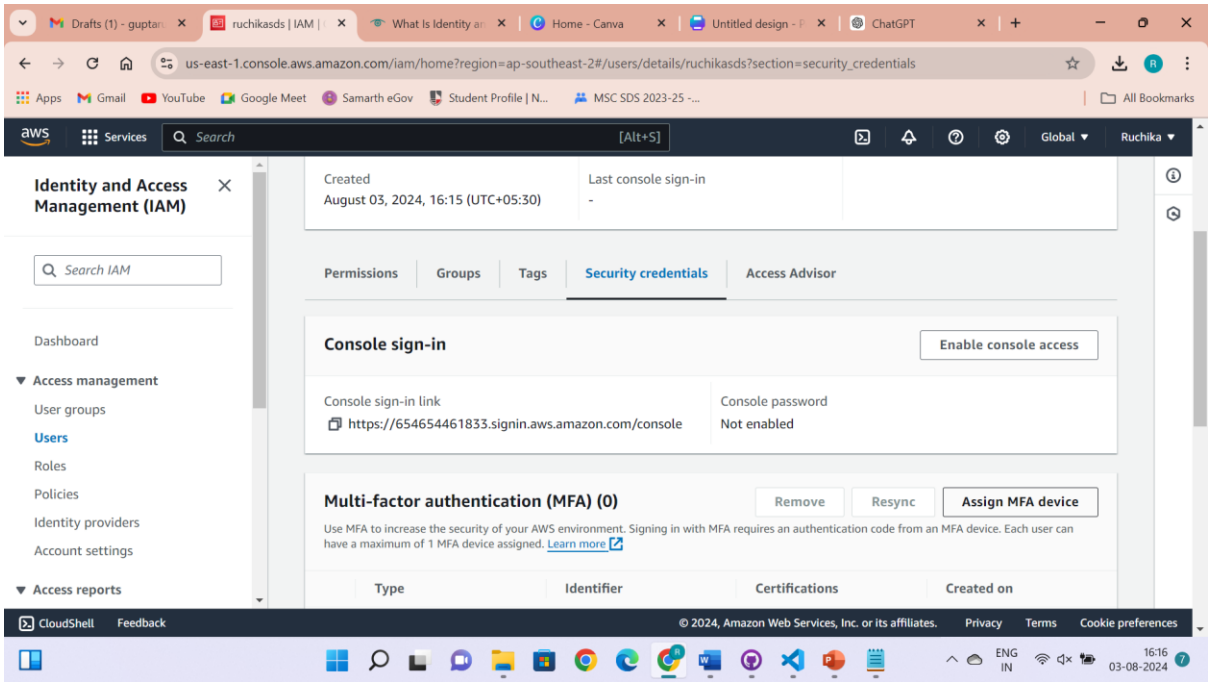


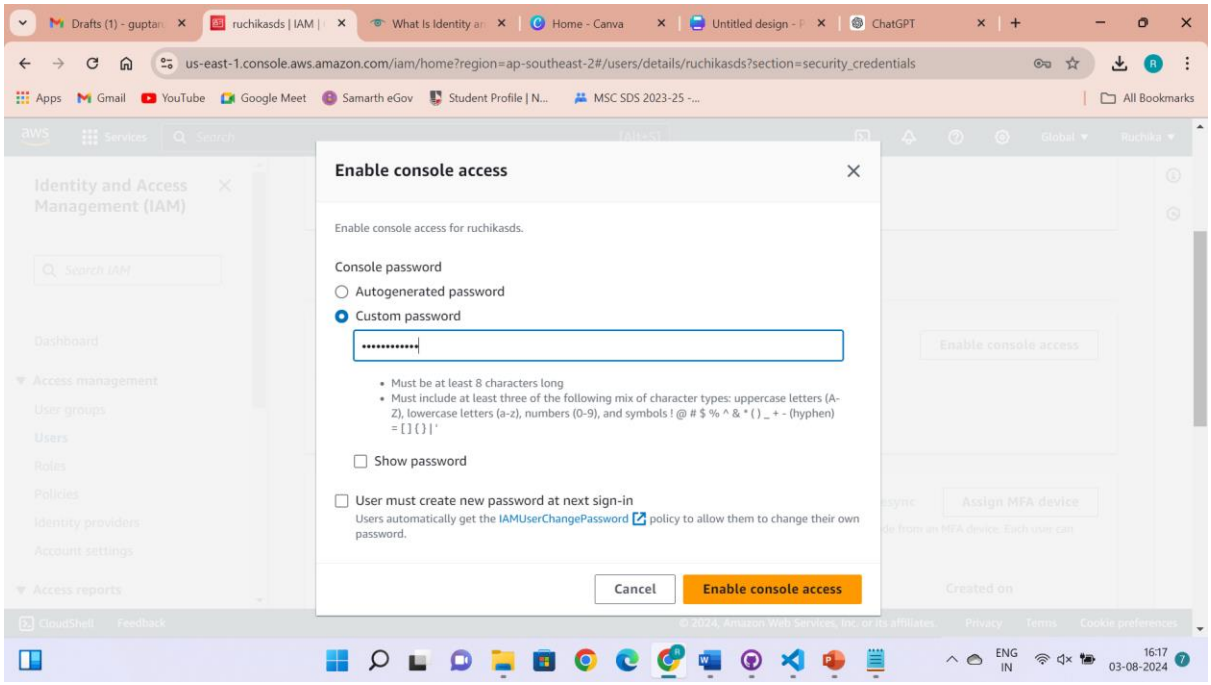

Drafts (1) - gupta
Create user | IAM
What Is Identity a
Home - Canva
Untitled design - F
ChatGPT
us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/users/create
Apps
Gmail
YouTube
Google Meet
Samarth eGov
Student Profile | N...
MSC SDS 2023-25 -...
All Bookmarks
aws
Services
Search
[Alt+S]
Global
Ruchika
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Specify user details
User details
User name
ruchikasds
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
16:14
03-08-2024

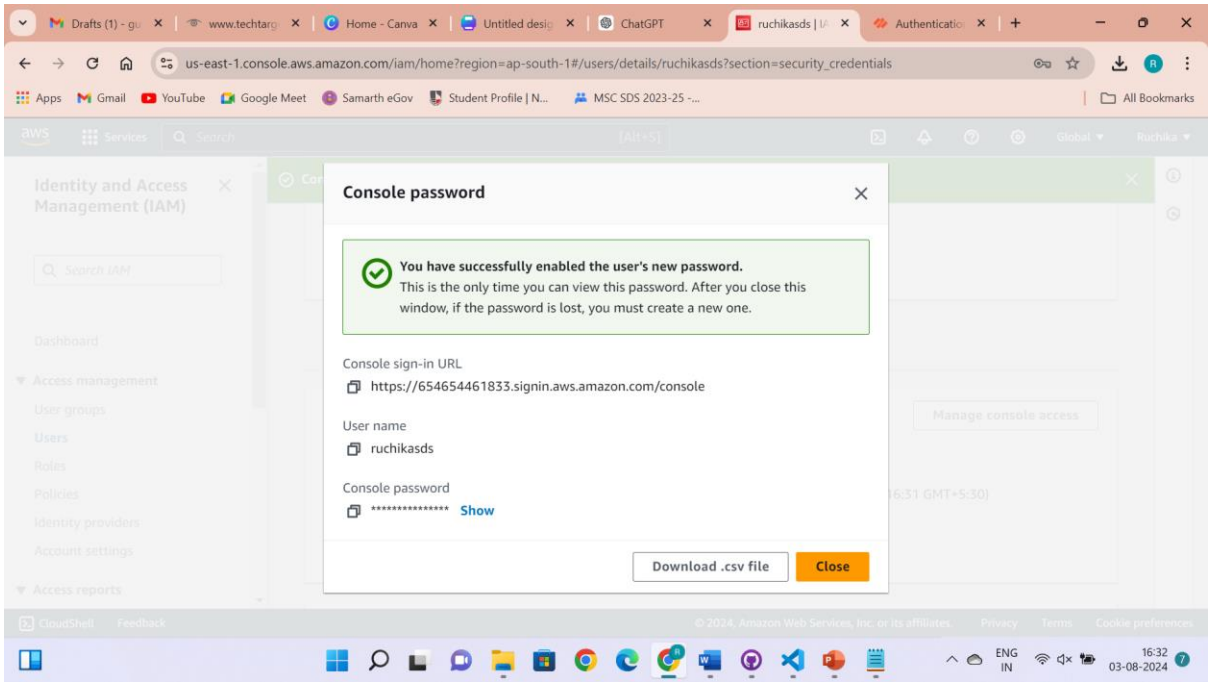

Drafts (1) - gupta
Create user | IAM
What Is Identity a
Home - Canva
Untitled design - F
ChatGPT
us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/users/create
Apps
Gmail
YouTube
Google Meet
Samarth eGov
Student Profile | N...
MSC SDS 2023-25 -...
All Bookmarks
aws
Services
Search
[Alt+S]
Global
Ruchika
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
Create group
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
16:14
03-08-2024


us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/users/create
Services
Search
[Alt+S]
Global
Ruchika
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
ruchikasds
Console password type
None
Require password reset
No
Permissions summary
Name
Type
Used as
No resources
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

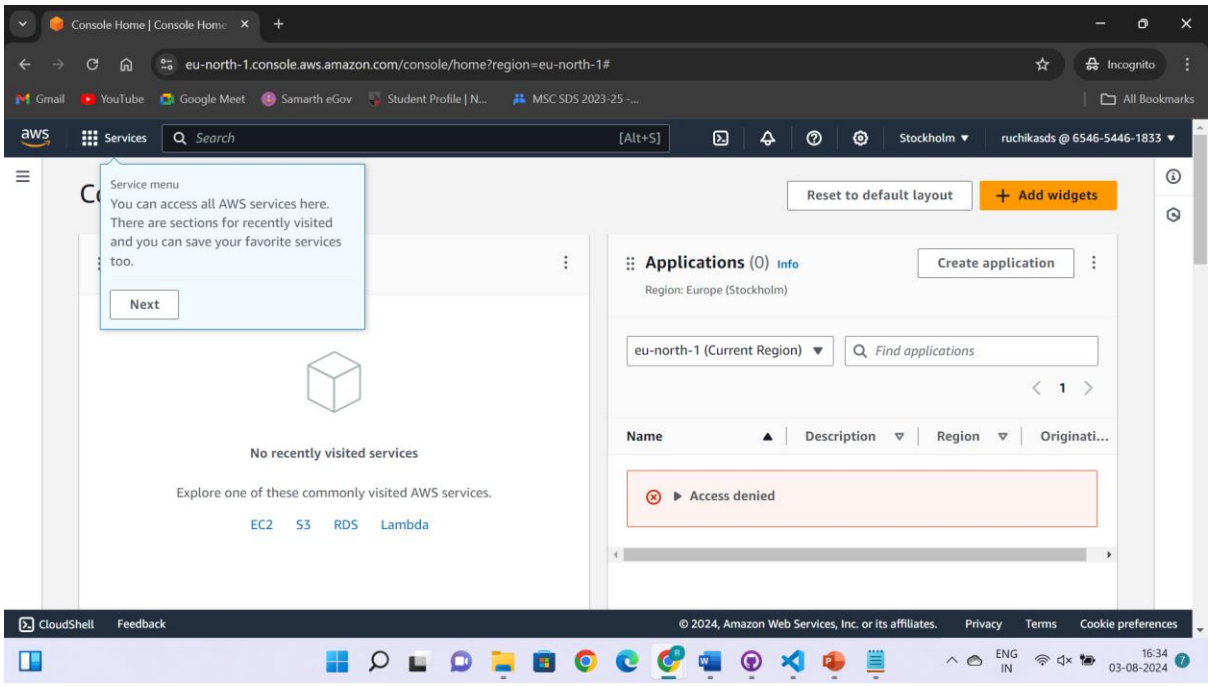

us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
IAM > Users
Users (1) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Group
Last activity
MFA
ruchikasds
/
0
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

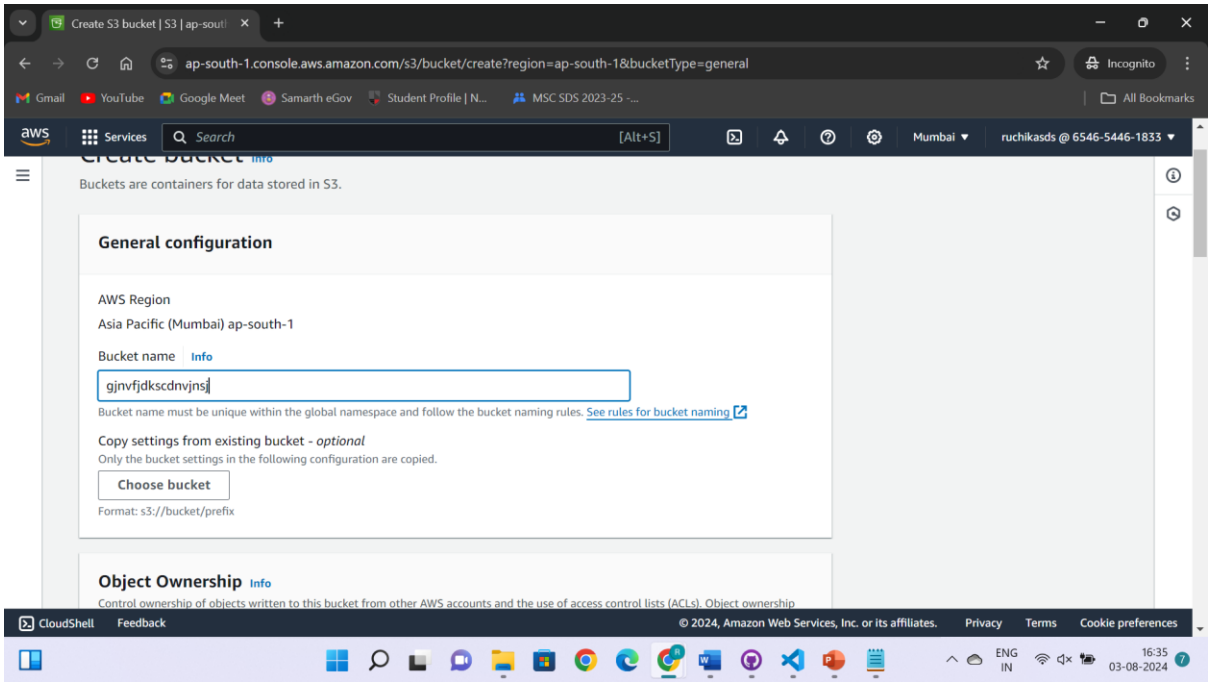

us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/users/details/ruchikasds?section=security_credentials
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Created
August 03, 2024, 16:15 (UTC+05:30)
Last console sign-in
-
Permissions
Groups
Tags
Security credentials
Access Advisor
Console sign-in
Enable console access
Console sign-in link
https://654654461833.signin.aws.amazon.com/console
Console password
Not enabled
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 1 MFA device assigned. Learn more
Type
Identifier
Certifications
Created on
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

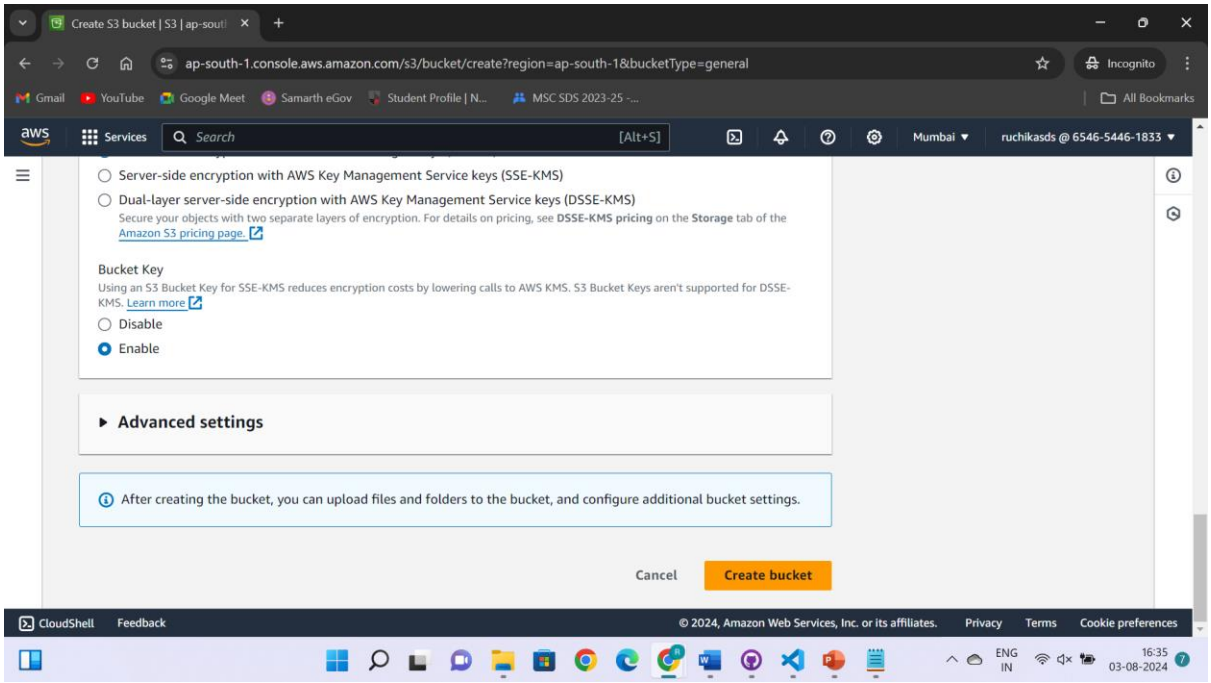

Enable console access
Enable console access for ruchikasds.
Console password
Autogenerated password
Custom password
Must be at least 8 characters long
Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '
Show password
User must create new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
Cancel
Enable console access

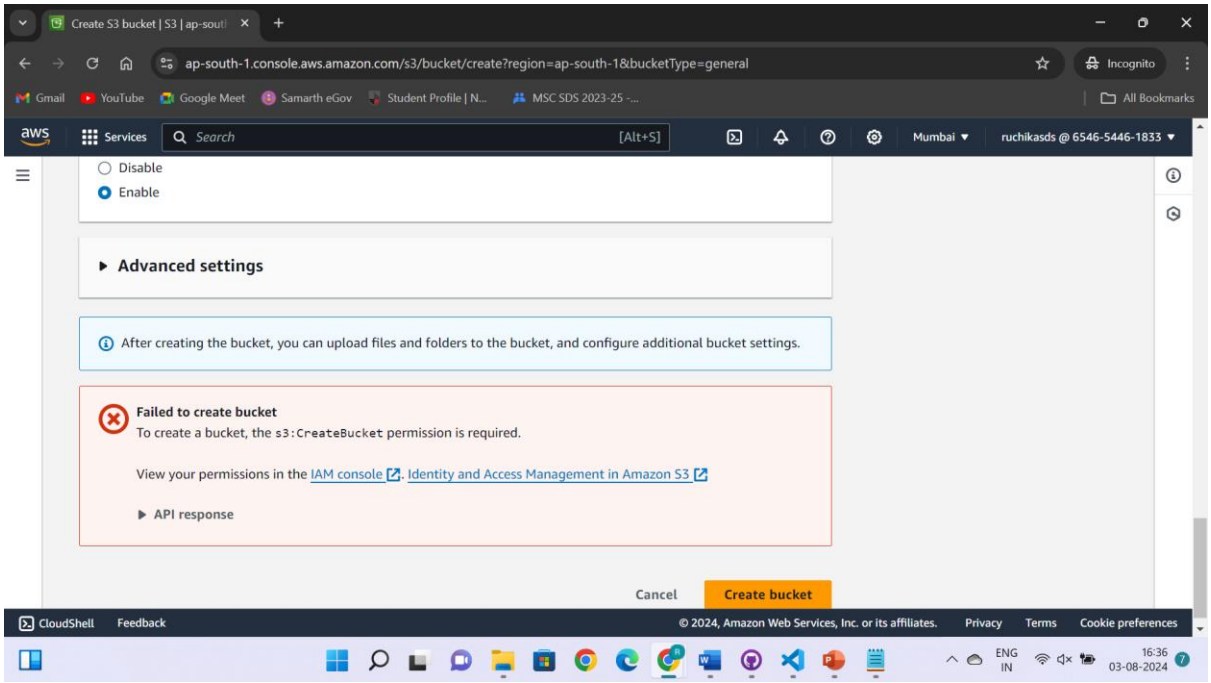


IAM USER (S3 CREATING BUCKET)

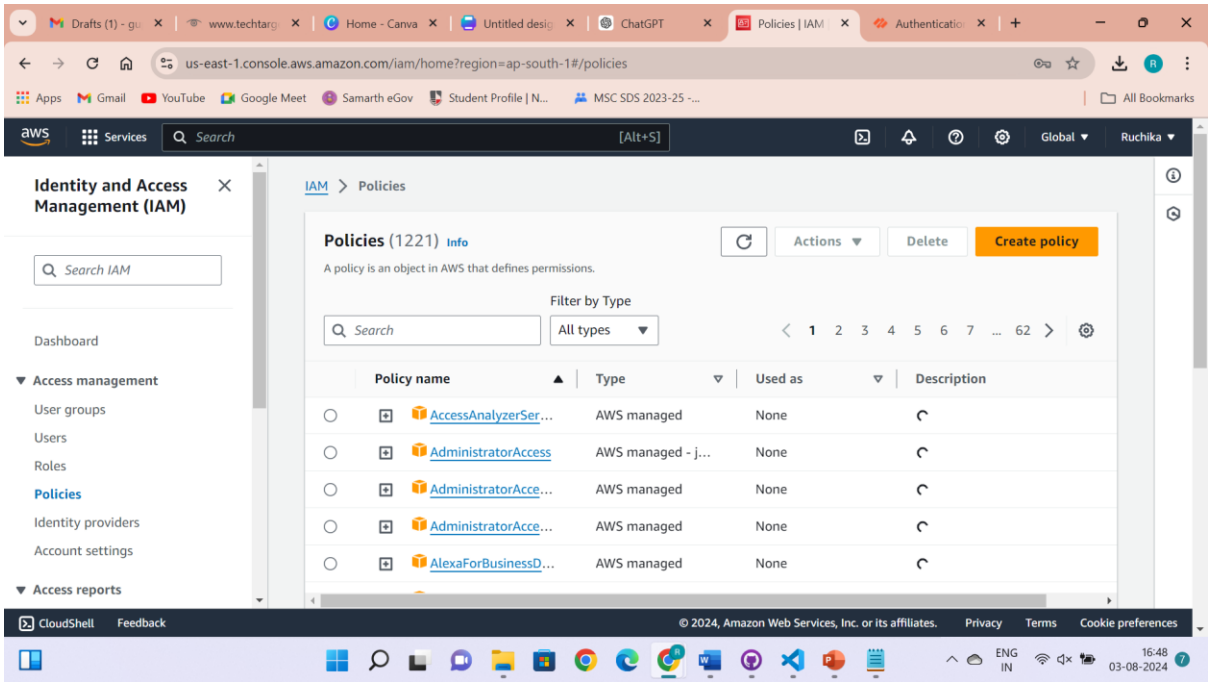


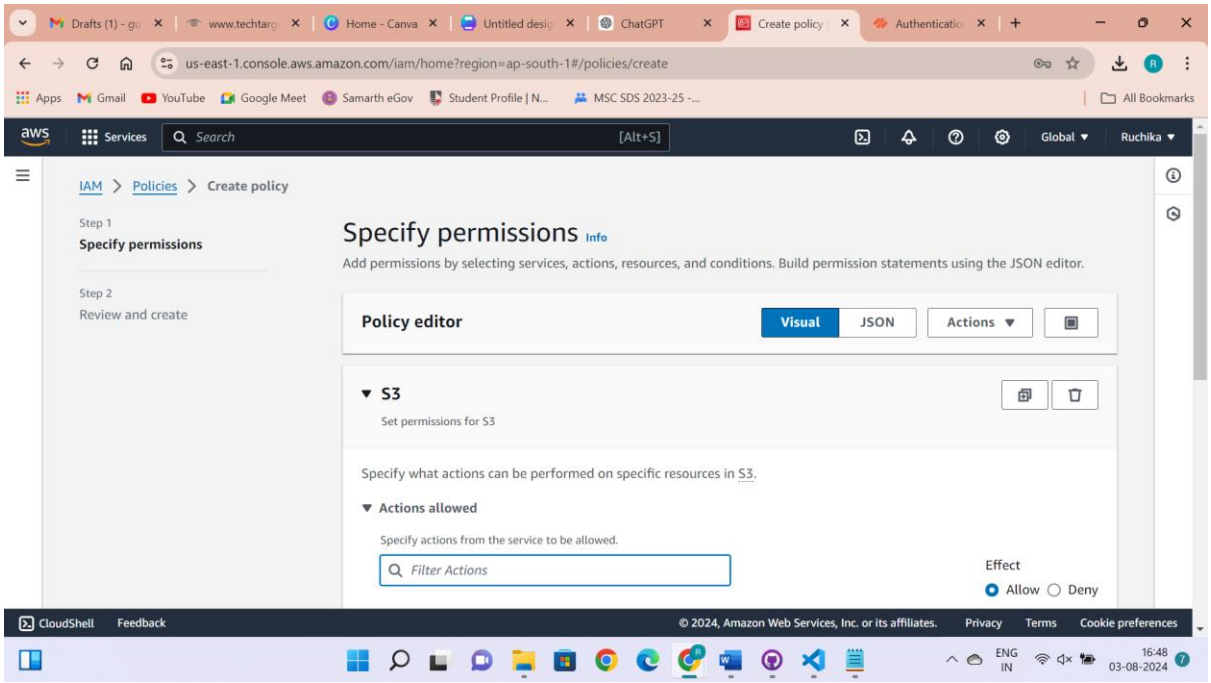

Create S3 bucket | S3 | ap-south
ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Incognito
Gmail
YouTube
Google Meet
Samarth eGov
Student Profile | N...
MSC SDS 2023-25 -...
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai
ruchikasds @ 6546-5446-1833
Buckets are containers for data stored in S3.
General configuration
AWS Region
Asia Pacific (Mumbai) ap-south-1
Bucket name
Info
gjnvfjdkscdnvjnsj
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
Object Ownership
Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
16:35
03-08-2024

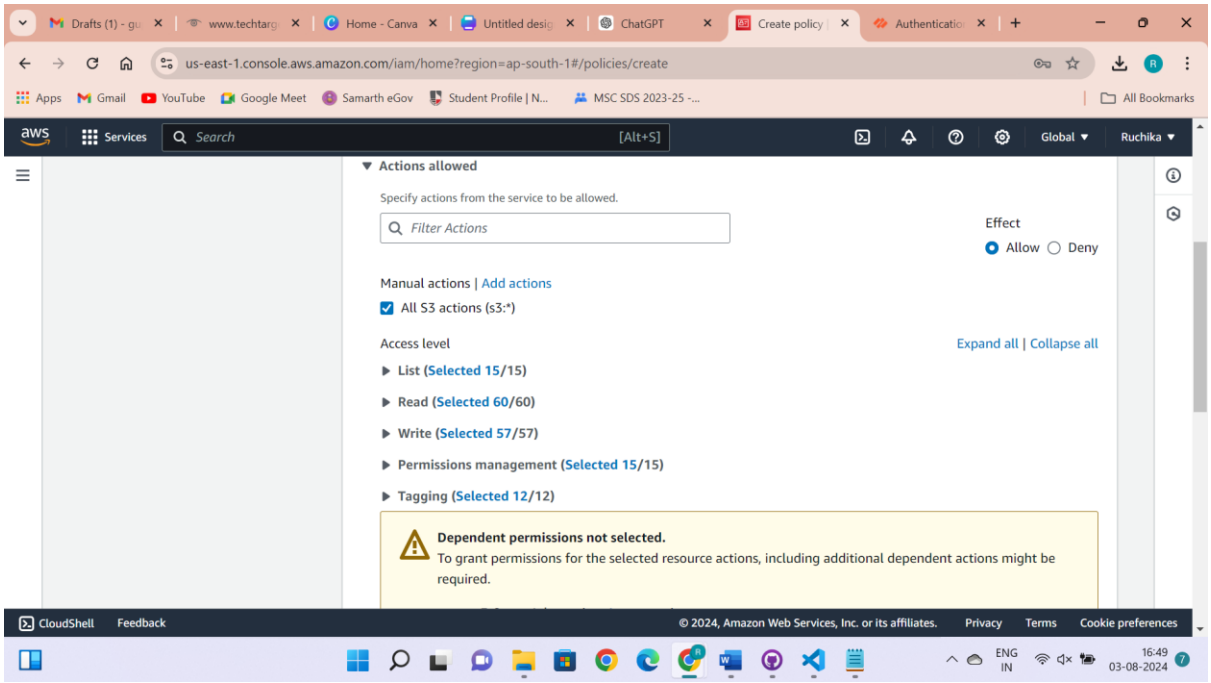

Create S3 bucket | S3 | ap-south
ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Incognito
Gmail
YouTube
Google Meet
Samarth eGov
Student Profile | N...
MSC SDS 2023-25 -...
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai
ruchikasds @ 6546-5446-1833
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page.
Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more
Disable
Enable
Advanced settings
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
16:35
03-08-2024

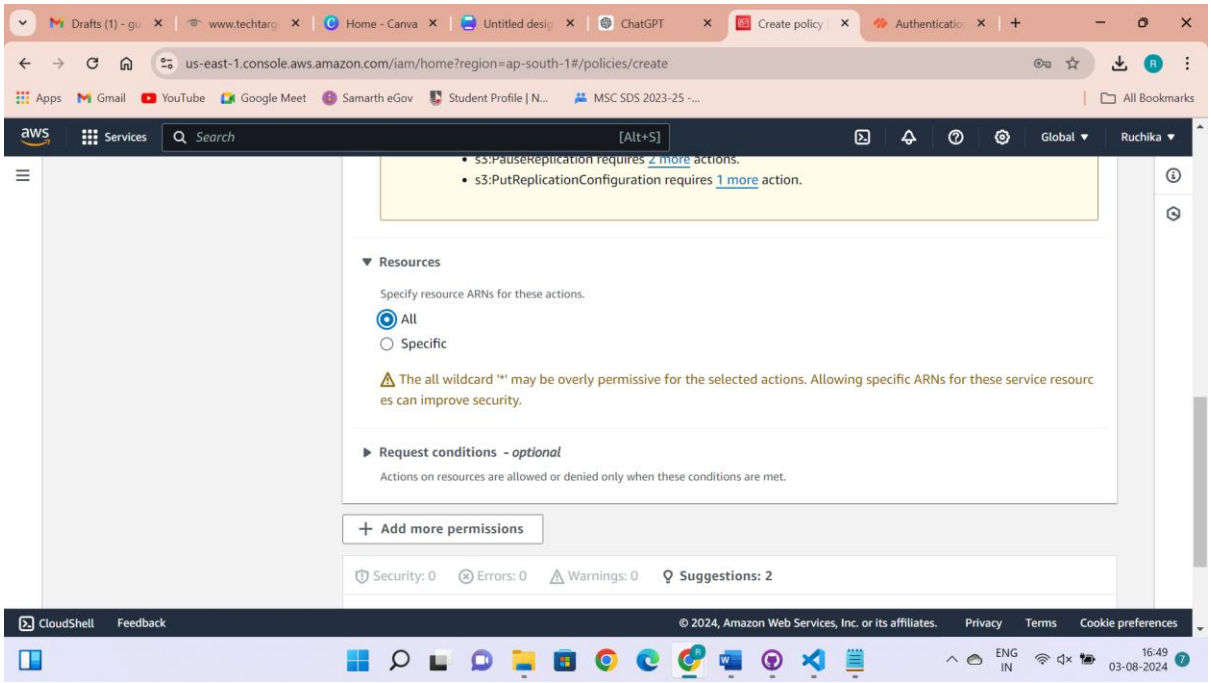

Create S3 bucket | S3 | ap-south-1
ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Incognito
Gmail
YouTube
Google Meet
Samarth eGov
Student Profile | N...
MSC SDS 2023-25 -...
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai
ruchikasds @ 6546-5446-1833
Disable
Enable
Advanced settings
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.
Failed to create bucket
To create a bucket, the s3:CreateBucket permission is required.
View your permissions in the IAM console. Identity and Access Management in Amazon S3
API response
Cancel
Create bucket
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
16:36
03-08-2024

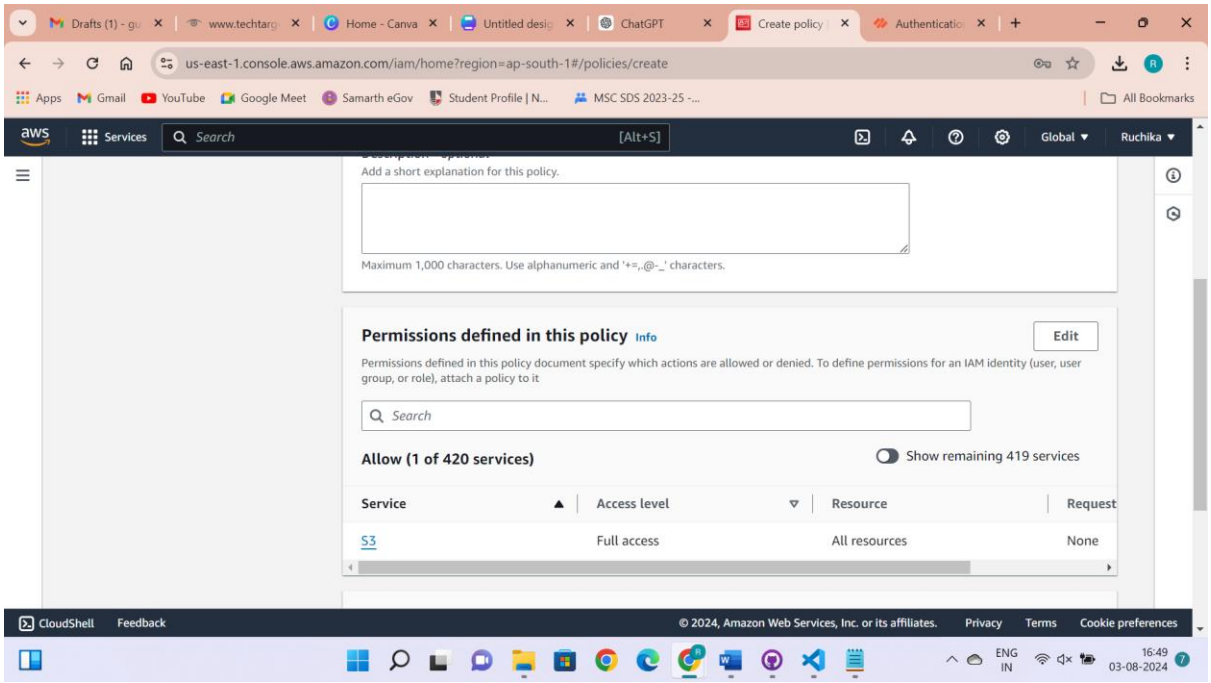
POLICY

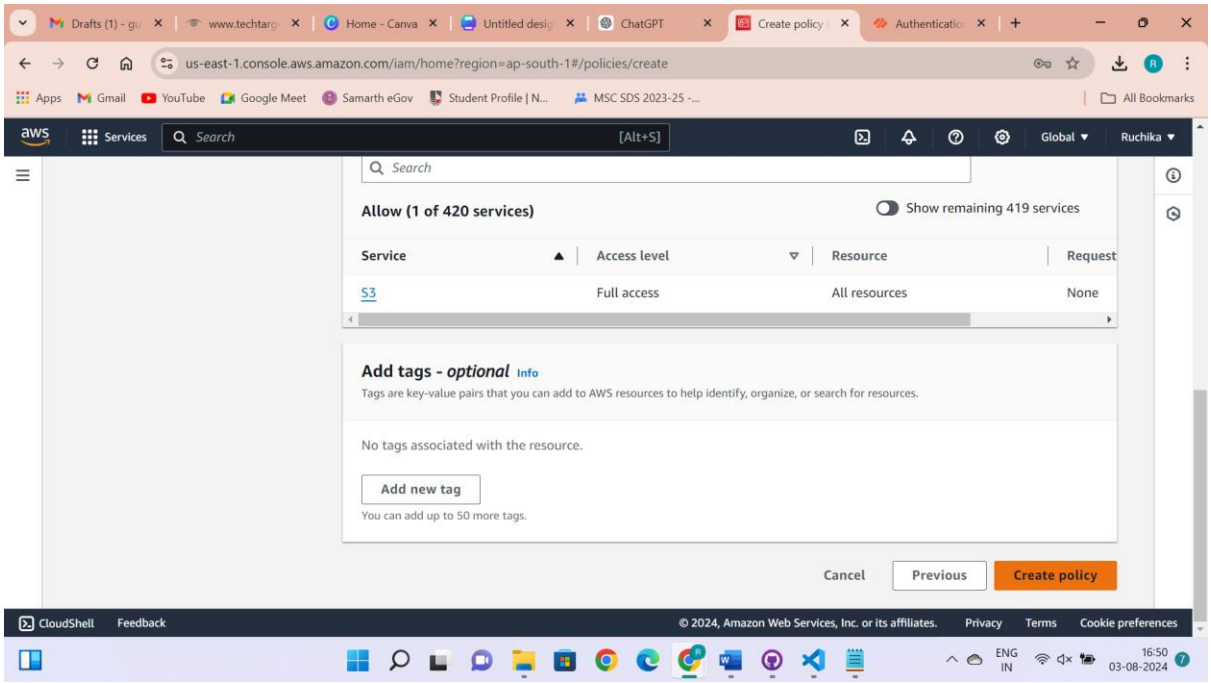

Drafts (1) - gu
www.techtarg
Home - Canva
Untitled desig
ChatGPT
Policies | IAM
Authentication
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies
Apps
Gmail
YouTube
Google Meet
Samarth eGov
Student Profile | N...
MSC SDS 2023-25 -...
All Bookmarks
aws
Services
Search
[Alt+S]
Global
Ruchika
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
IAM > Policies
Policies (1221) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 62
Policy name
Type
Used as
Description
AccessAnalyzerSer...
AWS managed
None
AdministratorAccess
AWS managed - j...
None
AdministratorAcce...
AWS managed
None
AdministratorAcce...
AWS managed
None
AlexaForBusinessD...
AWS managed
None
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
16:48
03-08-2024

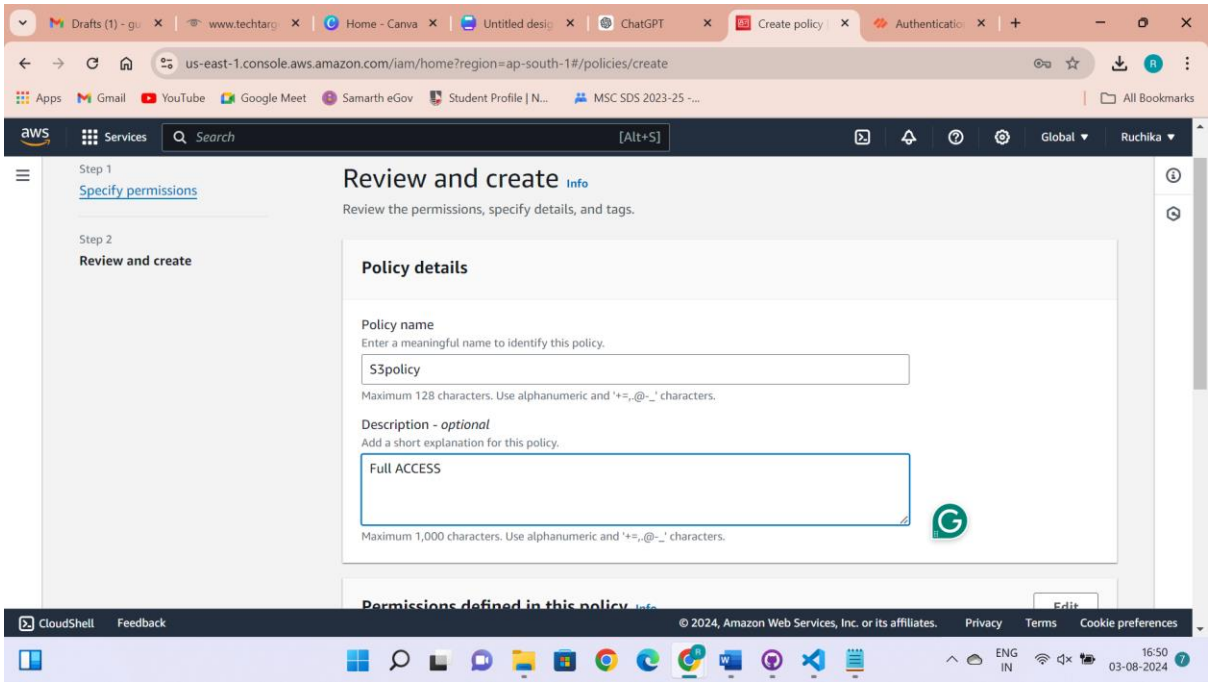

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Services
Search
[Alt+S]
Global
Ruchika
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
S3
Set permissions for S3
Specify what actions can be performed on specific resources in S3.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
16:48
03-08-2024

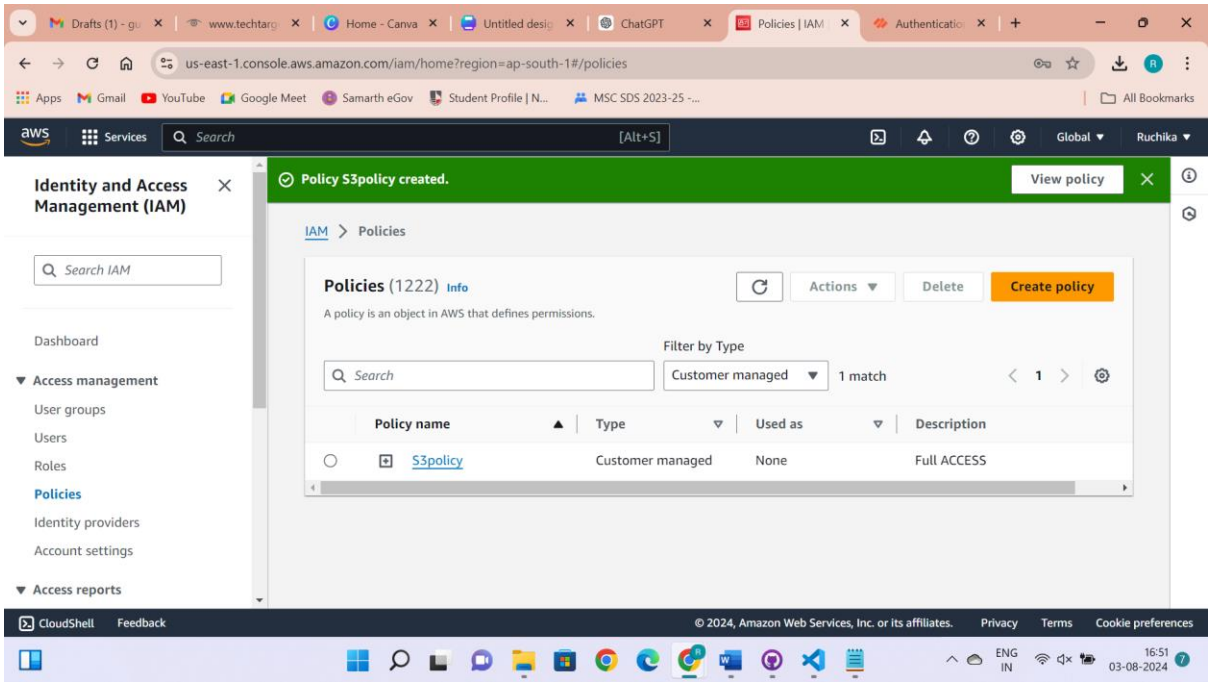

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Services
Search
[Alt+S]
Global
Ruchika
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All S3 actions (s3:*)
Access level
Expand all | Collapse all
List (Selected 15/15)
Read (Selected 60/60)
Write (Selected 57/57)
Permissions management (Selected 15/15)
Tagging (Selected 12/12)
Dependent permissions not selected.
To grant permissions for the selected resource actions, including additional dependent actions might be required.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
16:49
03-08-2024

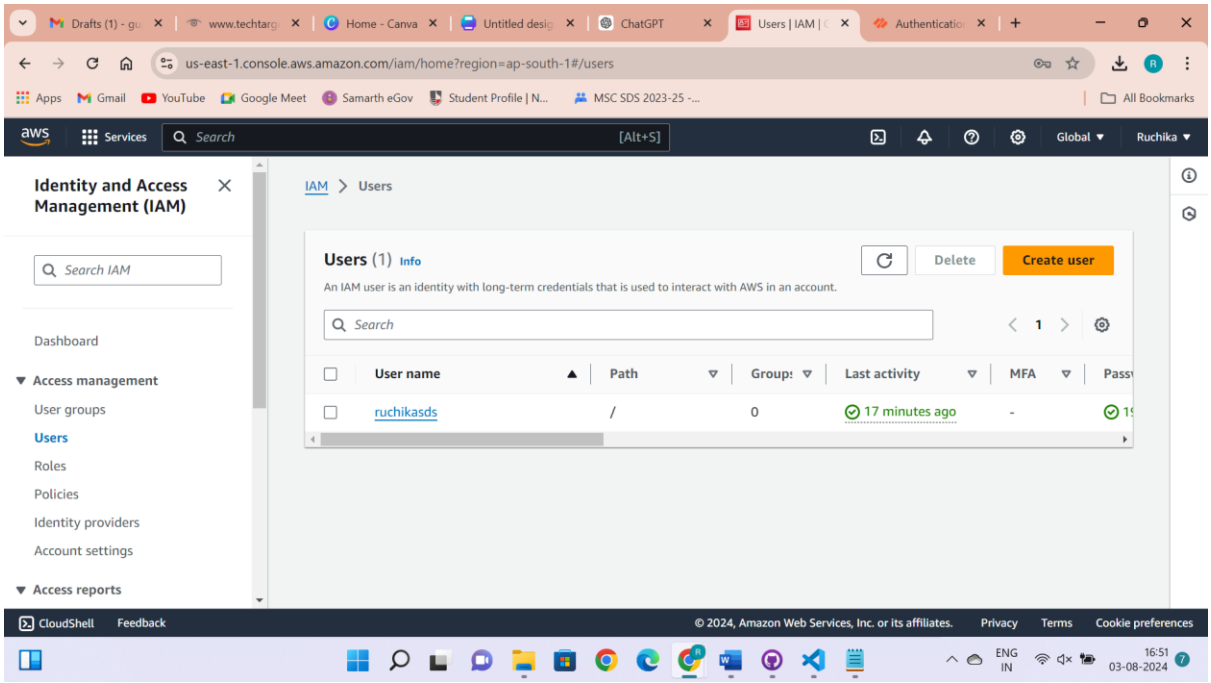

Create policy
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Services
Search
[Alt+S]
Global
Ruchika
s3:PutReplicationConfiguration requires 1 more action.
Resources
Specify resource ARNs for these actions.
All
Specific
The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.
Request conditions - optional
Actions on resources are allowed or denied only when these conditions are met.
Add more permissions
Security: 0
Errors: 0
Warnings: 0
Suggestions: 2
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
16:49
03-08-2024

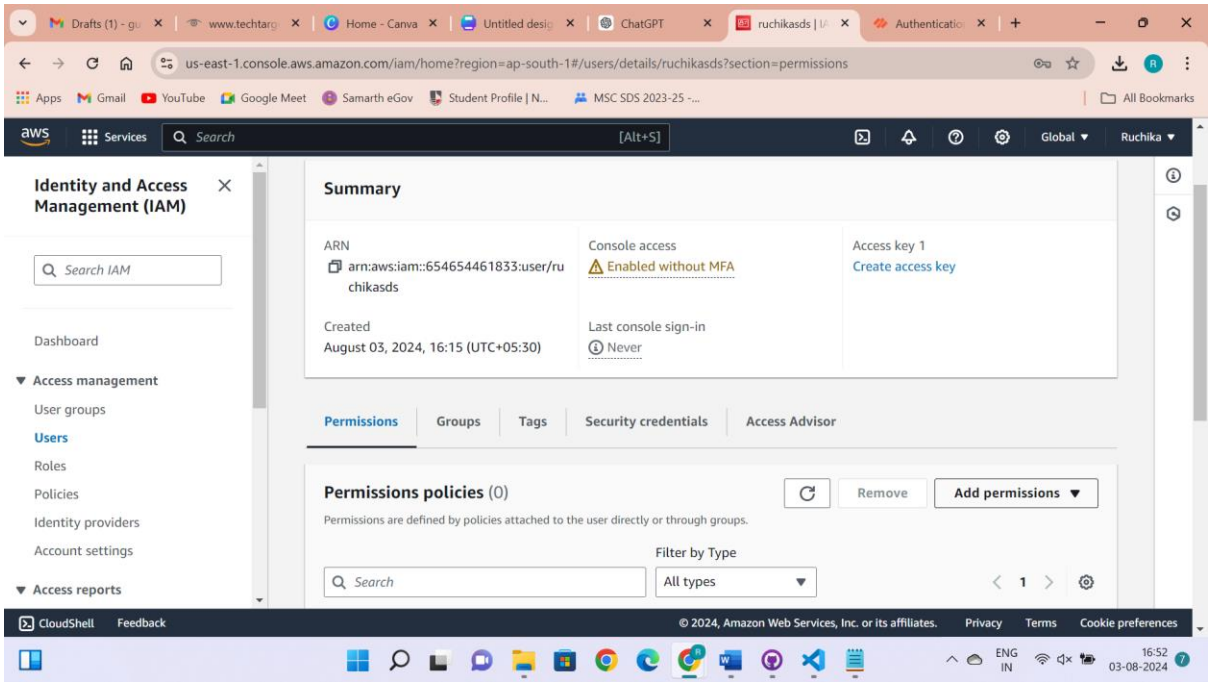

Create policy
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Services
Search
[Alt+S]
Global
Ruchika
Add a short explanation for this policy.
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (1 of 420 services)
Show remaining 419 services
Service
Access level
Resource
Request
S3
Full access
All resources
None
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
16:49
03-08-2024

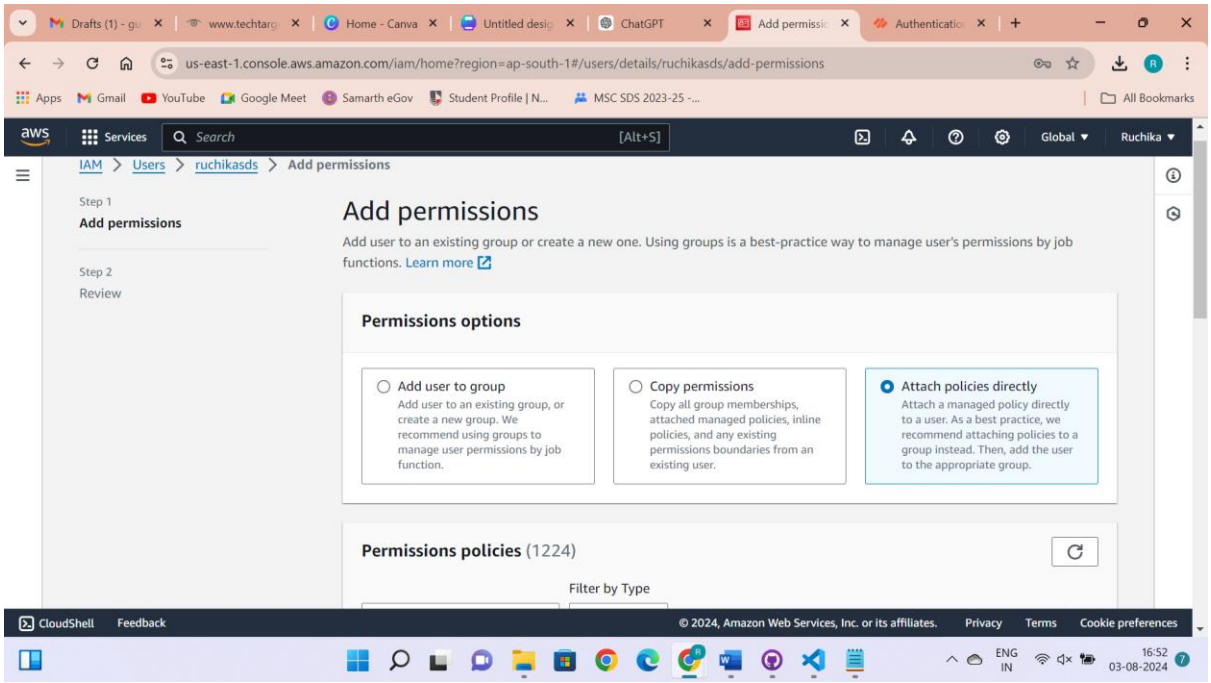

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Search
Allow (1 of 420 services)
Show remaining 419 services
Service
Access level
Resource
Request
S3
Full access
All resources
None
Add tags - optional Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create policy
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

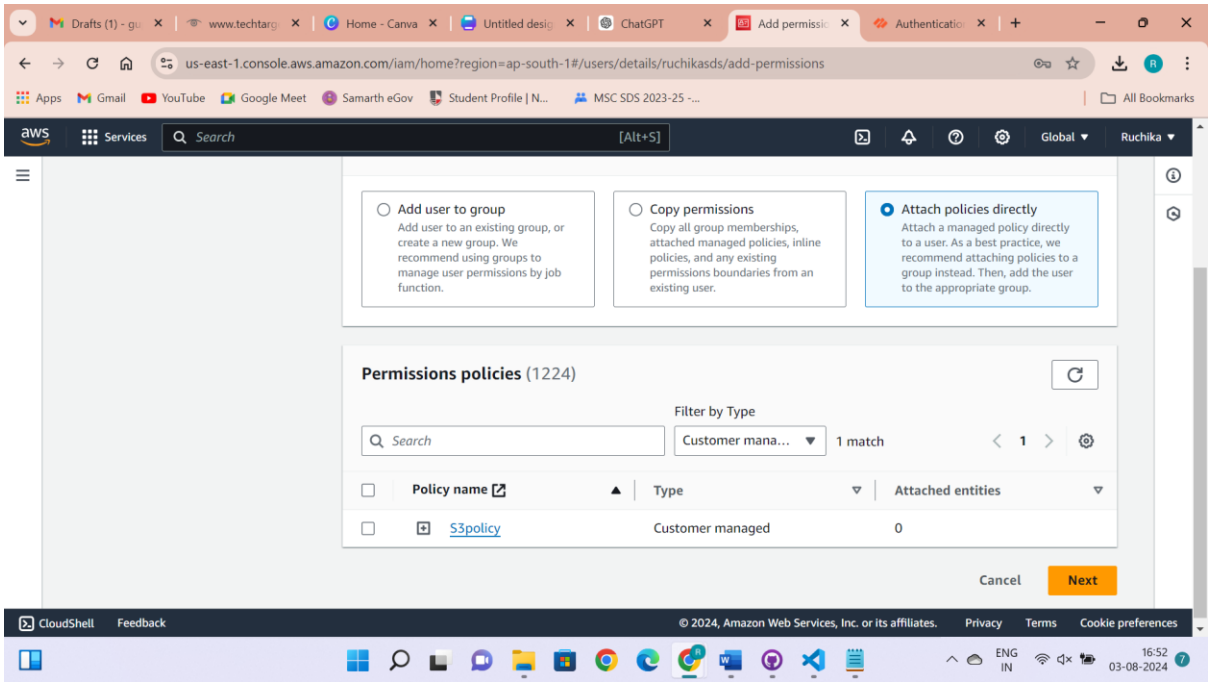

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
S3policy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Full ACCESS
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

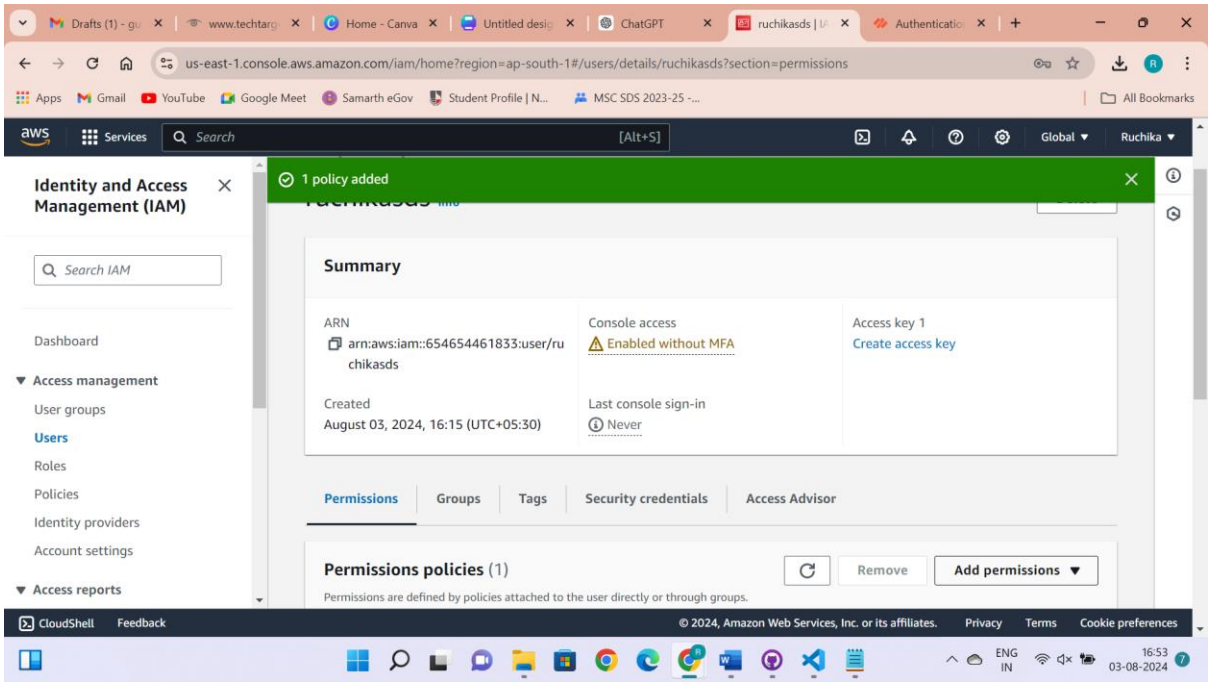

Policy S3policy created.
View policy
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
IAM > Policies
Policies (1222) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
Customer managed
1 match
Policy name
Type
Used as
Description
S3policy
Customer managed
None
Full ACCESS
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

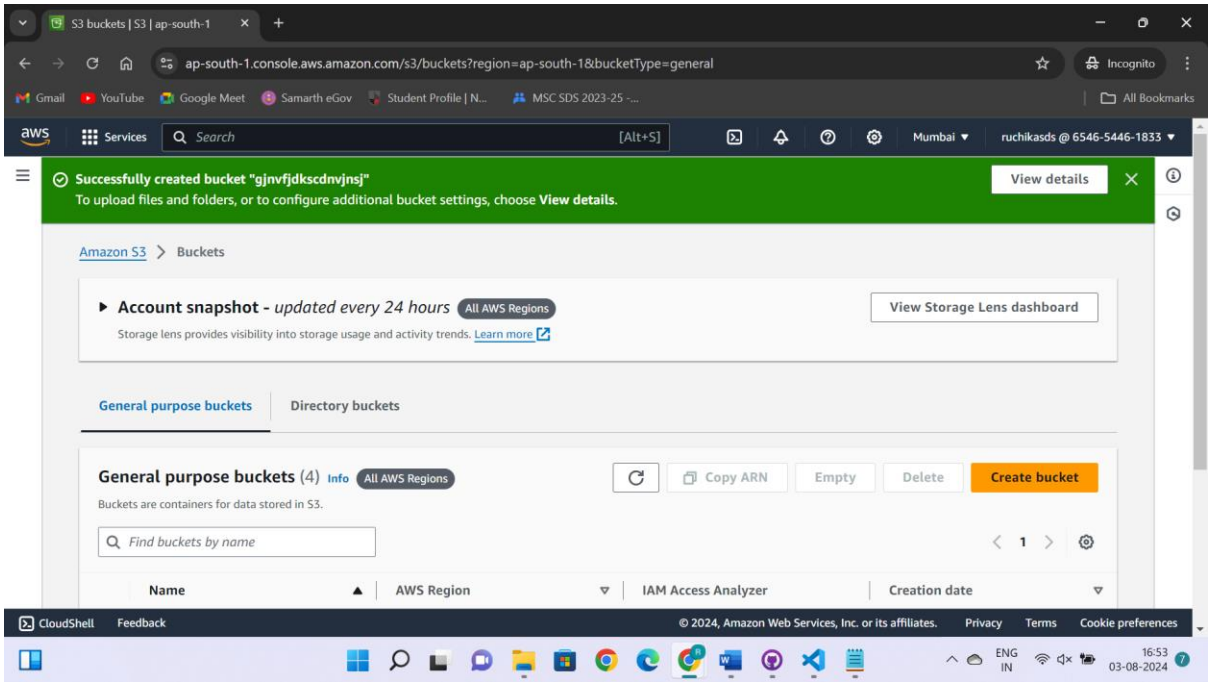

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
IAM > Users
Users (1) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Group
Last activity
MFA
ruchikasds
/
0
17 minutes ago
-
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/ruchikasds?section=permissions
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Summary
ARN
arn:aws:iam::654654461833:user/ruchikasds
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 16:15 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (0)
Remove
Add permissions
Permissions are defined by policies attached to the user directly or through groups.
Filter by Type
Search
All types
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

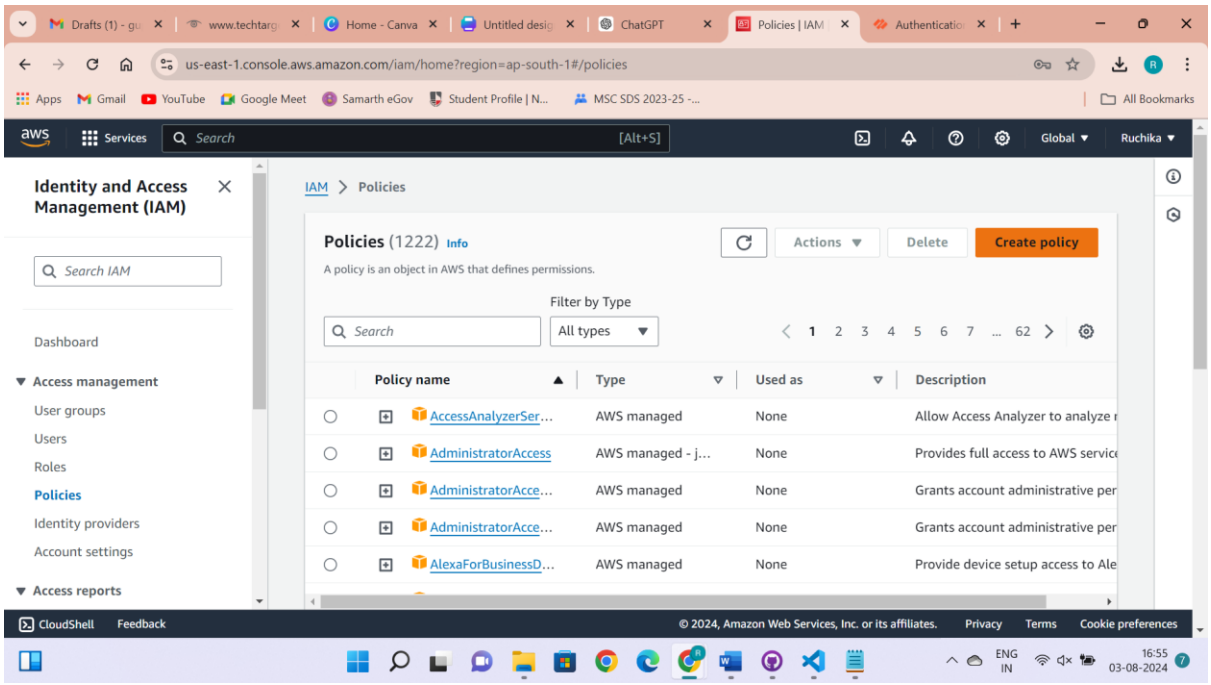

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/ruchikasds/add-permissions
IAM > Users > ruchikasds > Add permissions
Step 1
Add permissions
Step 2
Review
Add permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Permissions policies (1224)
Filter by Type
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

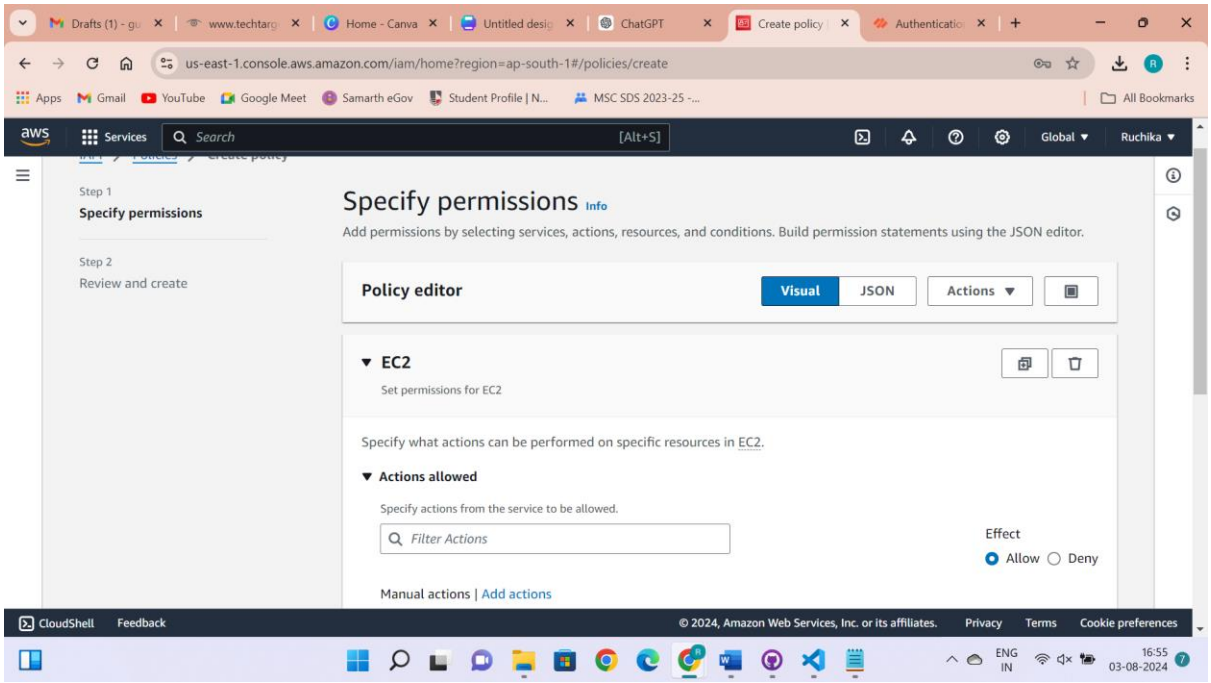

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/ruchikasds/add-permissions
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Permissions policies (1224)
Filter by Type
Search
Customer mana...
1 match
Policy name
Type
Attached entities
S3policy
Customer managed
0
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

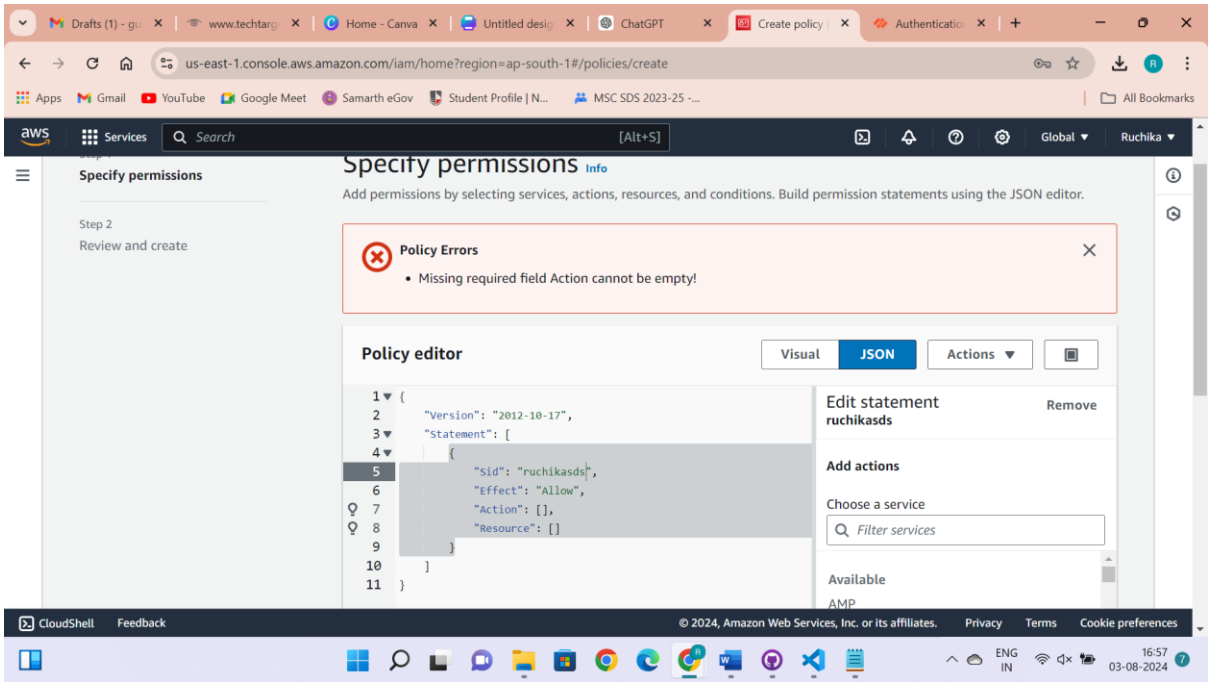

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/ruchikasds?section=permissions
1 policy added
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Summary
ARN
arn:aws:iam::654654461833:user/ruchikasds
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 16:15 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

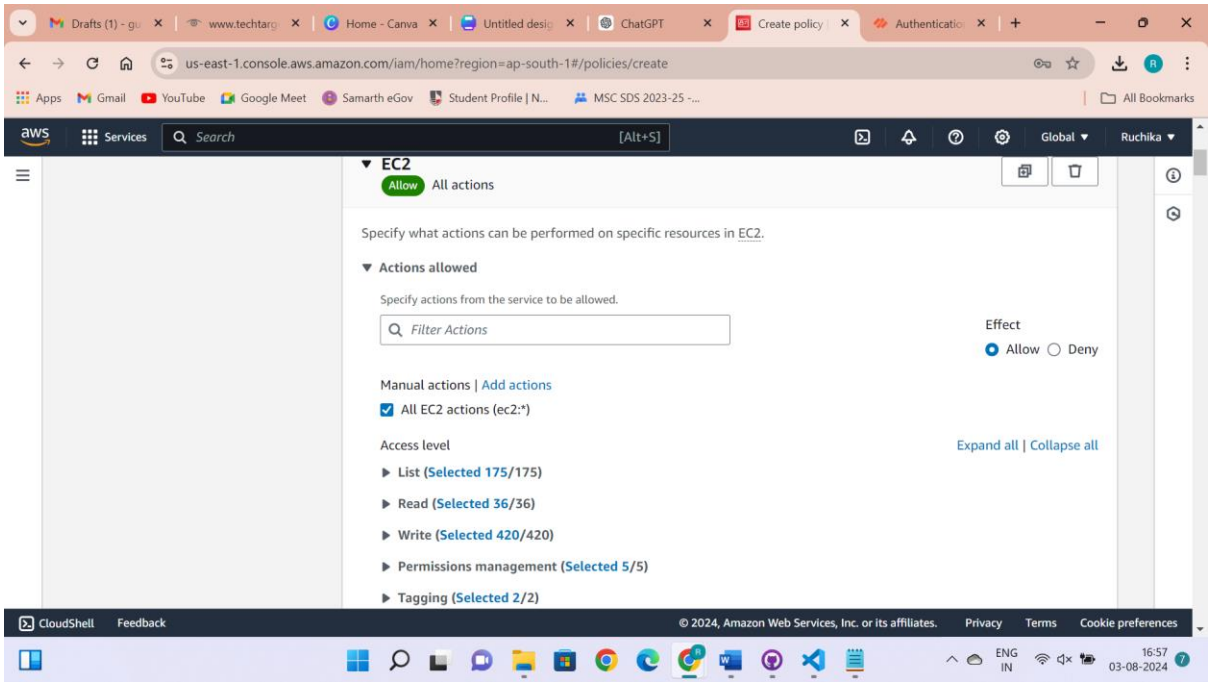


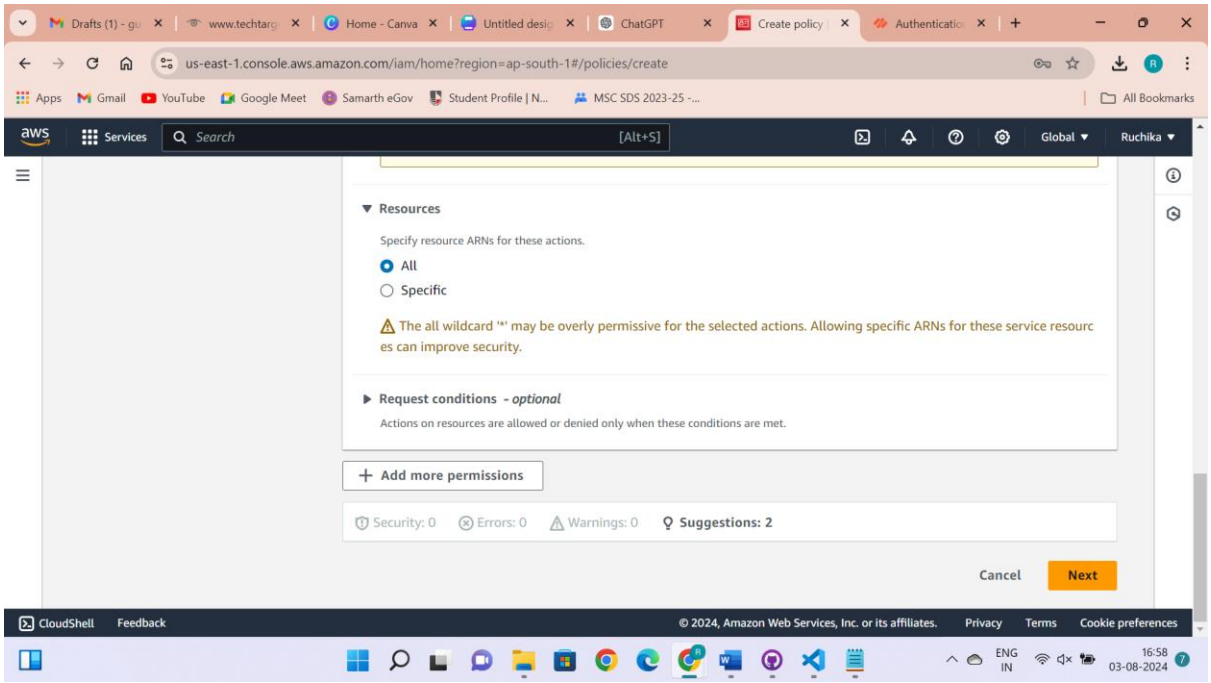
IAM USER (EC2 CREATING INSTANCE)

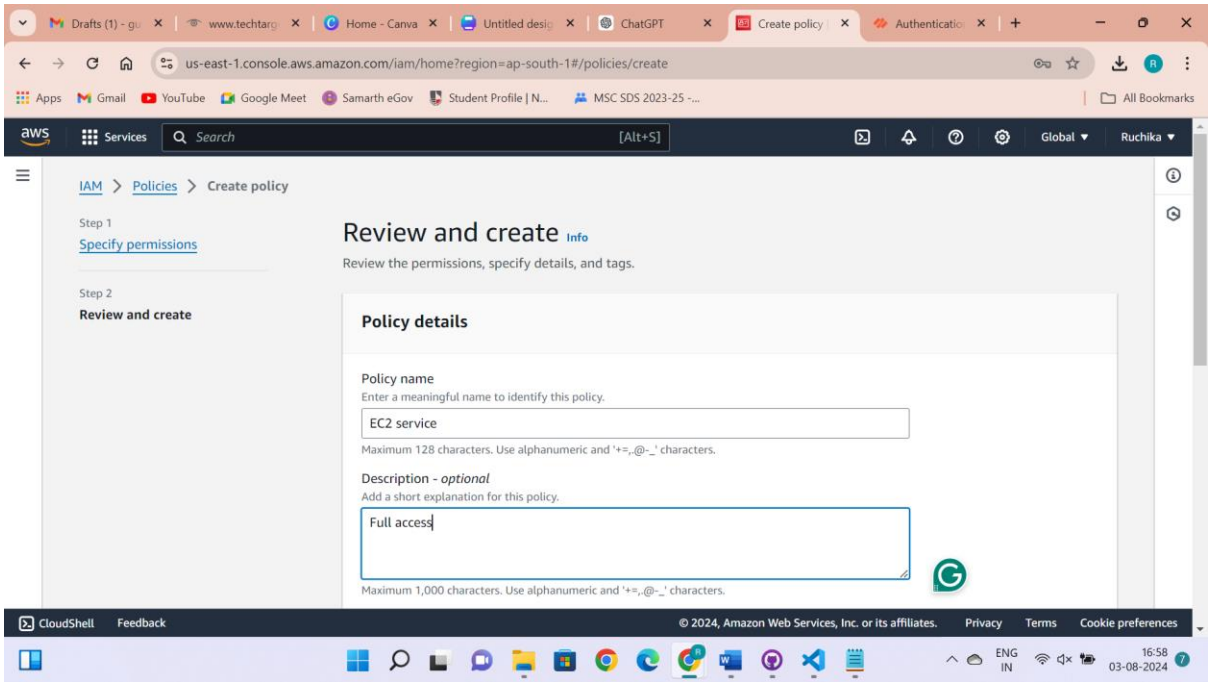


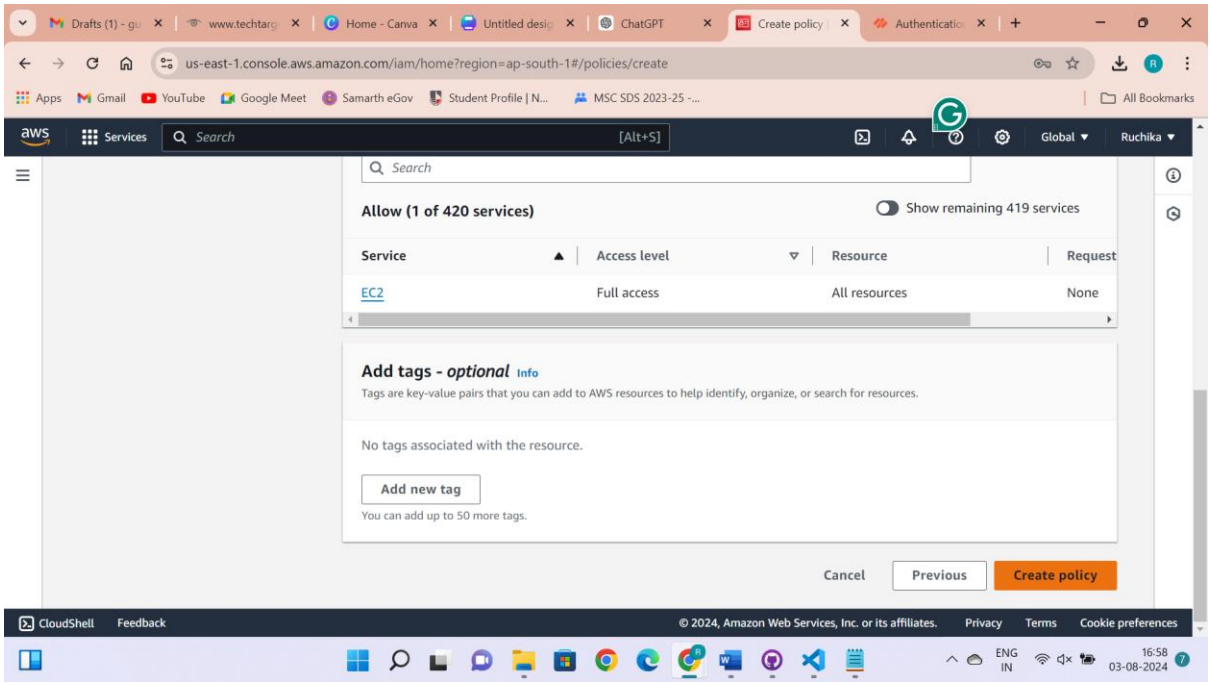

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Services
Search
[Alt+S]
Global
Ruchika
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
EC2
Set permissions for EC2
Specify what actions can be performed on specific resources in EC2.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
16:55
03-08-2024

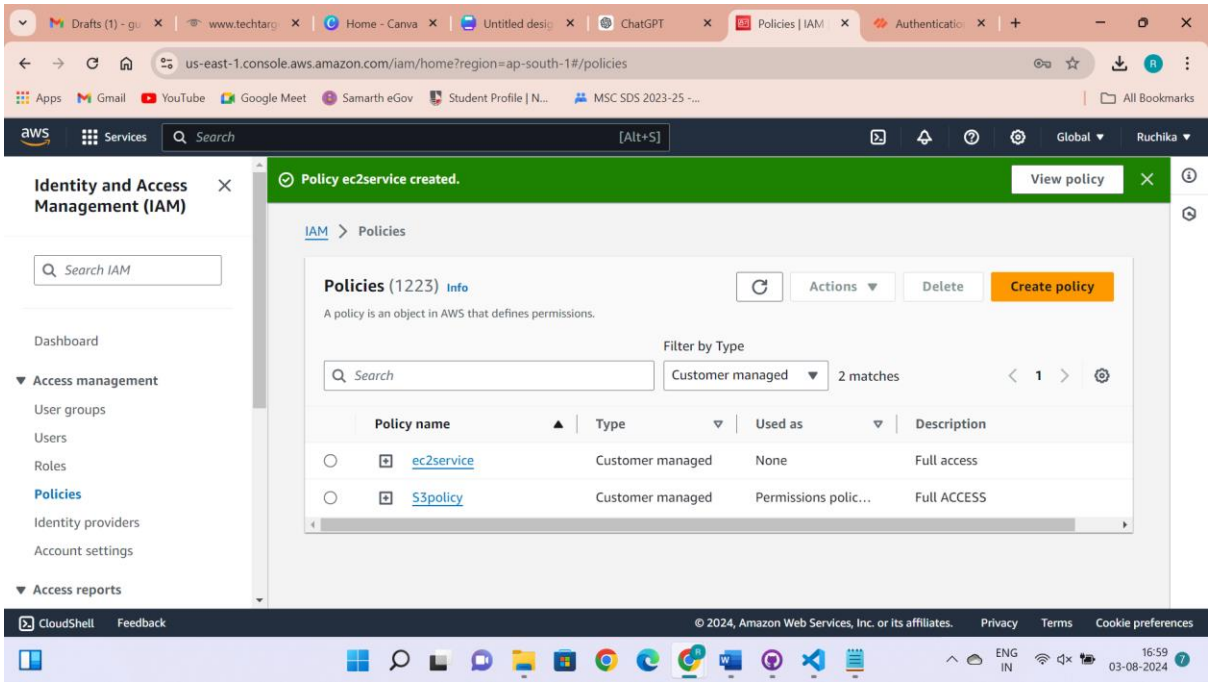

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Services
Search
[Alt+S]
Global
Ruchika
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy Errors
Missing required field Action cannot be empty!
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "ruchikasds",
"Effect": "Allow",
"Action": [],
"Resource": []
}
]
}
Edit statement
ruchikasds
Remove
Add actions
Choose a service
Filter services
Available
AMP
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
16:57
03-08-2024

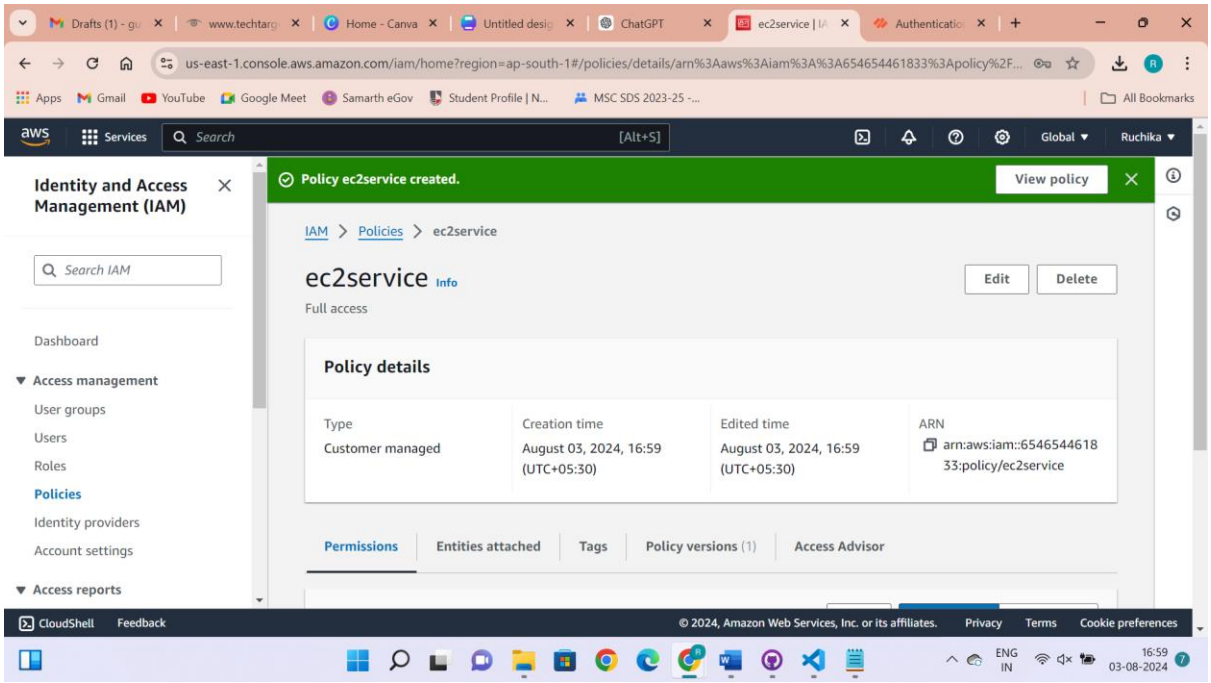

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Services
Search
[Alt+S]
Global
Ruchika
EC2
Allow
All actions
Specify what actions can be performed on specific resources in EC2.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All EC2 actions (ec2:*)
Access level
Expand all | Collapse all
List (Selected 175/175)
Read (Selected 36/36)
Write (Selected 420/420)
Permissions management (Selected 5/5)
Tagging (Selected 2/2)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

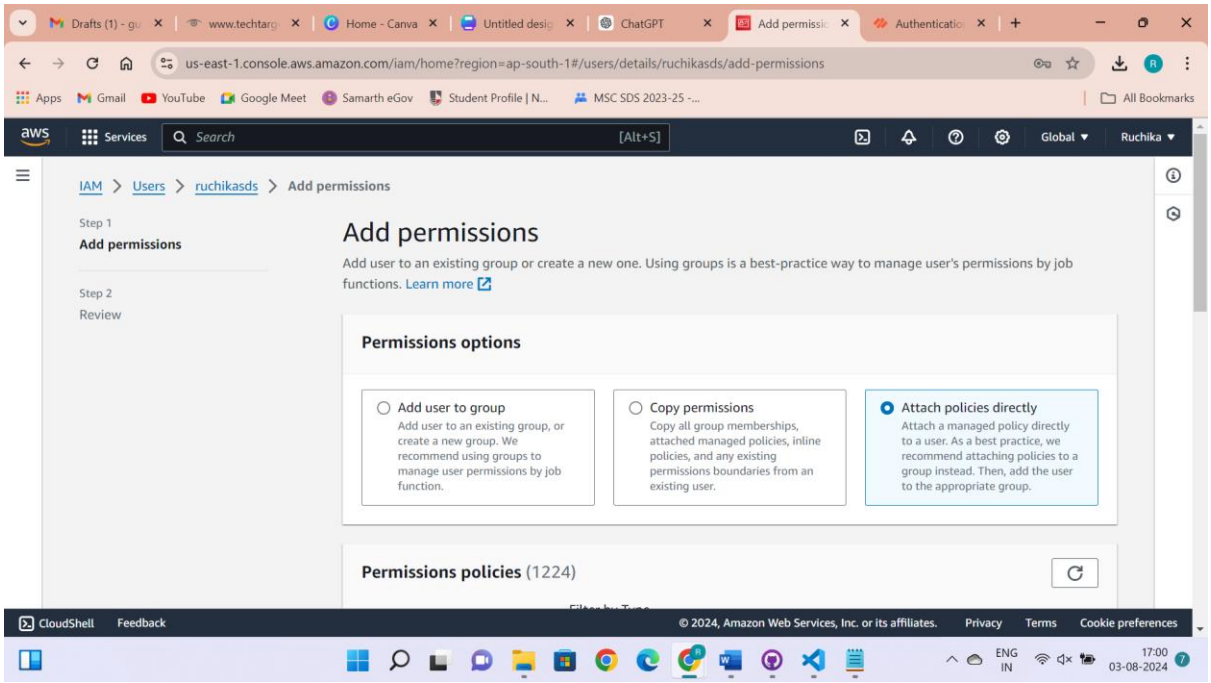

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Services
Search
[Alt+S]
Global
Ruchika
Resources
Specify resource ARNs for these actions.
All
Specific
The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.
Request conditions - optional
Actions on resources are allowed or denied only when these conditions are met.
Add more permissions
Security: 0
Errors: 0
Warnings: 0
Suggestions: 2
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

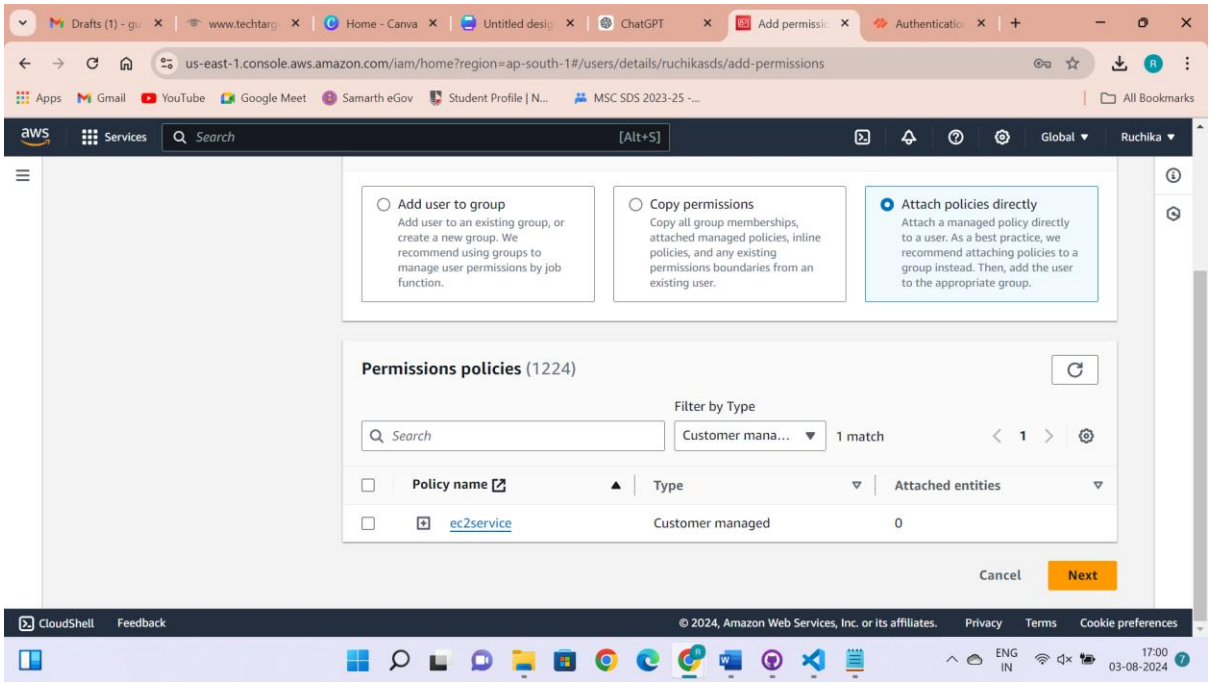

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Services
Search
[Alt+S]
Global
Ruchika
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
EC2 service
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Full access
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

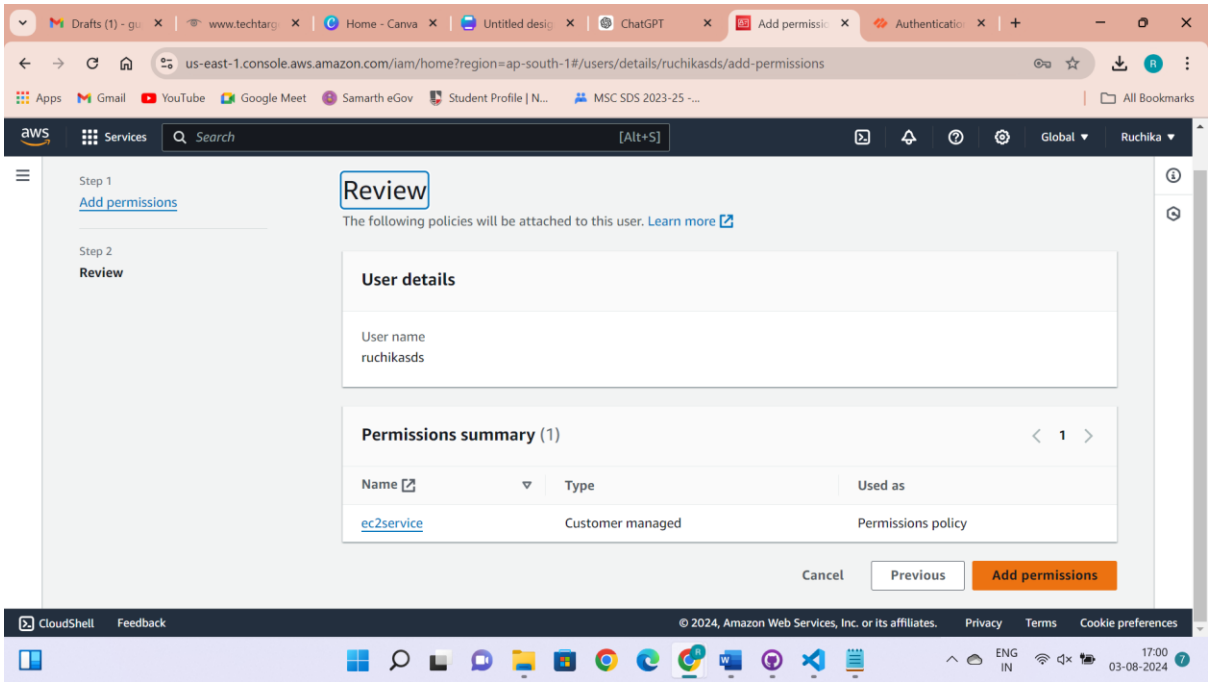

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Services
Search
[Alt+S]
Global
Ruchika
Search
Allow (1 of 420 services)
Show remaining 419 services
Service
Access level
Resource
Request
EC2
Full access
All resources
None
Add tags - optional Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create policy
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

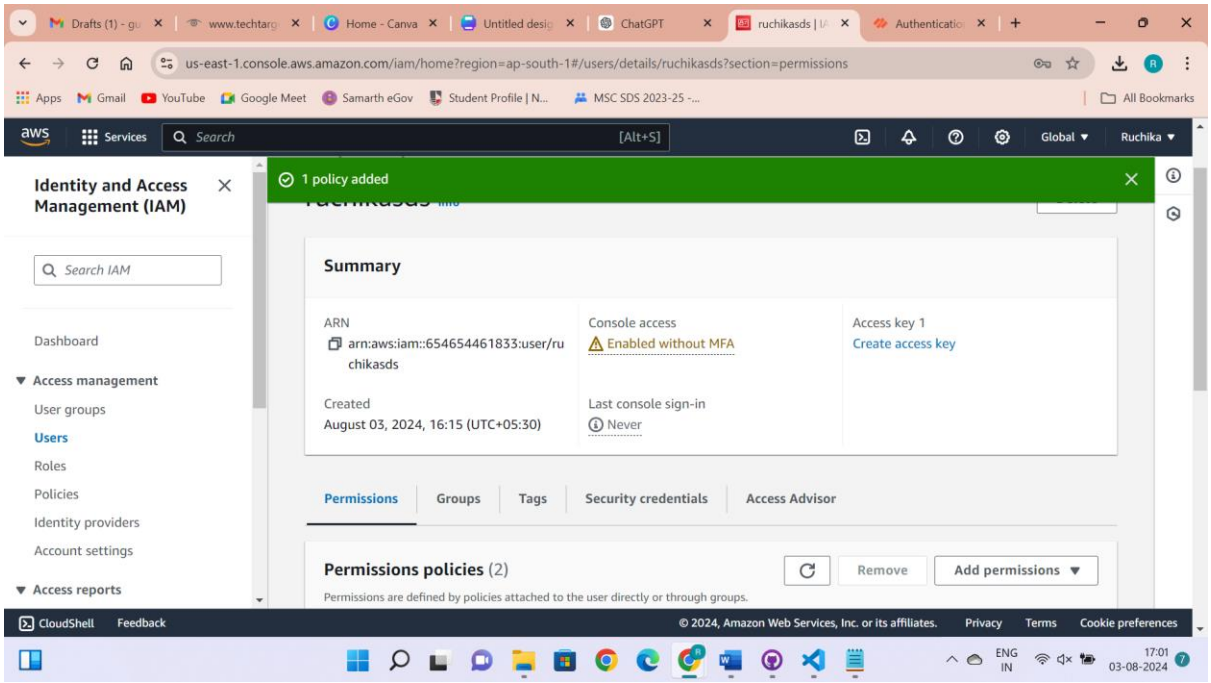

Policy ec2service created.
View policy
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
IAM > Policies
Policies (1223) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
Customer managed
2 matches
Policy name
Type
Used as
Description
ec2service
Customer managed
None
Full access
S3policy
Customer managed
Permissions polic...
Full ACCESS
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

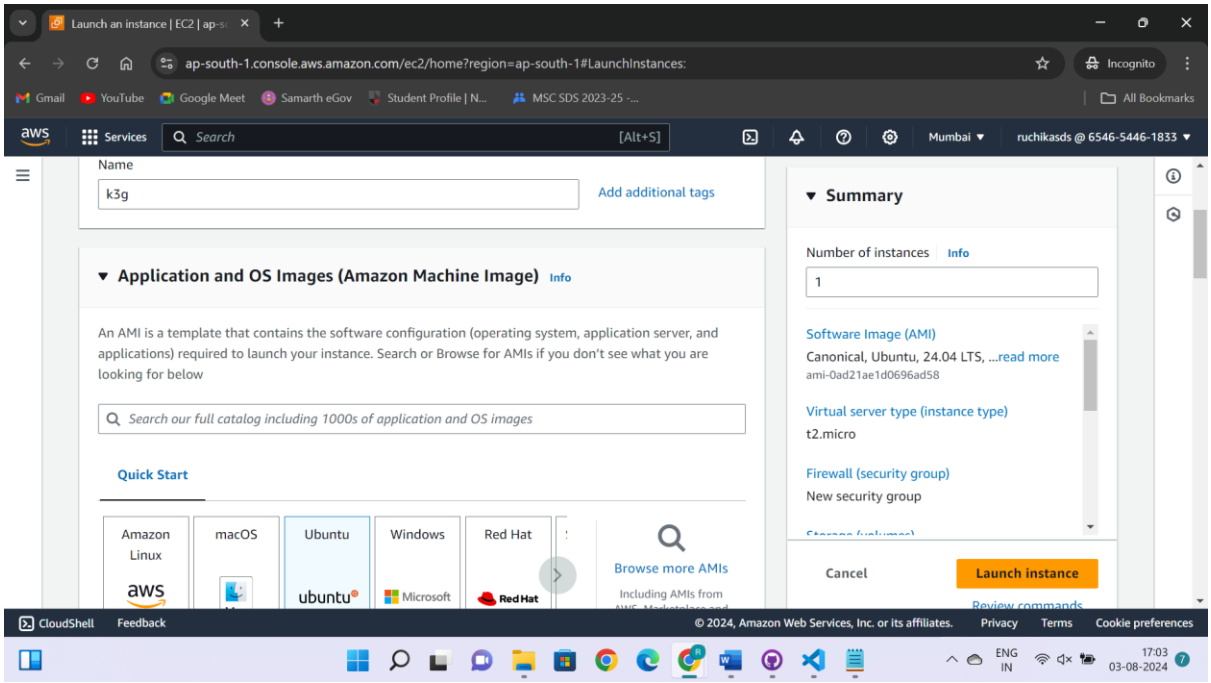

Policy ec2service created.
View policy
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
IAM > Policies > ec2service
ec2service Info
Full access
Edit
Delete
Policy details
Type
Customer managed
Creation time
August 03, 2024, 16:59 (UTC+05:30)
Edited time
August 03, 2024, 16:59 (UTC+05:30)
ARN
arn:aws:iam::654654461833:policy/ec2service
Permissions
Entities attached
Tags
Policy versions (1)
Access Advisor
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

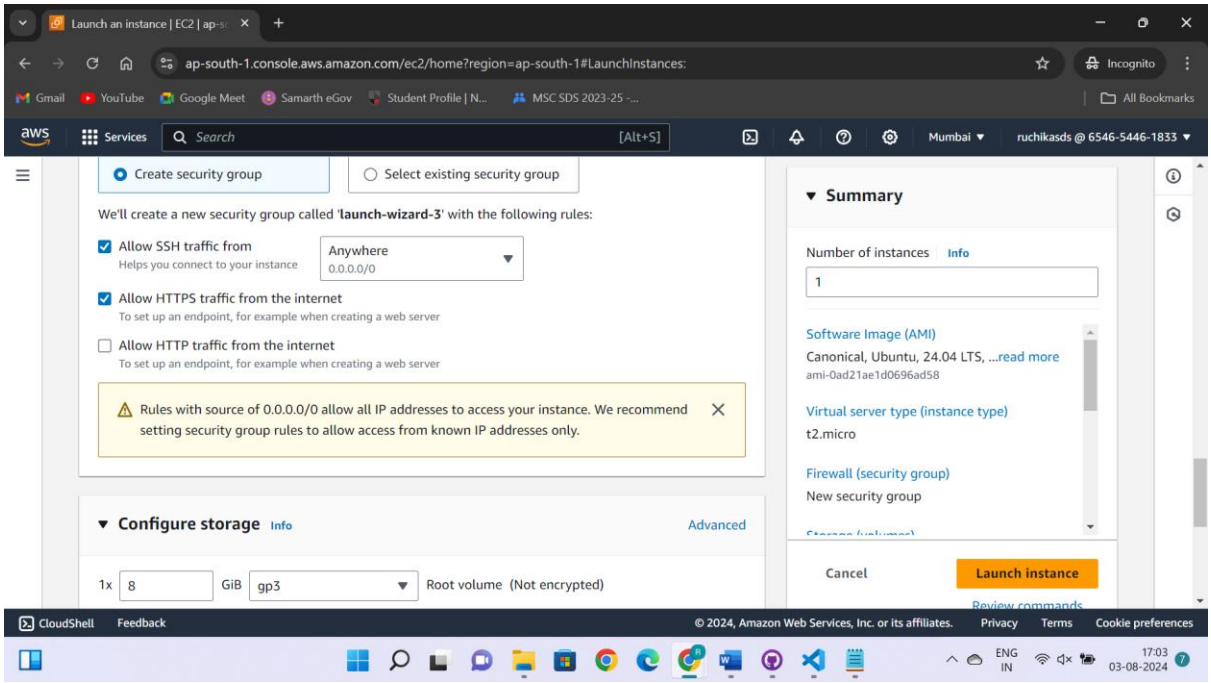

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/ruchikasds/add-permissions
Services
Search
[Alt+S]
Global
Ruchika
IAM > Users > ruchikasds > Add permissions
Step 1
Add permissions
Step 2
Review
Add permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Permissions policies (1224)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
17:00
03-08-2024

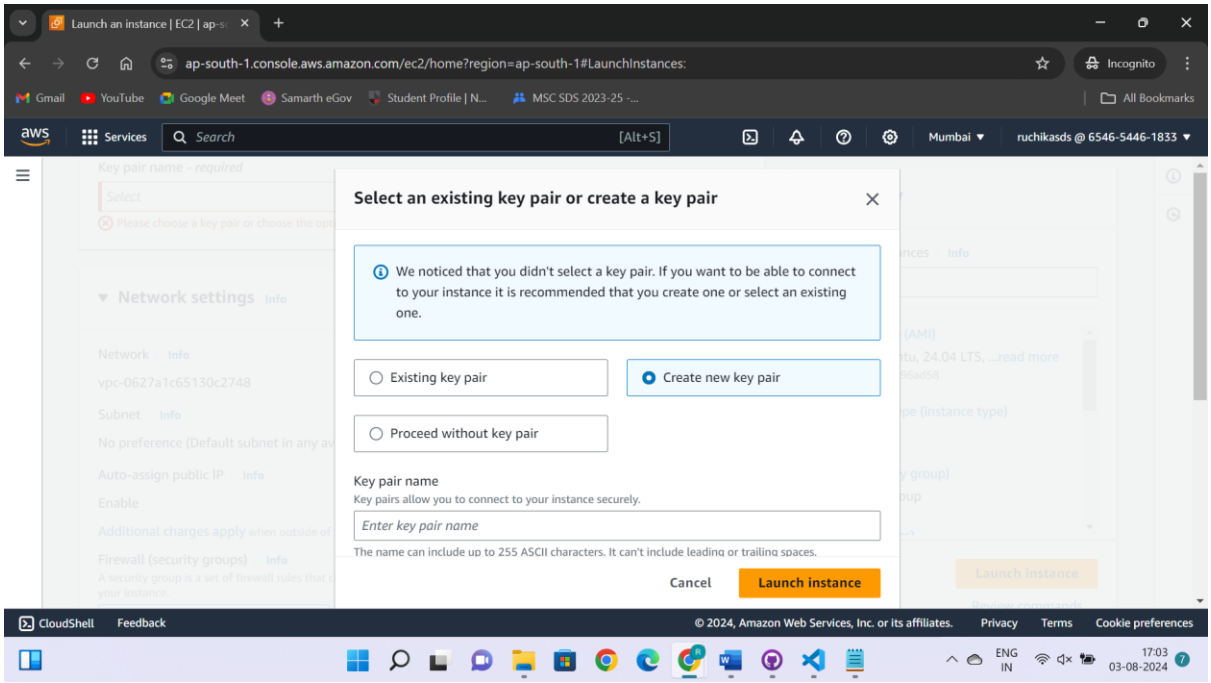

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/ruchikasds/add-permissions
Services
Search
[Alt+S]
Global
Ruchika
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Permissions policies (1224)
Filter by Type
Search
Customer mana...
1 match
1
Policy name
Type
Attached entities
ec2service
Customer managed
0
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
17:00
03-08-2024

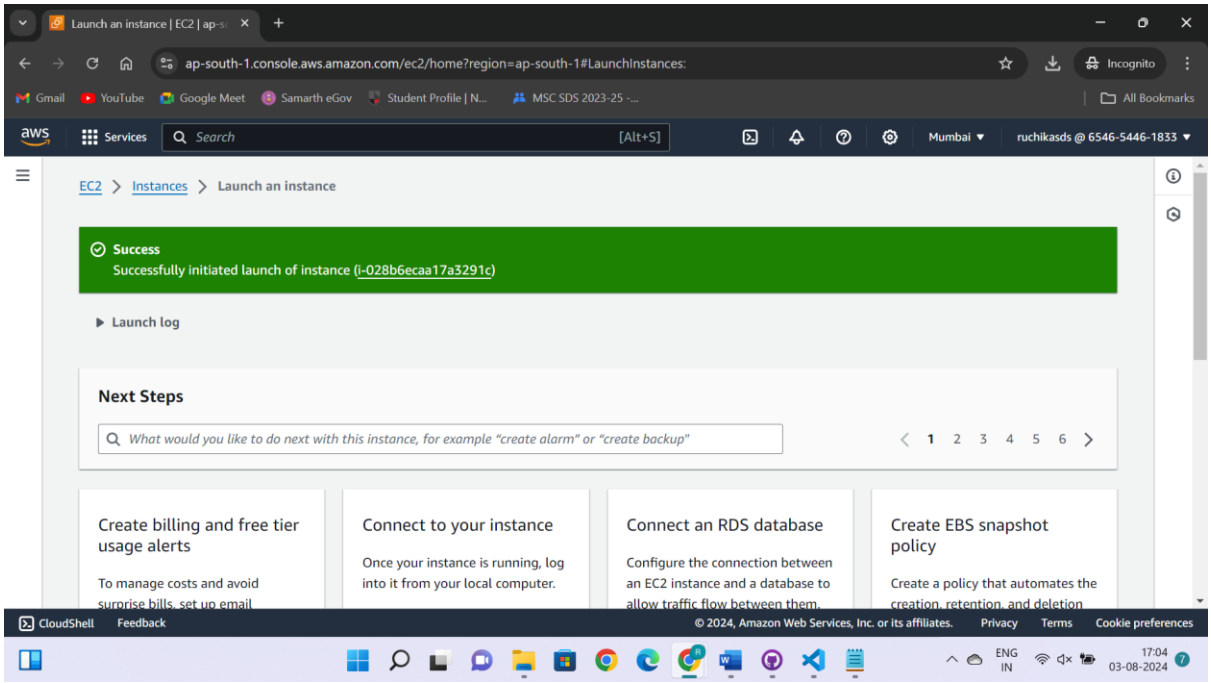

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/ruchikasds/add-permissions
Step 1
Add permissions
Step 2
Review
Review
The following policies will be attached to this user. Learn more
User details
User name
ruchikasds
Permissions summary (1)
Name
Type
Used as
ec2service
Customer managed
Permissions policy
Cancel
Previous
Add permissions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

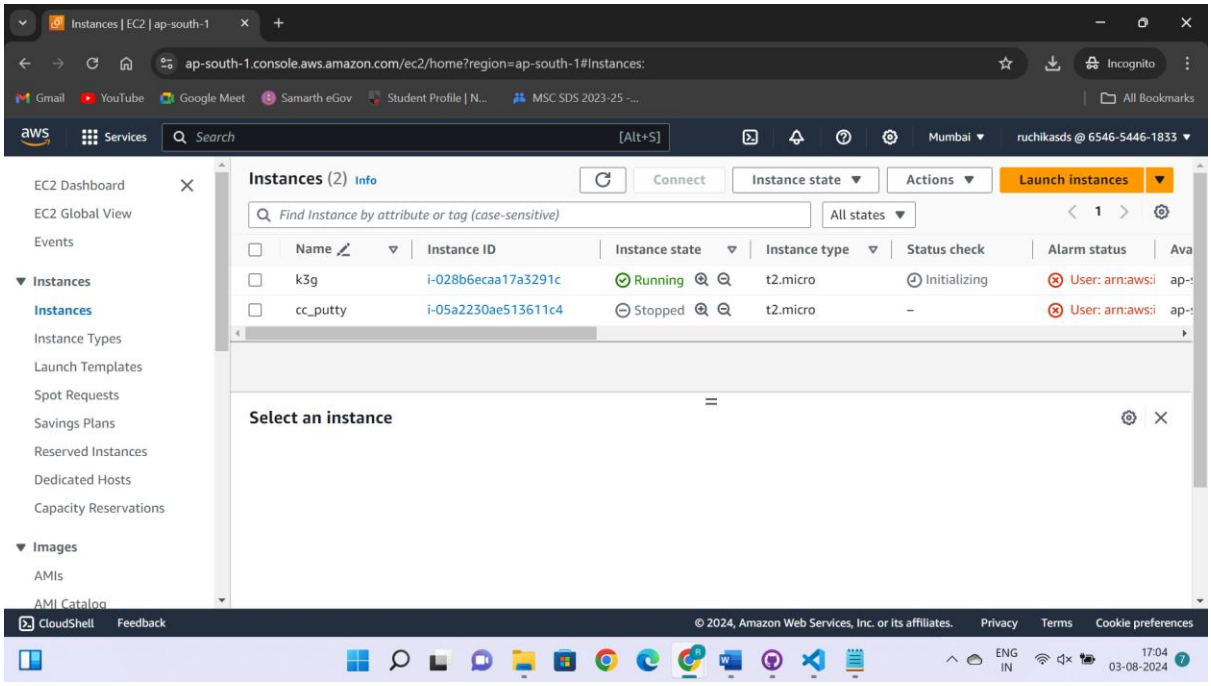

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/ruchikasds?section=permissions
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
1 policy added
Summary
ARN
arn:aws:iam::654654461833:user/ruchikasds
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 16:15 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (2)
Remove
Add permissions
Permissions are defined by policies attached to the user directly or through groups.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Launch an instance | EC2 | ap-s
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Incognito
Gmail
YouTube
Google Meet
Samarth eGov
Student Profile | N...
MSC SDS 2023-25 -...
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai
ruchikasds @ 6546-5446-1833
Name
k3g
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
Browse more AMIs
Including AMIs from
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-0ad21ae1d0696ad58
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
17:03
03-08-2024


Launch an instance | EC2 | ap-s
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Incognito
Gmail
YouTube
Google Meet
Samarth eGov
Student Profile | N...
MSC SDS 2023-25 -...
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai
ruchikasds @ 6546-5446-1833
Create security group
Select existing security group
We'll create a new security group called 'launch-wizard-3' with the following rules:
Allow SSH traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0
Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server
Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Configure storage Info
Advanced
1x
8
GiB
gp3
Root volume (Not encrypted)
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-0ad21ae1d0696ad58
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
17:03
03-08-2024


Launch an instance | EC2 | ap-s
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Incognito
Gmail
YouTube
Google Meet
Samarth eGov
Student Profile | N...
MSC SDS 2023-25 -...
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai
ruchikasds @ 6546-5446-1833
Select an existing key pair or create a key pair
We noticed that you didn't select a key pair. If you want to be able to connect to your instance it is recommended that you create one or select an existing one.
Existing key pair
Create new key pair
Proceed without key pair
Key pair name
Key pairs allow you to connect to your instance securely.
Enter key pair name
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
Cancel
Launch instance
Network settings
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
17:03
03-08-2024


Launch an instance | EC2 | ap-s
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Incognito
Gmail
YouTube
Google Meet
Samarth eGov
Student Profile | N...
MSC SDS 2023-25 -...
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai
ruchikasds @ 6546-5446-1833
EC2
Instances
Launch an instance
Success
Successfully initiated launch of instance (i-028b6ecaa17a3291c)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
1
2
3
4
5
6
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
17:04
03-08-2024


Instances | EC2 | ap-south-1
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:
Incognito
Gmail
YouTube
Google Meet
Samarth eGov
Student Profile | N...
MSC SDS 2023-25 -...
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai
ruchikasds @ 6546-5446-1833
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Instances (2) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
k3g
i-028b6ecaa17a3291c
Running
t2.micro
Initializing
User: arn:aws:i
cc_putty
i-05a2230ae513611c4
Stopped
t2.micro
–
User: arn:aws:i
Select an instance
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
17:04
03-08-2024