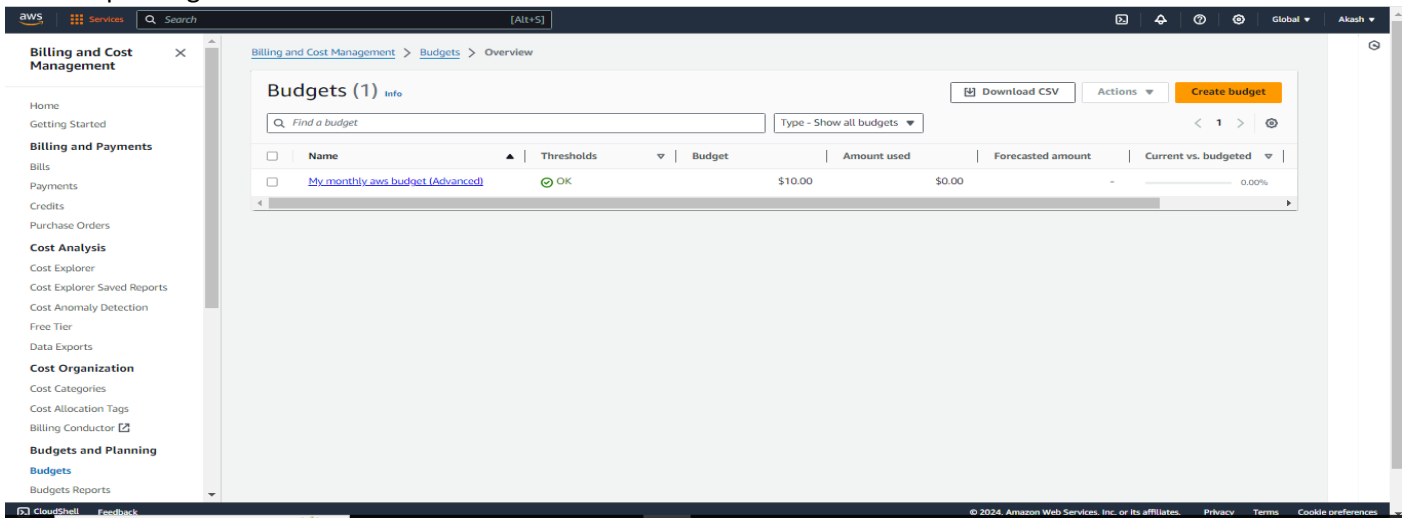


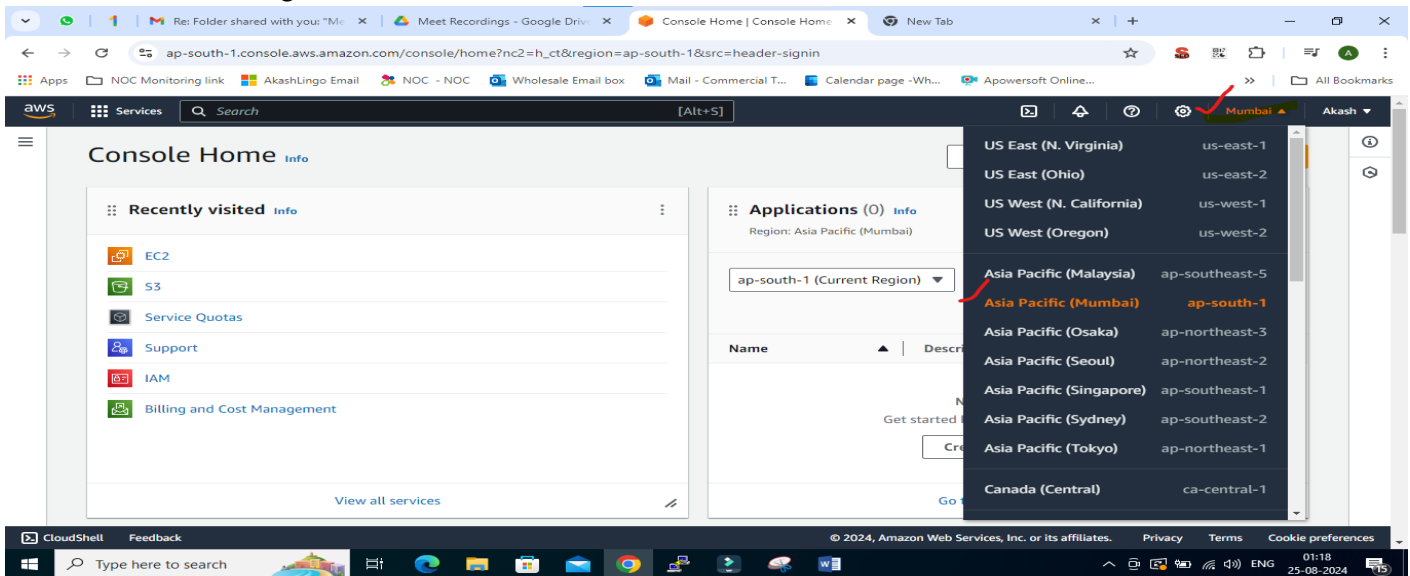
Practical:2 - IAM (Identity Access Management)

14th Aug 2024 (L-2) | Akash Ghuge

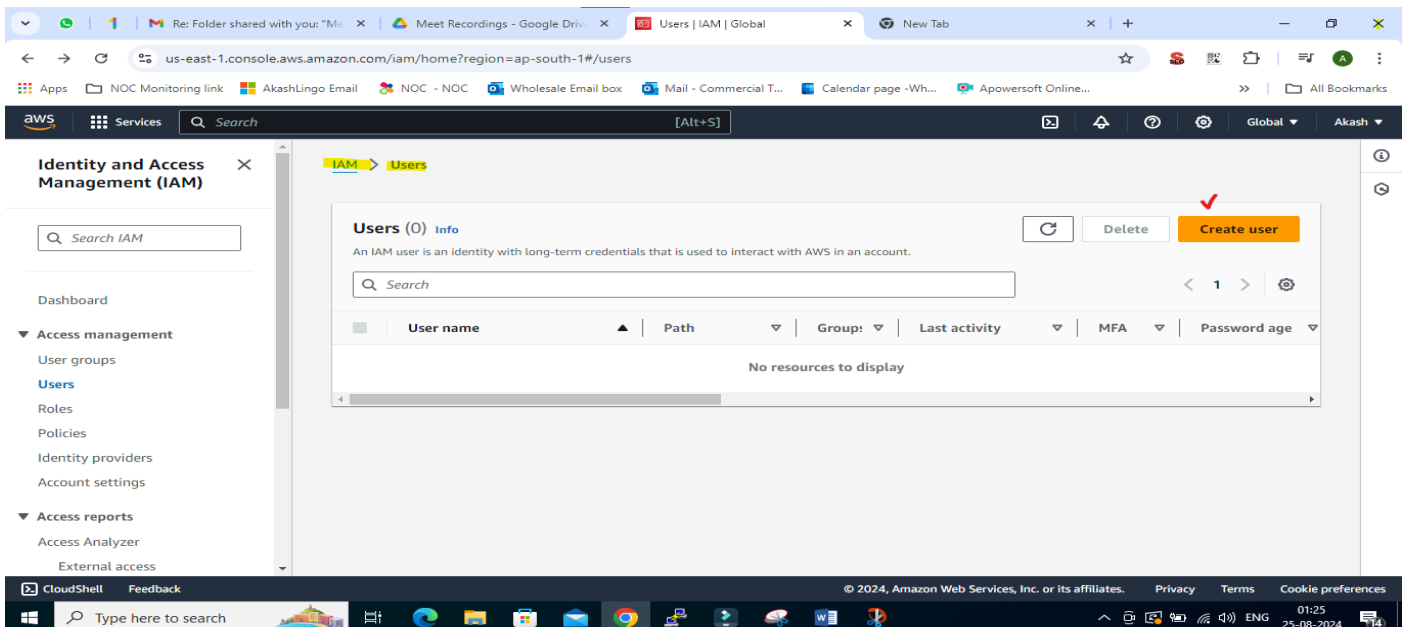
1. Setup billing alarm.



2. Set the Mumbai Regions:



3. Create User



us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create

Step 1
Set permissions

Step 2
Specify user details

Step 3
Review and create

Step 4
Retrieve password

User details

User name
Akash

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.

Are you providing console access to a person?

User type

☐ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ **I want to create an IAM user**
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS, CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☒ **Autogenerated password**
You can view the password after you create the user.

☐ Custom password
Enter a custom password for the user.

- 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

Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

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](#)

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

01:39
25-08-2024

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create

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 (1/1225)
Choose one or more policies to attach to your new user.

Filter by Type
All types 1 match

Policy name	Type	Attached entities
<input checked="" type="checkbox"/> IAMFullAccess	AWS managed	0

Set permissions boundary - optional

Cancel Previous **Next**

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

01:42
25-08-2024

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create

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
Akash

Console password type
Autogenerated

Require password reset
No

Permissions summary

Name	Type	Used as
<input checked="" type="checkbox"/> IAMFullAccess	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.

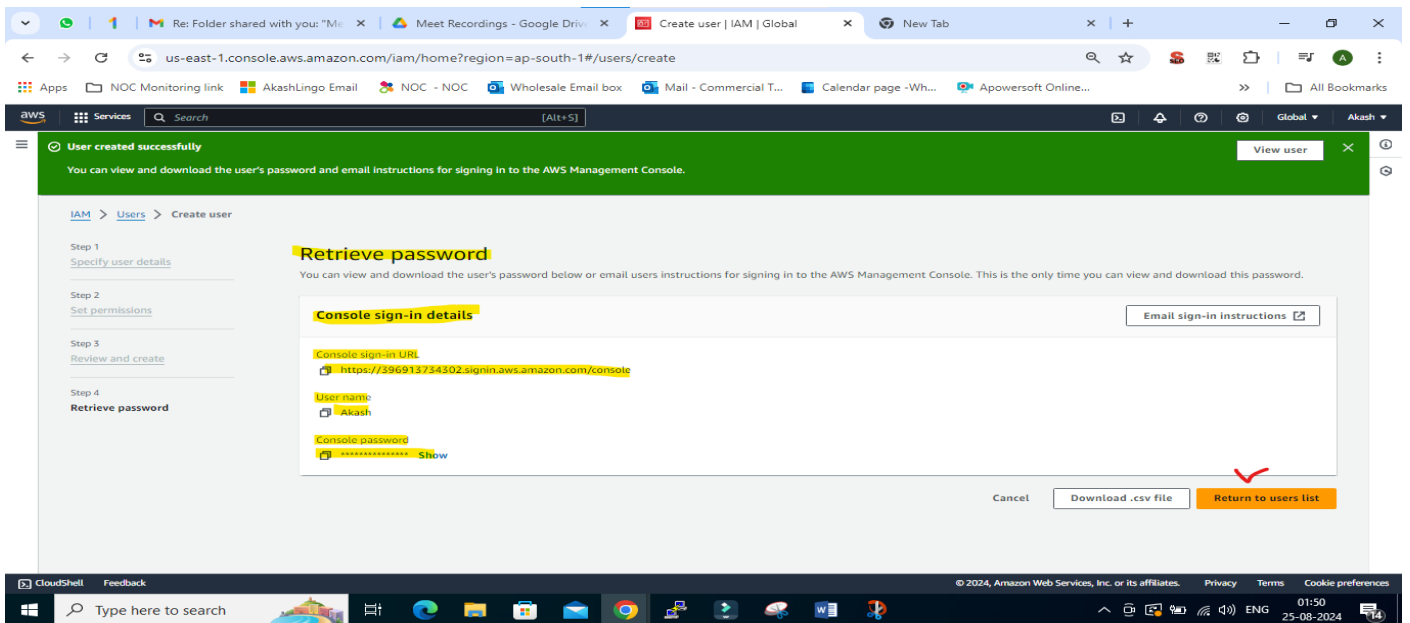
No tags associated with the resource.

[Add new tag](#)
You can add up to 50 more tags.

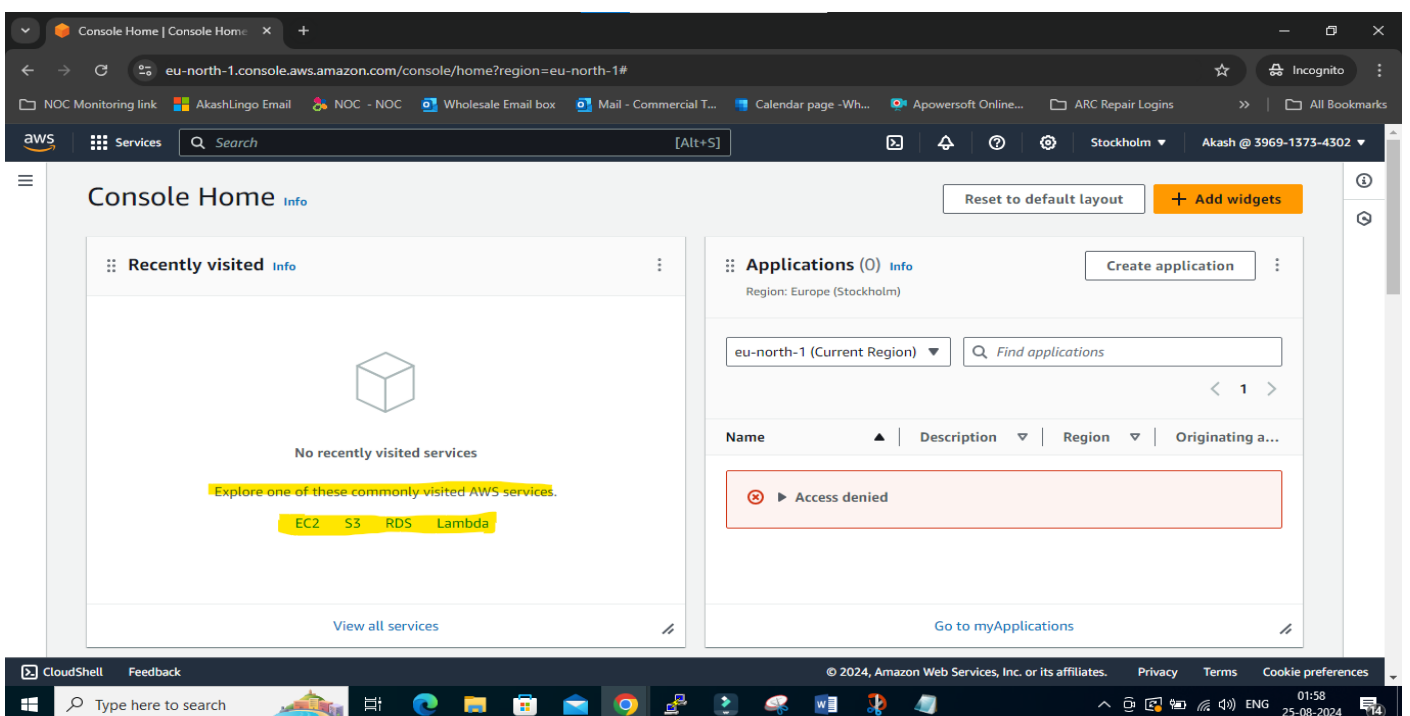
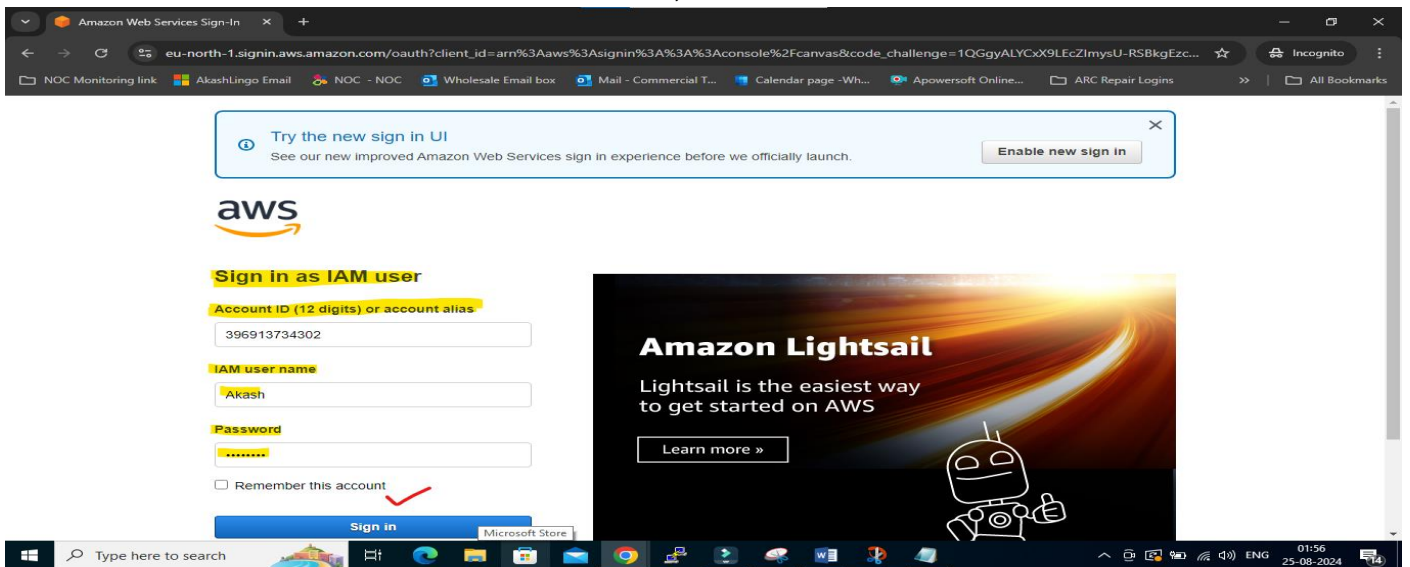
Cancel Previous **Create user**

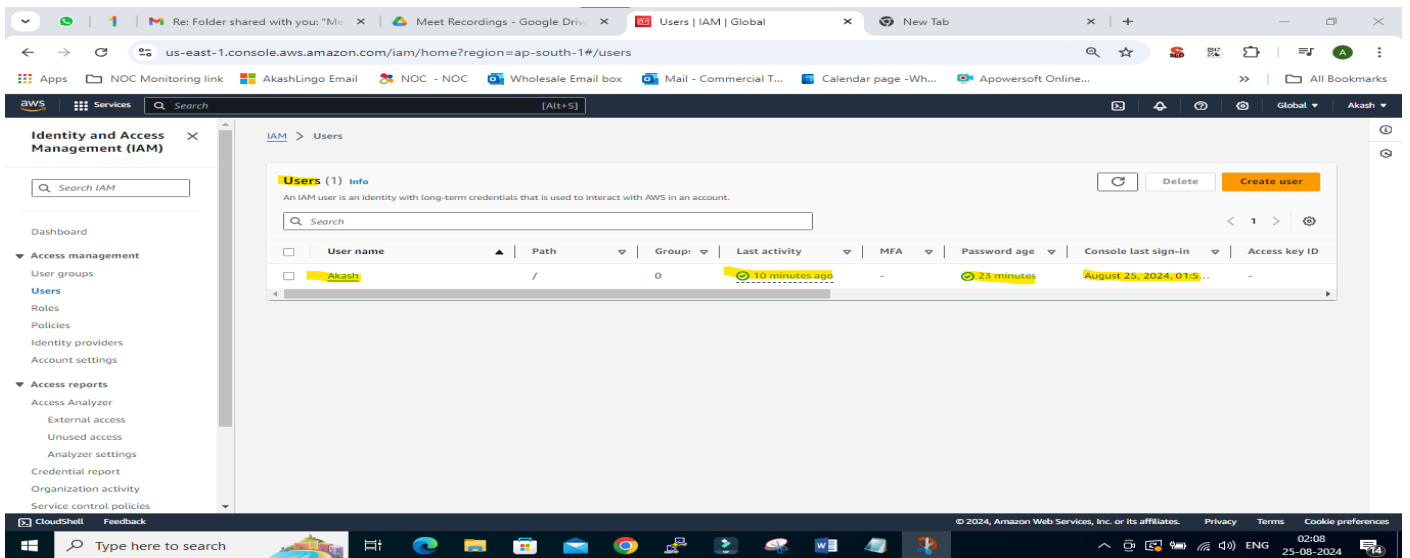
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

01:43
25-08-2024

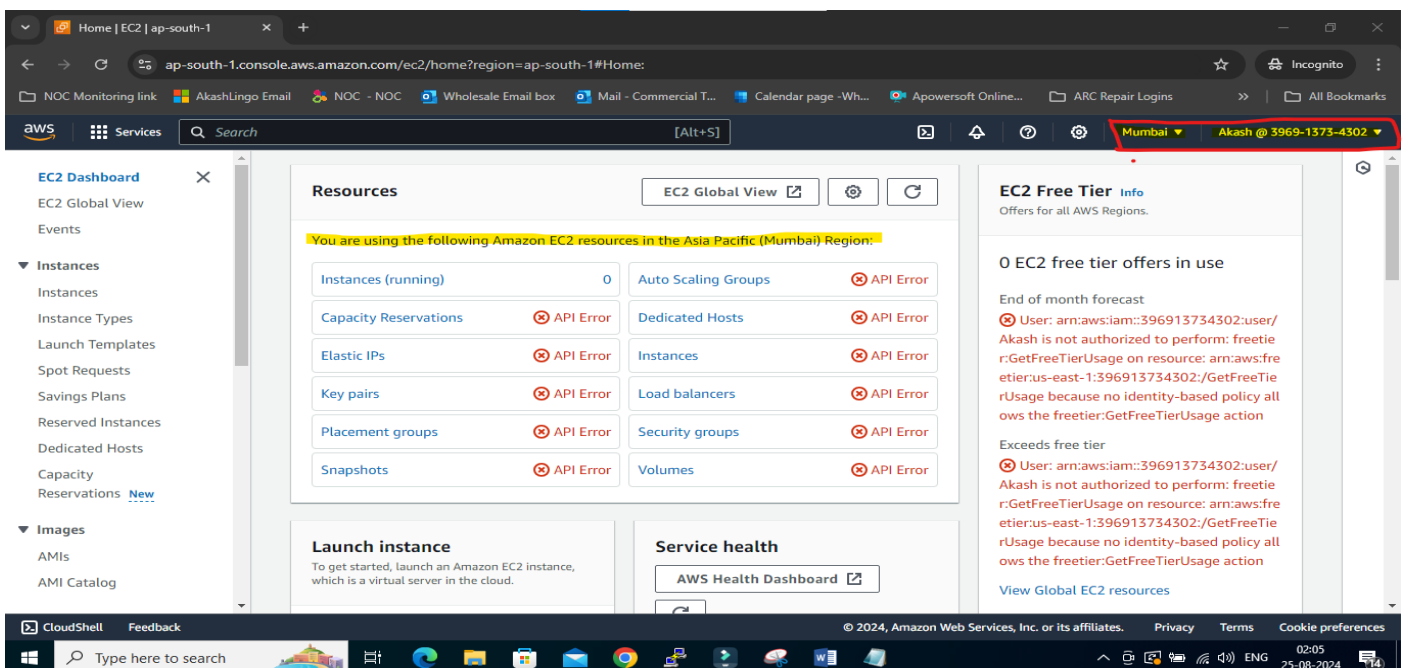
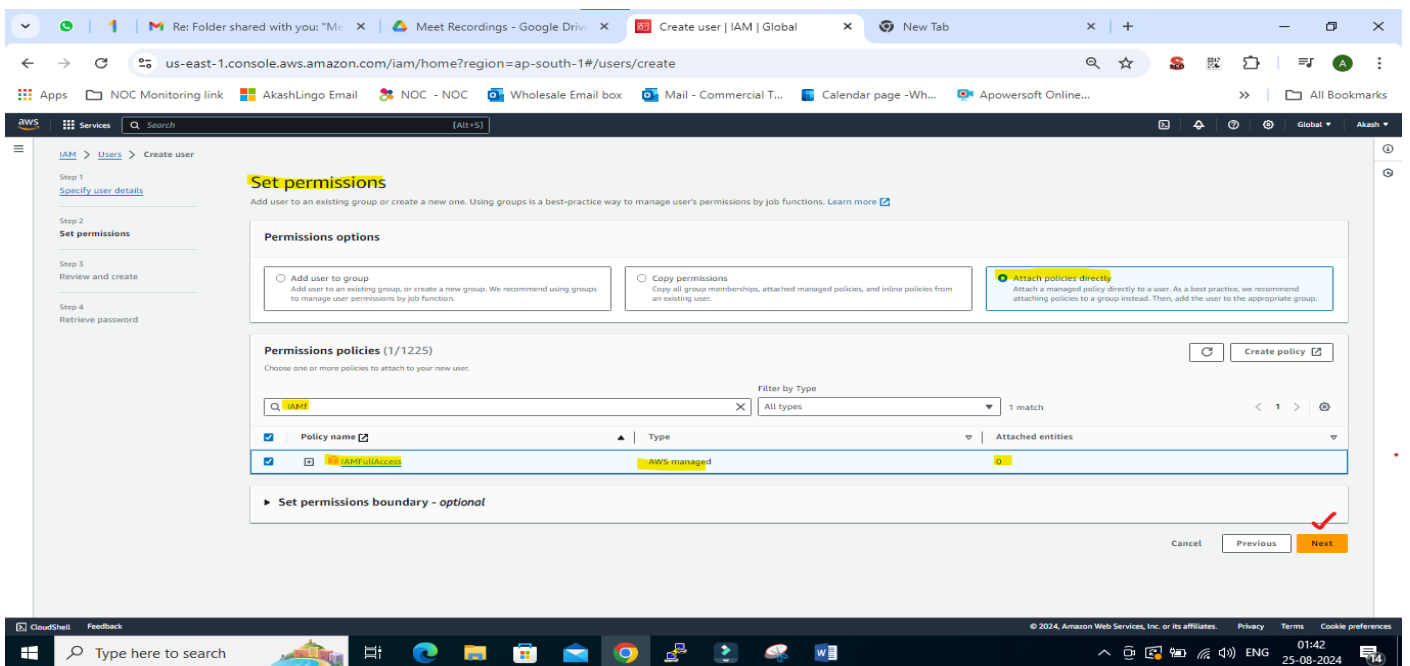


4. Used Different Browser to access IAM user with URL, ID & Password





5. IAM User are able to access all the services such as S3 & EC2 etc.



1. User: Airindia >> Policy S3 Full Access:

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create

Set permissions

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

User details

User name
airindia

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.

Are you providing console access to a person?

User type

☐ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☒ Autogenerated password
You can view the password after you create the user.

☐ Custom password
Enter a custom password for the user.

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

Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

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

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☐ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

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

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

Permissions policies (1/1225)

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

Filter by Type
All types 1 match

Policy name	Type	Attached entities
AmazonS3FullAccess	AWS managed	0

Set permissions boundary - optional

Cancel Previous Next

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/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
airindia

Console password type
Autogenerated

Require password reset
No

Permissions summary

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy

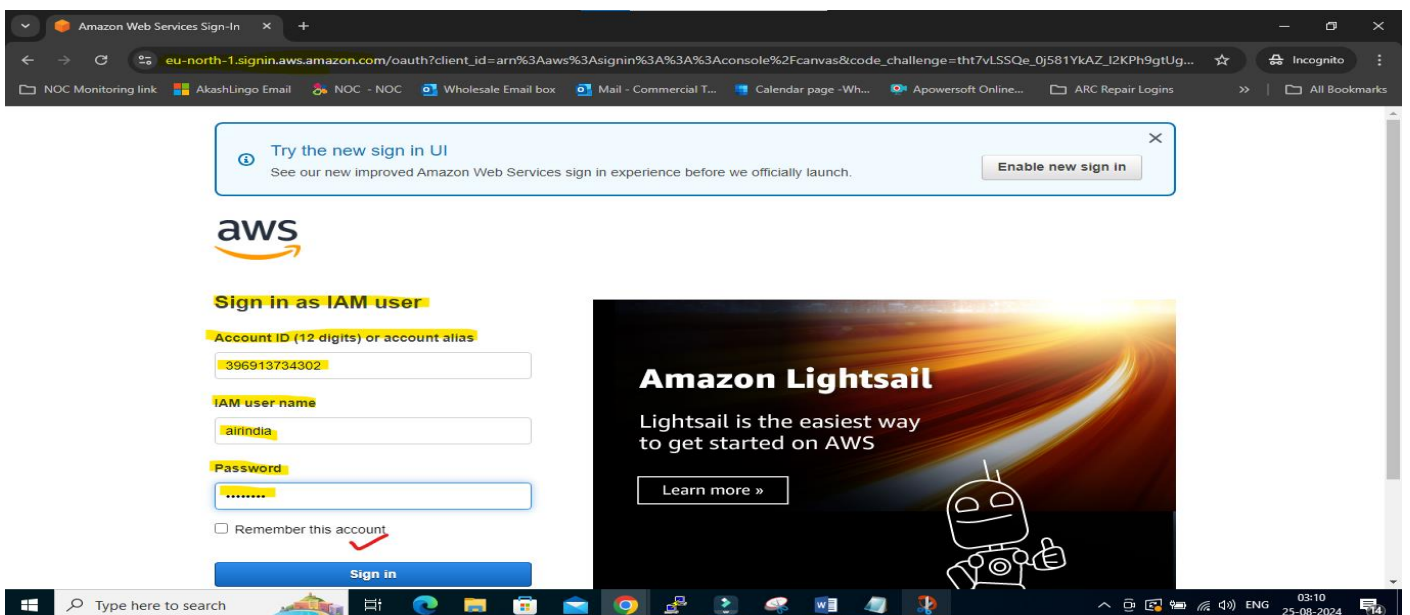
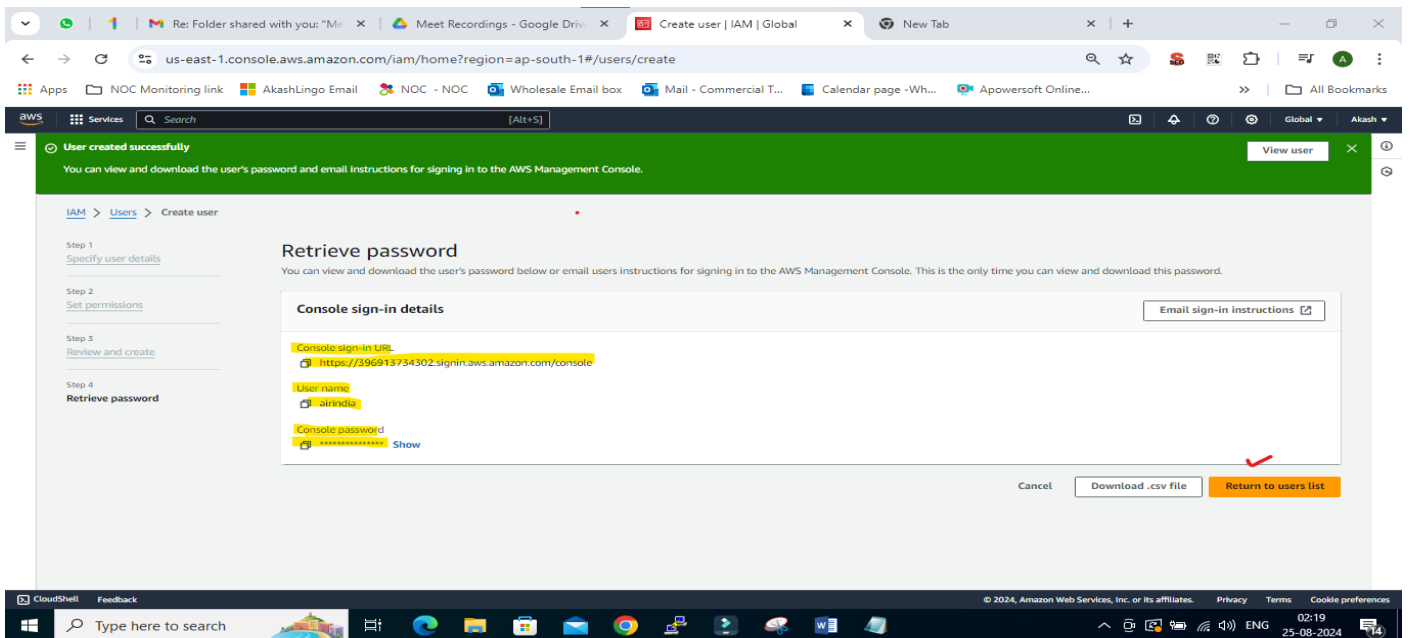
Tags - optional

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.

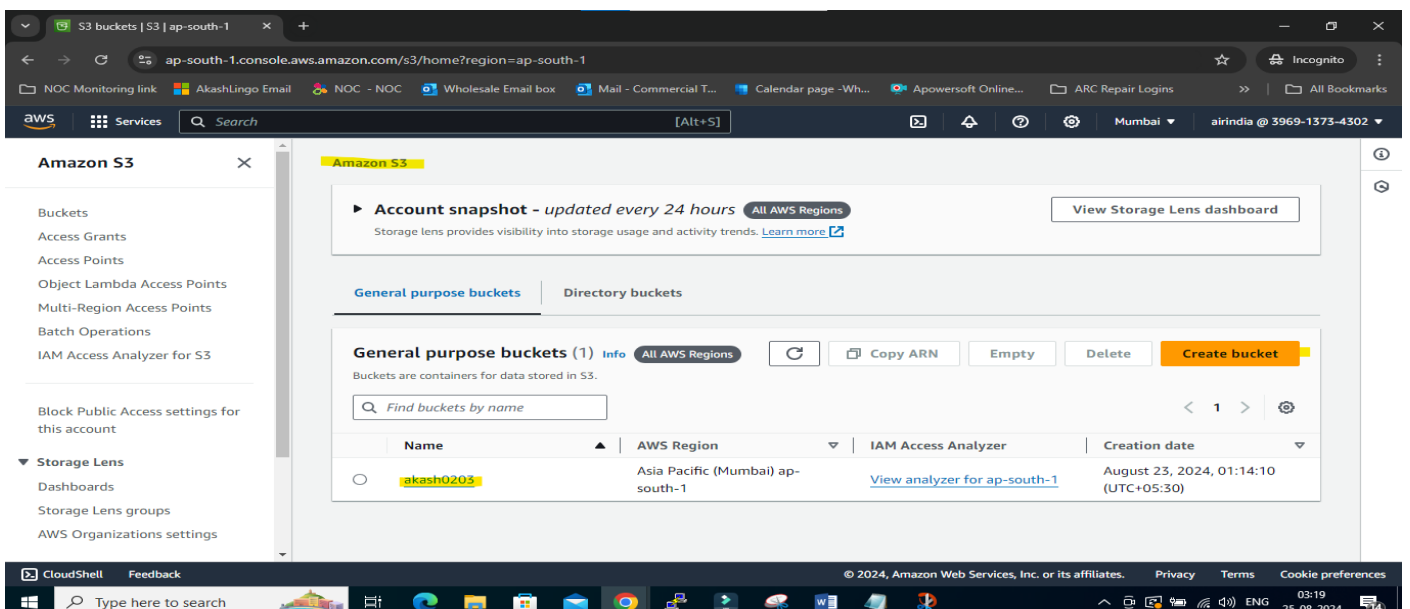
No tags associated with the resource.

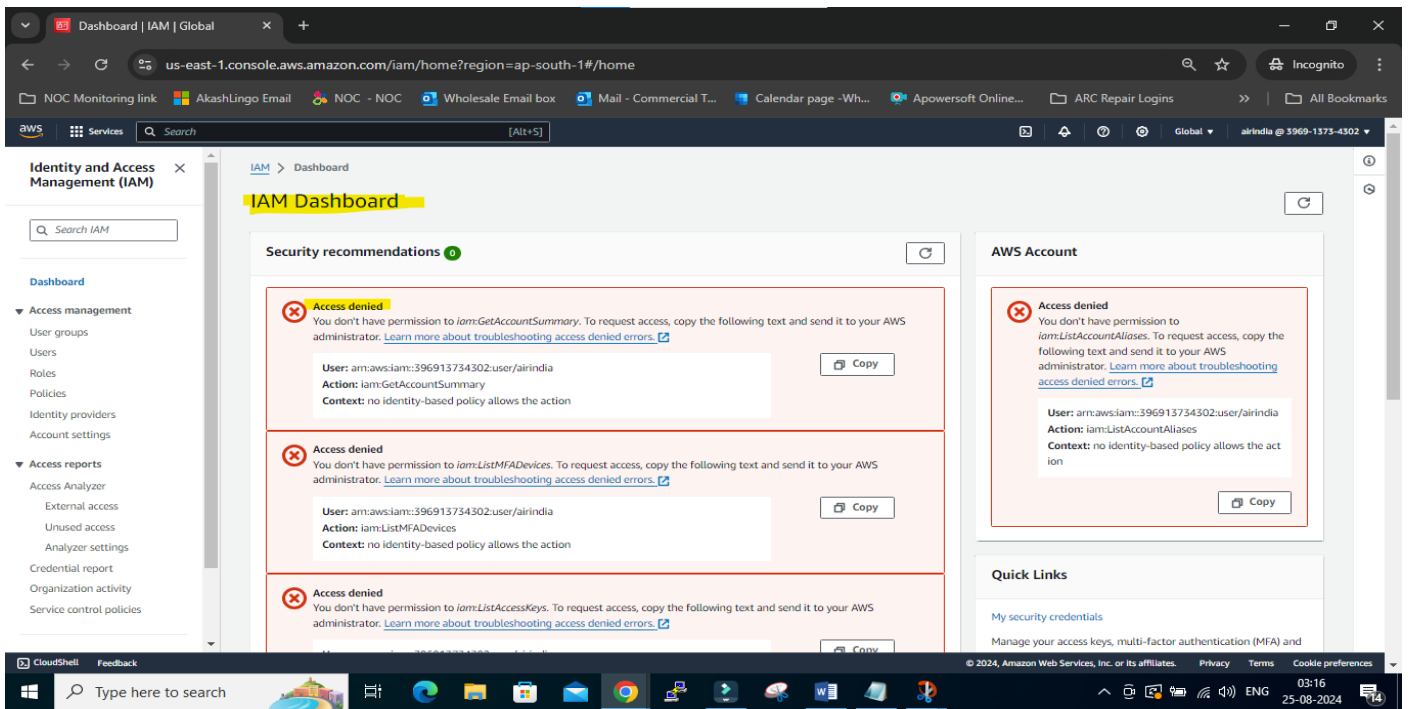
Add new tag
You can add up to 50 more tags.

Cancel Previous Create user

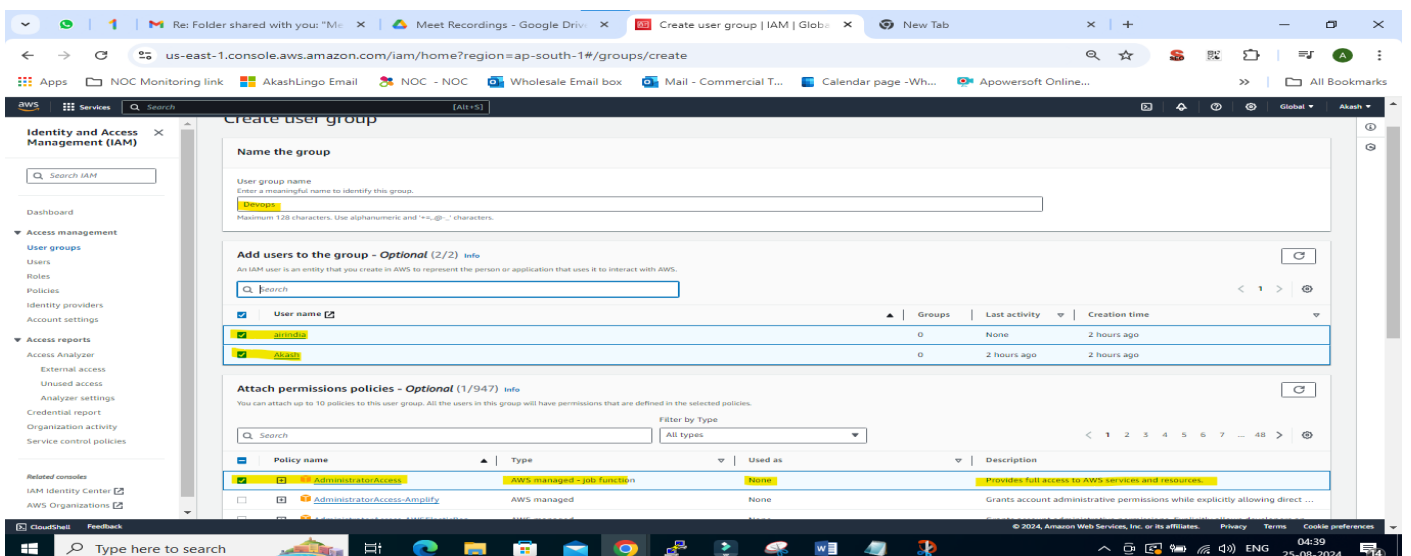
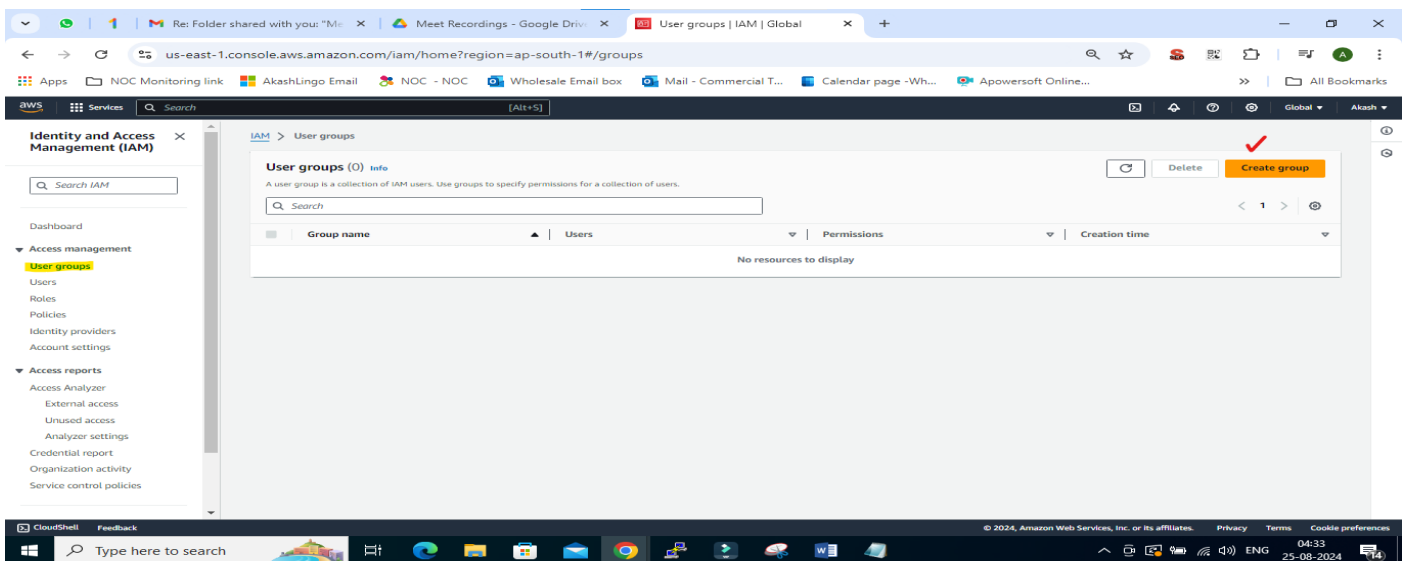


2. AirIndia user is only allow to access S3 not for IAM:





1. Create Groups:



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

Identity and Access Management (IAM)

Devops user group created.

User groups (1) info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

Group name	Users	Permissions	Creation time
Devops	2	Defined	Now

Users in this group

- airindia
- Akash

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/Devops?section=users

Devops info

Summary

User group name: Devops

Creation time: August 25, 2024, 04:59 (UTC+05:30)

ARN: arn:aws:iam::396913754502:group/Devops

Users (2)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Groups	Last activity	Creation time
airindia	1	1 hour ago	2 hours ago
Akash	1	2 hours ago	3 hours ago

2. Group level permission:

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/Devops?section=permissions

Devops info

Summary

User group name: Devops

Creation time: August 25, 2024, 04:59 (UTC+05:30)

ARN: arn:aws:iam::396913754502:group/Devops

Permissions policies (1) info

You can attach up to 10 managed policies.

Filter by Type: All types

Policy name	Type	Attached entities
AWSAdministratorAccess	AWS managed - job function	1

3. Individual permissions:

This screenshot shows the AWS IAM console for user 'Akash' in the 'us-east-1' region. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Related consoles. The main content area displays the user's summary, including their ARN, console access status, and creation date. Below the summary, the 'Permissions' tab is active, showing two policies: 'AdministratorAccess' and 'IAMFullAccess'. The 'Permissions policies (2)' section includes a search bar, a filter by type dropdown, and a table listing the policies with their names, types, and attachment methods. The 'Permissions boundary' section is currently not set.

Summary

- ARN: `arn:aws:iam::996915734502:user/Akash`
- Console access: Enabled without MFA
- Access key 1: [Create access key](#)
- Created: August 25, 2024, 01:44 (UTC+05:30)
- Last console sign-in: Today

Permissions policies (2)

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

Filter by Type: All types

Policy name	Type	Attached via
AdministratorAccess	AWS managed - job function	Group Devops
IAMFullAccess	AWS managed	Directly

Permissions boundary (not set)

This screenshot shows the AWS IAM console for user 'airindia' in the 'us-east-1' region. The interface is similar to the previous one, displaying the user's summary and permissions. The 'airindia' user was created on August 25, 2024, at 02:19 (UTC+05:30). The 'Permissions' tab shows two policies: 'AdministratorAccess' and 'AmazonS3FullAccess'. The 'Permissions policies (2)' section includes a search bar, a filter by type dropdown, and a table listing the policies with their names, types, and attachment methods. The 'Permissions boundary' section is currently not set.

Summary

- ARN: `arn:aws:iam::996915734502:user/airindia`
- Console access: Enabled without MFA
- Access key 1: [Create access key](#)
- Created: August 25, 2024, 02:19 (UTC+05:30)
- Last console sign-in: Today

Permissions policies (2)

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

Filter by Type: All types

Policy name	Type	Attached via
AdministratorAccess	AWS managed - job function	Group Devops
AmazonS3FullAccess	AWS managed	Directly

Permissions boundary (not set)

Access Key & Secret access Key:

The screenshot shows the AWS IAM console for a user named Akash. The 'Security credentials' tab is selected, displaying the following information:

- Summary:** ARN: `arn:aws:iam::396915754302:user/Akash`, Created: August 25, 2024, 01:44 (UTC+05:30). Console access is enabled without MFA. The last console sign-in was today.
- Access key 1:** A button to 'Create access key' is visible.
- Console sign-in:** A link to the console sign-in page is provided. The console password was updated 3 hours ago (2024-08-25 01:44 GMT+5:30). The last console sign-in was 3 hours ago (2024-08-25 01:57 GMT+5:30).
- Multi-factor authentication (MFA):** A message states that no MFA devices are assigned. Buttons for 'Remove', 'Resync', and 'Assign MFA device' are present.

This screenshot shows the same AWS IAM console page, but with the 'Access keys' section expanded. It displays the following information:

- Access keys (0):** A message states that no access keys are assigned. A button to 'Create access key' is visible.
- SSH public keys for AWS CodeCommit (0):** A message states that no SSH public keys are assigned. A button to 'Upload SSH public key' is visible.

The screenshot shows the 'Create access key' wizard in the AWS IAM console. The 'Access key best practices & alternatives' step is selected. The wizard provides guidance on using long-term credentials and offers several alternatives for creating an access key. The 'Recommended' alternative is selected, which involves using the AWS CLI V2 and enabling authentication through a user in the IAM Identity Center. The 'Next' button is highlighted with a red checkmark.

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Akash/create-access-key

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.



Step 1
[Access key best practices & alternatives](#)

Step 2 - optional
[Set description tag](#)

Step 3
Retrieve access keys

Retrieve access keys [Info](#)

Access key
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
	 Show

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](#).

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 05:27 25-08-2024

By using CLI:

1. Create & Deleted User:

```
C:\Users\Admin>aws iam create-user --user-name purvi ✓
{
  "User": {
    "Path": "/",
    "UserName": "purvi",
    "UserId": "AIDAVY2PG6KPPQSBK004Z",
    "Arn": "arn:aws:iam::396913734302:user/purvi",
    "CreateDate": "2024-08-25T12:02:50+00:00"
  }
}

C:\Users\Admin>aws iam create-user --user name purvi
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

    aws help
    aws <command> help
    aws <command> <subcommand> help

Unknown options: purvi

C:\Users\Admin>aws iam delete-user --user-name purvi ✓
```

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users

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

Users (4) [Info](#)

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

[Search](#)

	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
<input type="checkbox"/>	Aaru	/	0	5 minutes ago	-	8 minutes	August 25, 2024, 1
<input type="checkbox"/>	Akash	/	0	15 hours ago	-	15 hours	August 25, 2024, 0
<input type="checkbox"/>	purvi	/	0	-	-	-	-
<input type="checkbox"/>	Ravi	/	0	11 hours ago	-	11 hours	August 25, 2024, 0

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 17:34 25-08-2024

2. Create & Deleted Group:

```
Command Prompt
put-group-policy
put-role-policy
put-user-policy
remove-role-from-instance-profile
reset-service-specific-credential
set-default-policy-version
simulate-custom-policy
tag-instance-profile
tag-open-id-connect-provider
tag-role
tag-server-certificate
untag-instance-profile
untag-open-id-connect-provider
untag-role
untag-server-certificate
update-access-key
update-assume-role-policy
update-login-profile
update-role
update-saml-provider
update-server-certificate
update-signing-certificate
upload-ssh-public-key
upload-signing-certificate
wait
put-role-permissions-boundary
put-user-permissions-boundary
remove-client-id-from-open-id-connect-provider
remove-user-from-group
resync-mfa-device
set-security-token-service-preferences
simulate-principal-policy
tag-mfa-device
tag-policy
tag-saml-provider
tag-user
untag-mfa-device
untag-policy
untag-saml-provider
untag-user
update-account-password-policy
update-group
update-open-id-connect-provider-thumbprint
update-role-description
update-ssh-public-key
update-service-specific-credential
update-user
upload-server-certificate
wizard
help

C:\Users\Admin>aws iam create-group --group-name aapag
{
  "Group": {
    "Path": "/",
    "GroupName": "aapag",
    "GroupId": "AGPAVY2PG6KPJOYAJHLZJ",
    "Arn": "arn:aws:iam:396913734302:group/aapag",
    "CreateDate": "2024-08-25T12:21:09+00:00"
  }
}

C:\Users\Admin>aws iam delete-group --group-name aapag

An error occurred (NoSuchEntity) when calling the DeleteGroup operation: The group with name aapag cannot be found.

C:\Users\Admin>
```

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/groups

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
- Unused access
- Analyzer settings

User groups (2) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	aapag	0	Not defined	Now
<input type="checkbox"/>	Devops	0	Defined	13 hours ago

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search

17:51 25-08-2024

Theory – IAM (Identity Access Management)

IAM: Identity access management – User management

IMP: User, Group, Role, Policy Document

Login with 3 types

1. **GUI** – URL, ID, Password
2. **CLI** – Access Key & Secret access key
3. **Terraform** -
 1. Create user - Give permission to user – **Policy document** – Written in Jason (Java Script Object note- Key value pair) – EC2 Full access
 2. Policy Document Type: 1. AWS Managed & 2. Inline Policy
 3. While creating user we get ARL (Amazon Record Name) – Unique
 4. Ex. **arn:aws:iam::396913734302:user/Akash**
 5. Group - Give permission to Group – Policy document – Written in **Jason** – EC2 Full access
 6. **Role**- assign Policy Document - attached with instance – a) While creating the instance b) Already created in instance

Q. Why should I learn IAM service?

IAM is used for the user management with the help of IAM we managed the entire **user management lifecycle**.

User Management lifecycle

1. User ID Creation / User or Group Creation
2. Password creation
3. Email ID creation
4. Access Management / Policy Document