AWS MODULE

Submitted by -ADESH ARUN ADHAV

Submitted to- VIKUL SIR

Batch no.-Devops SA2409031

DATE- 18/10/2024

L2 -Login to AWS Console and Create IAM User, Role, and Group

Step 1: Log in to the AWS Management Console

1. Open the AWS management console.
2. Create your account in aws console by providing your details.
3. Enter your root account credentials to log in.

Step 2: Create an IAM User

1.navigate the IAM service in aws console

2.click on add on user.

3.enter username detail and give the access to the user

(for eg. Ec2 full access)

Step 3: Create a Group

1.Clik on create group

2. Give group name

3.After creating group open the group and add the user to the group

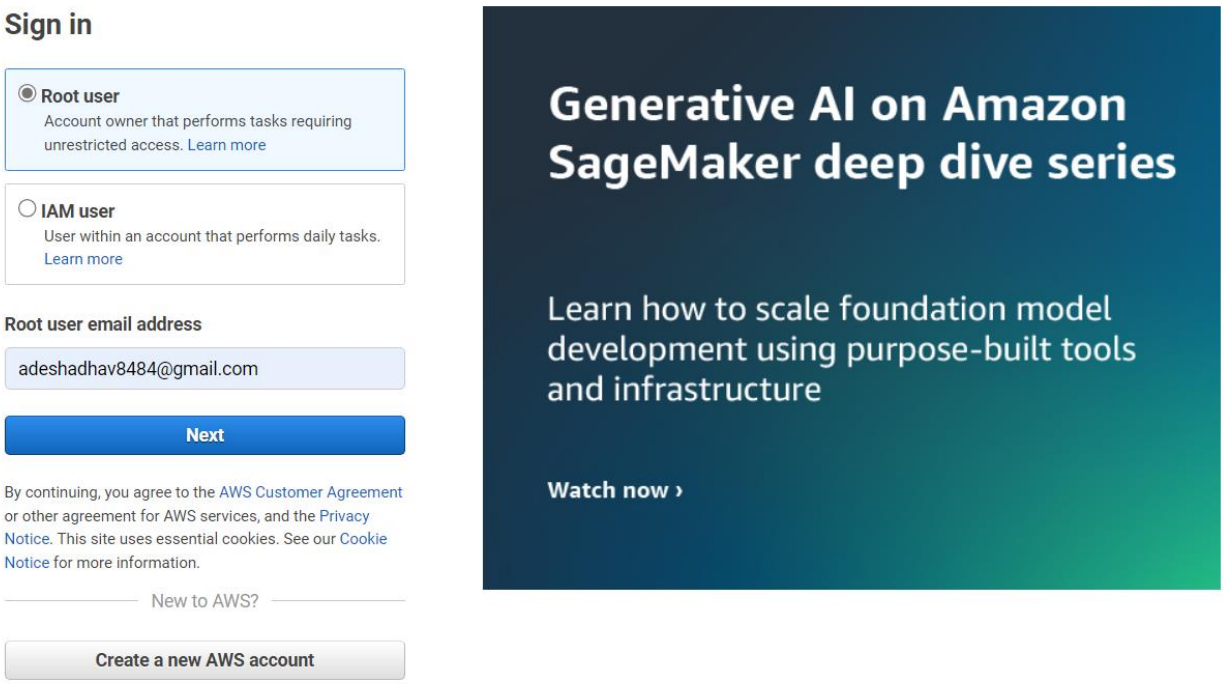
STEP 4 : Create an IAM Role

1.navigate to role services

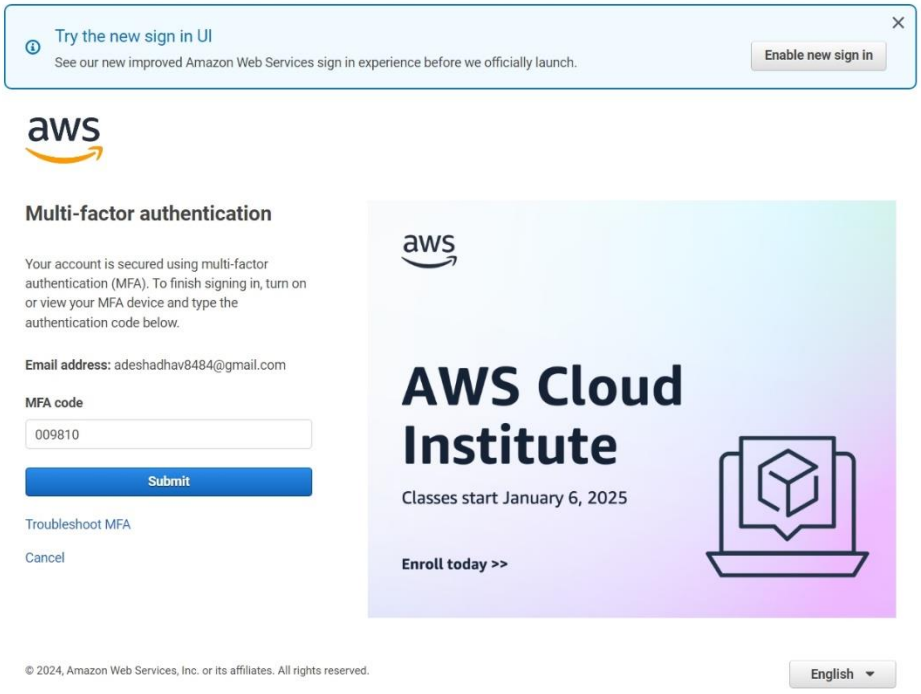
2.clik on create the role

3.Attach policies to the role by giving permission

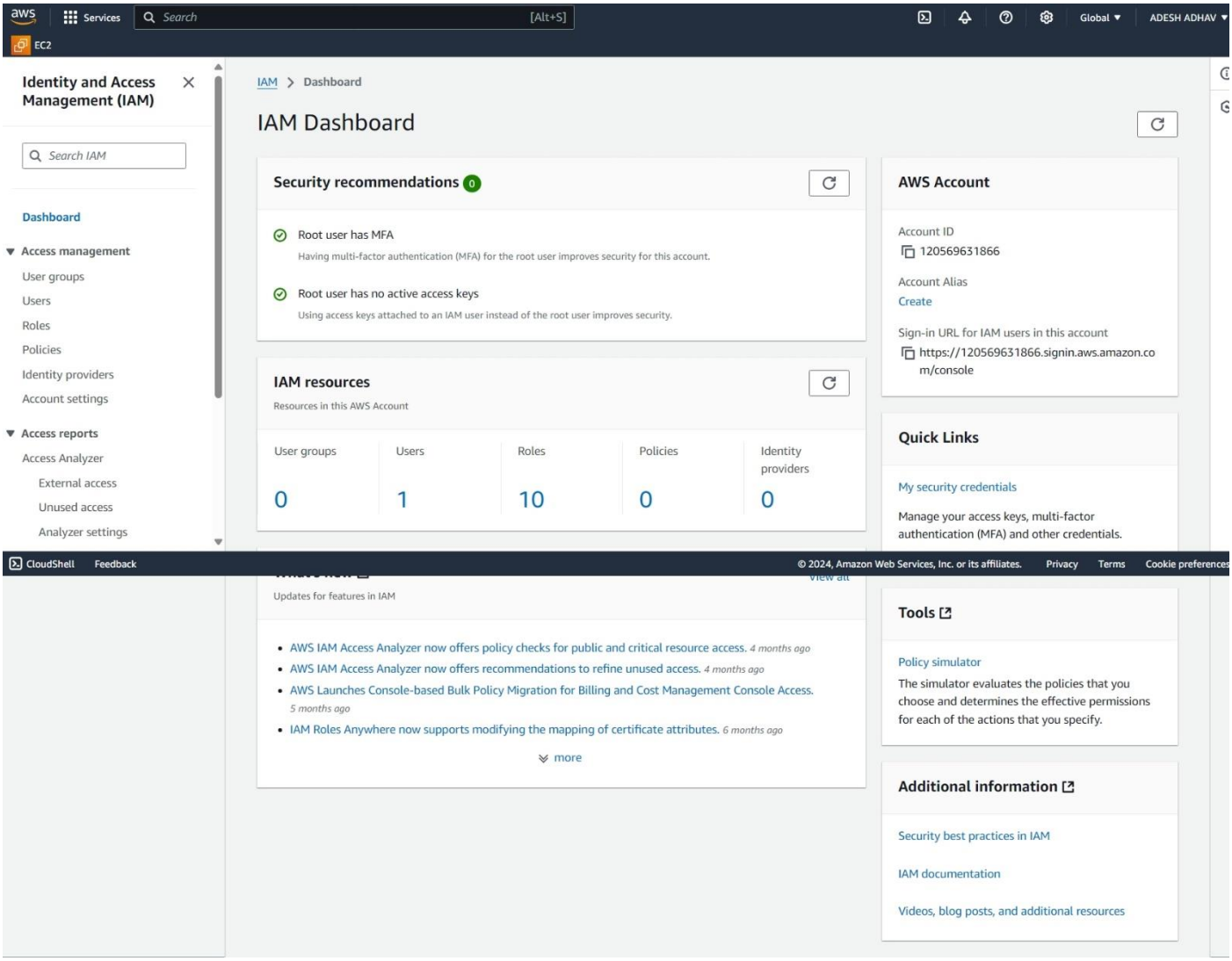
- Login to console



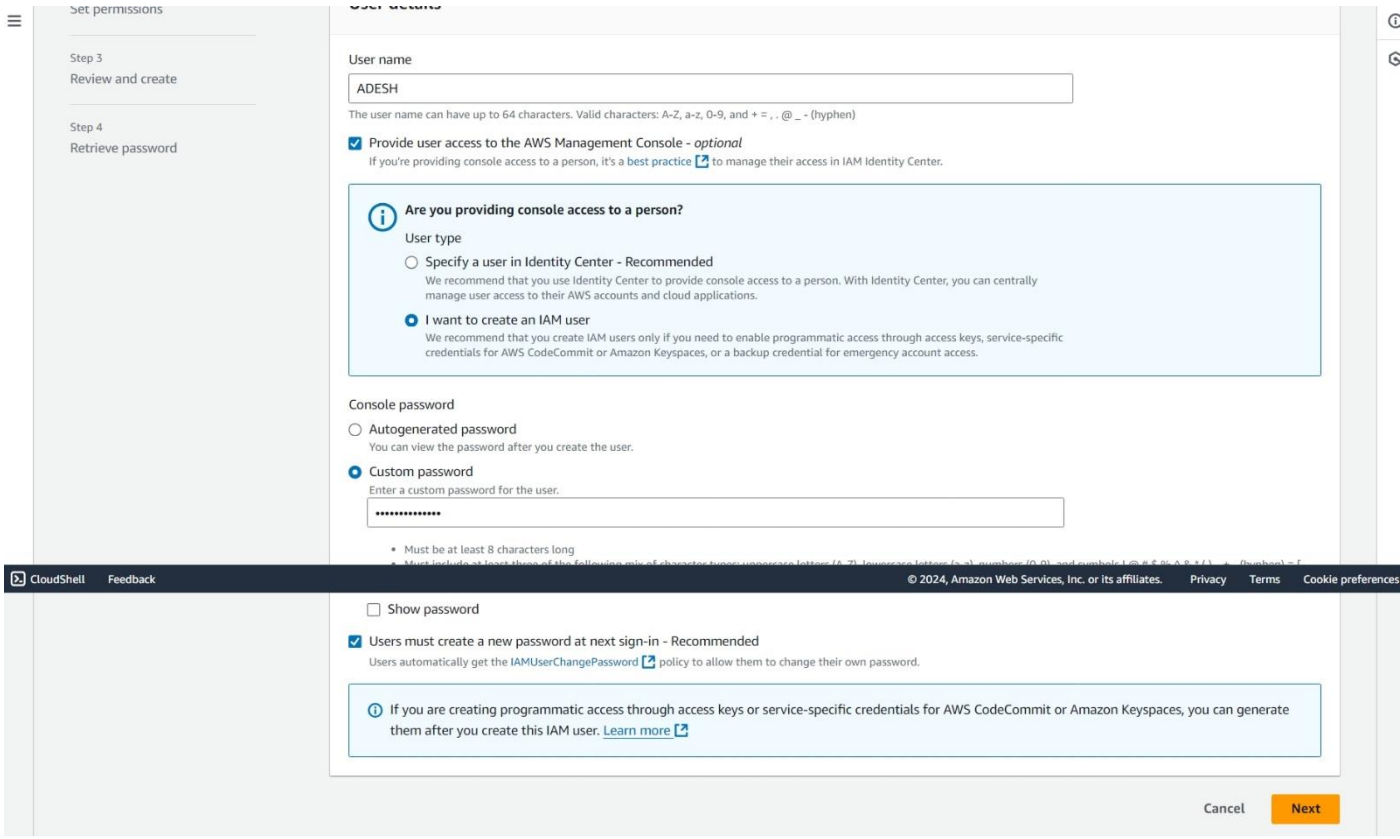
- Login credintial

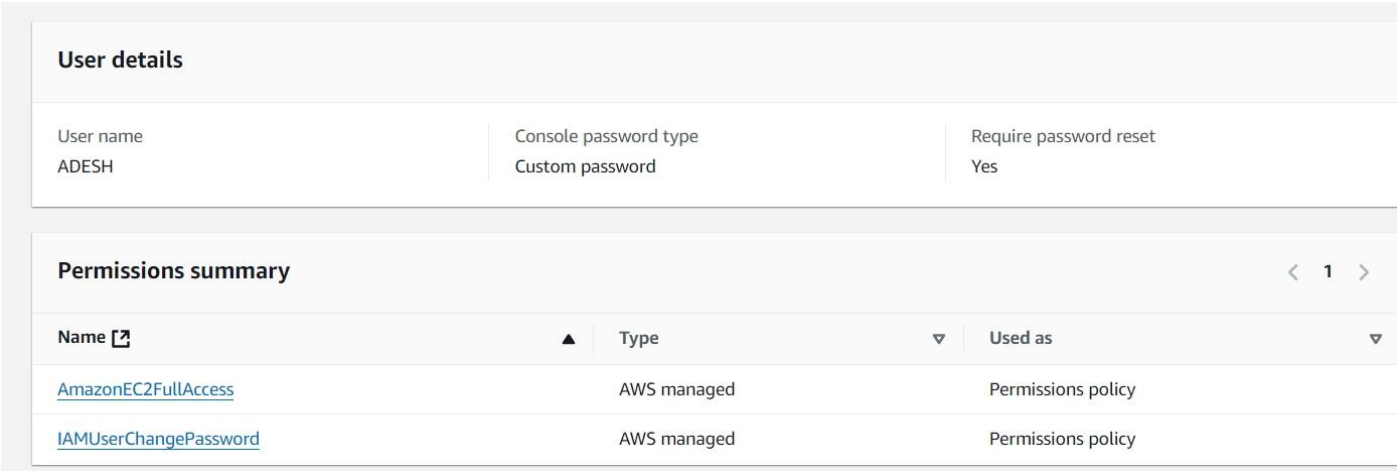


- IAM DASHBOARD

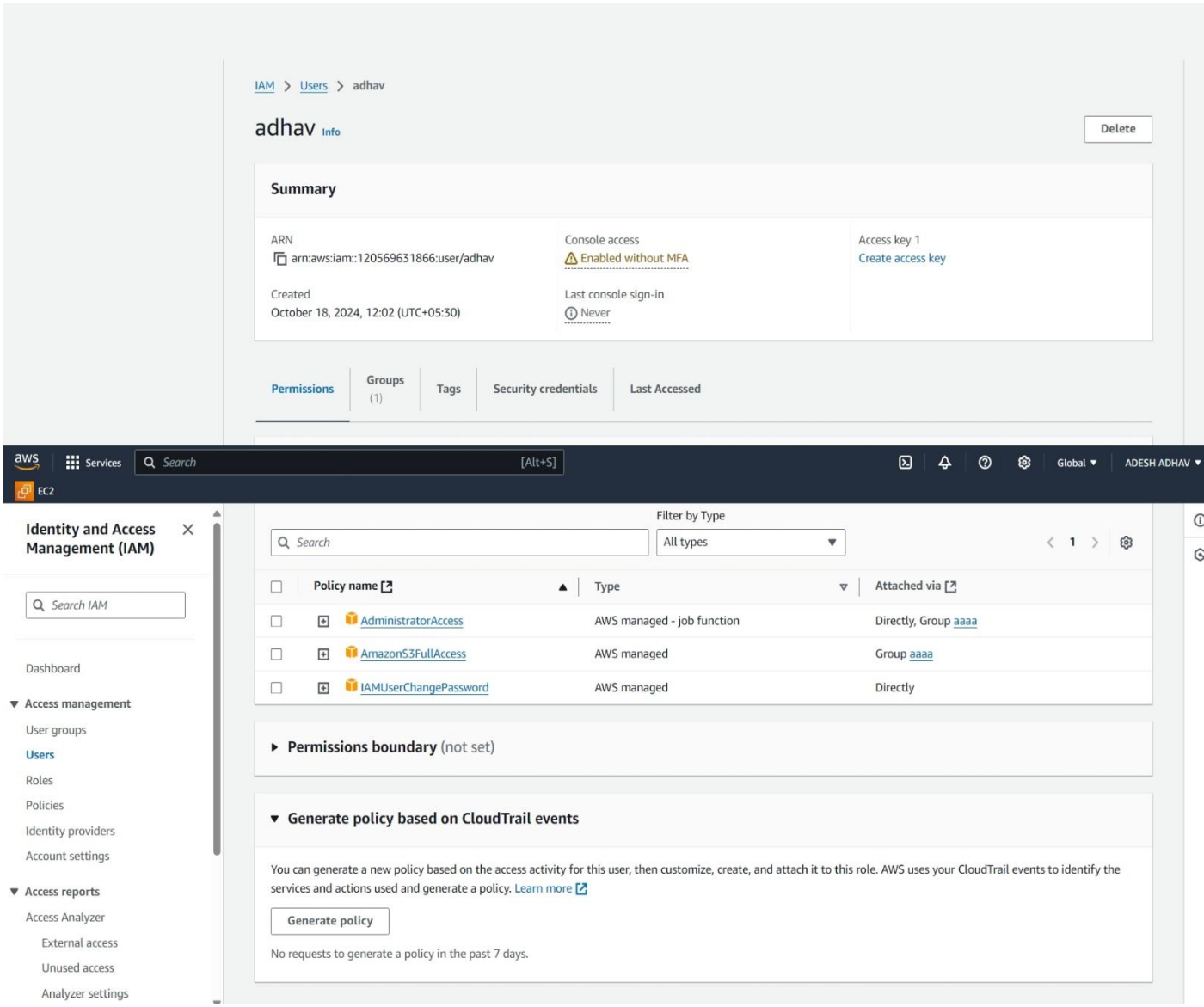


- CREATE USER

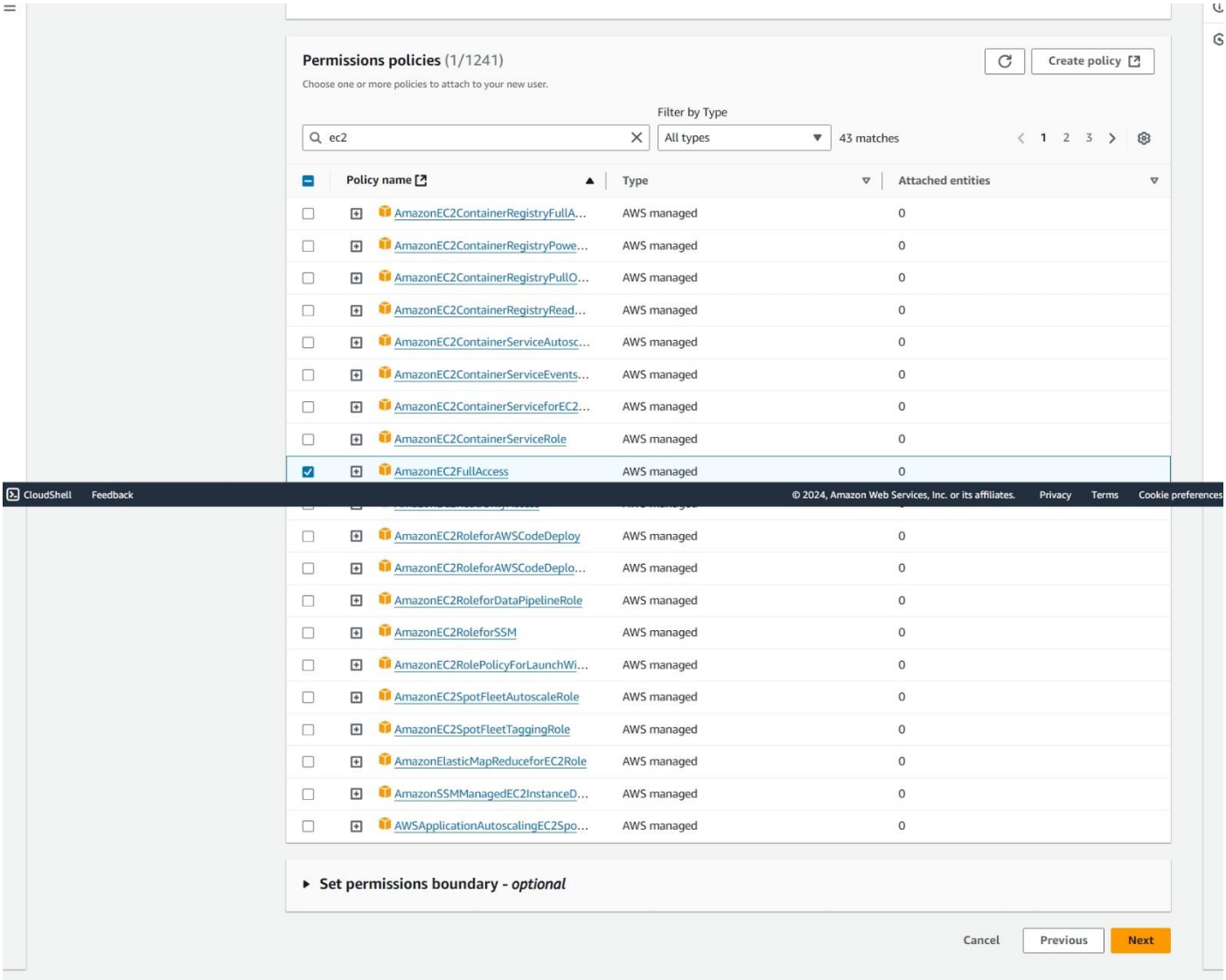

Set permissions
Step 3
Review and create
Step 4
Retrieve password
User name
ADESH
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a 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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
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

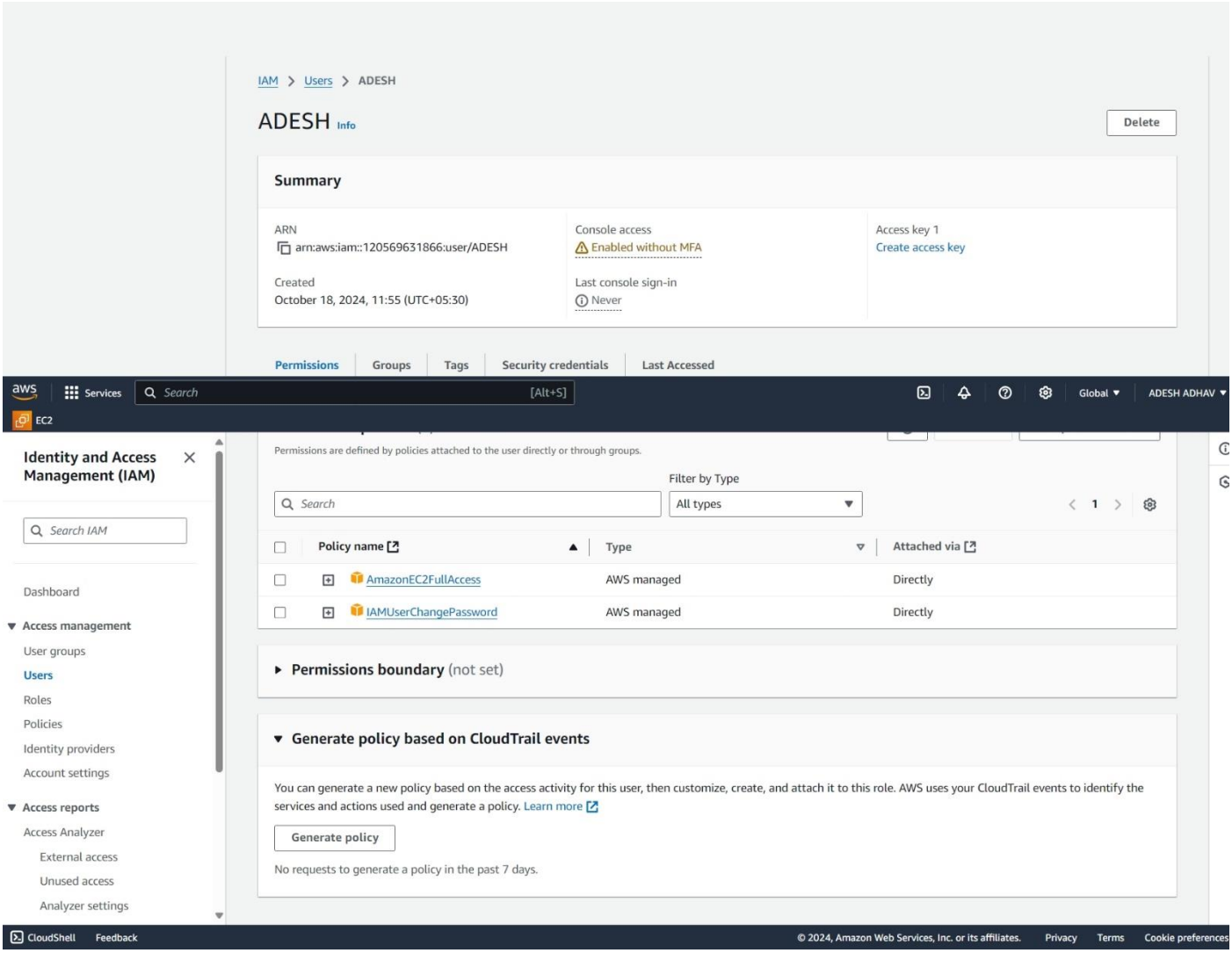

User details
User name
ADESH
Console password type
Custom password
Require password reset
Yes
Permissions summary
1
Name
Type
Used as
AmazonEC2FullAccess
AWS managed
Permissions policy
IAMUserChangePassword
AWS managed
Permissions policy

- **USER 2**

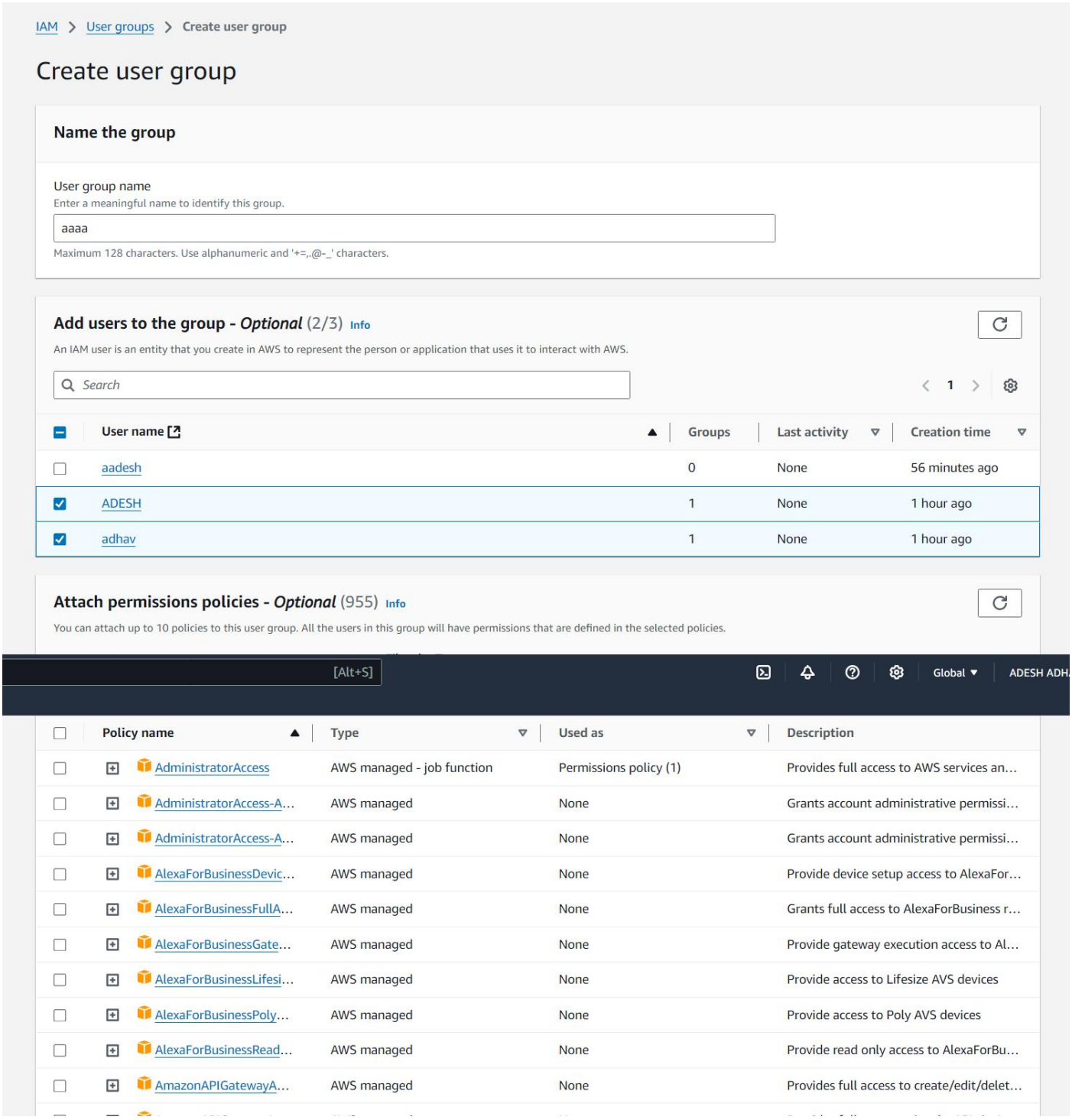

IAM > Users > adhav
adhav Info
Delete
Summary
ARN
arn:aws:iam::120569631866:user/adhav
Console access
Enabled without MFA
Access key 1
Create access key
Created
October 18, 2024, 12:02 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups (1)
Tags
Security credentials
Last Accessed
aws
Services
Search
[Alt+S]
Global
ADESH ADHAV
EC2
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
Search
All types
1
Policy name
Type
Attached via
AdministratorAccess
AWS managed - job function
Directly, Group aaaa
AmazonS3FullAccess
AWS managed
Group aaaa
IAMUserChangePassword
AWS managed
Directly
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
Generate policy
No requests to generate a policy in the past 7 days.

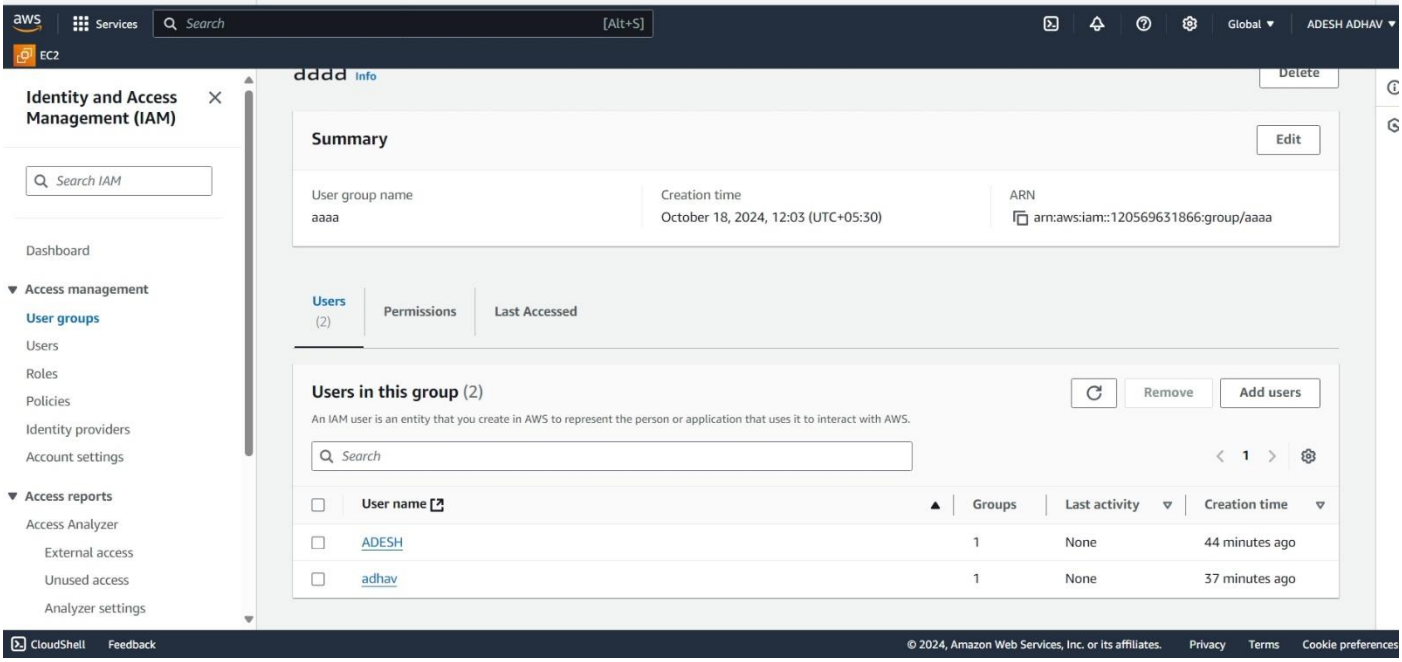
- PERMISSION TO THE USER

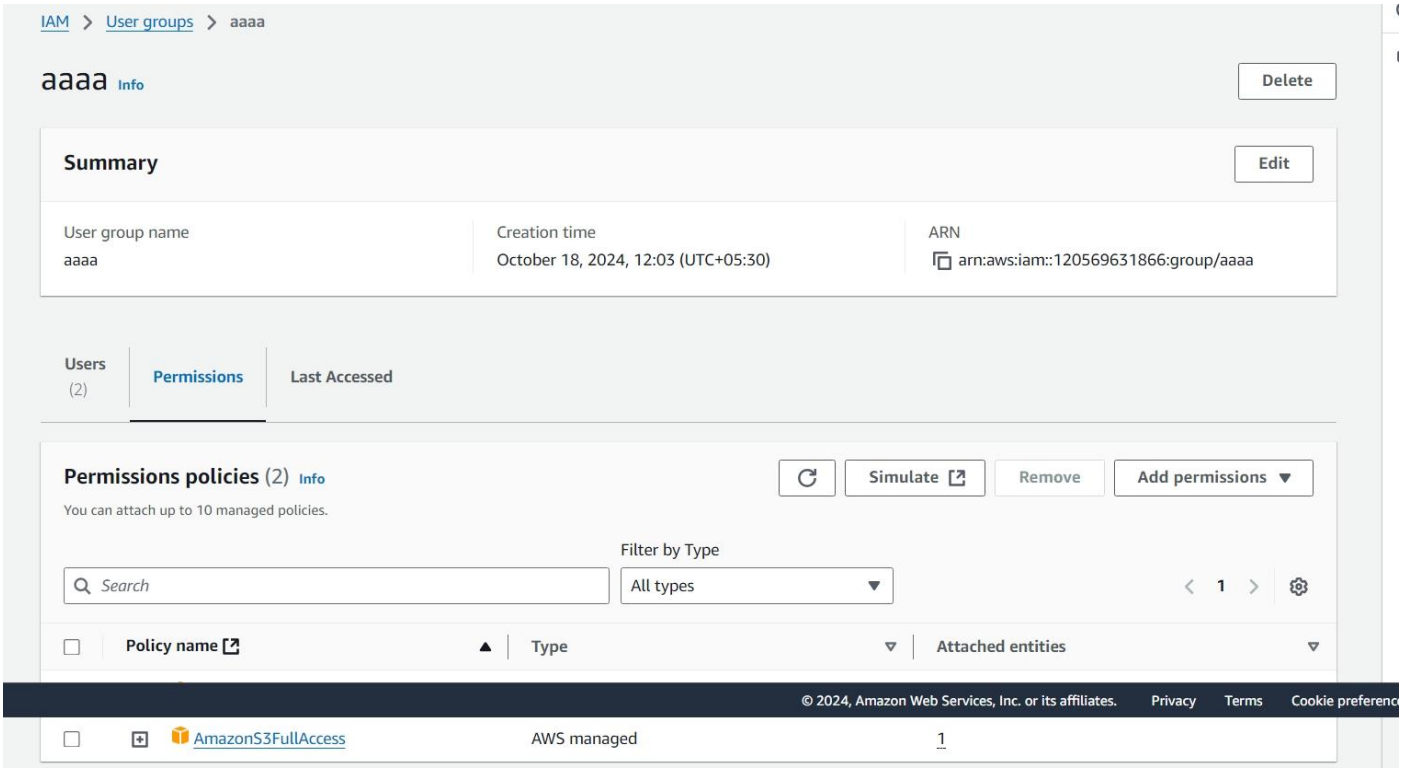



IAM > Users > ADESH
ADESH Info
Delete
Summary
ARN
arn:aws:iam::120569631866:user/ADESH
Console access
Enabled without MFA
Access key 1
Create access key
Created
October 18, 2024, 11:55 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Last Accessed
aws
Services
Search
[Alt+S]
Global
ADESH ADHAV
EC2
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
Permissions are defined by policies attached to the user directly or through groups.
Filter by Type
Search
All types
1
Policy name
Type
Attached via
AmazonEC2FullAccess
AWS managed
Directly
IAMUserChangePassword
AWS managed
Directly
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
Generate policy
No requests to generate a policy in the past 7 days.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

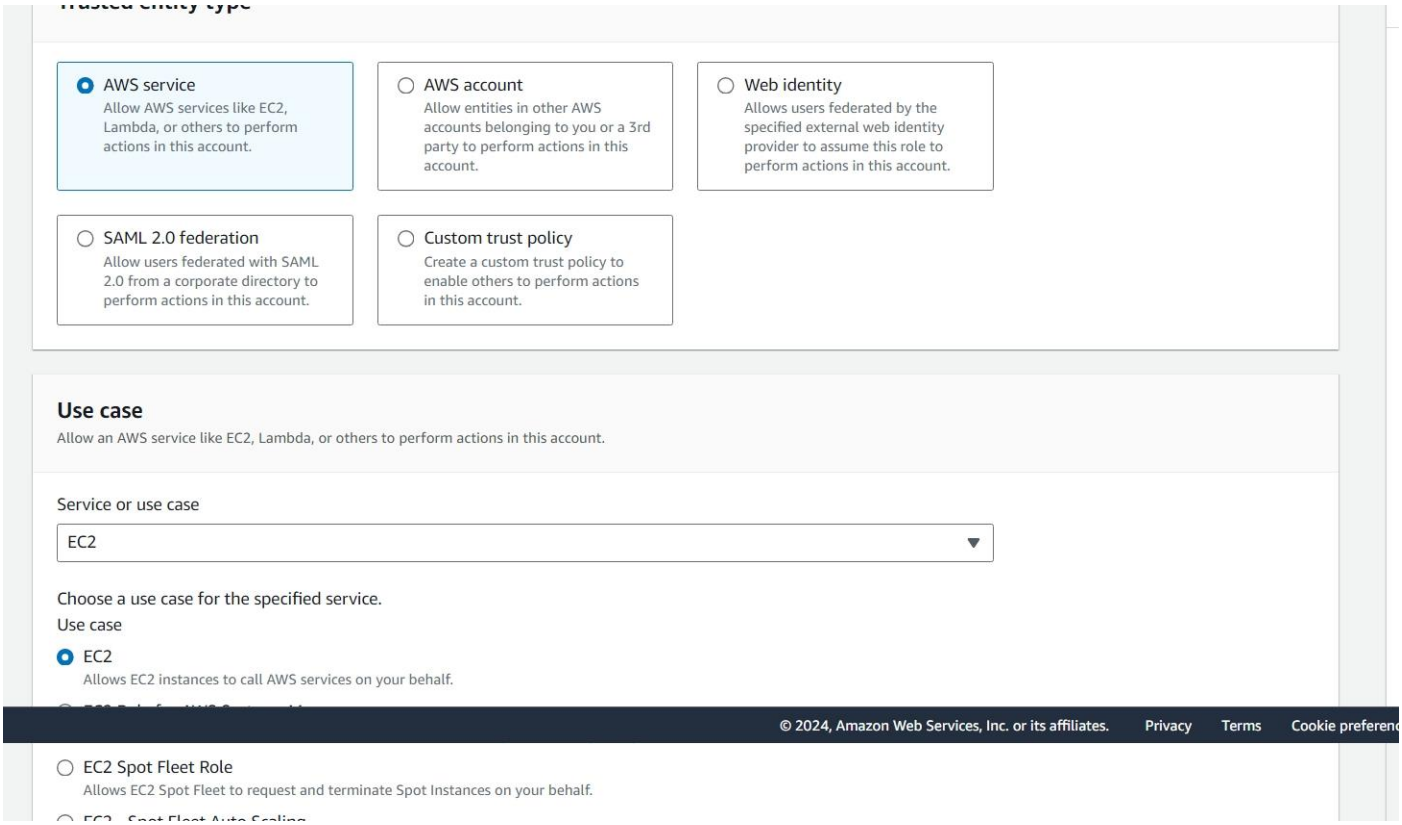
- CREATE GROUP

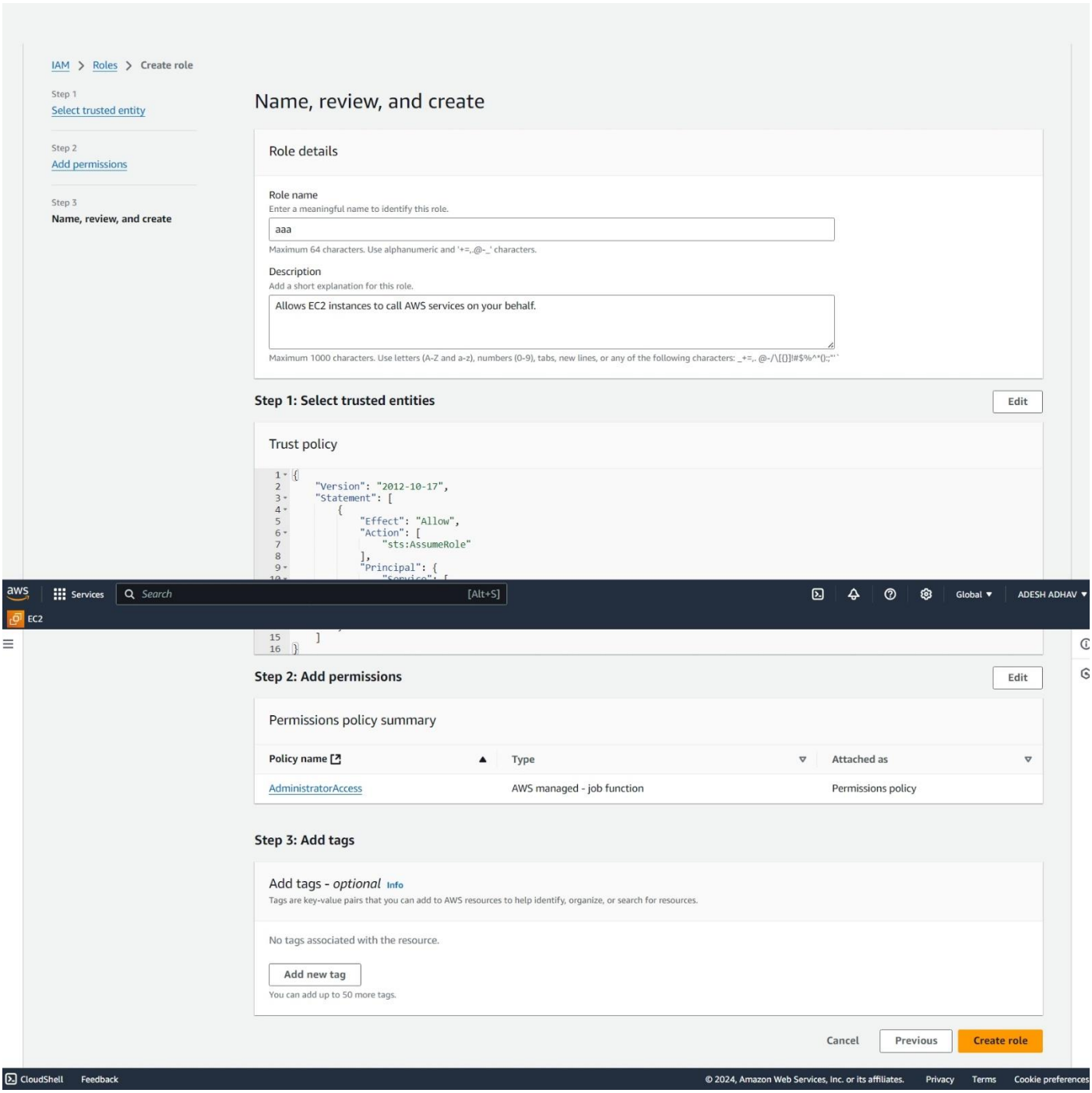



Services
Search
[Alt+S]
Global
ADESH ADHAV
EC2
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
dddd Info
Delete
Summary
Edit
User group name
aaaa
Creation time
October 18, 2024, 12:03 (UTC+05:30)
ARN
arn:aws:iam::120569631866:group/aaaa
Users (2)
Permissions
Last Accessed
Users in this group (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.
Remove
Add users
Search
User name
Groups
Last activity
Creation time
ADESH
1
None
44 minutes ago
adhav
1
None
37 minutes ago
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


IAM > User groups > aaaa
aaaa Info
Delete
Summary
Edit
User group name
aaaa
Creation time
October 18, 2024, 12:03 (UTC+05:30)
ARN
arn:aws:iam::120569631866:group/aaaa
Users (2)
Permissions
Last Accessed
Permissions policies (2) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter by Type
Search
All types
Policy name
Type
Attached entities
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
AmazonS3FullAccess
AWS managed
1

- ROLE




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.
aaa
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^*();"'`
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"sts:AssumeRole"
],
"Principal": {
]
}
aws
Services
Search
[Alt+S]
Global
ADESH ADHAV
EC2
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
AdministratorAccess
AWS managed - job function
Permissions policy
Step 3: Add tags
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 role
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

THANK YOU