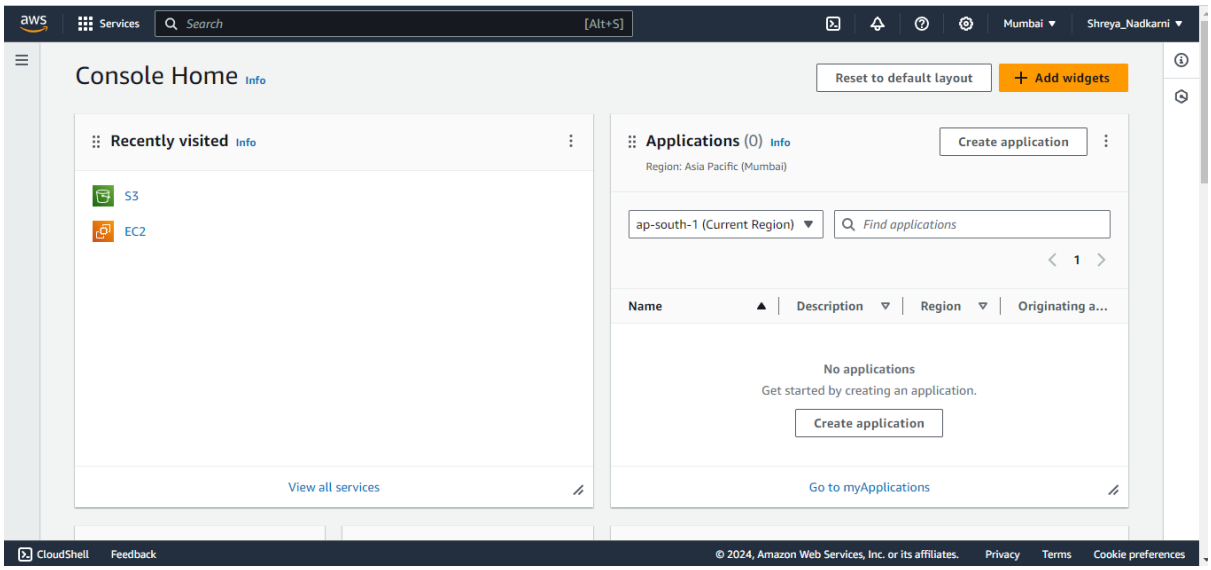
SVKM'S NMIMS Nilkamal School of Mathematics, Applied Statistics & Analytics Master of Science (Statistics & Data Science)

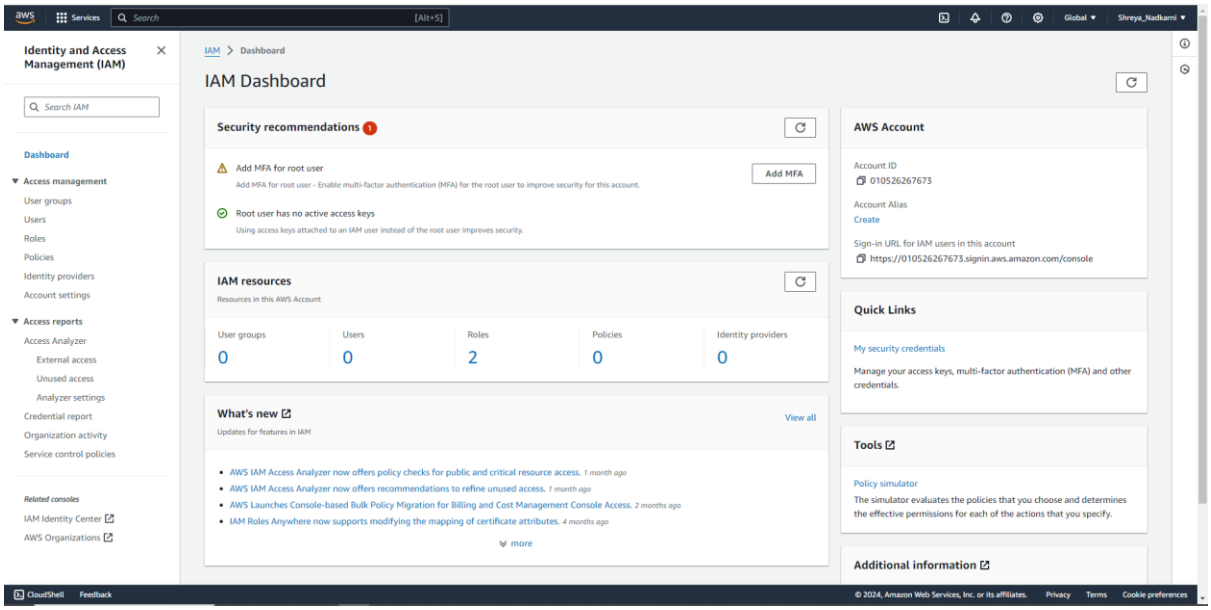
Practical-3 Identity Access Management.

Name: Shreya Nadkarni
SAP ID: 86062300047
Roll No: A042

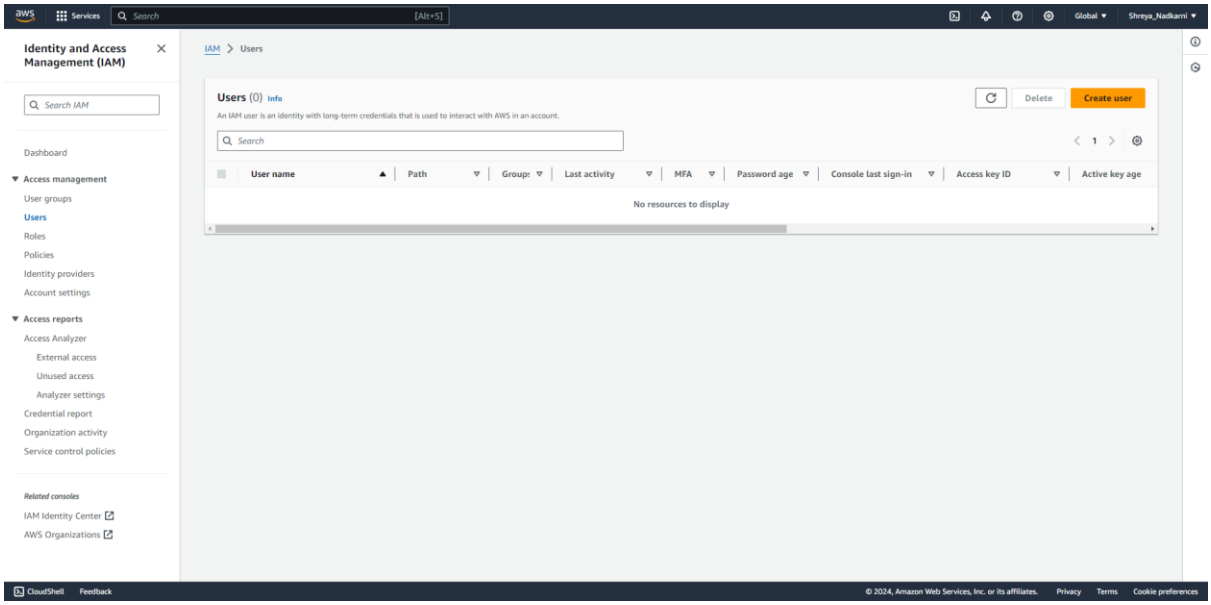
Q1. Create and Implement policies IAM user for accessing any 4 services from the aws user and group.

Sign in to the AWS Management Console and navigate to the IAM service by searching for "IAM" in the search bar.

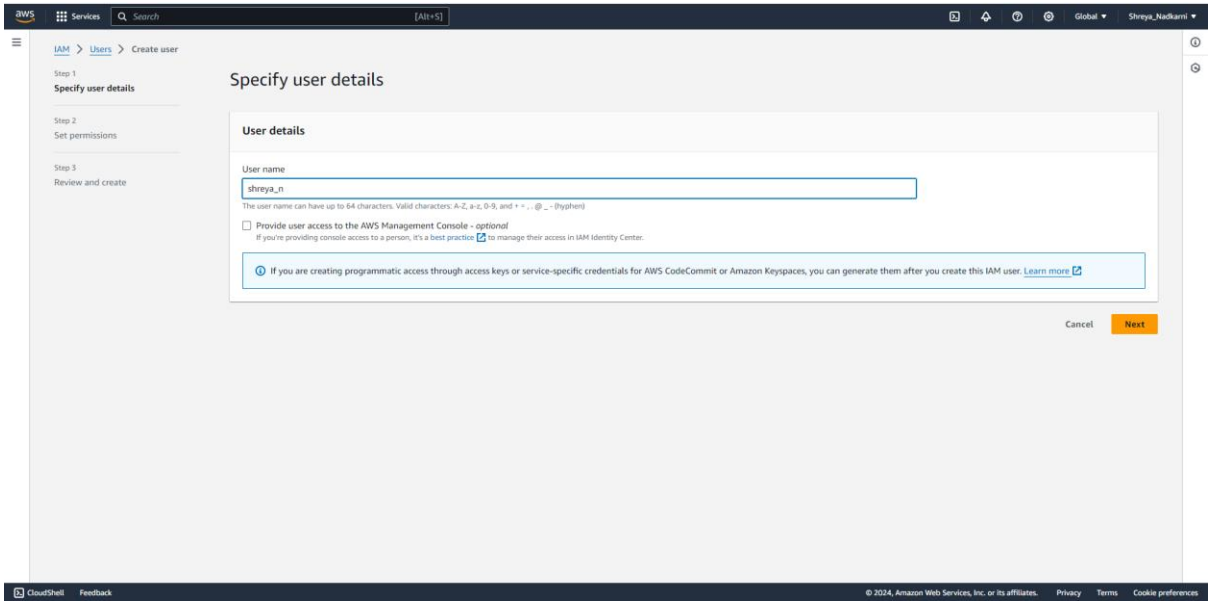




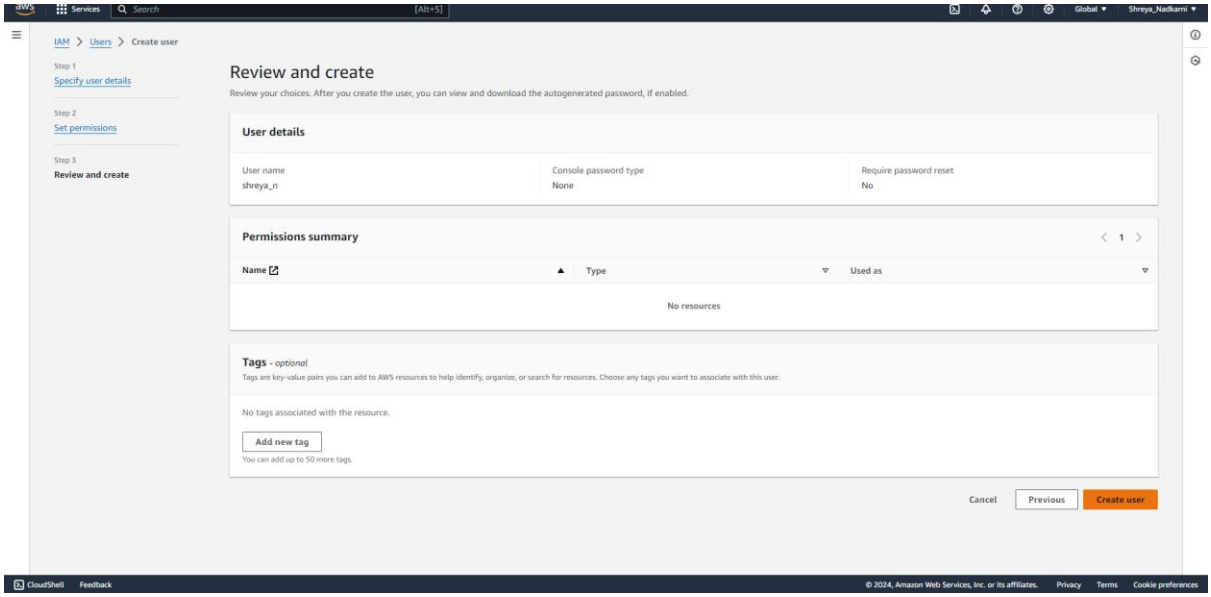
Click on "Users" in the left-hand menu under IAM. Click on the "create user" button.



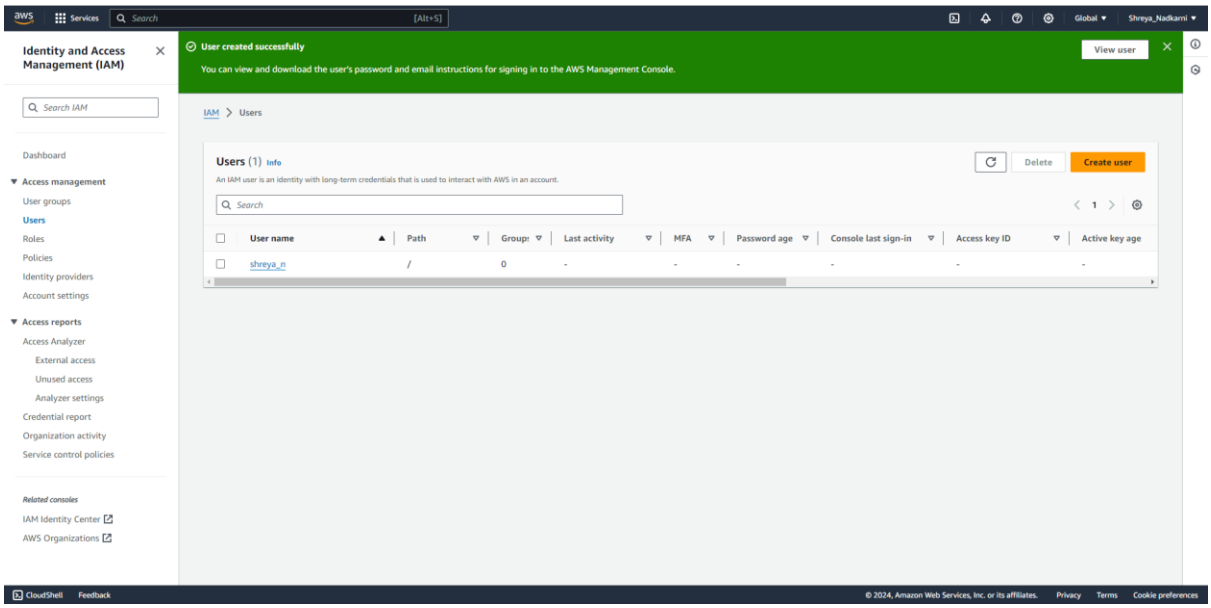
Enter a username for the new IAM user.



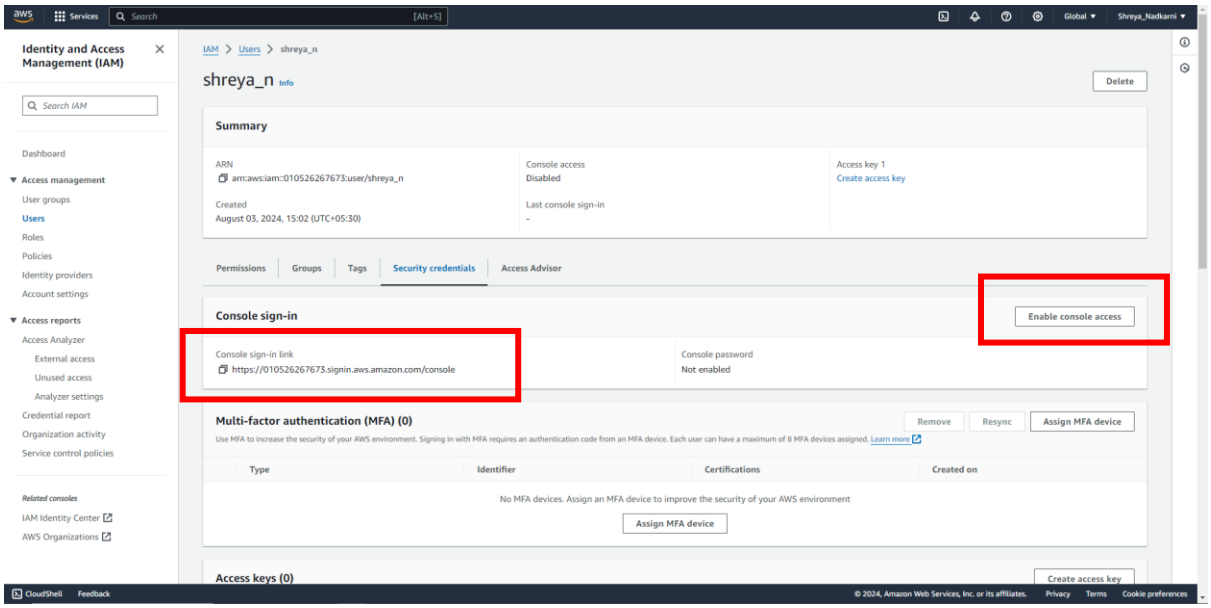
Review the user details and permissions. Click "Create user" to finish creating the IAM user.

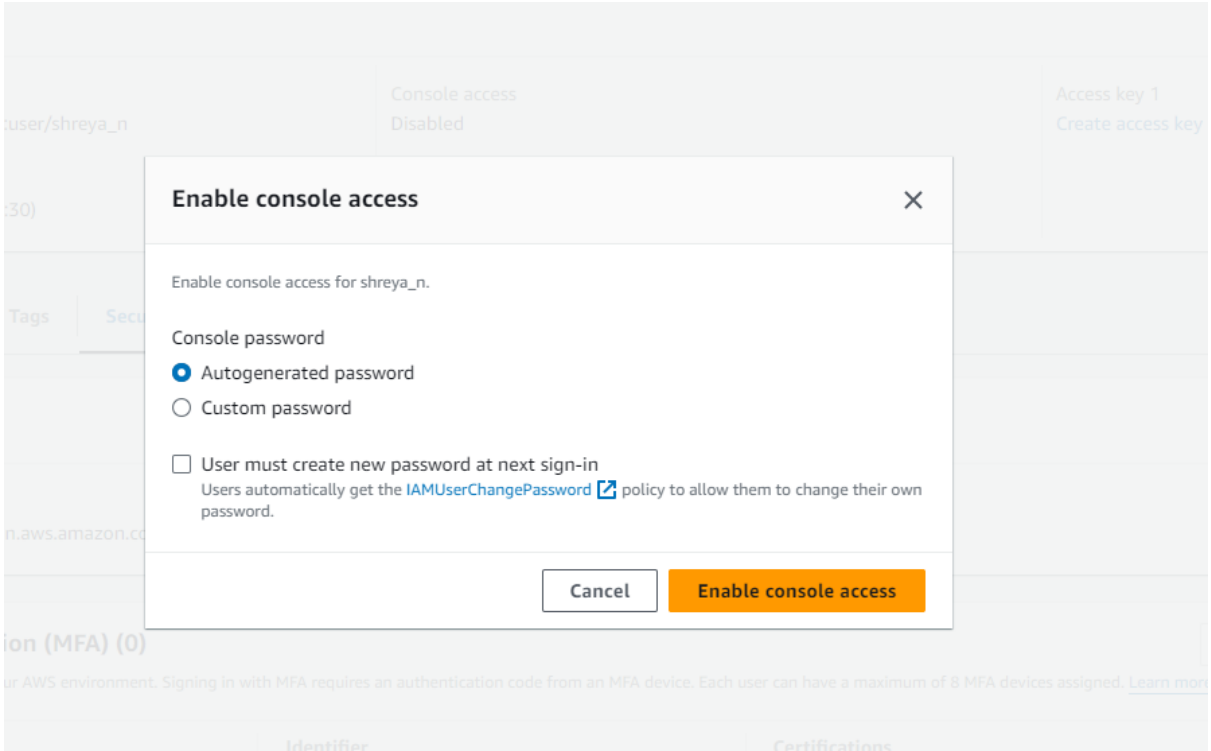


Boom! new user is created

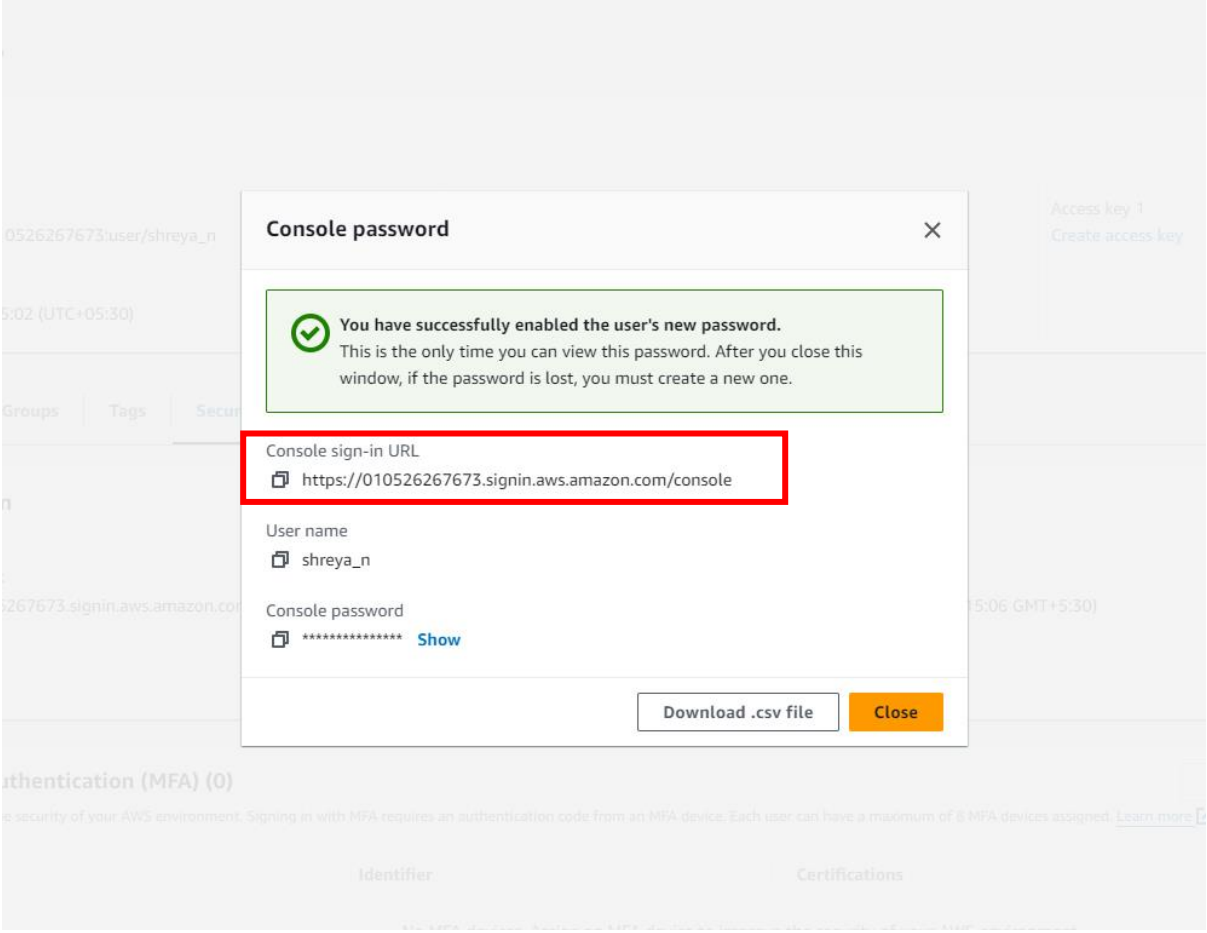


Click on “enable console access”, this will provide with access credentials (Access Key ID and Secret Access Key) for programmatic access. Make sure to save these securely.

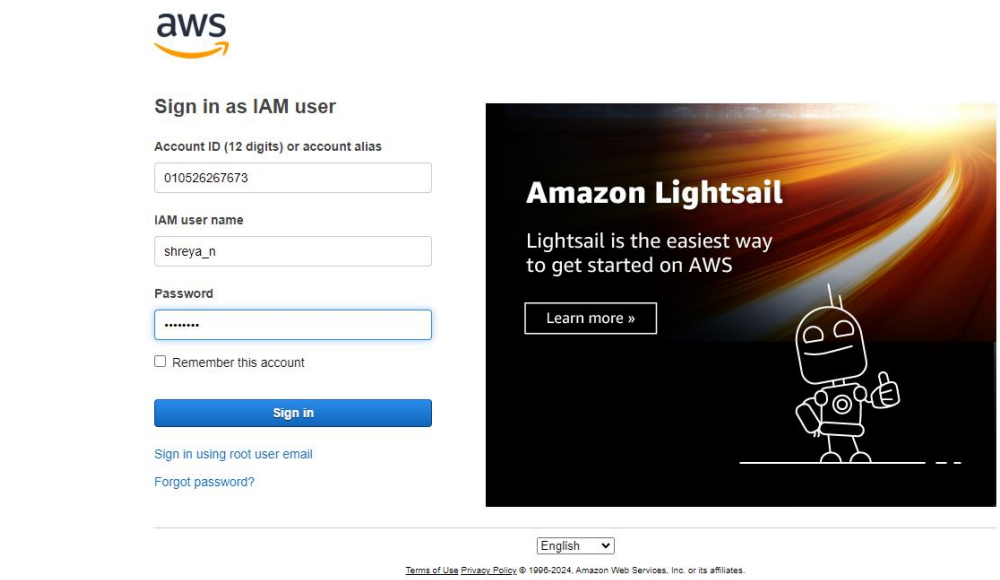




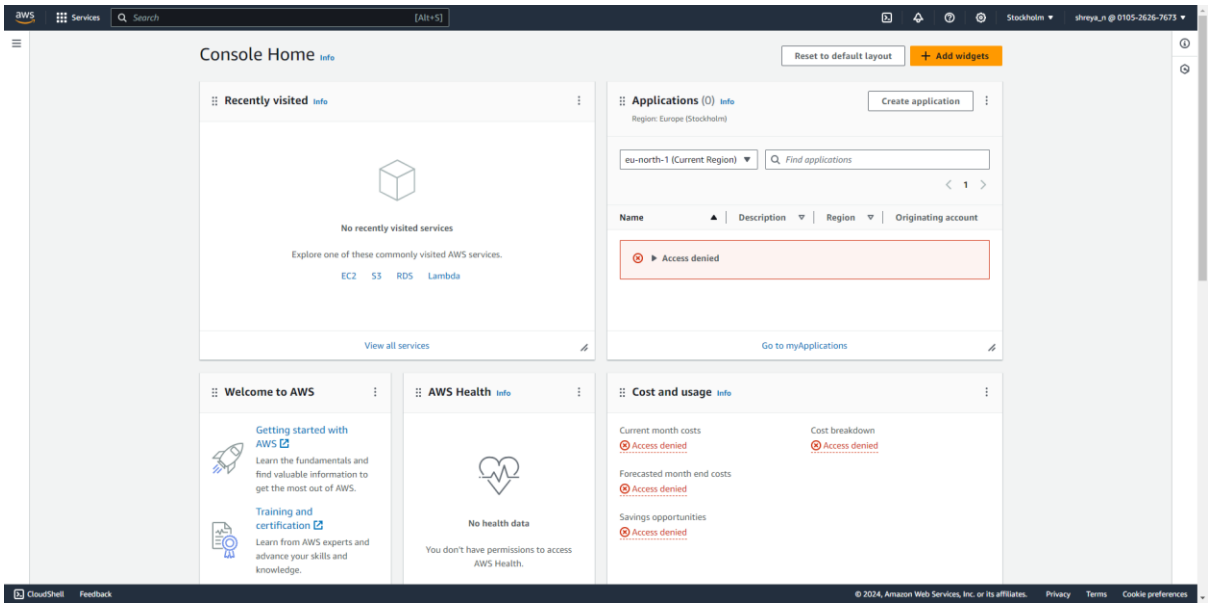
Copy the console sign-in link.



Use the IAM user credentials to verify access to the AWS services specified in the policy. Ensure that the user/group can perform the allowed actions and is restricted from actions not specified in the policy. Open new incognito tab in browser and paste the copied console sign-in URL. And login with the IAM user's User name and password.

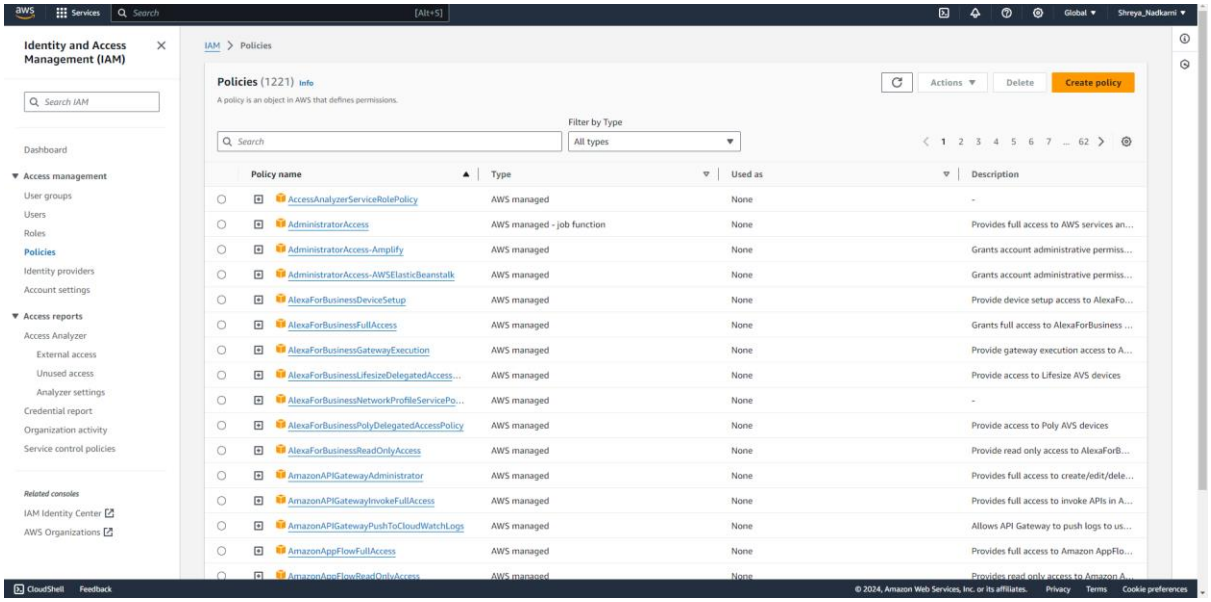


After logging in to IAM User account, the following window opens and shows the AWS Management Console with access denied messages, indicating that the user does not have the necessary permissions to view or access specific resources or services.



Follow these Steps for Creating and Implementing Policies for Accessing AWS Services:

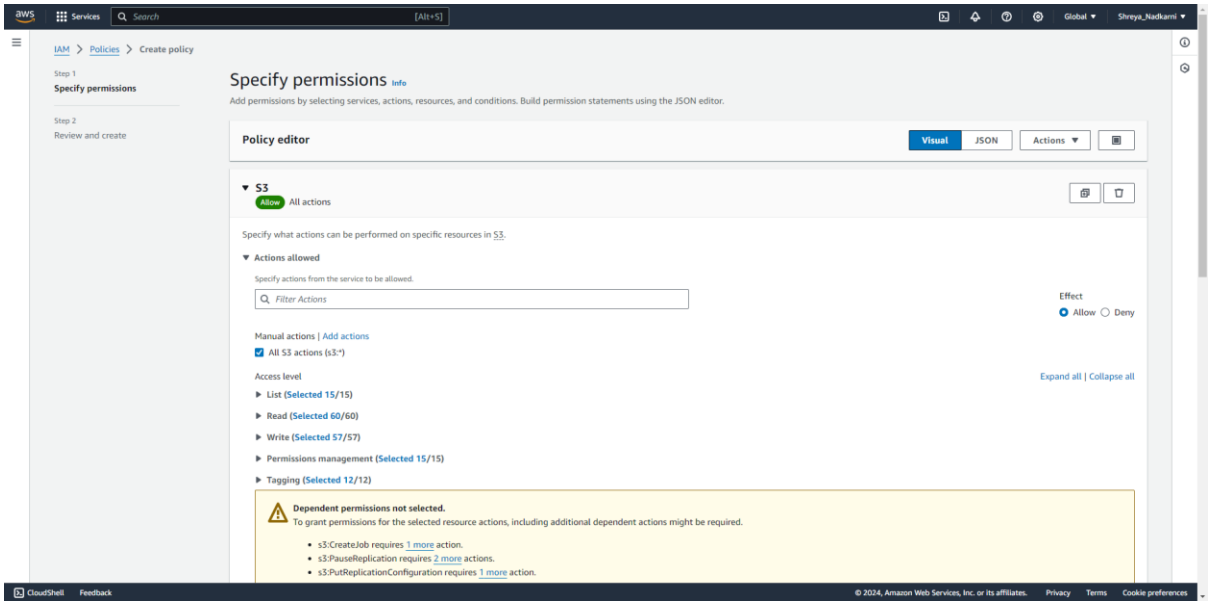
Navigate to IAM > Policies > Create policy.



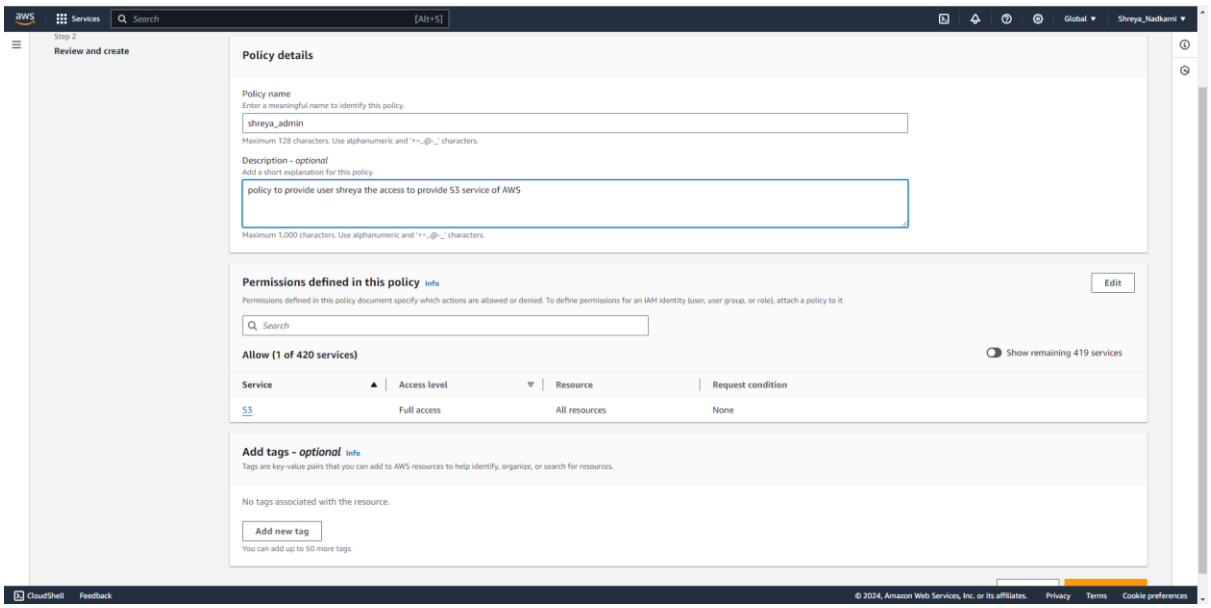
Choose "JSON" as the policy language and define the policy document. Here’s an example for accessing four AWS services.

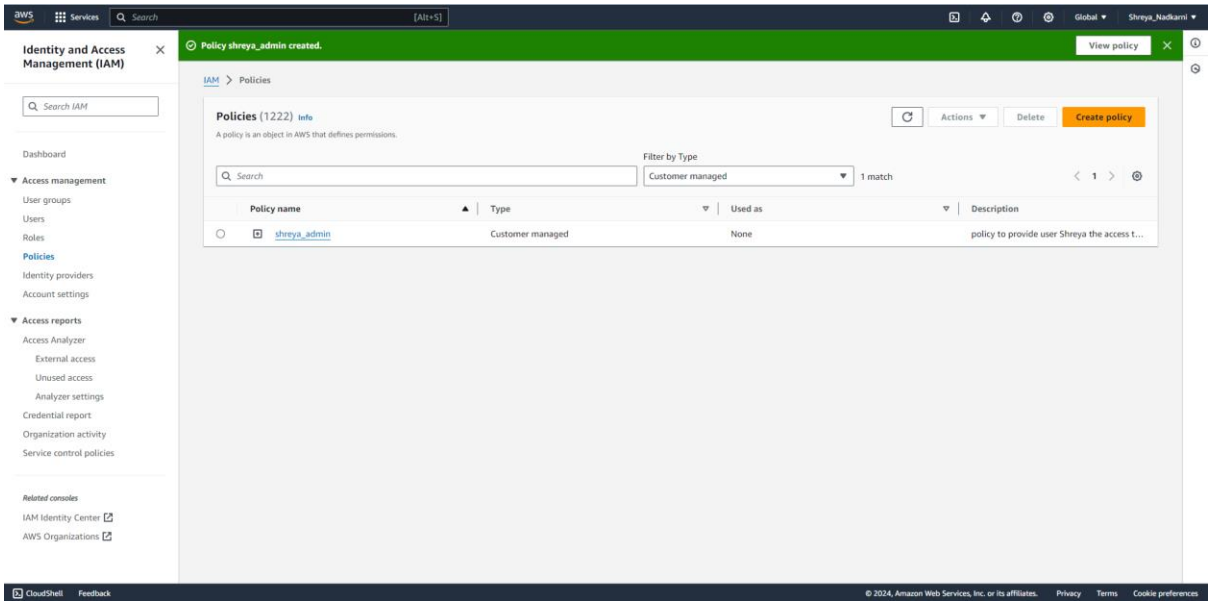
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:*",
                "ec2:*",
                "rds:*",
                "lambda:*"
            ],
            "Resource": "*"
        }
    ]
```

Adjust the actions and resources as per your specific requirements and best practices.

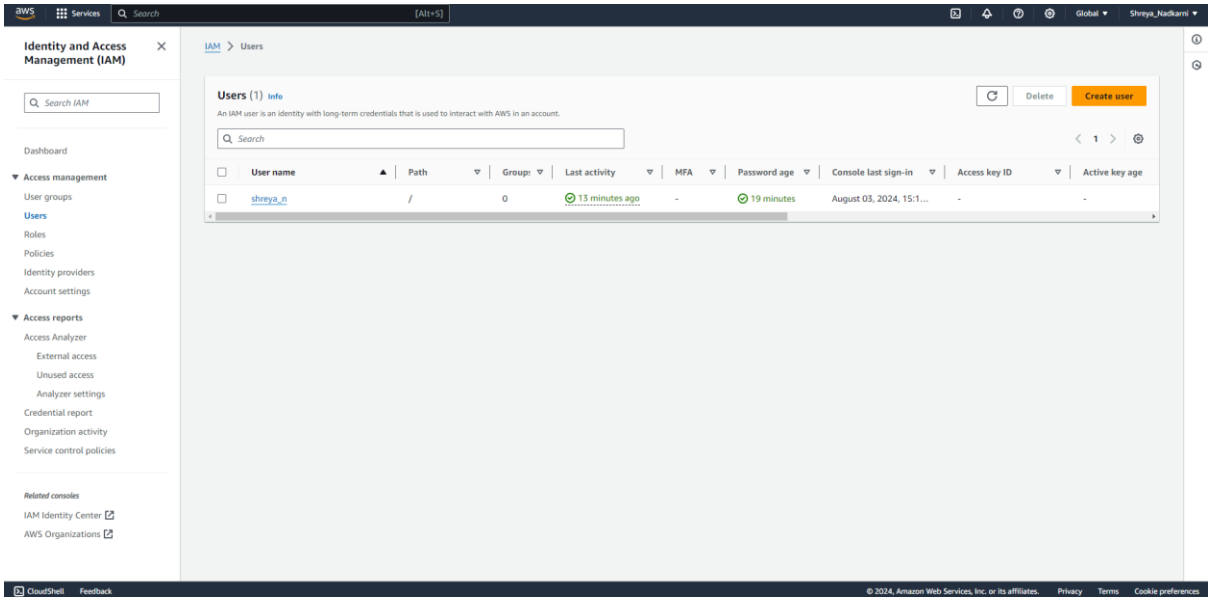


Provide appropriate policy details and click on the “create policy”.

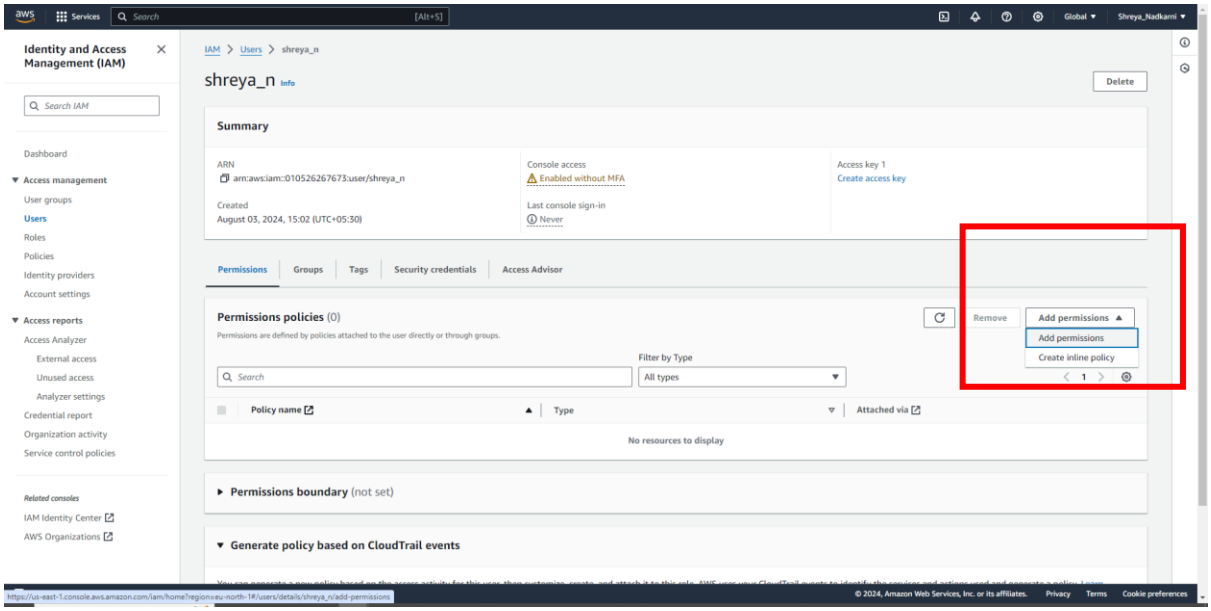




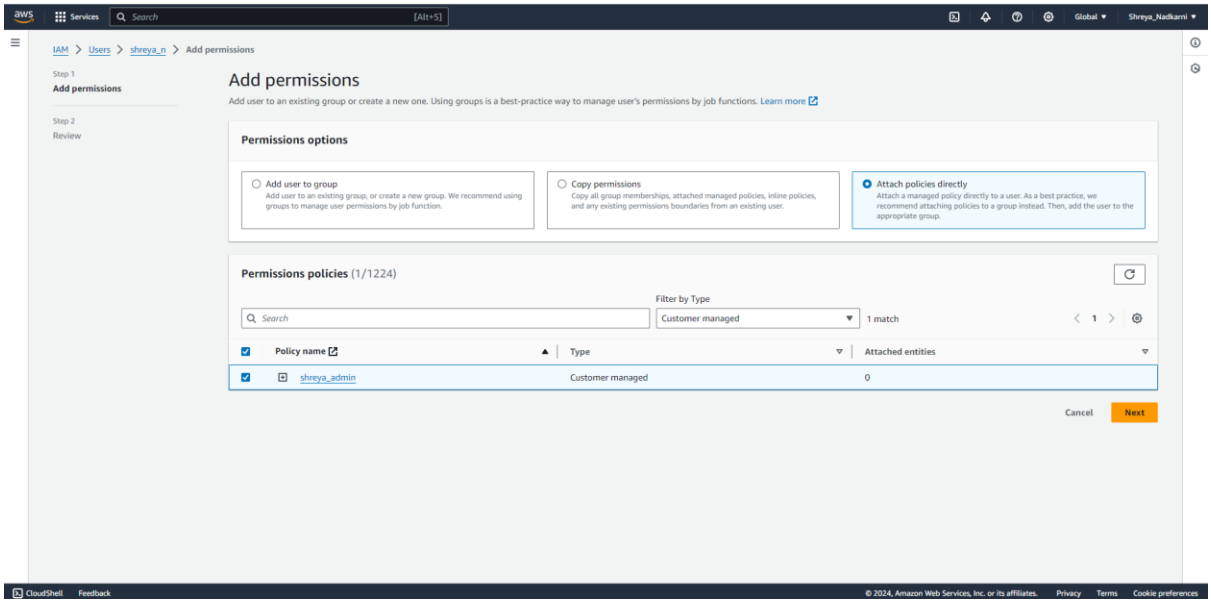
Once the policy is created, navigate to IAM > Users or IAM and Select the IAM user to which you want to attach the policy.

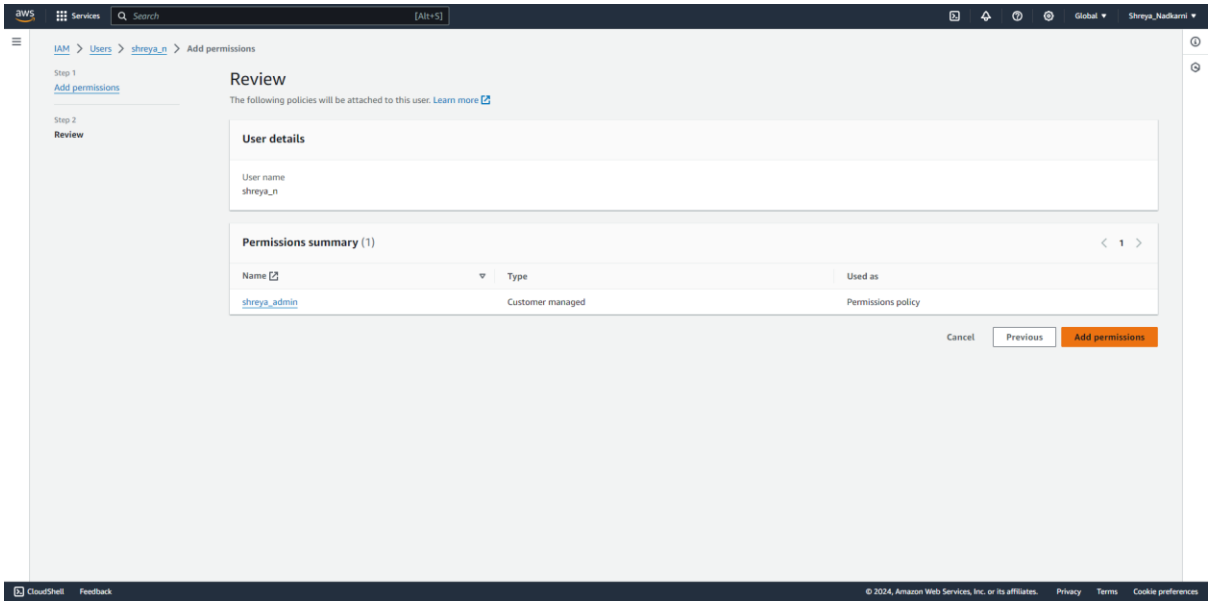


In the permissions tab, click "Add permissions" or "Attach policies".

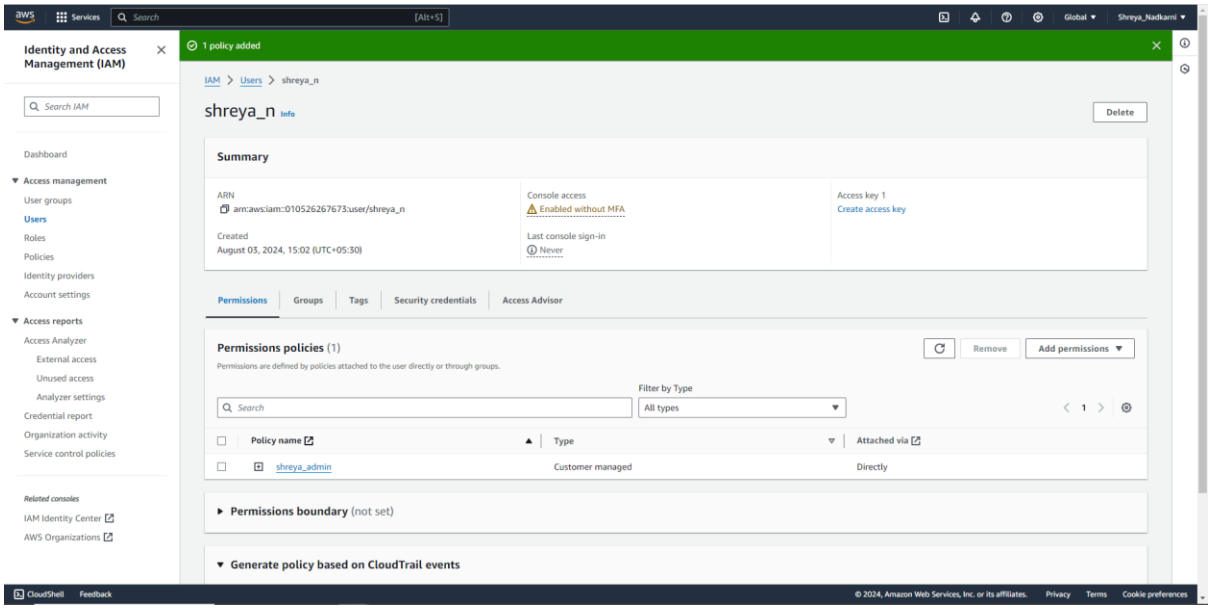


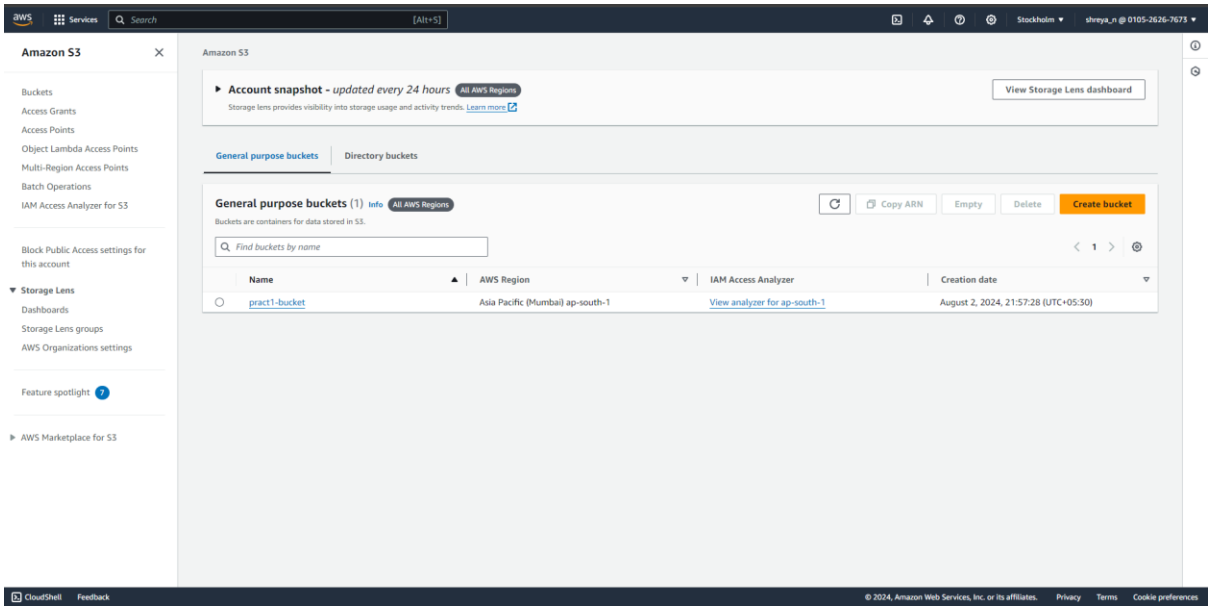
Search for and select the policy you created. Click "Add permissions" to assign the policy.

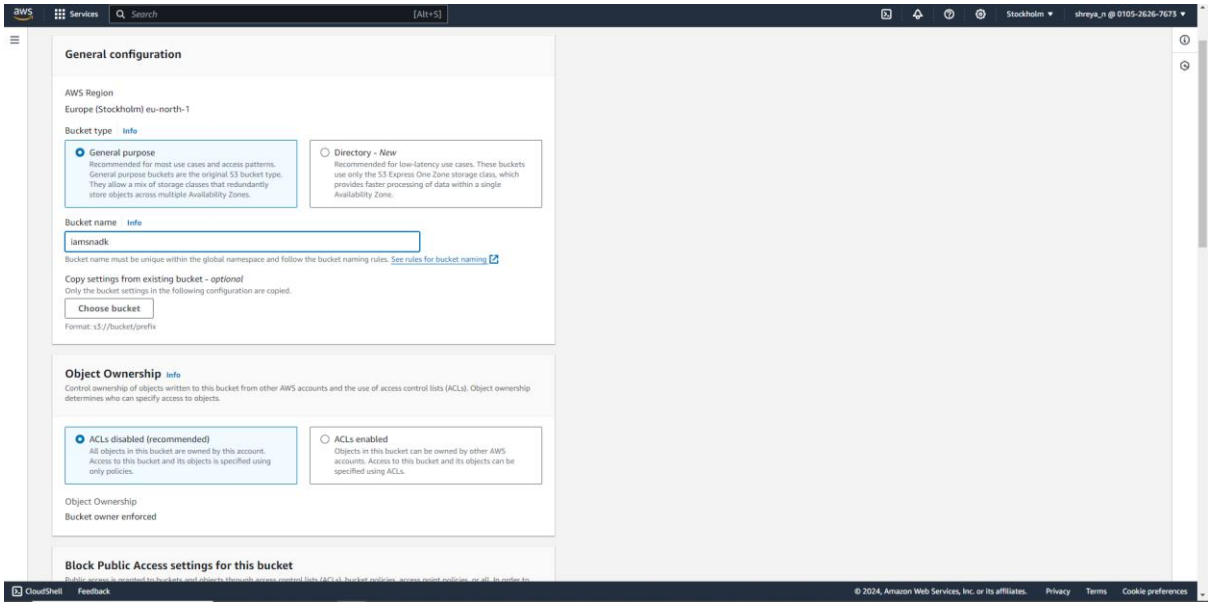




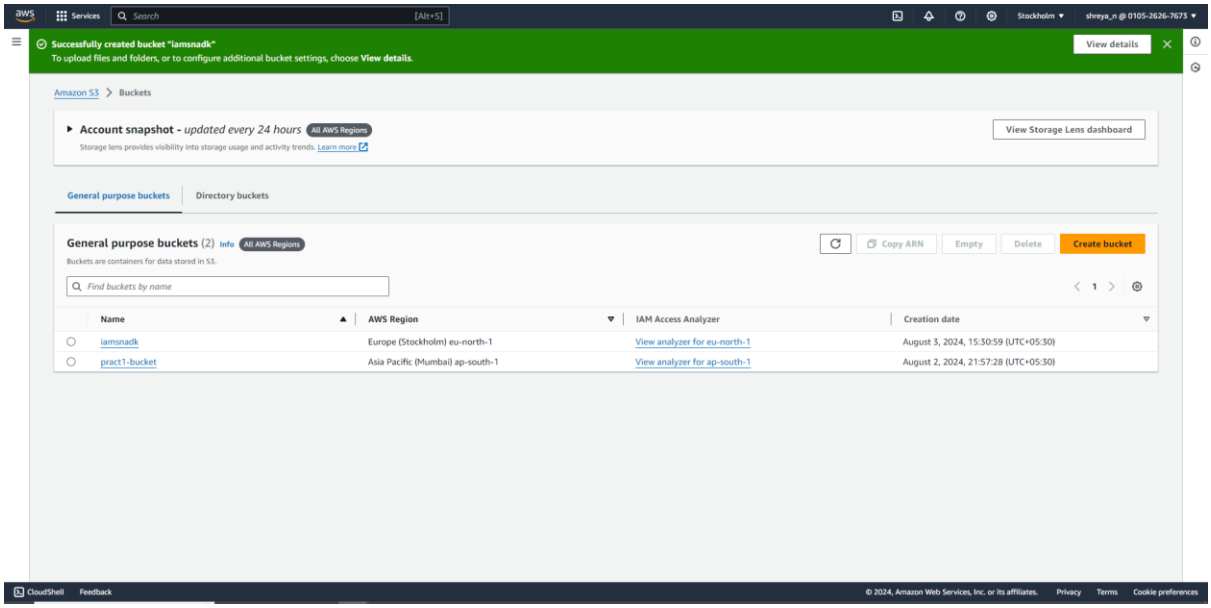
Navigate to IAM user account opened in the incognito mode and ensure that the user can perform the allowed S3 actions.




Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3
Account snapshot - updated every 24 hours
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1)
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
pract1-bucket
Asia Pacific (Mumbai) ap-south-1
View analyzer for ap-south-1
August 2, 2024, 21:57:28 (UTC+05:30)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

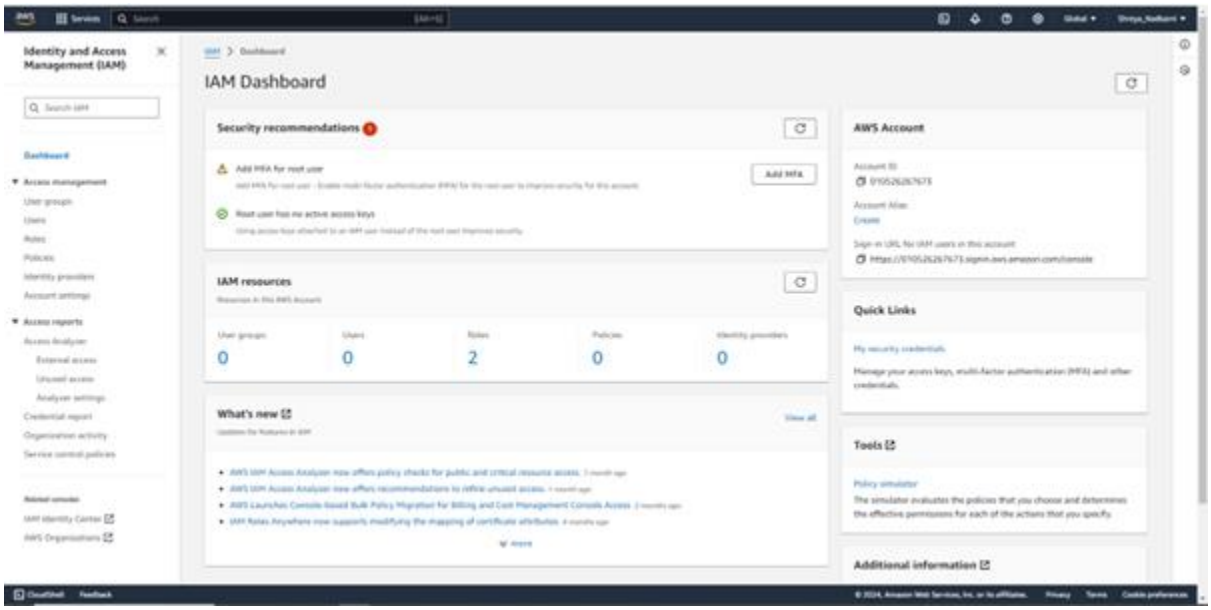

General configuration
AWS Region
Europe (Stockholm) eu-north-1
Bucket type
General purpose
Directory - New
Bucket name
iamsnadk
Copy settings from existing bucket - optional
Choose bucket
Object Ownership
ACLs disabled (recommended)
ACLs enabled
Object Ownership
Bucket owner enforced
Block Public Access settings for this bucket
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Boom! IAM user is able to perform the allowed S3 actions.



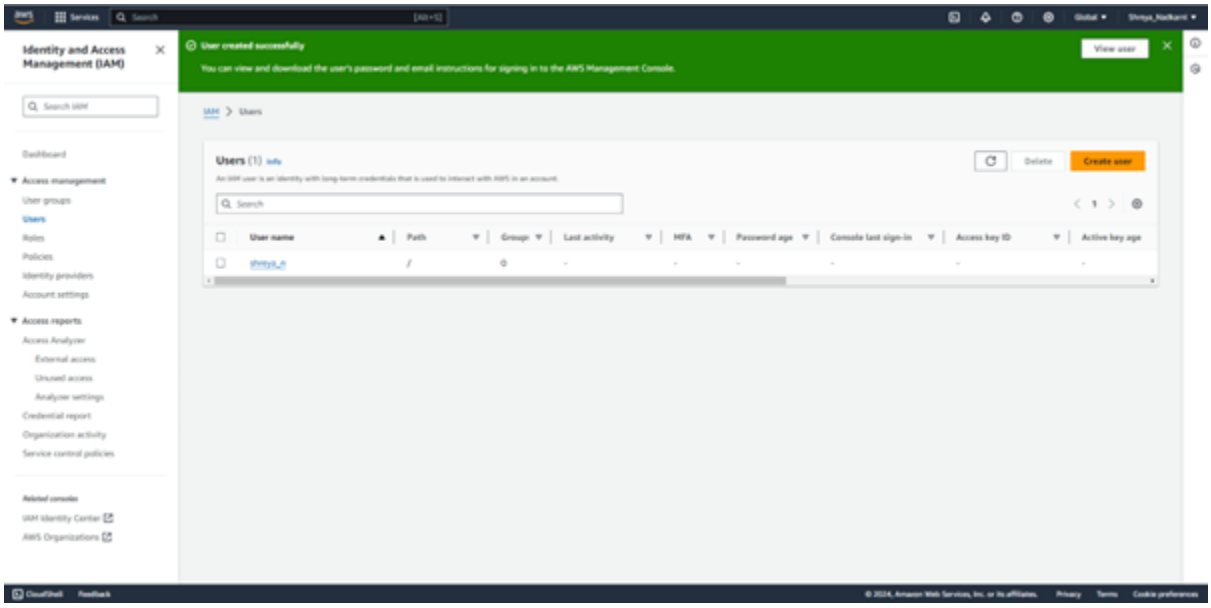
Steps to Attach the EC2 Policy to an IAM User:

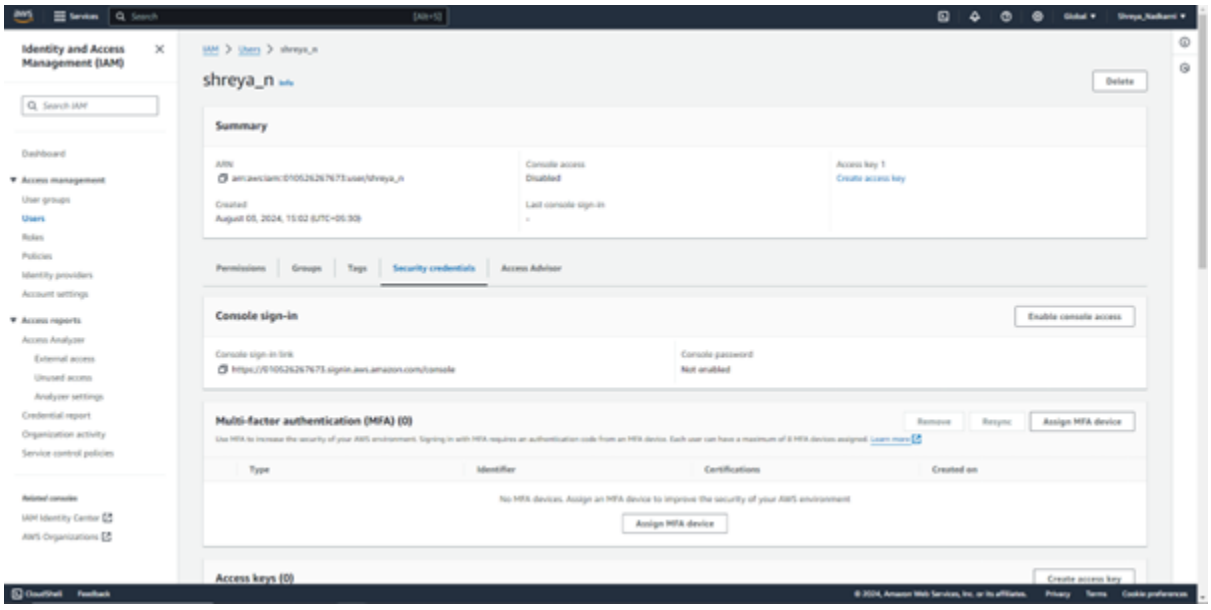
Sign in to the AWS Management Console and navigate to the IAM service by searching for "IAM" in the search bar.



In the IAM dashboard, click on "Users" in the left-hand menu.

From the list of users, select the IAM user to whom you want to attach the EC2 policy.



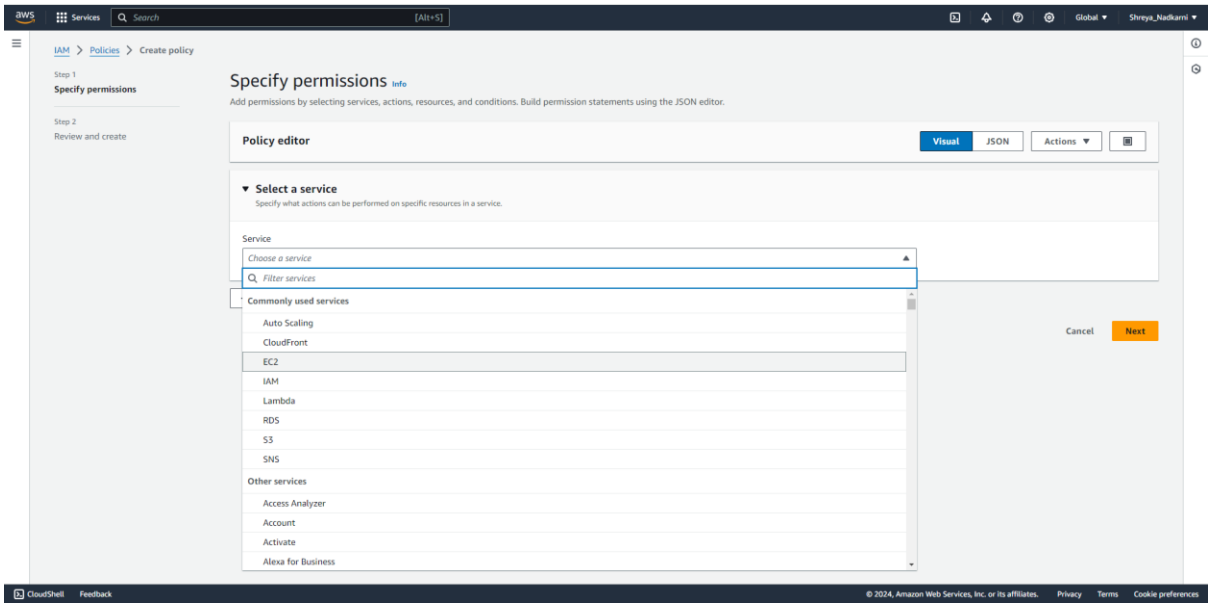


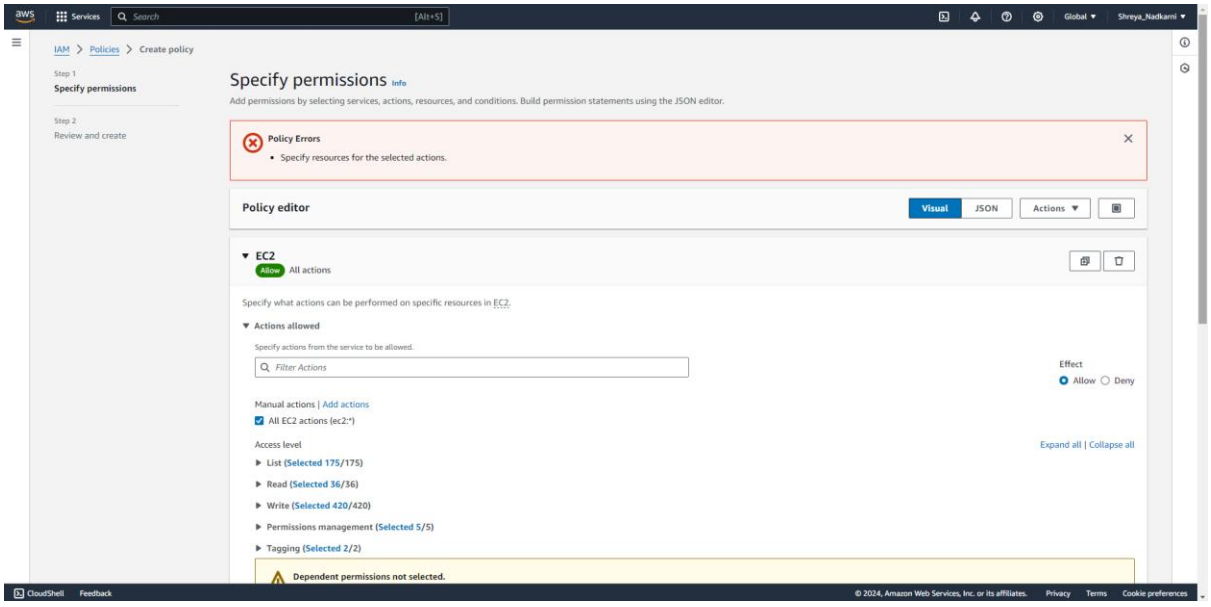
In the "Add permissions" wizard, choose "Attach policies directly" to assign policies directly to the user.

In the search bar, type "EC2" to filter the available policies related to Amazon EC2.

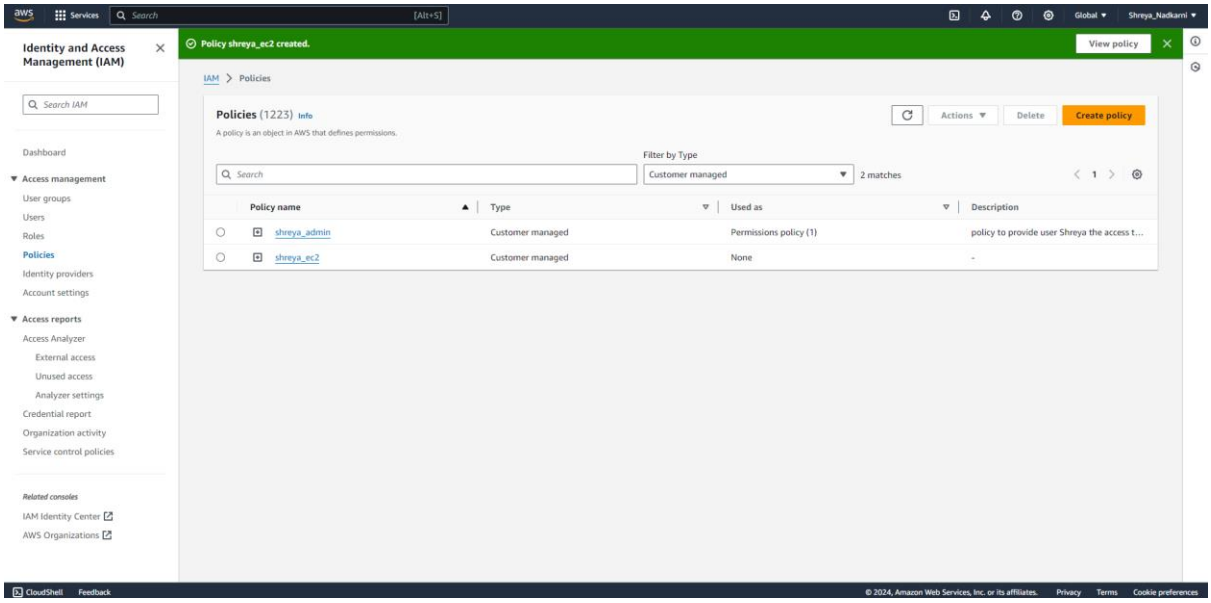
Select the **AmazonEC2FullAccess** policy from the list. This policy grants full access to Amazon EC2 resources.

After selecting the policy, click "Next: Review."

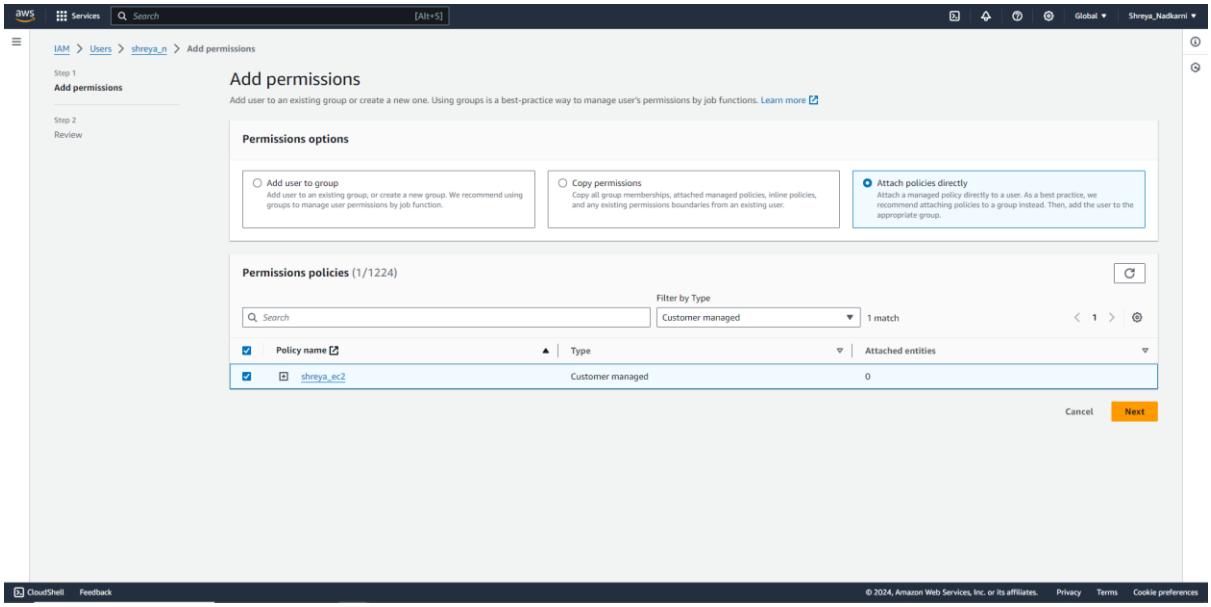


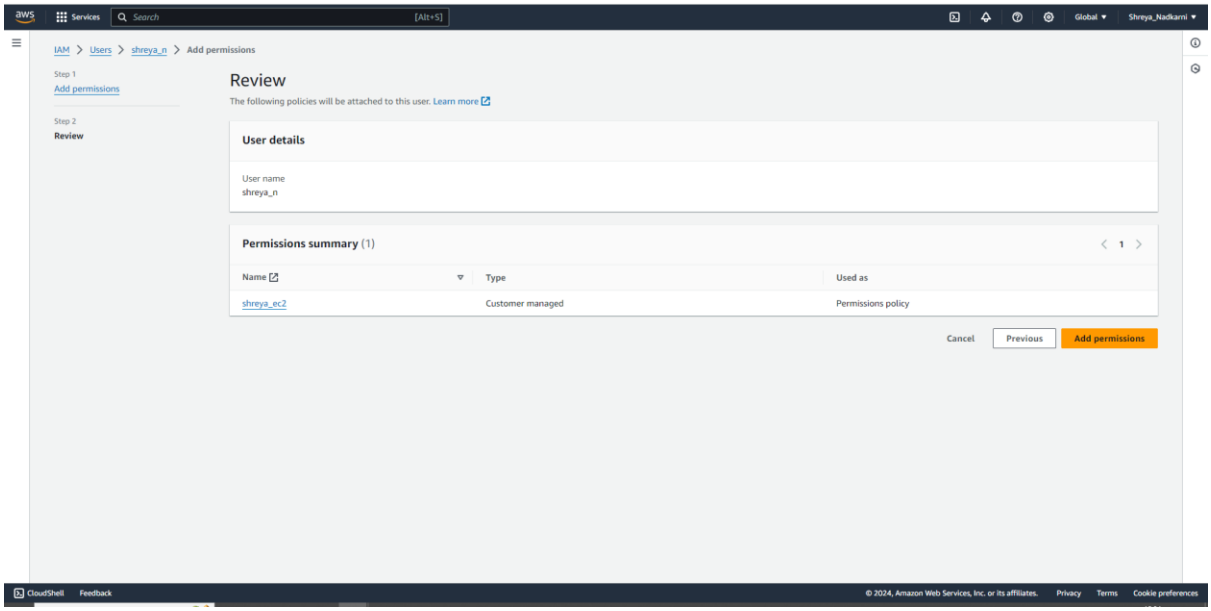


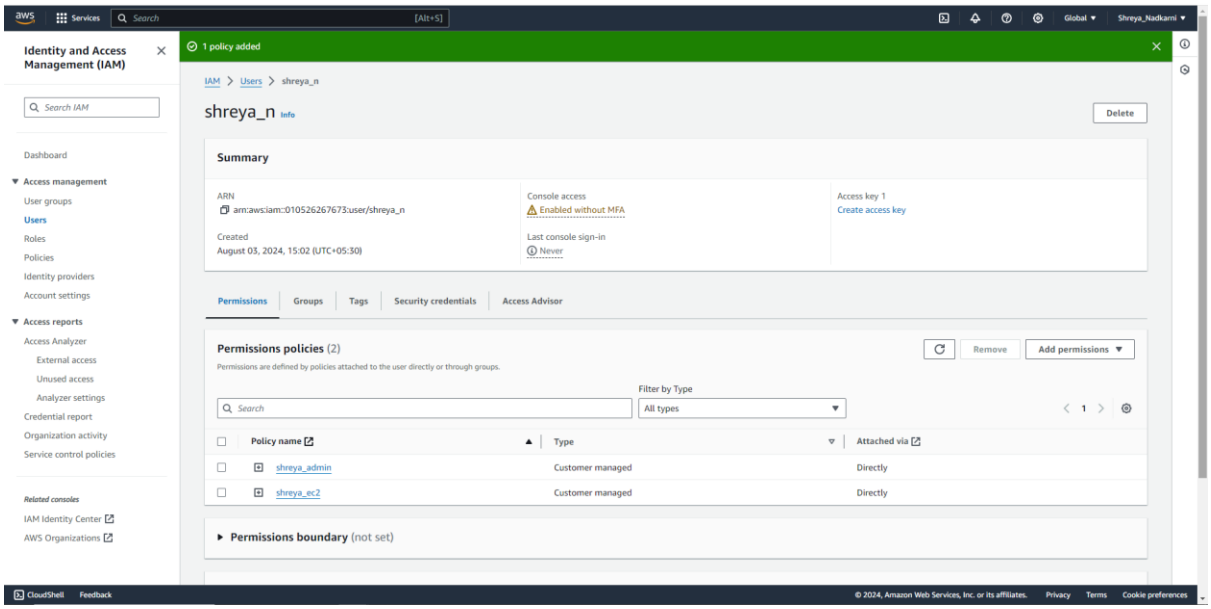
Boom! New policy created.

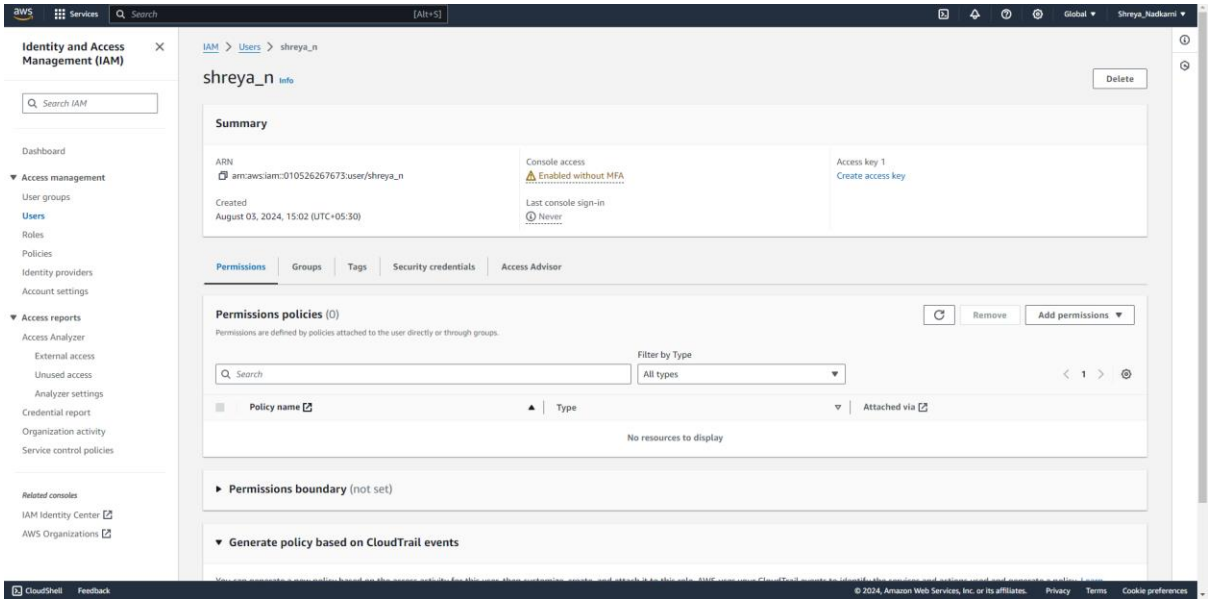


Now repeat the above same steps for attaching this EC2 policy to new IAM user




Services
Search
[Alt+S]
Global
Shreya_Nadkarni
IAM > Users > shreya_n > 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
shreya_n
Permissions summary (1)
Name
Type
Used as
shreya_ec2
Customer managed
Permissions policy
Cancel
Previous
Add permissions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
Global
Shreya_Nadkarni
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
Related consoles
IAM Identity Center
AWS Organizations
1 policy added
IAM > Users > shreya_n
shreya_n Info
Delete
Summary
ARN
arn:aws:iam::010526267673:user/shreya_n
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 15:02 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (2)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
Search
All types
Policy name
Type
Attached via
shreya_admin
Customer managed
Directly
shreya_ec2
Customer managed
Directly
Permissions boundary (not set)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
Global
Shreya_Nadkarni
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
Related consoles
IAM Identity Center
AWS Organizations
IAM > Users > shreya_n
shreya_n Info
Delete
Summary
ARN
arn:aws:iam::010526267673:user/shreya_n
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 15:02 (UTC+05:30)
Last console sign-in
Never
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
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences