

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

Practical-3 Identity Access Management.

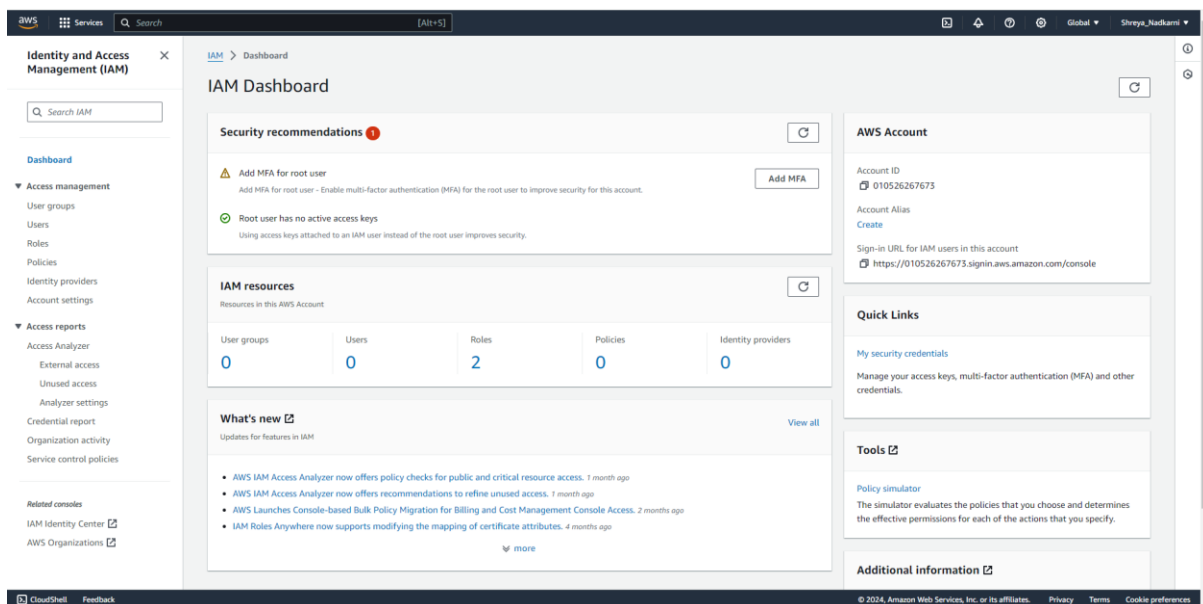
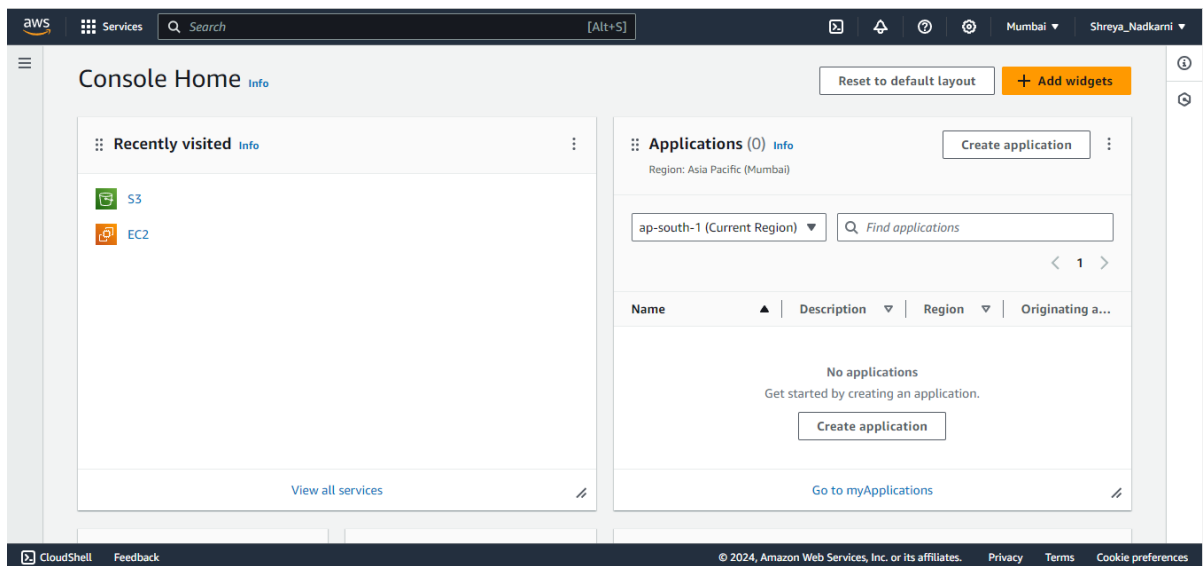
Name: Shreya Nadkarni

SAP ID: 86062300047

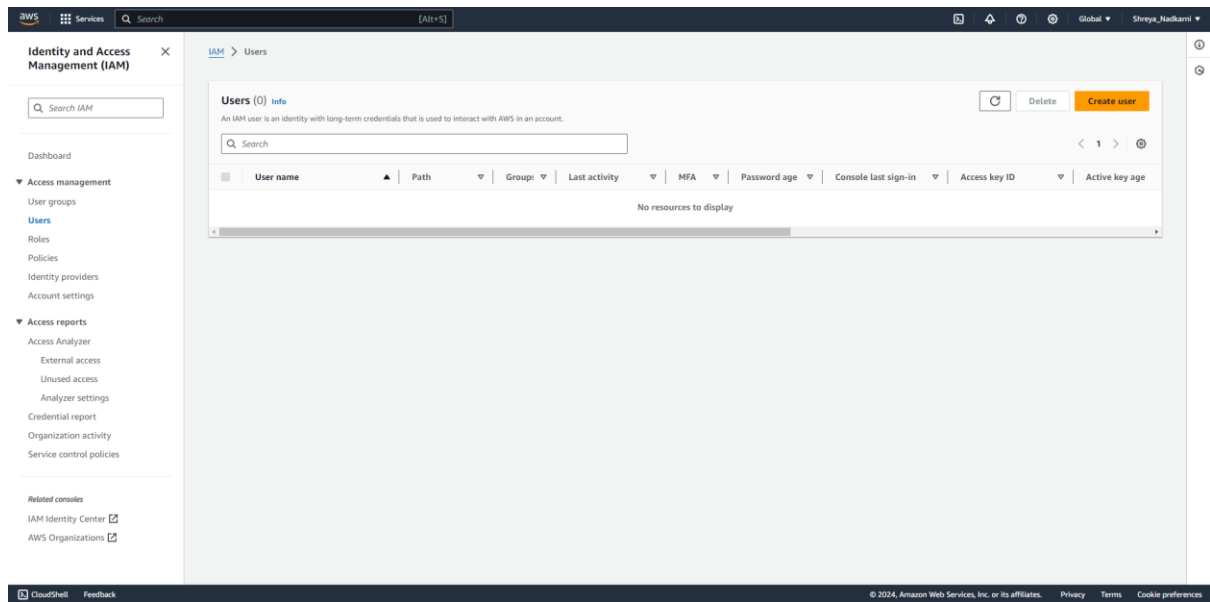
Roll No: A042

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

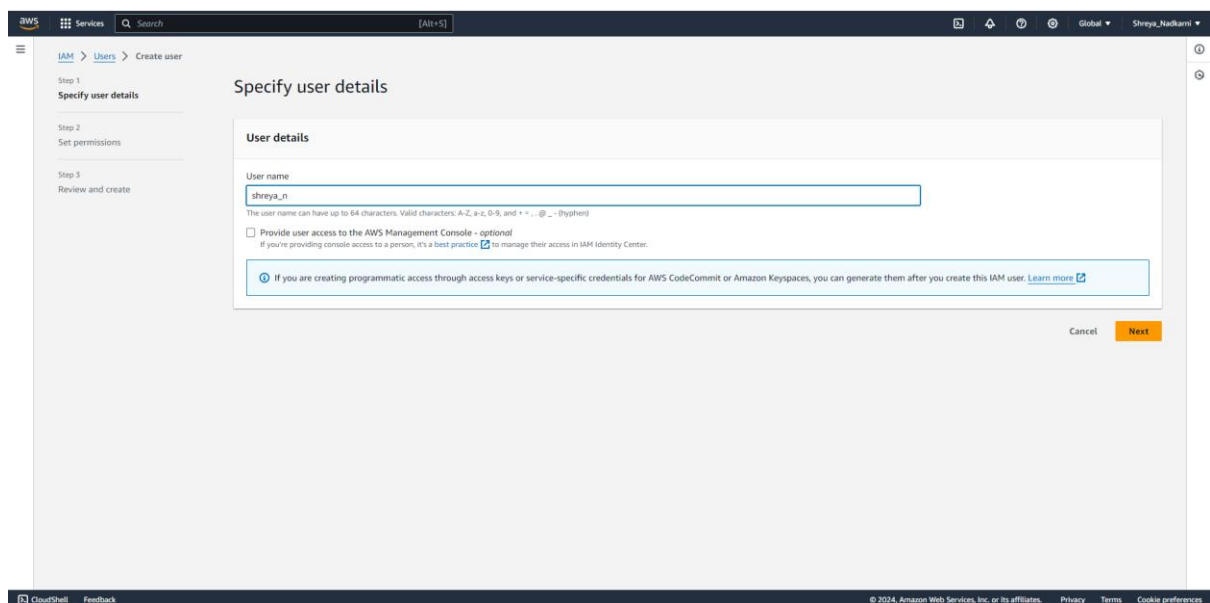
Sign in to the AWS Management Console and navigate to the IAM service by searching for "IAM" in the search bar.



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.

The screenshot shows the 'Review and create' step of the AWS IAM 'Create user' process. The left sidebar indicates the progress: Step 1 (Specify user details), Step 2 (Set permissions), and Step 3 (Review and create). The main content area is titled 'Review and create' and includes a sub-header 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.'

User details

User name shreya_n	Console password type None	Require password reset No
-----------------------	-------------------------------	------------------------------

Permissions summary

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.

Buttons at the bottom: [Cancel](#), [Previous](#), and [Create user](#).

Boom! new user is created

The screenshot shows the 'Users' page in the AWS IAM console. A green banner at the top indicates 'User created successfully' with the message: 'You can view and download the user's password and email instructions for signing in to the AWS Management Console.' and a [View user](#) button.

The left sidebar shows the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Related consoles.

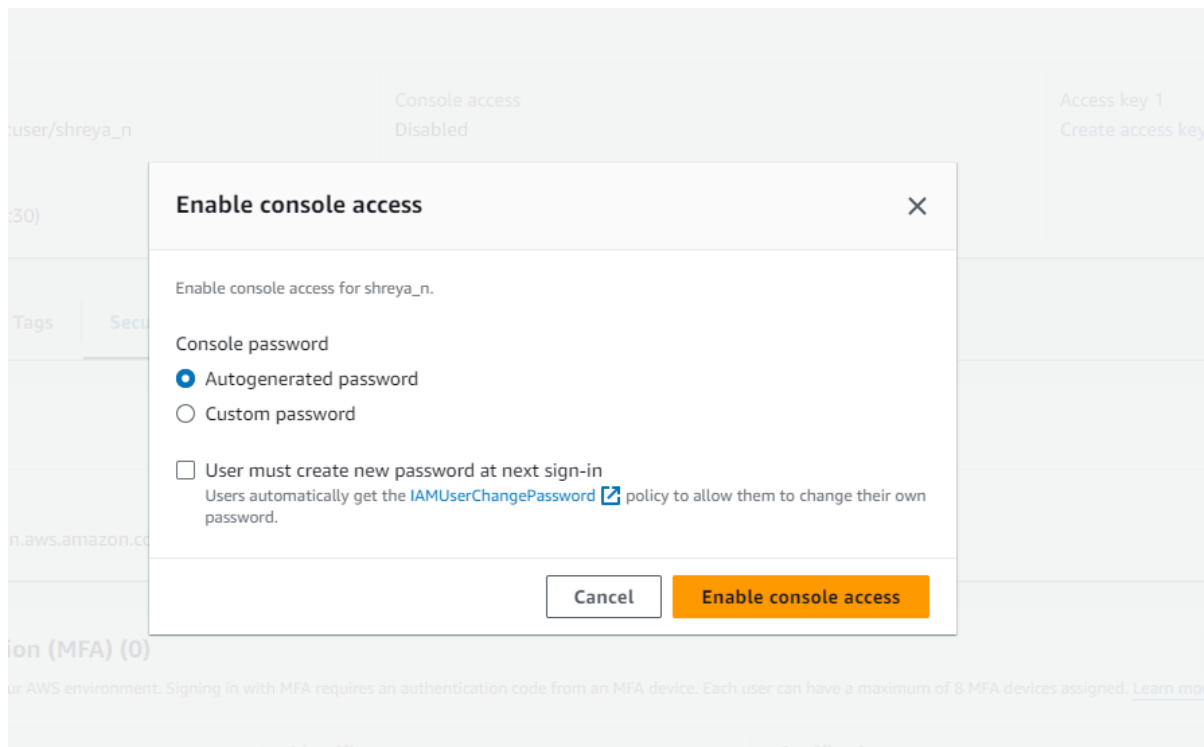
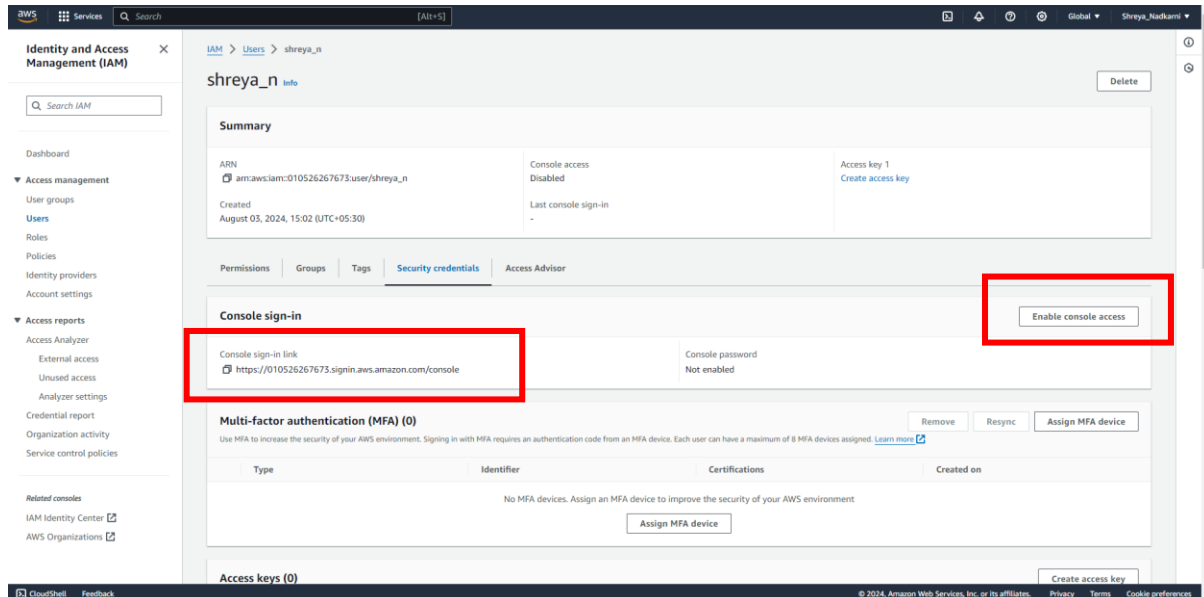
Users (1) Info

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

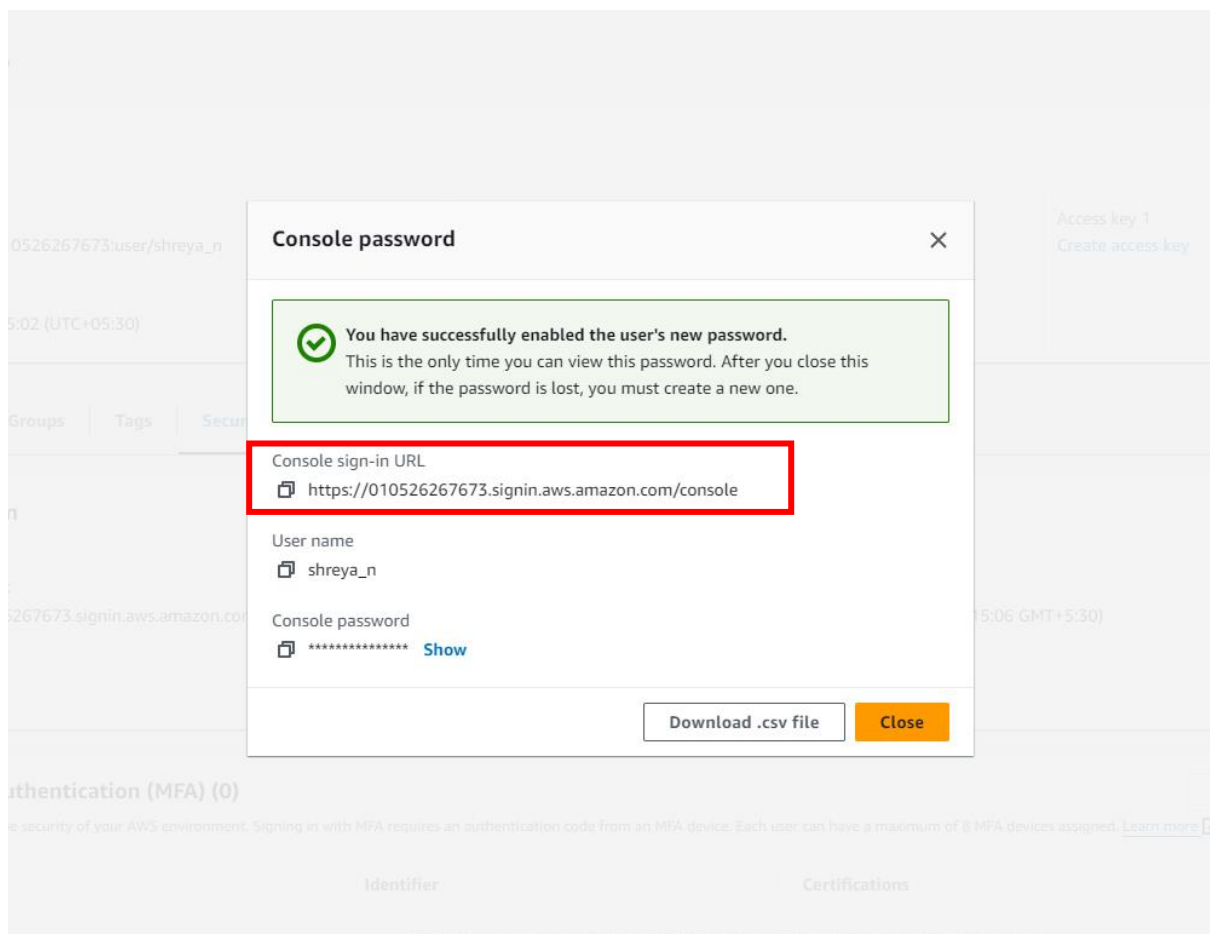
	User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age
<input type="checkbox"/>	shreya_n	/	0	-	-	-	-	-	-

Buttons at the top right of the table: [Refresh](#), [Delete](#), and [Create user](#).

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.



Sign in as IAM user

Account ID (12 digits) or account alias

010526267673

IAM user name

shreya_n

Password

☐ Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

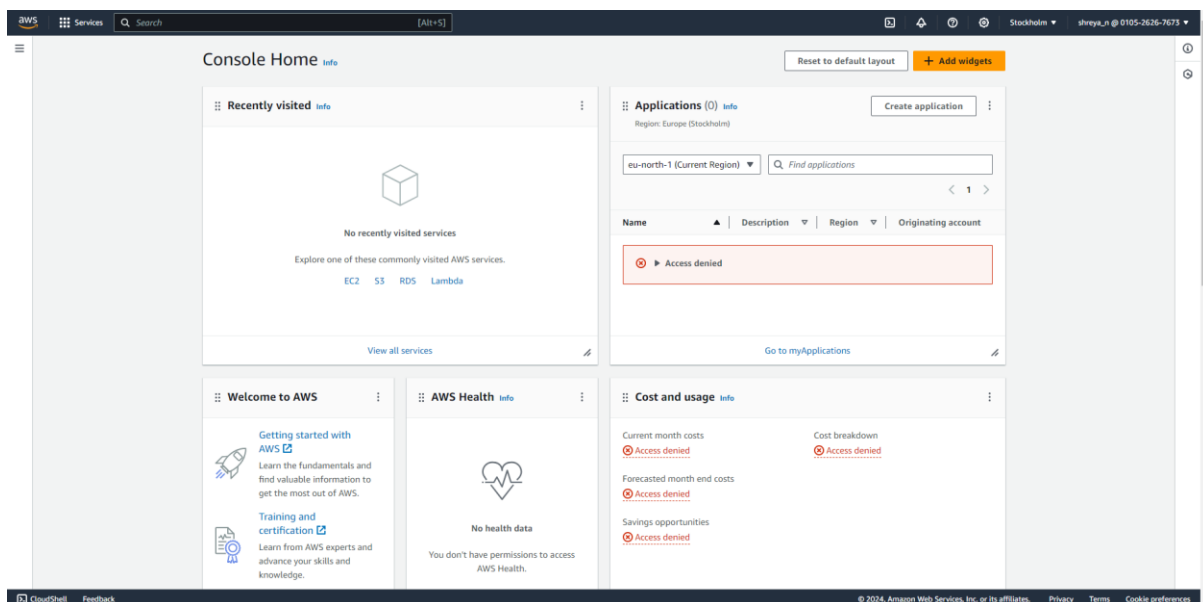
[Learn more »](#)



English

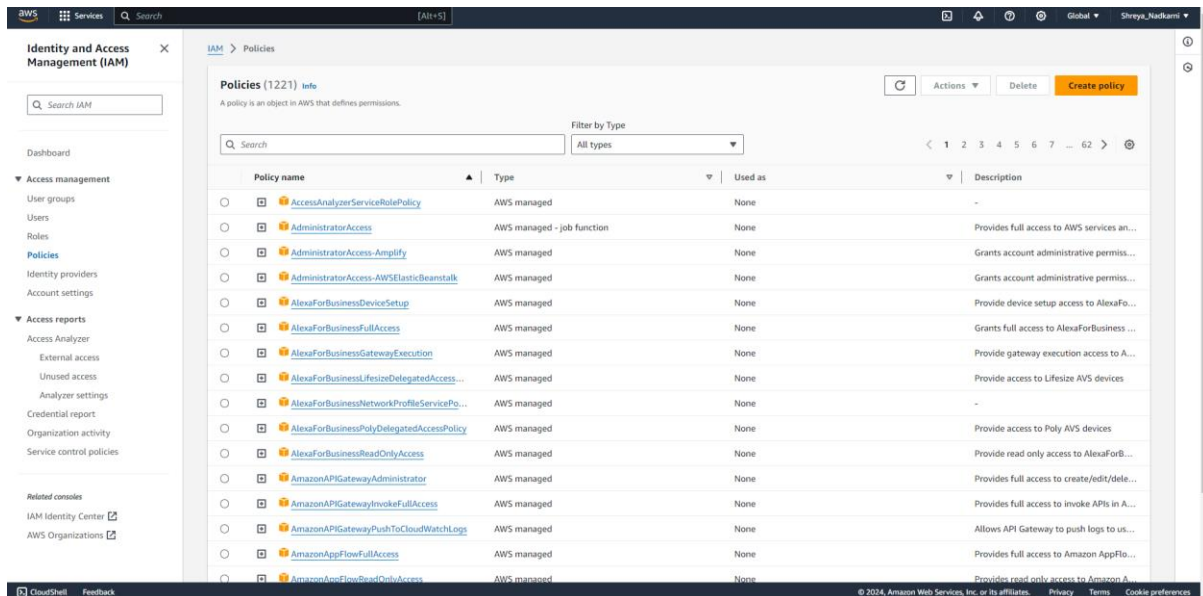
[Terms of Use](#) [Privacy Policy](#) © 1996-2024, Amazon Web Services, Inc. or its affiliates.

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:

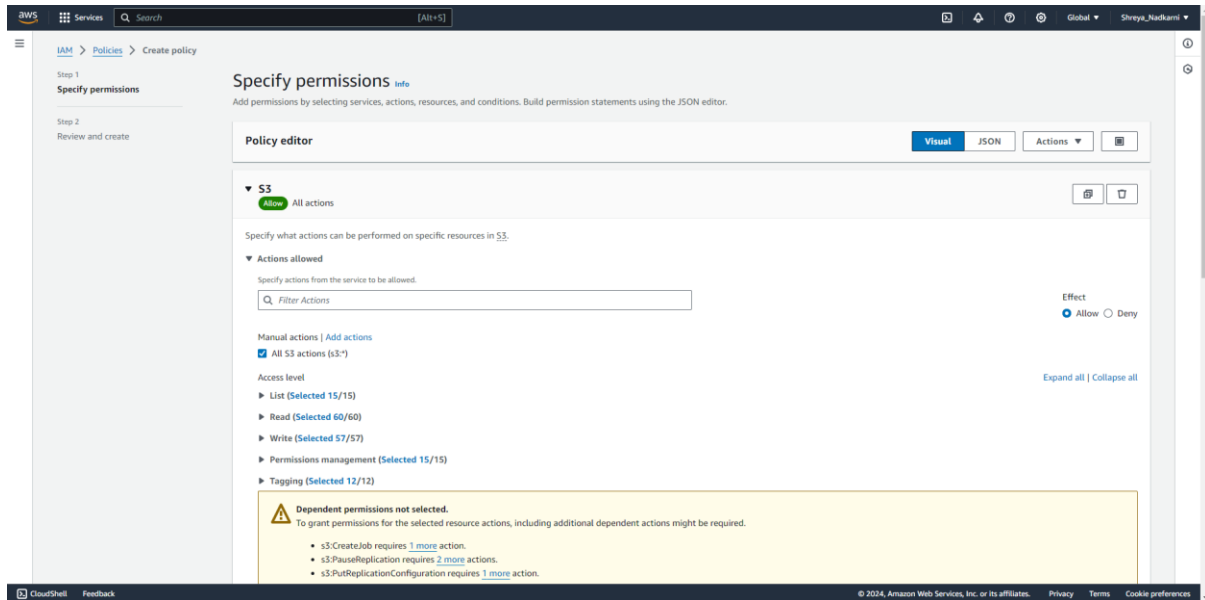
Navigate to IAM > Policies > Create policy.



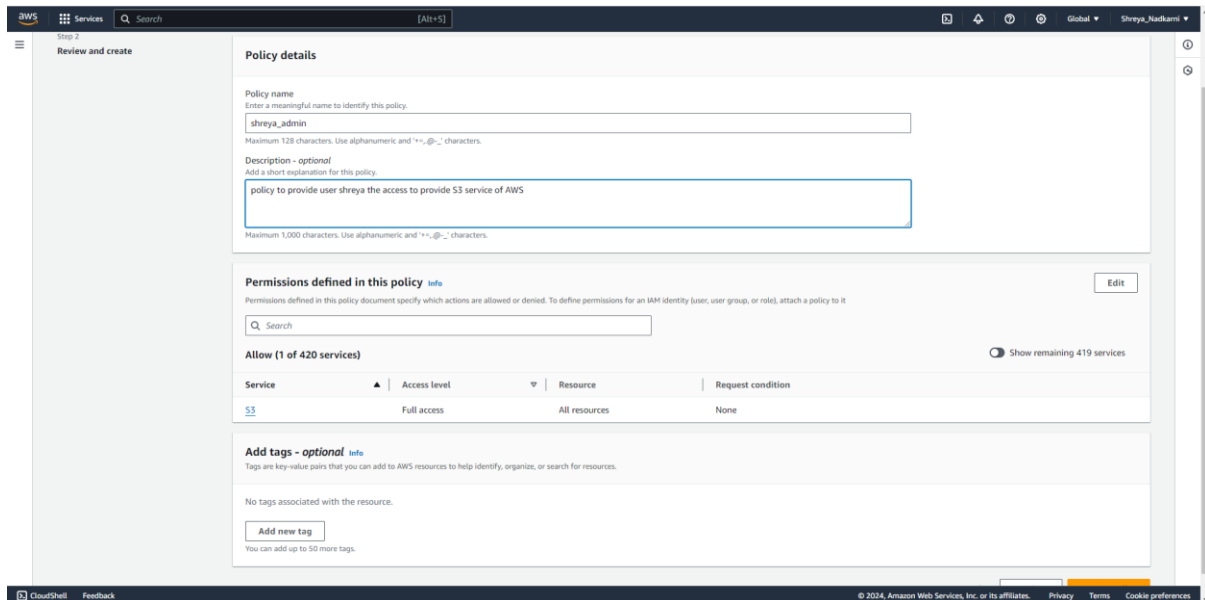
Choose "JSON" as the policy language and define the policy document. Here's an example for accessing four AWS services.

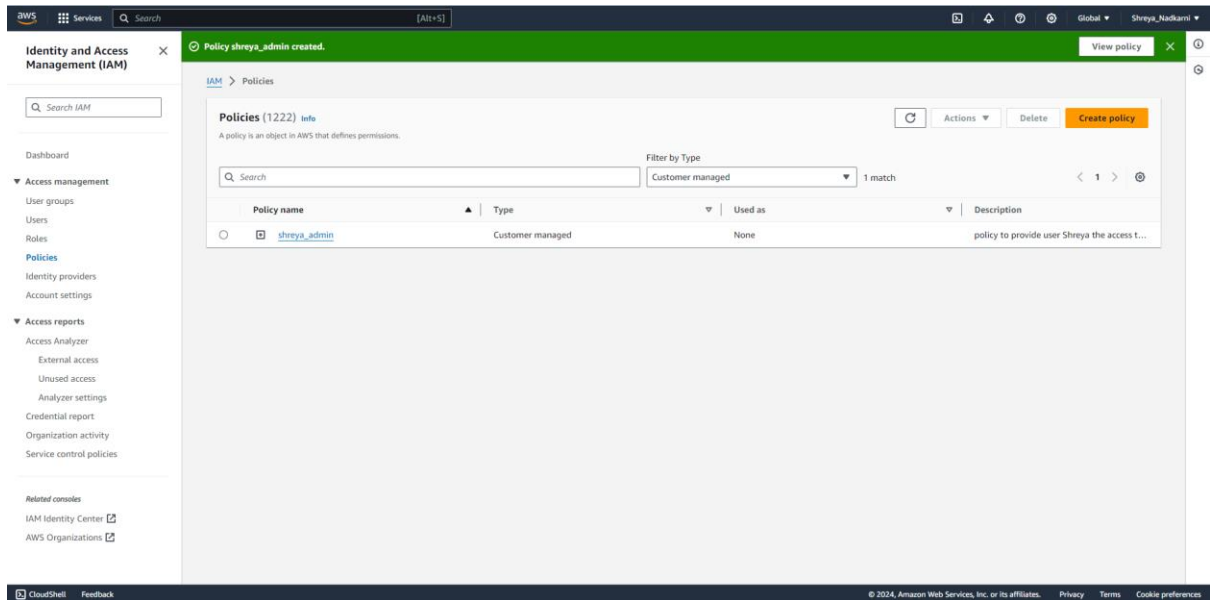
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:*",
        "ec2:*",
        "rds:*",
        "lambda:*"
      ],
      "Resource": "*"
    }
  ]
}
```

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

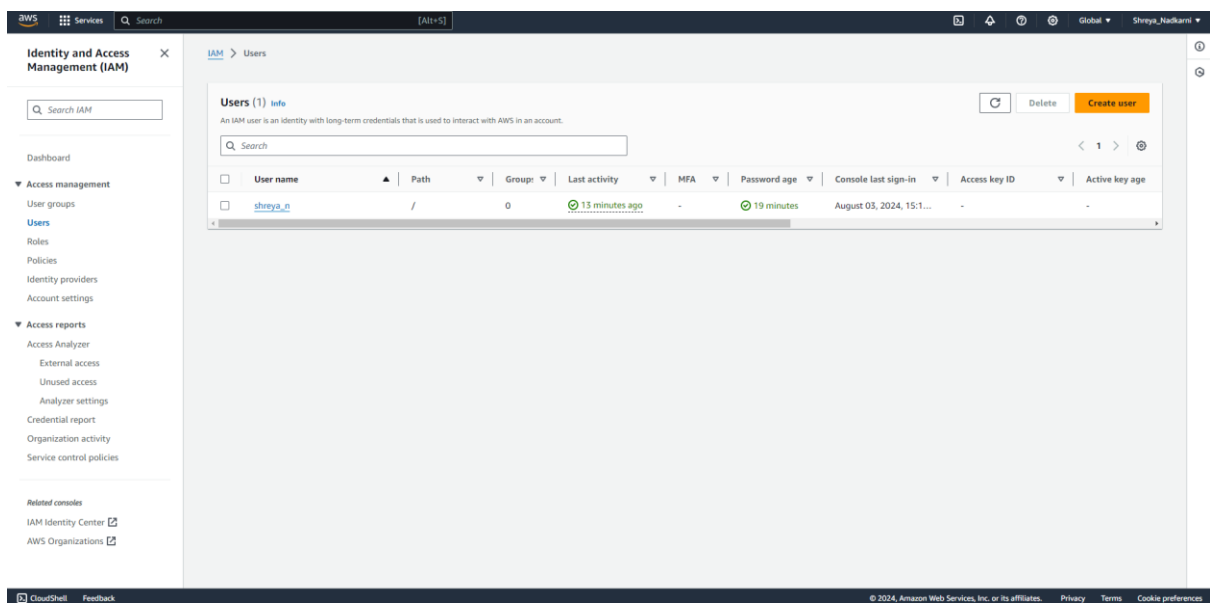


Provide appropriate policy details and click on the “create policy”.

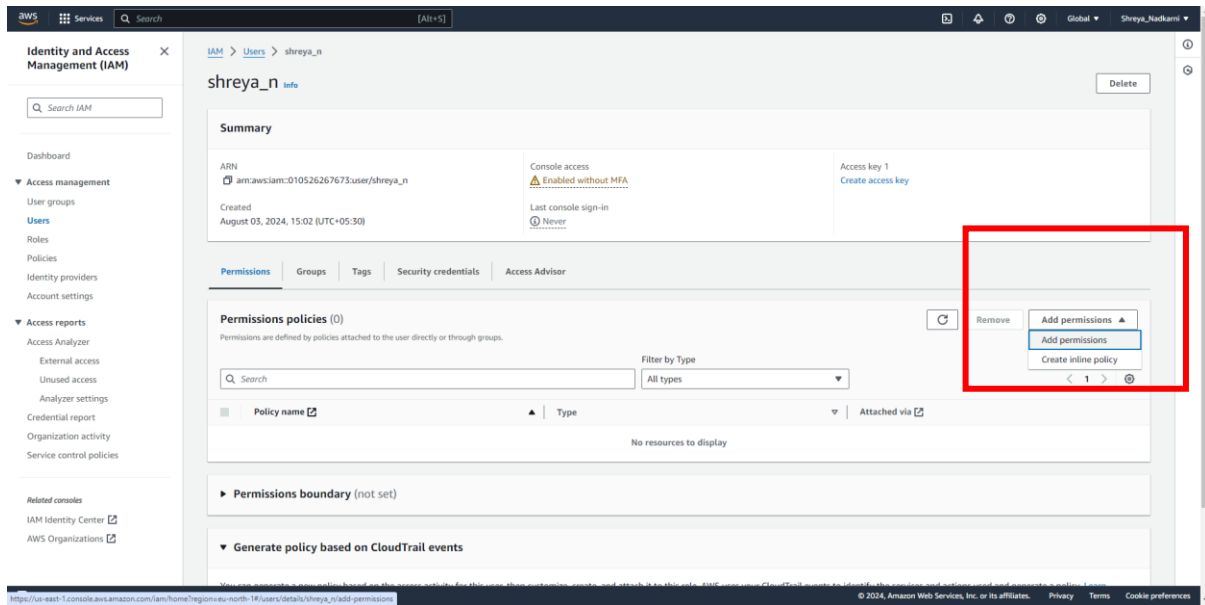




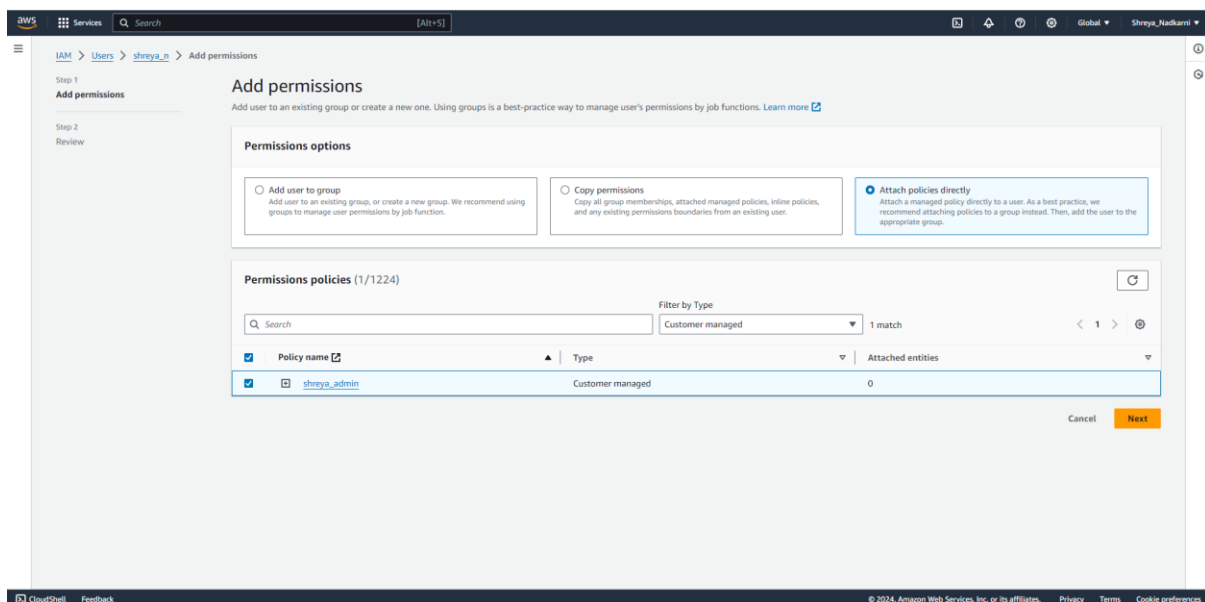
Once the policy is created, navigate to IAM > Users or IAM and Select the IAM user to which you want to attach the policy.

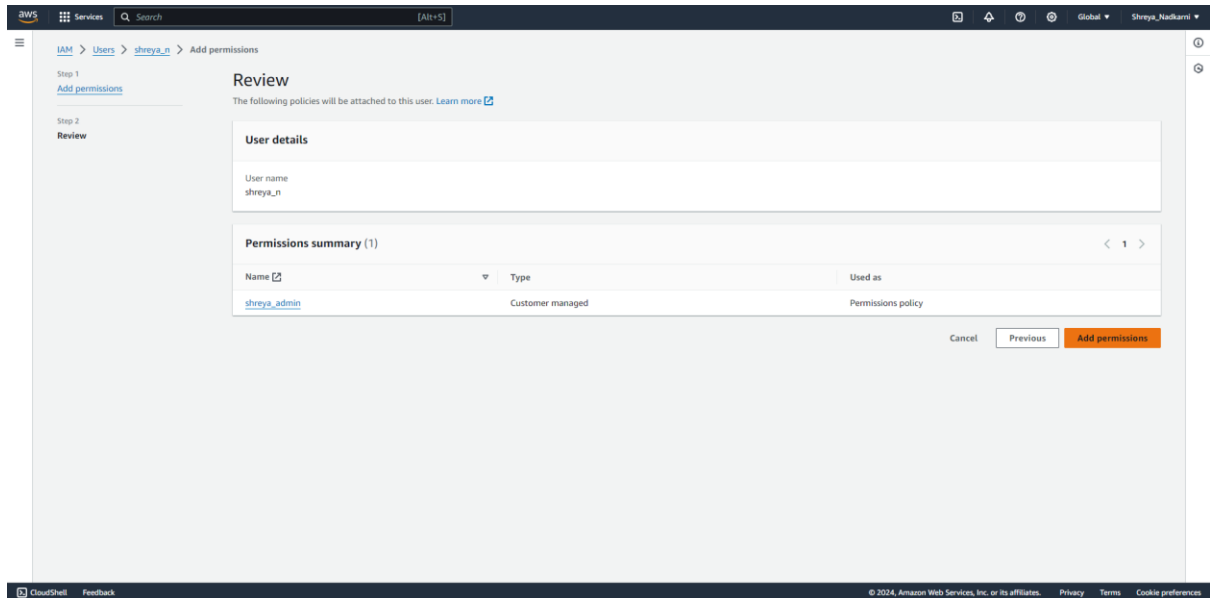


In the permissions tab, click "Add permissions" or "Attach policies".

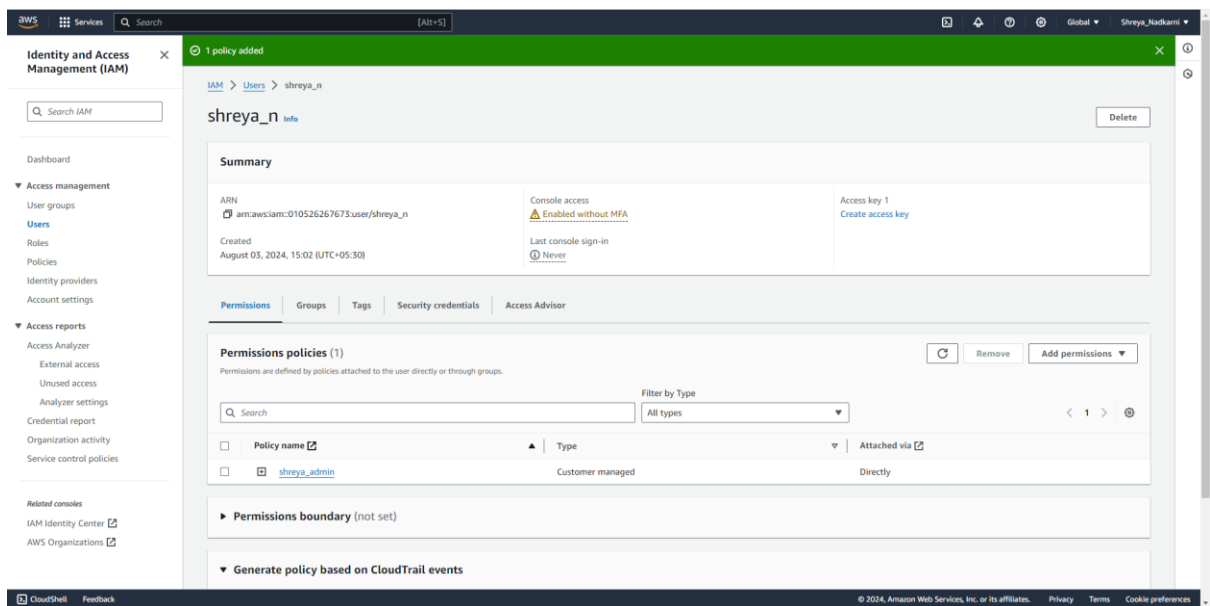


Search for and select the policy you created. Click "Add permissions" to assign the policy.





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

Account snapshot - updated every 24 hours

View Storage Lens dashboard

General purpose buckets

Directory buckets

General purpose buckets (1)

Buckets are containers for data stored in S3.

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

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory - New

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name

iamonadk

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

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended)

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

Block Public Access settings for this bucket

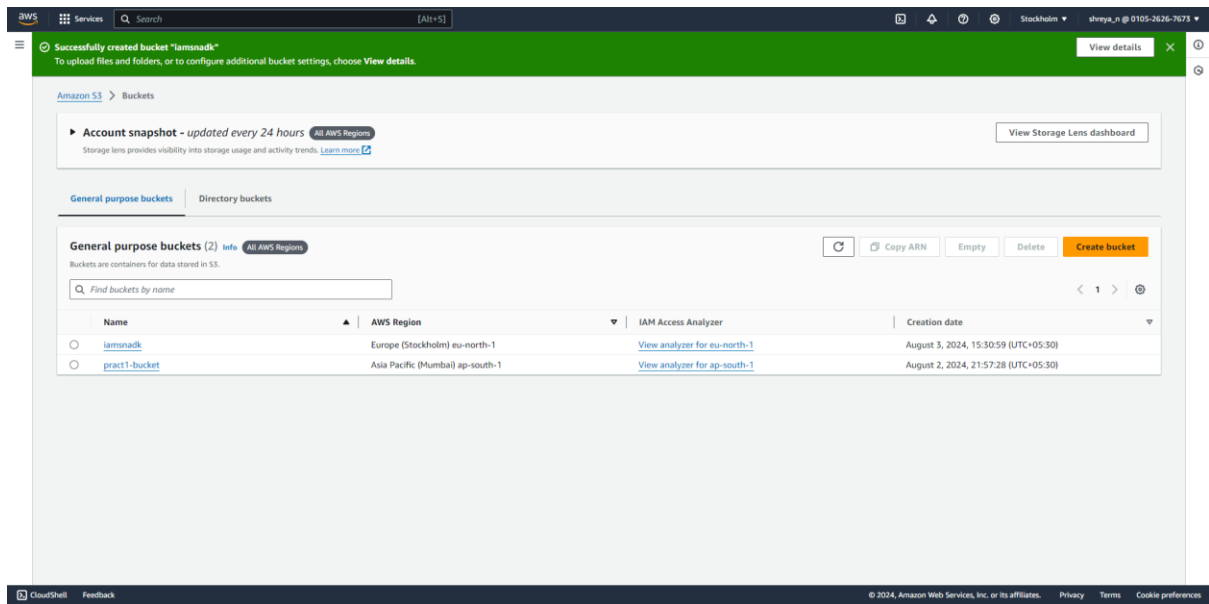
Public access controls to buckets and objects through access control lists (ACLs), bucket policies, access point policies, and the bucket policy.

CloudShell

Feedback

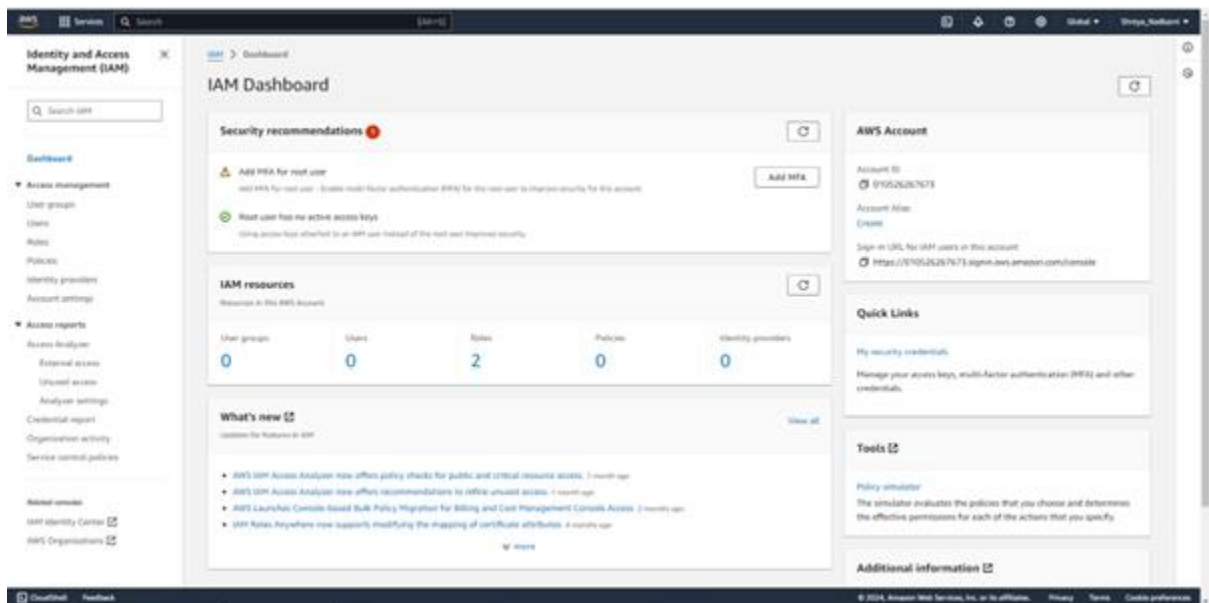
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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



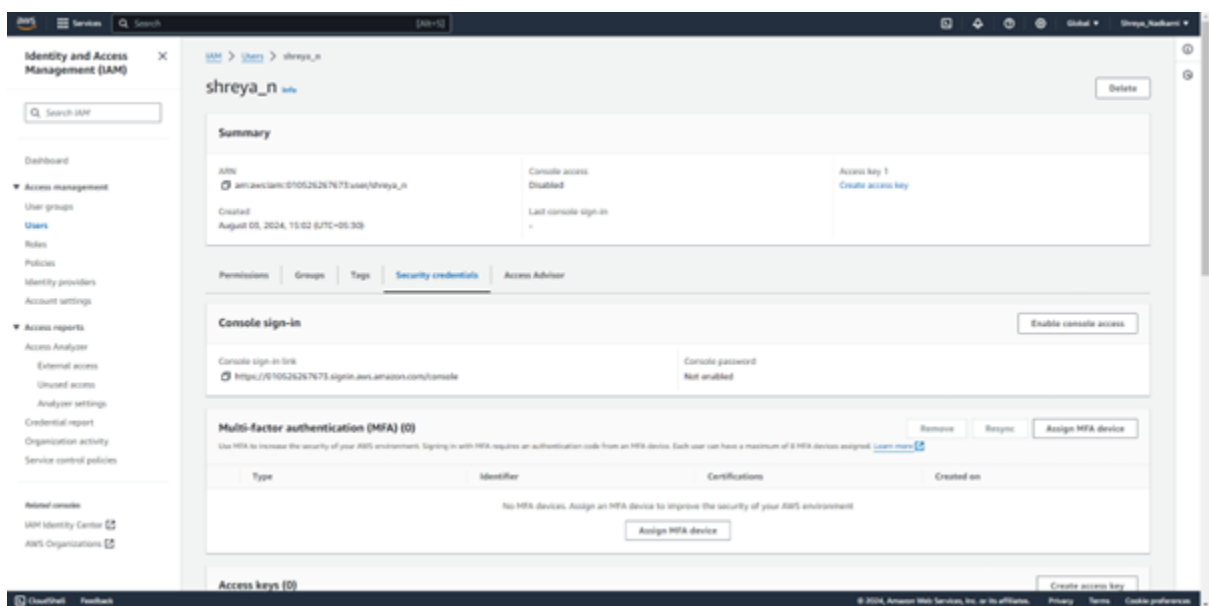
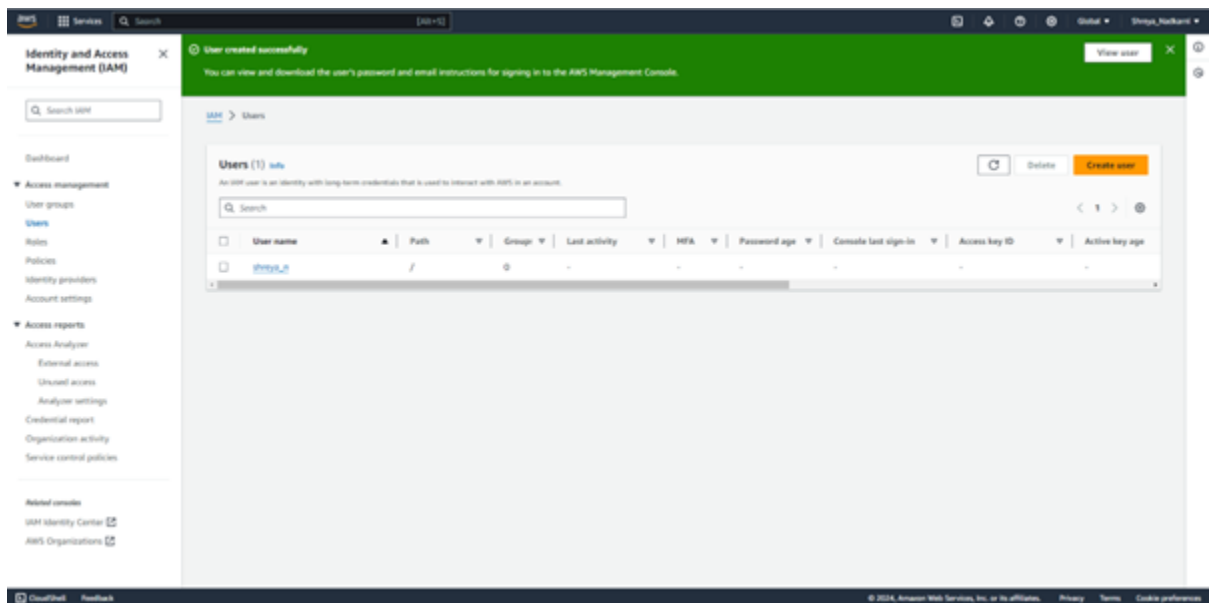
Steps to Attach the EC2 Policy to an IAM User:

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.

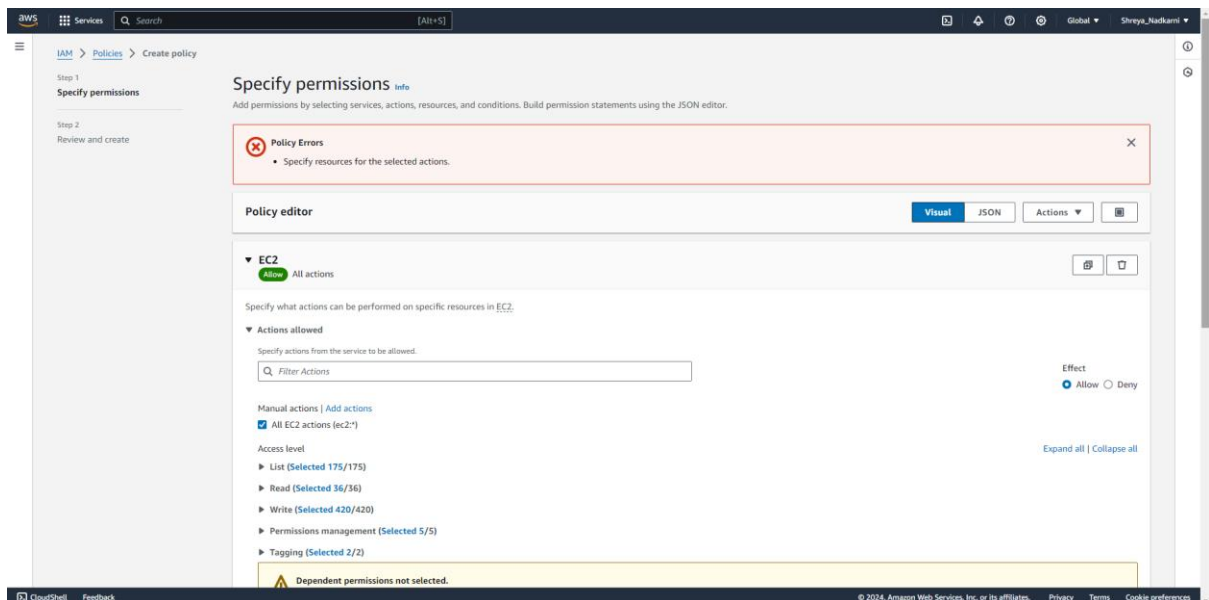
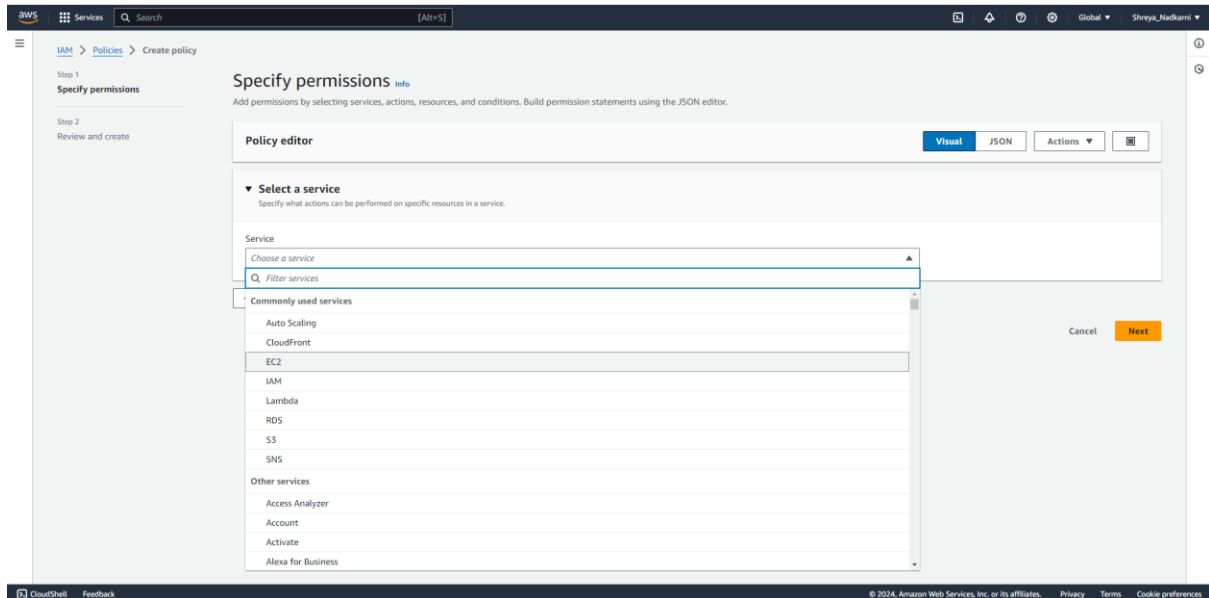


In the "Add permissions" wizard, choose "Attach policies directly" to assign policies directly to the user.

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.

The screenshot shows the AWS IAM console with a green notification banner at the top stating "Policy shreya_ec2 created." Below the banner, the "Policies" page is displayed. The left sidebar shows the "Identity and Access Management (IAM)" menu with options like Dashboard, Access management, and Access reports. The main content area shows a list of policies. The "Policy shreya_ec2" is highlighted in blue.

Policy name	Type	Used as	Description
shreya_admin	Customer managed	Permissions policy (1)	policy to provide user Shreya the access t...
shreya_ec2	Customer managed	None	-

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

The screenshot shows the "Add permissions" step in the AWS IAM console. The left sidebar shows the "Users" menu with the "shreya_n" user selected. The main content area shows the "Add permissions" page. The "Permissions options" section has three radio buttons: "Add user to group", "Copy permissions", and "Attach policies directly". The "Attach policies directly" option is selected. Below this, the "Permissions policies" section shows a list of policies. The "Policy shreya_ec2" is highlighted in blue.

Policy name	Type	Attached entities
shreya_ec2	Customer managed	0

