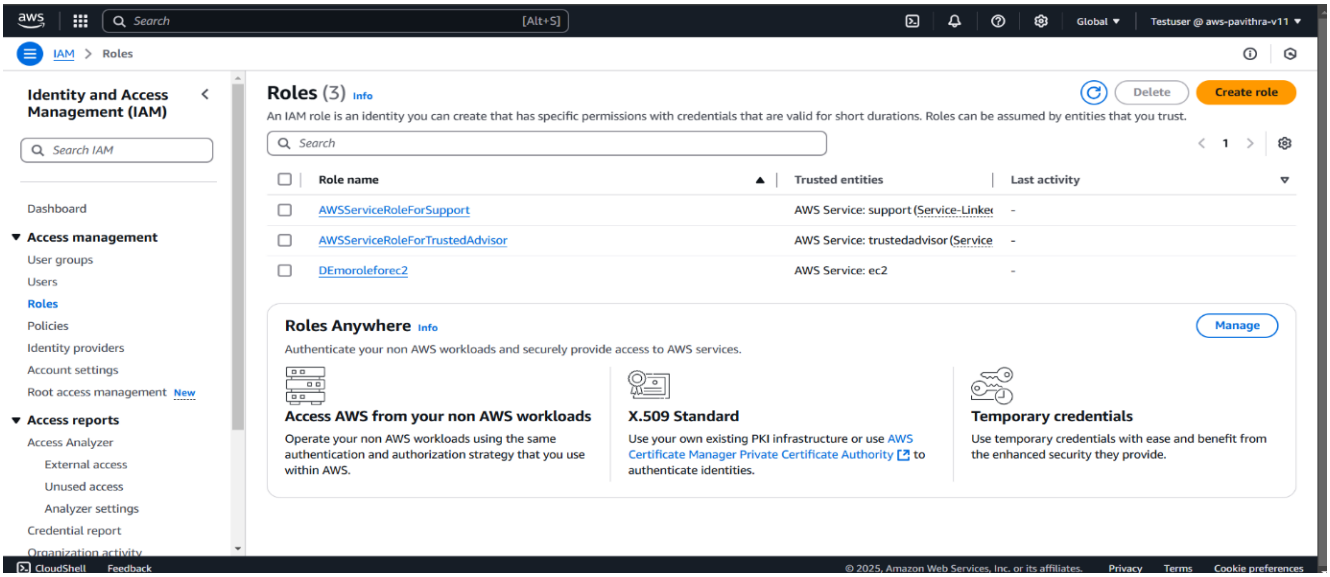
Part 1: Create IAM Roles for Developers

IAM roles allow controlled access to AWS resources without sharing credentials.

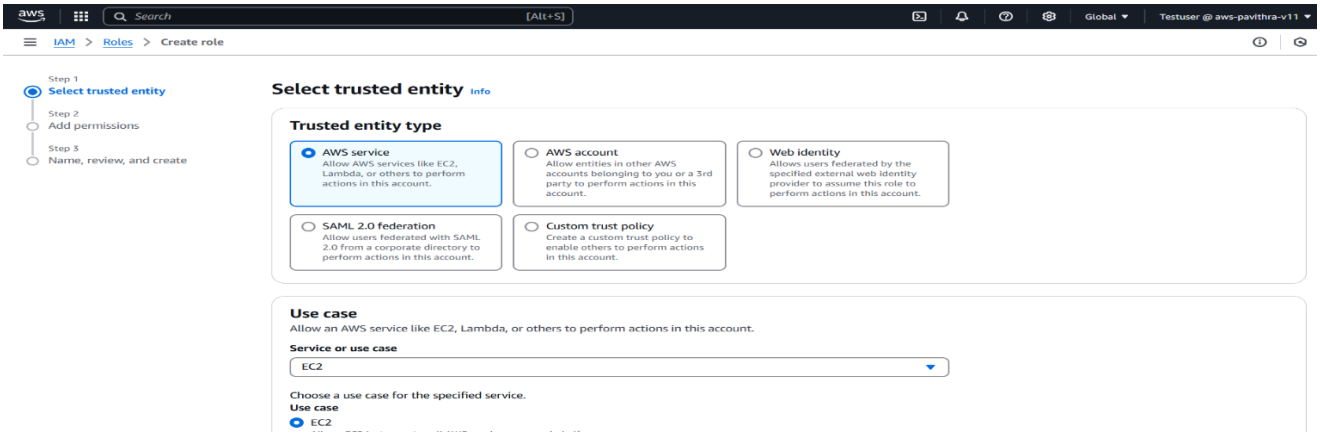
Step 1.1: Navigate to IAM Roles

1. Log in to the AWS Management Console.
2. Open the **IAM Dashboard** and select **Roles** from the navigation pane.
3. Click **Create role**.



Step 1.2: Define Trusted Entity

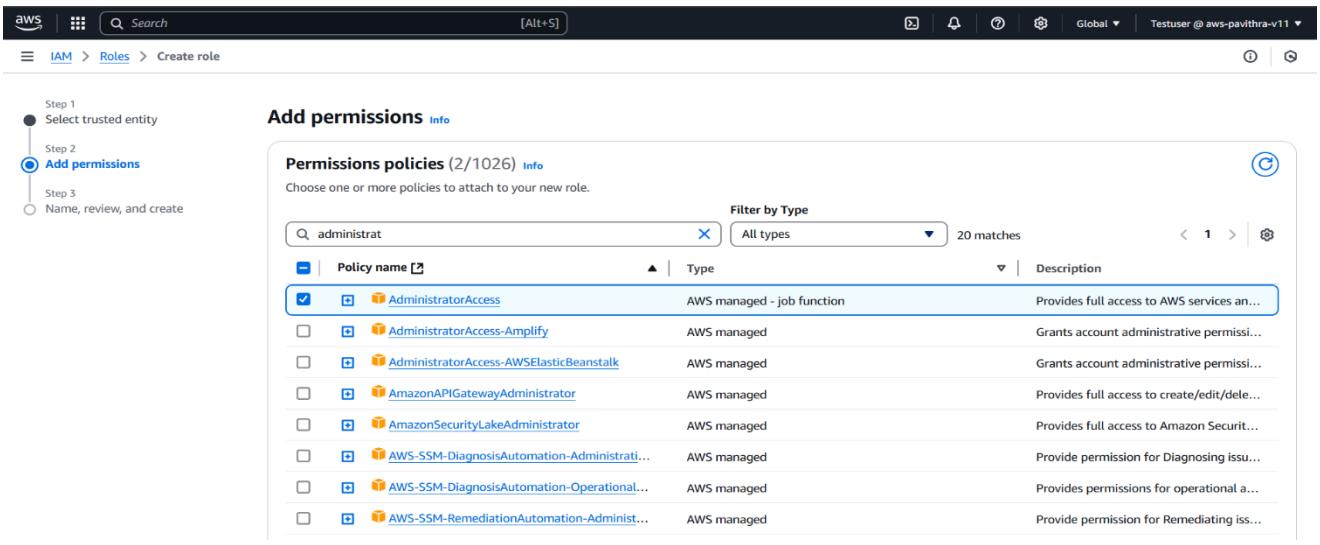
1. Choose a trusted entity type:
    - For applications: **AWS service** (e.g., EC2).
    - For users: **Another AWS account** or **IAM users**.
2. Click **Next**.

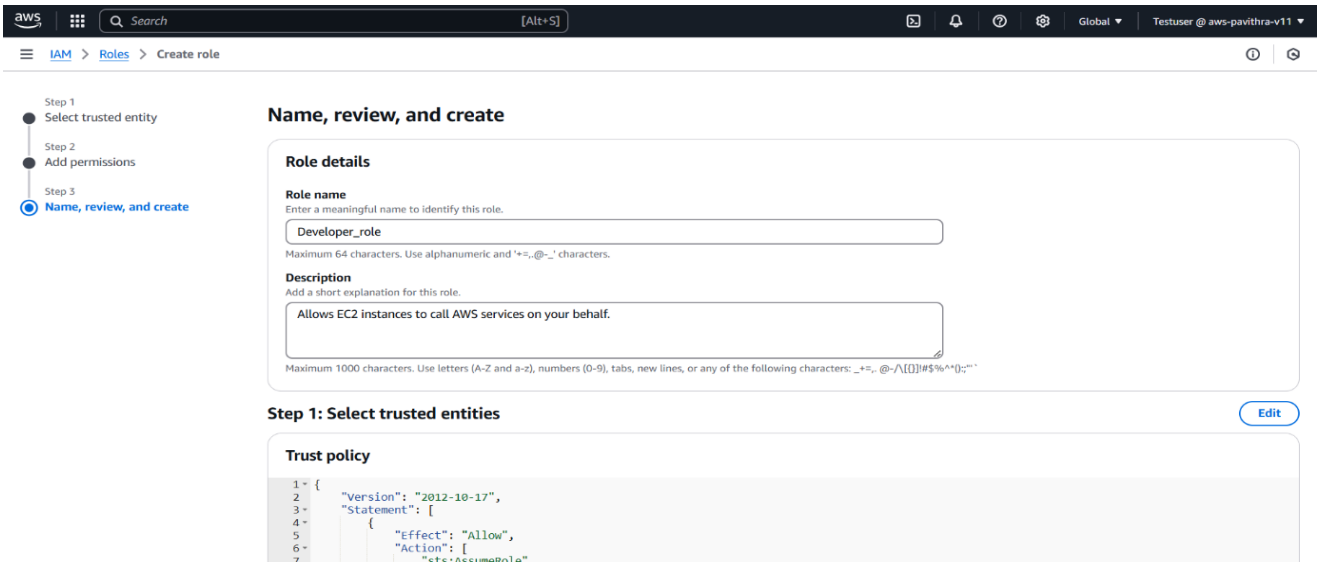


Step 1.3: Attach a Policy

1. Select an existing policy or create a custom policy:
    - For developers, attach **AmazonS3ReadOnlyAccess** for read-only access to S3.
    - For sensitive workloads, attach **AdministratorAccess** (restricted use).

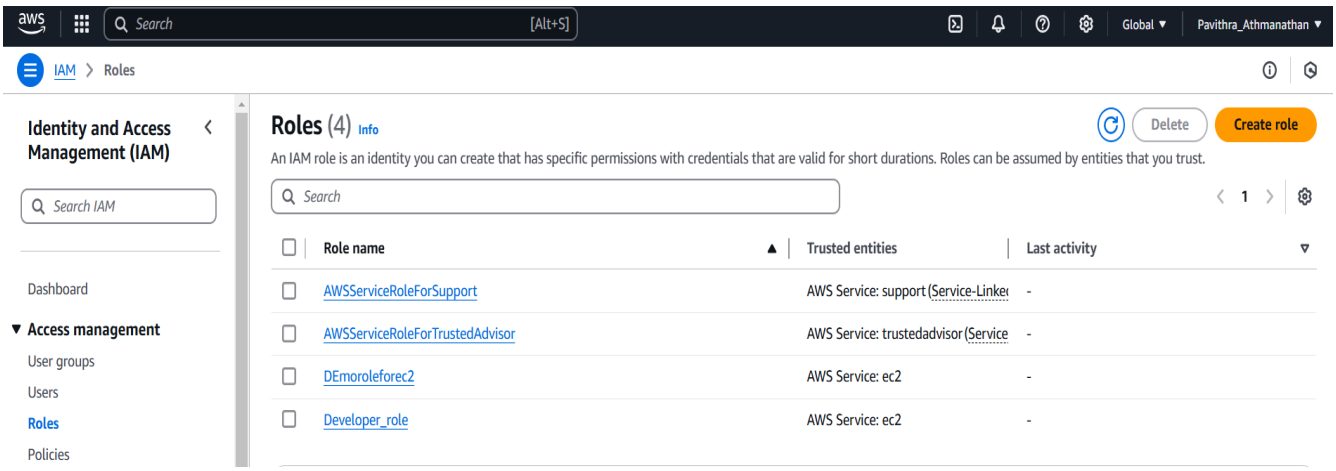
2. Click **Next** and provide a **Role name** (e.g., DeveloperRole).





Step 1.4: Review and Create

1. Verify details and click **Create role**.



Part 2: Define IAM Policies

IAM policies restrict or grant access to AWS services.

Step 2.1: Create a Custom Policy

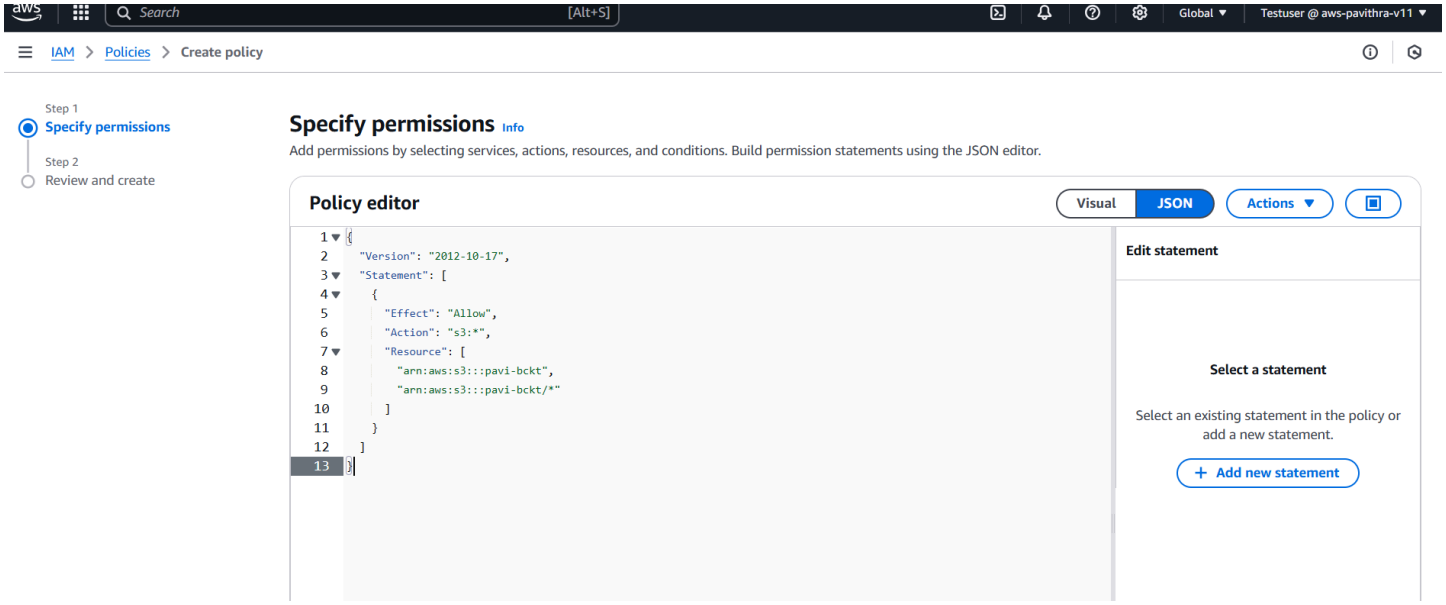
1. Navigate to **IAM Policies** and click **Create policy**.

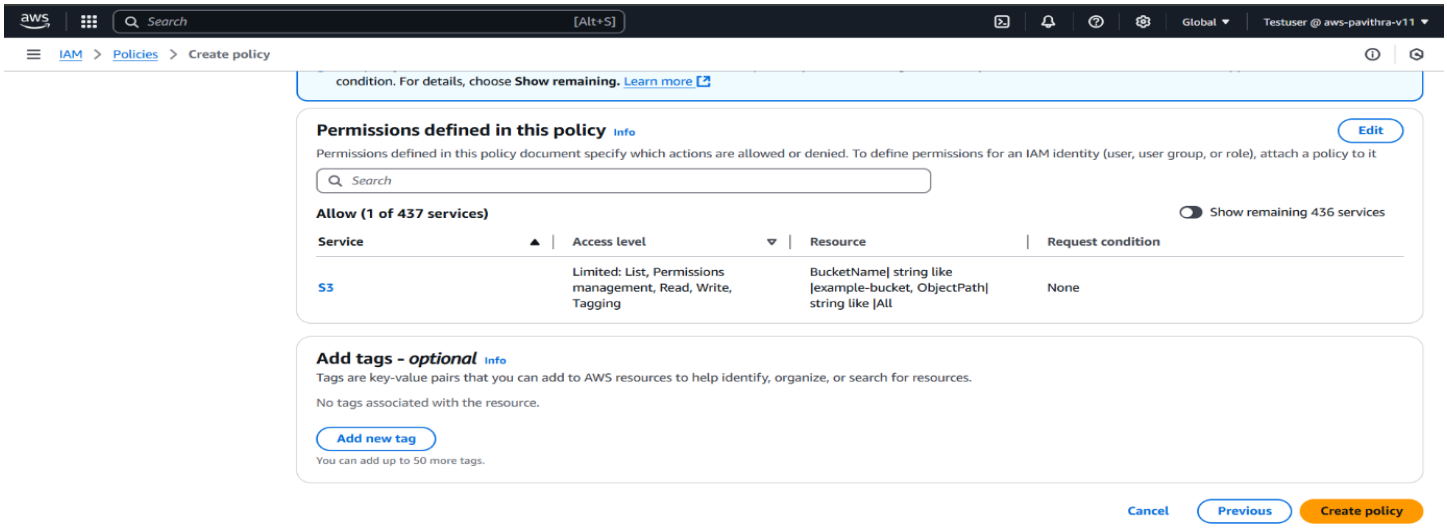
Define permissions in JSON format:

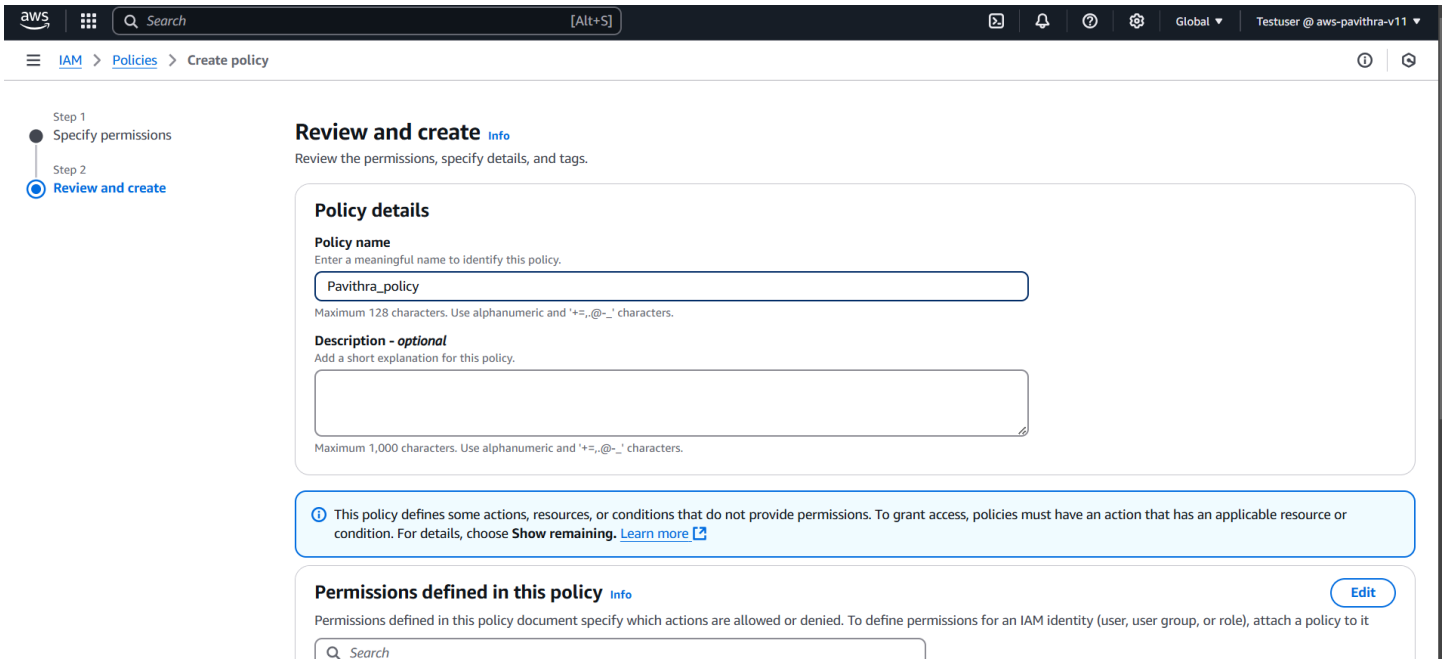
```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "s3:*",
   "Resource": "arn:aws:s3:::example-bucket/*"
  }
 ]
}
```

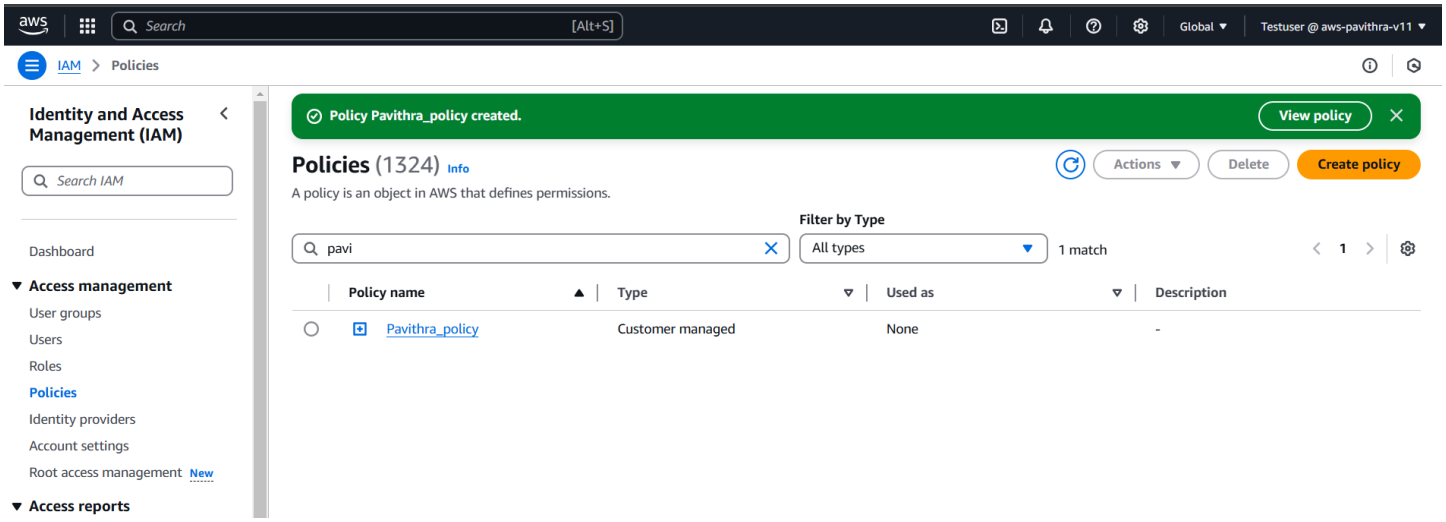
2.

3. Click **Review policy**, provide a name (e.g., S3FullAccess), and save.



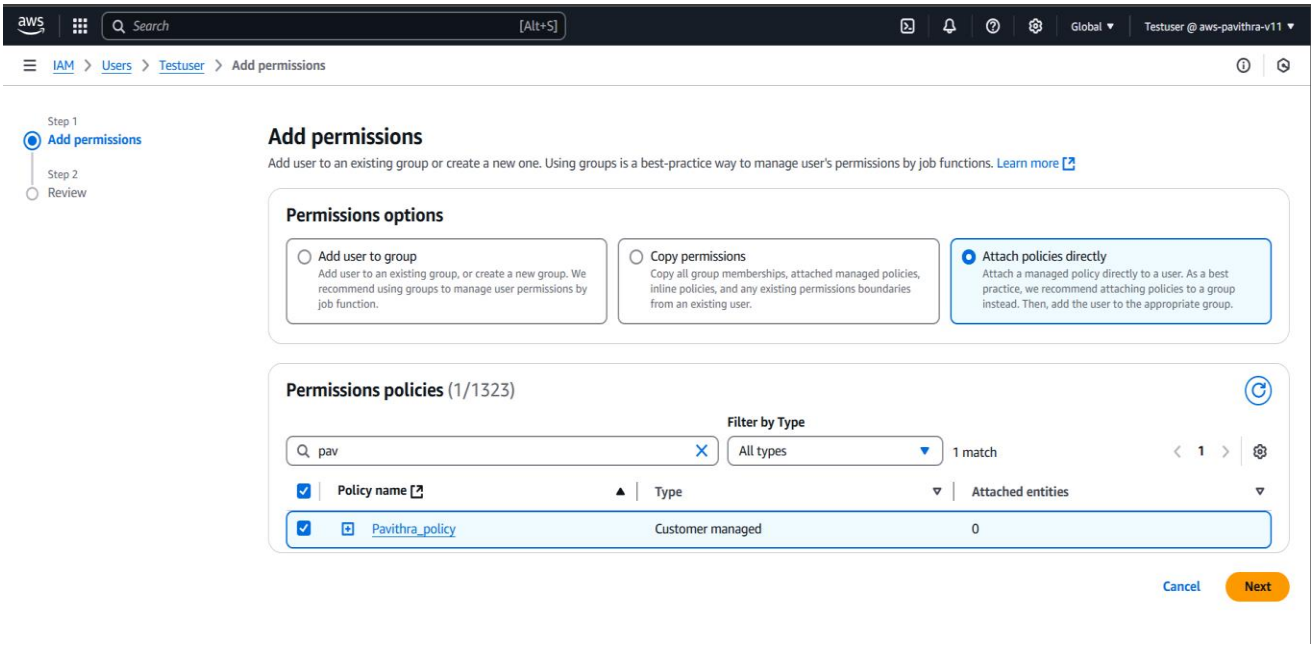


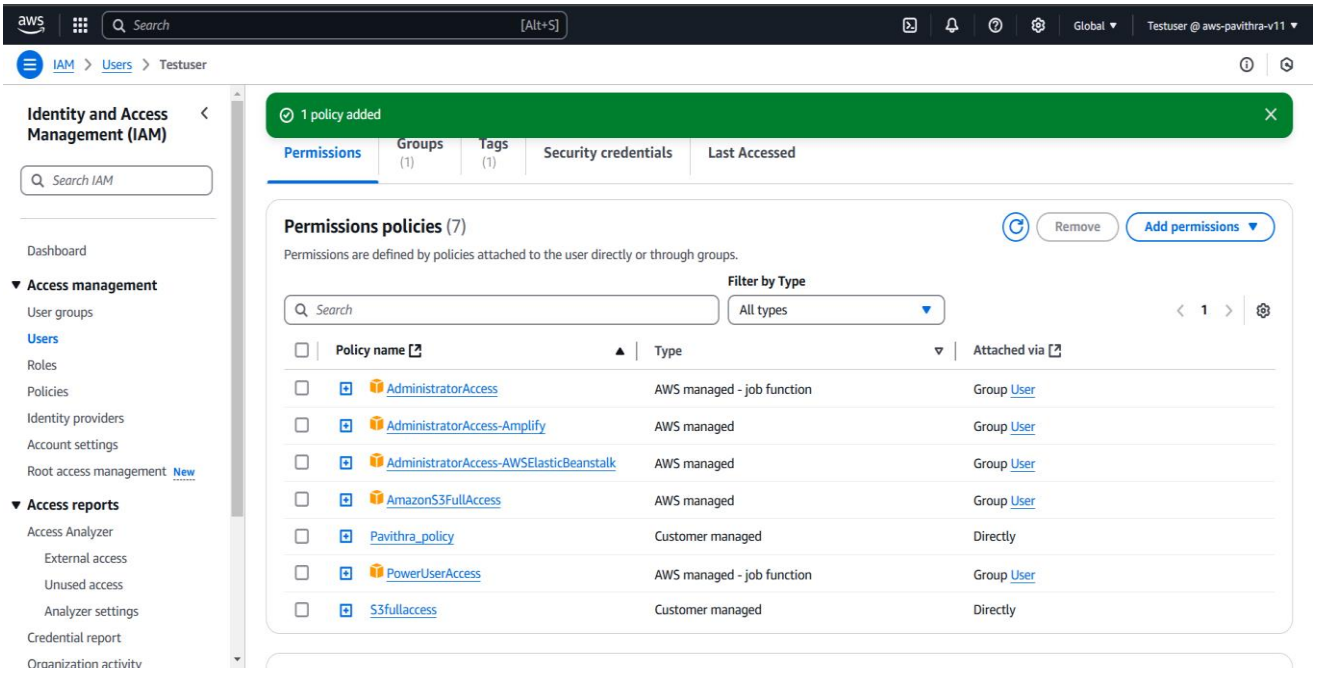




Step 2.2: Attach Policy to a Role or User

1. Go to **Roles** or **Users** in IAM.
2. Attach the newly created policy (e.g., S3FullAccess) to the required entity.



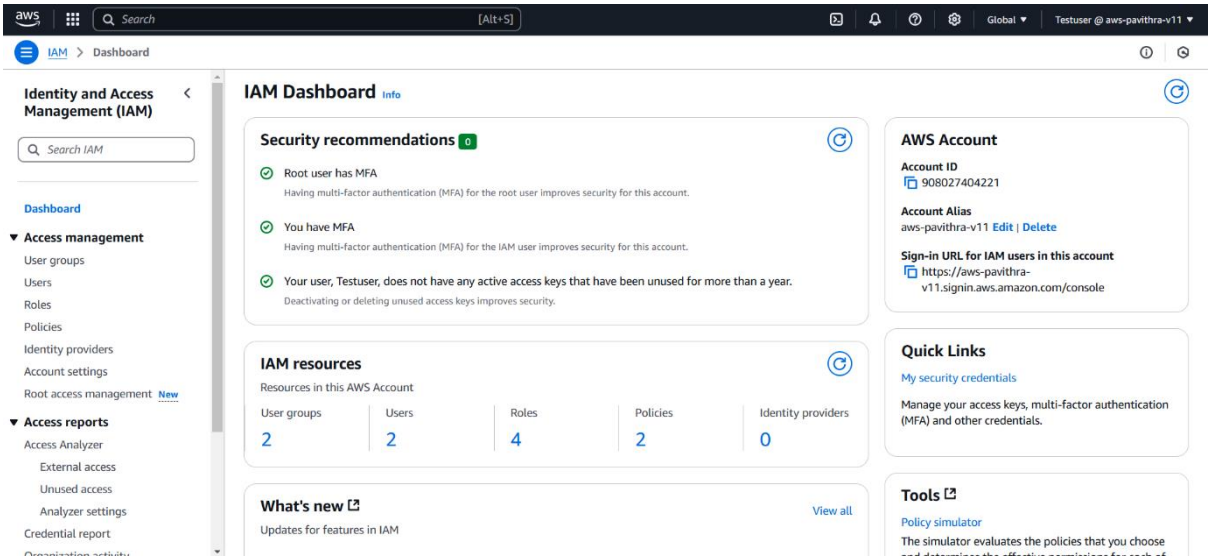


Part 3: Secure Access with MFA

MFA adds an extra layer of security to AWS accounts.

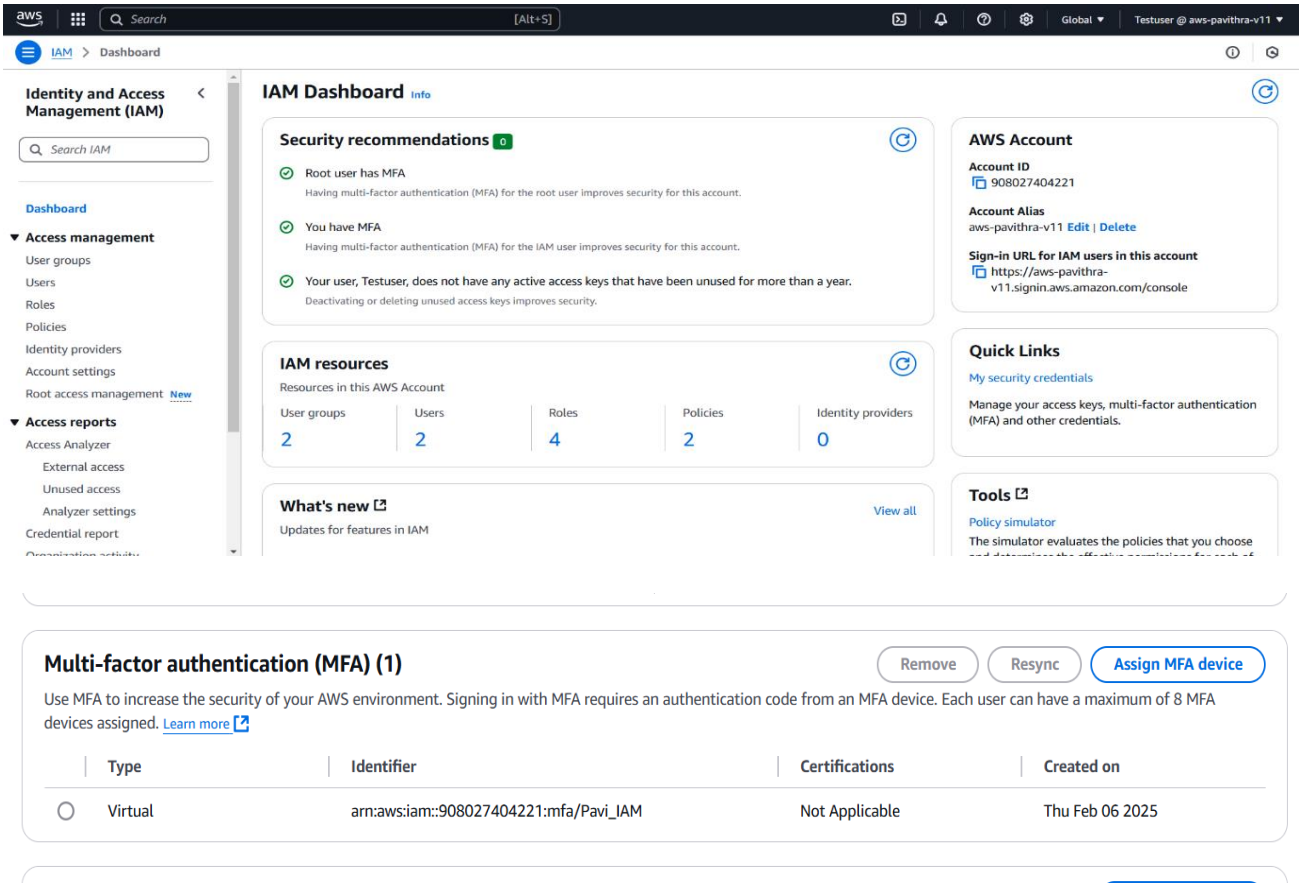
Step 3.1: Enable MFA for Root User

1. Log in as the root user and navigate to **My Security Credentials**.
2. Under **Multi-Factor Authentication (MFA)**, click **Activate MFA**.
3. Choose a device type (e.g., virtual MFA using Google Authenticator).
4. Scan the QR code, input the codes generated, and save.



Step 3.2: Enable MFA for IAM Users

1. Go to the **IAM Dashboard** and select **Users**.
2. Choose a user and click **Security credentials**.
3. Under **MFA**, click **Manage** and follow the steps to activate MFA.



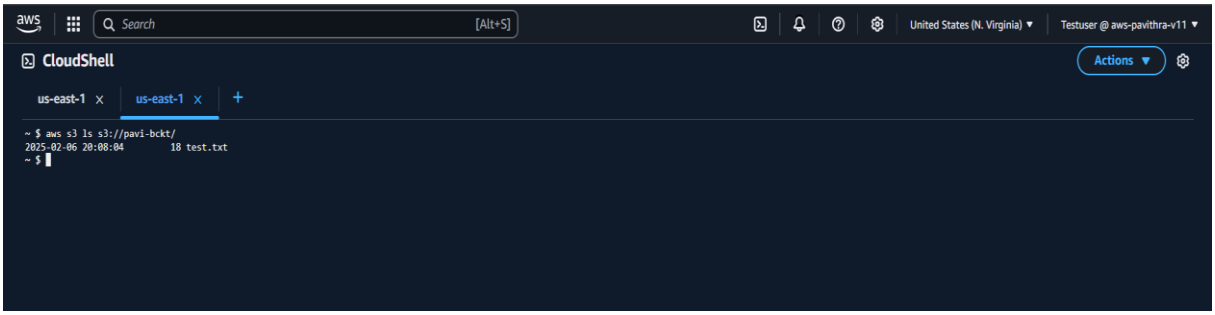
Part 4: Test Access

1. Log in as the developer to the AWS Management Console or AWS CLI.\n2. Verify the roles and policies applied:

Run CLI commands such as:

aws s3 ls s3://example-bucket

- Ensure access matches the permissions defined in the policies.



2. Test MFA by logging in with the generated codes.