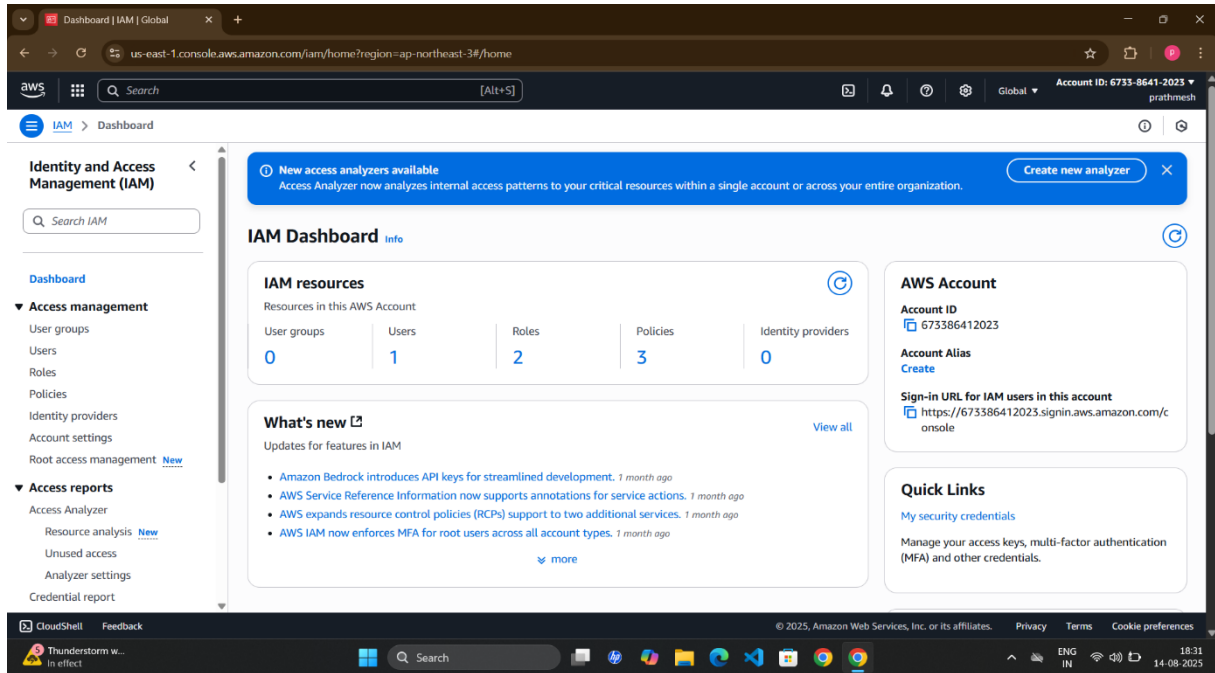


Q.1) Create an IAM policy that allows full access to EC2 within the Mumbai region.

Ans :-

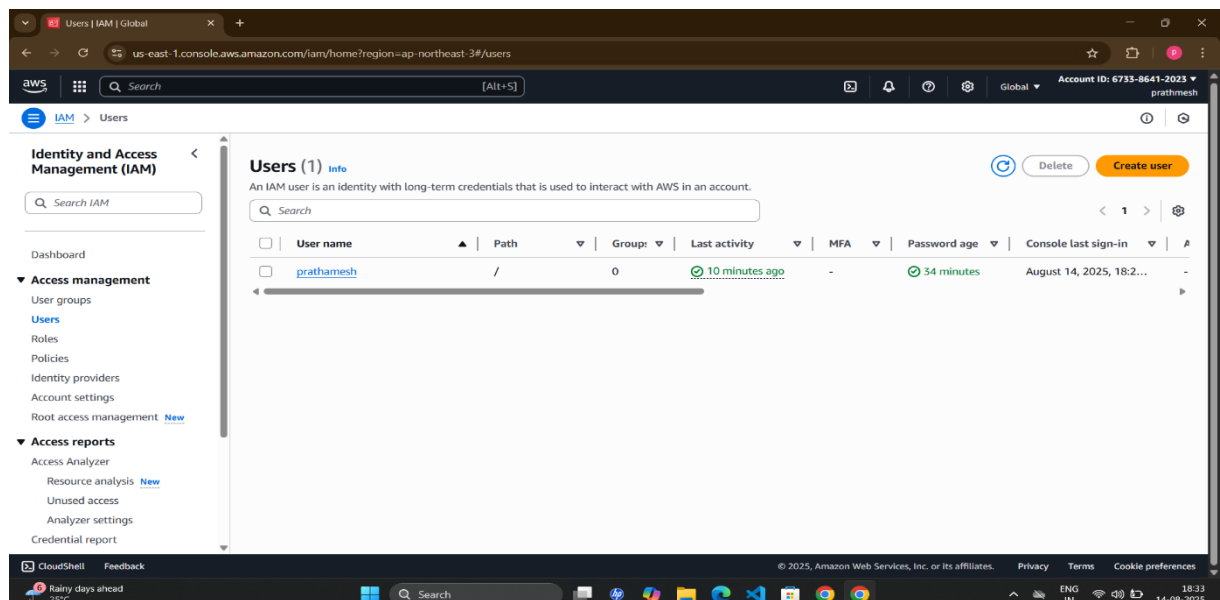
Step 1:- Sign in to AWS Management Console

Step 2:- Open IAM Service



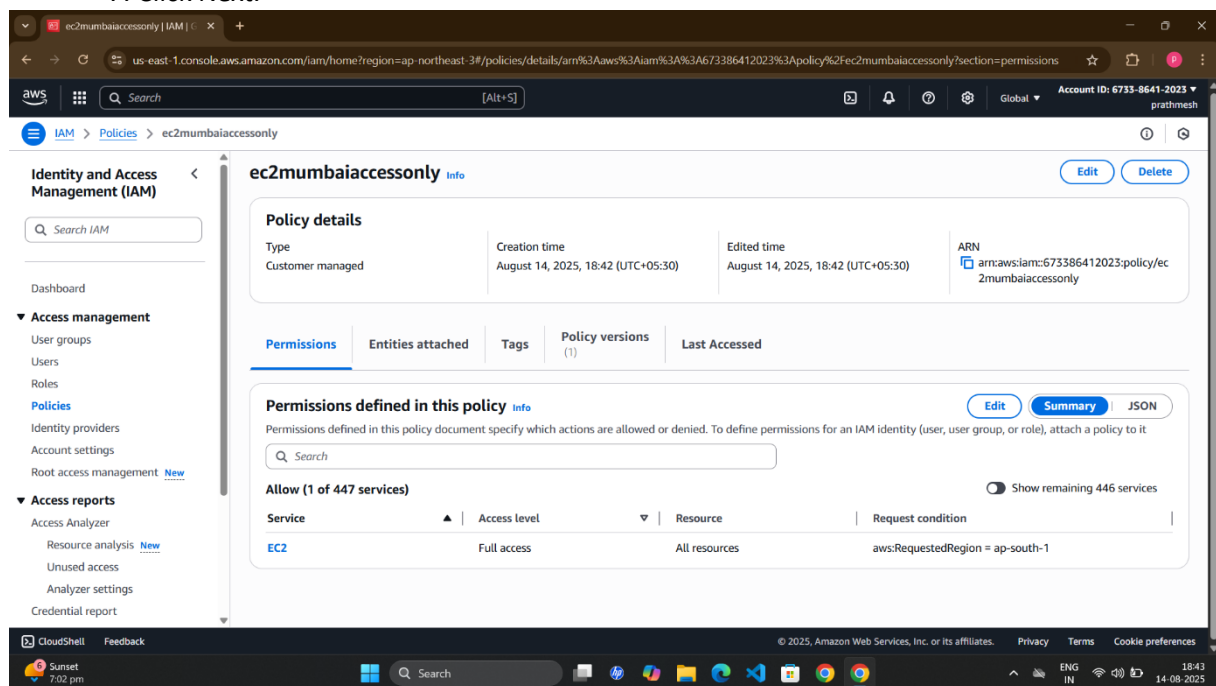
Step 3:- Create a user prathmesh

1. Specify user details
2. Set permissions
3. Review and create



Step 4:- Create a Custom Policy in visual Editor.

1. In IAM dashboard, click Policies in the left menu.
2. Click Create policy.
3. Service: Search and select EC2.
4. Actions: Select All EC2 actions.
5. Resources: Select All resources
6. Request conditions:
 - Click Add condition.
 - Condition key: Search and select aws:RequestedRegion.
 - Operator: StringEquals.
 - Value: Type ap-south-1 (Mumbai region code).
7. Click Next.



Step 5:- Attach the Policy to User prathmesh.

1. In IAM dashboard, click Users → Select prathmesh.
2. Go to Permissions tab → Click Add permissions.
3. Choose Attach policies directly.
4. Search for ec2mumbaiaccessonly → Tick the checkbox.
5. Click Next → Add permissions.

Step 6:- Test the Policy

launching EC2 in another region (N. Virginia)

The screenshot shows the AWS Management Console for the eu-north-1 region (Stockholm). The left sidebar contains the navigation menu with categories like EC2, Images, and Elastic Block Store. The main content area is divided into several sections: Resources, Launch instance, Service health, Zones, and Account attributes. The Resources section displays a table of EC2 resources with columns for resource type and count. The Launch instance section provides a button to launch a new instance. The Service health section shows an error message: "An error occurred: An error occurred retrieving service health information". The Zones section lists available zones. The Account attributes section shows account details.

Resource	Count
Instances (running)	0
Dedicated Hosts	0
Key pairs	0
Security groups	0
Auto Scaling Groups	0
Elastic IPs	0
Load balancers	0
Snapshots	0
Capacity Reservations	0
Instances	0
Placement groups	0
Volumes	0

launching EC2 in Mumbai region (ap-south-1)

The screenshot shows the AWS Management Console for the ap-south-1 region (Mumbai). The layout is similar to the previous screenshot, but the Resources section shows a different set of EC2 resources. The Launch instance section provides a button to launch a new instance. The Service health section shows an error message: "An error occurred: An error occurred retrieving service health information". The Zones section lists available zones. The Account attributes section shows account details.

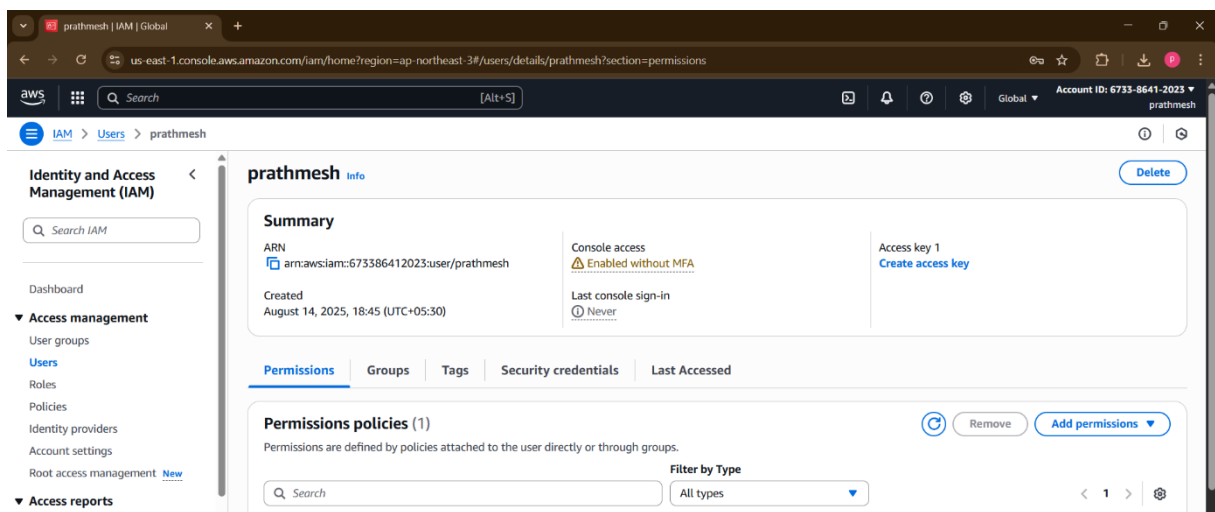
Resource	Count
Instances (running)	0
Dedicated Hosts	0
Key pairs	1
Security groups	2
Auto Scaling Groups	0
Elastic IPs	0
Load balancers	0
Snapshots	0
Capacity Reservations	0
Instances	1
Placement groups	0
Volumes	1

Q.2) Create a Time-Based policy.

Ans :-

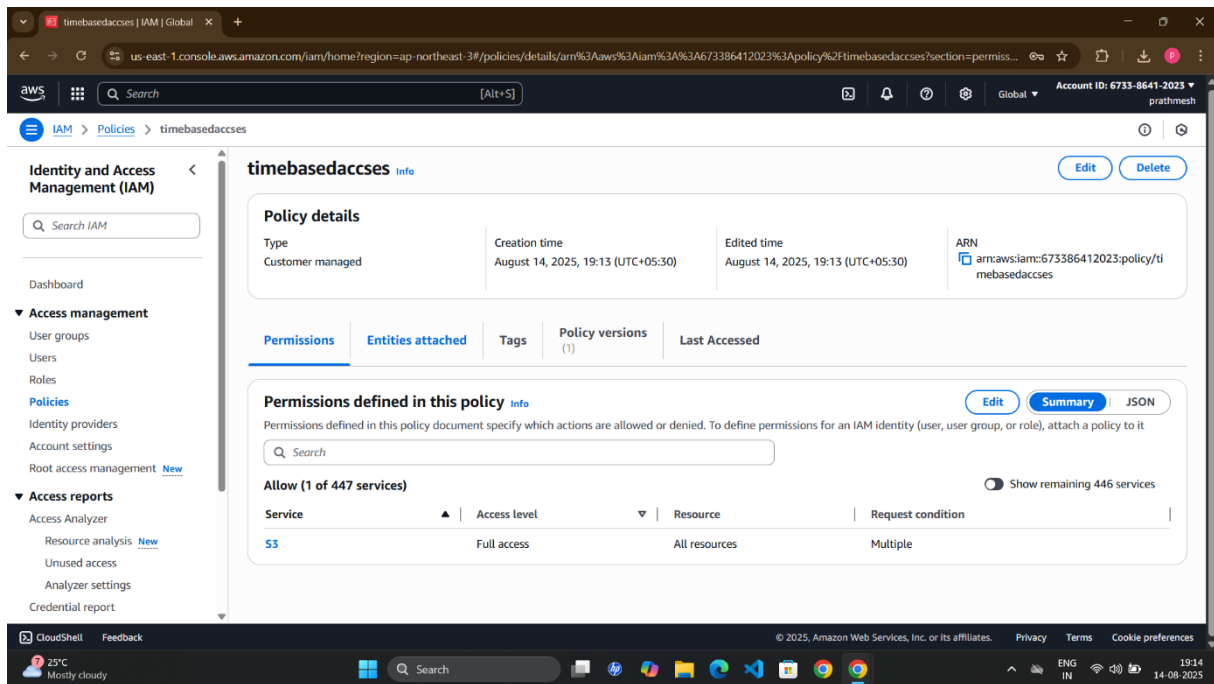
Step 1 :- Create a prathmesh User

1. Specify user details
2. Set permissions
3. Review and create



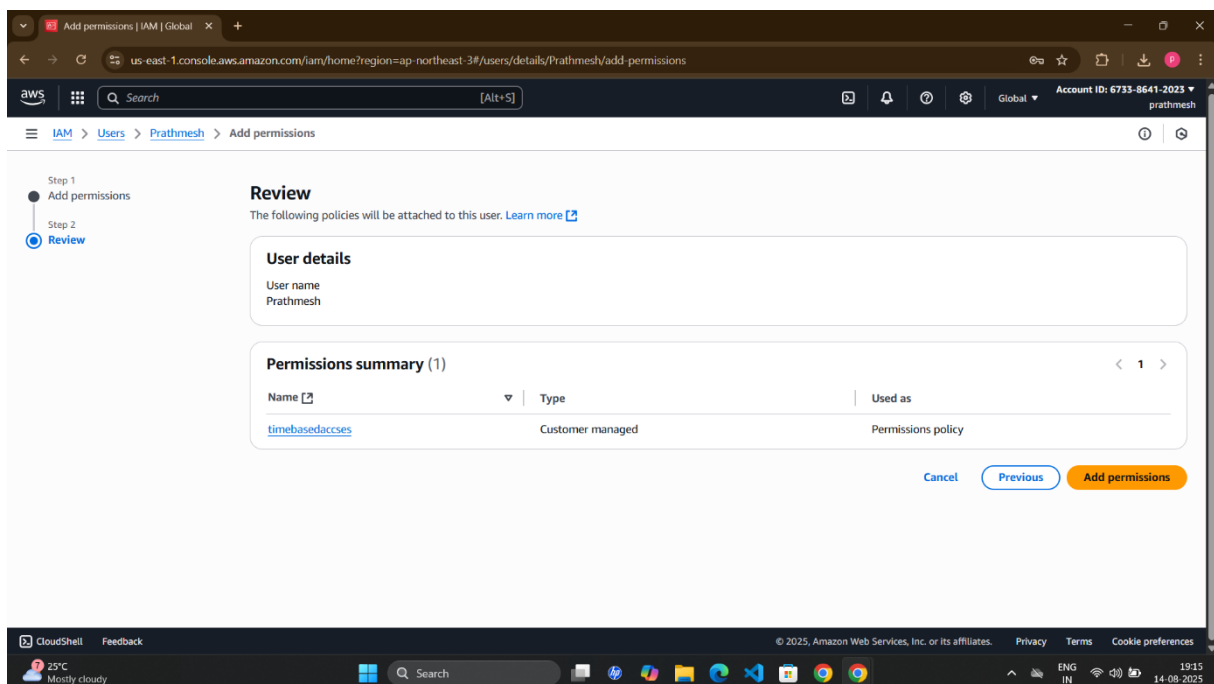
Step 2:- Create a Time-Based Policy

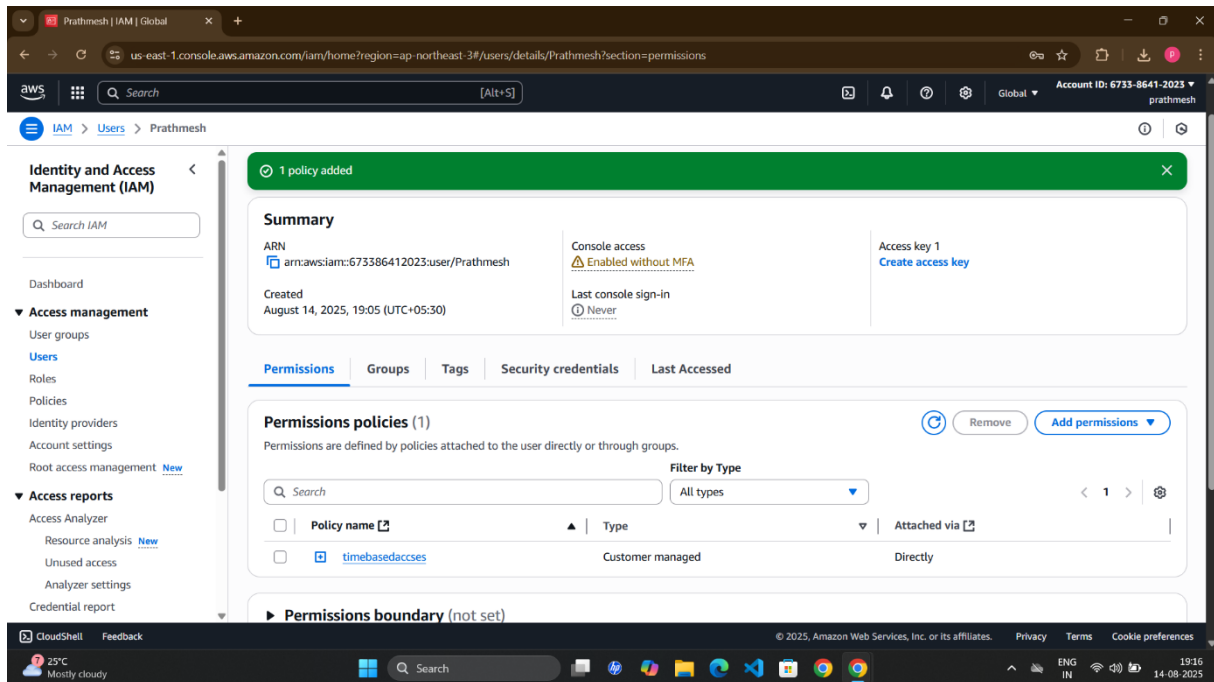
1. In IAM, click Policies
2. Create policy
3. Service: Choose the service S3
4. Actions: Select All S3 actions.
5. Resources: Select All resources
6. Request conditions, Click Add condition:
 - Condition key: aws:CurrentTime
 - Operator: DateGreaterThanEquals
 - Value: 2025-08-14T13:57:00Z
7. Click Add another condition:
 - Condition key: aws:CurrentTime
 - Operator: DateLessThanEquals
 - Value: 2025-08-14T14:57:00Z.



Step 3:- Attach Policy to the Temporary User

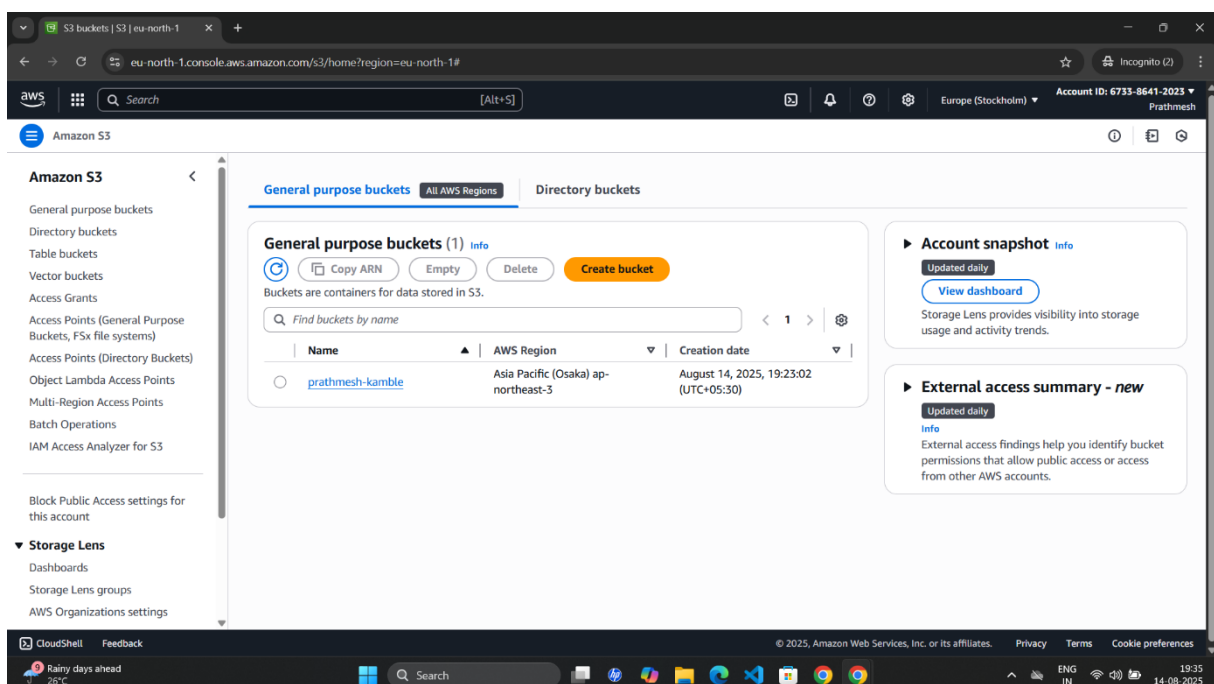
1. In IAM, go to Users → Select temporary-consultant.
2. Go to Permissions → Add permissions → Attach policies directly.
3. Search for TimeBasedAccess → Tick → Add permissions.





Step 4: Test the Policy

Log in as temp during allowed time



After allowed time

