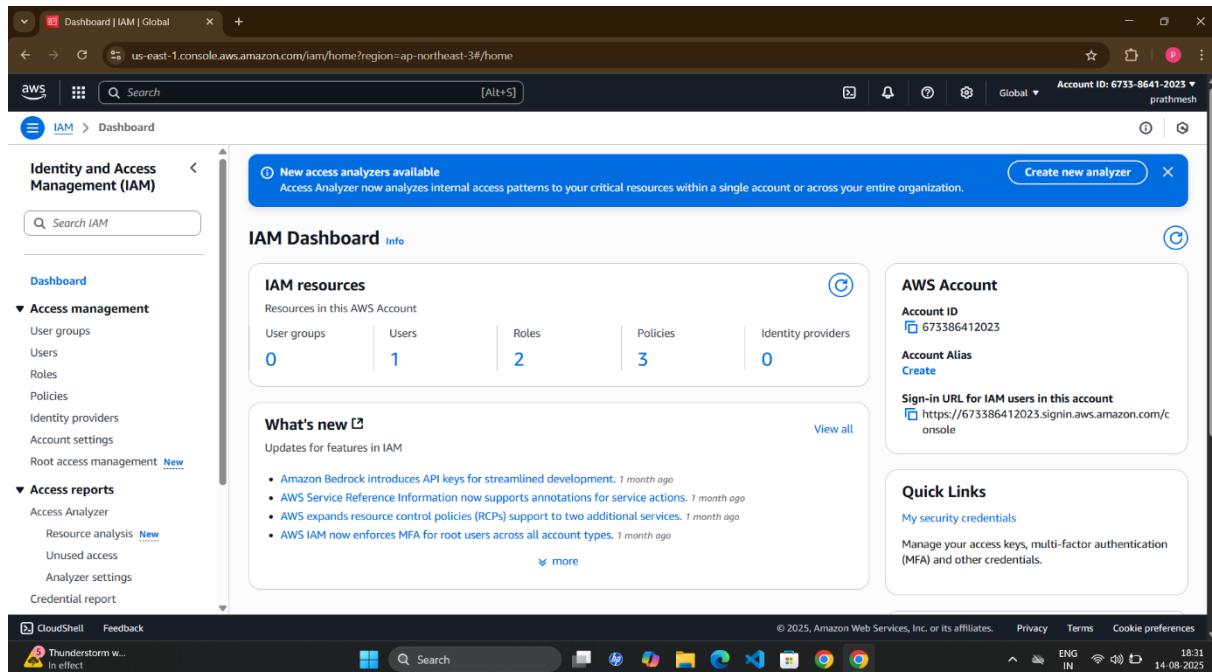


Q.1) Create an IAM policy that allows full access to EC2 within the Mumbai region.

Ans :-

Step 1:- Sign in to AWS Management Console

Step 2:- Open IAM Service



The screenshot shows the IAM Dashboard with the following statistics:

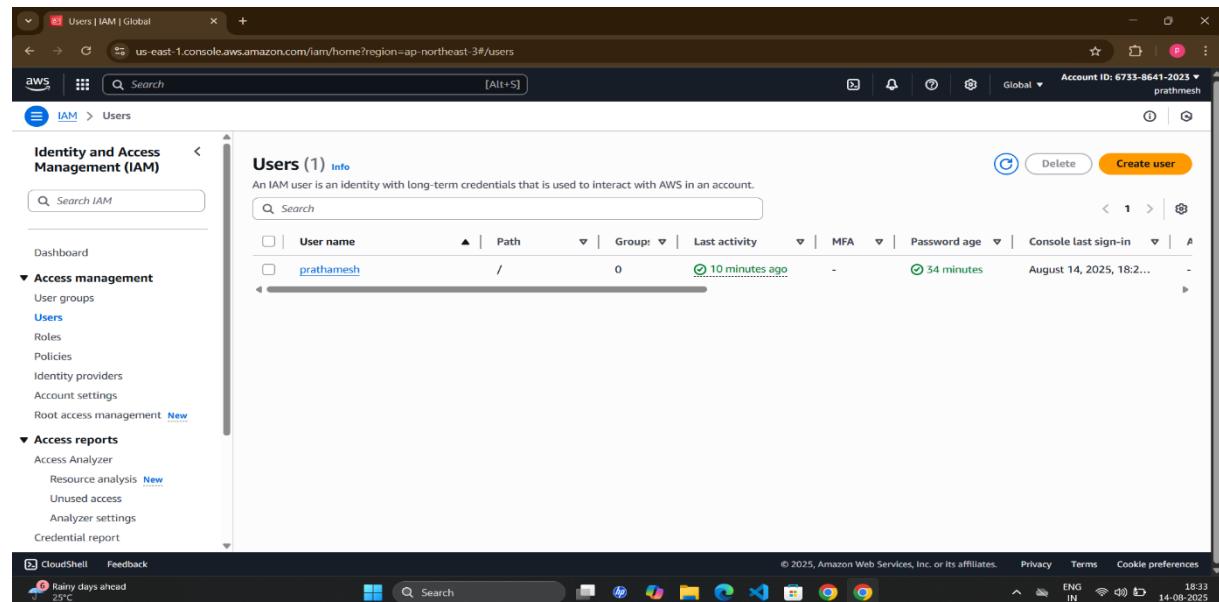
User groups	Users	Roles	Policies	Identity providers
0	1	2	3	0

What's new

- Amazon Bedrock introduces API keys for streamlined development. 1 month ago
- AWS Service Reference Information now supports annotations for service actions. 1 month ago
- AWS expands resource control policies (RCPs) support to two additional services. 1 month ago
- AWS IAM now enforces MFA for root users across all account types. 1 month ago

Step 3:- Create a user prathmesh

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



The screenshot shows the IAM Users page with one user listed:

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
prathmesh	/	0	10 minutes ago	-	54 minutes	August 14, 2025, 18:23...

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.

The screenshot shows the AWS IAM console with the policy named 'ec2mumbaiaccessonly'. The 'Policy details' section shows it is a Customer managed policy created on August 14, 2025. The 'Permissions' tab is selected, showing one rule: 'Allow (1 of 447 services)' for 'EC2' with 'Full access' to 'All resources' under the condition 'aws:RequestedRegion = ap-south-1'.

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 EC2 Dashboard for the Europe (Stockholm) Region. The left sidebar includes links for Dashboard, Instances, Images, and Elastic Block Store. The main content area displays a summary of resources (Instances running: 0, Auto Scaling Groups: 0, Capacity Reservations: 0), a Launch instance section with 'Launch instance' and 'Migrate a server' buttons, a Service health section showing an error, and a Zones section. A right sidebar details EC2 Free Tier offers, noting an error for the 'GetFreeTierUsage' action.

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

The screenshot shows the AWS EC2 Dashboard for the Asia Pacific (Mumbai) Region. The left sidebar is identical to the previous screenshot. The main content area displays a summary of resources (Instances running: 0, Auto Scaling Groups: 0, Capacity Reservations: 0), a Launch instance section with 'Launch instance' and 'Migrate a server' buttons, a Service health section showing an error, and a Zones section. A right sidebar details EC2 Free Tier offers, noting an error for the 'GetFreeTierUsage' action.

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

The screenshot shows the AWS IAM User Details page for a user named 'prathmesh'. The left sidebar shows navigation options like Dashboard, Access management, and Access reports. The main panel displays the user's ARN (arn:aws:iam::673386412023:user/prathmesh), creation date (August 14, 2025, 18:45 UTC+05:30), and console access status (Enabled without MFA). It also shows a single access key created. The 'Permissions' tab is selected, showing one attached policy. A search bar and filter dropdown are visible at the bottom of the permissions section.

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: DateGreaterThanOrEqual
 - Value: 2025-08-14T13:57:00Z
7. Click Add another condition:
 - Condition key: aws:CurrentTime
 - Operator: DateLessThanOrEqual
 - Value: 2025-08-14T14:57:00Z.

timebasedaccses

Policy details

Type: Customer managed

Creation time: August 14, 2025, 19:13 (UTC+05:30)

Edited time: August 14, 2025, 19:13 (UTC+05:30)

ARN: arn:aws:iam::673386412023:policy/timebasedaccses

Permissions **Entities attached** **Tags** **Policy versions (1)** **Last Accessed**

Permissions defined in this policy

Allow (1 of 447 services)

Service	Access level	Resource	Request condition
S3	Full access	All resources	Multiple

Show remaining 446 services

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.

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: Prathmesh

Permissions summary (1)

Name	Type	Used as
timebasedaccses	Customer managed	Permissions policy

Add permissions

Prathmesh | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=ap-northeast-3#/users/details/Prathmesh?section=permissions

IAM > Users > Prathmesh

Identity and Access Management (IAM)

Summary

ARN: arn:aws:iam::673386412023:user/Prathmesh

Console access: Enabled without MFA

Created: August 14, 2025, 19:05 (UTC+05:30)

Last console sign-in: Never

Access key 1: Create access key

Permissions Groups Tags Security credentials Last Accessed

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

Policy name: timebasedacces

Type: Customer managed

Attached via: Directly

Permissions boundary (not set)

CloudShell Feedback

25°C Mostly cloudy

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG IN 19:16 14-08-2025

Step 4: Test the Policy

Log in as temp during allowed time

S3 buckets | S3 | eu-north-1

eu-north-1.console.aws.amazon.com/s3/home?region=eu-north-1#

Amazon S3

General purpose buckets All AWS Regions Directory buckets

General purpose buckets (1) [Info](#)

[Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	Creation date
prathmesh-kamble	Asia Pacific (Osaka) ap-northeast-3	August 14, 2025, 19:23:02 (UTC+05:30)

Account snapshot [Info](#)

Updated daily

[View dashboard](#)

Storage Lens provides visibility into storage usage and activity trends.

External access summary - new [Info](#)

Updated daily

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

CloudShell Feedback

Rainy days ahead 26°C

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG IN 19:35 14-08-2025

After allowed time

The screenshot shows the AWS S3 console interface. The left sidebar is titled "Amazon S3" and includes sections for "General purpose buckets" (with options like Directory buckets, Table buckets, Vector buckets, Access Grants, Access Points (General Purpose Buckets, FSx file systems), Access Points (Directory Buckets), Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3) and "Storage Lens" (with options like Dashboards, Storage Lens groups, AWS Organizations settings). The main content area is titled "General purpose buckets" and shows a table with one row. The first column contains a red-bordered box with an "Error" icon and the text "Access Denied". A button labeled "Diagnose with Amazon Q" is also present. To the right of the table are two callout boxes: "Account snapshot" (updated daily) which links to the "View dashboard" and provides information about Storage Lens; and "External access summary - new" (info) which links to the "Info" section and describes external access findings. The browser's address bar shows the URL <https://eu-north-1.console.aws.amazon.com/s3/buckets?region=eu-north-1&bucketType=general>. The system tray at the bottom indicates the date as 14-08-2025.

