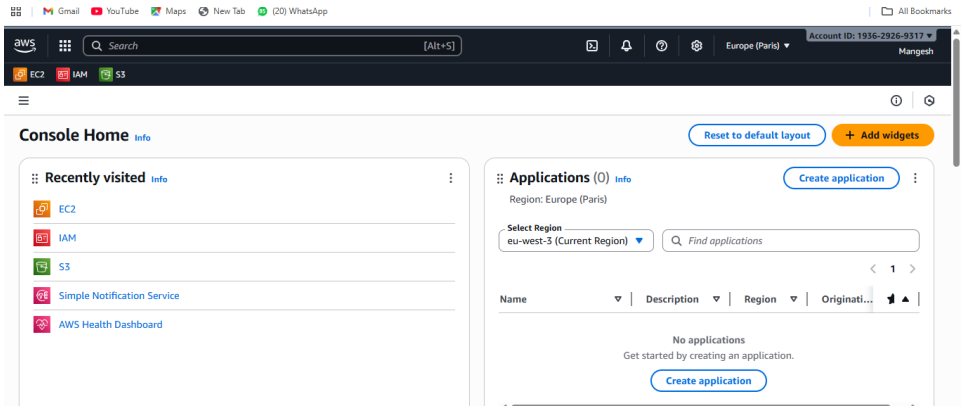
Time Based Policy using IAM Service

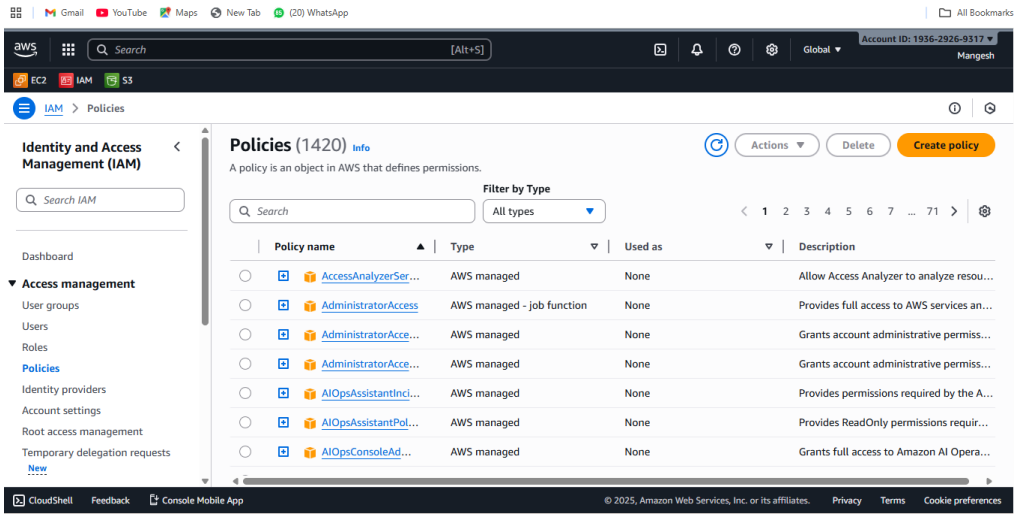
In AWS IAM you can make a time-based policy using policy conditions, so that after the time expires the policy remains attached but becomes inaccessible (inactive).

Steps :

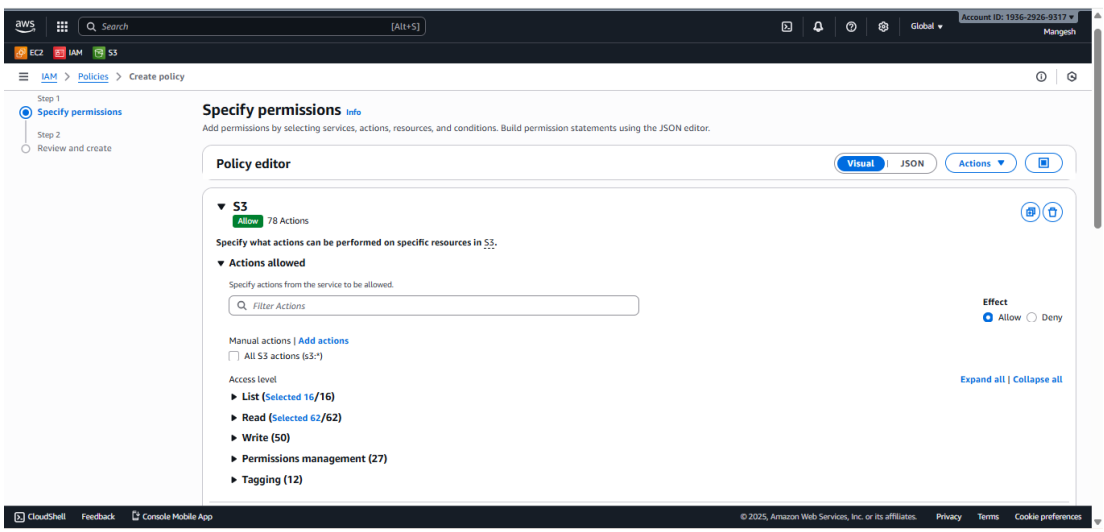
Step 1. Sign in to the AWS Management Console with an account that can create IAM policies.



Step 2. Go into IAM Service , In the left menu click Policies.



Step 3. Click Create policy, Choose Visual editor tab, Select service Ex. S3 and Select the Actions you want to allow (ex. List,read,etc).



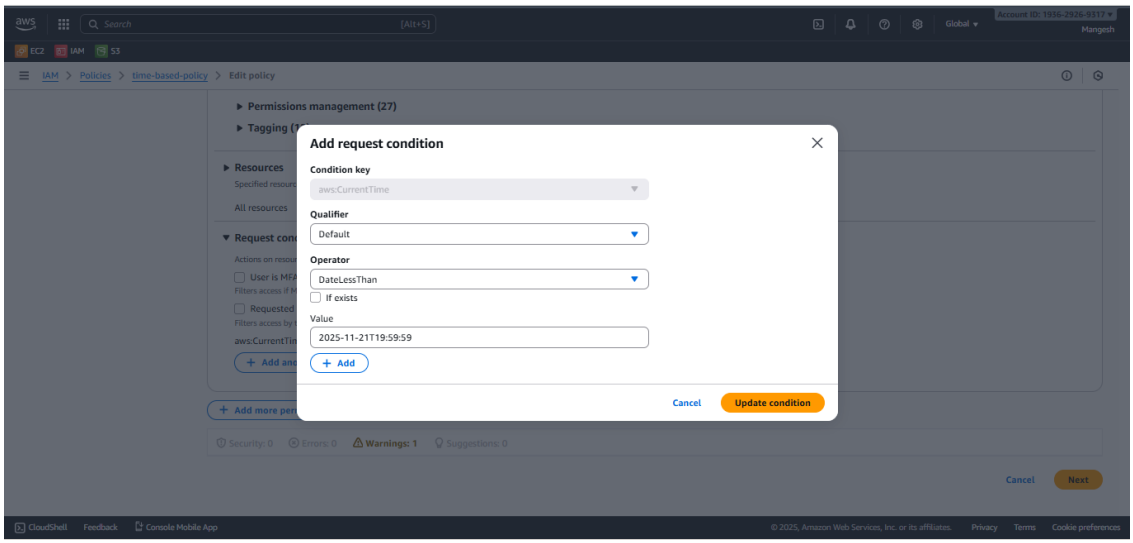
Step 4. Select the resources (All resources or specific buckets). → Scroll down to Request conditions → add condition

Condition key category → Date Operators

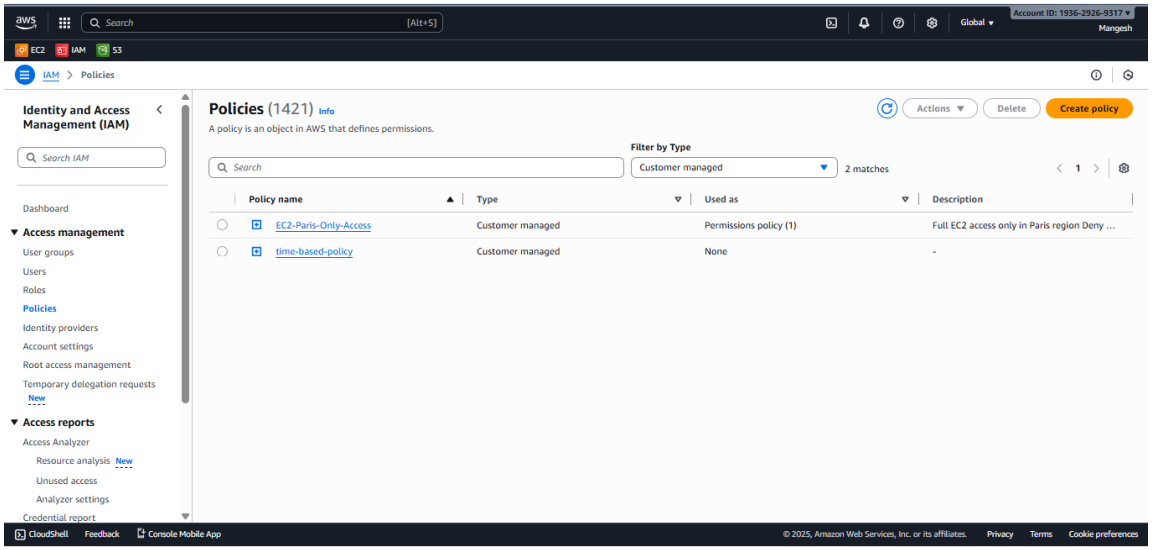
Condition key → aws:CurrentTime

Enter date and time in UTC format.

Add condition and click next.

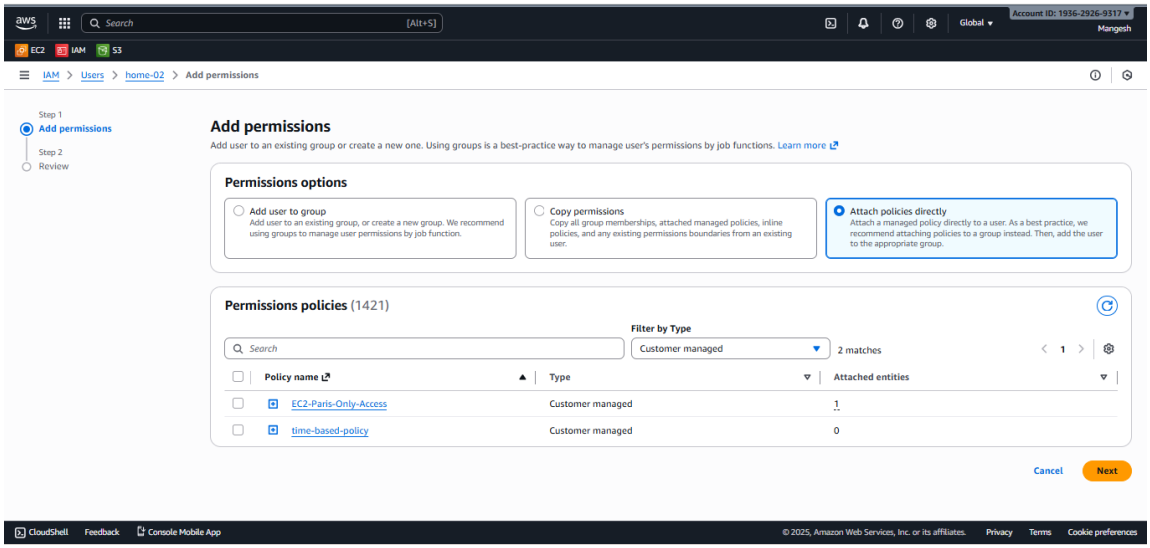


Step 5 . Review and Create policy.

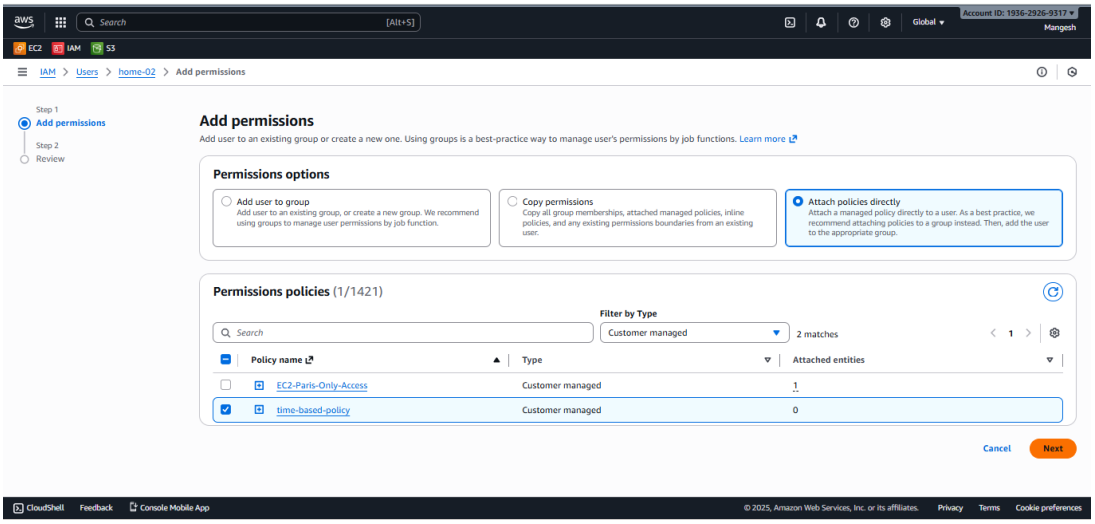


Policy created ‘ time-based-policy’

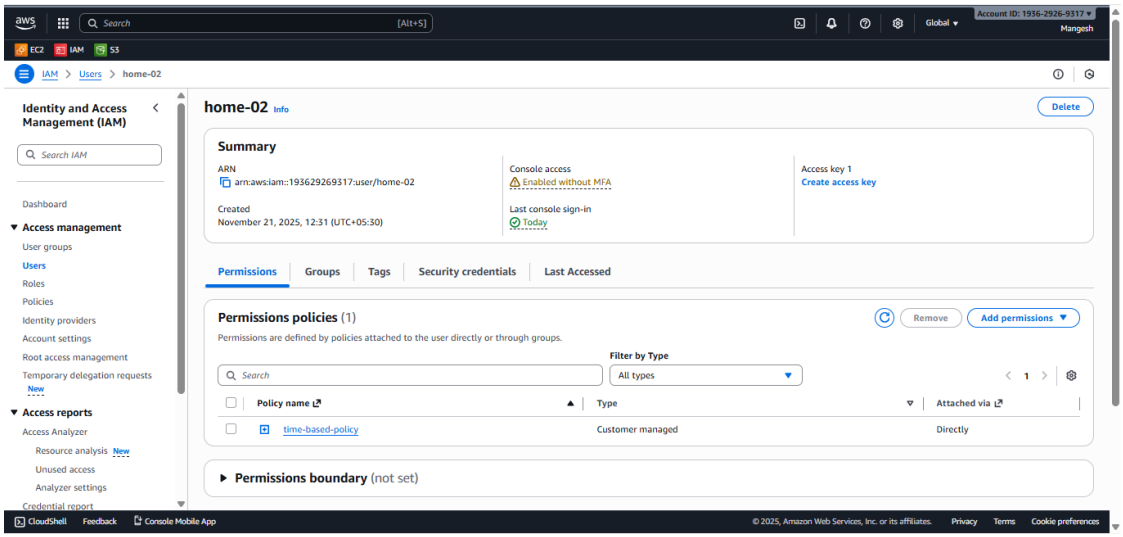
Step 6. Go to IAM →Users →home-02 →Add Permissions



Step 7 . Add Permissions → Attach Policies directly → Select your policy name → Tik the checkbox → Click Add Permissions.



Step 8. Review the policy that we attached.

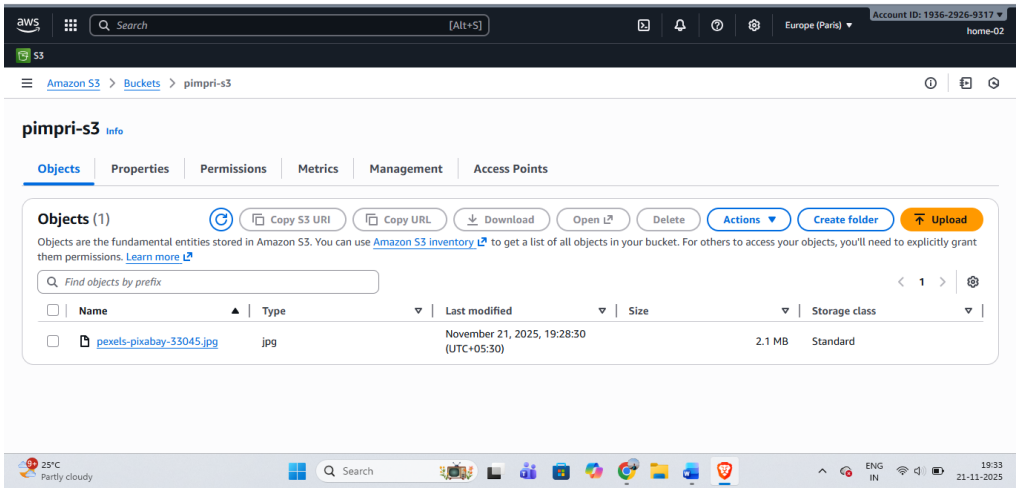


Policy has been attached to IAM user (home-02).

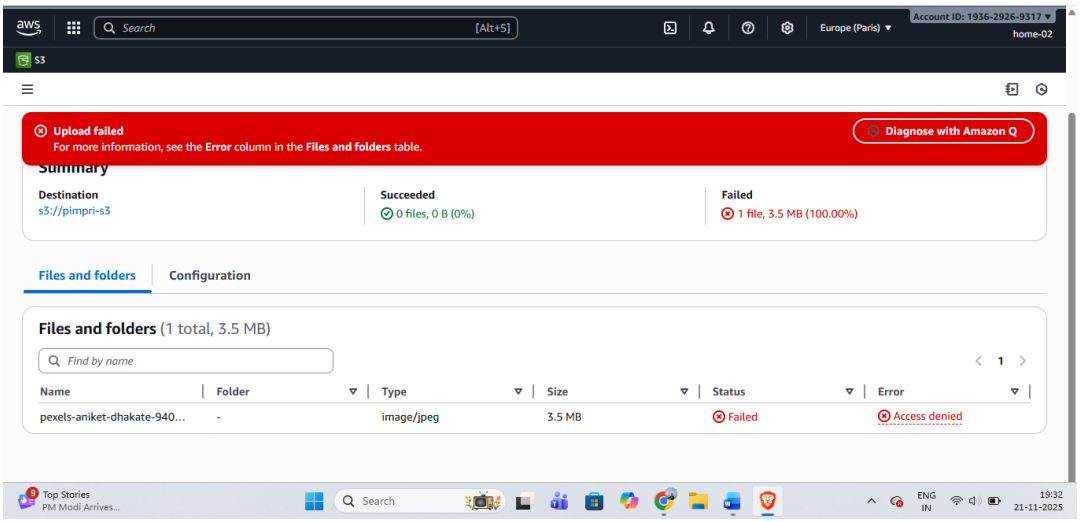
Step 9. Try to Access S3 bucket and create a S3 bucket .

IAM user read and list the S3 bucket.IAM user have an access to read and list the bucket .

IAM have access this bucket within the time 19:33:55 . → Action will succeed.



But IAM user cannot have an access to upload the data in the bucket because it has only read and list access.



Step 10. Check after the time limit of access is expired. → Access Denied.