Task

Q. 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).

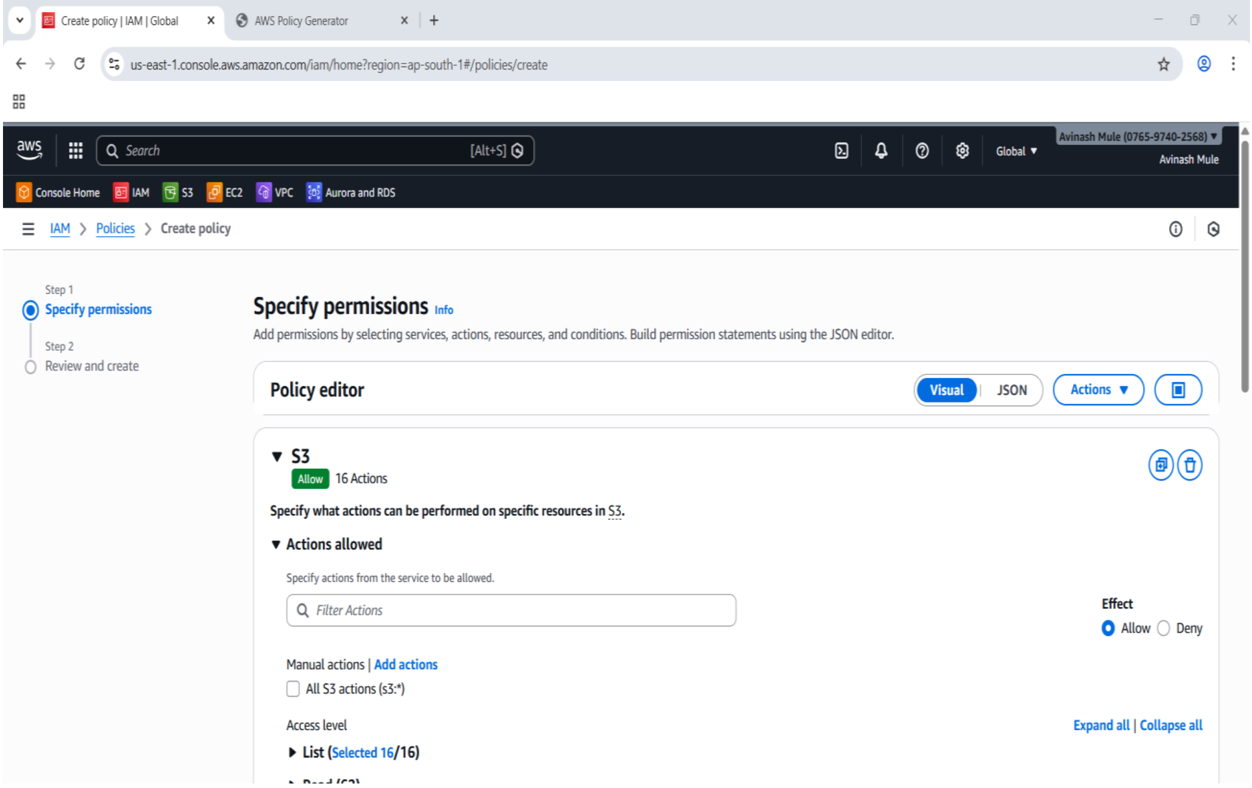
Steps:

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).

Select all actions .


Create policy | IAM | Global
AWS Policy Generator
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
aws
Search
[Alt+S]
Global ▾
Avinash Mule (0765-9740-2568) ▾
Avinash Mule
Console Home
IAM
S3
EC2
VPC
Aurora and RDS
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Info
Visual
JSON
Actions ▾
Add actions
Expand all | Collapse all

Specify permissions

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

▾ S3

Allow 16 Actions

Specify what actions can be performed on specific resources in S3.

▾ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect

● Allow ○ Deny

Manual actions | Add actions

□ All S3 actions (s3:*)

Access level

▸ List (Selected 16/16)

▸ Read (63)

Step 4. Select the resources (All resources or specific buckets). ◊ Scroll down to

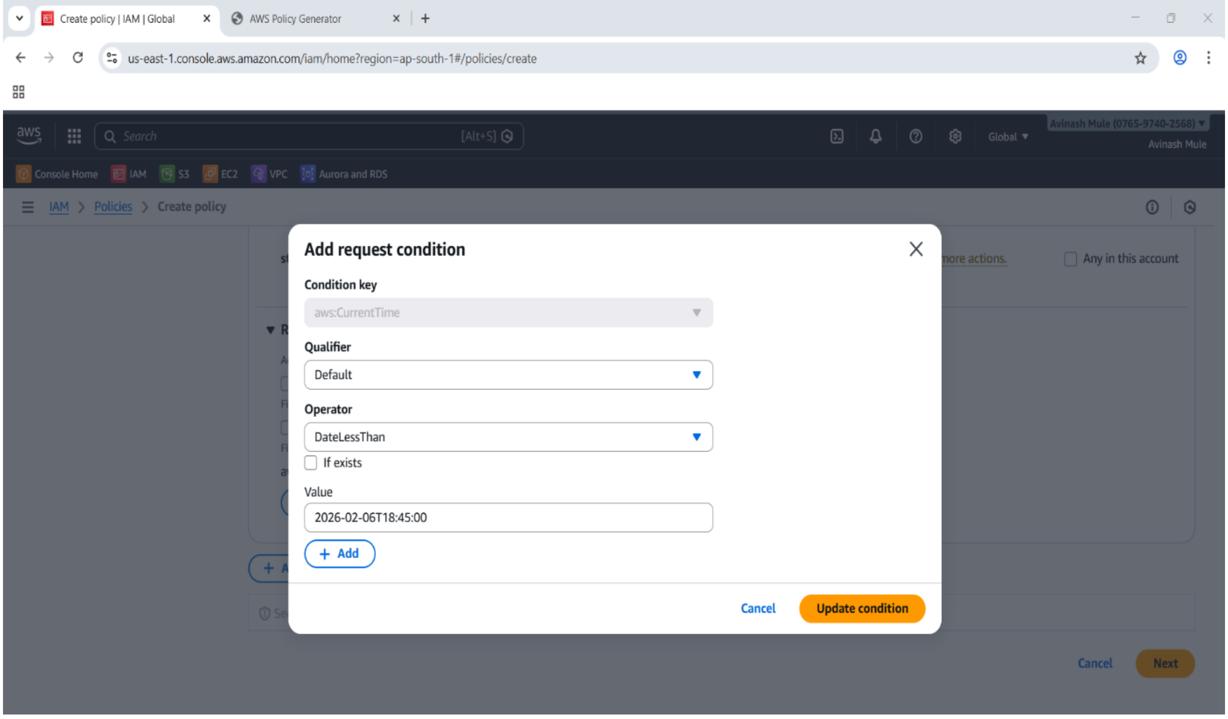
Request conditions > add condition

Condition key category > Date Operators

Condition key > aws:CurrentTime

Enter date and time in UTC format.

Add condition and click next.



Create policy | IAM | Global
AWS Policy Generator
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Search
[Alt+S]
Global ▾
Avinash Mule (0765-9740-2568) ▾
Avinash Mule
Console Home
IAM
S3
EC2
VPC
Aurora and RDS
IAM > Policies > Create policy
more actions.
Any in this account
Cancel
Next

Add request condition

Condition key: aws:CurrentTime

Qualifier: Default

Operator: DateLessThan

□ If exists

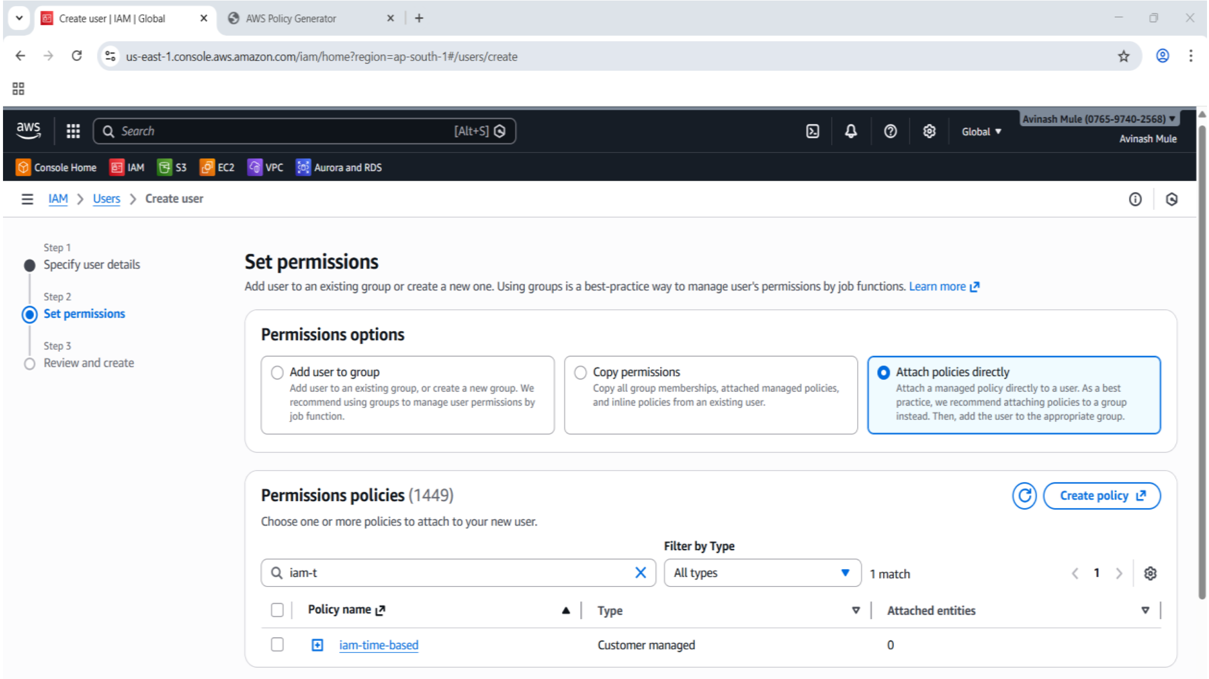
Value: 2026-02-06T18:45:00

+ Add
Cancel
Update condition

Step 5 . Review and Create policy.

Policy created “time-based-policy

Step 6. Create an IAM user and attach this policy to the user.


Create user | IAM | Global
AWS Policy Generator
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Search
[Alt+S]
Global
Avinash Mule (0765-9740-2568)
Avinash Mule
Console Home
IAM
S3
EC2
VPC
Aurora and RDS
IAM > Users > Create user

Step 1
● Specify user details

Step 2
● Set permissions

Step 3
○ Review and create

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1449)

Choose one or more policies to attach to your new user.

Filter by Type

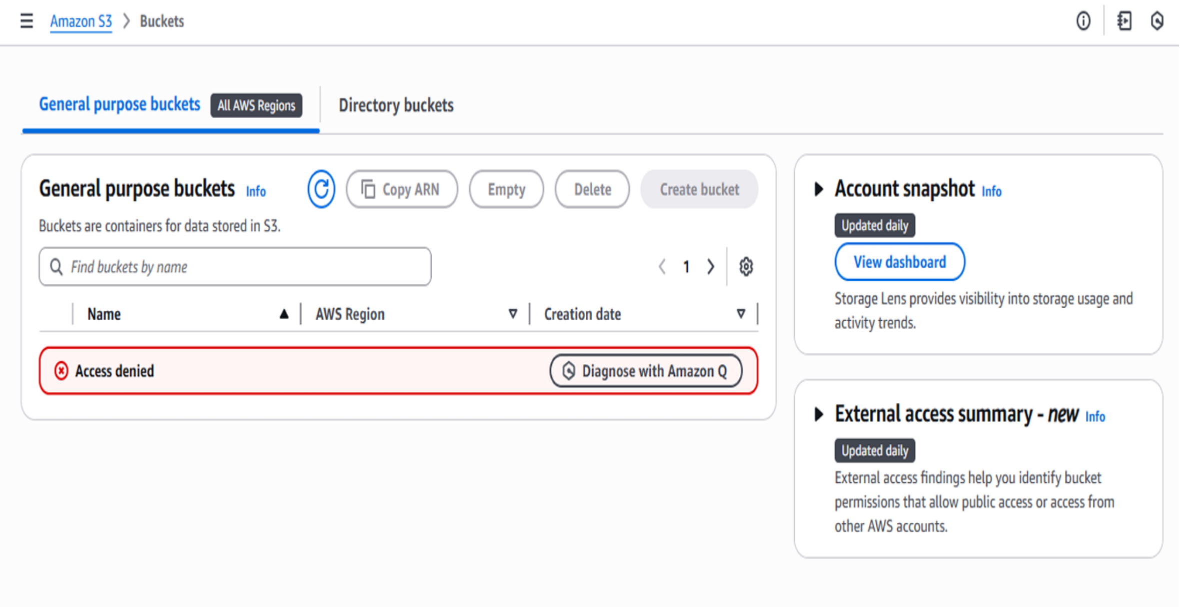
iam-t | All types | 1 match

□	Policy name	Type	Attached entities
□	iam-time-based	Customer managed	0

Successfully attached the policy to the user .

Now wait until the time expires and after the time expire try to access the bucket.

Step 7 . Try to create the the s3 bucket.



General purpose buckets

Buckets are containers for data stored in S3.

Name	AWS Region	Creation date

Access denied

Storage Lens provides visibility into storage usage and activity trends.

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

After the time limit of access is expired. > Access Denied.