Grant User Full Access of S3 Permission for Only 30 Minutes.

Use Cases:

1. Temporary File Uploads or Downloads

Allow users to upload or download files securely for a short period without permanent access to your S3 bucket.

Example: A partner or vendor needs to upload data for a one-time project.

2. Secure Data Processing

Enable a third-party service or application to process data stored in an S3 bucket within a limited time frame.

Example: Grant access to a machine learning model hosted externally to train on specific datasets.

3. Disaster Recovery or Backup Access

Provide short-term access for recovery purposes in case of emergencies.

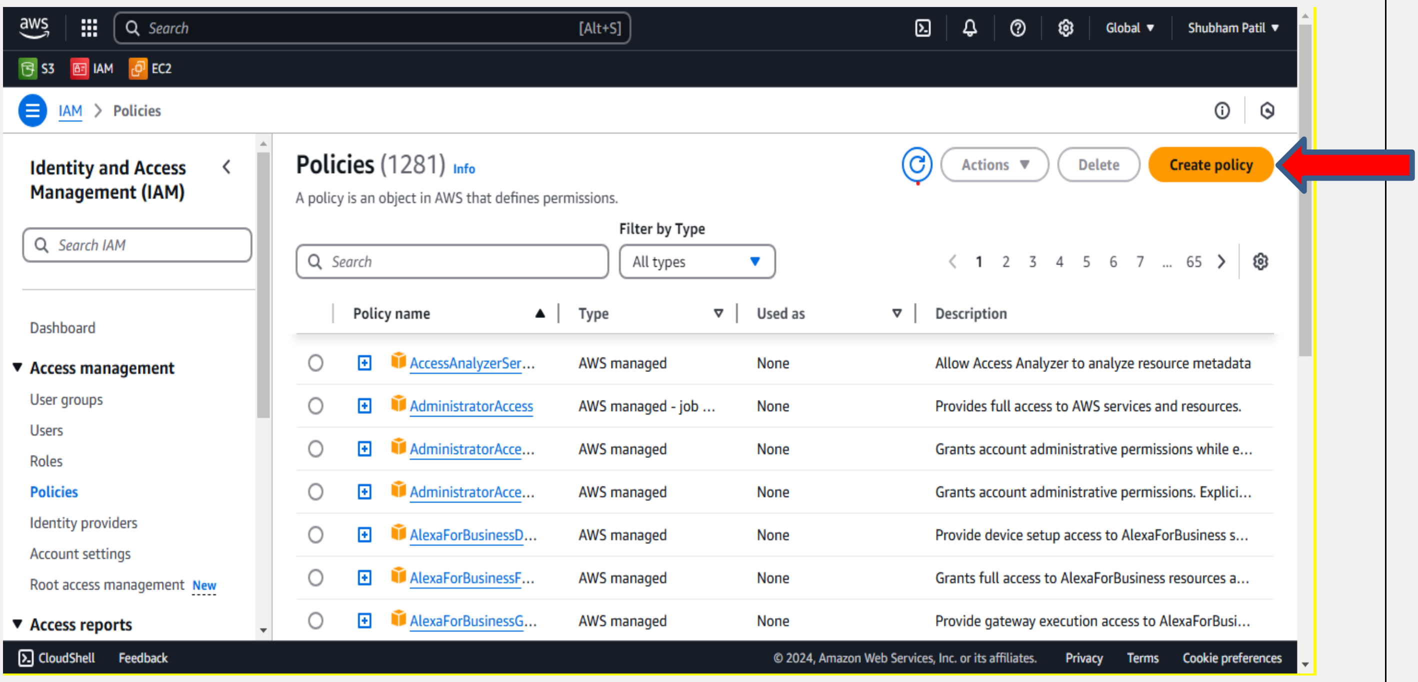
Example: A system administrator needs to restore files but shouldn't have long-term access.

4. Temporary Developer or Tester Access

Developers or QA testers may need full access to S3 for troubleshooting or feature validation.

Example: Debugging issues related to an application interacting with S3.

Step:1- Go to IAM→Policies and Create new policy.

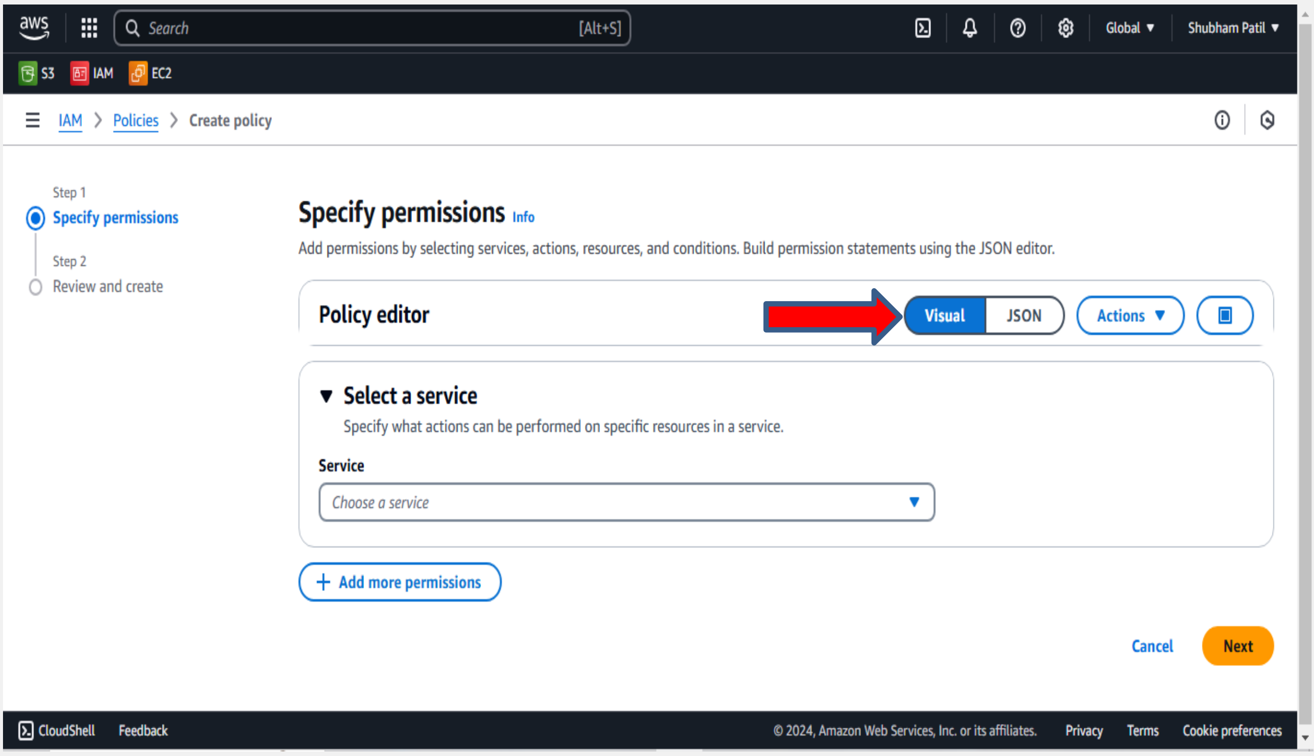


Policies (1281) Info

A policy is an object in AWS that defines permissions.

	Policy name ▲	Type ▽	Used as ▽	Description
○	AccessAnalyzerSer...	AWS managed	None	Allow Access Analyzer to analyze resource metadata
○	AdministratorAccess	AWS managed - job ...	None	Provides full access to AWS services and resources.
○	AdministratorAcce...	AWS managed	None	Grants account administrative permissions while e...
○	AdministratorAcce...	AWS managed	None	Grants account administrative permissions. Explici...
○	AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaForBusiness s...
○	AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness resources a...
○	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to AlexaForBusi...

Step:2- Select Visual policy editor and Select s3 Service then Allow all Actions, Specify all Resources.



Specify permissions Info

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

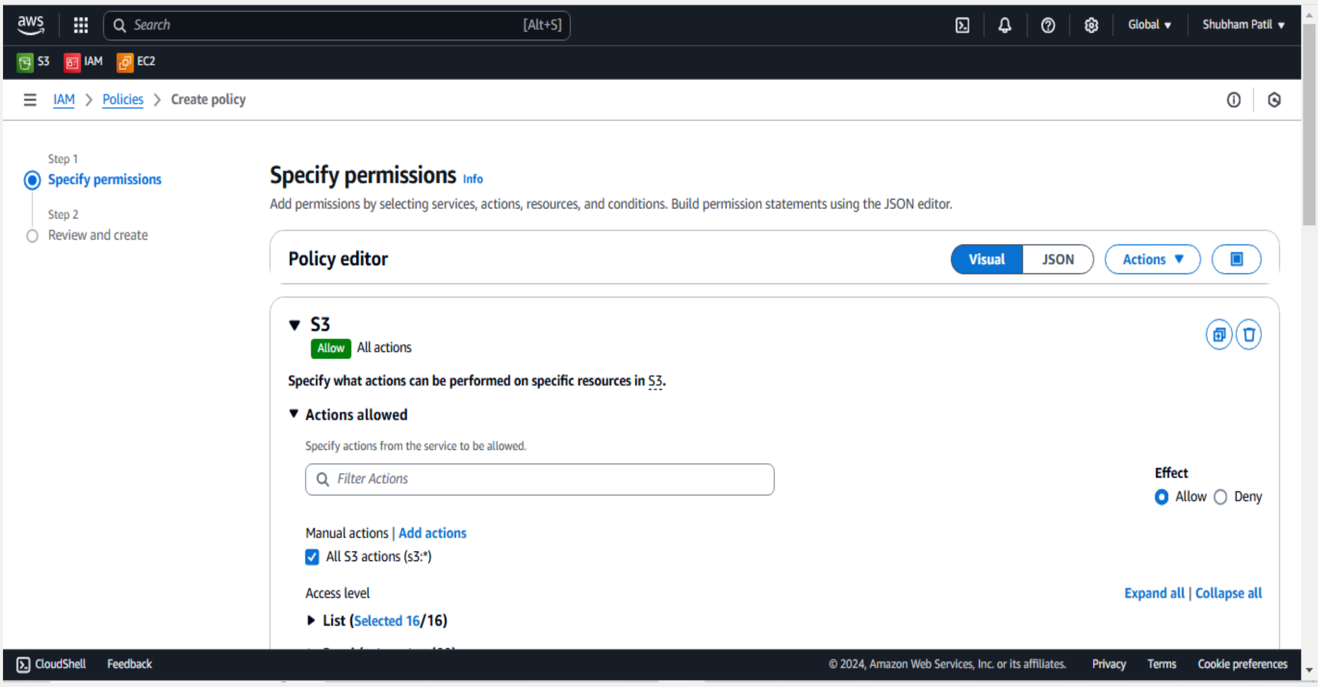
Policy editor

▼ Select a service

Specify what actions can be performed on specific resources in a service.

Service

Choose a service ▼



Step 1
● Specify permissions

Step 2
○ Review and create

Specify permissions Info

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

Policy editor

▼ **S3**

Allow All 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

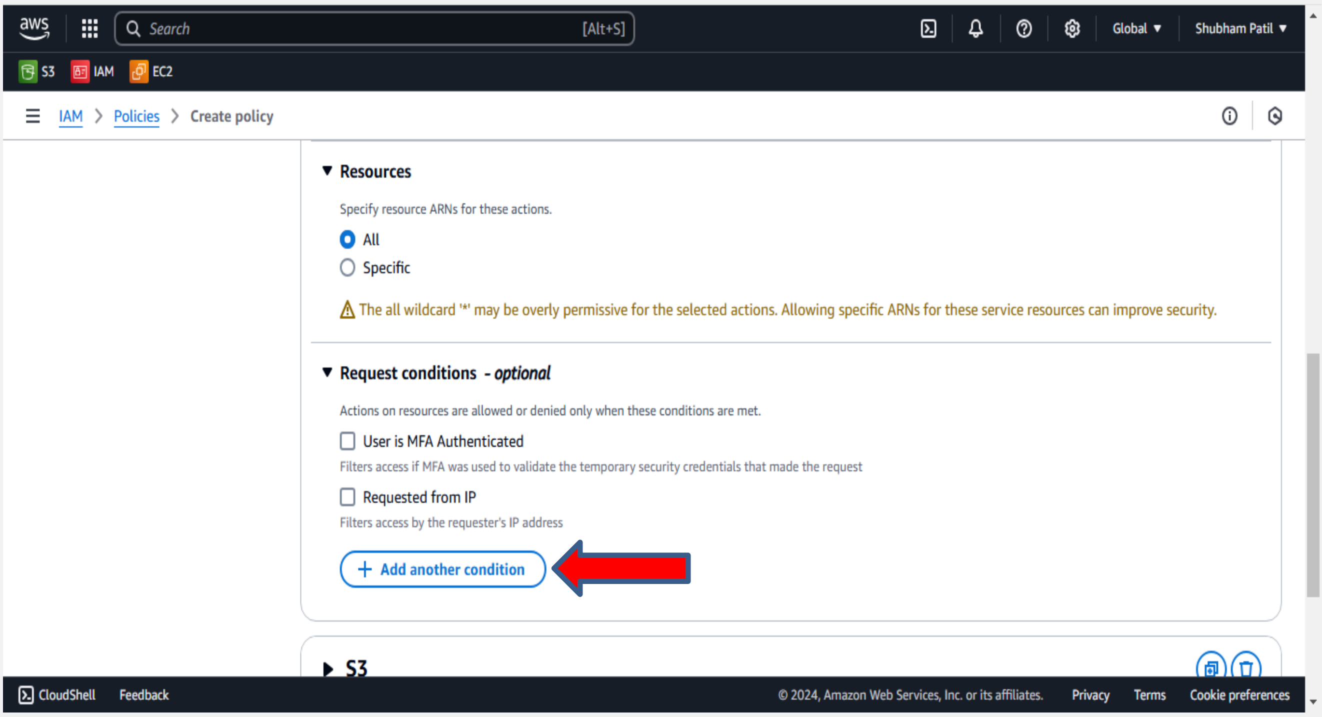
☑ All S3 actions (s3:*)

Access level

Expand all | Collapse all

▶ List (Selected 16/16)

Step:3- Now go to Request conditions option and Add another condition



▼ **Resources**

Specify resource ARNs for these actions.

● All

○ Specific

⚠ The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▼ **Request conditions** - *optional*

Actions on resources are allowed or denied only when these conditions are met.

□ User is MFA Authenticated

Filters access if MFA was used to validate the temporary security credentials that made the request

□ Requested from IP

Filters access by the requester's IP address

Step:4- Select Condition key=aws:CurrentTime

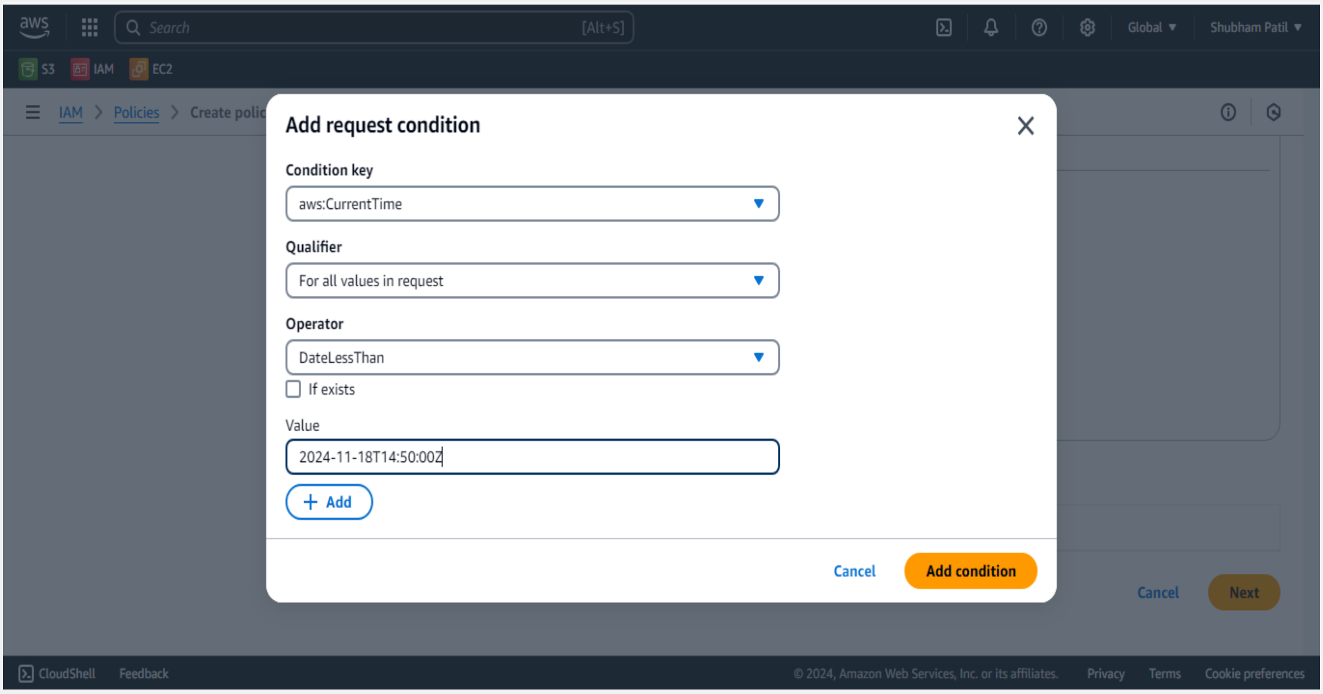
Qualifier= For all values in request

Operator= DateLessThan

Value=2024-11-17T14:50:00Z

# Here value is given in UTC format to give access for only 30 minutes from now.

And Add condition



Add request condition

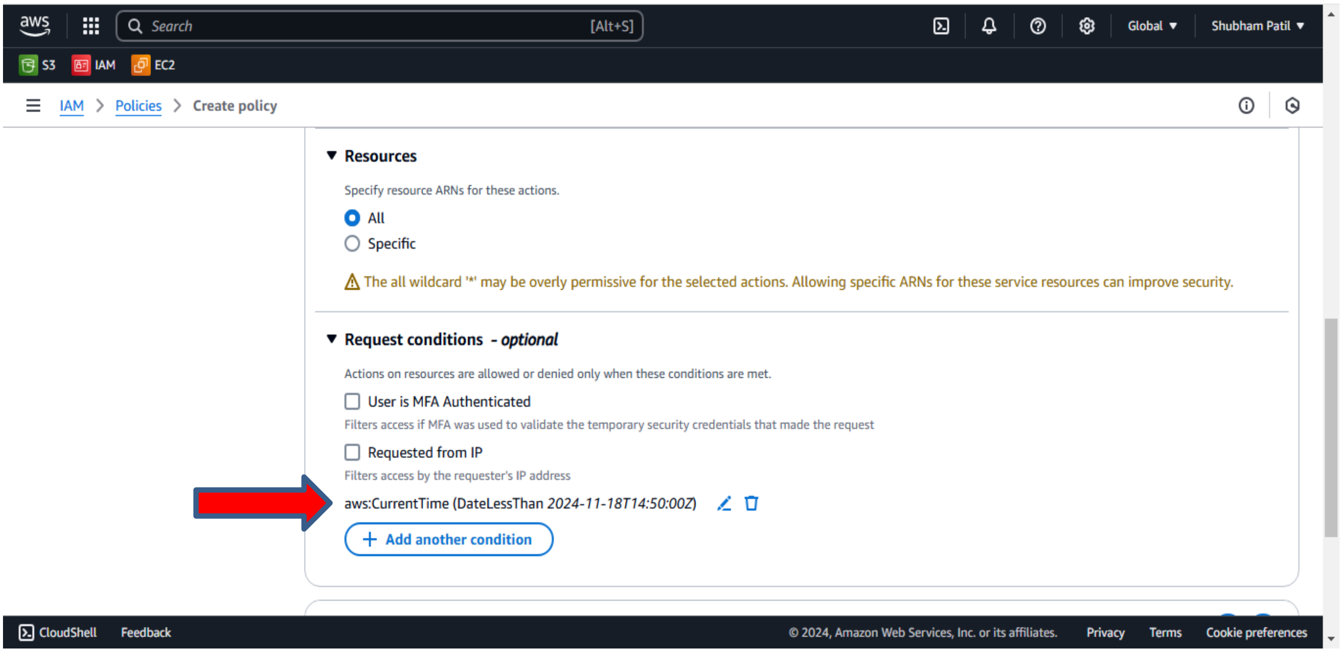
Condition key: aws:CurrentTime

Qualifier: For all values in request

Operator: DateLessThan

□ If exists

Value: 2024-11-18T14:50:00Z



▼ Resources

Specify resource ARNs for these actions.

● All

○ Specific

⚠ The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▼ Request conditions - *optional*

Actions on resources are allowed or denied only when these conditions are met.

□ User is MFA Authenticated

Filters access if MFA was used to validate the temporary security credentials that made the request

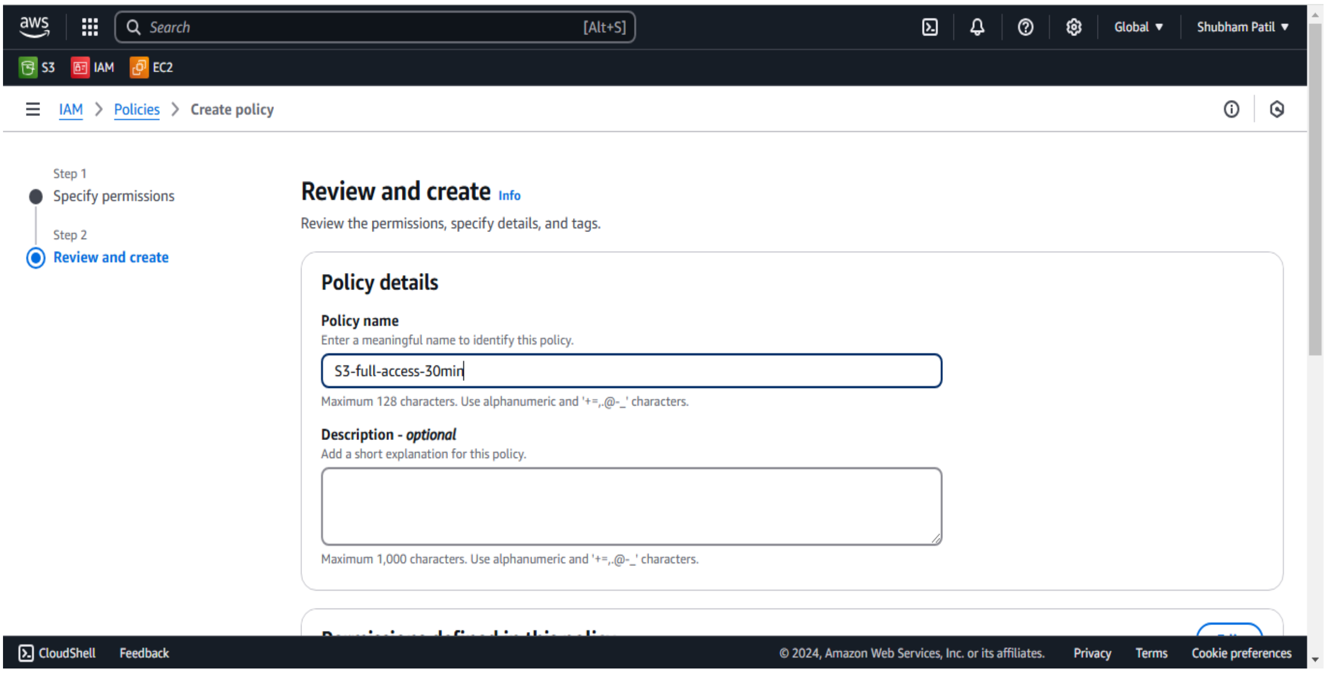
□ Requested from IP

Filters access by the requester's IP address

aws:CurrentTime (DateLessThan *2024-11-18T14:50:00Z*)

+ Add another condition

Step:4- Give Policy name and Create Policy.



Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

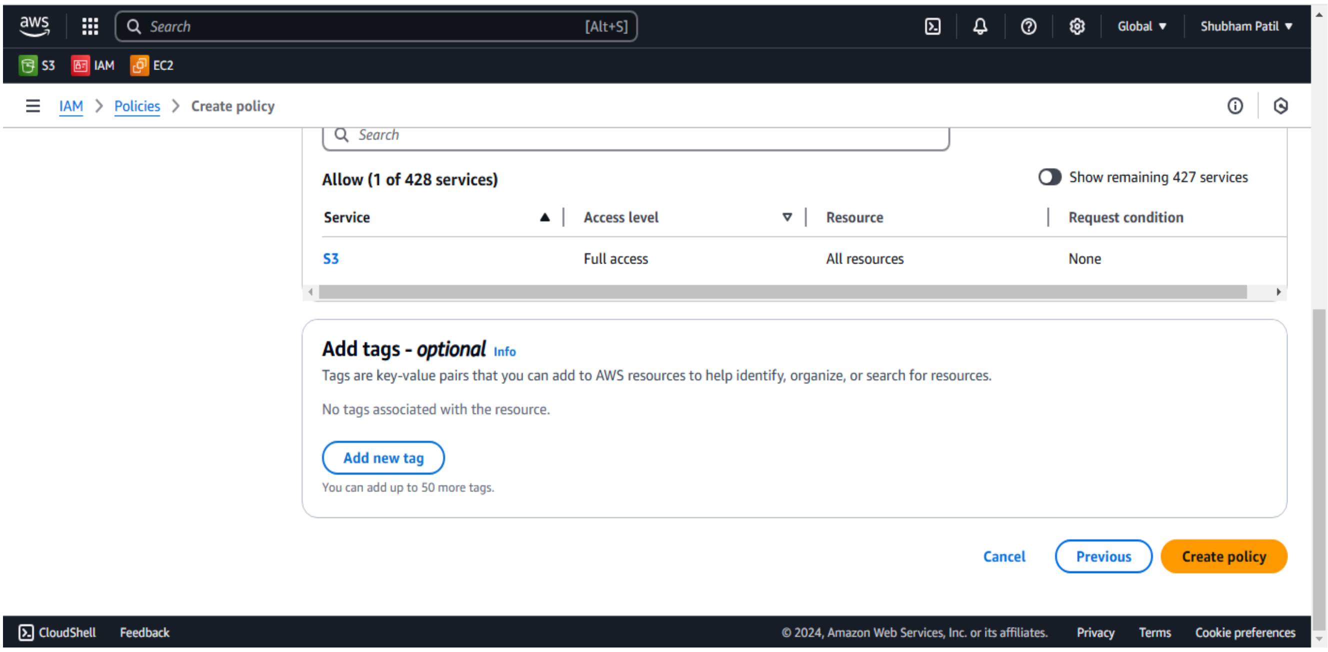
S3-full-access-30min

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.



Allow (1 of 428 services)

Show remaining 427 services

Service	Access level	Resource	Request condition
S3	Full access	All resources	None

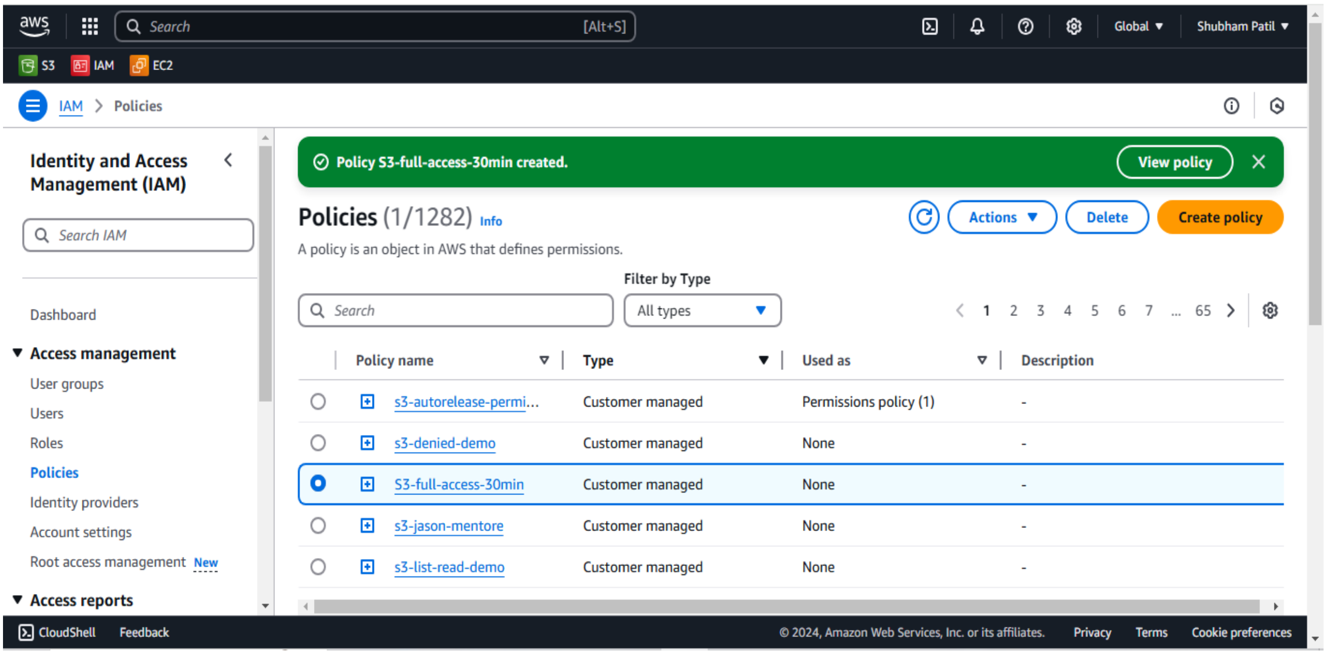
Add tags - *optional* Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.



Policy S3-full-access-30min created.

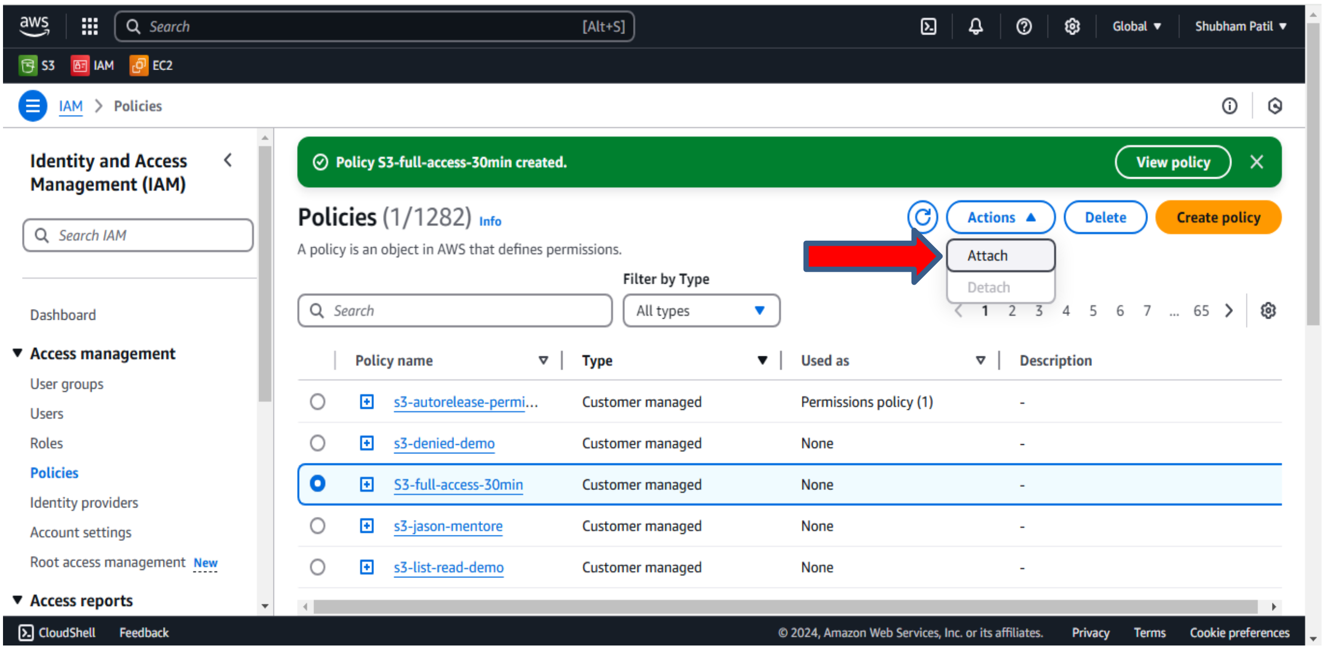
Policies (1/1282) Info

A policy is an object in AWS that defines permissions.

Filter by Type: All types

	Policy name	Type	Used as	Description
○	s3-autorelease-permi...	Customer managed	Permissions policy (1)	-
○	s3-denied-demo	Customer managed	None	-
●	S3-full-access-30min	Customer managed	None	-
○	s3-jason-mentore	Customer managed	None	-
○	s3-list-read-demo	Customer managed	None	-

Step:5- Now Attach this Policy to user for Give Full access of s3 service only for 30 Minutes.

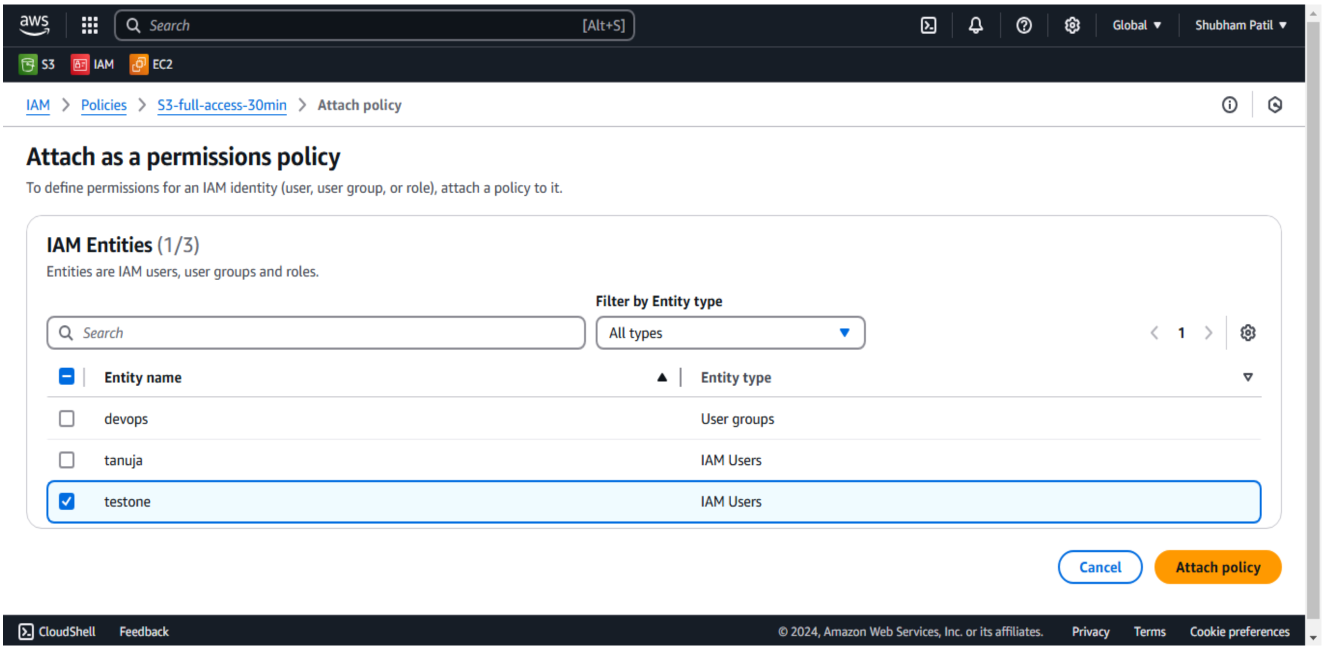


Policy S3-full-access-30min created.

Policies (1/1282) Info

A policy is an object in AWS that defines permissions.

	Policy name	Type	Used as	Description
○	s3-autorelease-permi...	Customer managed	Permissions policy (1)	-
○	s3-denied-demo	Customer managed	None	-
●	S3-full-access-30min	Customer managed	None	-
○	s3-jason-mentore	Customer managed	None	-
○	s3-list-read-demo	Customer managed	None	-



Attach as a permissions policy

To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

IAM Entities (1/3)

Entities are IAM users, user groups and roles.

☐	Entity name	Entity type
☐	devops	User groups
☐	tanuja	IAM Users
☑	testone	IAM Users