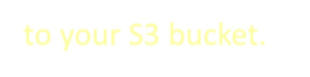


**Use Cases:**



**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.



**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.

1

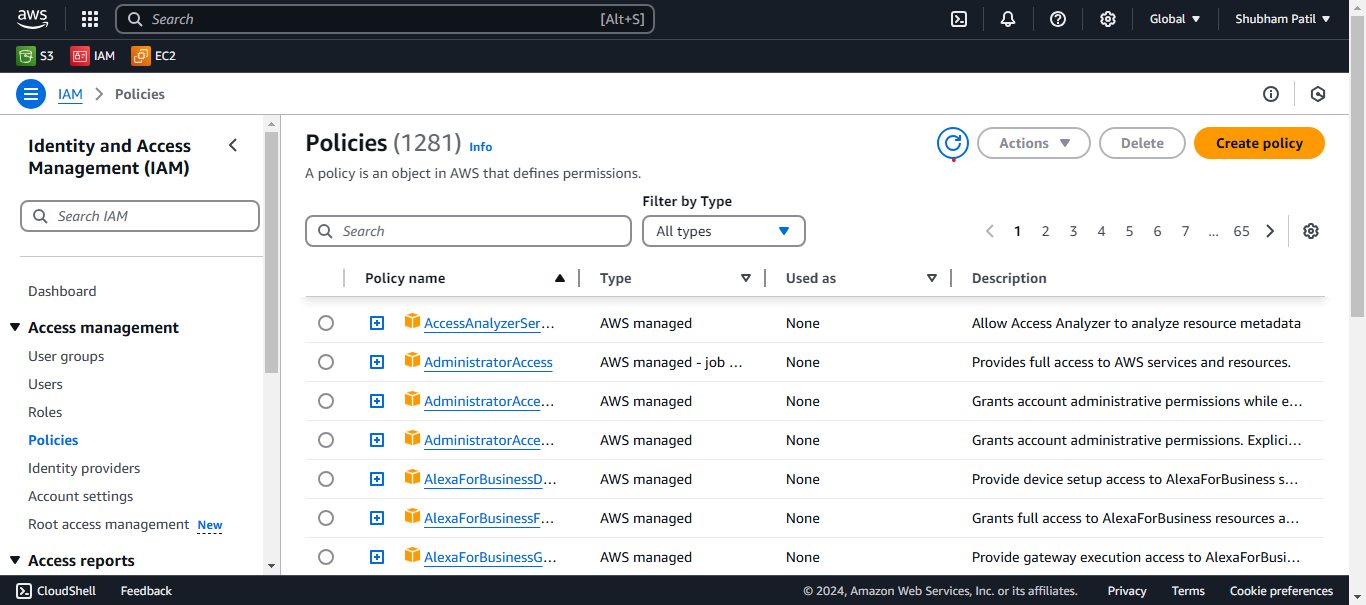


**3. Disaster Recovery or Backup Access**

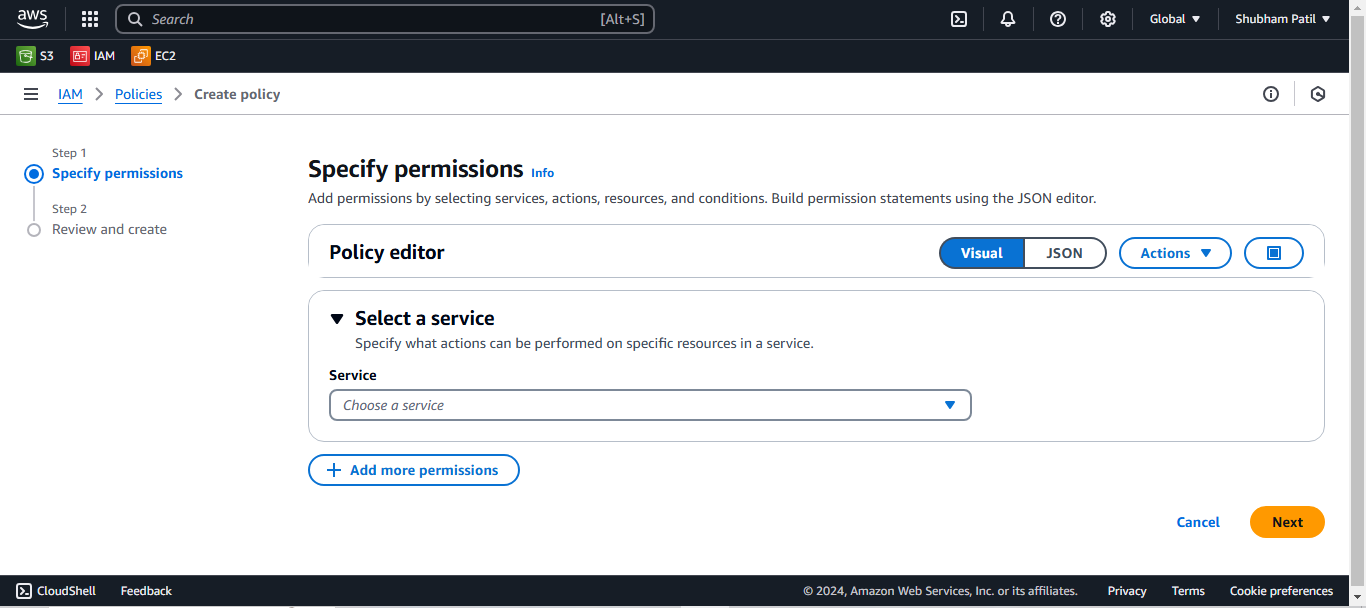
Provide short-term access for recovery purposes in case of emergencies.

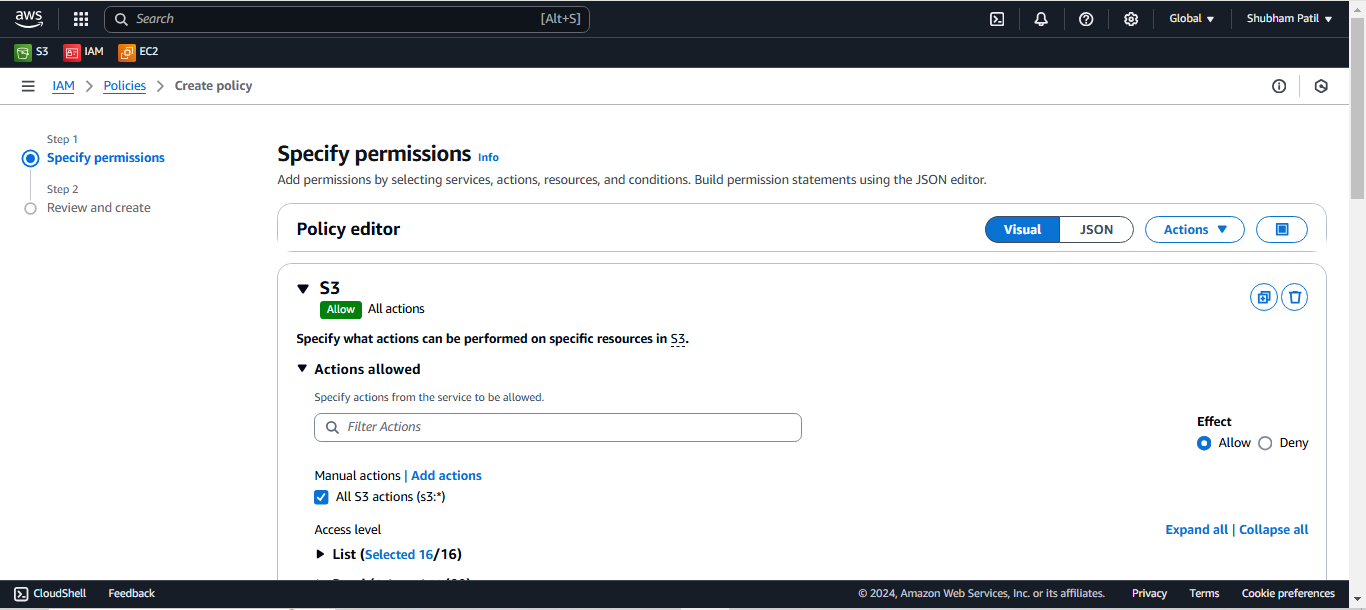
**Example**: A system administrator needs to restore files but shouldn’t have long-term access.

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

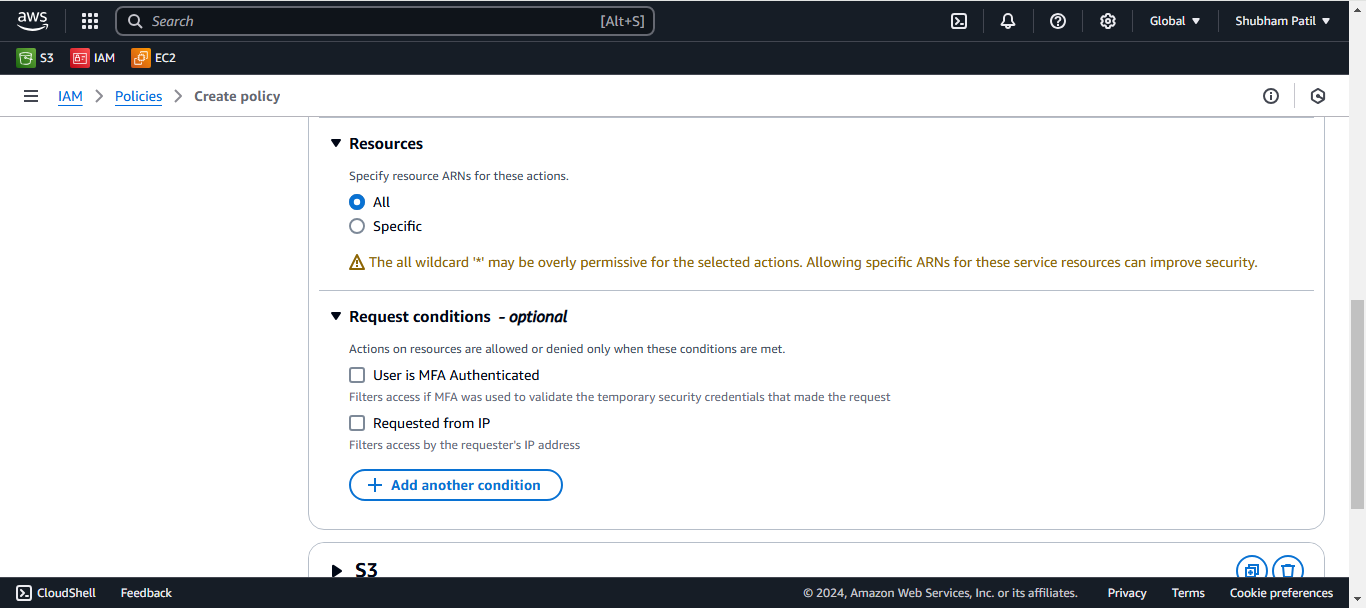


Step:2- Select Visual policy editor and Select s3 Service then Allow all Actions, Specify all Resources.





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



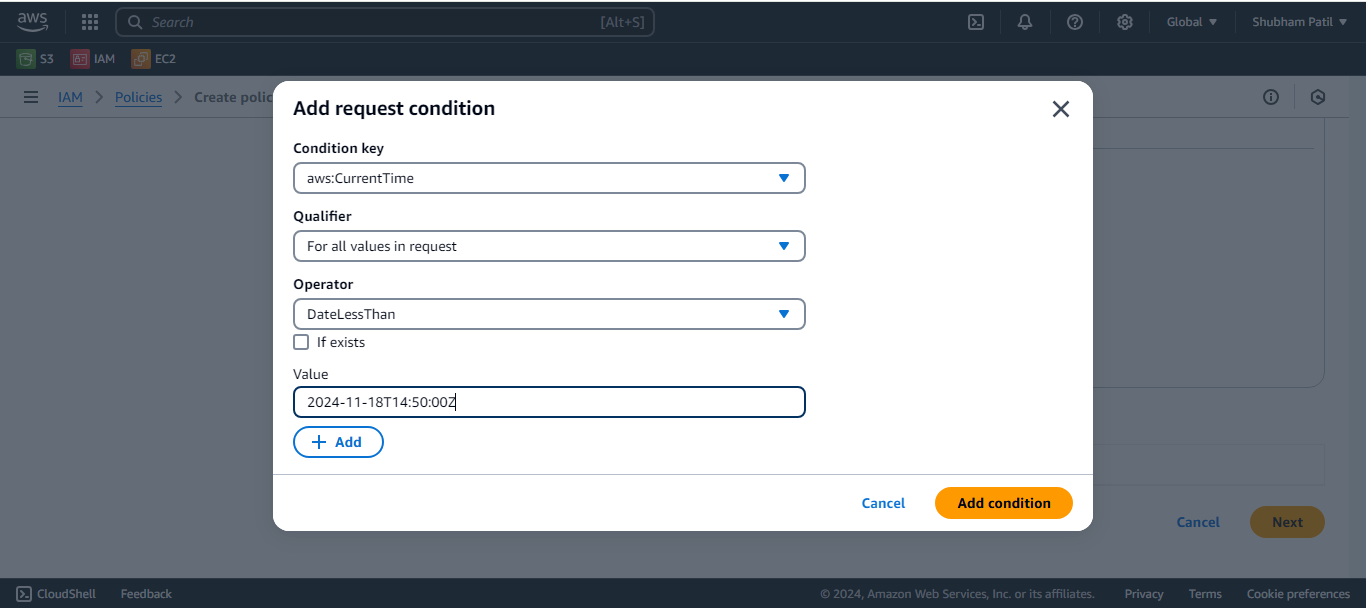
Step:4- Select Condition key=aws:CurrentTime

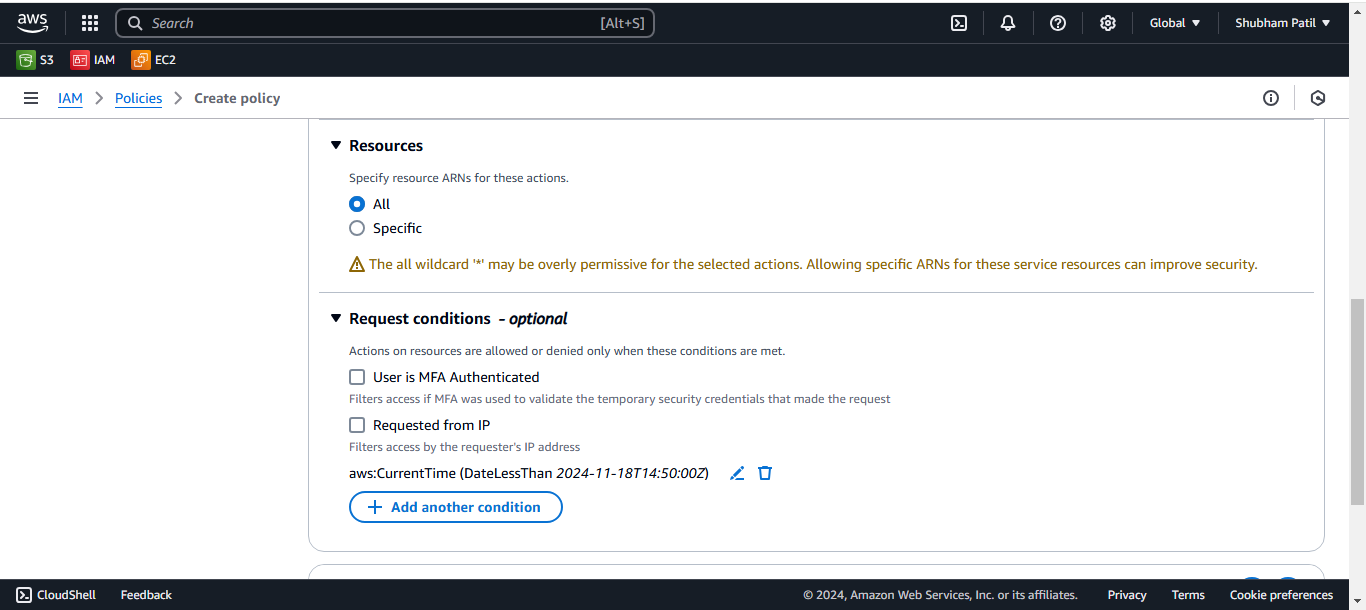
Qualifier= For all values in request Operator= DateLessThan

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

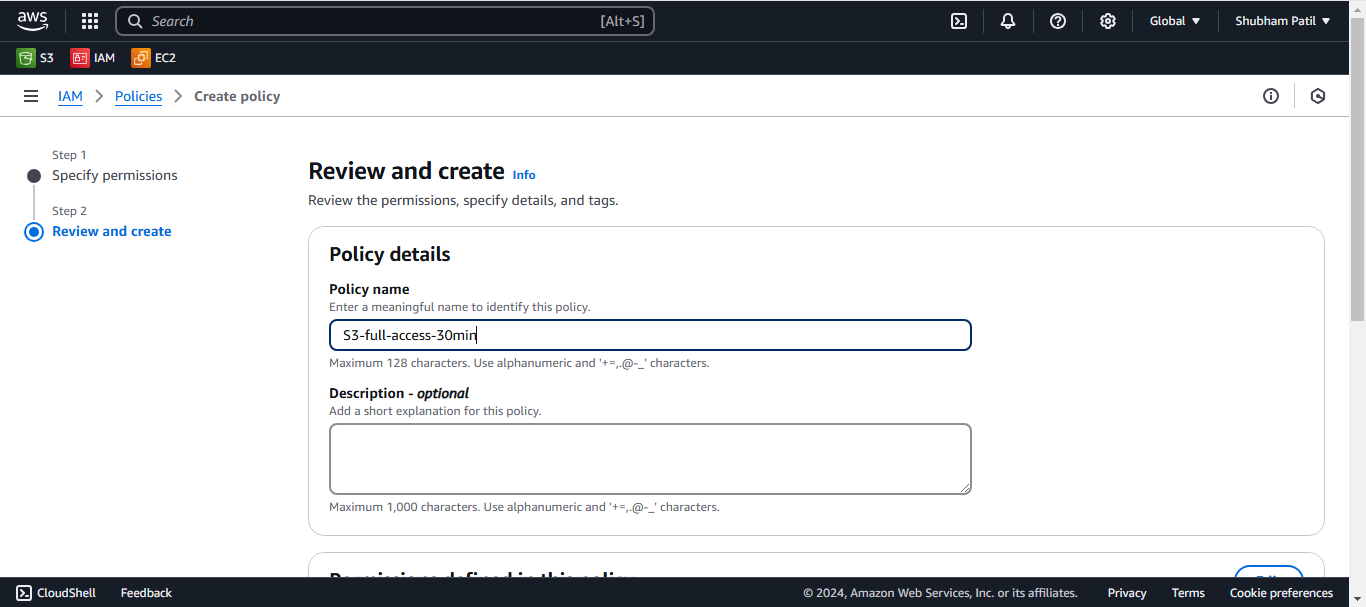
**# Here value is given in UTC format to give access for only 30 minutes from now.**

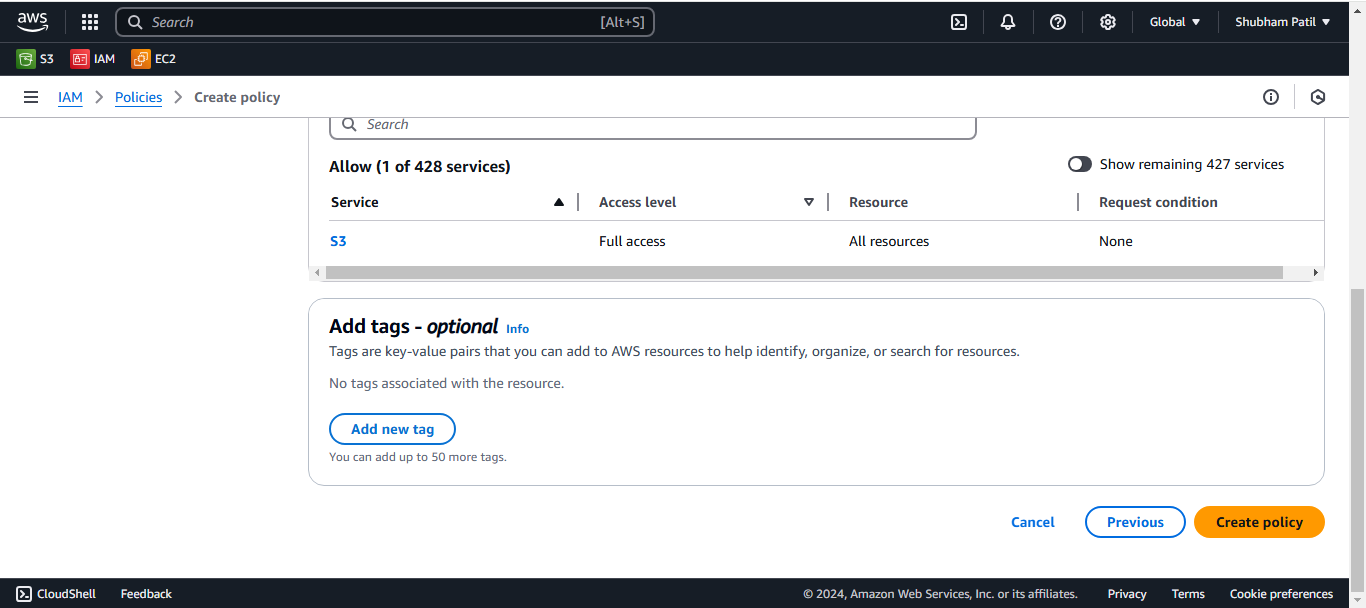
And Add condition

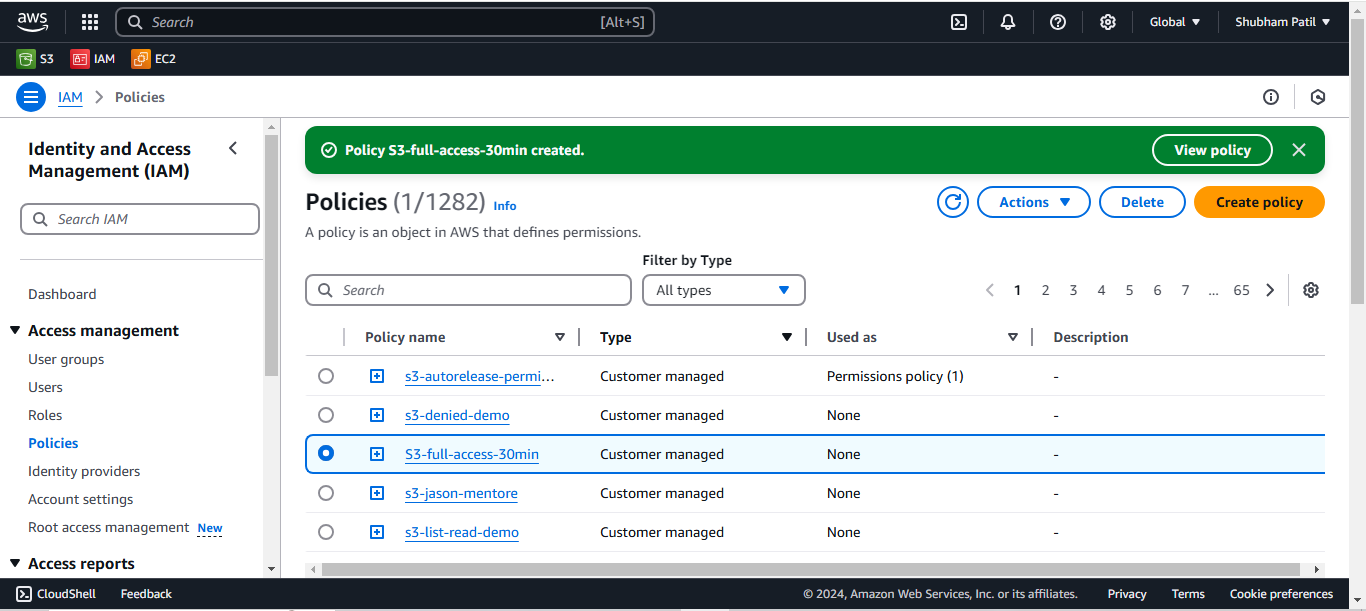




Step:4- Give Policy name and Create Policy.







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

