# Secure Cloud File Storage with IAM and Audit Logging in AWS

Prepared by Mayank Jain

1. **Project Summary:**

"Configured secure file storage in AWS using S3, with strict IAM policies and CloudTrail logging to monitor access and protect data."

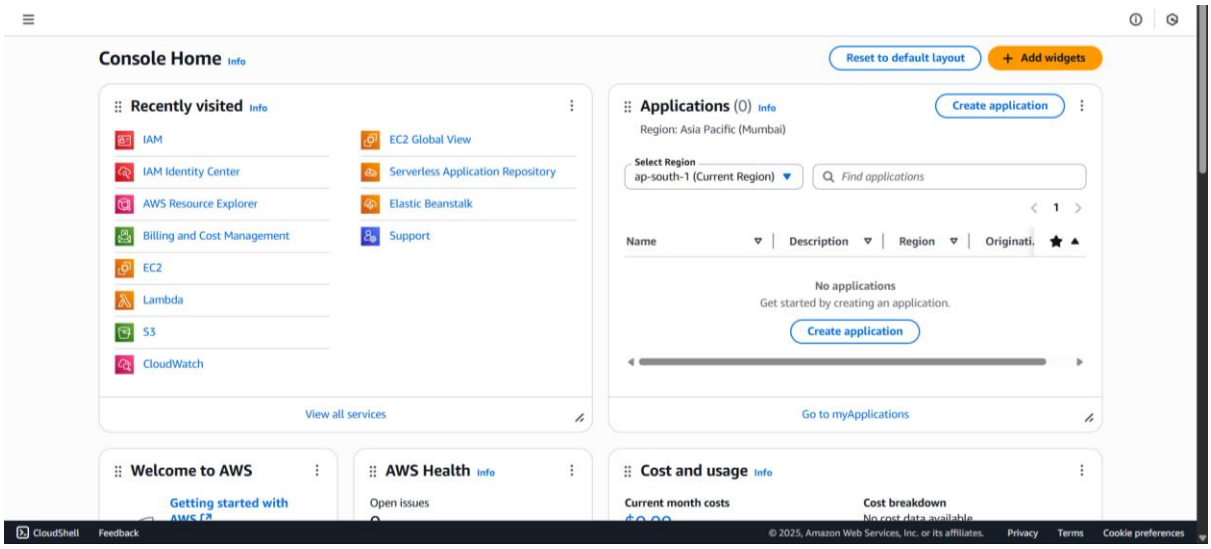
2. **Tools Used:**
   - AWS S3
   - IAM
   - Cloudtrail

3. **Security Features Implemented:**
   - Private S3 bucket
   - IAM-based least-privilege access
   - Default encryption
   - CloudTrail audit logging

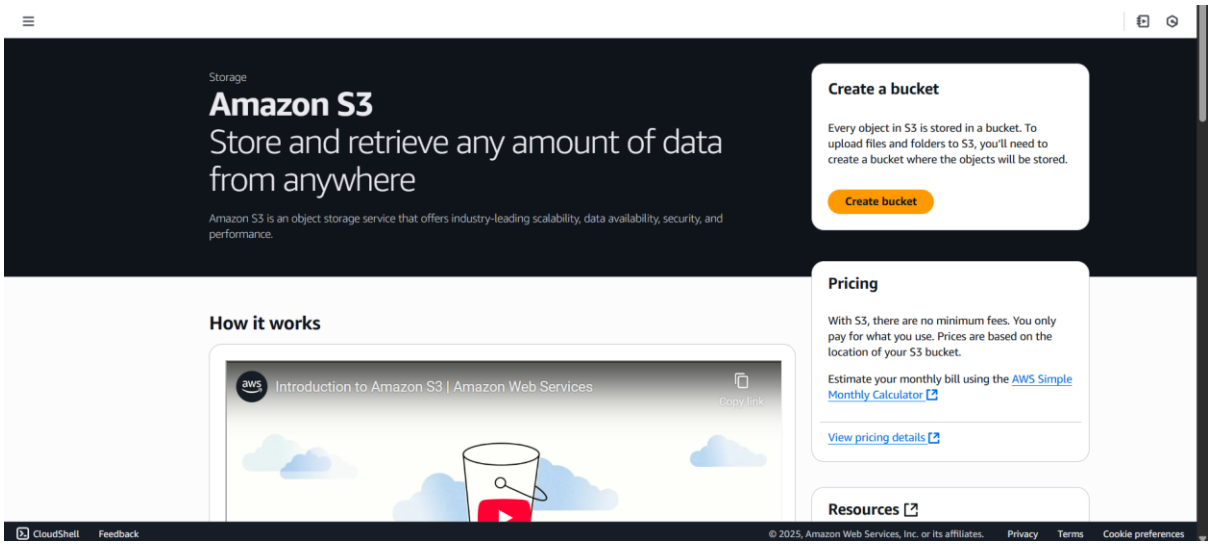
4. **Outcome:**
   - Read-only user created
   - Unauthorized actions blocked
   - Audit logs successfully recorded in CloudTrail

**Steps:**

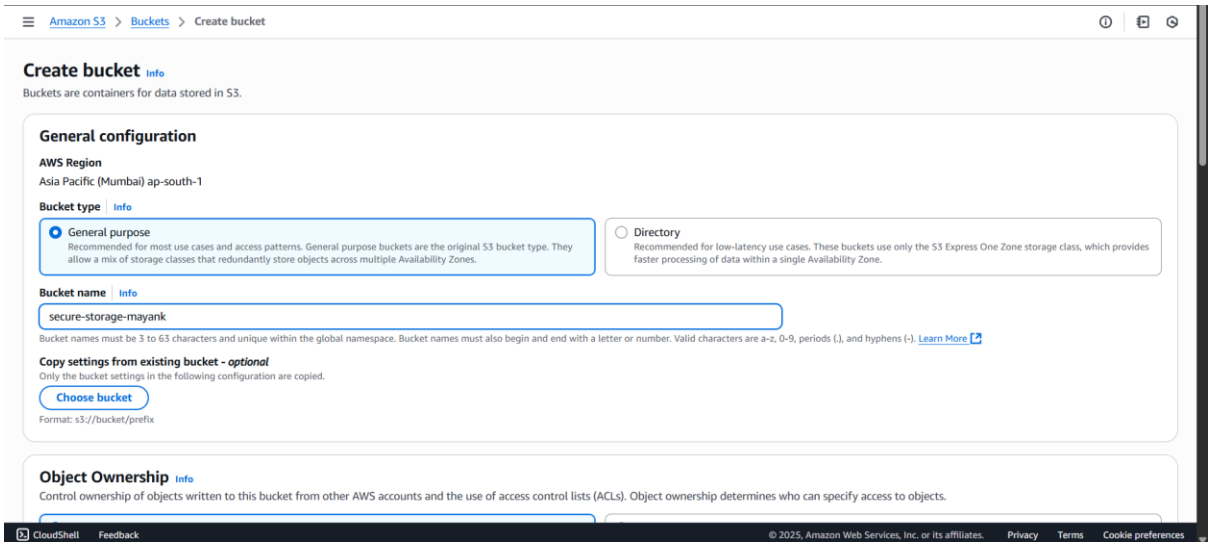
1. Log in to your Amazon AWS account and go to the **S3 service** in the AWS Console

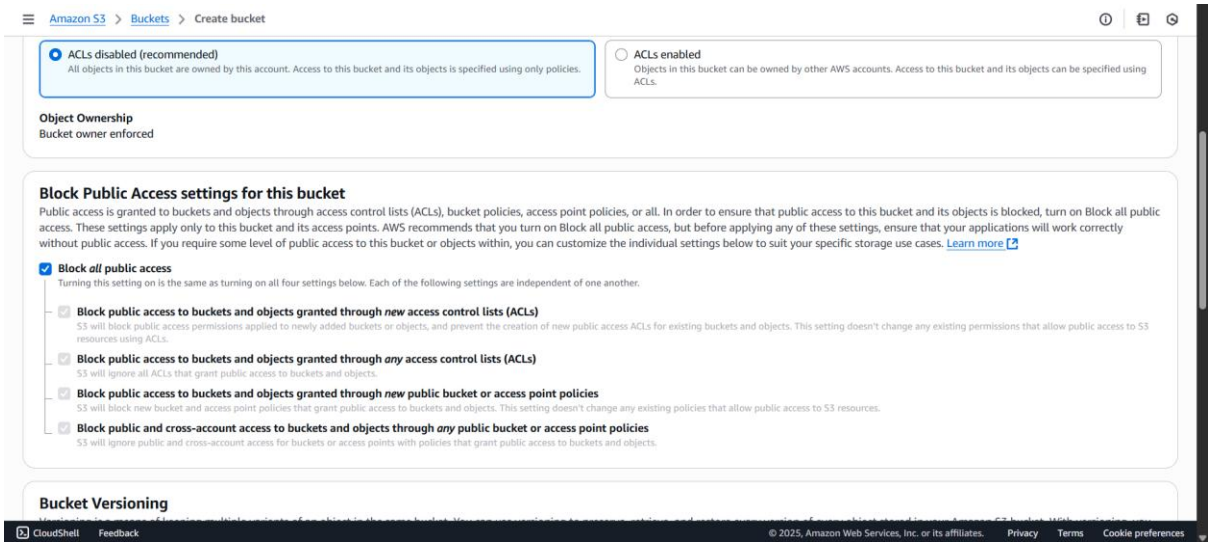


2. Click **“Create bucket”.**

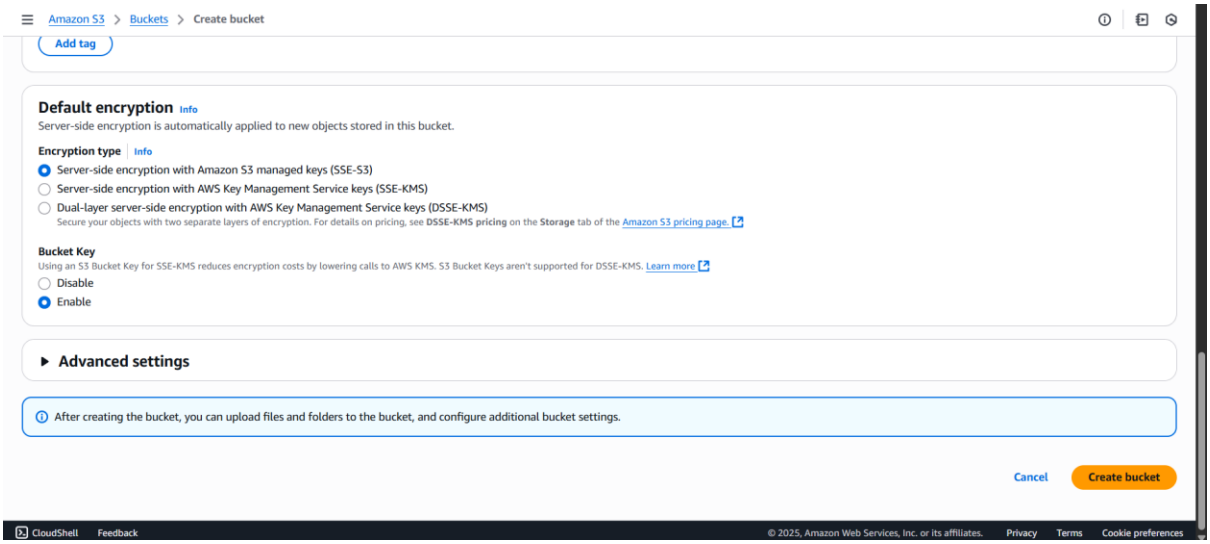



**3.** Name it **secure-storage-mayank** and keep default settings for the bucket.

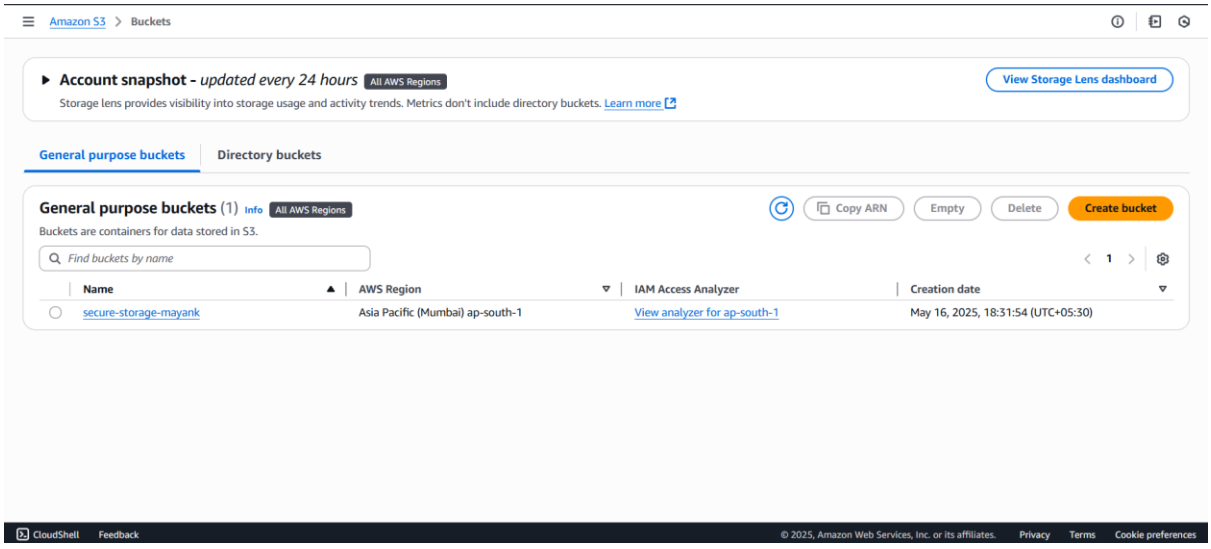


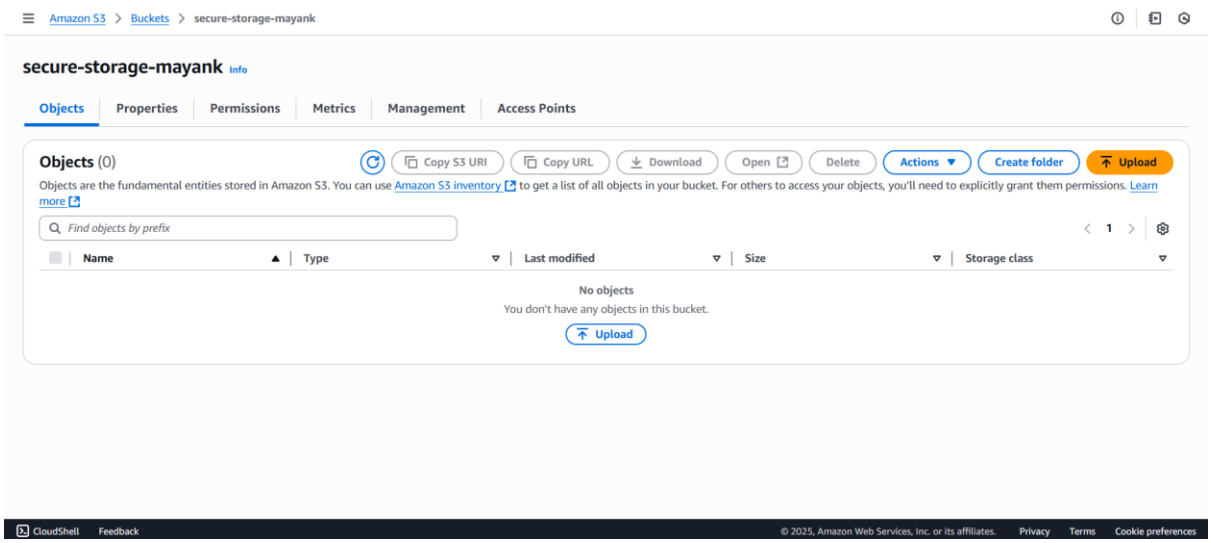



4. Click **Create Bucket**.

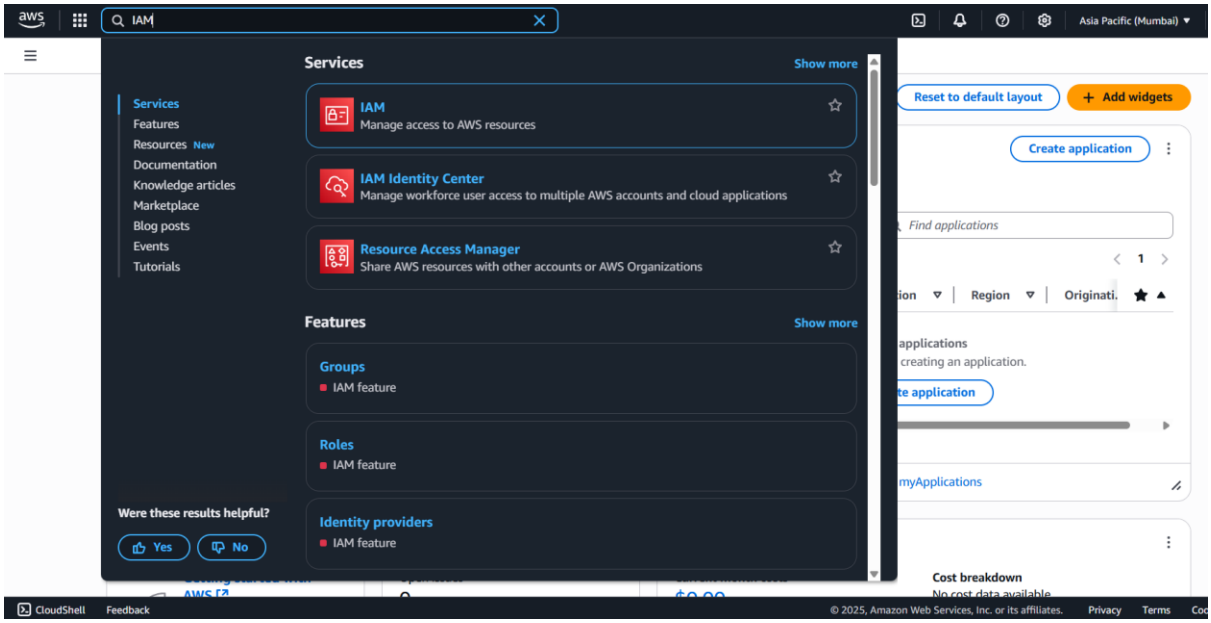



5. In the list of General purpose buckets, you will be able to see the created S3 bucket **secure-storage-mayank**.

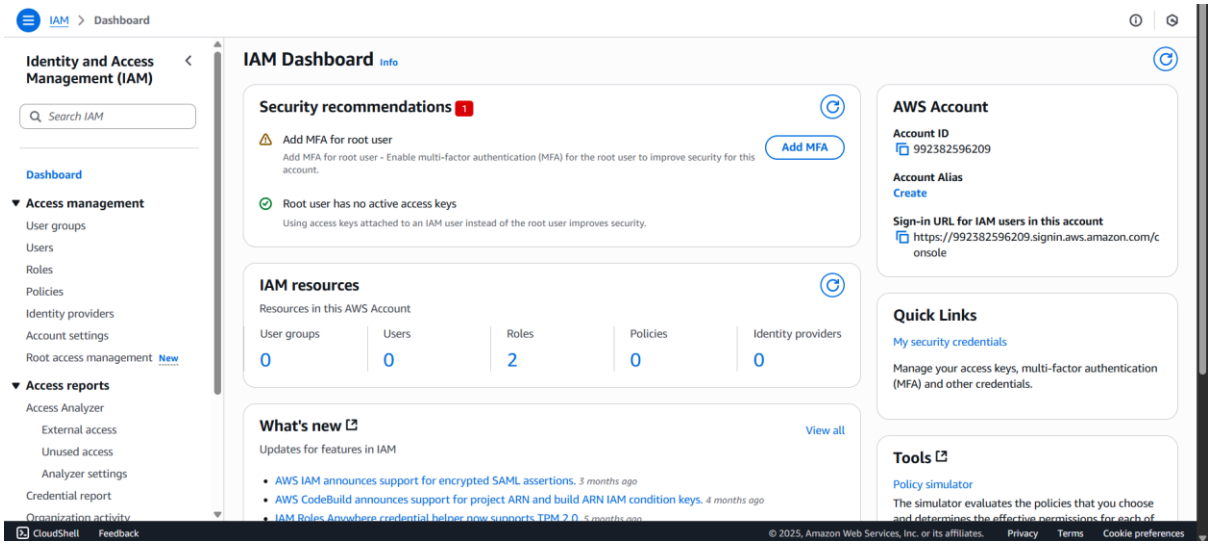




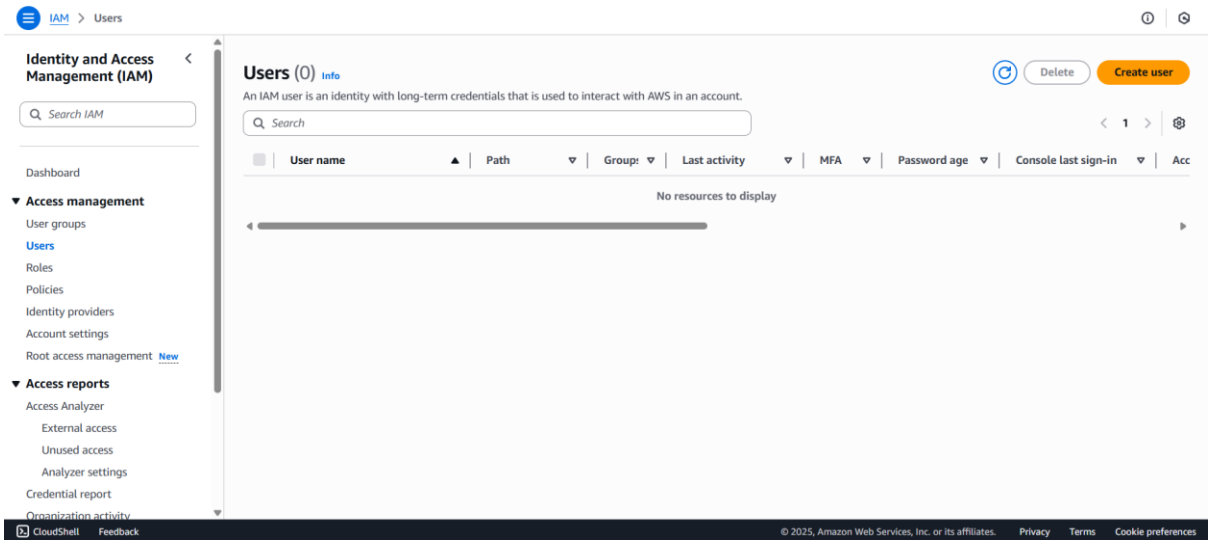

6. Go to **IAM.**



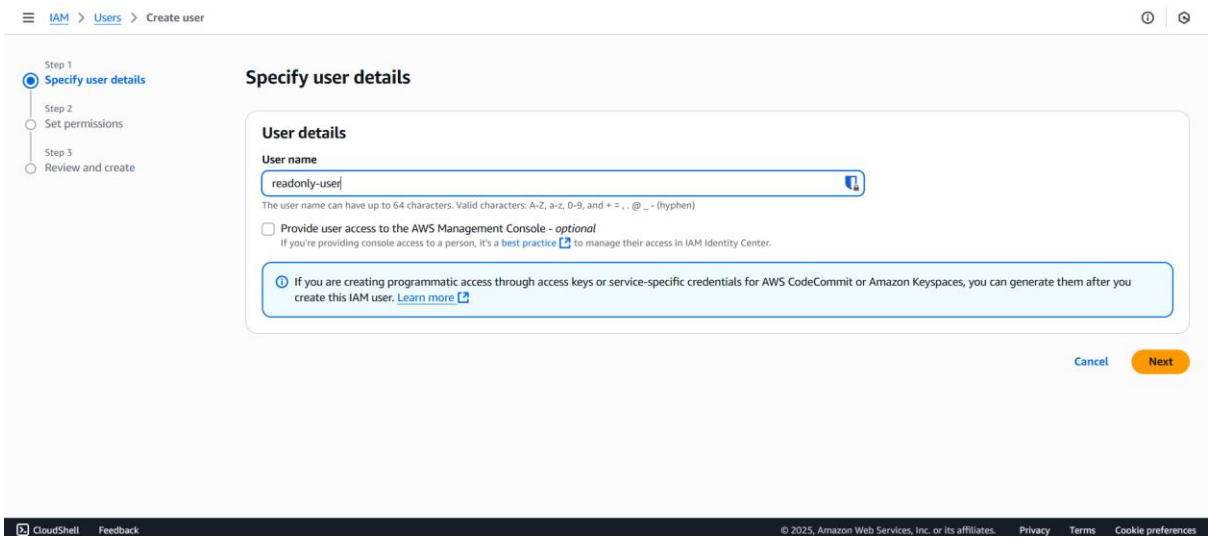

7. Click on **Users.**



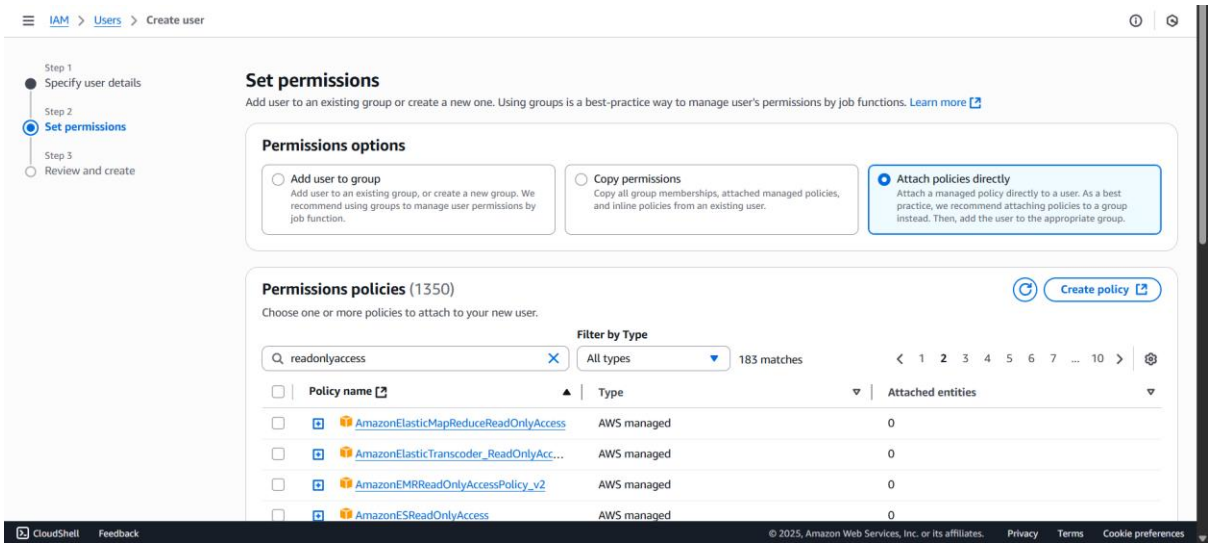

8. Click on **Create User**.




9. Enter the username: **readonly-user**.

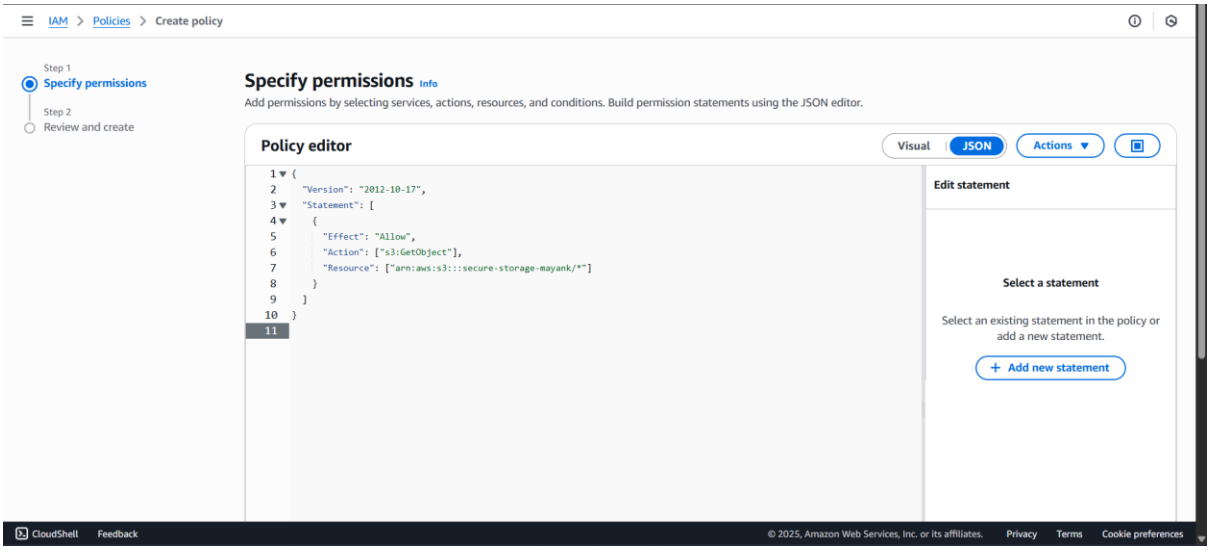



10. Click on **Attach policies directly** and then click on **Create Policy** to create your custom policy.

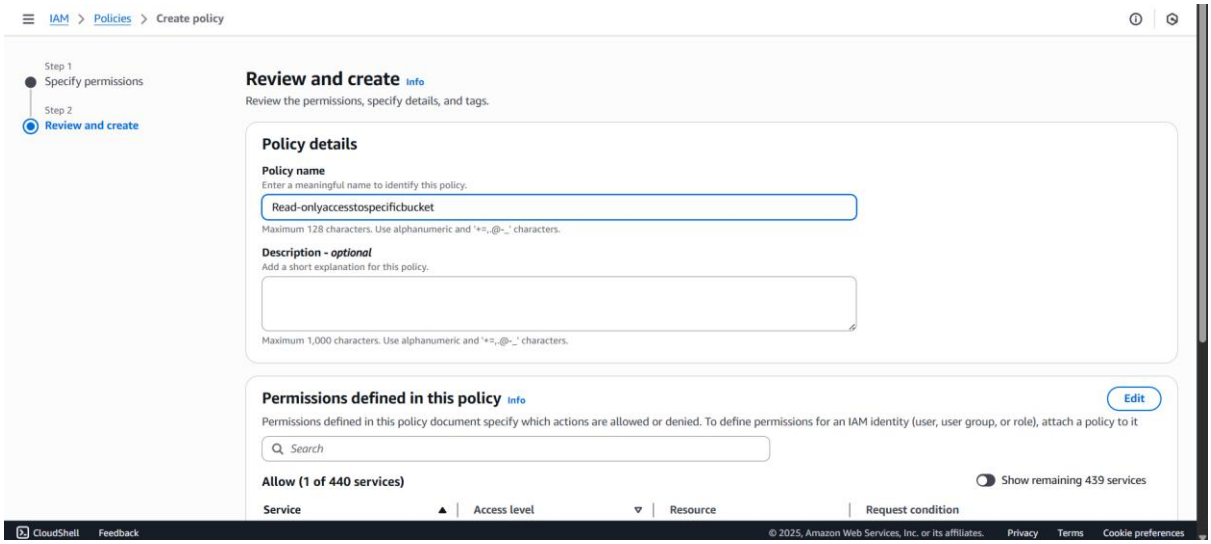



11. Choose **Json** as the option and specify the permissions. Paste the following statement in the Policy editor and click on **Next**.

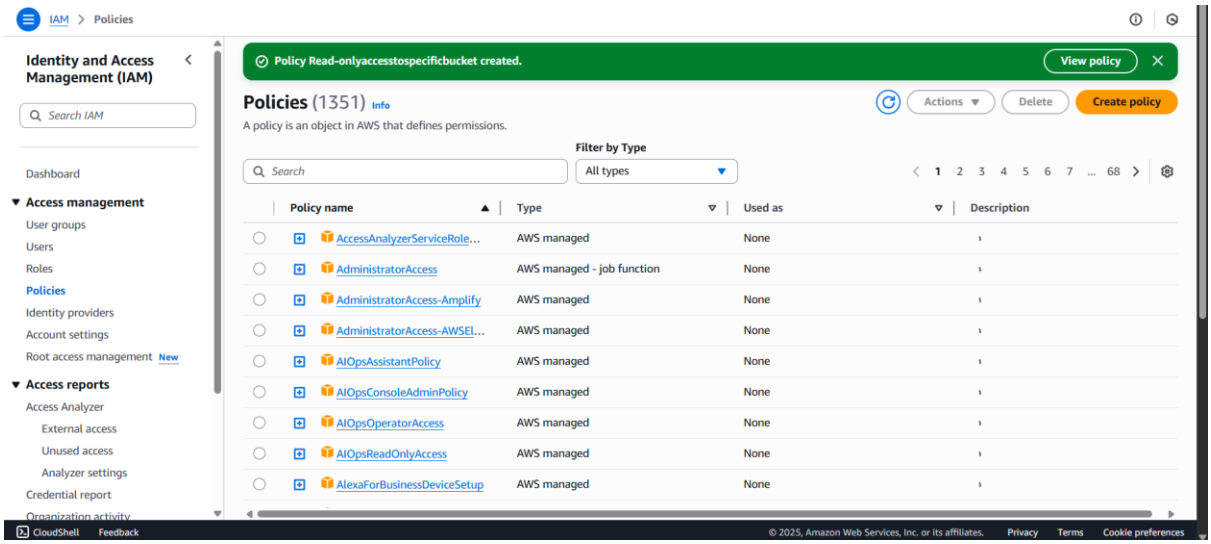
```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": ["s3:GetObject"],
   "Resource": ["arn:aws:s3:::secure-storage-mayank/*"]
  }
 ]
}
```



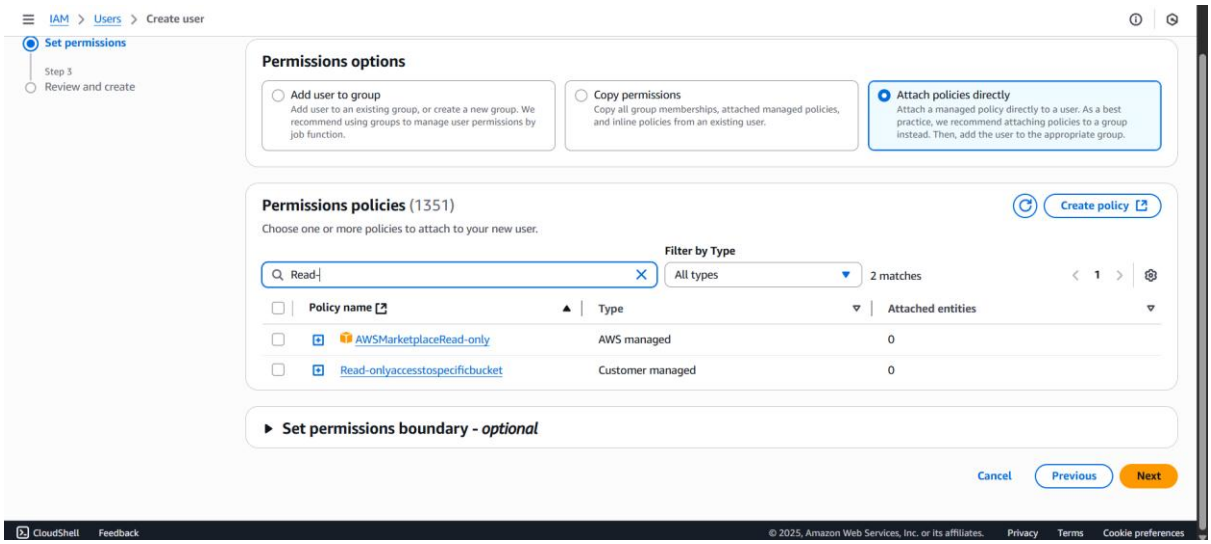

12. Give the policy name and click on **Create Policy**.

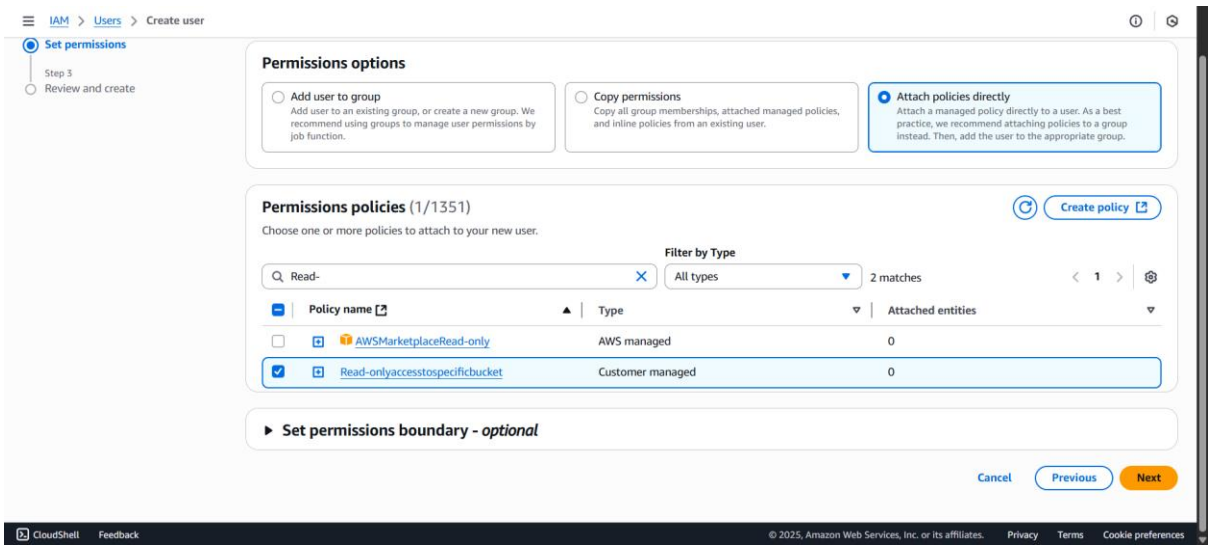



13. Your policy is created message shows.

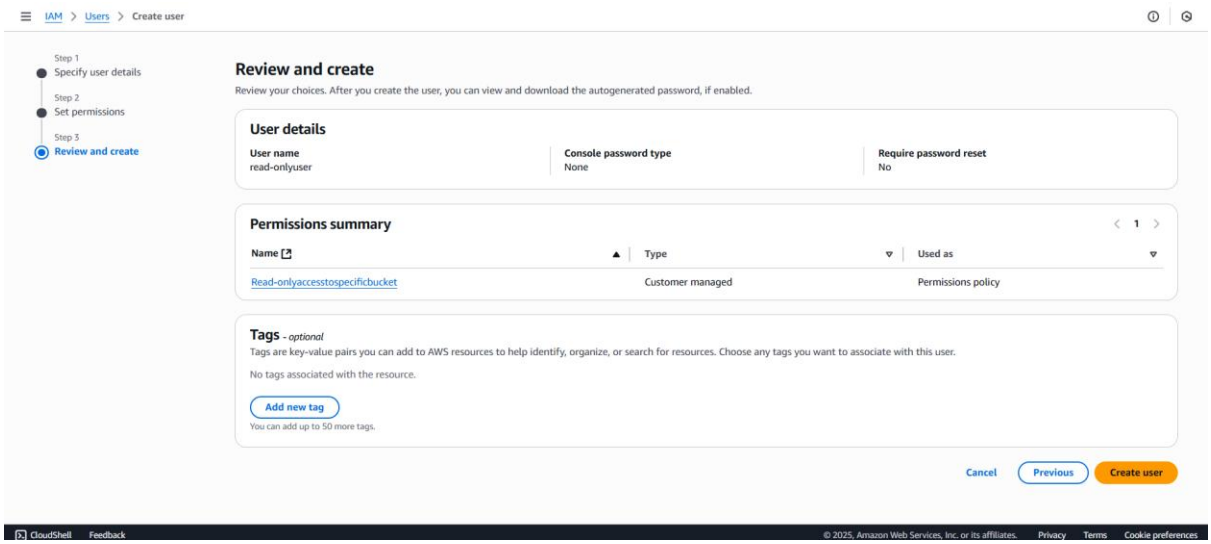


14. Now we resume the process of giving permission to our user and attach the policy we just created and click on **Next**.

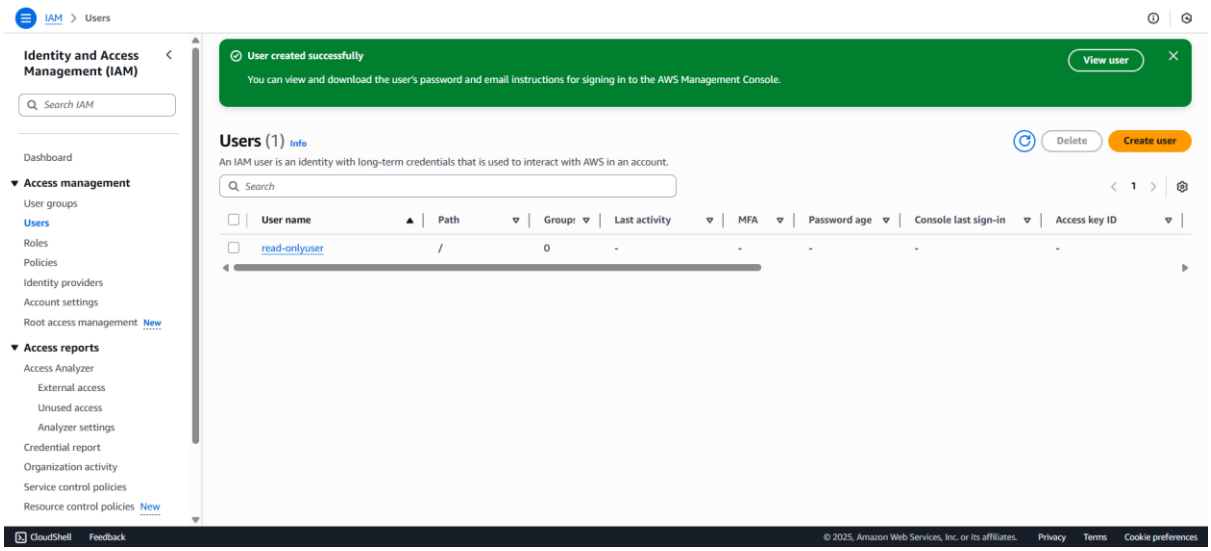


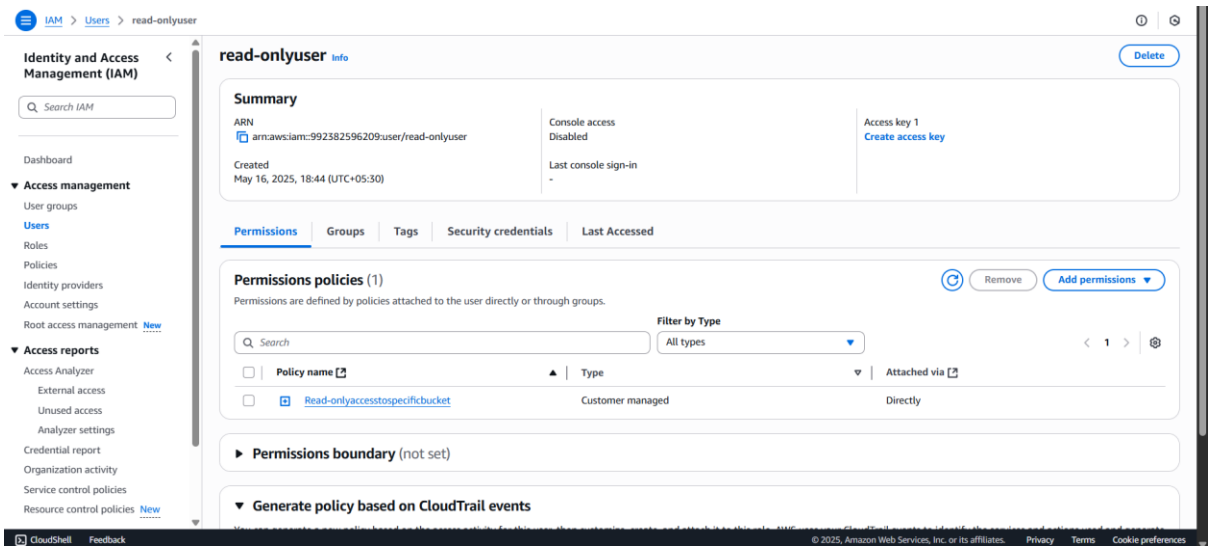




15. Review the information and permissions for the user and click on **Create User**.

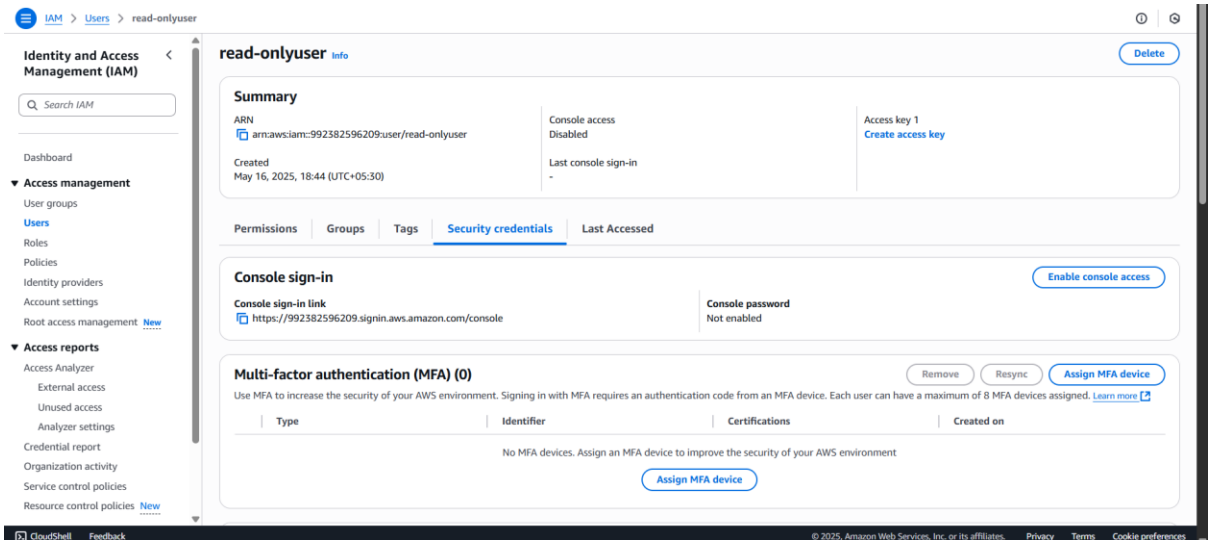



16. User created successfully message appears. You can click on the user to see his information and permissions.

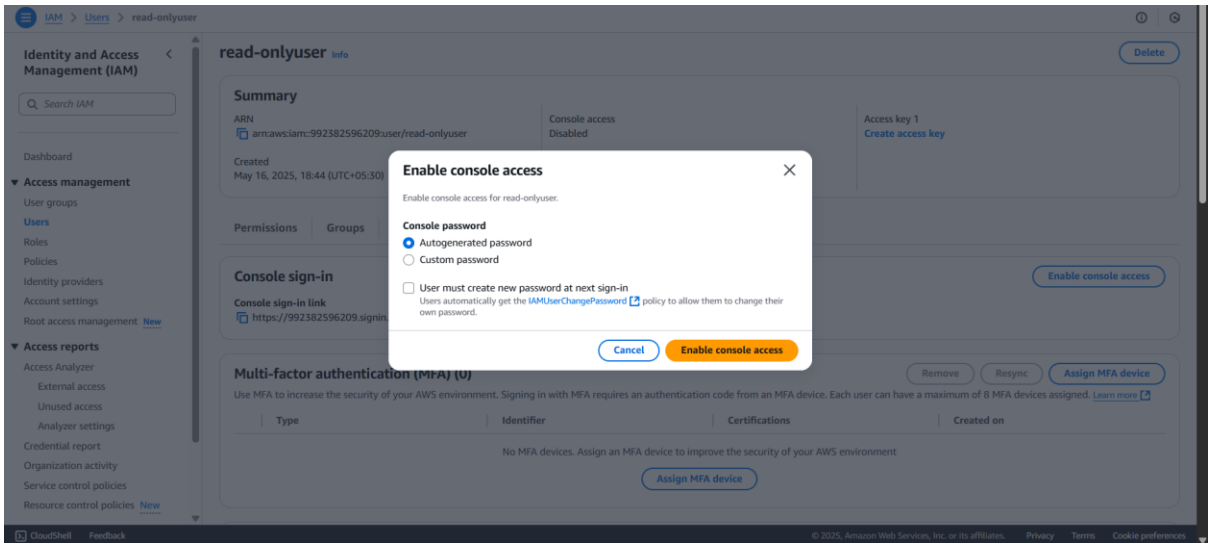


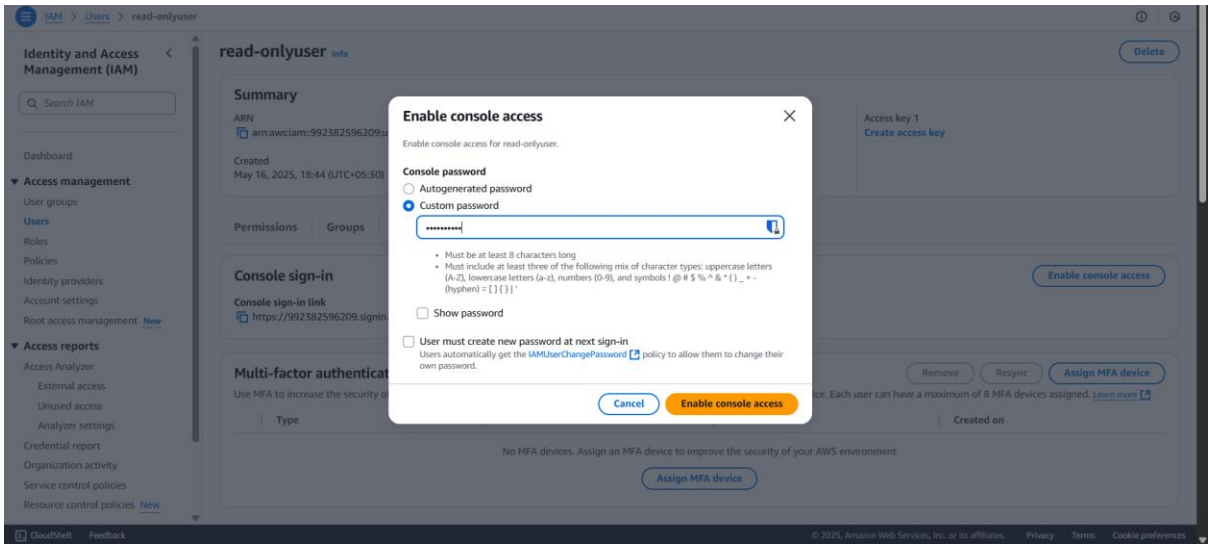



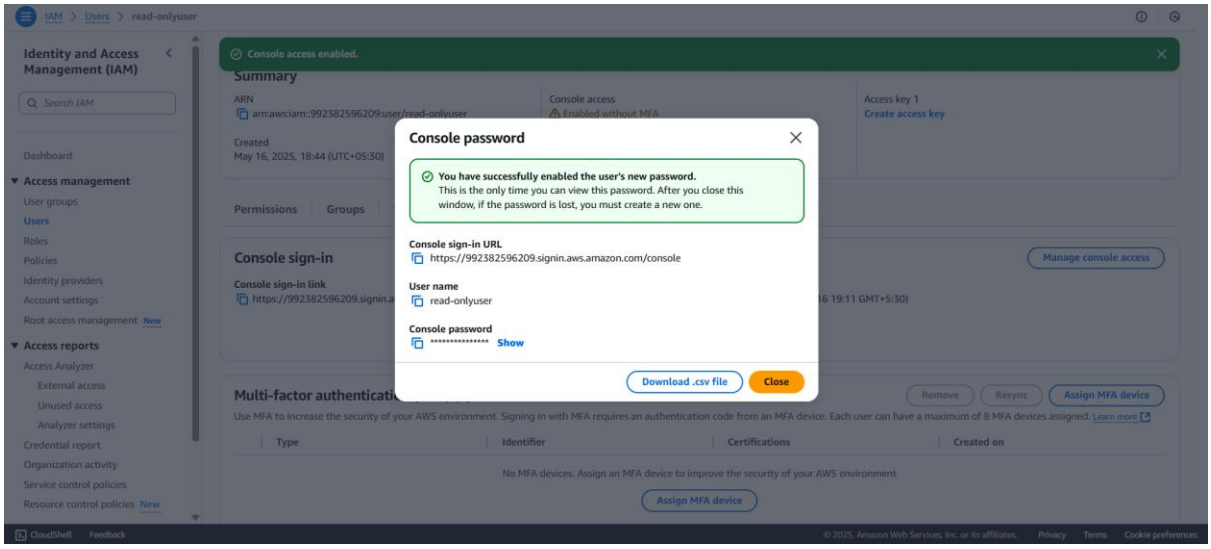

17. Go to **Security Credentials** and click on **Enable Console Access.**



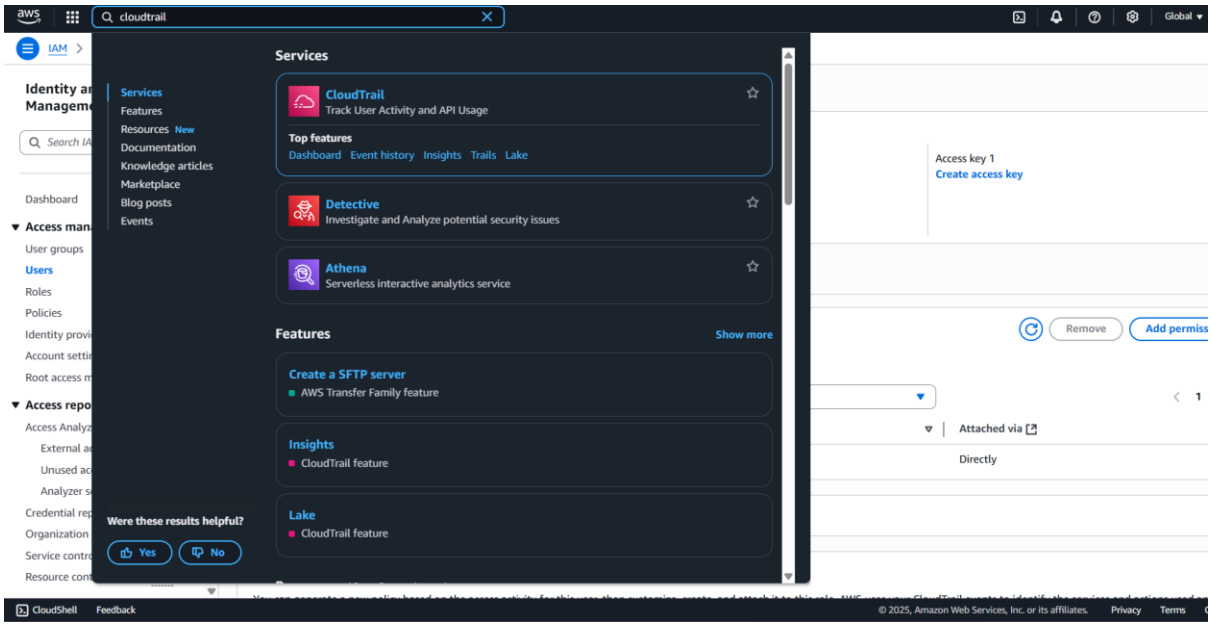

18. Click on **Custom Password** for providing a password of your choice and click on **Enable Console Access**.



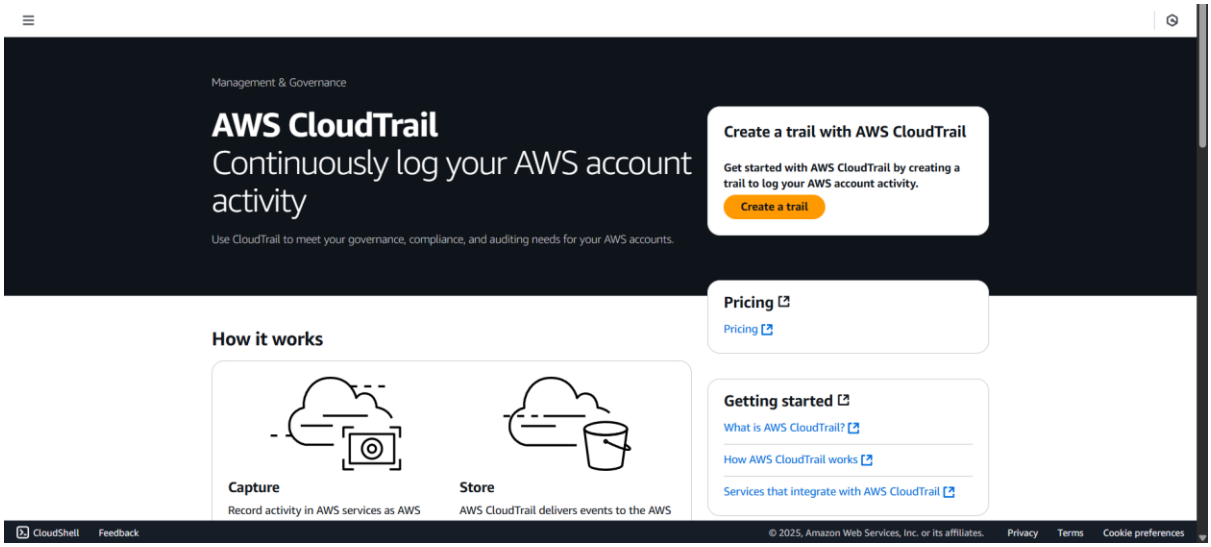





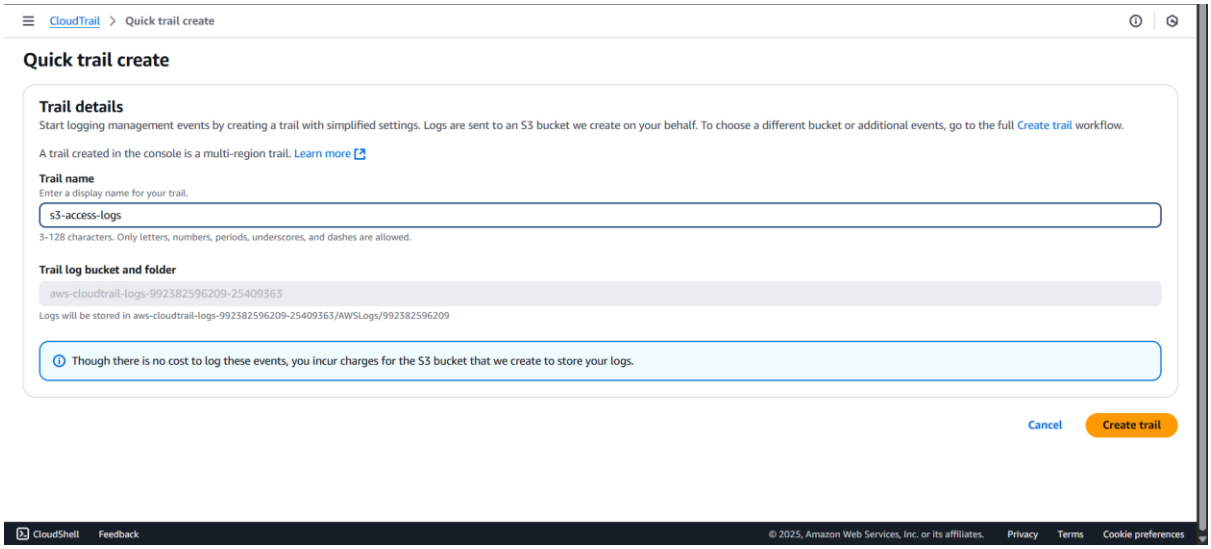

19. Now go to **Cloudtrail** to enable audit logging.



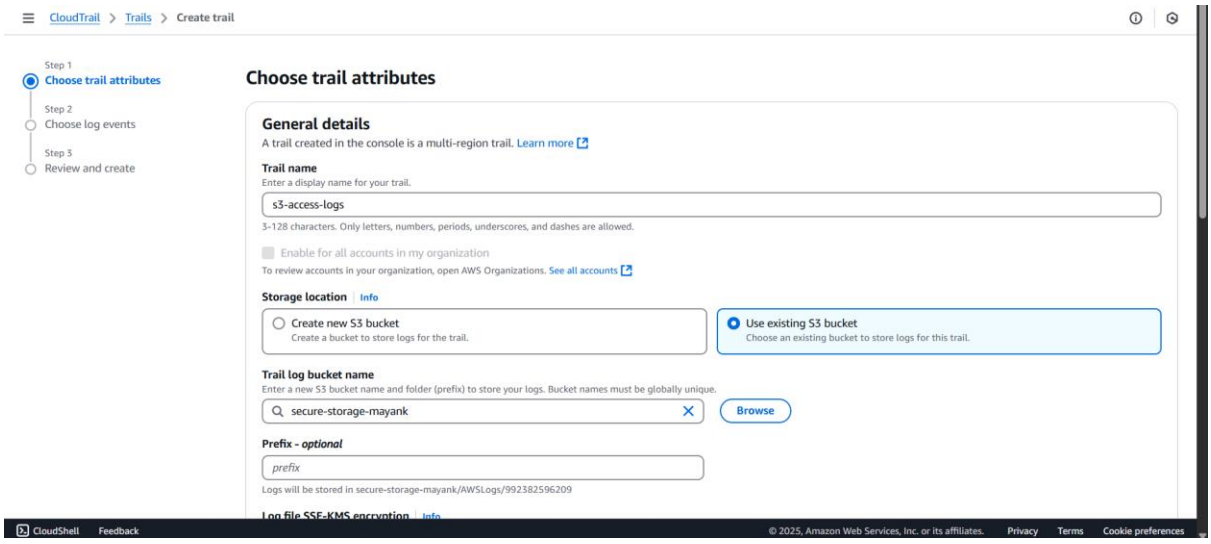

20. Click on **Create a trail**.



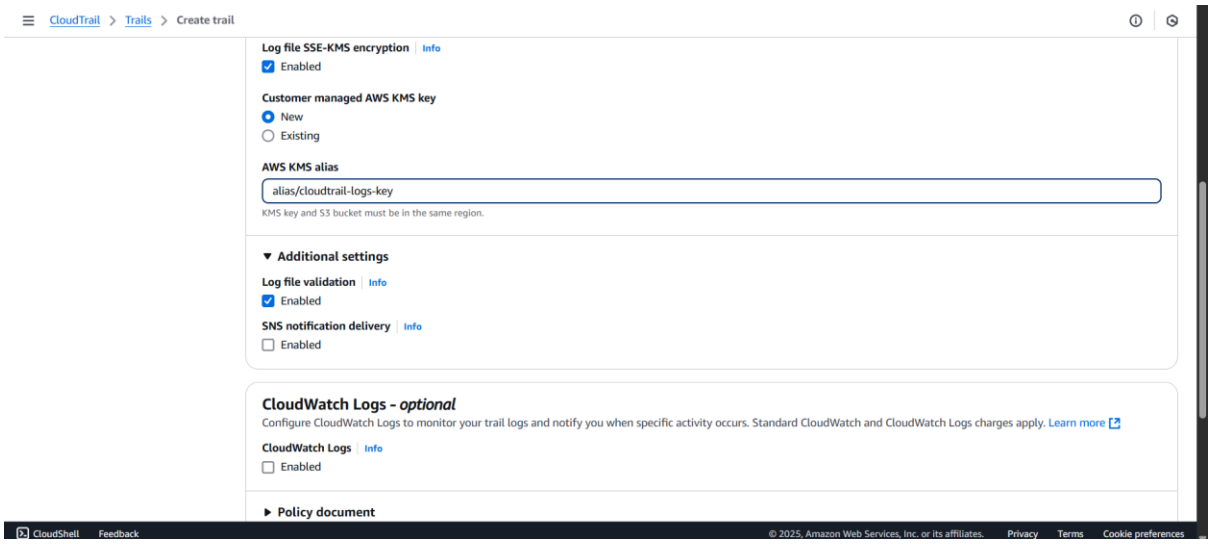

21. Either create a **Quick Trail** or click on **Create Trail** in the first line to see the full workflow as in this case.



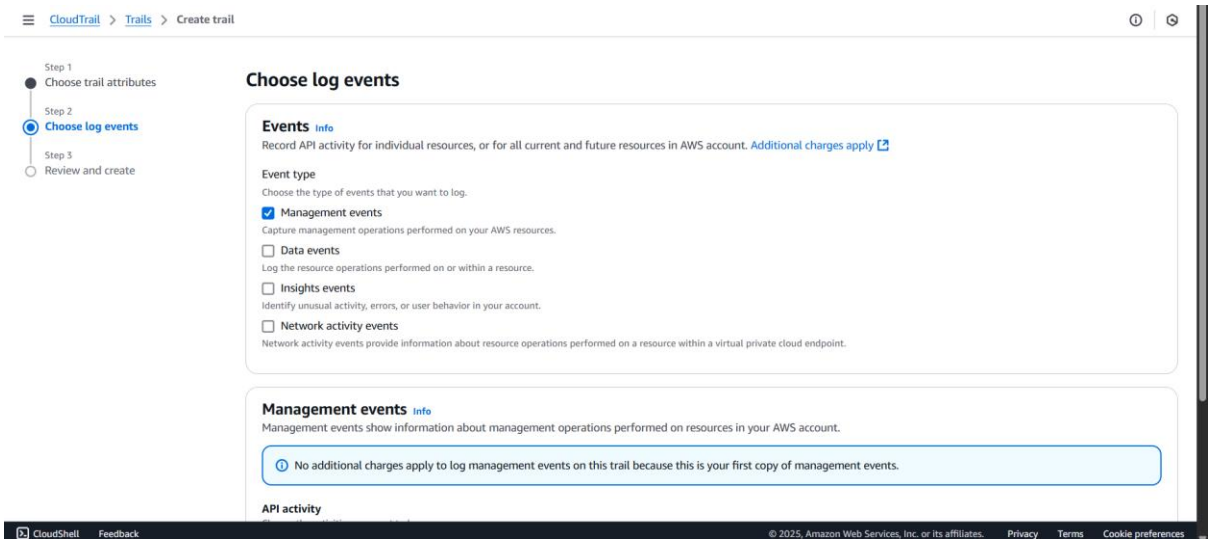

22. Provide the **Trail Name** (s3-access-logs) and choose **Use existing S3 bucket** and choose the bucket we created previously.

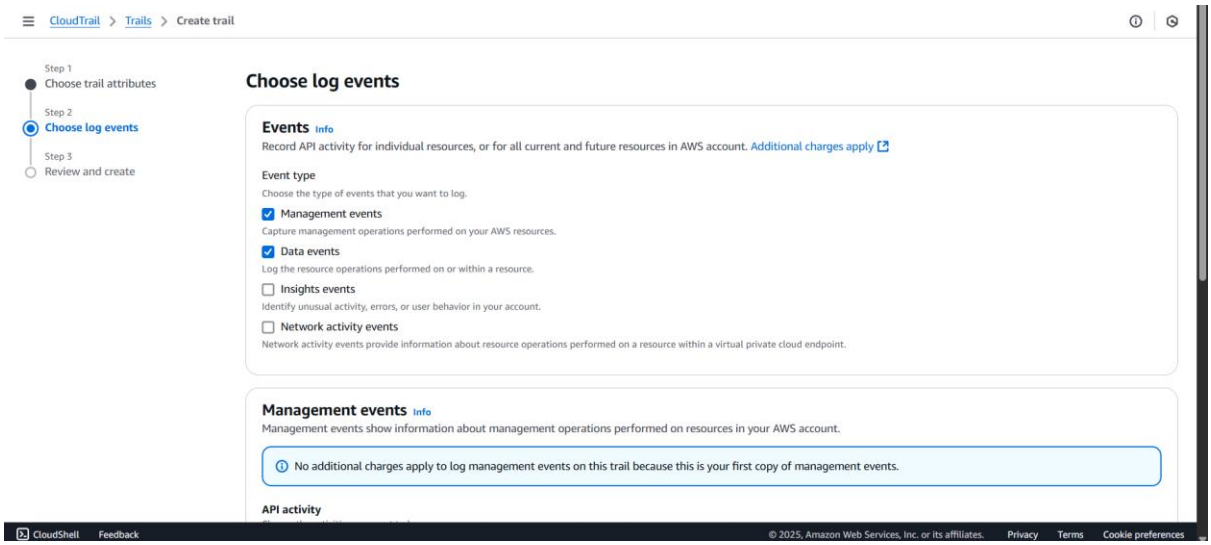


23. Provide a key name for the AWS KMS alias to create a new key.

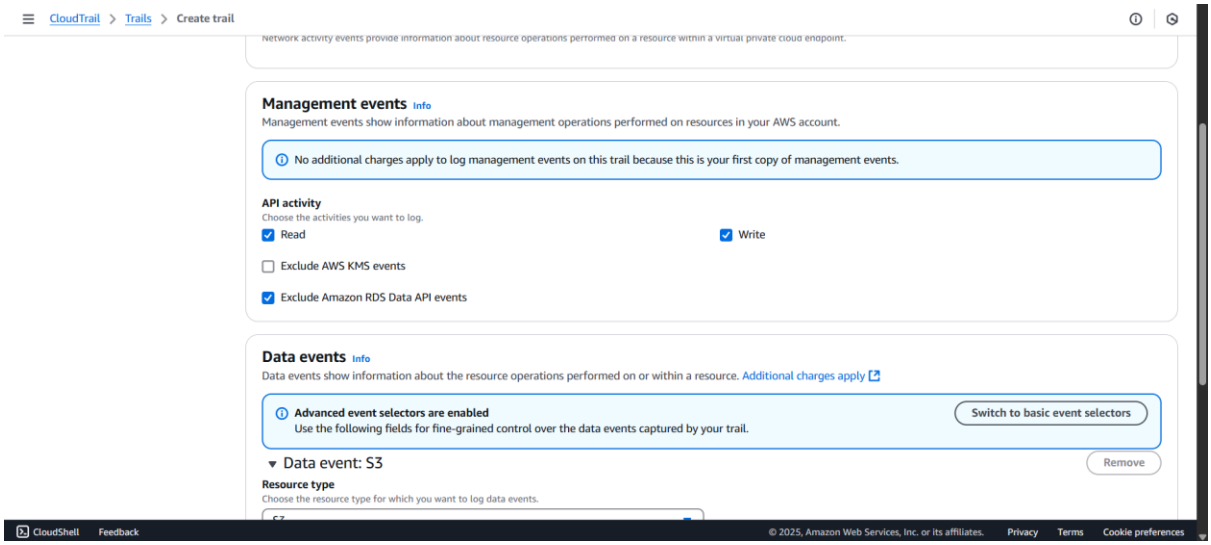



24. Choose Management and Data events.

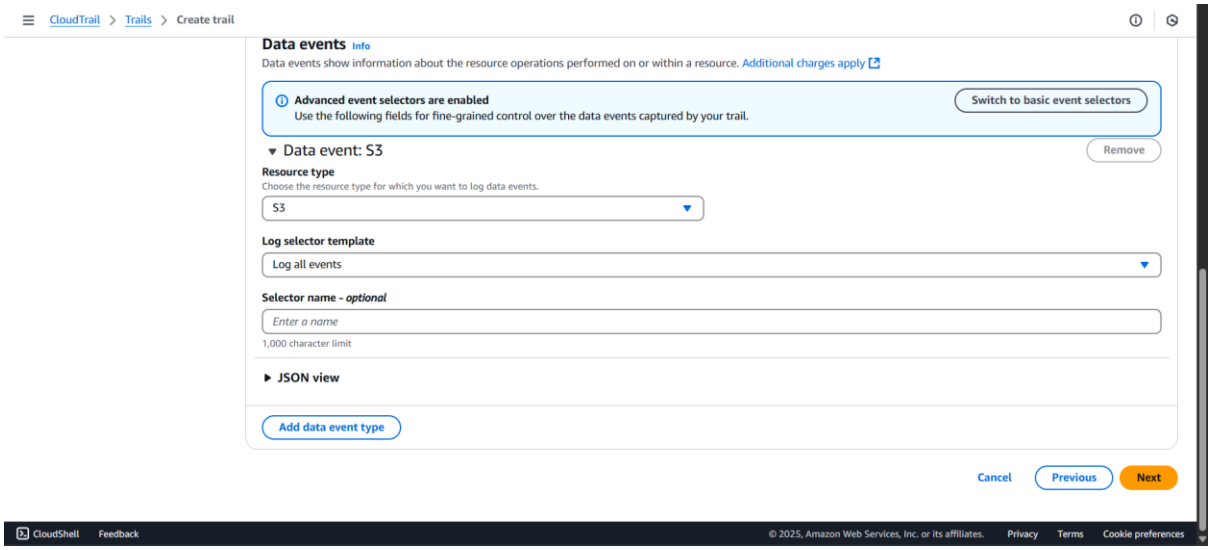


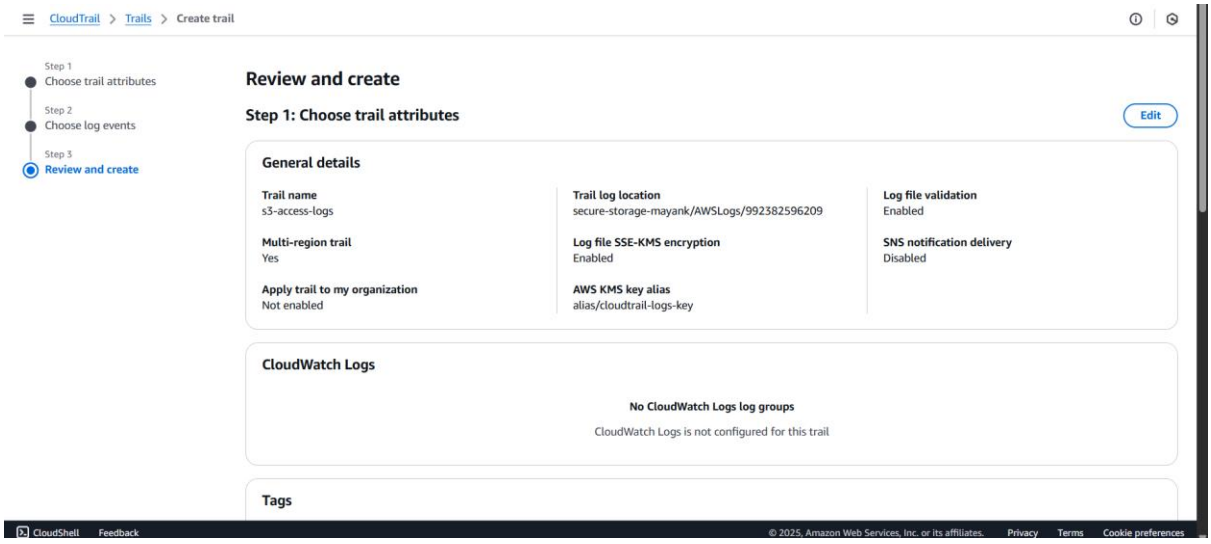

25. Choose the events you want to log in Managed events.

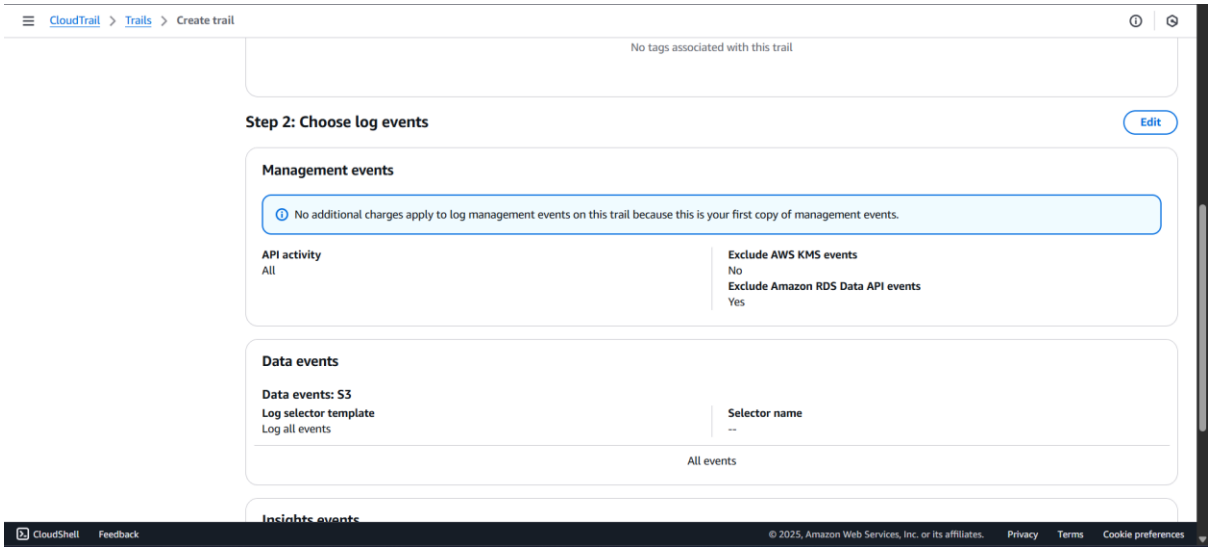


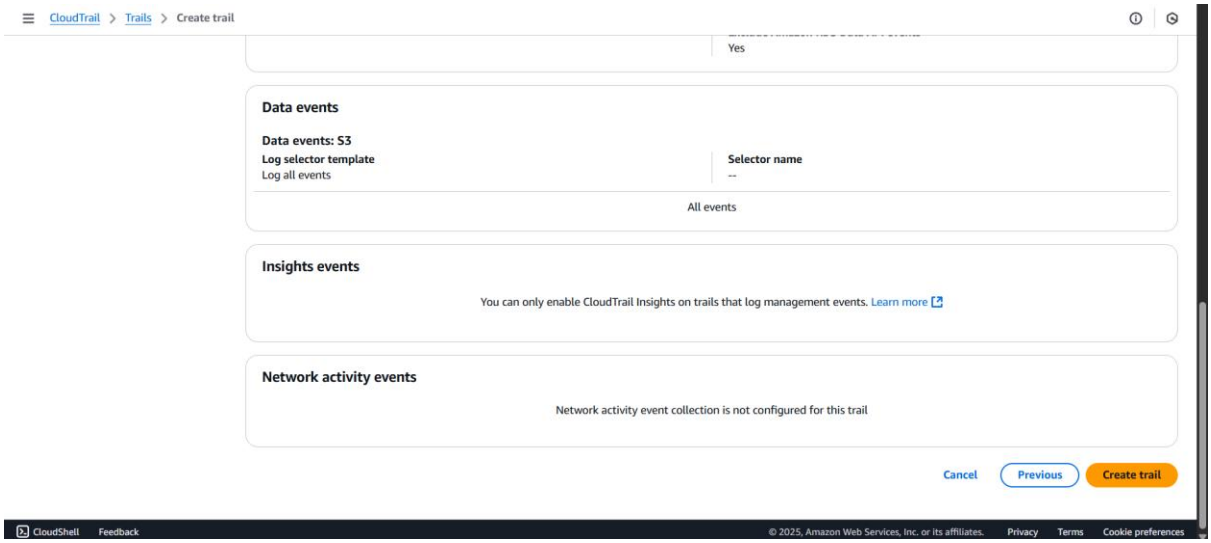

26. In Data events, select **Resource Type** as **S3** and **Log all events**.



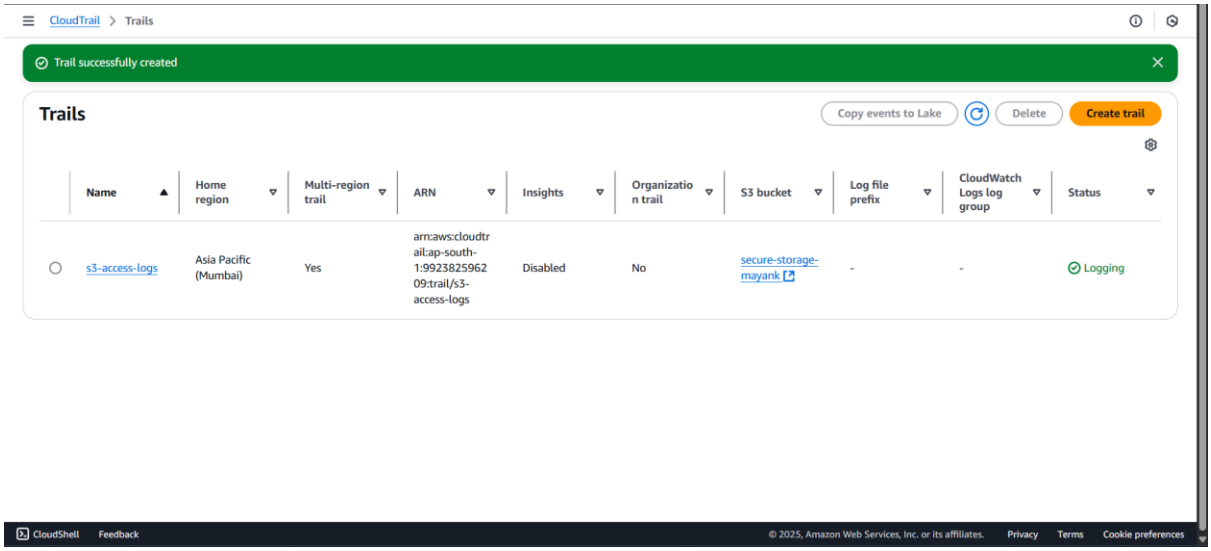

27. Review the information and click on **Create Trail**.



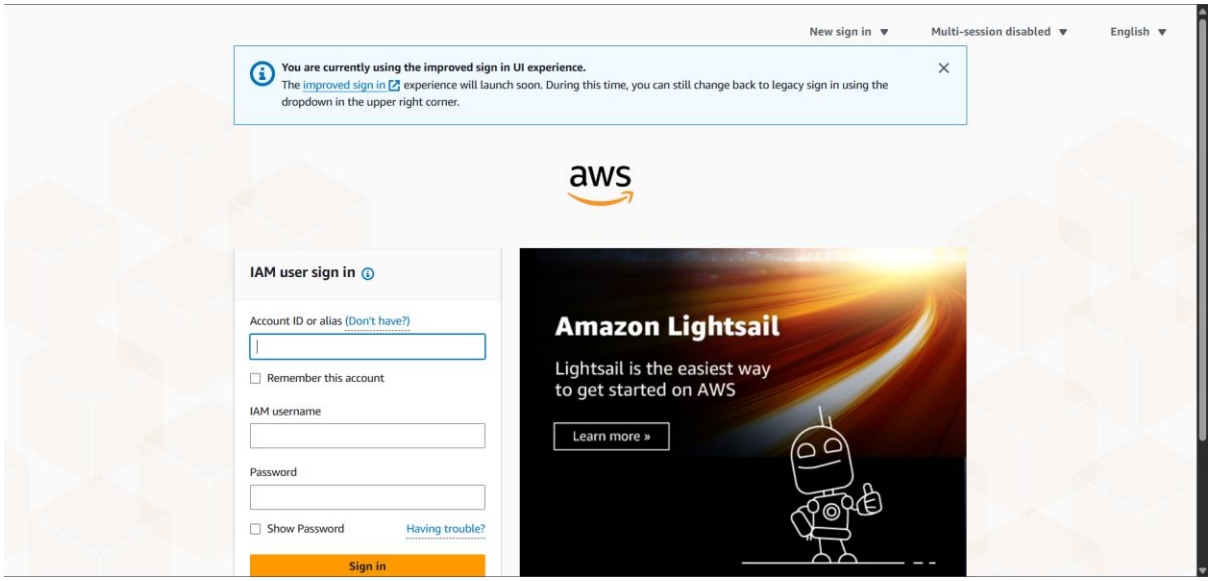


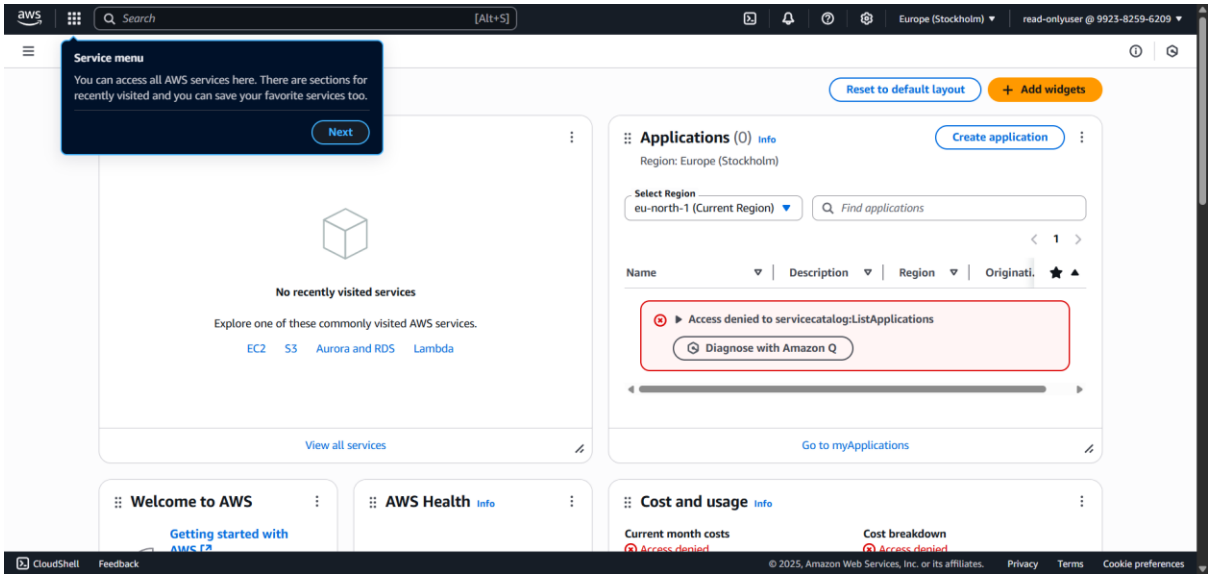




28. Trail successfully created message appears.

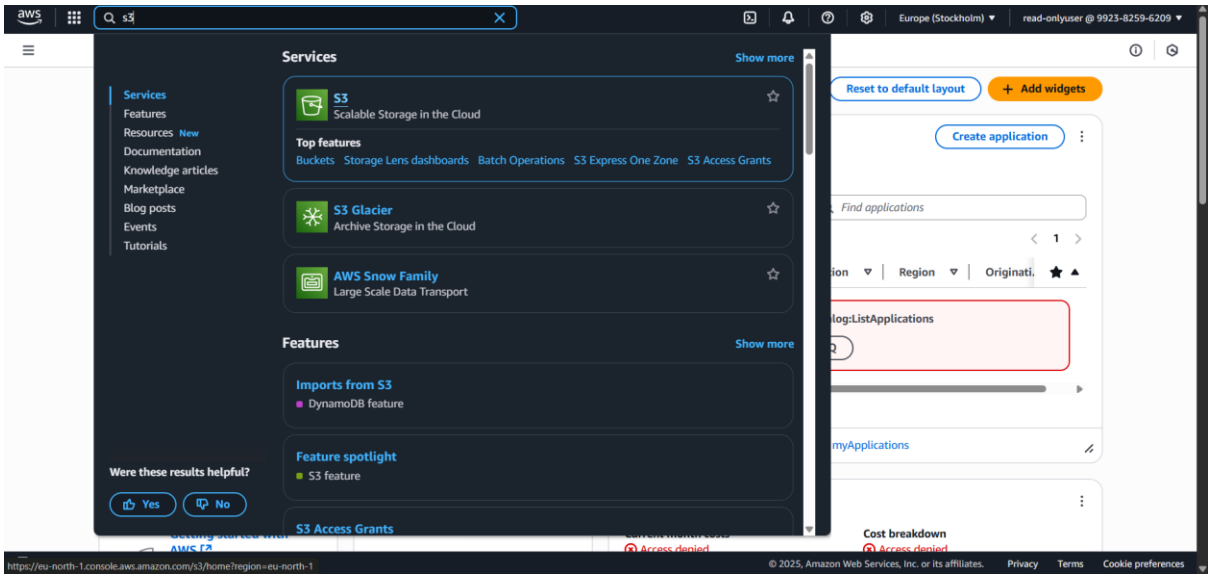



29. Login to the new user that you created (read-onlyuser).

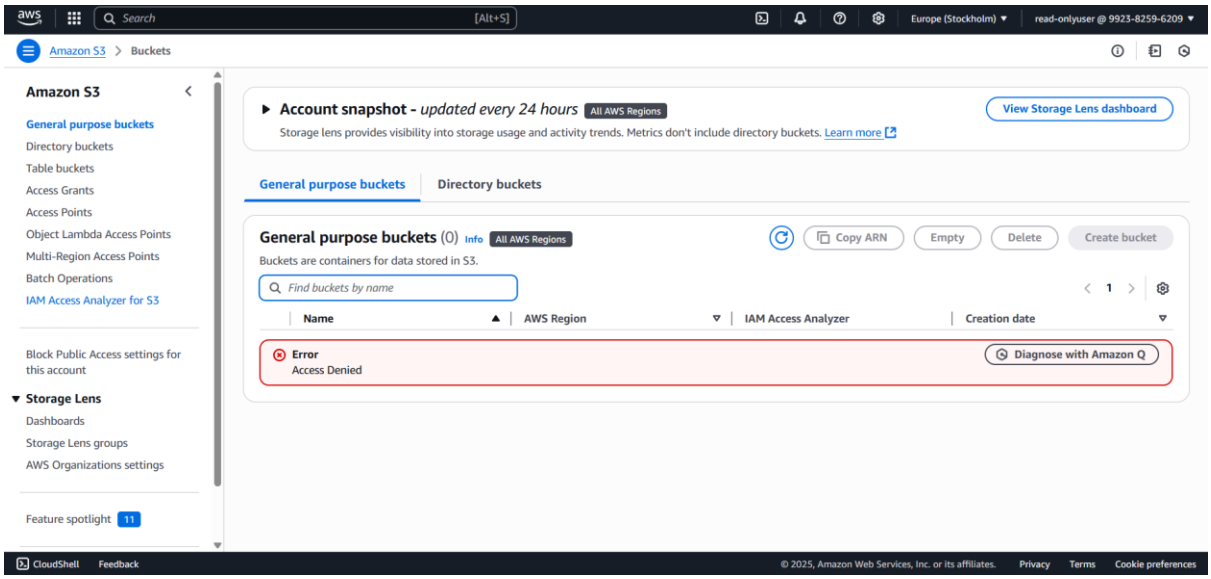


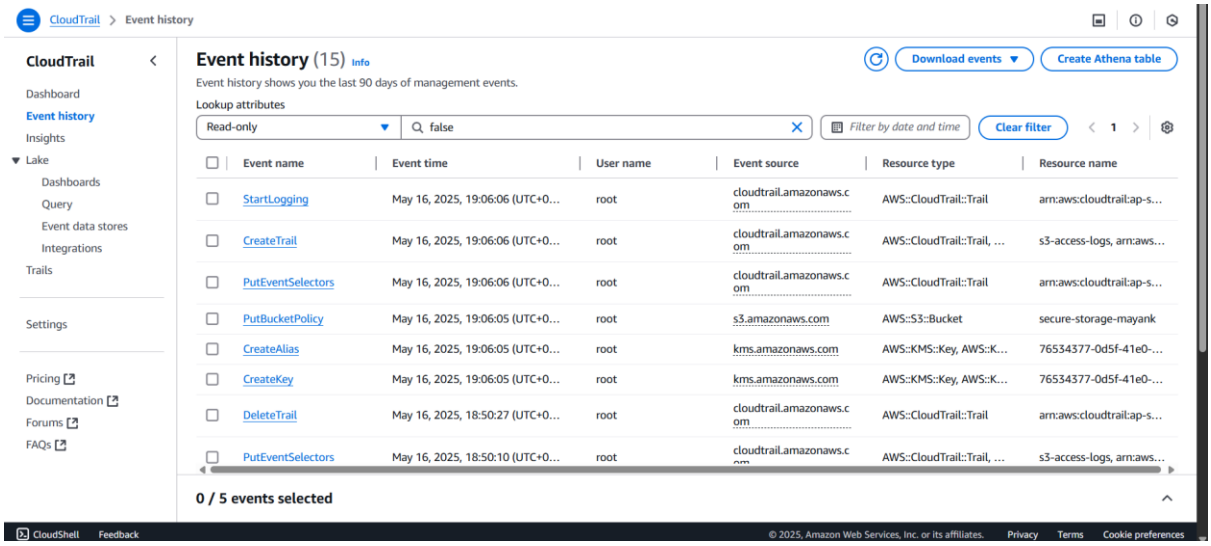

30. Go to S3 using the new user.

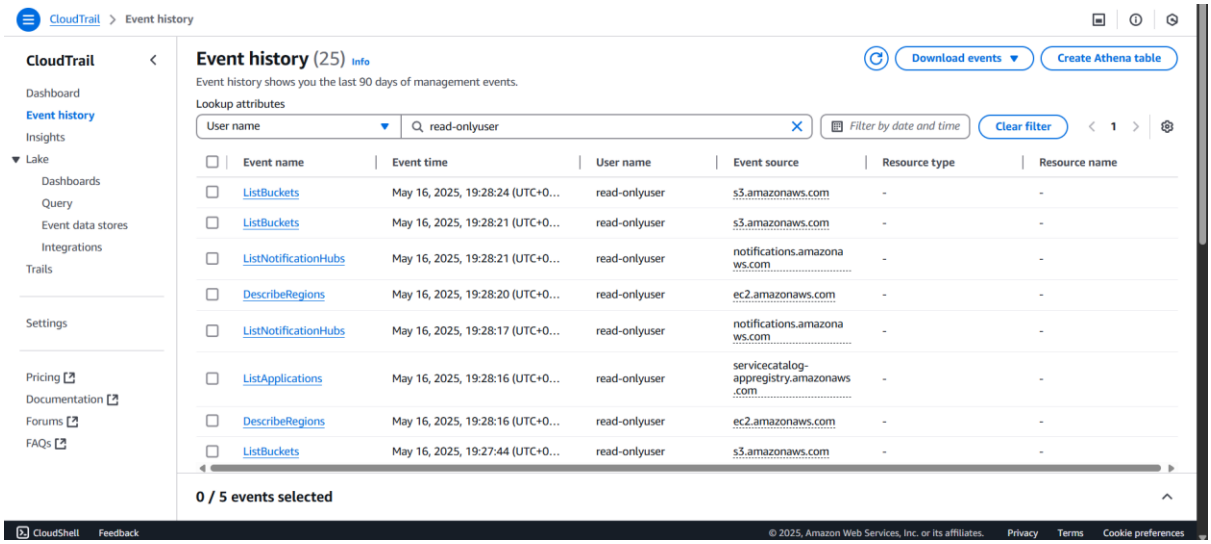


31. You will see that the **Access Denied** message, as the user does not have permission.




32. Now go to the root user and then go to **Event History** in **Cloudtrail** to see the audit logs from root user and read-onlyuser.




CloudTrail > Event history
CloudTrail
Dashboard
Event history
Insights
Lake
Dashboards
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Forums
FAQs
Event history (25) Info
Event history shows you the last 90 days of management events.
Download events
Create Athena table
Lookup attributes
User name
read-onlyuser
Filter by date and time
Clear filter
1
Event name
Event time
User name
Event source
Resource type
Resource name
ListBuckets
May 16, 2025, 19:28:24 (UTC+0...
read-onlyuser
s3.amazonaws.com
ListBuckets
May 16, 2025, 19:28:21 (UTC+0...
read-onlyuser
s3.amazonaws.com
ListNotificationHubs
May 16, 2025, 19:28:21 (UTC+0...
read-onlyuser
notifications.amazonaws.com
DescribeRegions
May 16, 2025, 19:28:20 (UTC+0...
read-onlyuser
ec2.amazonaws.com
ListNotificationHubs
May 16, 2025, 19:28:17 (UTC+0...
read-onlyuser
notifications.amazonaws.com
ListApplications
May 16, 2025, 19:28:16 (UTC+0...
read-onlyuser
servicecatalog-appregistry.amazonaws.com
DescribeRegions
May 16, 2025, 19:28:16 (UTC+0...
read-onlyuser
ec2.amazonaws.com
ListBuckets
May 16, 2025, 19:27:44 (UTC+0...
read-onlyuser
s3.amazonaws.com
0 / 5 events selected
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences