Project Overview

Goal:

Enable secure, automated access to AWS S3 buckets from Linux systems using IAM roles/policies and local permission controls.

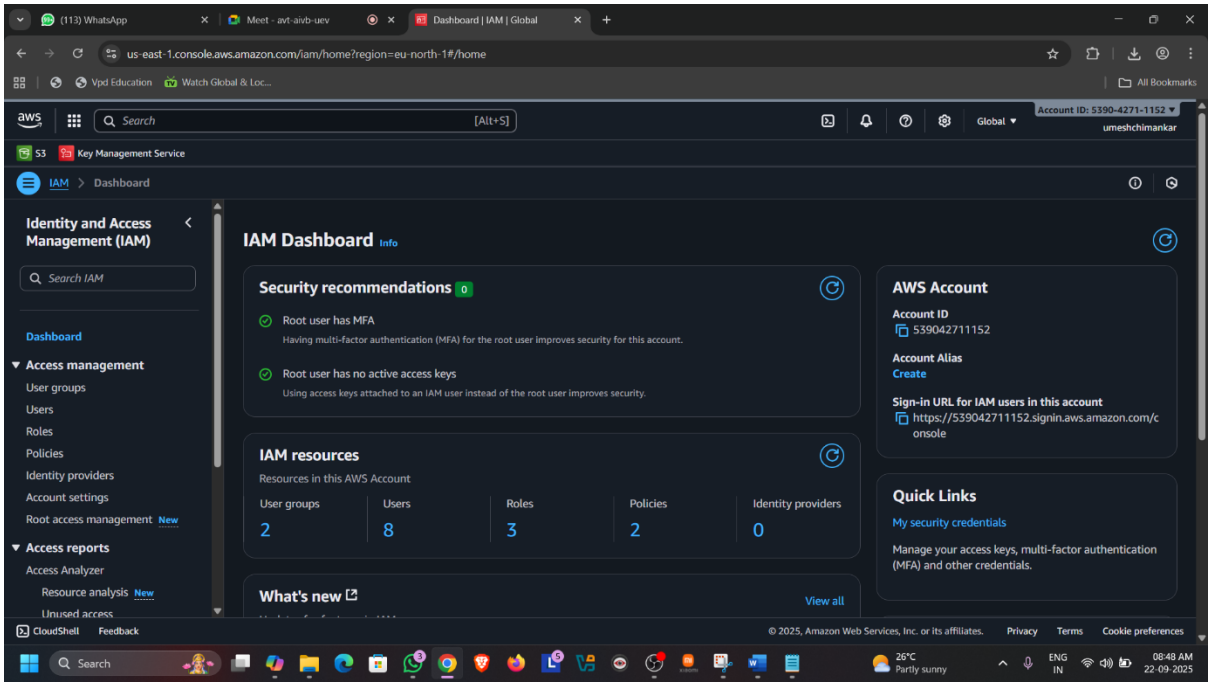
Use Case Examples:

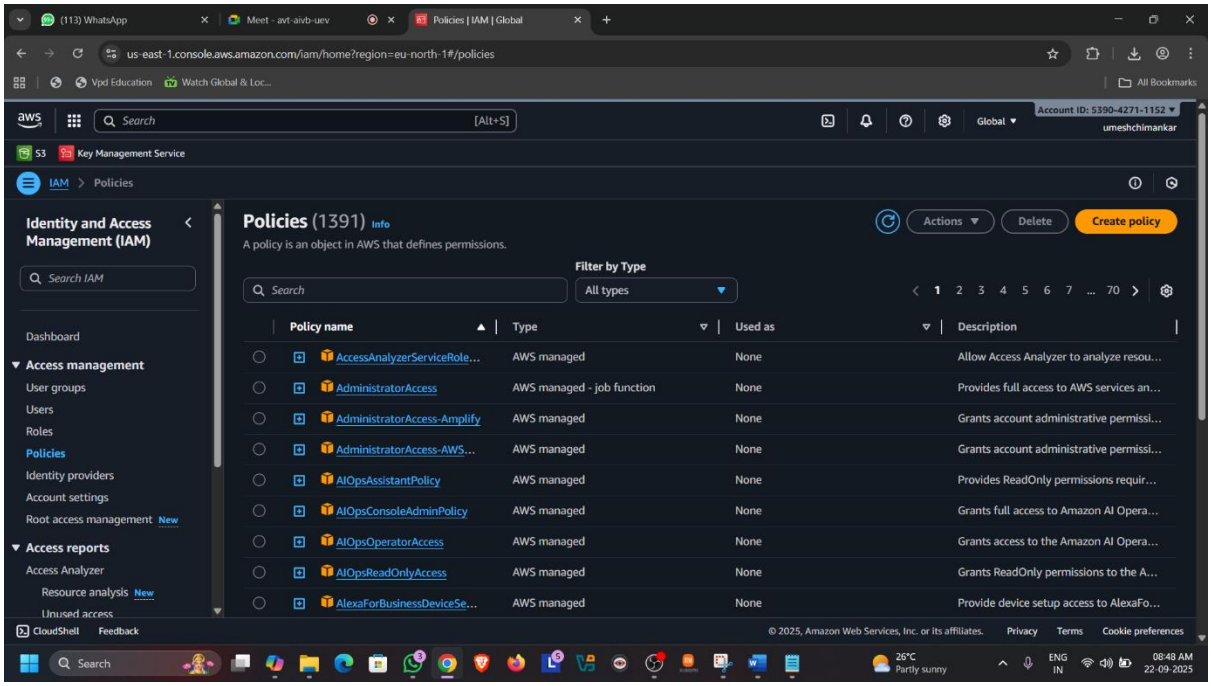
- Centralized logging to S3 from Linux VMs
- Backup scripts pushing data to S3
- Controlled access for specific users/groups on Linux

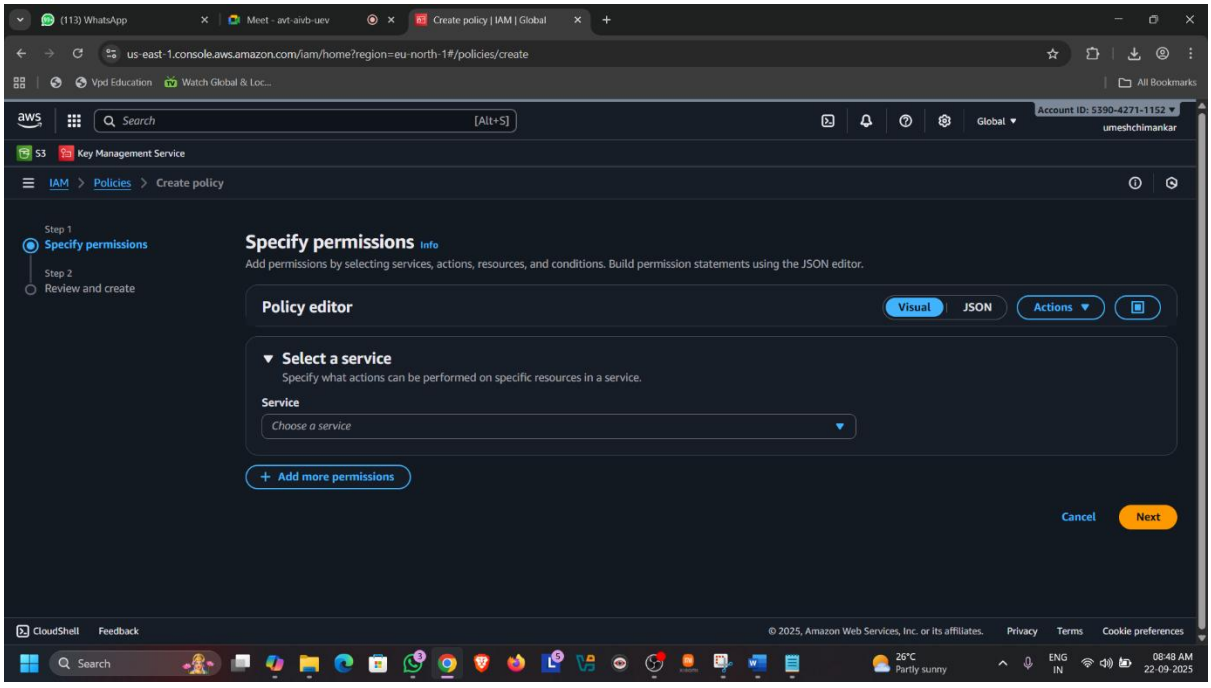
Key Components

Step 1. IAM Policy Design and S3 Bucket Creation

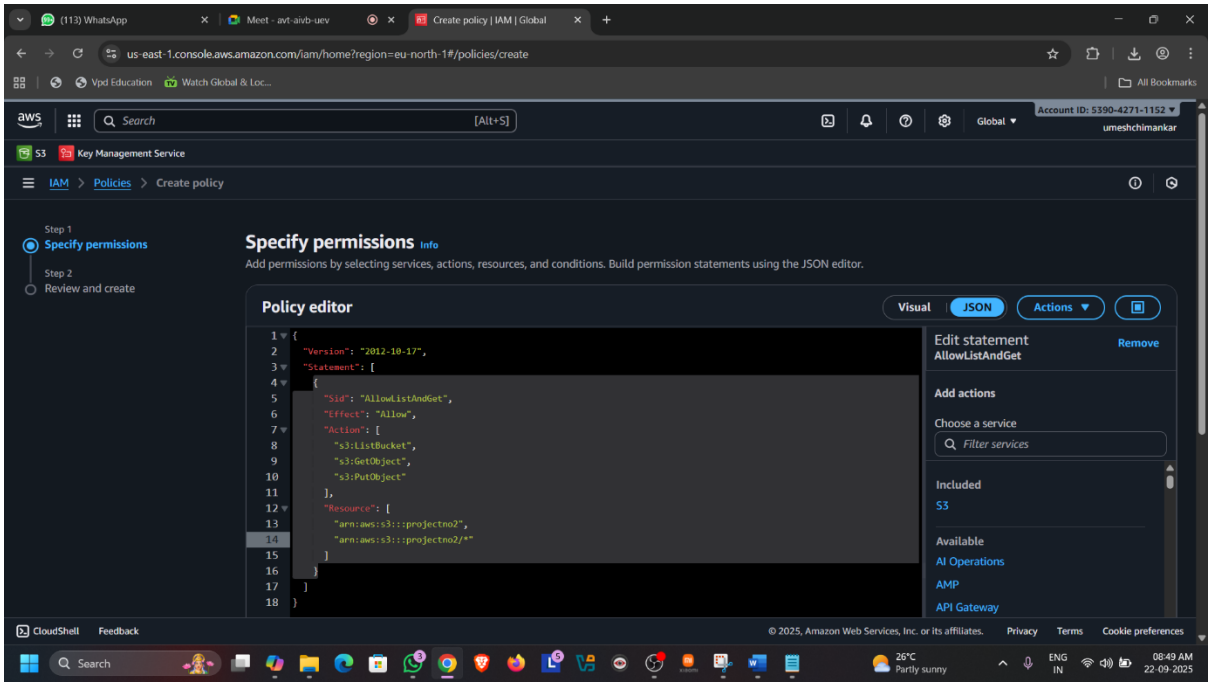
Goto IAM Service

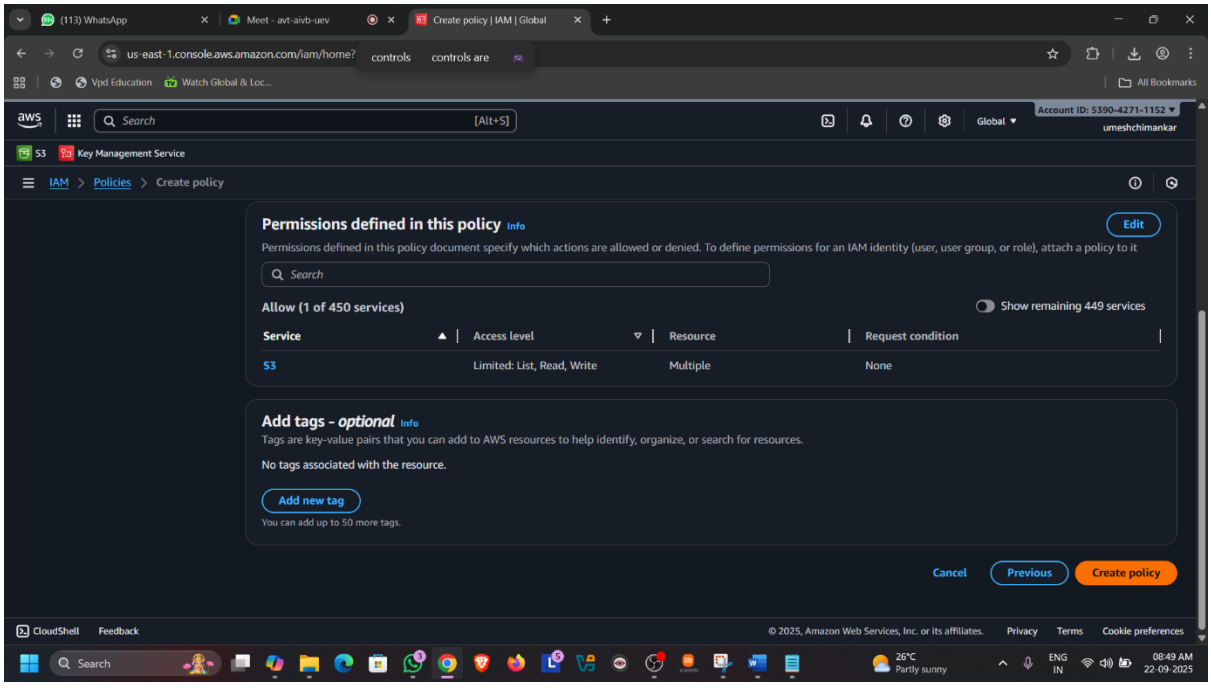


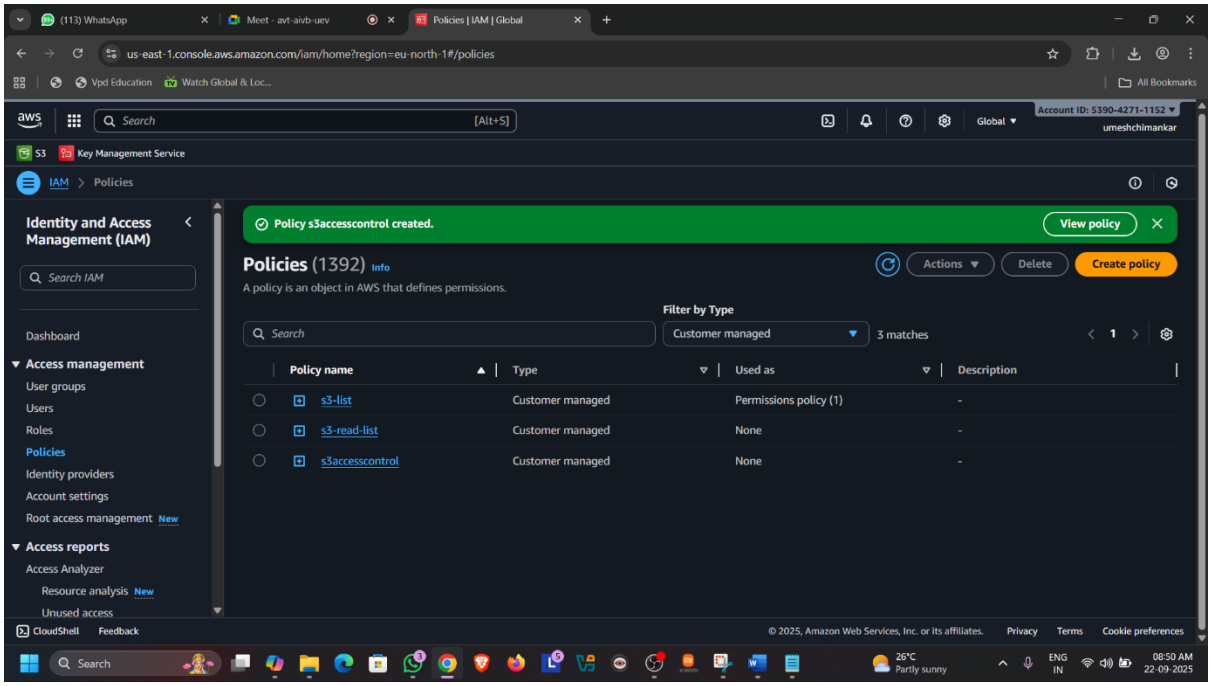




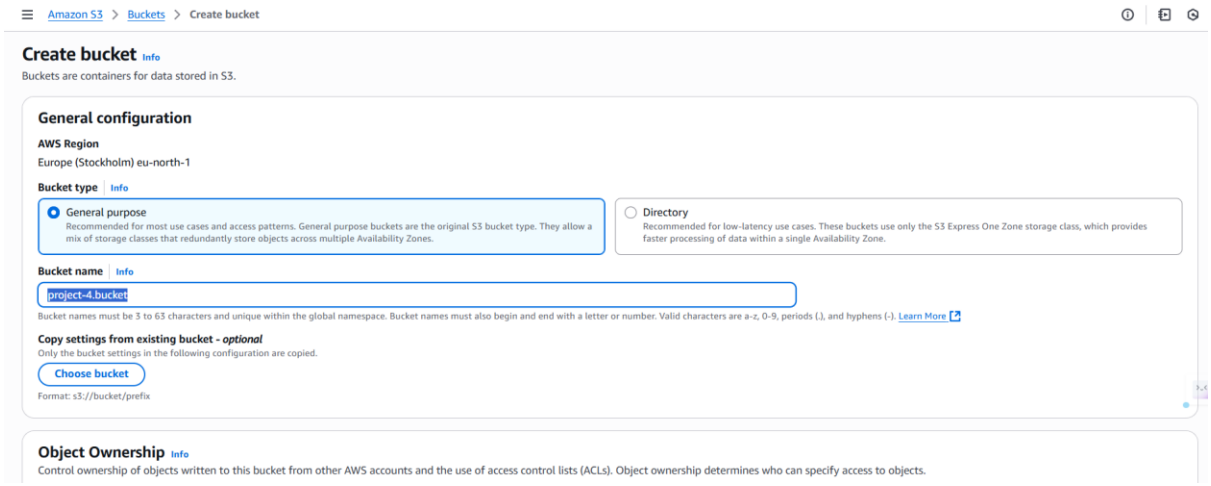
Create a fine-grained IAM policy to control access to specific S3 buckets.


Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create
Account ID: 5390-4271-1152
umeshchimankar
IAM > Policies > Create policy
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
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AllowListAndGet",
"Effect": "Allow",
"Action": [
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject"
],
"Resource": [
"arn:aws:s3:::projectno2",
"arn:aws:s3:::projectno2/*"
]
}
]
}
Edit statement
AllowListAndGet
Remove
Add actions
Choose a service
Filter services
Included
S3
Available
AI Operations
AMP
API Gateway
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?
controls
controls are
Account ID: 5390-4271-1152
umeshchimankar
IAM > Policies > Create policy
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (1 of 450 services)
Show remaining 449 services
Service
Access level
Resource
Request condition
S3
Limited: List, Read, Write
Multiple
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.
Cancel
Previous
Create policy
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



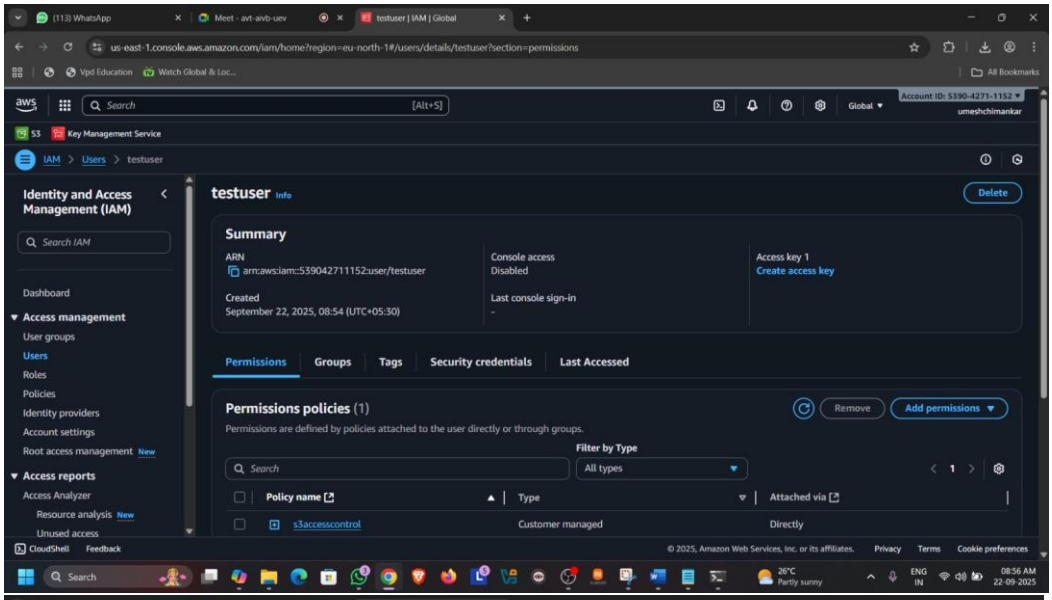
Now create S3 Bucket

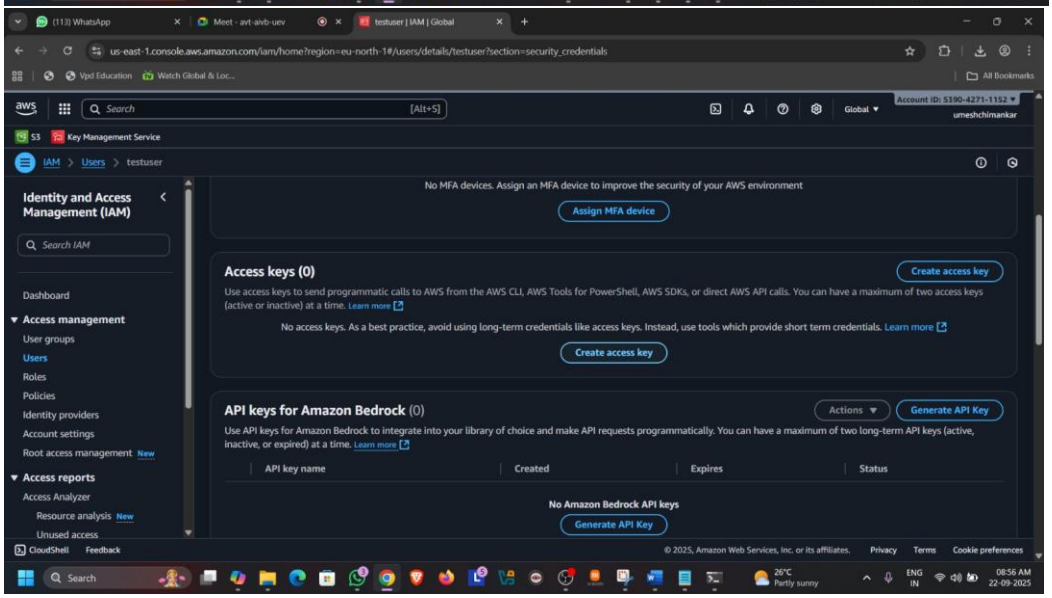


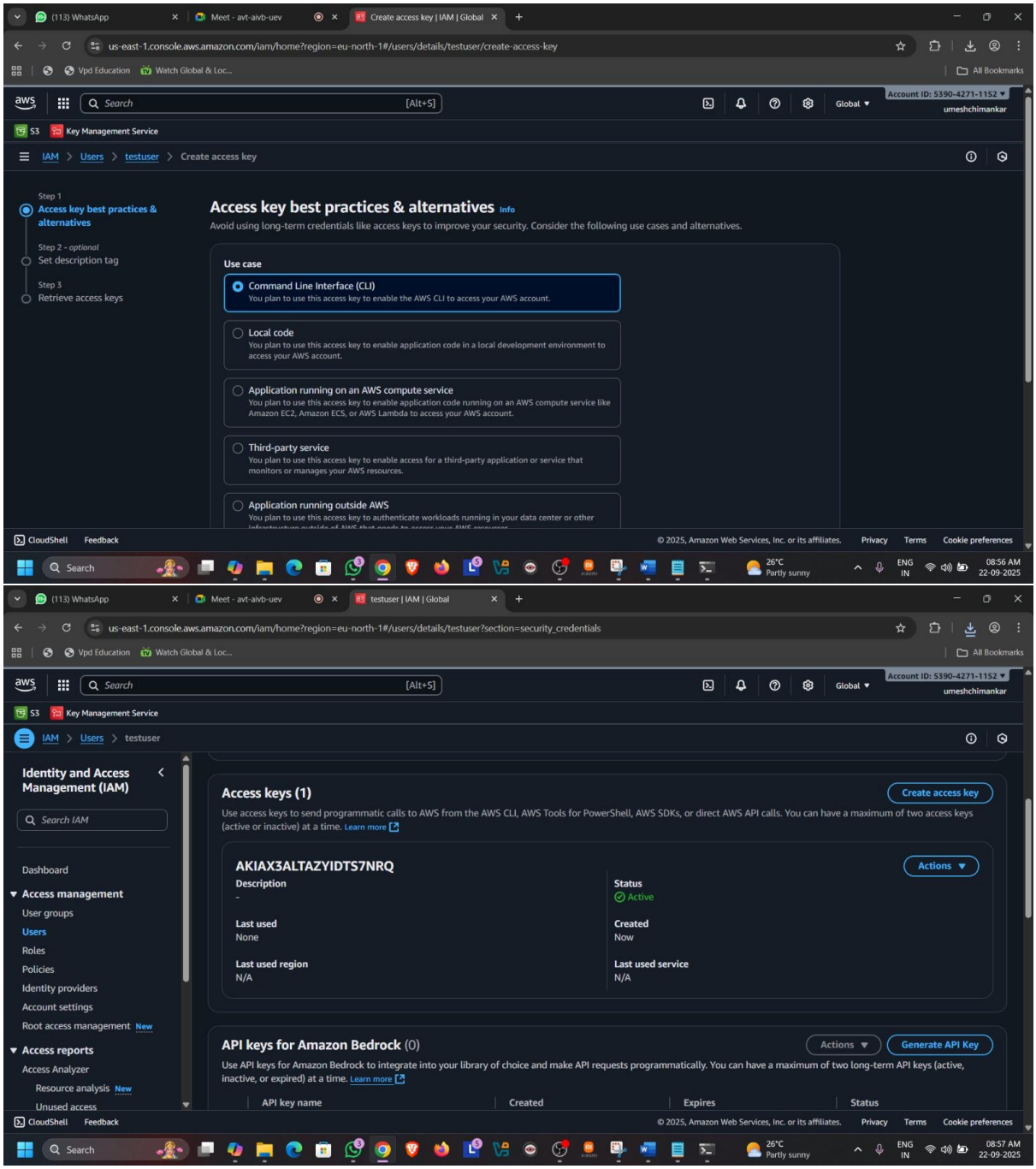
Step 2. IAM Role or User Setup

- Attach the above policy to an IAM role (for EC2) or IAM user (for CLI access).
- If using EC2, assign the role to the instance via instance profile.

Create user “testuser” and download their access key


testuser | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/testuser?section=permissions
Search
[Alt+S]
Global
Account ID: 5390-4271-1152
umeshchimankar
Key Management Service
IAM > Users > testuser
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Unused access
testuser Info
Delete
Summary
ARN
arn:aws:iam::539042711152:user/testuser
Console access
Disabled
Access key 1
Create access key
Created
September 22, 2025, 08:54 (UTC+05:30)
Last console sign-in
-
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
Search
All types
Policy name
Type
Attached via
s3accesscontrol
Customer managed
Directly
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
26°C
Partly sunny
ENG
IN
08:56 AM
22-09-2025


testuser | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/testuser?section=security_credentials
Search
[Alt+S]
Global
Account ID: 5390-4271-1152
umeshchimankar
Key Management Service
IAM > Users > testuser
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Unused access
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device
Access keys (0)
Create access key
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more
No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more
Create access key
API keys for Amazon Bedrock (0)
Actions
Generate API Key
Use API keys for Amazon Bedrock to integrate into your library of choice and make API requests programmatically. You can have a maximum of two long-term API keys (active, inactive, or expired) at a time. Learn more
API key name
Created
Expires
Status
No Amazon Bedrock API keys
Generate API Key
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
26°C
Partly sunny
ENG
IN
08:56 AM
22-09-2025

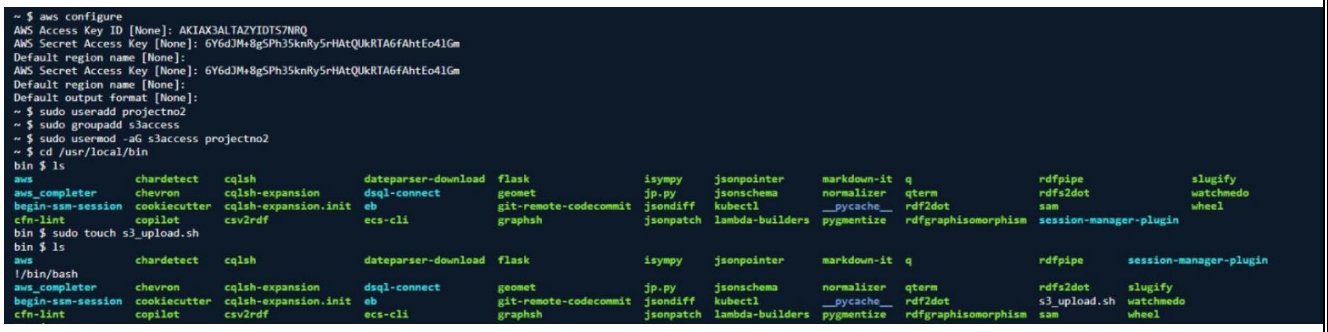


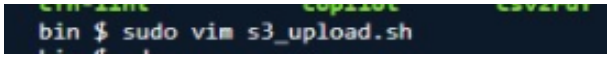
Step 3. Linux Configuration

Install AWS CLI & Configure Credentials

Open CloudShell and login through Access key.

Step 4. Create Local User & Group





create **s3_upload.sh** file and write below script

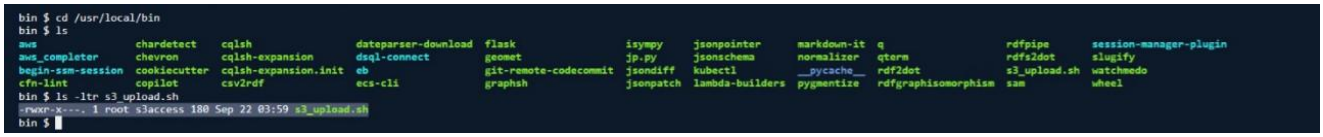
```
#!/bin/bash
# /usr/local/bin/s3_upload.sh
BUCKET="project-4.bucket"
FILE="$1"
if [[ ! -f "$FILE" ]]; then echo "File not found!"
exit 1
fi
aws s3 cp "$FILE" "s3://$BUCKET/"
```

Step 5. Set File Permissions

Ensure only authorized users can run the S3 access script.

Testing & Validation

- Test with a user in group.
- Validate IAM permissions.
- Monitor CloudTrail for access logs.



Contribution:

Sakshi Jain

Jay Soni

Nikita Binnar

Ankita Shinde

Umesh Chimankar

Kaveri Kanawade