Project Title: Hybrid Access Control for AWS S3 Using IAM and Linux User Management

**Description:**

This project demonstrates secure and controlled access to an Amazon S3 bucket by combining **AWS IAM policies** with **Linux-level user permissions** on an EC2 instance. The main goal is to ensure that only authorized users can access specific S3 resources — both from the AWS cloud perspective (IAM) and the local system perspective (Linux).

It involves:

* Creating an IAM policy that grants read-only access to a specific S3 bucket.
* Assigning the policy to an IAM user or EC2 role.
* Creating a Linux user on an EC2 instance and restricting access to AWS credentials and S3 scripts using file system permissions.
* Writing and executing a shell script that uses the AWS CLI to interact with the S3 bucket.
* Enforcing least-privilege access using both IAM policy and Linux system permissions.

**Key Features:**

* Fine-grained access to S3 buckets using IAM.
* Use of Aws cli for scripting S3 operations.
* Linux user management for secure on-instance access control.
* Practical implementation of cloud security best practices (least privilege principle).

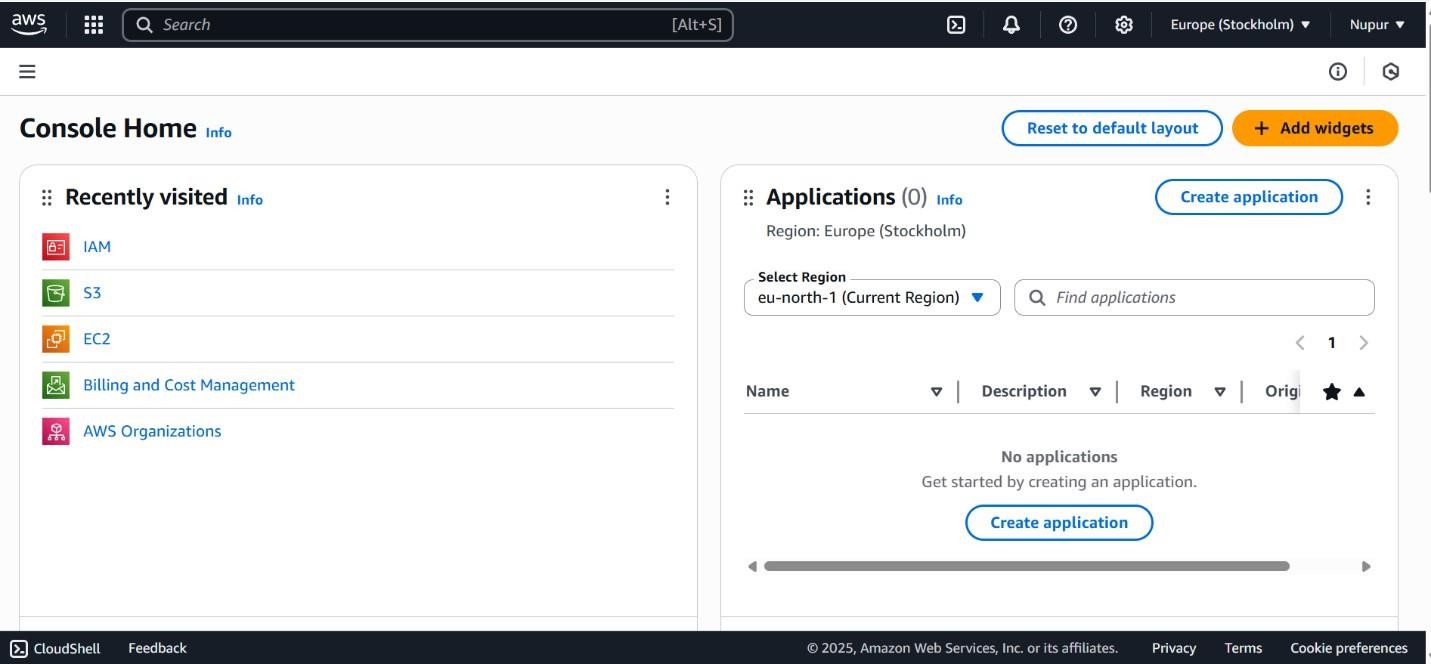
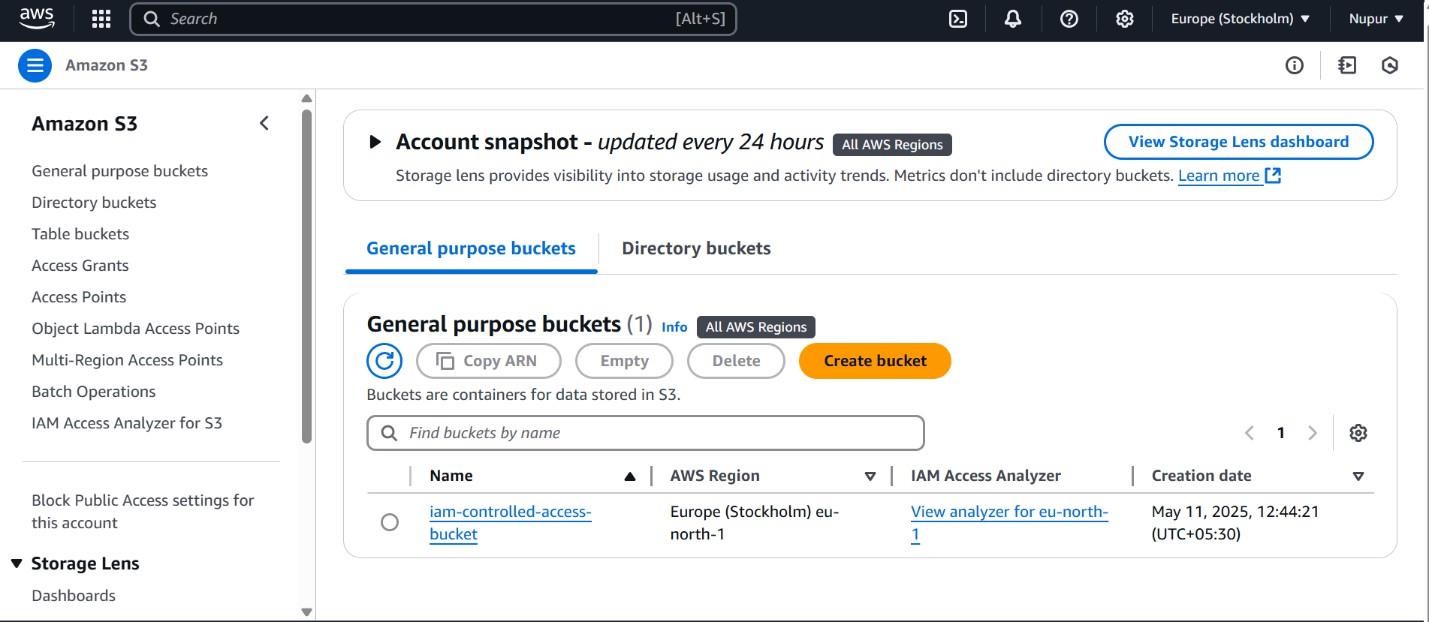
**Tools & Technologies:**

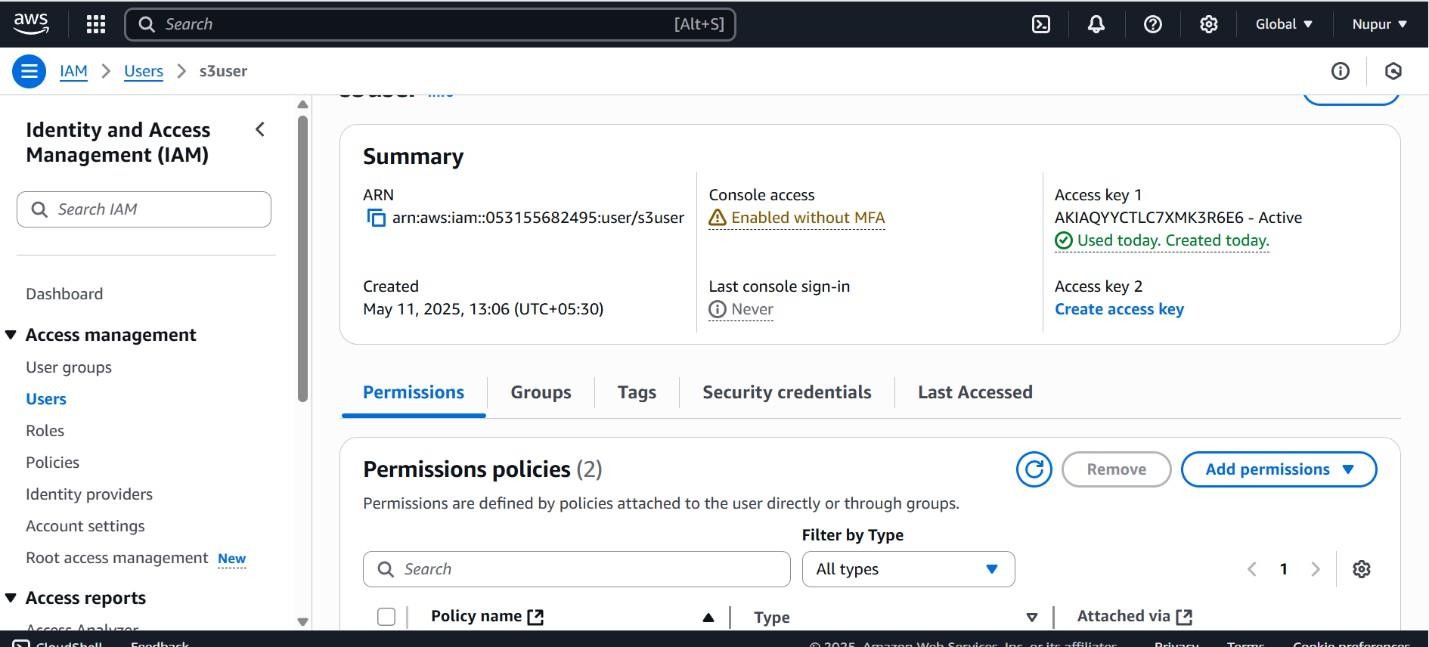
* **Amazon S3**
* **AWS IAM**
* **Amazon EC2 (Linux)**
* **AWS CLI**
* **Shell Scripting**
* **Linux (Ubuntu / Amazon Linux 2)**

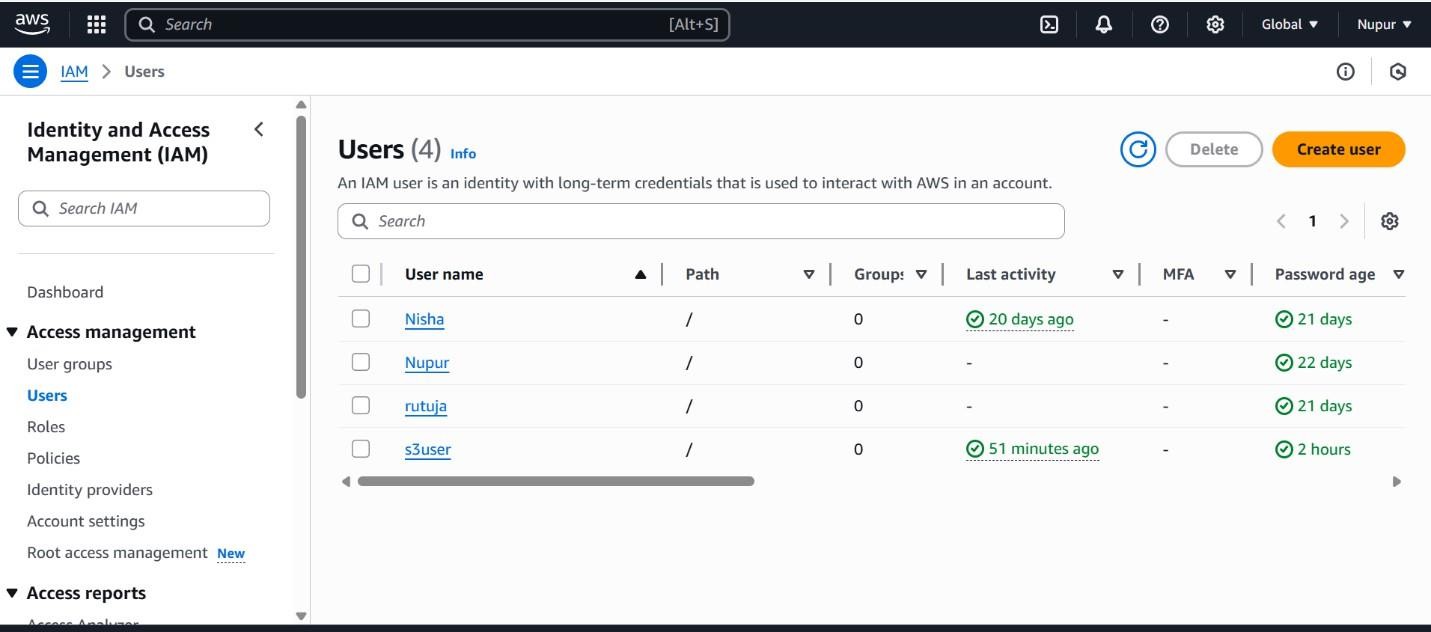
**Security Practices Used:**

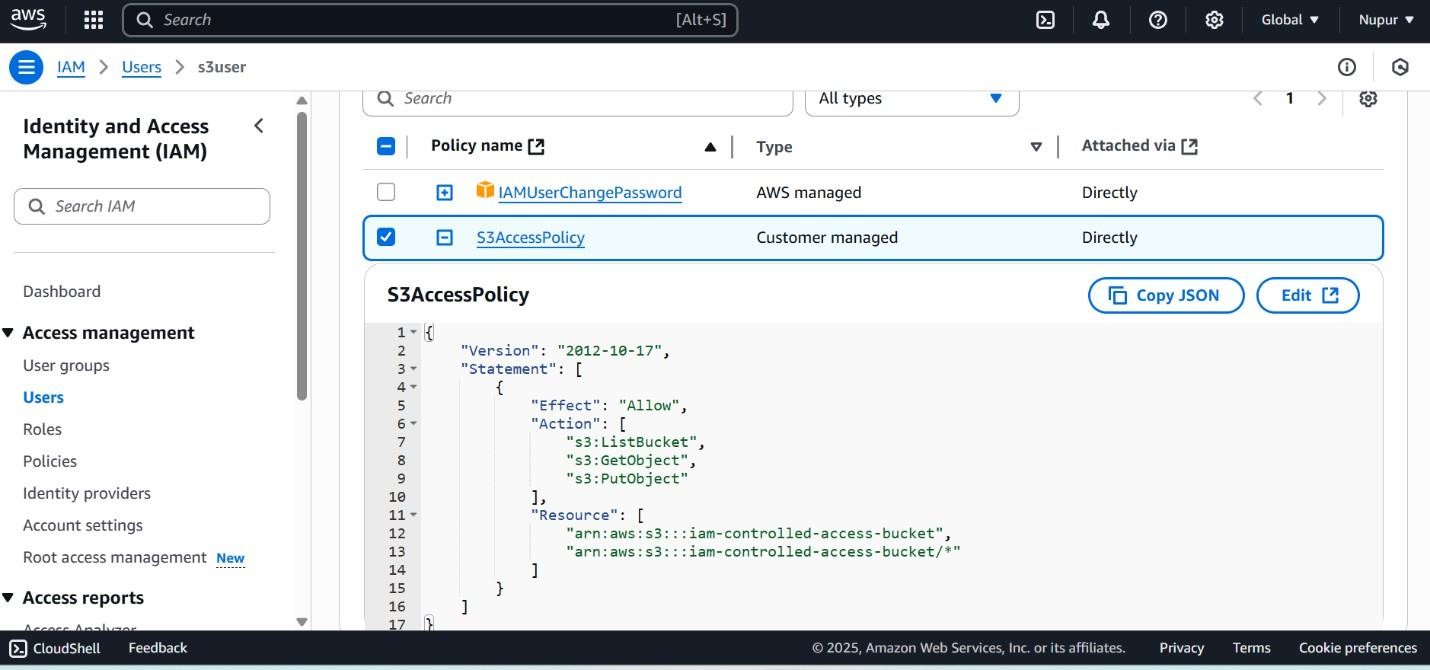
* IAM policy restrictions to bucket and actions.
* Linux file permission (chmod /chown) for user-based credential access control.
* Minimal permissions granted on both AWS and OS levels.

**Step-by-Step Guide:-**

1. **Log in to AWS Management Console.**
2. **Create an S3 Bucket**
3. **Go to IAM > Users > Add user.**

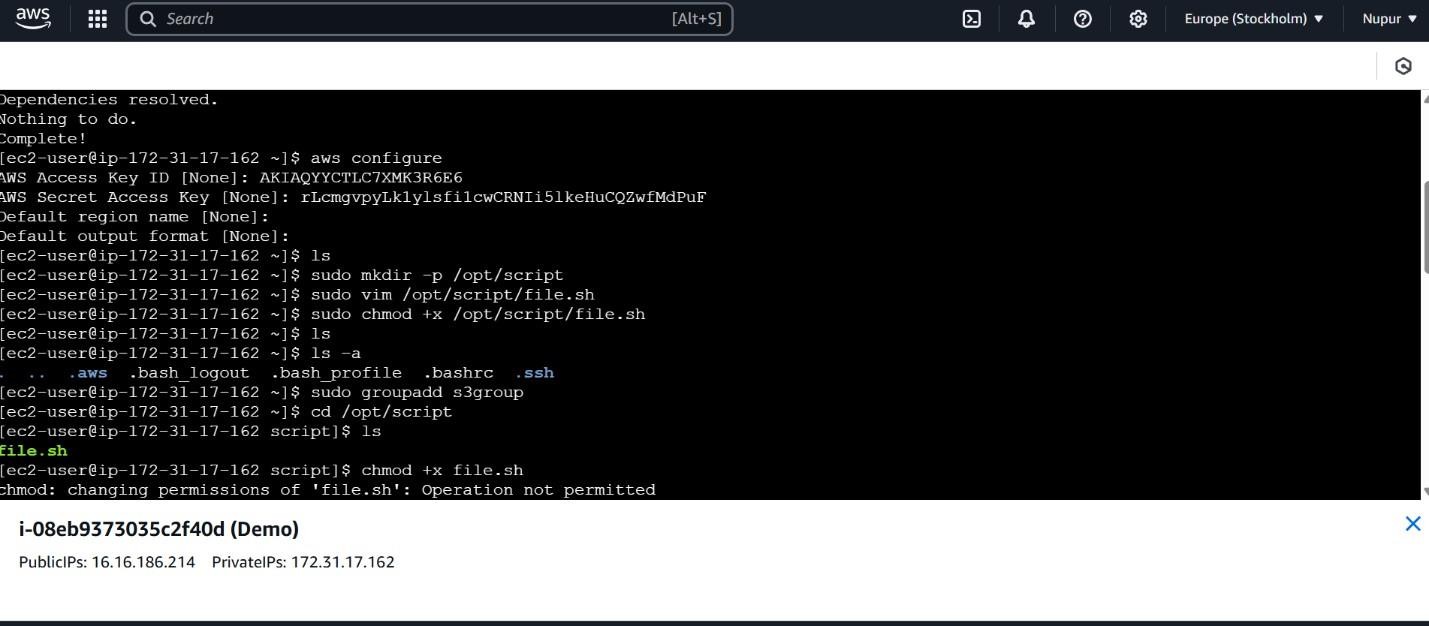
****

1. **Create a Custom IAM Policy -** In the IAM Console, go to Policies > Create policy. Use the JSON editor and paste the following policy

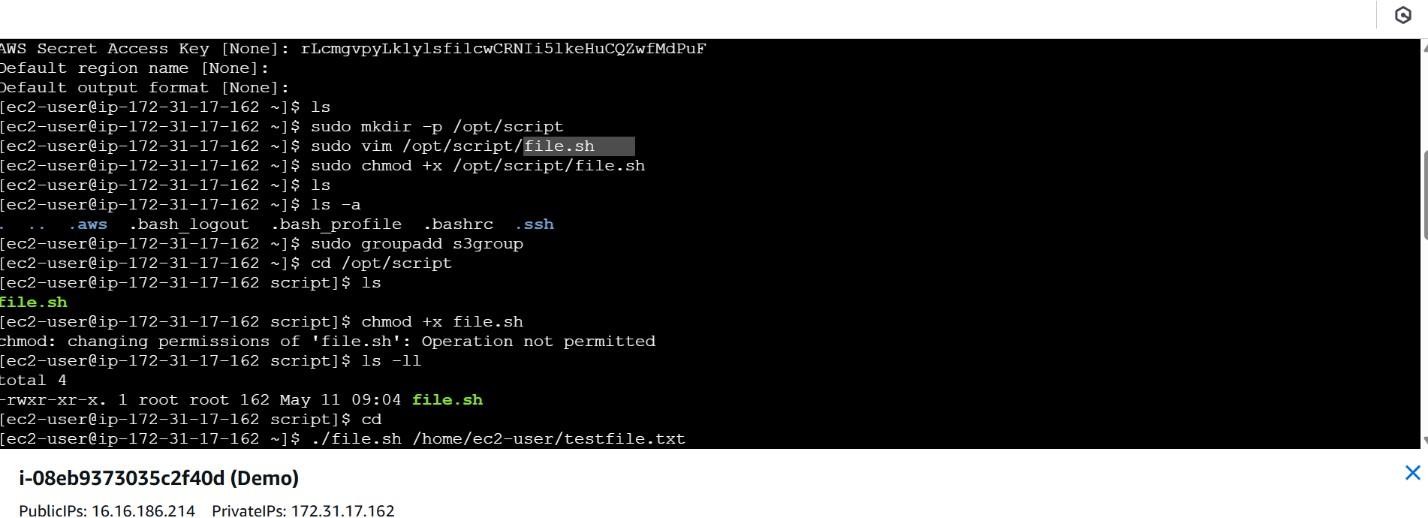


Click Review policy, give it a name, and click Create policy. Now assign this custom policy to the IAM user.

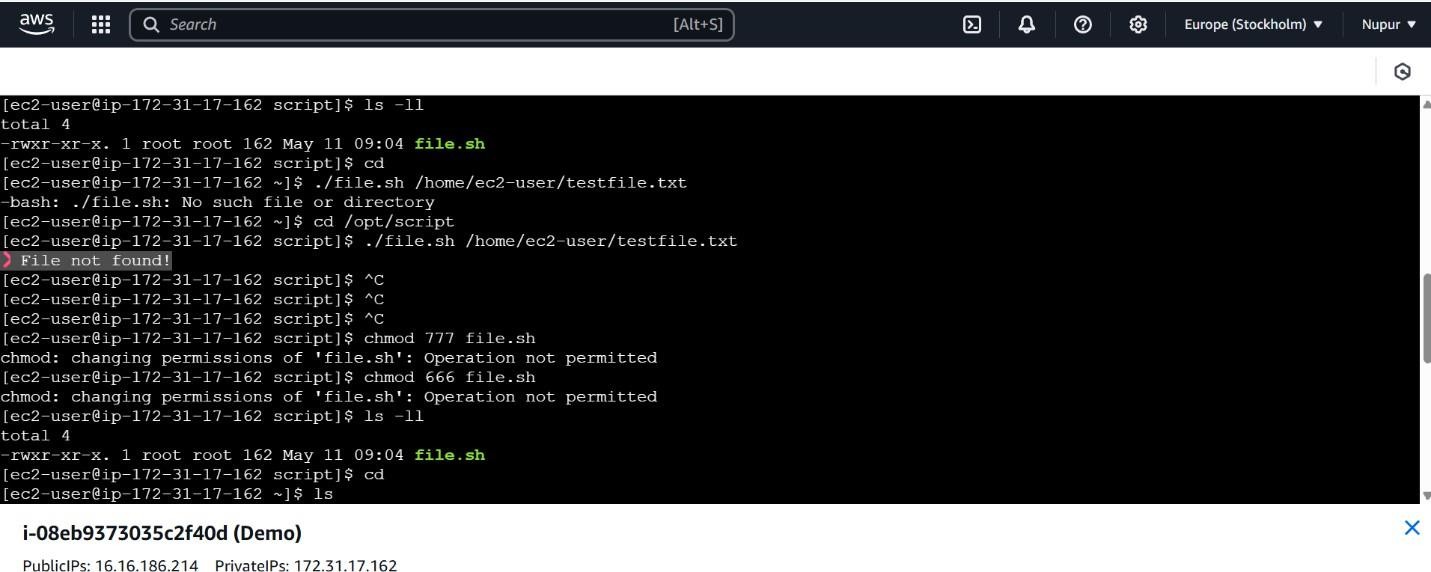
1. **Set Up AWS CLI on Linux**
2. Create folder



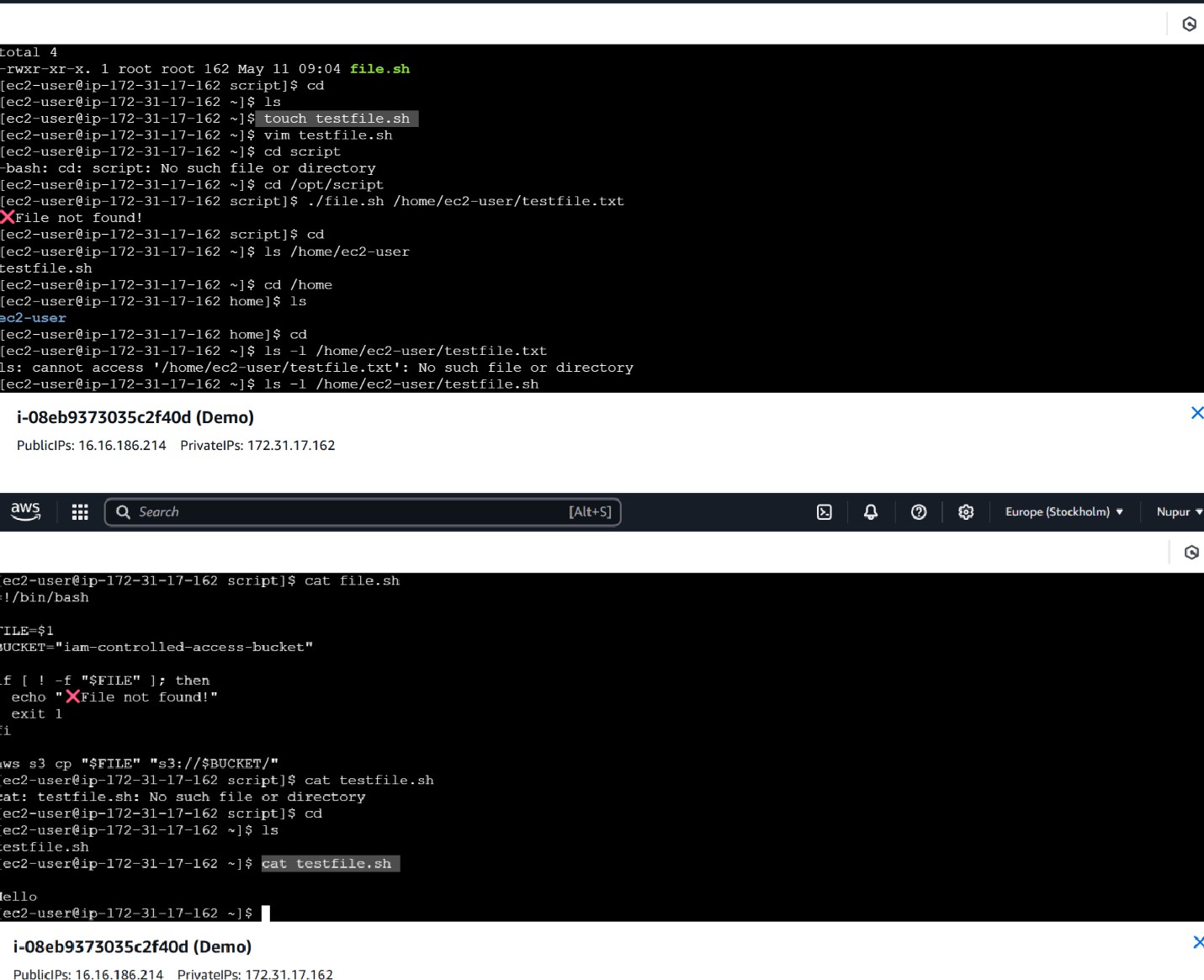
1. **Create the S3 Access Script**
2. **Assign Linux Permissions to the Script**



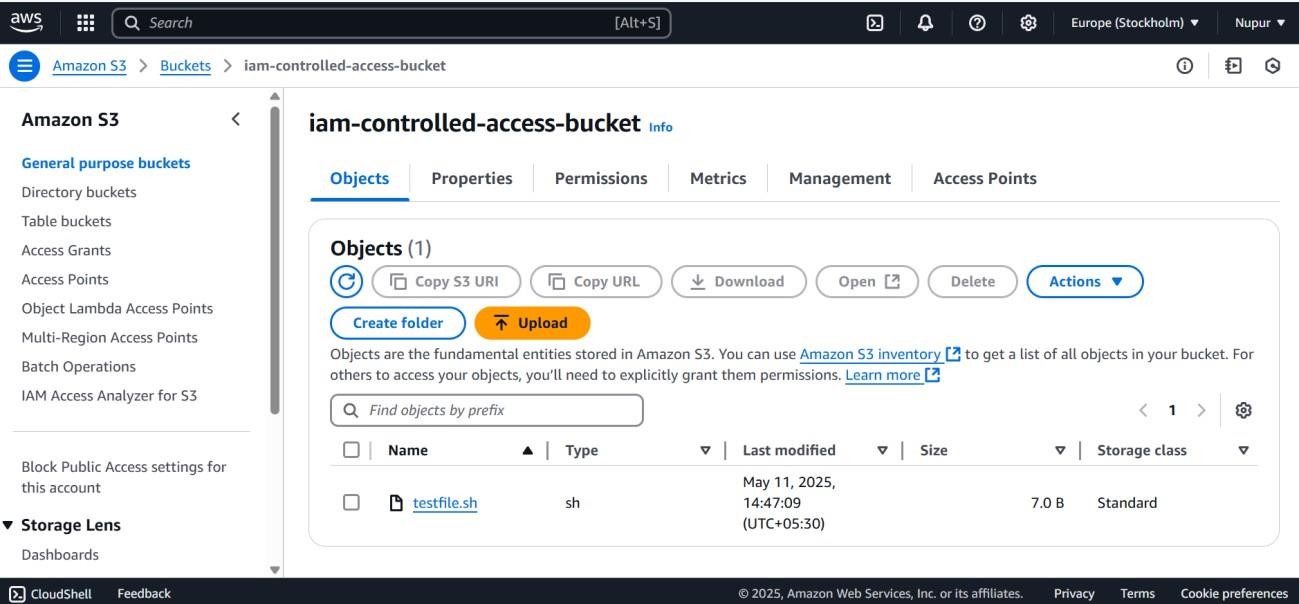
1. **Automate and Enhance the Script**
   * **Error Handling**: Add checks for errors in your script (e.g., if the file doesn’t exist or there’s an issue with permissions).
   * **Logging**: Log outputs into a file to track script activities.

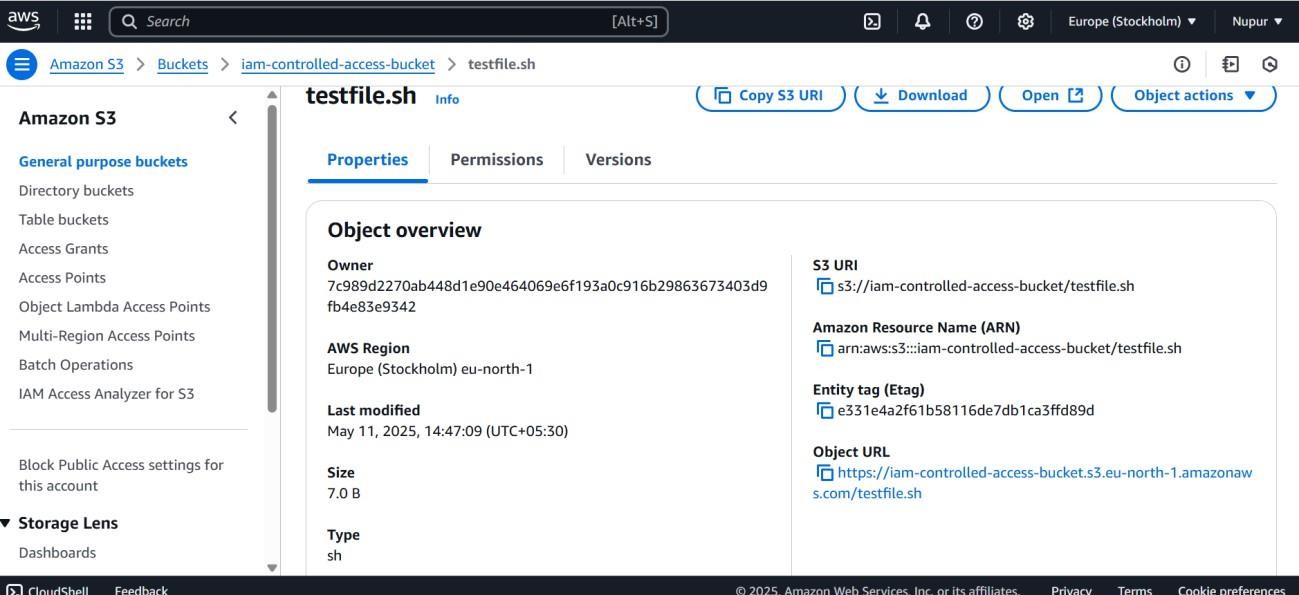


1. **File creation-**



1. **Verification and Permission Testing**

****



**Project Summary:**

This project demonstrates how to securely manage access to an AWS S3 bucket using a combination of IAM policies and Linux file permissions. It involves creating IAM users with specific access rights (read-only or full access) and automating S3 interactions (like file upload, download, and listing) through a Bash script using the AWS CLI. The script is permission-protected on the local Linux system to ensure only authorized users can execute it. This setup provides a secure, role-based access mechanism both at the cloud level (via IAM) and the system level (via Linux), ensuring controlled and automated S3 usage.