ITECH1502 Cybersecurity Fundamentals

Week 9 Lab Activities

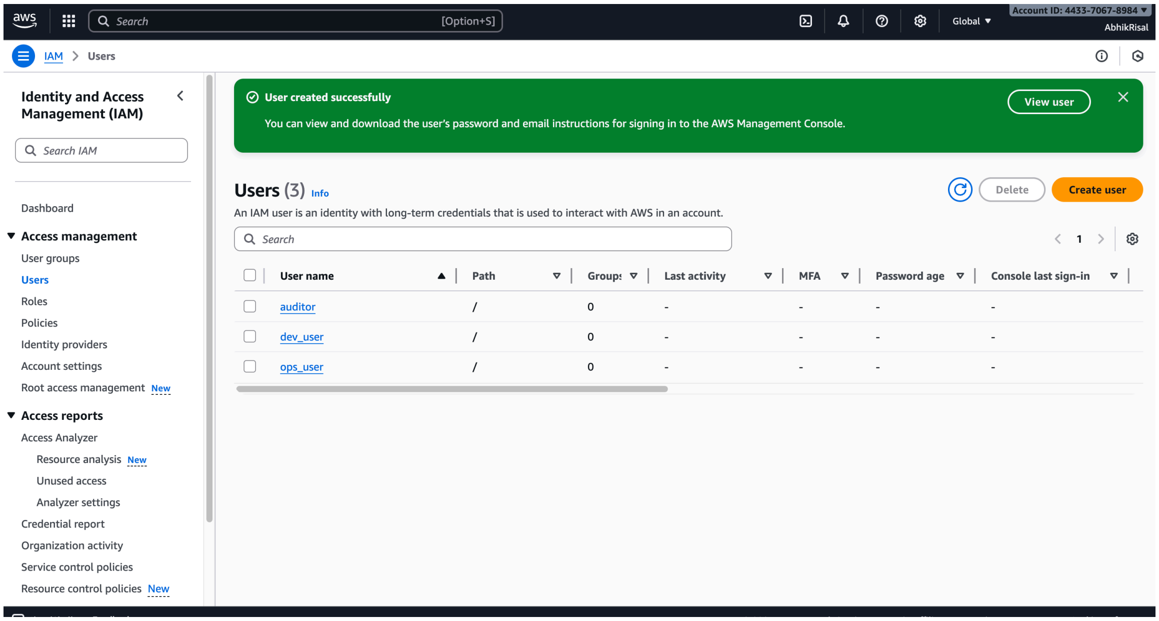
Network, Cloud, and Application Security

Task Overview

For Week 9, I selected the IAM Simulation & Least Privilege activity. The task required me to design IAM roles, create user accounts, enforce the principle of least privilege, and apply multi-factor authentication (MFA). I created three IAM users (`dev_user`, `ops_user`, and `auditor`), assigned each to a group with custom policies, and tested their permissions using the lab bucket `lab-abhikrisal`. Evidence from each step is provided below.

Evidence (Screenshots)

Screenshot 1: Users list (dev_user, ops_user, auditor).



User created successfully

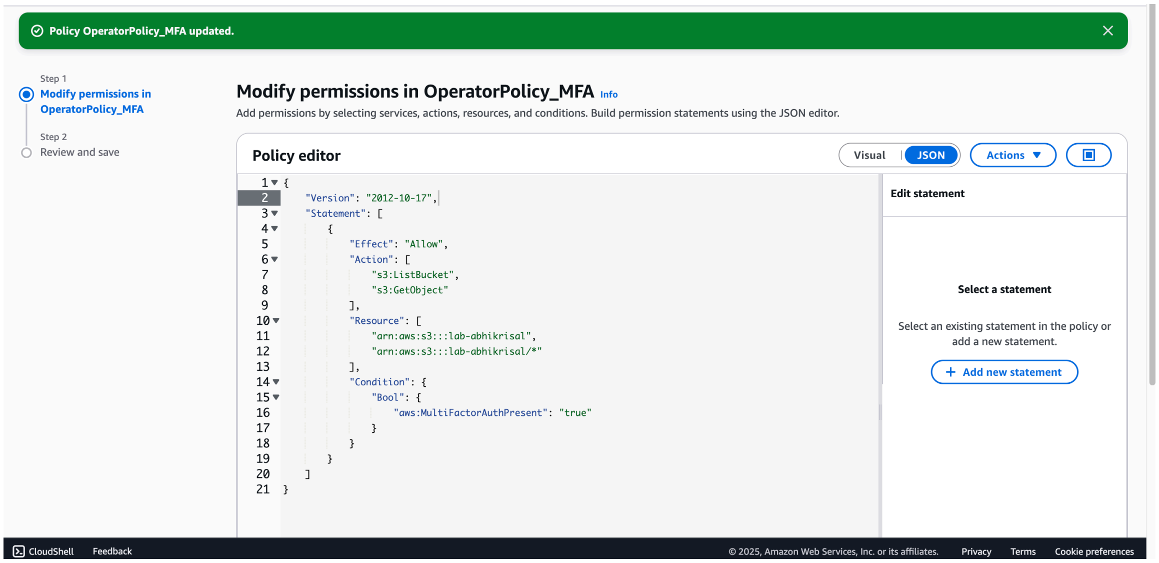
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Users (3) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in
auditor	/	0	-	-	-	-
dev_user	/	0	-	-	-	-
ops_user	/	0	-	-	-	-

Screenshot 2: Role/Policy JSON or attachment for least privilege setup.



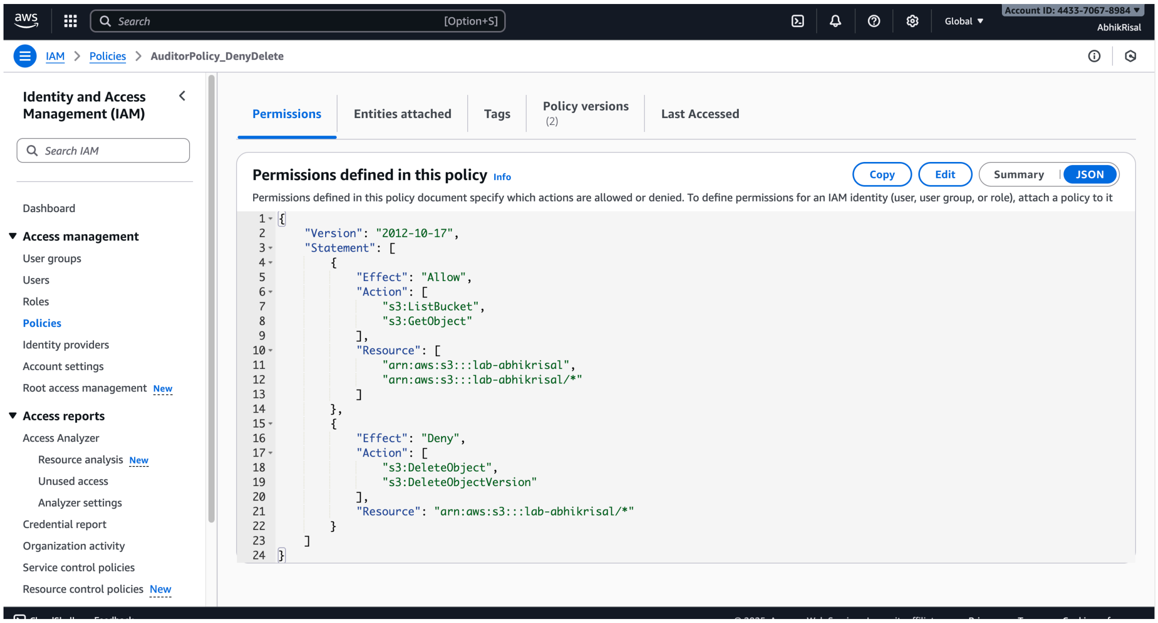
Policy OperatorPolicy_MFA updated.

Modify permissions in OperatorPolicy_MFA

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::lab-abhikrisal",
                "arn:aws:s3:::lab-abhikrisal/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        }
    ]
}
```

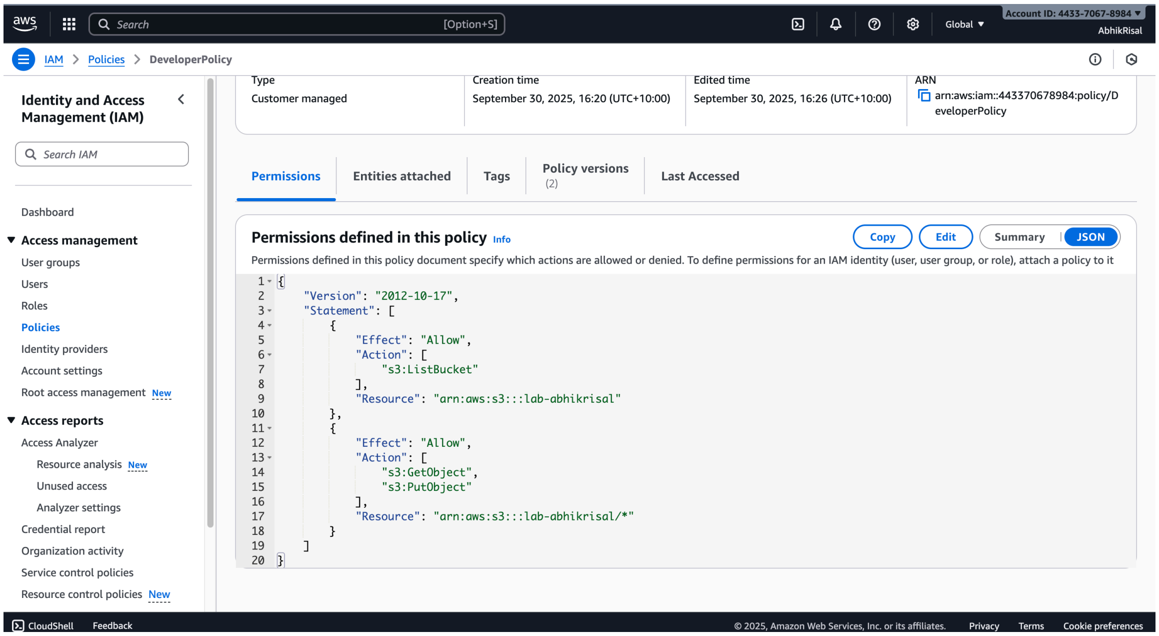
Select an existing statement in the policy or add a new statement.



Permissions defined in this policy

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::lab-abhikrisal",
                "arn:aws:s3:::lab-abhikrisal/*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObject",
                "s3:DeleteObjectVersion"
            ],
            "Resource": "arn:aws:s3:::lab-abhikrisal/*"
        }
    ]
}
```



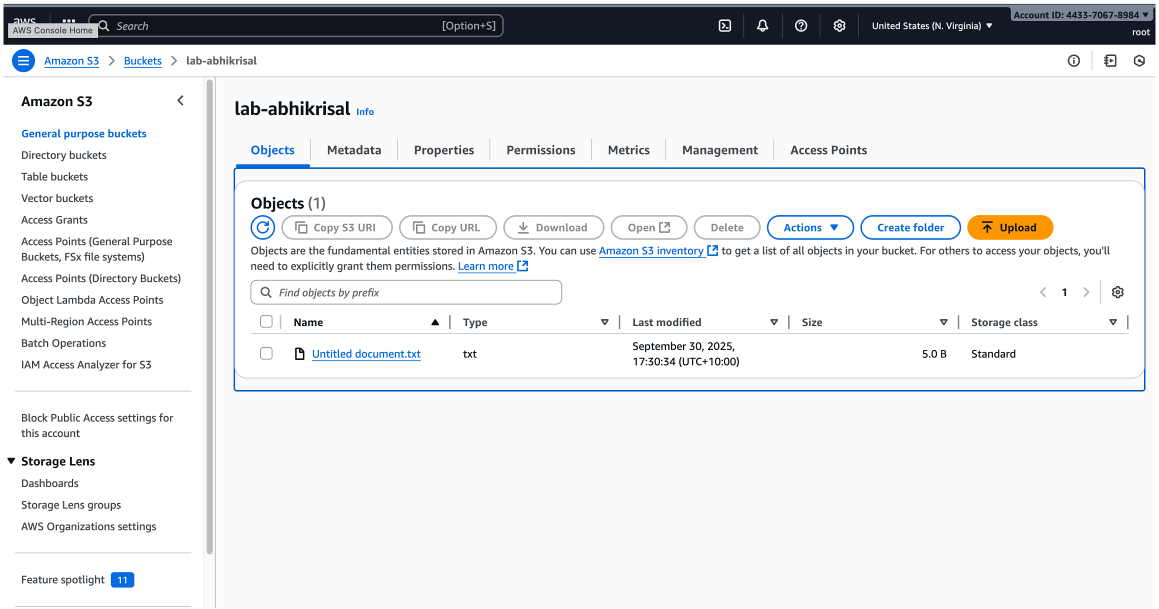
Type	Creation time	Edited time	ARN
Customer managed	September 30, 2025, 16:20 (UTC+10:00)	September 30, 2025, 16:26 (UTC+10:00)	arn:aws:iam::443370678984:policy/DeveloperPolicy

Permissions defined in this policy Info

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::lab-abhikrisal"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::lab-abhikrisal/*"
        }
    ]
}
```

File Upload



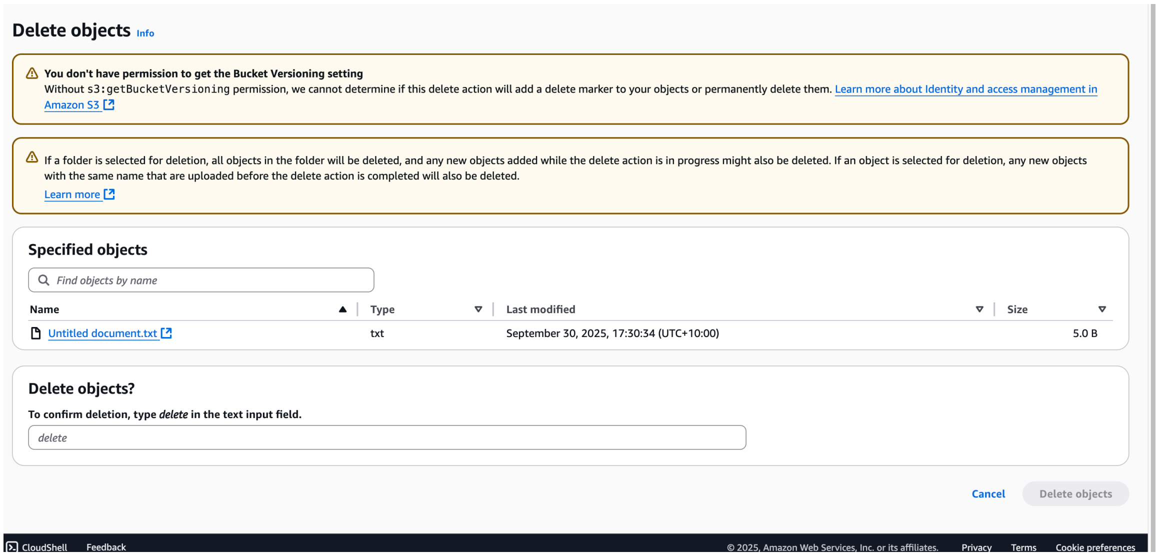
lab-abhikrisal Info

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class
Untitled document.txt	txt	September 30, 2025, 17:30:34 (UTC+10:00)	5.0 B	Standard

Access Denied



Delete objects Info

⚠ **You don't have permission to get the Bucket Versioning setting**
Without `s3:getBucketVersioning` permission, we cannot determine if this delete action will add a delete marker to your objects or permanently delete them. Learn more about Identity and access management in Amazon S3

⚠ If a folder is selected for deletion, all objects in the folder will be deleted, and any new objects added while the delete action is in progress might also be deleted. If an object is selected for deletion, any new objects with the same name that are uploaded before the delete action is completed will also be deleted.
Learn more

Specified objects

Find objects by name

Name	Type	Last modified	Size
Untitled document.txt	txt	September 30, 2025, 17:30:34 (UTC+10:00)	5.0 B

Delete objects?

To confirm deletion, type *delete* in the text input field.

delete

Reflection

In this lab, I implemented IAM policies to enforce least privilege and MFA within AWS IAM. Three users were created: `dev_user`, `ops_user`, and `auditor`. The developer role was granted only the ability to upload and list files within the `lab-abhikrisal` S3 bucket, the operator role was restricted to read-only access but required MFA, and the auditor role was limited to read-only actions with an explicit Deny on deletes. This setup ensured that each role had only the minimum permissions necessary.

During testing, `dev_user` successfully uploaded a file, while `auditor` was denied access when attempting to delete it, confirming that least privilege was applied. The `ops_user` initially could not download objects without MFA enabled, but succeeded once MFA was assigned, proving layered authentication worked as designed. These outcomes demonstrated clear enforcement of both role-based access control and strong authentication.

The lab highlighted risks such as insider misuse, privilege escalation, and credential theft, and showed how properly designed IAM policies mitigate them. Enforcing MFA on privileged accounts adds a strong safeguard against stolen passwords, while limiting user permissions reduces the potential impact of an account compromise. In real-world SMEs, applying least privilege and MFA consistently would not only reduce security risks but also align with compliance requirements. Overall, this exercise reinforced how IAM design directly improves network, cloud, and application security.