

ITECH1502 Cybersecurity Fundamentals

Week 9 Lab Activities

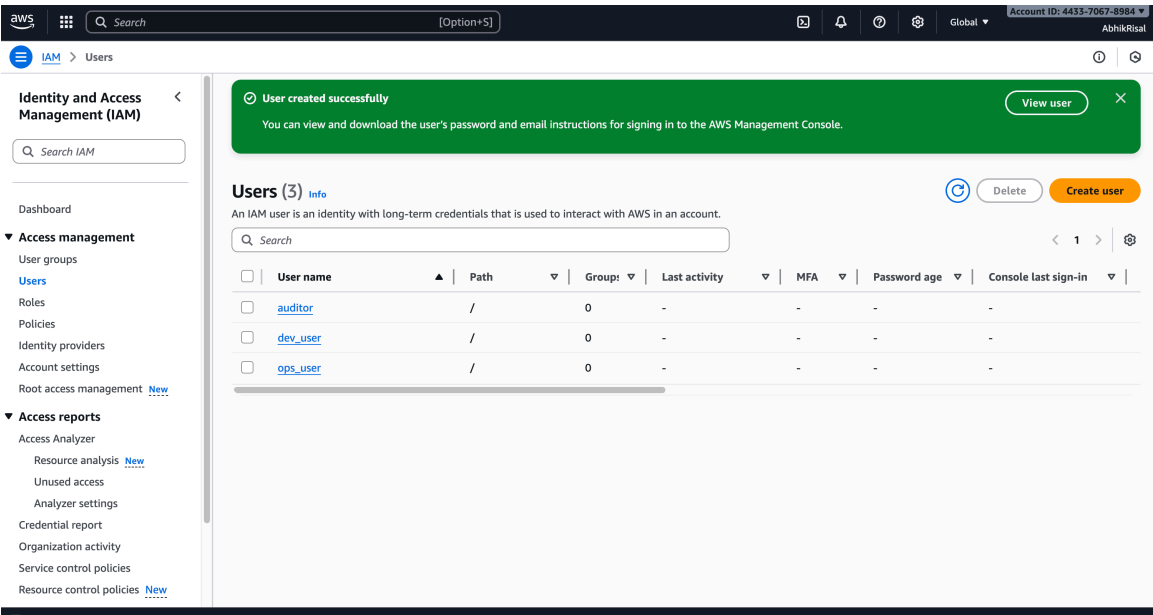
Network, Cloud, and Application Security

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).



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

Policy OperatorPolicy_MFA updated.

Step 1

Modify permissions in OperatorPolicy_MFA

Step 2

Review and save

Modify permissions in OperatorPolicy_MFA

Info

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

Policy editor

VisualJSONActions

1 {
2 "Version": "2012-10-17",
3 "Statement": [
4 {
5 "Effect": "Allow",
6 "Action": [
7 "s3:ListBucket",
8 "s3:GetObject"
9],
10 "Resource": [
11 "arn:aws:s3:::lab-abhikrisal",
12 "arn:aws:s3:::lab-abhikrisal/*"
13],
14 "Condition": {
15 "Bool": {
16 "aws:MultiFactorAuthPresent": "true"
17 }
18 }
19 }
20]
21 }

Edit statement

Select a statement

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

+ Add new statement

CloudShellFeedback

© 2025, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

aws

Search

[Option+S]

Account ID: 4433-7067-8984

AbhikRisal

IAM > Policies > AuditorPolicy_DenyDelete

123

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

PermissionsEntities attachedTagsPolicy versions (2)Last Accessed

Permissions defined in this policy

Info

CopyEditSummaryJSON

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

1 {
2 "Version": "2012-10-17",
3 "Statement": [
4 {
5 "Effect": "Allow",
6 "Action": [
7 "s3:ListBucket",
8 "s3:GetObject"
9],
10 "Resource": [
11 "arn:aws:s3:::lab-abhikrisal",
12 "arn:aws:s3:::lab-abhikrisal/*"
13],
14 },
15 {
16 "Effect": "Deny",
17 "Action": [
18 "s3:DeleteObject",
19 "s3:DeleteObjectVersion"
20],
21 "Resource": "arn:aws:s3:::lab-abhikrisal/*"
22 }
23]
24 }

CloudShellFeedback

© 2025, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

aws [Search] [Option+S] Global Account ID: 4433-7067-8984 AbhikRisal

IAM > Policies > DeveloperPolicy

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
- Analyzer settings
- Credential report
- Organization activity
- Service control policies
- Resource control policies New

CloudShell Feedback

Type: Customer managed

Creation time: September 30, 2025, 16:20 (UTC+10:00)

Edited time: September 30, 2025, 16:26 (UTC+10:00)

ARN: arn:aws:iam::443370678984:policy/DeveloperPolicy

Permissions Entities attached Tags Policy versions (2) Last Accessed

Permissions defined in this policy Info Copy Edit Summary JSON

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

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:ListBucket"
8       ],
9       "Resource": "arn:aws:s3:::lab-abhikrisal"
10    },
11    {
12      "Effect": "Allow",
13      "Action": [
14        "s3:GetObject",
15        "s3:PutObject"
16      ],
17      "Resource": "arn:aws:s3:::lab-abhikrisal/*"
18    }
19  ]
20 }
```

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

File Upload

aws [Search] [Option+S] United States (N. Virginia) Account ID: 4433-7067-8984 root

Amazon S3 > Buckets > lab-abhikrisal

Amazon S3

General purpose buckets

- Directory buckets
- Table buckets
- Vector buckets
- Access Grants
- Access Points (General Purpose Buckets, FSx file systems)
- Access Points (Directory Buckets)
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight 11

lab-abhikrisal Info

Objects Metadata Properties Permissions Metrics Management Access Points

Objects (1)

Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

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](#)

Find objects by prefix

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	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
<div><div></div>Untitled document.txt</div>	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

Cancel

Delete objects

CloudShell

Feedback

© 2025 Amazon Web Services, Inc. or its affiliates

Privacy

Terms

Cookie preferences

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.