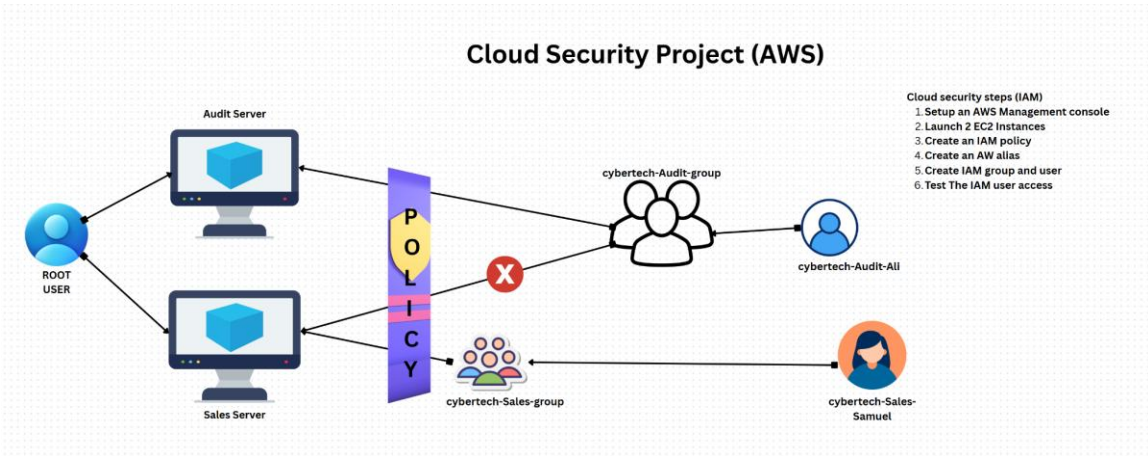


# AWS IAM Cloud Security Project

## 1. Project Overview

I completed this project on cloud security controls in Amazon Web Services (AWS), focusing on Identity and Access Management (IAM). The goal was to create a least-privilege policy, attach it to a user group, and verify that the policy correctly restricts actions on two Amazon EC2 instances (audit and sales).

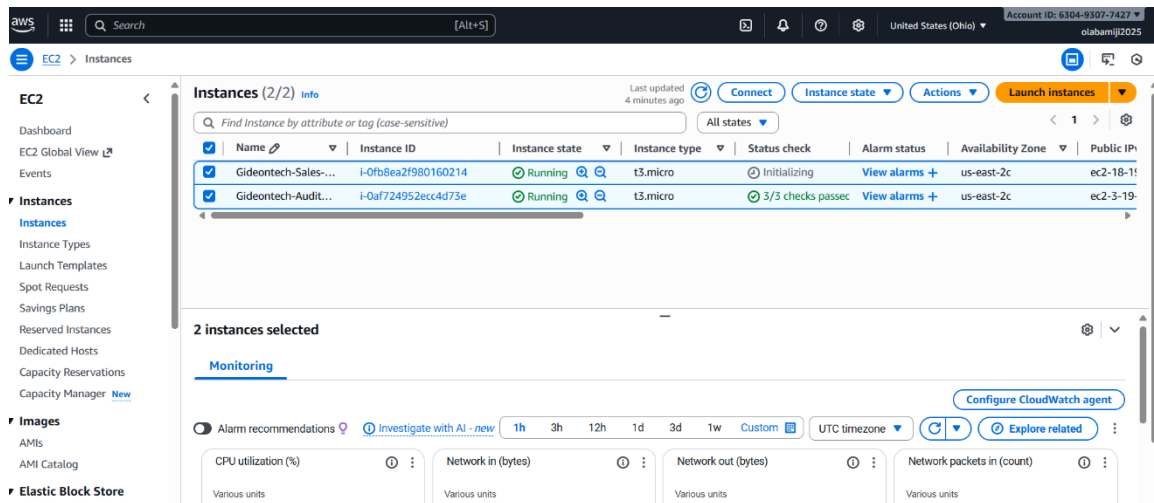


## 2. Tools & Concepts

- AWS IAM – users, groups, policies, account alias
- Amazon EC2 – instance tagging and lifecycle actions
- JSON policy syntax – Effect, Action, Resource
- Principle of least privilege and policy testing

## 3. Tagging Strategy

|   |                     |             |           |
|---|---------------------|-------------|-----------|
| I applied a descriptive tag to each EC2 instance: |                     |             |           |
| Instance  | Tag Key             |             | Tag Value |
| audit   |                     | Environment | Audit     |
| sales   | Environment   Sales |             |           |



## 4. Creating the IAM Policy

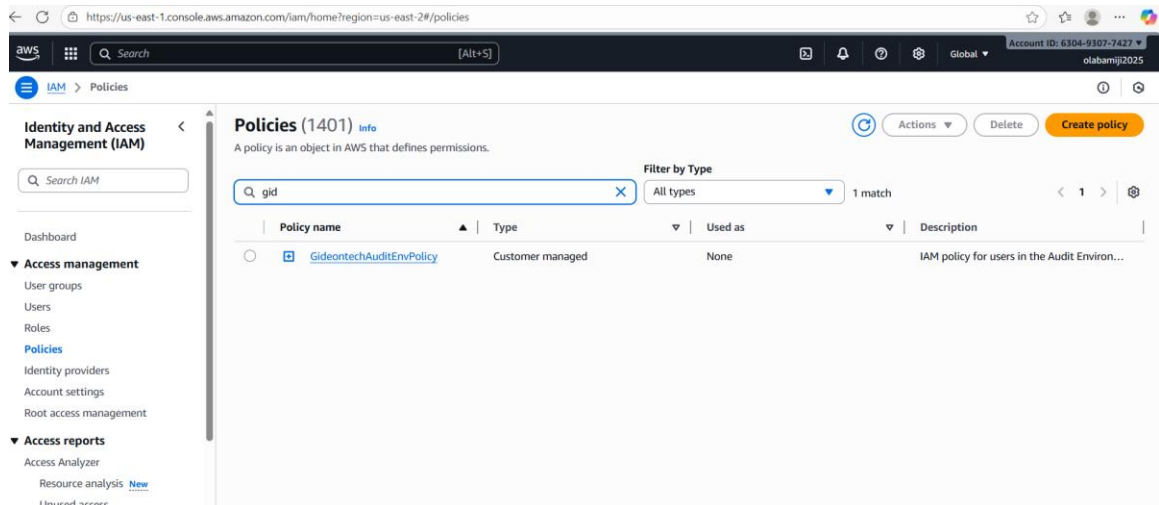
I authored the following JSON policy to block instance stop/start actions on the audit server but allow those actions on the sales server:

**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": "ec2:*",
7       "Resource": "*",
8       "Condition": {
9         "StringEquals": {
10          "ec2:ResourceTag/Env": "Audit"
11        }
12      }
13    },
14    {
15      "Effect": "Allow",
16      "Action": "ec2:Describe*",
17      "Resource": "*"
18    },
19    {
20      "Effect": "Deny",
21      "Action": [
22        "ec2:DeleteTags",
23        "ec2:CreateTags"
24      ],
25      "Resource": "*"
26    }
27  ]
28 }
```




## 5. Account Alias

I set a memorable account alias to replace the default numeric URL, making sign-in easier for team members.

### AWS Account

**Account ID**  
 630493077427

**Account Alias**  
gideontechusers [Edit](#) | [Delete](#)

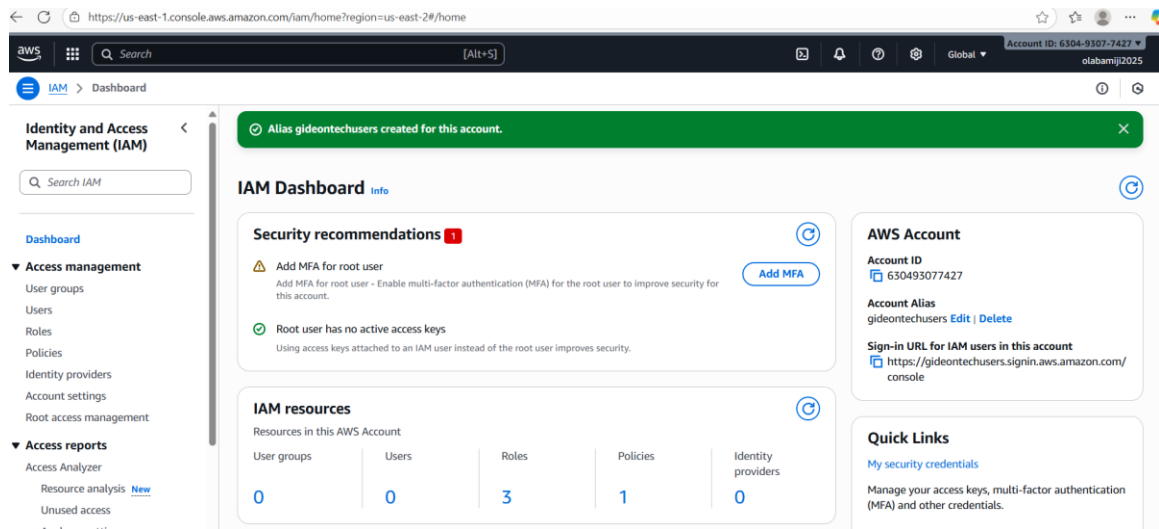
**Sign-in URL for IAM users in this account**  
 <https://gideontechusers.signin.aws.amazon.com/console>

### Quick Links

[My security credentials](#)

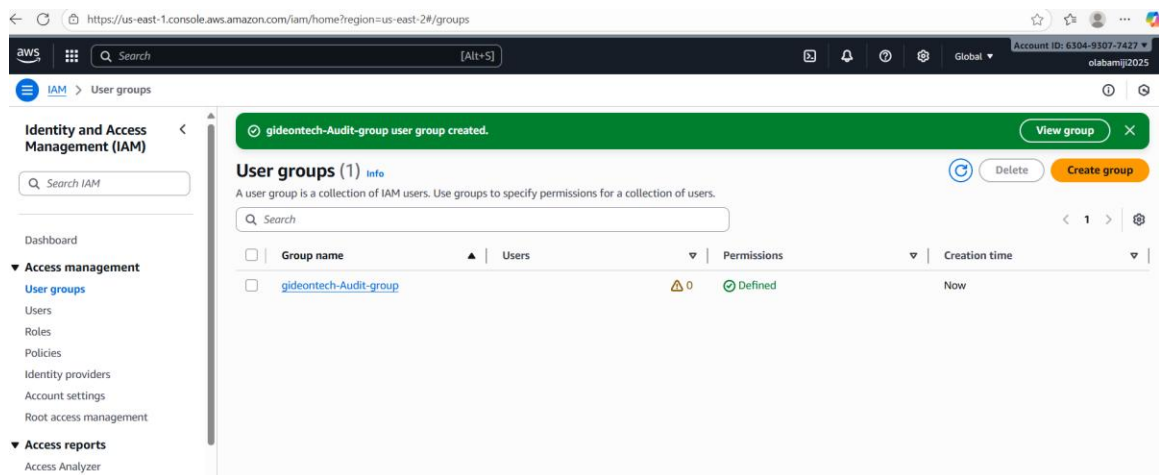
Manage your access keys, multi-factor authentication (MFA) and other credentials.

### Tools



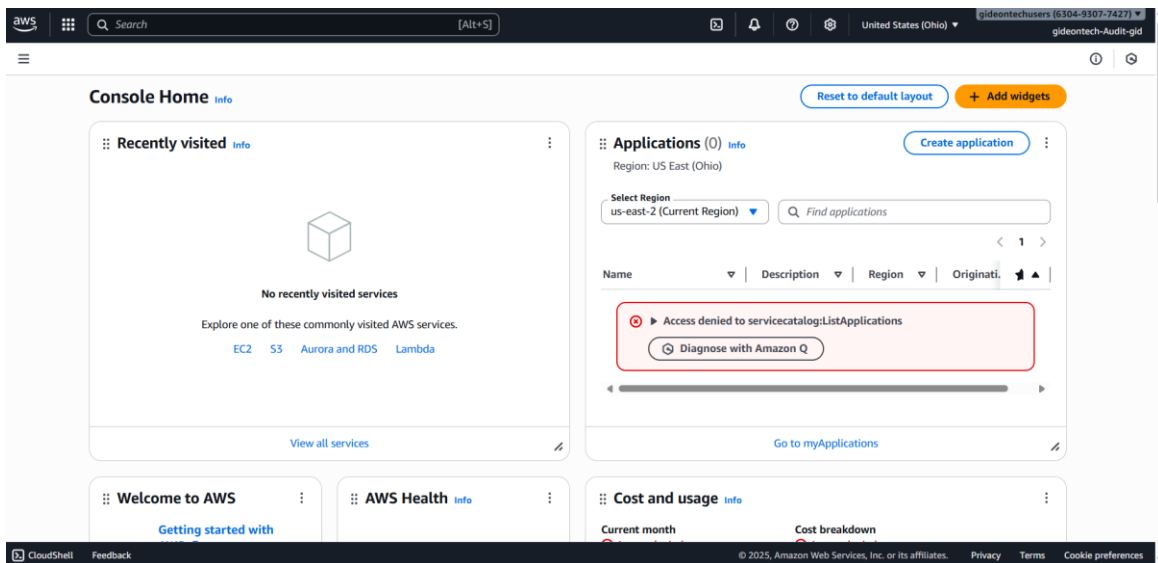
## 6. IAM Users & Groups

1. I Created an IAM user group called gideontech-Audit-group.
2. Attached is the **gideontechAuditEnvPolicy** policy to the group.
3. I have added individual IAM users who require controlled EC2 access.



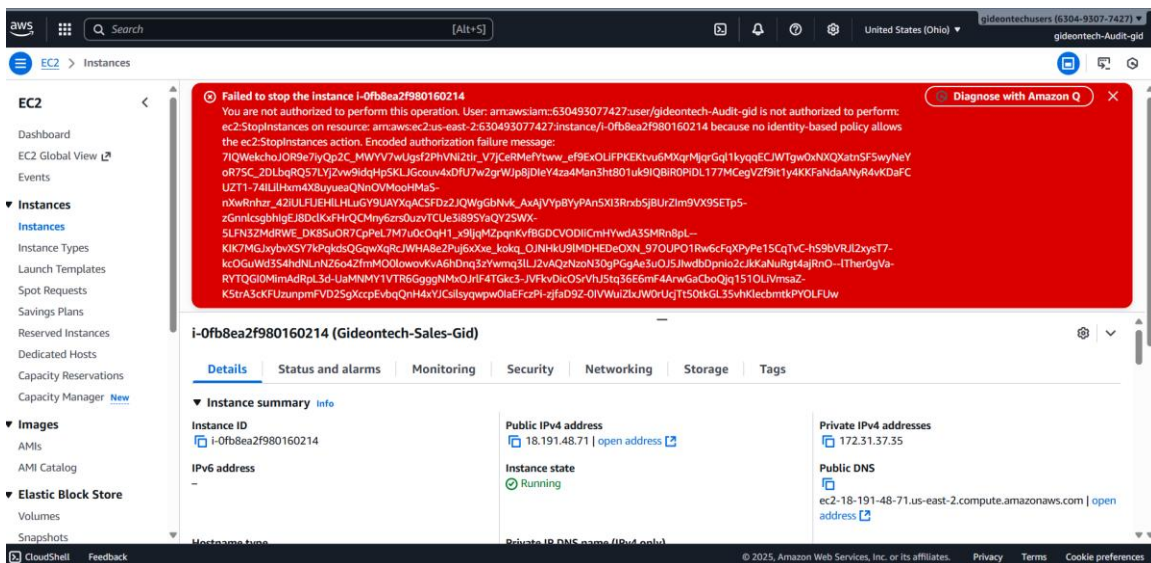
## 7. Logging in as an IAM User

- IAM users can sign in through:
- AWS Management Console (using the new alias <https://gideontechusers.signin.aws.amazon.com/console>)
  - AWS CLI via programmatic keys



## 8. Testing the Policy

| Test  | Action         | Expected | Result           | Actual       | Result    |
|-------|----------------|----------|------------------|--------------|-----------|
| Stop  | audit instance | Denied   | Access denied    | error        | displayed |
| Stop  | sales instance | Allowed  | Instance stopped | successfully |           |
| Start | audit instance | Denied   | Access denied    | error        | displayed |
| Start | sales instance | Allowed  | Instance started | successfully |           |



IAM Dashboard Info

Security recommendations 0


⊗ Access denied

You don't have permission to `iam:GetAccountSummary`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

**User:** arn:aws:iam::288645738432:user/cybertech-Audit-Ali

**Action:** iam:GetAccountSummary

**Context:** no identity-based policy allows the action

 Diagnose with Amazon Q

⊗ Access denied

You don't have permission to `iam:ListMFADevices`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

**User:** arn:aws:iam::288645738432:user/cybertech-Audit-Ali

**Action:** iam:ListMFADevices

**Context:** no identity-based policy allows the action

⊗ Failed to stop the instance i-0b9626f2835a5f977

You are not authorized to perform this operation. User: arn:aws:iam::288645738432:user/cybertech-Audit-Ali is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:288645738432:instance/i-0b9626f2835a5f977 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: sAveffO1FXITMRJ52xofnO4bpSGLz7IFqT-w1DqTxLoat\_IV4T5r87OVMMHxzfSSmG4VXfVa2cdWhfQ1uQO0shFk8kUgfZhoC9Tn\_lhCnKyVswG-blgkFFw9OLb4-2CT9TP841I8ni9O6EaSTAt0ztgtsh2t1VXnMzhUuPZeqMg3Ajek6wr21590c0le6YNjRMmccGw8Gd\_xH9dlfdp-4ilwlF0H1uwTpAt1QHqqr8FbW3kjOue7UMNuHGzJzgCiiA30Q5pqHwW1\_ALxzQAulhMpW9i6xdEiwRRLOfQG\_W-dDTm6Z7YNPth09weBuulXatLbc13Mz5-cIFyB\_0PBgVz8xKMy4kuncI\_zDmT3Nfyv0sszpKwvYxm8Du71JN3r5TmByIKAIW0cA0nzcOFVWIQ9kigwxbT-gocongZgZGILqW2RxlqW8XBC42OEN3IIZ-URc-xY2CS1palfmclLRIDvCBZjNWP4rK\_0WgaADMkzFgQjk7xmnnNmFi2mgHr5Aw46VvHCp-pqURgYZ\_Oa8xBnq7y6luLZ\_MxlUb20pZDhB0SynHoNGRmOMRzRy1etyCipN14aBfvWB12hSkMoXobUZawc9Rat-Pk\_vPSbim-Opv1riuGTCT-YJtIZ6FSYUFEcxnmX6B3iFHggGT0p6sDazlXMCX3g2yqEqbTNSf-CIWszbvA7Ck5mSyf8nt1po\_-8fBDM67ZwyEe21nGxikjEmj\_nMMMMQVPqk46tBhdwRYHLxQQA2b-cG58fOMUsv\_eHnT1xBHLtkVMB7VxU-\_Scg\_KyhwQIMrGy4NR4Ho\_RumoDyK8aWNLTlxh-j1yTKrJk8ctDTf11QzyfSAKRTQp\_-j1QBrzXEA47t8IXAwqRD3vWCNE3PL3YfwcYpRHP

 Diagnose with Amazon Q

Instances (1/2) Info

All states

i-0b9626f2835a5f977 (Cybertech-sales-Ali)

[Details](#) | [Status and alarms](#) | [Monitoring](#) | [Security](#) | [Networking](#) | [Storage](#) | [Tags](#)

←

↻

https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/home

🔍 Search [Alt+S]

🔔

🌐 Global

gideontechusers (6304-9307-7427)

gideontech-Audit-gid

🏠 IAM > Dashboard

Identity and Access Management (IAM)

🔍 Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

▼ Access reports

Access Analyzer

Resource analysis [New](#)

Unused access

Analyzer settings

Credential report

🔔

🔄

IAM Dashboard

Info

🔔

🔄

Security recommendations

0

🔔

🔄

Access denied to iam:ListMFADevices

You don't have permission to iam:ListMFADevices. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: arn:aws:iam::630493077427:user/gideontech-Audit-gid

Action: iam:ListMFADevices

Context: no identity-based policy allows the action

🔍

Diagnose with Amazon Q

🔔

🔄

Access denied to iam:ListAccessKeys

You don't have permission to iam:ListAccessKeys. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: arn:aws:iam::630493077427:user/gideontech-Audit-gid

Action: iam:ListAccessKeys

Context: no identity-based policy allows the action

🔍

Diagnose with Amazon Q

🔔

🔄

AWS Account

🔔

🔄

Access denied to iam:ListAccountAliases

You don't have permission to iam:ListAccountAliases. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: arn:aws:iam::630493077427:user/gideontech-Audit-gid

Action: iam:ListAccountAliases

Context: no identity-based policy allows the action

🔍

Diagnose with Amazon Q

🔔

🔄

Quick Links

My security credentials

Manage your access keys, multi-factor authentication

🔍 CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)