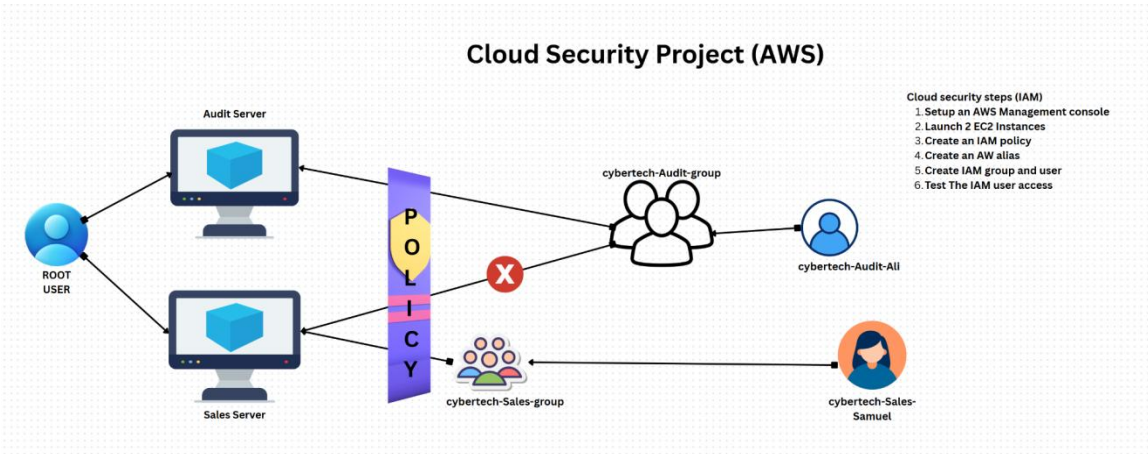


# AWS IAM Cloud Security Project

## 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					

Instances (1/2) [Info](#) Last updated less than a minute ago [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Find Instance by attribute or tag (case-sensitive) [All states](#)

Instance state = running [Clear filters](#)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input type="checkbox"/>	cybertech-aud...	i-03e590b416cd54355	Running	t3.micro	3/3 checks passed	<a href="#">View alarms +</a>	eu-north-1b	ec2-13-6t
<input checked="" type="checkbox"/>	cybertech-sale...	i-0c4adcc4d506a3321	Running	t3.micro	Initializing	<a href="#">View alarms +</a>	eu-north-1b	ec2-16-1t

## 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

604345806270

### Account Alias

cybertechemployees [Edit](#) | [Delete](#)

### Sign-in URL for IAM users in this account

<https://cybertechemployees.signin.aws.amazon.com/console>

## 6. IAM Users & Groups

1. Created an IAM user group called Cybertech-Audit-group.
2. Attached the **CybertechAuditEnvPolicy** policy to the group.
3. Added individual IAM users who require controlled EC2 access.

The screenshot shows the AWS Management Console's EC2 Instances page. The left sidebar contains navigation links for EC2, Dashboard, AWS Global View, Events, and a list of instance-related services. The main content area shows a table of instances. Two instances are listed: 'CyberTech-Audit-Oluwaseyi' (Running) and 'CyberTech-Sales-Oluwaseyi' (Running). The details for 'CyberTech-Sales-Oluwaseyi' are expanded, showing 2 vCPUs and Capacity Reservation settings.

Name	Instance ID	Instance state	Instance type	Status check	Alarm state
CyberTech-Audit-Oluwaseyi	i-038745706dff3498d	Running	t3.micro	3/3 checks passed	View alarm
CyberTech-Sales-Oluwaseyi	i-0d7c515d2c3654dcc	Running	t3.micro	Initializing	View alarm

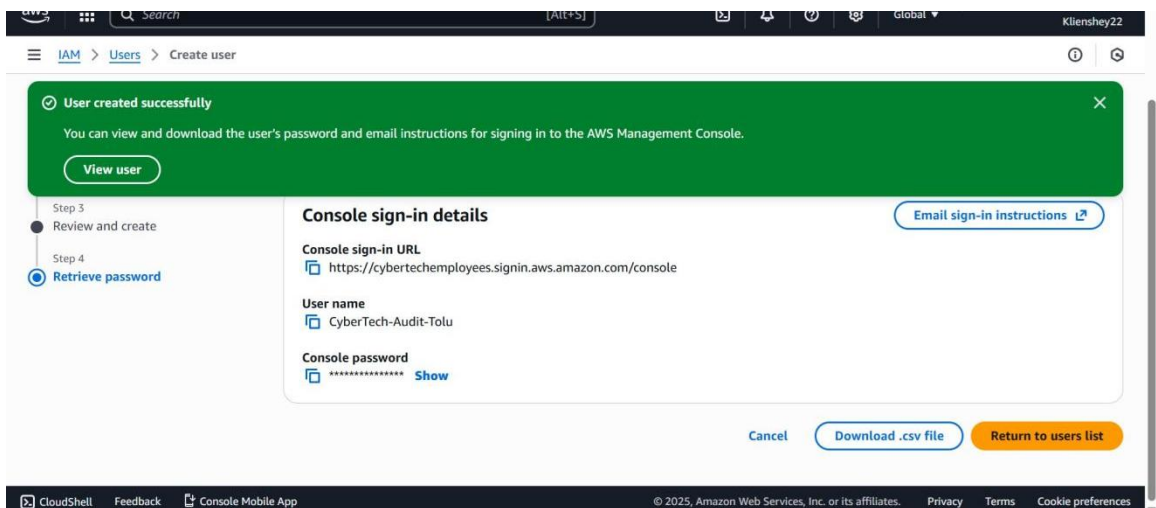
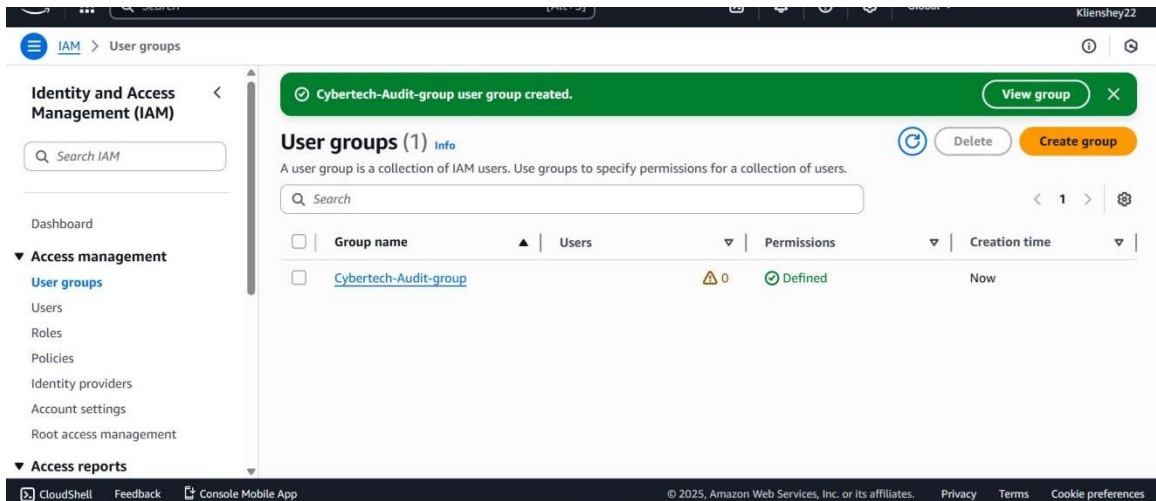
**i-0d7c515d2c3654dcc (CyberTech-Sales-Oluwaseyi)**

Number of vCPUs: 2

**Capacity reservation** Info

Capacity Reservation ID: -

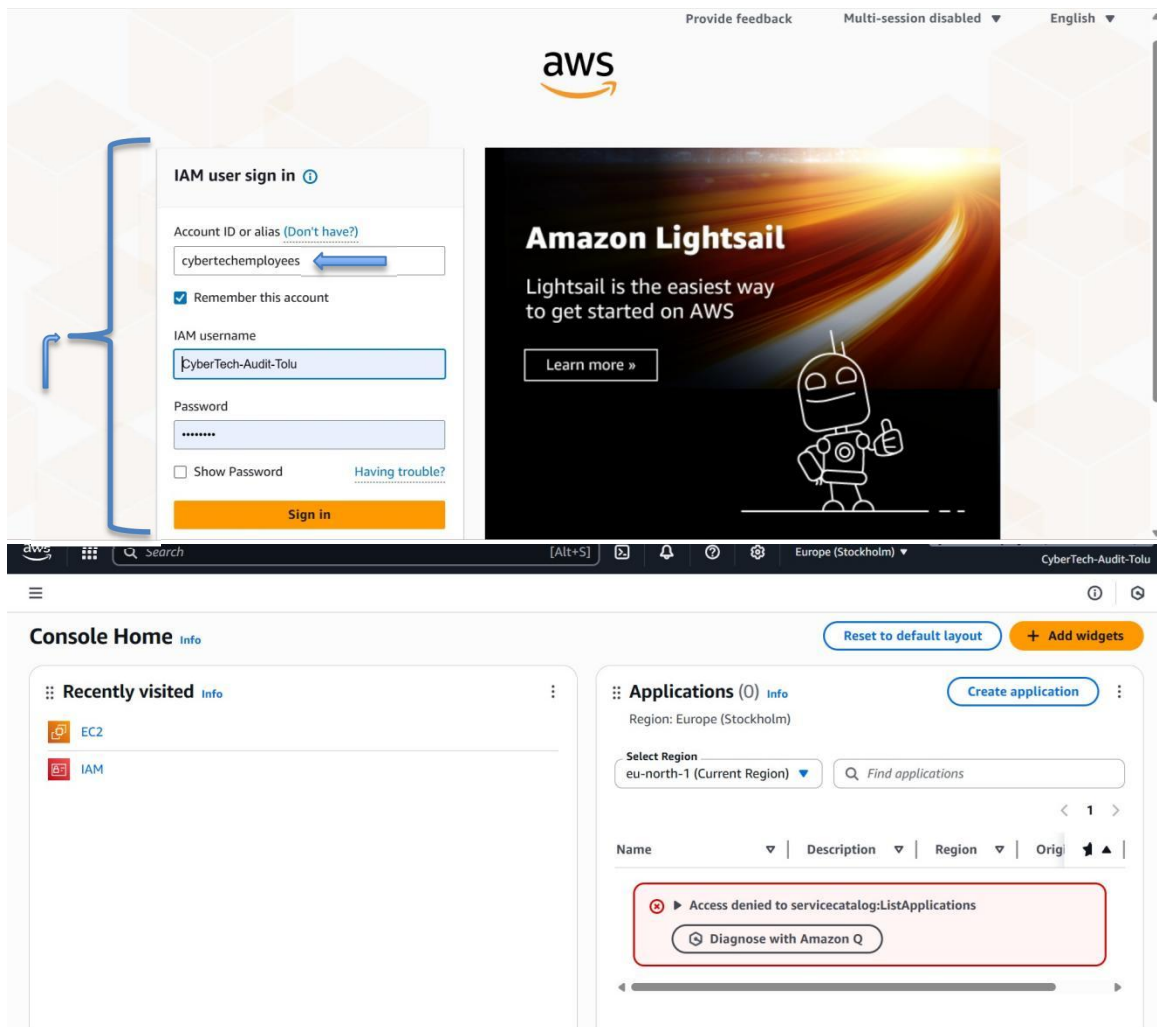
Capacity Reservation setting: open



## 7. Logging in as an IAM User

IAM users can sign in through:

- AWS Management Console (using the new alias URL)
- 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	

aws [Search] [Alt+S] Europe (Stockholm) CyberTech-Audit-Tolu

EC2 > Instances

EC2

- Dashboard
- AWS Global View
- Events
- Instances
  - Instances
  - Instance Types
  - Launch Templates
  - Spot Requests
  - Savings Plans
  - Reserved Instances
  - Dedicated Hosts
  - Capacity Reservations
  - Capacity Manager
- Images

Instances (1/2) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID
CyberTech-Audit-...	i-038745706dff349d
CyberTech-Sales-...	i-0d7c515d2c3654dcc

i-0d7c515d2c3654dcc (CyberTech-Sales-Oluwaseyi)

Details Status and alarms Monitor

Instance summary Info

Instance ID i-0d7c515d2c3654dcc

Public IP address 51.20.77.47

Launch instances

Launch instance from template

Migrate a server

Connect

Stop instance

Start instance

Reboot instance

Hibernate instance

Terminate (delete) instance

Instance diagnostics

Instance settings

Networking

Security

Image and templates

Instance state

Actions

Launch instances

Instance...

Status check

Alarm status

Av

t3.micro 3/3 checks passed User: arn:aws:iam:604345806270:user/CyberTech-Audit-Tolu eu

t3.micro 3/3 checks passed User: arn:aws:iam:604345806270:user/CyberTech-Audit-Tolu eu

Private IPv4 addresses

Public DNS

CloudShell Feedback Console Mobile App

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

aws [Search] [Alt+S] Global CyberTech-Audit-Tolu

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

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:604345806270:user/CyberTech-Audit-Tolu

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:604345806270:user/CyberTech-Audit-Tolu

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:604345806270:user/CyberTech-Audit-Tolu

Action: iam:ListAccountAliases

Context: no identity-based policy allows the action

Diagnose with Amazon Q

CloudShell Feedback Console Mobile App

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

aws [Search] [Alt+S] Europe (Stockholm) CyberTech-Audit-Tolu

EC2 > Instances

EC2

- Dashboard
- AWS Global View
- Events
- Instances
  - Instances
  - Instance Types
  - Launch Templates
  - Spot Requests
  - Savings Plans
  - Reserved Instances
  - Dedicated Hosts
  - Capacity Reservations
  - Capacity Manager
- Images

Instances (1/2) Info

Find Instance by attribute or tag (case-sensitive)

All states

Instance ID	Instance state	Instance...	Status check	Alarm status	Availability Zone	Public IPv4 DNS
i-038745706dff349d	Running	t3.micro	3/3 checks passed	User: arn:aws:iam:604345806270:user/CyberTech-Audit-Tolu	eu-north-1a	ec2-13-61-17-70
i-0d7c515d2c3654dcc	Running	t3.micro	3/3 checks passed	User: arn:aws:iam:604345806270:user/CyberTech-Audit-Tolu	eu-north-1a	ec2-51-20-77-47

i-0d7c515d2c3654dcc (CyberTech-Sales-Oluwaseyi)

51.20.77.47 [Public IP]

vpc-0e94f9e5a3e923e96

User: arn:aws:iam:604345806270:user/CyberTech-Audit-Tolu is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: \* because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action

Retry

Notifications 4 0 0 0 0 0

Connect Instance state Actions Launch instances

CloudShell Feedback Console Mobile App

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

