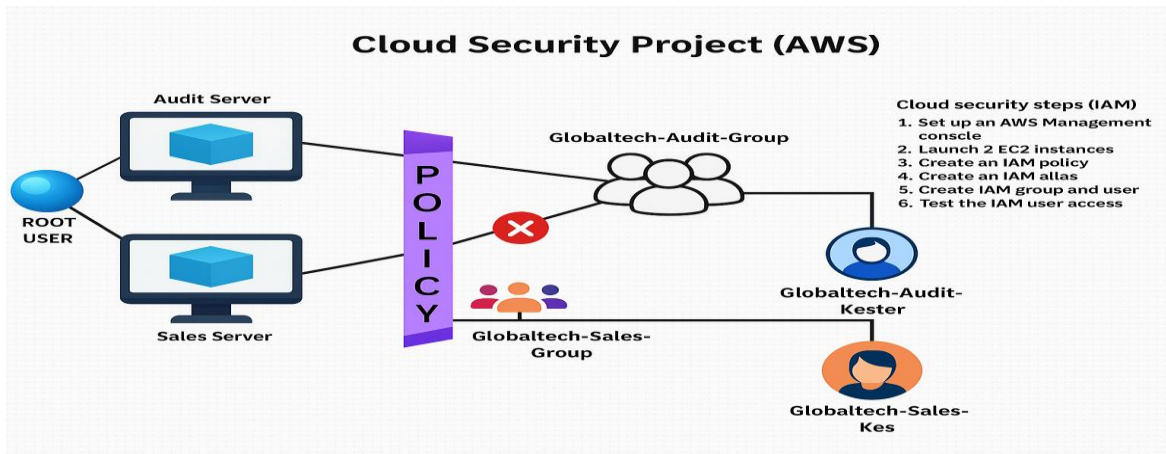


AWS IAM Cloud Security Project

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

Instance	Tag Key	Tag Value
audit	Environment	Audit
sales	Environment Sales	

Instances (2) Info

⌂

Connect

Instance state ▾

Actions ▾

Launch instances

< 1 >

⚙

🔍 Find Instance by attribute or tag (case-sensitive)

All states ▾

<input type="checkbox"/>	Name <div>✎</div> ▾	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status
<input type="checkbox"/>	Globaltech-Au...	i-0dbf9eed23348f588	<div>✔ Running</div> <div><div>🔍</div><div>🔄</div></div>	t3.micro	<div>✔ 3/3 checks passec</div>	<div>View alarms +</div>
<input type="checkbox"/>	Globaltech-Sal...	i-006c77dbd0402f274	<div>✔ Running</div> <div><div>🔍</div><div>🔄</div></div>	t3.micro	<div>✔ 3/3 checks passec</div>	<div>View alarms +</div>

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

 285253872210

Account Alias

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

Sign-in URL for IAM users in this account

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

6. IAM Users & Groups

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

Instances (1/2) Info							
<div><div><div>Q Find Instance by attribute or tag (case-sensitive)</div></div><div><div>Connect</div><div>Instance state ▾</div><div>Actions ▾</div><div>Launch instances ▾</div></div></div>							
<div>All states ▾</div> <div>< 1 > ⚙</div>							
<input checked="" type="checkbox"/>	Name ↗ ▾	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone ▾
<input checked="" type="checkbox"/>	Globaltech-Au...	i-0dbf9eed23348f588	Running 🔍 🔍	t3.micro	3/3 checks passed View alarms +		ca-central-1b
<input type="checkbox"/>	Globaltech-Sal...	i-006c77dbd0402f274	Running 🔍 🔍	t3.micro	3/3 checks passed View alarms +		ca-central-1b

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

Console Home [Info](#)

Reset to default layout

+ Add widgets

Recently visited [Info](#)

EC2

IAM

Applications (0) [Info](#)

Create application

Region: Canada (Central)

Select Region

ca-central-1 (Current Region) ▾

Find applications

< 1 >

Name ▾

Description ▾

Region ▾

Orig [↗](#) ▴ ▾

Access denied to servicecatalog:ListApplications

Diagnose with Amazon Q

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 DashboardInfo

Security recommendations0

⊗ 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::285253872210:user/Globaltech-Audit-Ekene

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::285253872210:user/Globaltech-Audit-Ekene

Action: iam:ListAccessKeys

Context: no identity-based policy allows the action

Diagnose with Amazon Q

⊗ Failed to stop the instance i-006c77dbd0402f274

You are not authorized to perform this operation. User: arn:aws:iam::285253872210:user/Globaltech-Audit-Ekene is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:ca-central-1:285253872210:instance/i-006c77dbd0402f274 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: AtD07qrBvQj2UTAB_3AfceJ6wT9w7Vrlp-Te3Z7XZLQ3fA3FTOAGDGNbF2sR_z-DJL5idHk8SGo83U2YH5nftDWWSqdJNNCObh04cMSWC6TaL_bDirSUJR4kN1Ba6-x4dC_rI_QPbITGqb_zgwO2SeJnEzOnpjQXoqdWXetZ4wa2CtDY-z87TyY9s5xhTG2cmKoop38Jn0HdrePwTEPwABF27D4b2OnSf44qqI7dK3wMNd-55OPJBQhJuaqBFXpoagDAJh5mSTE6MF-fHfYgK9WxmzvmDlsG_r03Gc-77WHn2O58hwKLO3yMWae0F7QOTIG-dHtHdxDCSVBbv75ELVIXCgYCbOvB2sUdk-btT3KDDBJyAZZl6GxJ0moT6AbfQ-aLE7_D68yVJzMXHtBPX627vHavZ2ddcirJfG1bFFIpot9tU4EnKAC0Zn69GHUHQADYBbUqCXZEXCQJIMLFUQ79f6U6JAN4-L_o311MON5iw2PLTy1PuY_-JITDI23U-p5BpFlsfrFEsUzo7v7ggg5l6-xHDwto-dZR1fJqWhUX-Y2a6B5B5hUZMR2zRhVQvqyt1ckIH0lpZzVoltYIEcKqnDXMuIlOLE5ITQyTqWcP20J9vQ-dJOxY847ygFIKdg7_LhSeM2fQkIUJdOm-euQYh9wJTM20jYf3IHlplsFYLCQZoQoY0uZndsh-sh0E3126At-ykGFF_T4crRISW-GoQ78tN217GcRUDvuUDDsDtKvztimRDGLb1JXmxPtCP_STID_pwLh-_ahSNx6hhkjpWWEMUHZ-DyXlnrtAUSeetTxHskyBYQ76FwExeoKkV6PFagcVMBKvg5bqE3-Vf1r2JY-GpyOT2ehkFqvm-glKRsa5FPIVOA25omhHMjGQa4

Diagnose with Amazon Q

Instances (1/2)Info

ConnectInstance stateActionsLaunch instances

i-006c77dbd0402f274 (Globaltech-Sales-Kes)

