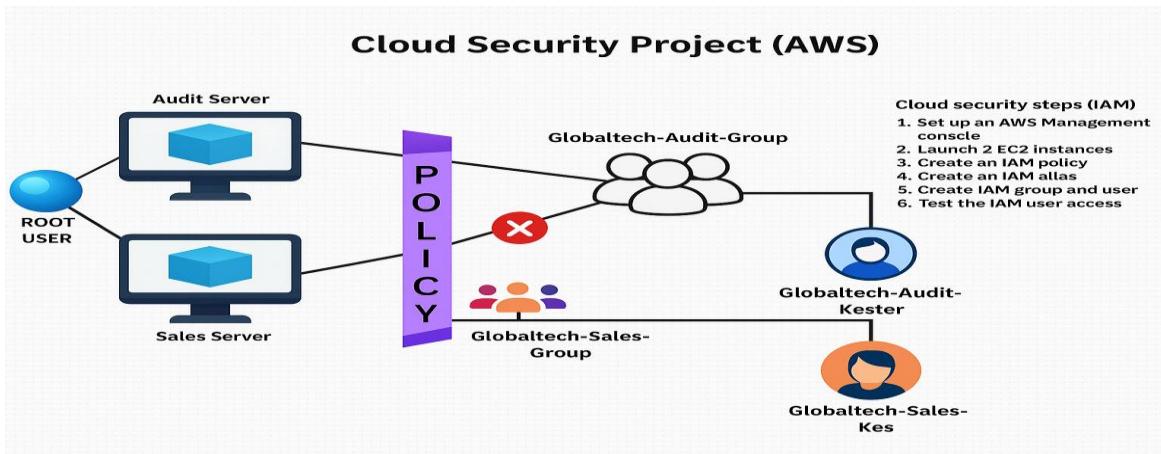


AWS IAM Cloud Security Project

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 (2) Info		Connect	Instance state ▾	Actions ▾	Launch instances	▼
<input type="text"/> Find Instance by attribute or tag (case-sensitive)		All states ▾				◀ 1 ▶ ⚙
□	Name ⚡	Instance ID	Instance state	Instance type	Status check	Alarm status
□	Globaltech-Au...	i-0dbf9eed23348f588	Running Q Q	t3.micro	3/3 checks passed View alarms +	View alarms +
□	Globaltech-Sal...	i-006c77dbd0402f274	Running Q Q	t3.micro	3/3 checks passed View alarms +	View alarms +

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](#)

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

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

Instances (1/2) Info						
		 Connect	Instance state ▾	Actions ▾	Launch instances	▼
Q Find Instance by attribute or tag (case-sensitive)		All states ▾	< 1 > ⌂			
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 +	ec2-35-1l

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](#)

Name	Description	Region	Origin
 Access denied to servicecatalog>ListApplications			

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 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](#) 

 **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](#) 

 **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: AtD07qrBv0j2UTAB_3AfceJ6wT9w7Vrlp-Te327XZLQ3fA3FTOAeGDNBf2sR_z-DJL5idtHk8SGo83U2YHSnftWWsSqdJNNCoBh04cMSWC6TaL_bDlrSUJR4kN1Ba6-x4dc_rL_QPbITGqb_2gwO2SeJnExOnpjQXoqdWetZ4wa2CtDvYz87Ty9SxhTG2cmkkoop58JnHdpePwEPwABF27D4b2OnSf44qqj7dK3wMNd-550PJQBQhfojUaqbFXpoagDAJhSmSTE6MF-fHfygkqVxmzvmdIsG_r03Gc-77WhIn2058hwkLO3yMwaeF7Q0T1G-dHtHdxCSVBbv75ELVlXCgYCboVb2sUdk-btT3KDD8jAYZ2l6fGxJm0t76abfQ-aL68yVjzMxHTbPX627vHav2ZddcirJfG1bfFlpot9tU4EnkAC02n69GHUHQADYBbUqCXZExCQUJMLfUQ79f6U6JAN4-I_031tMONSiw2PLTy1Pu_y_JTDI23U-p5BpfspfrEsUzo7v7ggq5l6-xHDwto-dZR1fJqWhUx-Y2a6B58ShUZMR2rRhVqvgyt1KtIH0lpZzV0ltYEcIKqnDXMuII0LE5jTQyTqWcP20J9vQ-dJOrXy847ygFiKdg7_LhSeM2fQkiUJdOm-euQYh9wJTM20jf3IHipsFYLCQzOqoYoZndsh-sh0E3126At-ykGff_T4crI5W-GoQ7Btch217GrUDvuuUDDsdtKvtzlmRDGb1JXmxPtCP_STID_pwlh_-ahSNx6hhkjpWWEMUhZ-DyxlnrtAUSeetTxHskyBYQ76FwExeoKKV6PFagcVMBkVg5bqE3-Vf1r2JY-GpyOT2ehkfQvm-gIKRsaX5FPIVOA25omhHMjGQa

 [Diagnose with Amazon](#) 

Instances (1/2) [Info](#)  [Connect](#)  [Instance state](#)  [Actions](#)  [Launch instances](#) 

i-006c77dbd0402f274 (Globaltech-Sales-Kes)

