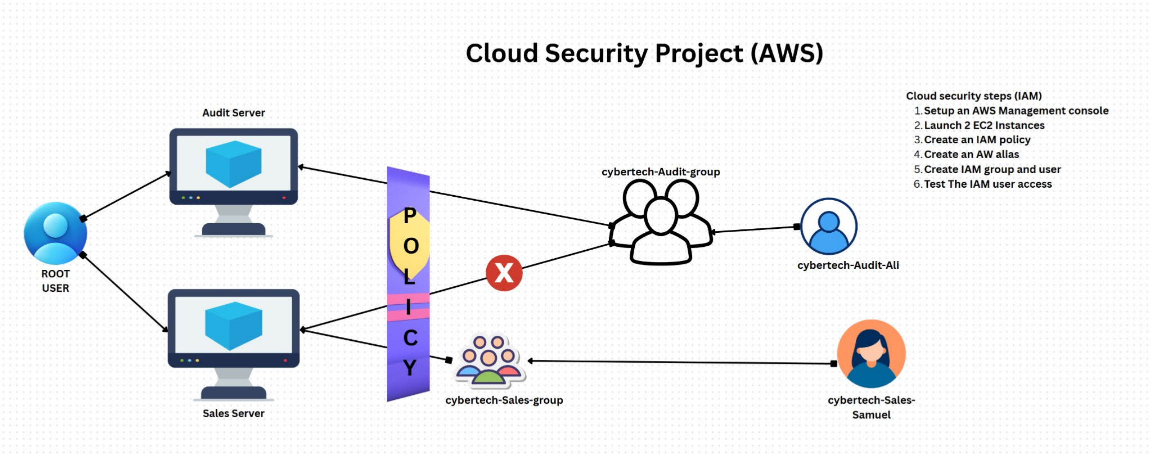
AWS IAM Cloud Security Project

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).



Cloud Security Project (AWS)

Cloud security steps (IAM)

1. Setup an AWS Management console
2. Launch 2 EC2 Instances
3. Create an IAM policy
4. Create an AW alias
5. Create IAM group and user
6. Test The IAM user access

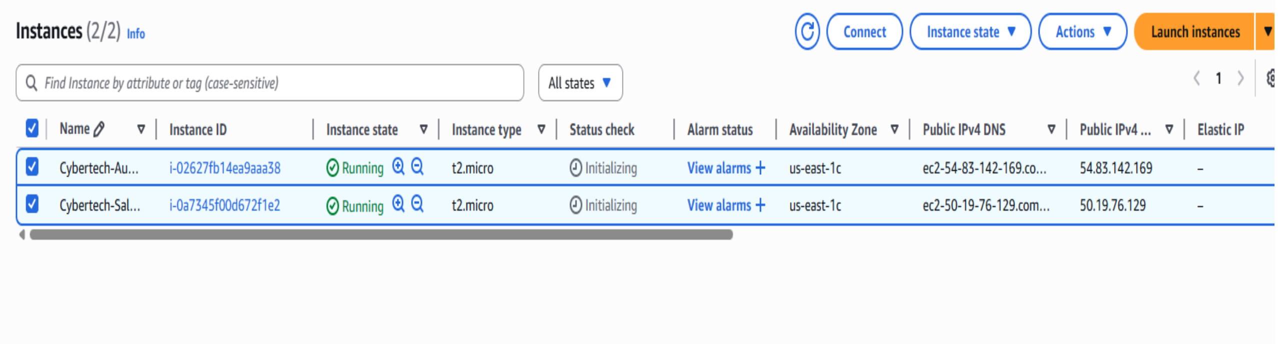
2. Tools & Concepts

- 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:

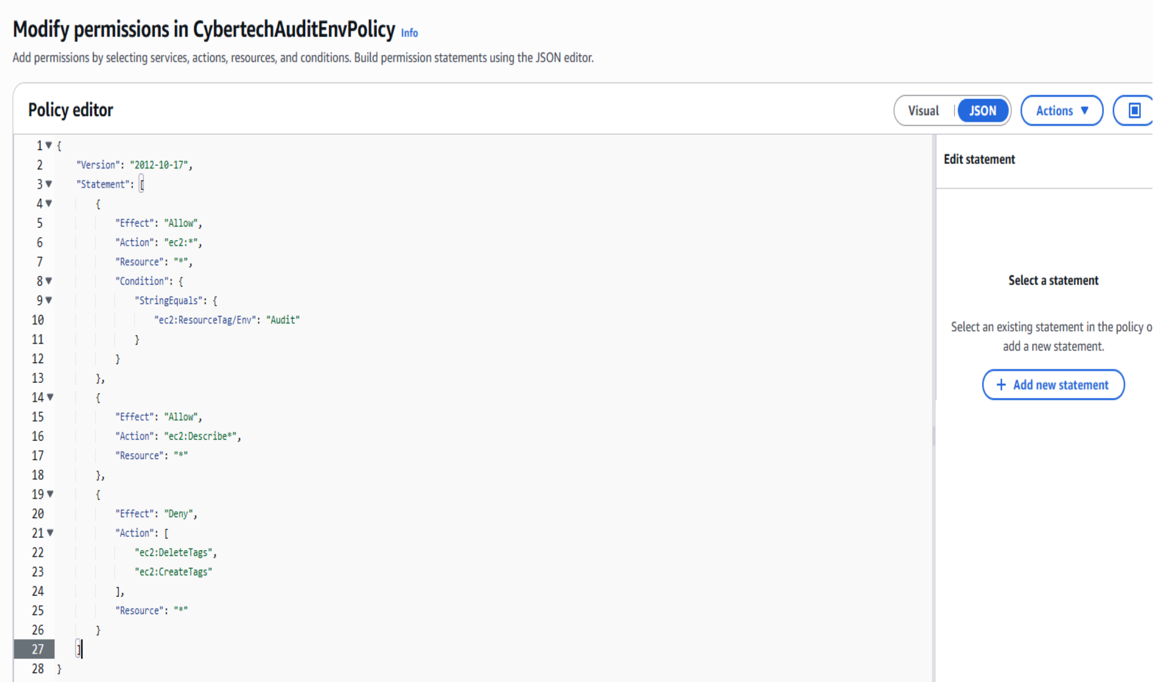
Instance	Tag Key	Tag Value
audit	Environment	Audit
sales	Environment	Sales


Instances (2/2) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☑	Cybertech-Au...	i-02627fb14ea9aaa38	Running	t2.micro	Initializing	View alarms +	us-east-1c	ec2-54-83-142-169.co...	54.83.142.169	–
☑	Cybertech-Sal...	i-0a7345f00d672f1e2	Running	t2.micro	Initializing	View alarms +	us-east-1c	ec2-50-19-76-129.com...	50.19.76.129	–

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:


Modify permissions in CybertechAuditEnvPolicy Info

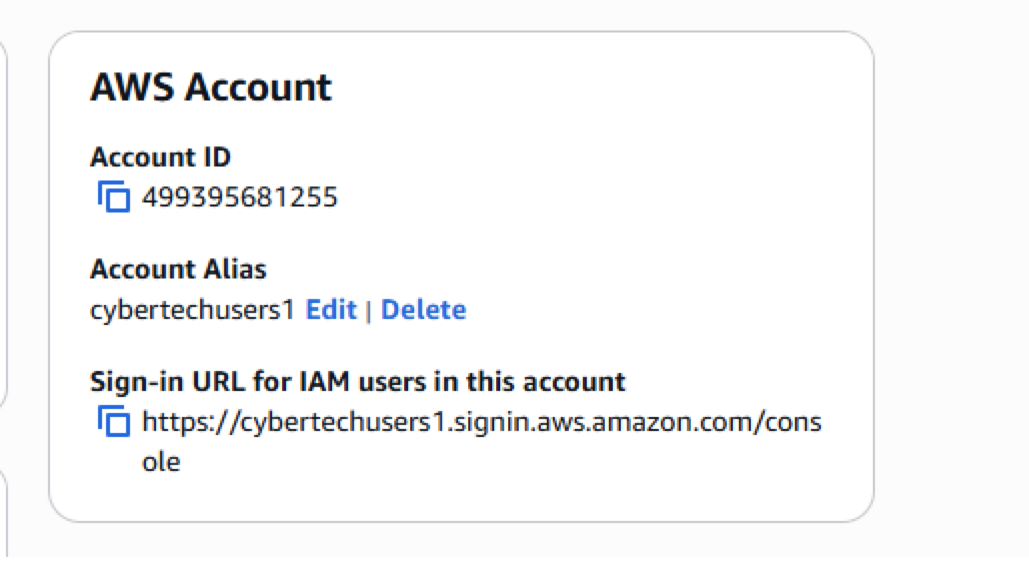
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Env": "Audit"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DeleteTags",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Account Alias

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



AWS Account

Account ID

499395681255

Account Alias

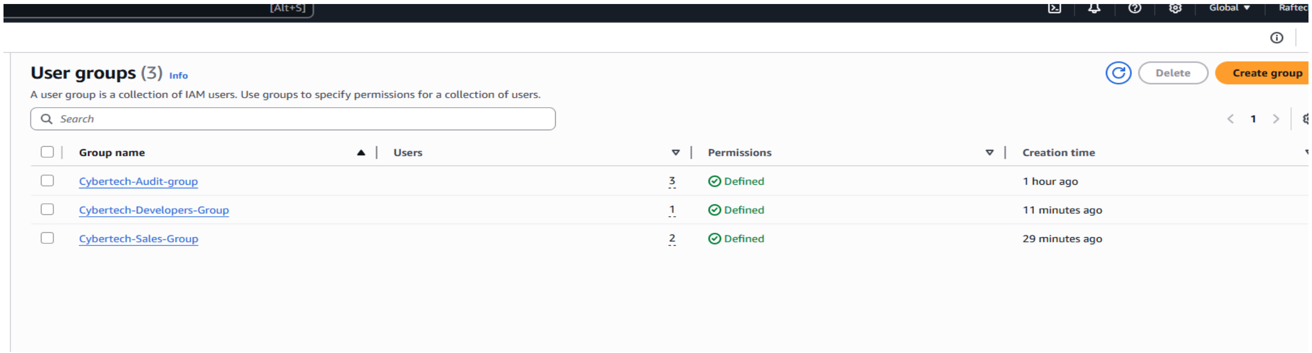
cybertechusers1 Edit | Delete

Sign-in URL for IAM users in this account

https://cybertechusers1.signin.aws.amazon.com/console

6. IAM Users & Groups

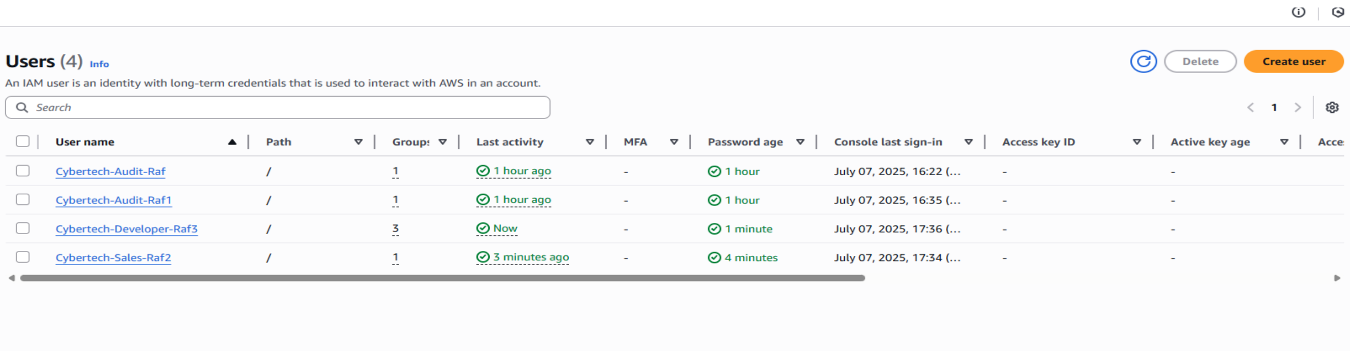
1. Created an IAM user group called Developers.
2. Attached the **CybertechAuditEnvPolicy** policy to the group.
3. Added individual IAM users who require controlled EC2 access.



User groups (3) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□ Group name	Users	Permissions	Creation time
□ Cybertech-Audit-group	3	✓ Defined	1 hour ago
□ Cybertech-Developers-Group	1	✓ Defined	11 minutes ago
□ Cybertech-Sales-Group	2	✓ Defined	29 minutes ago



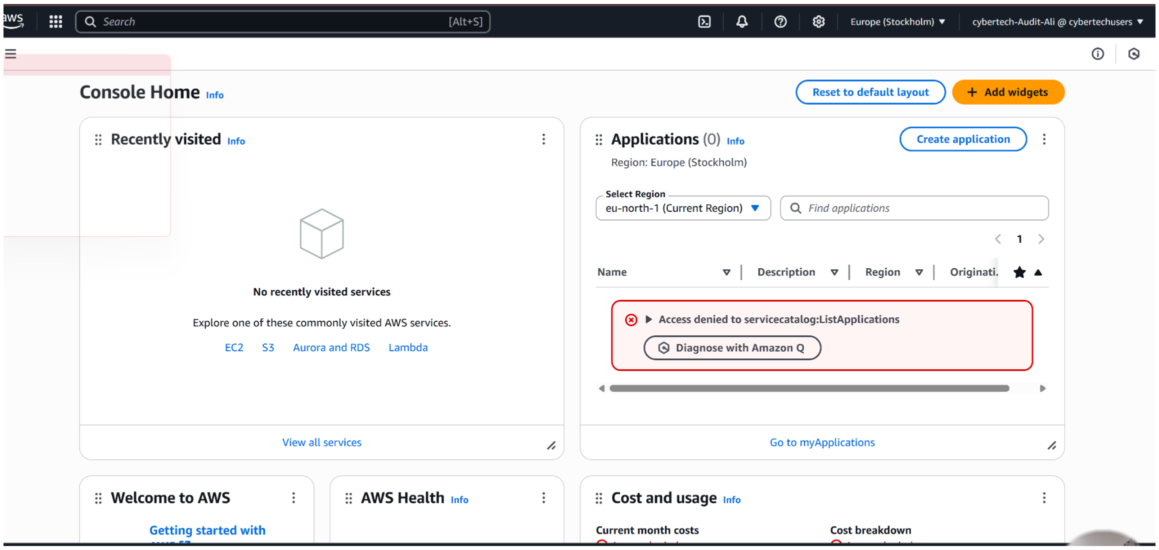
Users (4) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□ User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age	Acce
□ Cybertech-Audit-Raf	/	1	✓ 1 hour ago	-	✓ 1 hour	July 07, 2025, 16:22 (...	-	-	
□ Cybertech-Audit-Raf1	/	1	✓ 1 hour ago	-	✓ 1 hour	July 07, 2025, 16:35 (...	-	-	
□ Cybertech-Developer-Raf3	/	3	✓ Now	-	✓ 1 minute	July 07, 2025, 17:36 (...	-	-	
□ Cybertech-Sales-Raf2	/	1	✓ 3 minutes ago	-	✓ 4 minutes	July 07, 2025, 17:34 (...	-	-	

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

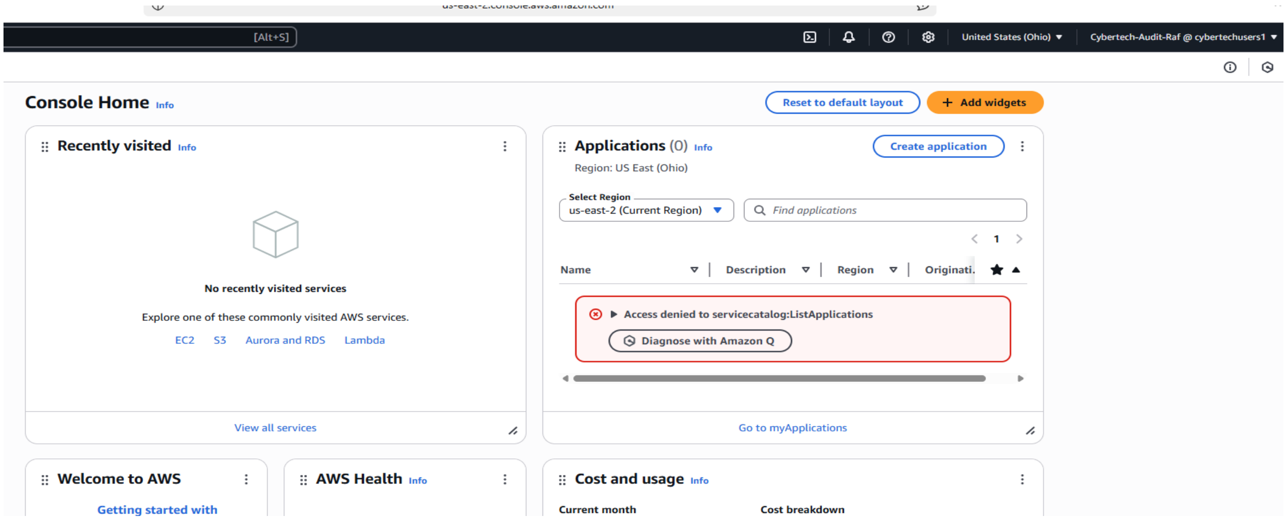


No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 Aurora and RDS Lambda

Access denied to servicecatalog:ListApplications

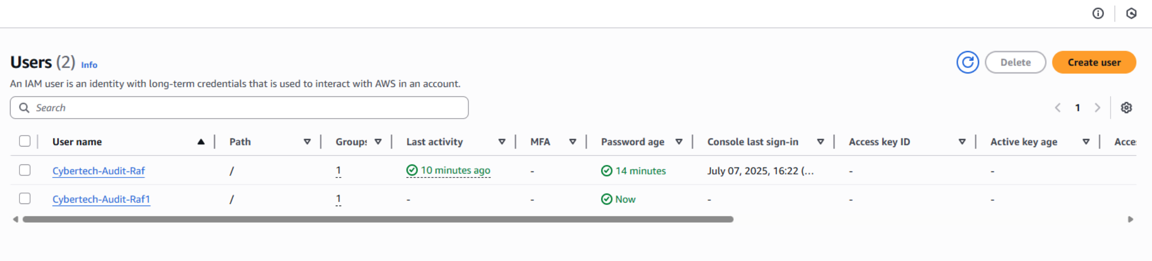


No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 Aurora and RDS Lambda

Access denied to servicecatalog:ListApplications

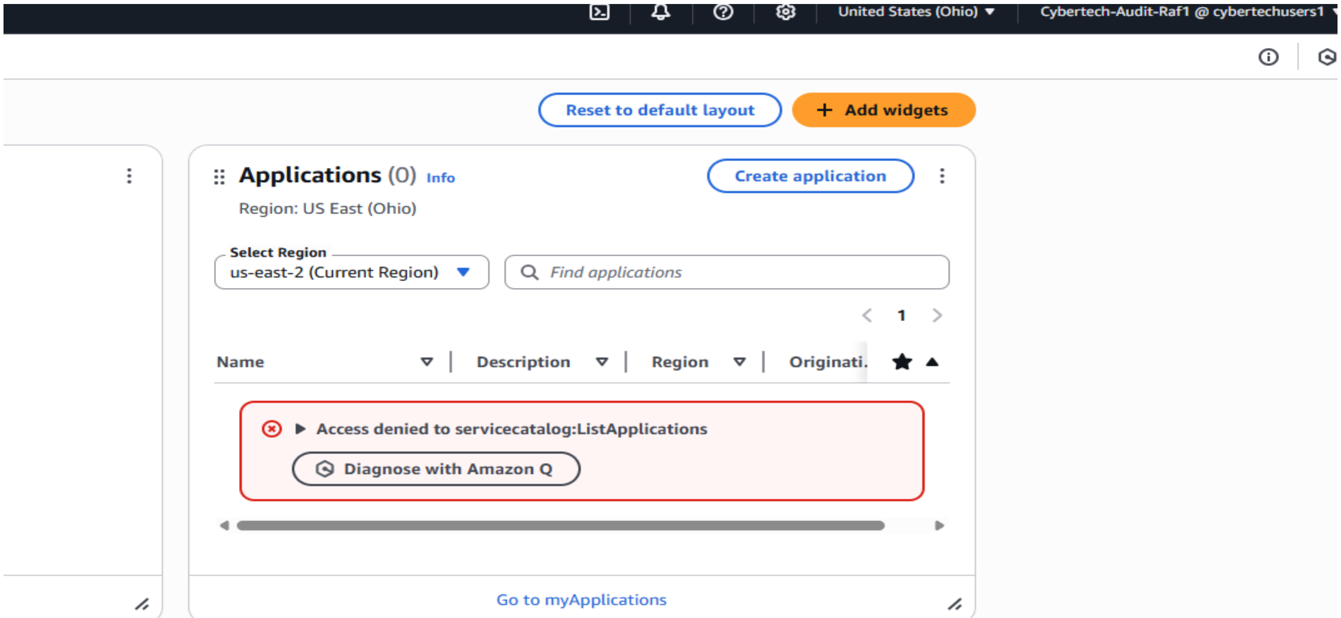


An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

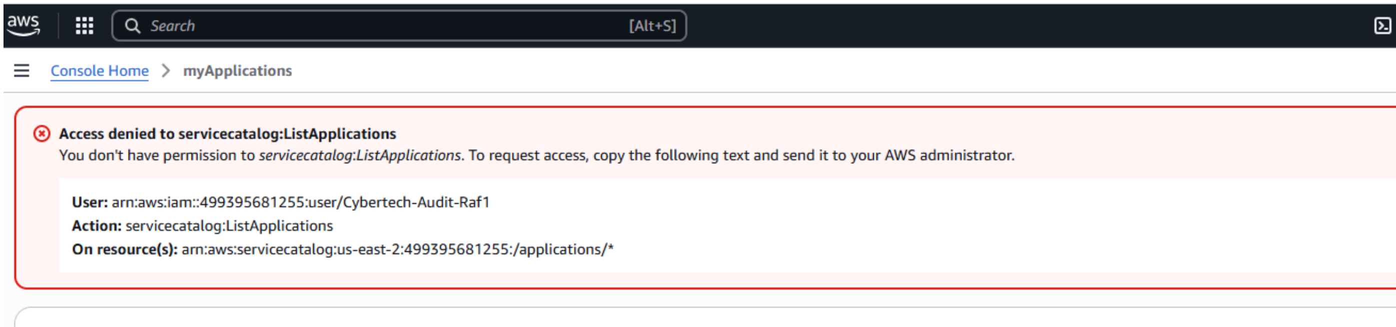
□	User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age	Acce
□	Cybertech-Audit-Raf	/	1	✓ 10 minutes ago	-	✓ 14 minutes	July 07, 2025, 16:22 (...	-	-	
□	Cybertech-Audit-Raf1	/	1	-	-	✓ Now	-	-	-	

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



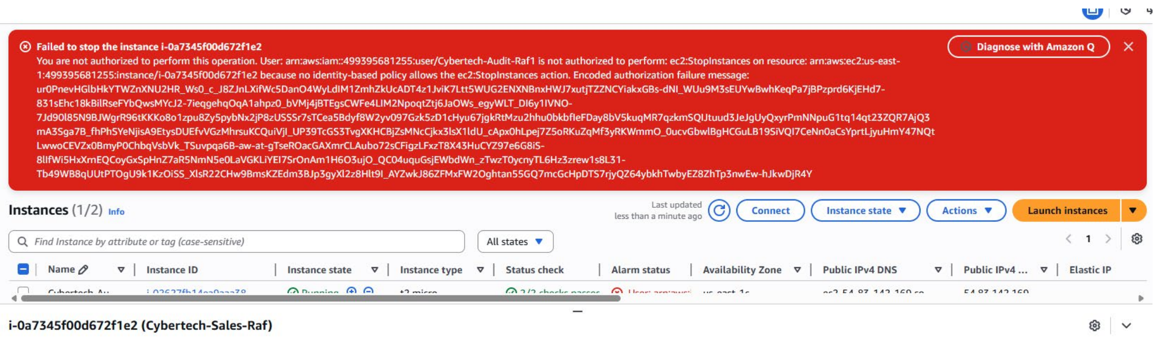
Access denied to servicecatalog:ListApplications



Access denied to servicecatalog:ListApplications

You don't have permission to *servicecatalog:ListApplications*. To request access, copy the following text and send it to your AWS administrator.

User: arn:aws:iam::499395681255:user/Cybertech-Audit-Raf1
Action: servicecatalog:ListApplications
On resource(s): arn:aws:servicecatalog:us-east-2:499395681255:/applications/*



Failed to stop the instance i-0a7345f00d672f1e2

You are not authorized to perform this operation. User: arn:aws:iam::499395681255:user/Cybertech-Audit-Raf1 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:499395681255:instance/i-0a7345f00d672f1e2 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message:

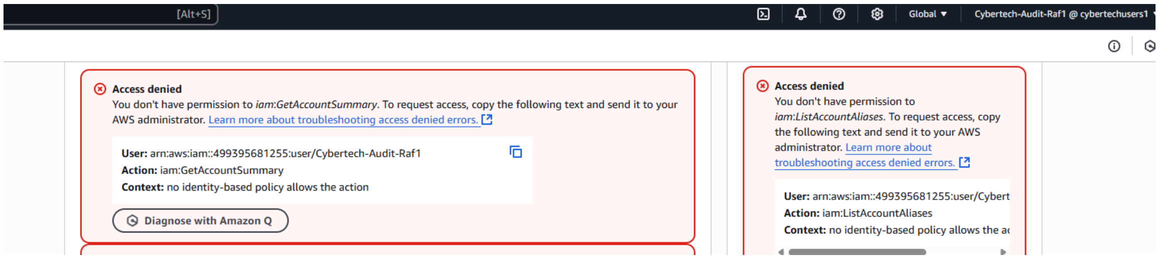
```
ur0PnevHGlbHkYTWZnXNU2HR_Ws0_c_J8ZJnLXifWc5DanO4WyLdIM1ZmhZkUcADT4z1JviK7Ltt5WUG2ENXNBnxHWJ7xutjTZZNCYiakxGBs-dNI_WUu9M3sEUYwBwhKeqPa7jBPzprd6KjEHd7-
831sEhc18kBilRseFYbQwsMYcJ2-7ieqgehqOqA1ahpz0_bVMj4jBTEgsCWFe4LIM2NpoqtZtj6JaOWs_egyWLT_DI6y1IVNO-
7Jd90l85N9BJWgrR96tKKKo8o1zpu8Zy5pybNx2jP8zUSSSr7sTCea5Bdyf8W2yv097Gzk5zD1cHyu67jgkRtMzu2hhu0bkbfIeFDay8bV5kuqMR7qzkmSQIJtuud3JeJgUyQxyrPmNNpuG1tq14qt23ZQR7AjQ3
mA3Sga7B_fhPhSYeNjisA9EtysDUEfvVGzMhrsuKCQuiVjI_UP39TcGS3TvgXKHCBjZsMNcCjkx3lsX1ldU_cApx0hLpej7Z5oRKuZqMf3yRKWmmO_0ucvGbwlBgHCGuLB19SiVQI7CeNn0aCsYprtLjyuHmY47NQt
LwwoCEVZx0BmyP0ChbqVsbVk_TSuvpqa6B-aw-at-gTseROacGAXmrCLAubo72sCFigzLFxzT8X43HuCYZ97e6G8iS-
8llfWi5HxXrnEQCoyGxSpHnZ7aR5NmN5e0LaVGKLiYEI7SrOnAm1H6O3ujO_QC04uquGsjEWbdWn_zTwzT0ycnyTL6Hz3zrew1s8L31-
Tb49WB8qUUtPTOgU9k1KzOiSS_XlsR22CHw9BmsKZEdm3BJp3gyXl2z8Hlt9I_AYZwkJ86ZFMxFW2Oghtan55GQ7mcGcHpDTS7rjyQZ64ybkhTwbyEZ8ZhTp3nwEw-hJkwDjR4Y
```

Instances (1/2) Info

Last updated
less than a minute ago

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☐	Cybertech-Au...	i-02627fb14aa0aaa78	Running	t2.micro	2/2 checks passed	User: arn:aws:i...	us-east-1c	ec2-54-87-142-160.co...	54.87.142.160	

i-0a7345f00d672f1e2 (Cybertech-Sales-Raf)



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::499395681255:user/Cybertech-Audit-Raf1
Action: iam:GetAccountSummary
Context: no identity-based policy allows the action

Access denied

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::499395681255:user/Cybert
Action: iam:ListAccountAliases
Context: no identity-based policy allows the ac