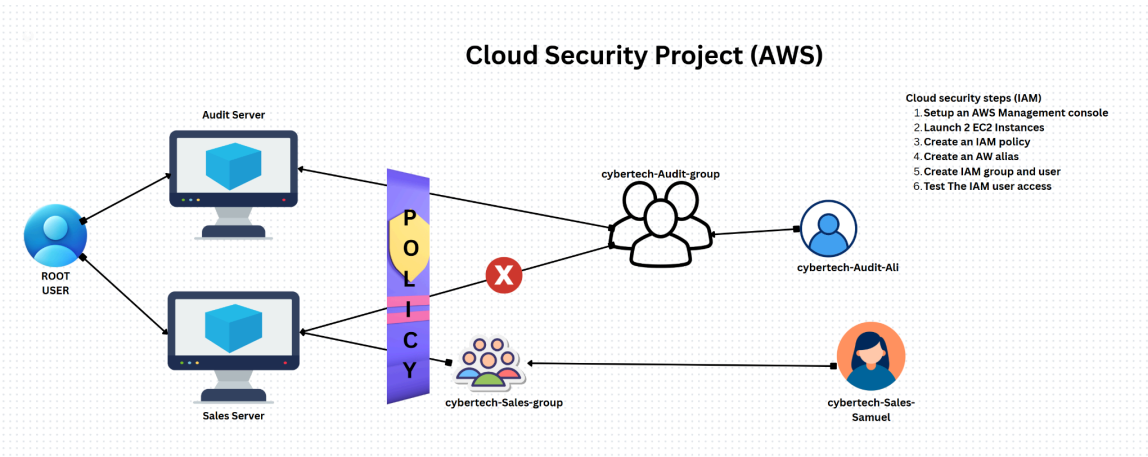
AWS IAM Cloud Security Project

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).



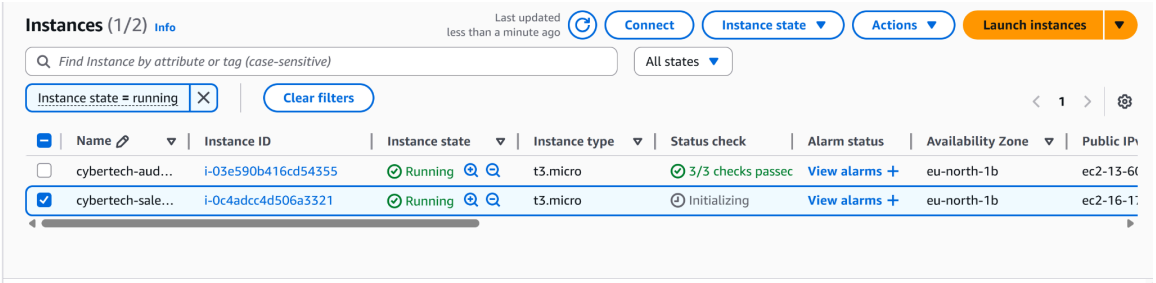
2. Tools & Concepts

- 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

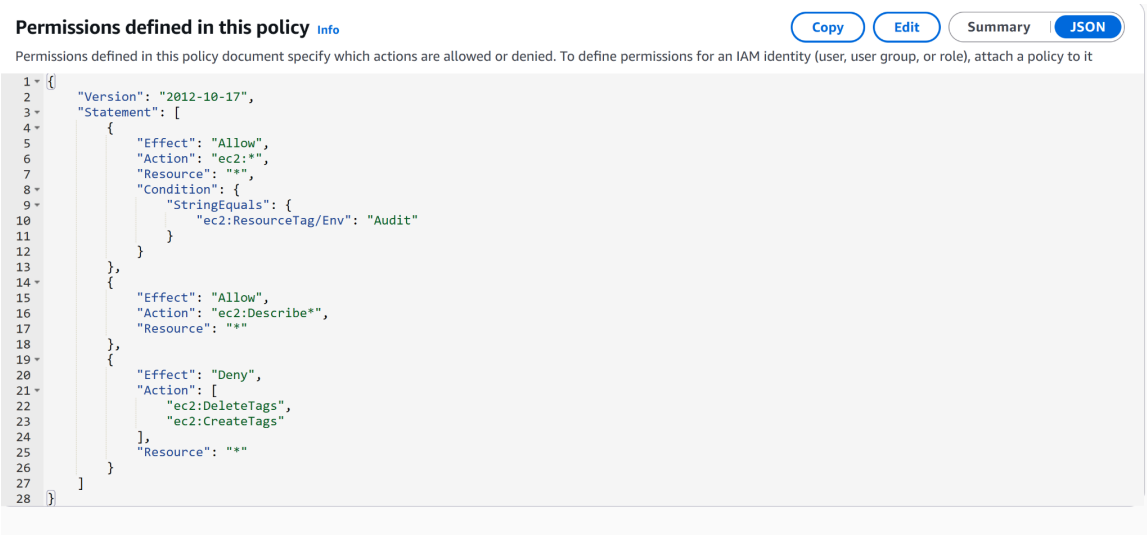
I applied a descriptive tag to each EC2 instance:

Instance	Tag Key	Tag Value
audit	Environment	Audit
sales	Environment	Sales



4. Creating the IAM Policy

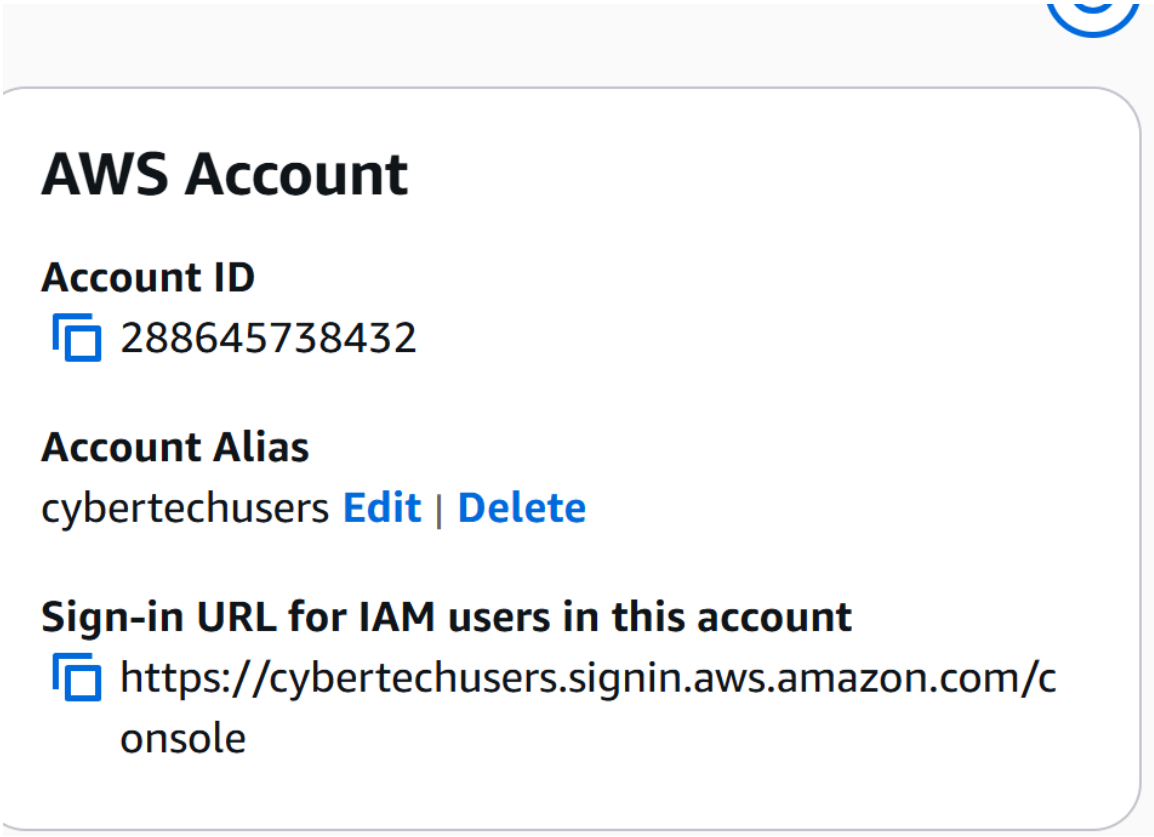
I authored the following JSON policy to block instance stop/start actions on the audit server but allow those actions on the sales server:




```
{
    "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": "*"
        }
    ]
}
```

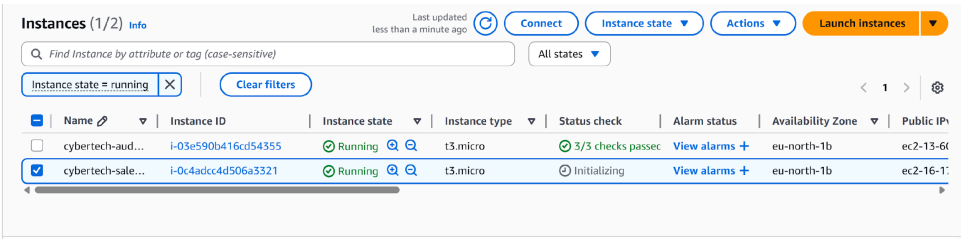
5. Account Alias

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



6. IAM Users & Groups

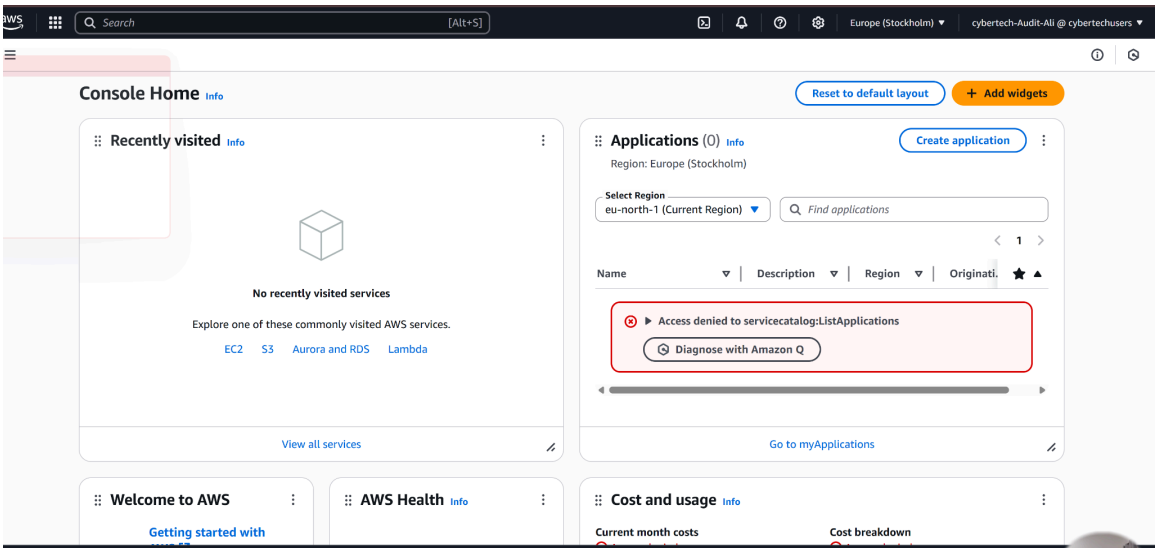
1. Created an IAM user group called Developers.
2. Attached the **CybertechAuditEnvPolicy** policy to the group.
3. Added individual IAM users who require controlled EC2 access.



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

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

Diagnose with Amazon Q

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: sAVefFO1FXiTMRJ52xofhO4bpSGLz7iFqT-w1DqTxLoat_lV4T5r87OVMHxzrfSSmG4VXfVa2cDWhfQ1uQO0shFk8kUgfZhoC9Tn_IhCnKyVswG-blgkFFw9OLb4-2CT9TP841l8nI9O6EaSTAt0ztgtsh2t1VXnMzhUuPZeqMg3Ajek6wr21S90c0le6YNjRMmocGw8Gd_xH9dlfdp-4ilwIF0H1uwTpAt1QHgqr8FbW3kJ0ue7UMNuHGzJzgCiiA30Q5pqHwW1_ALxzQAulhMpW9i6xdEiwRRL0fQG_W-dDTm6Z7YNPth09woBuuiXzLbc13Mz5-ciFyB_0PBgVz8xKMy4kuncI_zDmTsNfyv0sszpKwvYxm8Du71JN3rSTmBylKAIW0cA0nzxOFVWIQ9kigwtxbT-gocngZgZGlLqW2RxlqW8XBC42OEN3llZ-URe-xYZCS1palfmIcLRiDvCBZjNWPr4rK_0WgaADMkzFgQjk7xmnnNmFi2mgHr5Aw46VvHCp-pqURgYZ_Oa8xBnq7y6luLZ_MxIUb20pZDhB0SynHoNGRm0MRzRy1etyCipN14aBfvWB12hSkMoXobUZawc9Rat-Pk_vPSbim-Opv1riuGTCT-YJtIZ6FSYUFfECxnmX6B3iFHqgGTOp6sDAzIXMCX3g2yqEqbTN5f-ClWsZbvA7Ck5m5yf8nt1po_-8fBDM67ZwyEe21nGxikjEmj_nMMMfQVPqk46tBHdwRYHLxQQA2b-cG58fOMUsv_eHnT1xBHLtkVMB7VxU-_Scg_KyhwQlMrGy4NR4Ho_RumoDyK8aWNLTIxh-j1yTKrJk8ctDTtf11lQzyfSAKRTQp_-j1QBrzXEA47t8IXxAwqRD3vWCNE3PL3YfwcYpRHP

Instances (1/2) Info

Connect | Instance state | Actions | Launch instances

Find Instance by attribute or tag (case-sensitive) | All states | 1

i-0b9626f2835a5f977 (Cybertech-sales-Ali)

Details | Status and alarms | Monitoring | Security | Networking | Storage | Tags