AWS Cloud Console Configuration & Hardening Project.

Project Overview

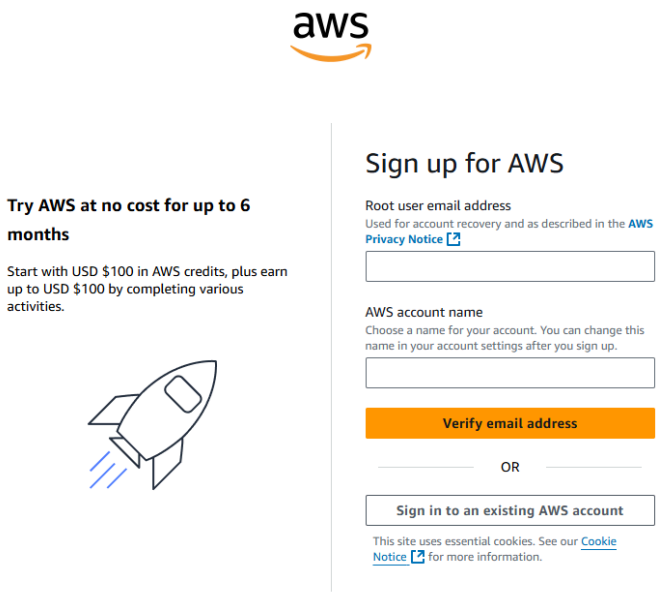
This project demonstrates how to securely configure and harden the AWS Management Console using IAM best practices. The goal is to reduce unauthorized access, apply least privilege permissions, and validate access control through testing.

Key security concepts covered:

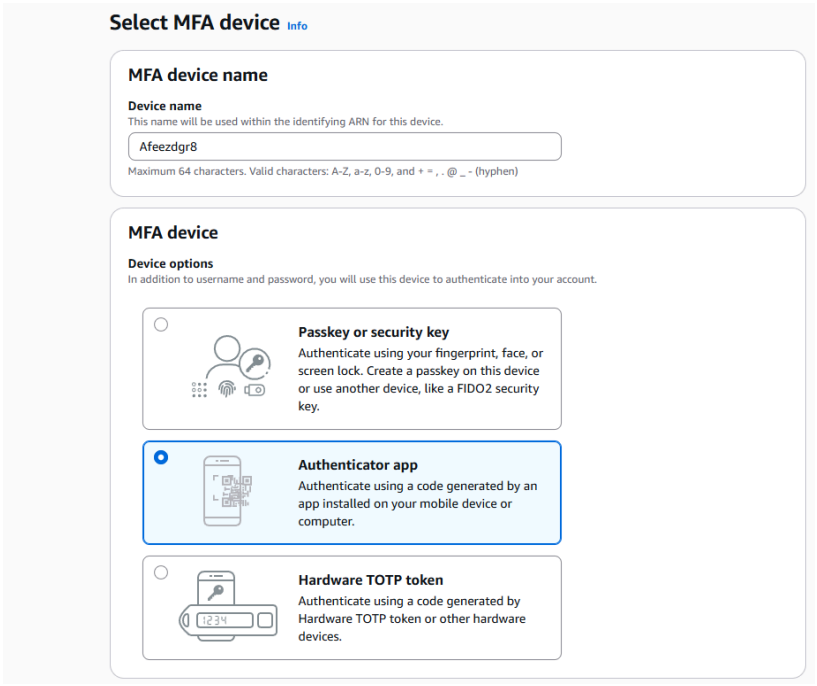
- AWS Management Console Root Account set up (secured)
- Setting up 2 EC2 instances
- Creating an IAM Policy
- Creating an AW Alias
- Creating IAM group & User
- Test the IAM user access

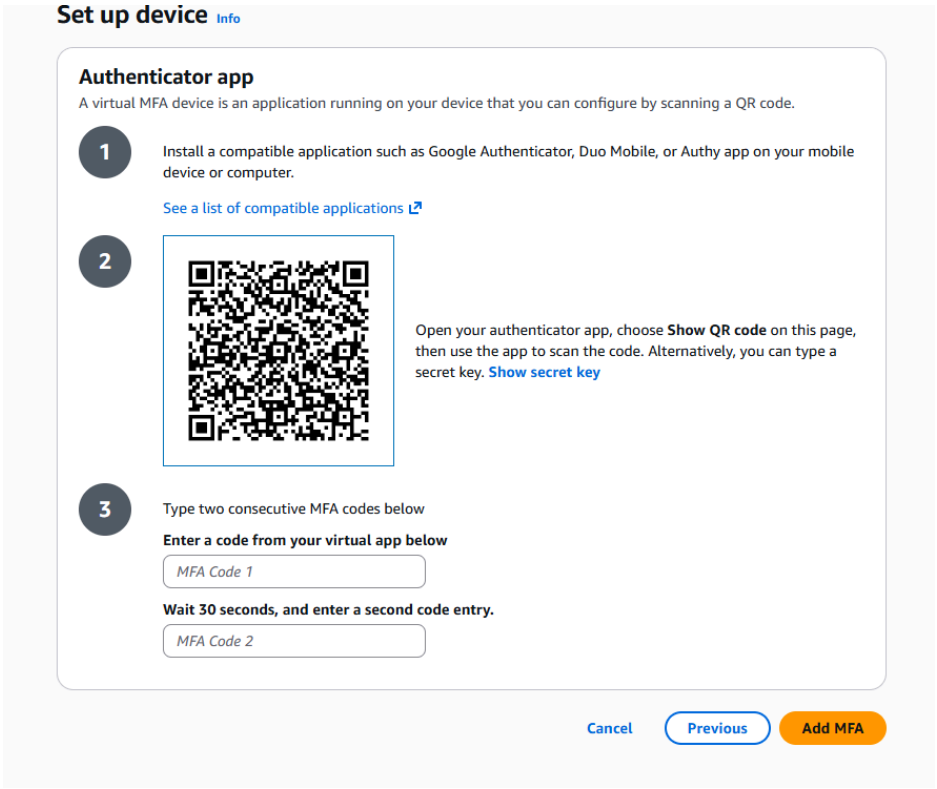
Setting Up the AWS Management Console

I went on https://aws.amazon.com/ to create an account. I signed up as a new user. I completed the identity and billing set up.



I logged in as a root user and was immediately prompted to add a Multi Factory authentication which I did.

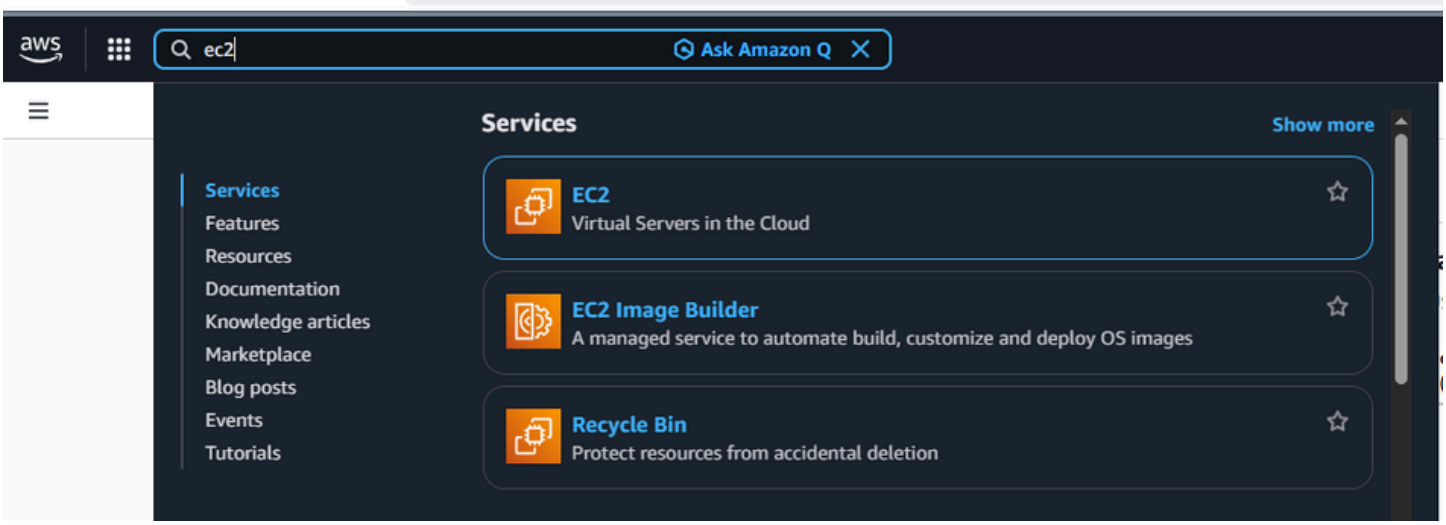




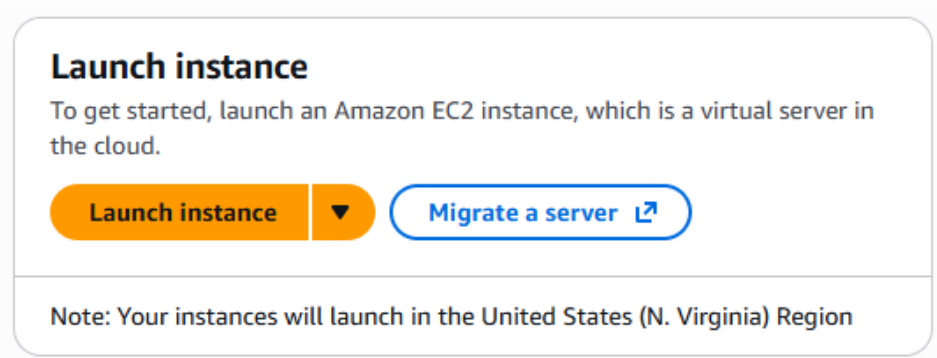
Multi Factory authentication was activated.

Setting up 2 EC2 instances

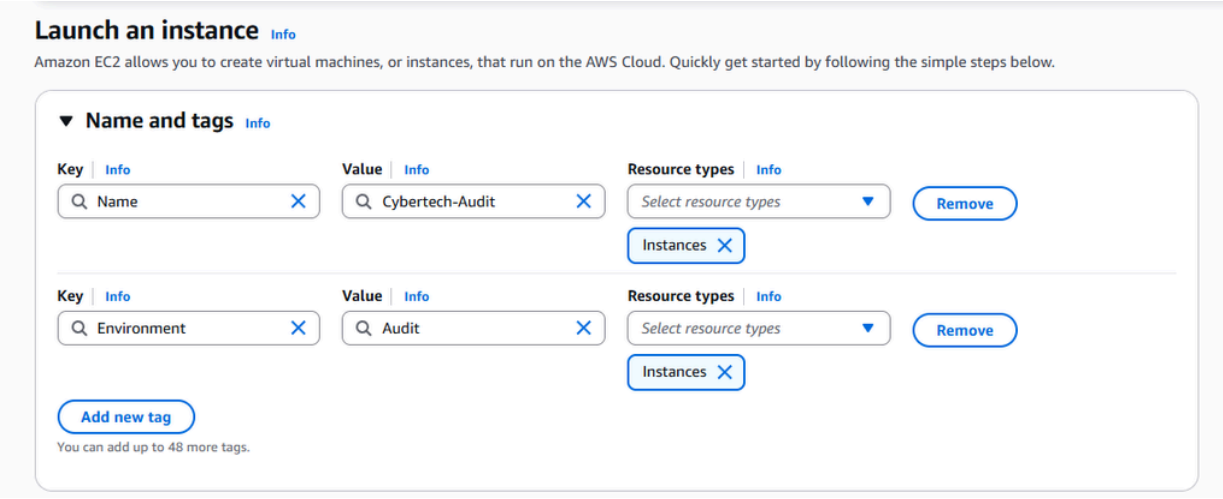
In order to be able to create the 2 EC2 (Audit & Sales) I clicked on the search bar and typed EC2. I selected the first one that says “Virtual Servers in the cloud”.



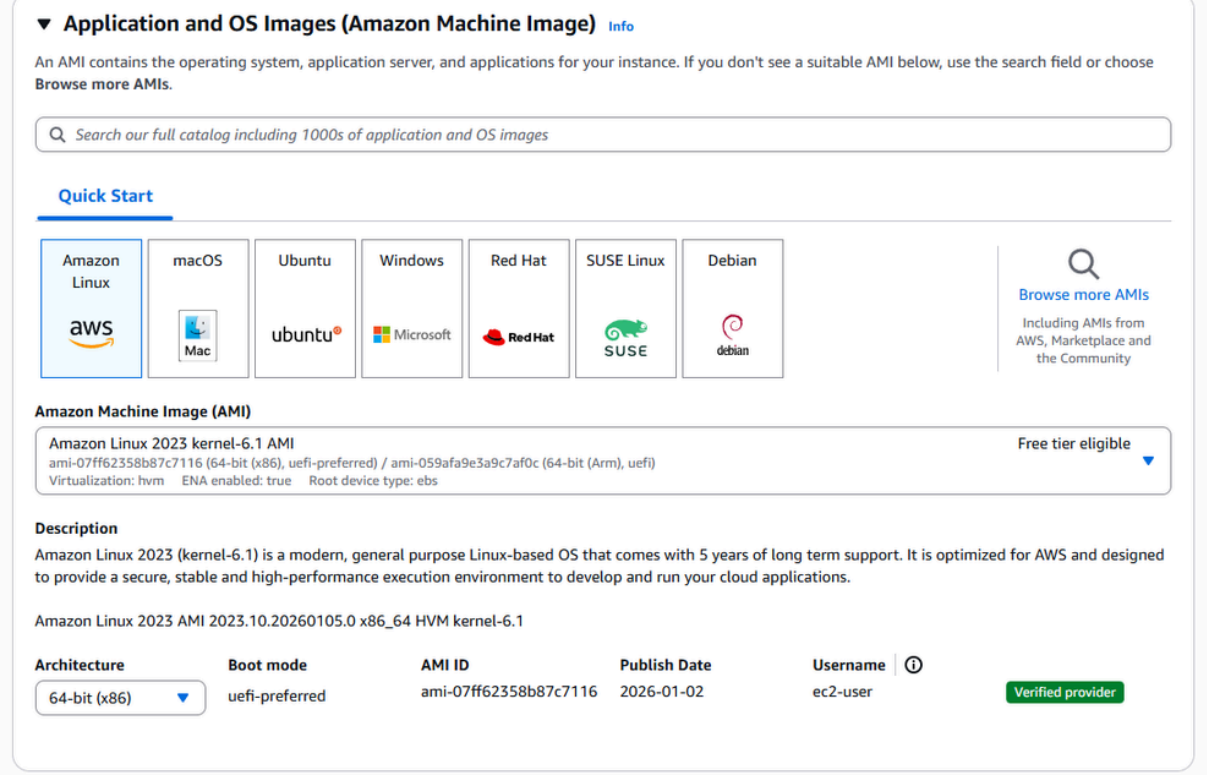
I clicked on “Launch Instances”



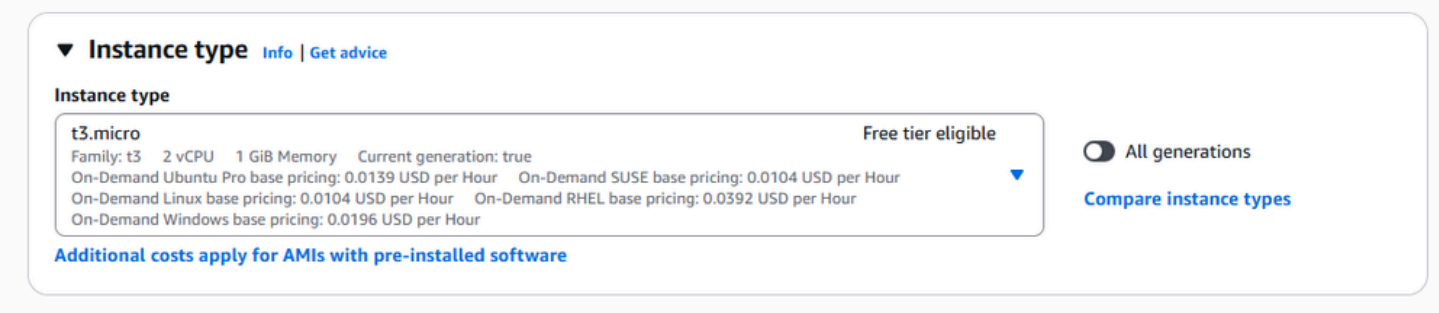
I input the name and added a new tag to indicate which environment it belongs, which is the Audit environment.



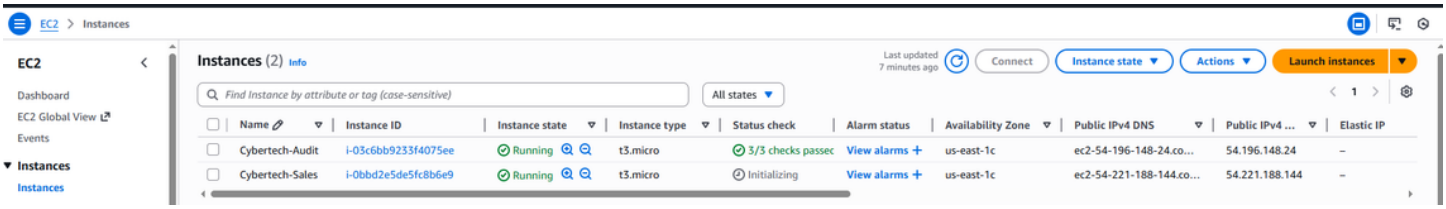
The next step is the selection of the AMI which is the operating system I want the server to run on. I chose the Amazon Linux AMI.



I moved on to the instance type which refers to the number of core and Ram I want to assign to it. I selected t3.micro which can run 2vCPU and has 1GB of memory.



I then launch my instances and created the second one following the same steps and settings and my two EC2 has been created.

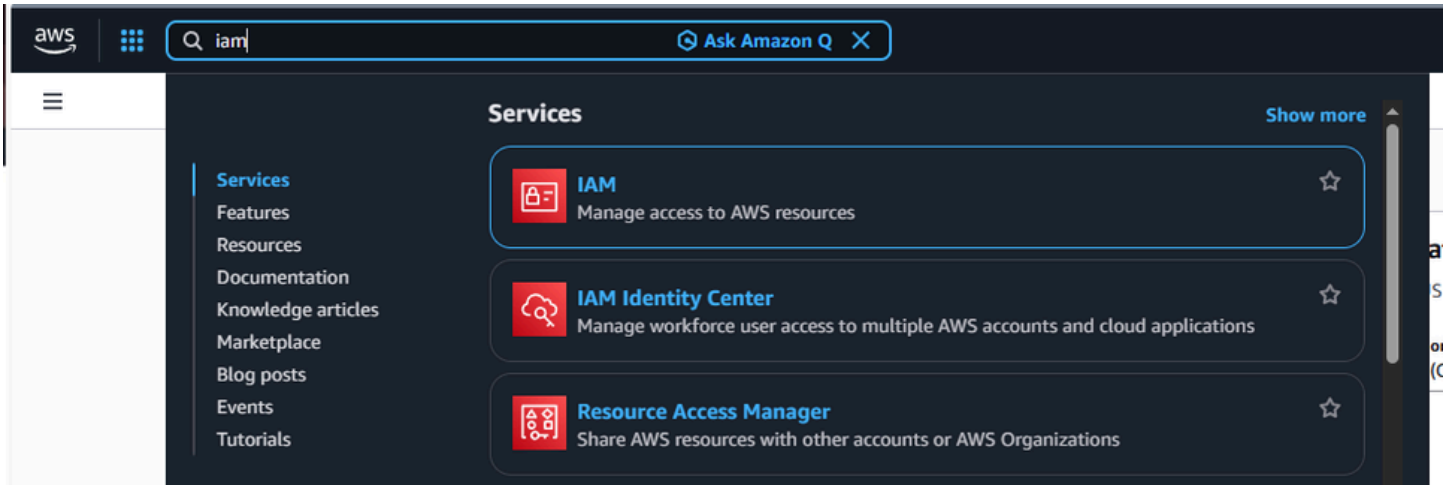


Creating an IAM Policy

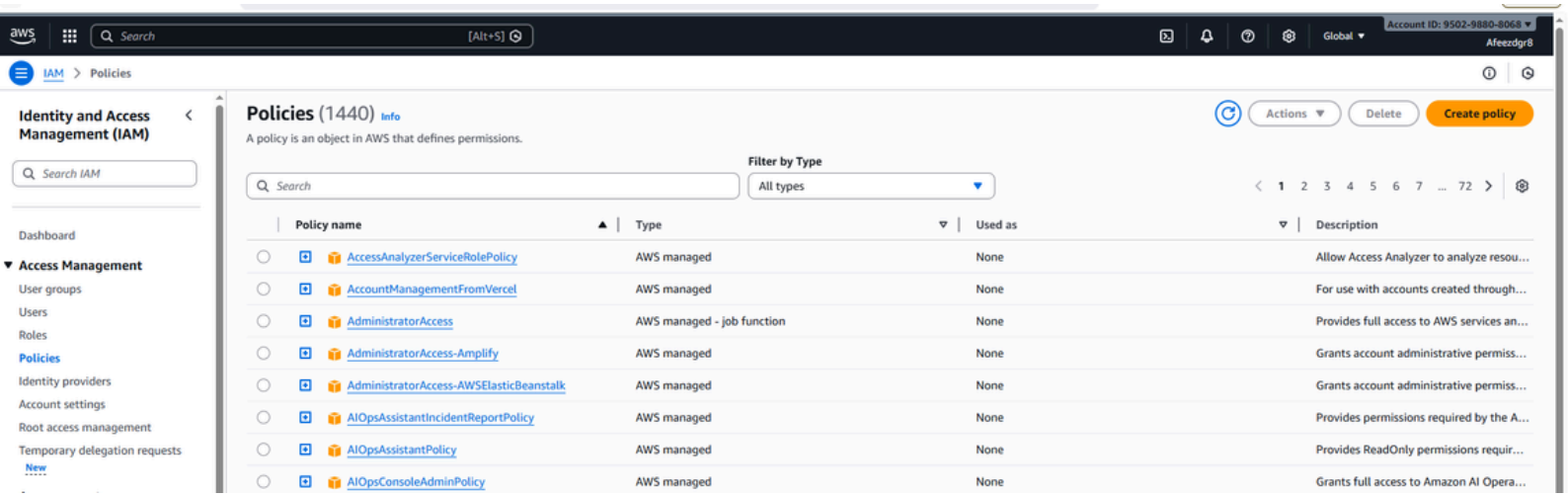
Moving on in the cloud security project, I want to create a policy.

Policies are role which tells who has access to what on our cloud infrastructure.

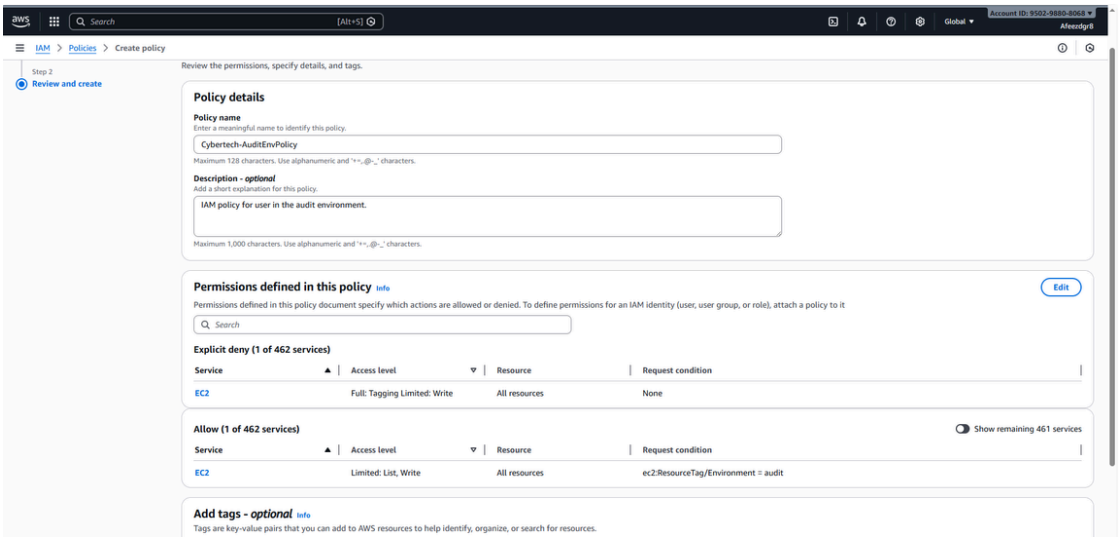
To do that, I will search for IAM in the search bar and select the first option.

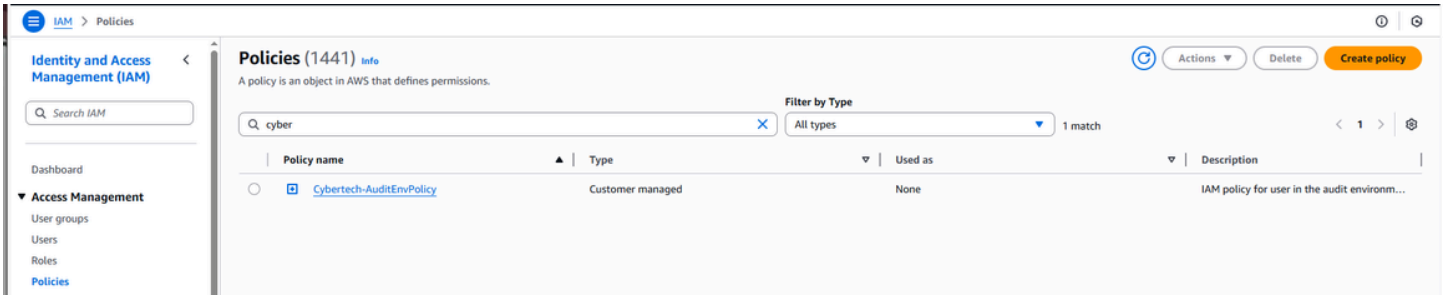


I navigate to policy and I click on “create policy” in order to create my own policy.



I added the policy I created and gave it a name and clicked on “create policy”.

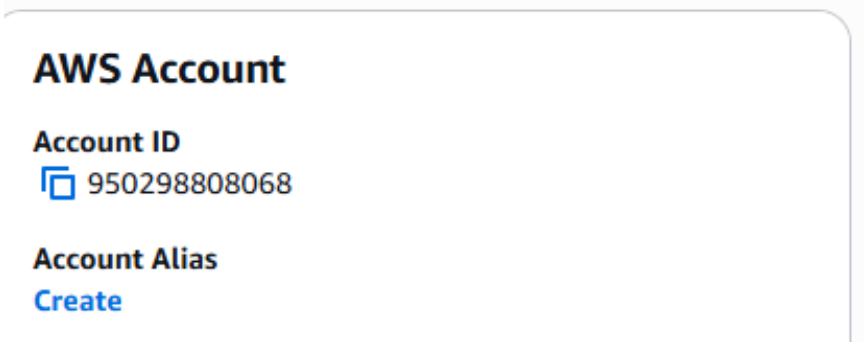


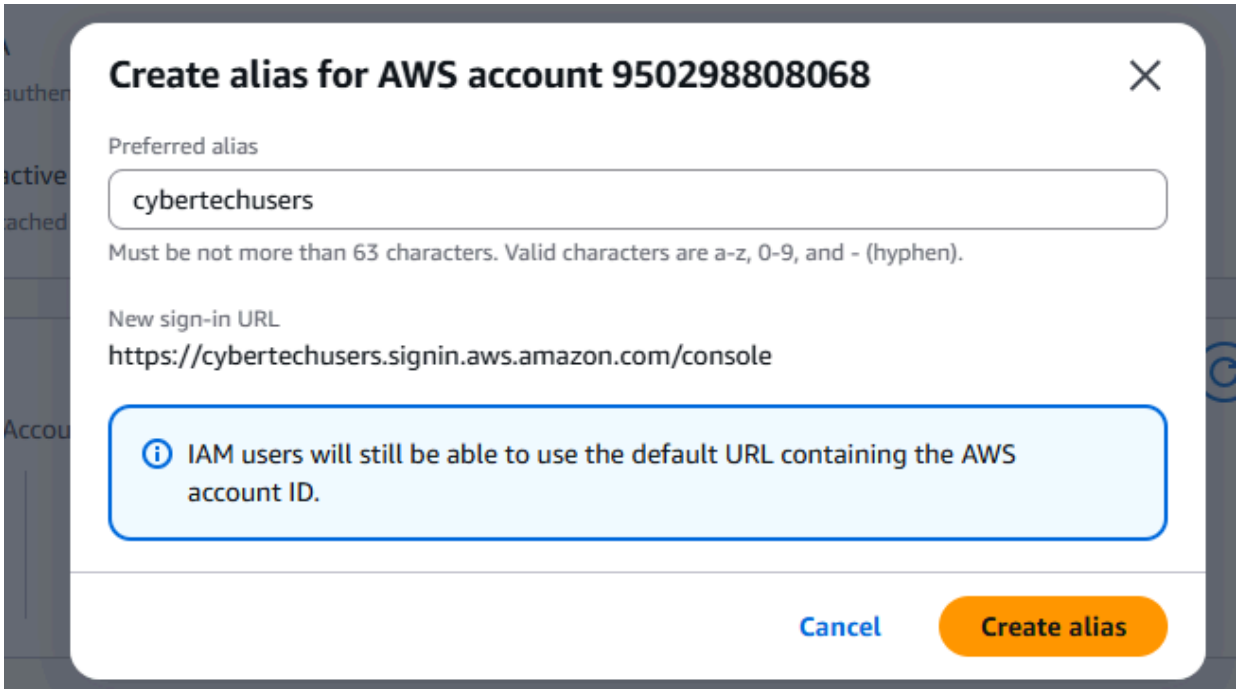


Creating an AW Alias

As I am currently logged in as a root user, I want to make logging for users to be easy, so I will create an alias login for them.

I will click on the search bar and search for IAM, and click on “create” under account alias. I gave it a name and clicked on create alias.





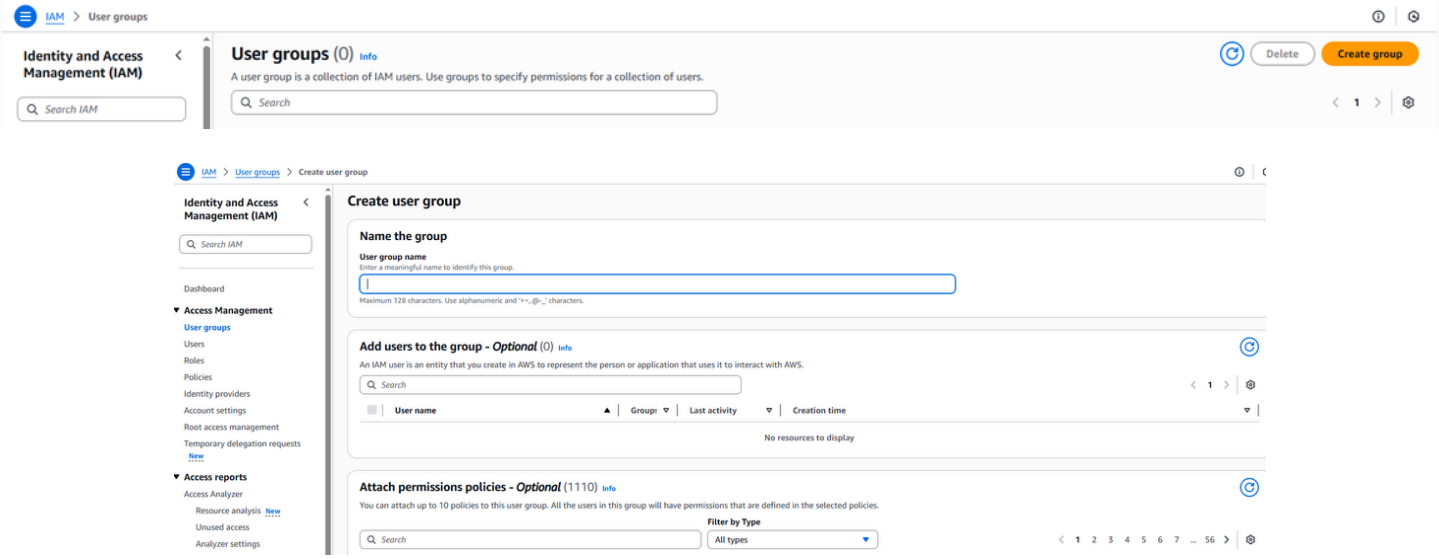
Creating IAM group & User

The next step I want to do is to create the groups and users.

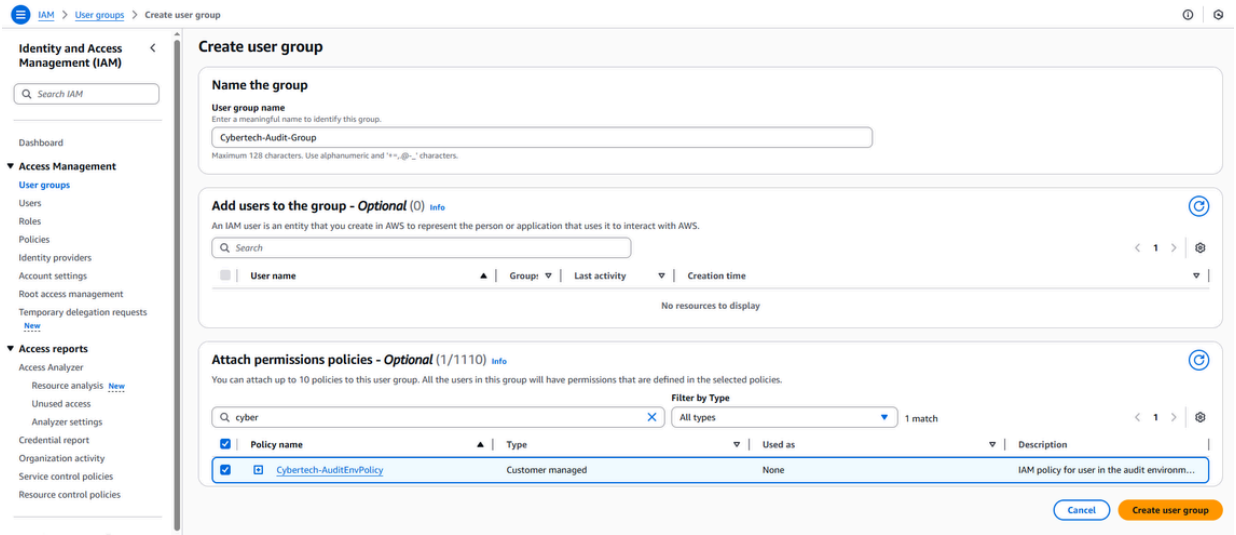
A group consist of different IAM users. The importance of creating a group is to make it easy when we want to apply a policy, it will affect all users in that group. Which makes it eaiser to assign policy to users.

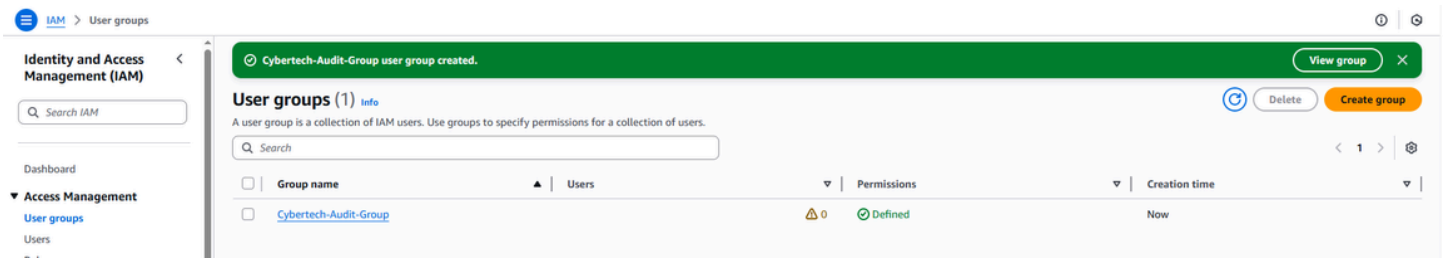
IAM user is a member of a group.

To create a group, I search for IAM in the search bar and I clicked on “User group”, then I clicked on create group.

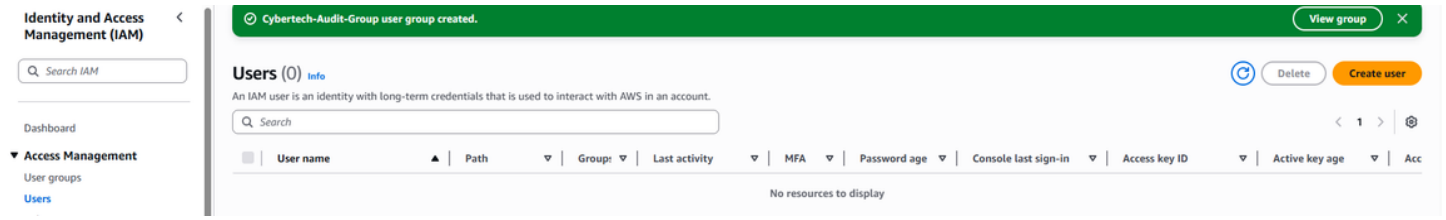


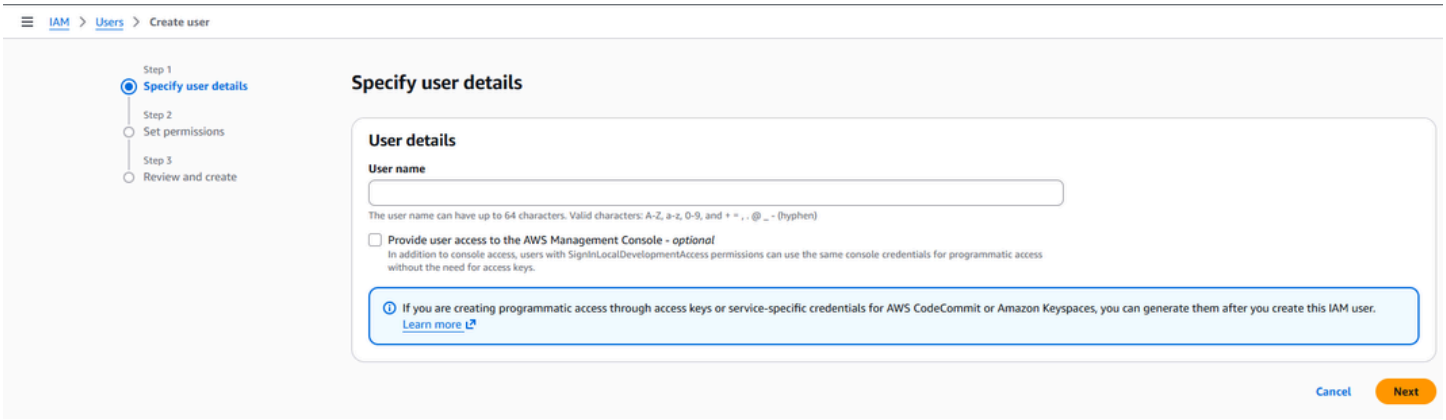
I gave my group a name and I attached the policy I previously created and I clicked on “create user group”.



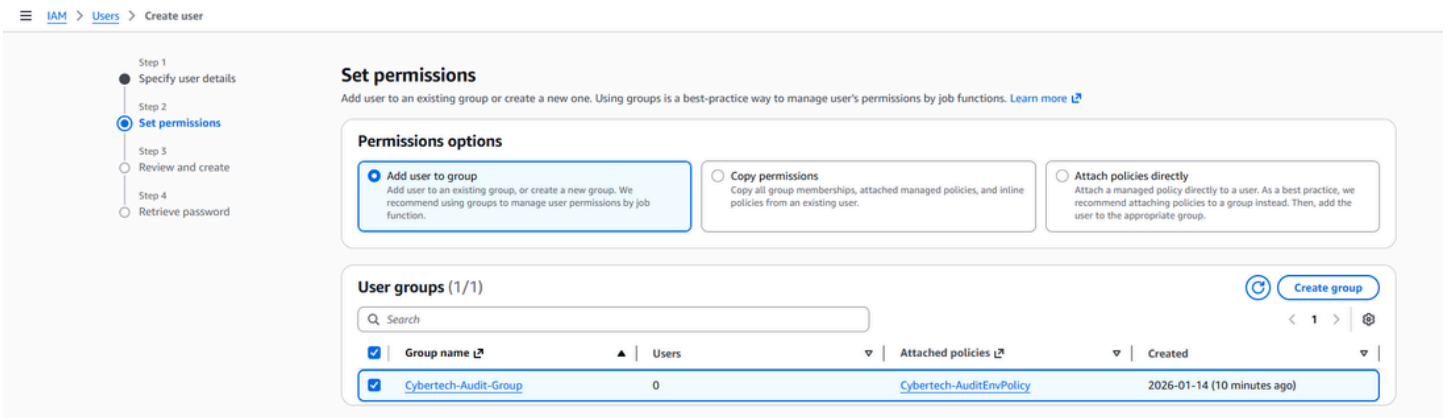


The next thing I want to do is to create user. In the same IAM tab, I clicked on “users”, then i clicked on create user.

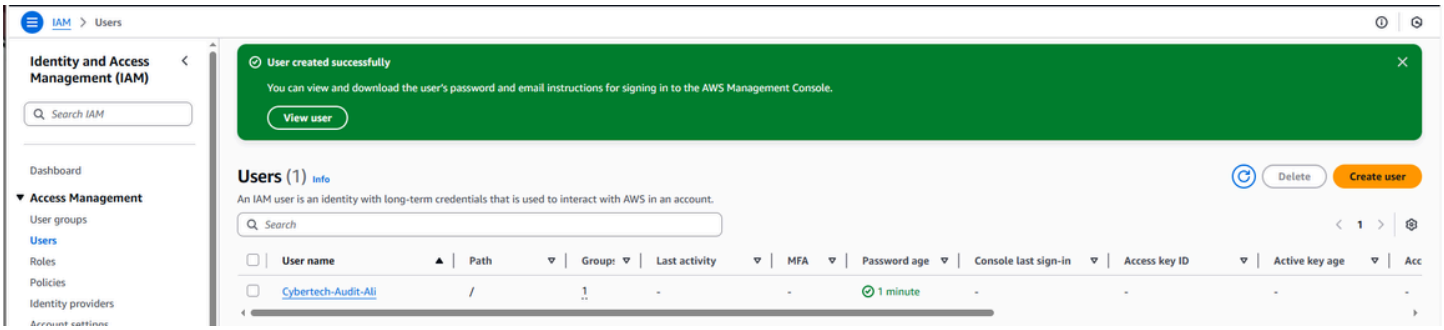




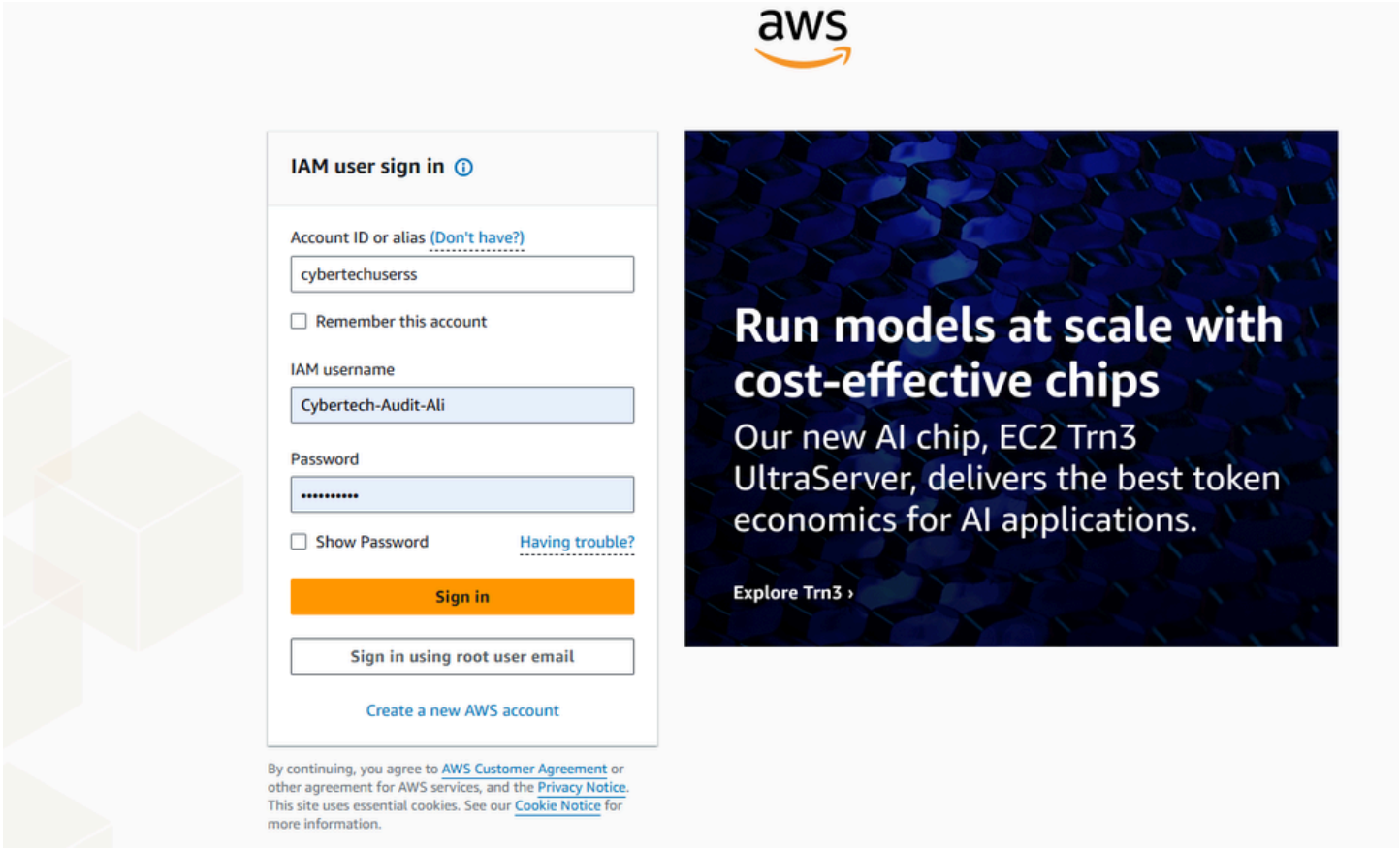
I added the user to the group I previously created.

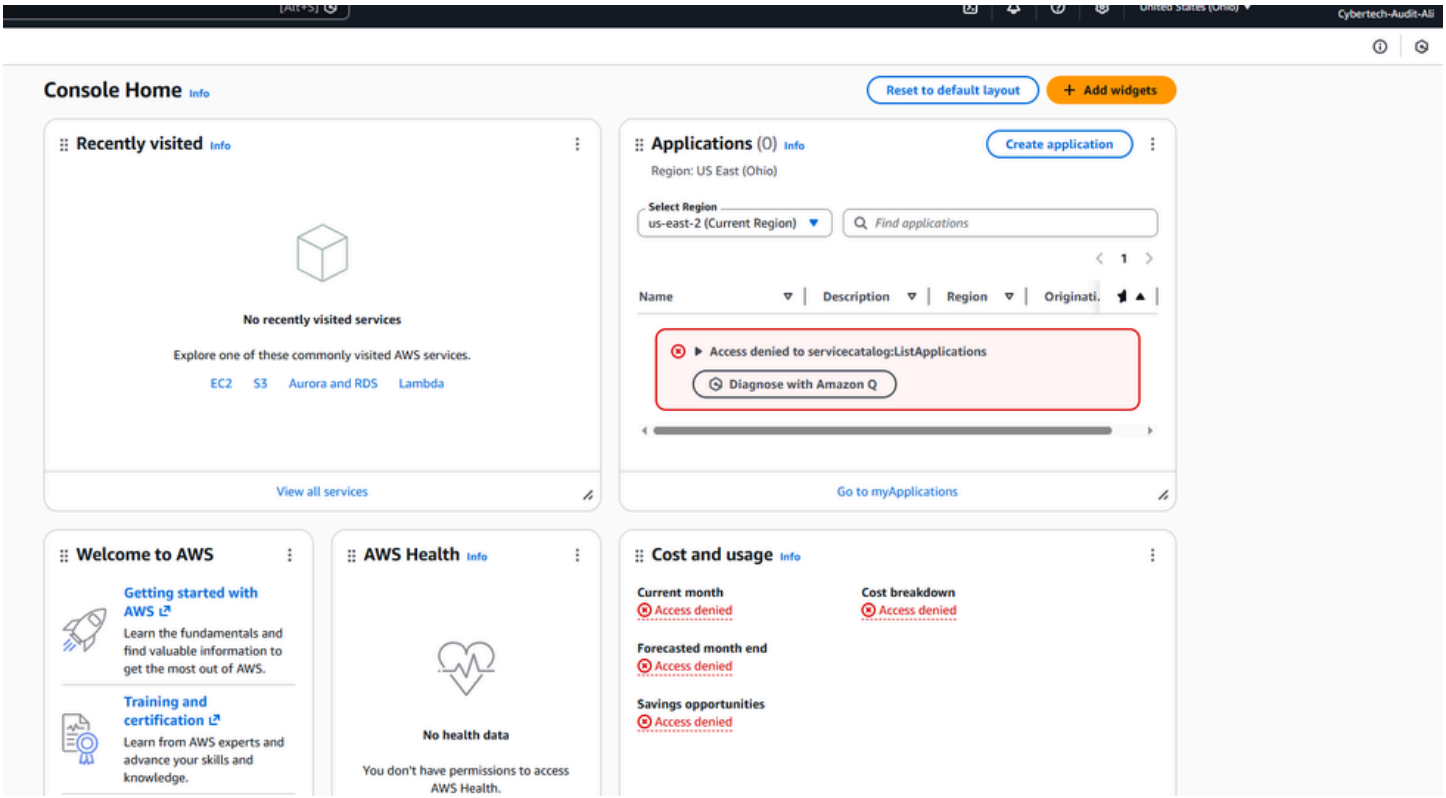


User created successfully and added to a group.



I signed in as the new user created.

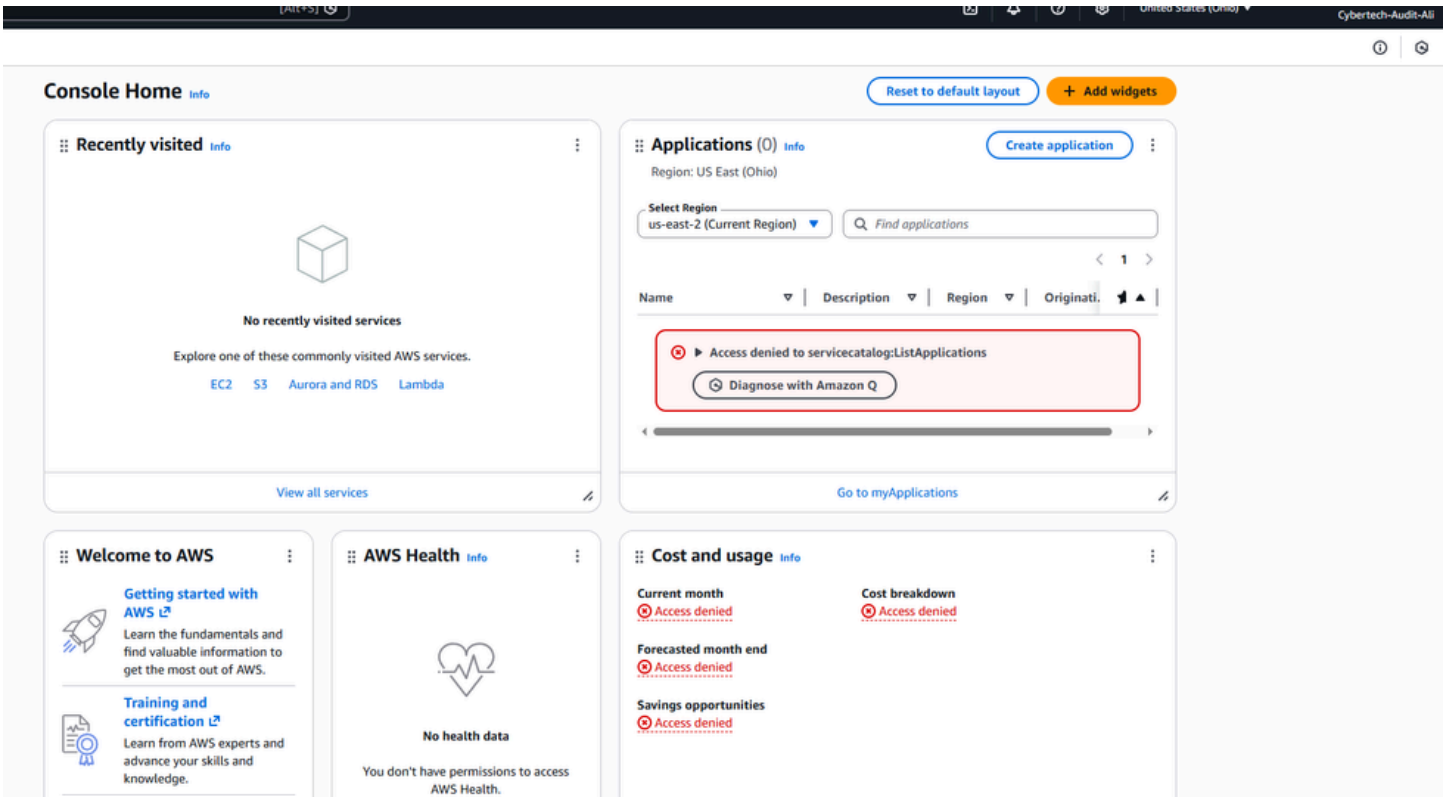




Test the IAM user access.

Finally, I want to test if the policy works.

After signing in as the user, we can see the policy works due to the “access denied” message it display.



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::950298808068:user/Cybertech-Audit-Ali
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::950298808068:user/Cybertech-Audit-Ali
Action: iam:ListAccessKeys
Context: no identity-based policy allows the action

Diagnose with Amazon Q

IAM resources

Resources in this AWS Account

Access denied to iam:GetAccountSummary
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::950298808068:user/Cybertech-Audit-Ali
Action: iam:GetAccountSummary
Context: no identity-based policy allows the action

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::950298808068:user/Cybertech-Audit-Ali
Action: iam:ListAccountAliases
Context: no identity-based policy allows the action

Diagnose with Amazon Q

Quick Links

My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator

The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.