

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.



Try AWS at no cost for up to 6 months

Start with USD \$100 in AWS credits, plus earn up to USD \$100 by completing various activities.



Sign up for AWS

Root user email address
Used for account recovery and as described in the [AWS Privacy Notice](#)

AWS account name
Choose a name for your account. You can change this name in your account settings after you sign up.

Verify email address

OR

Sign in to an existing AWS account

This site uses essential cookies. See our [Cookie Notice](#) for more information.

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


Select MFA device [Info](#)

MFA device name
Device name
 This name will be used within the identifying ARN for this device.


Maximum 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

MFA device
Device options
 In addition to username and password, you will use this device to authenticate into your account.


☐


Passkey or security key
 Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

☒


Authenticator app
 Authenticate using a code generated by an app installed on your mobile device or computer.


☐


Hardware TOTP token
 Authenticate using a code generated by Hardware TOTP token or other hardware devices.

Set up device [Info](#)

Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

- 1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)
- 

Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)
- 3 Type two consecutive MFA codes below
Enter a code from your virtual app below

Wait 30 seconds, and enter a second code entry.

[Cancel](#)

[Previous](#)

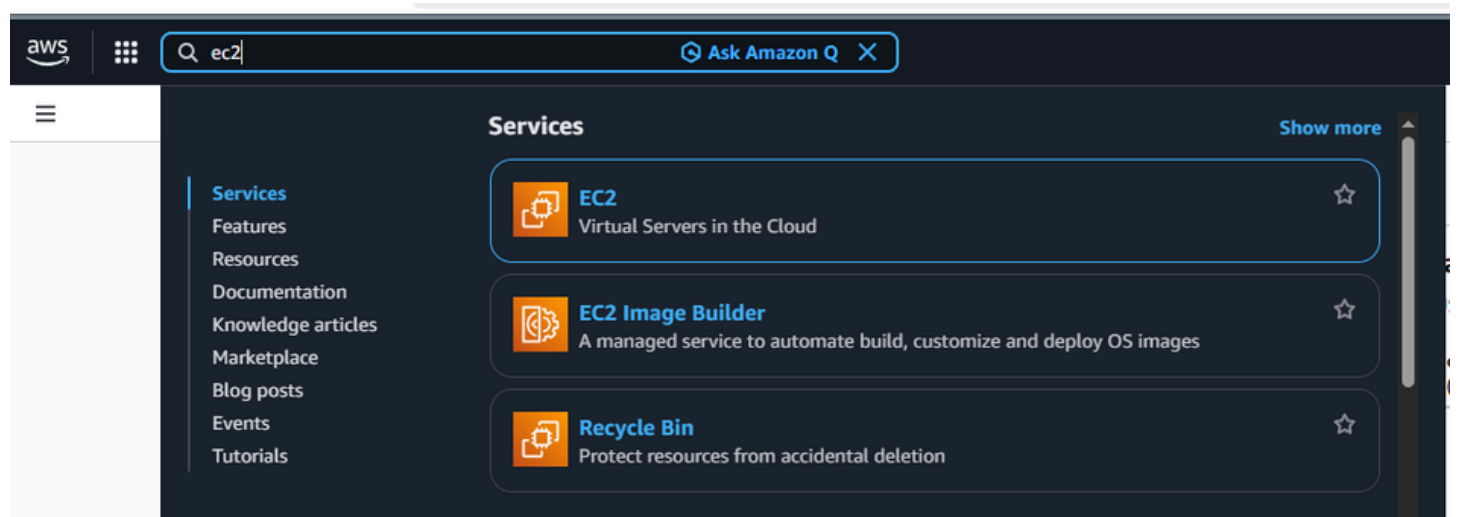
[Add MFA](#)

Multi Factory authentication was activated.

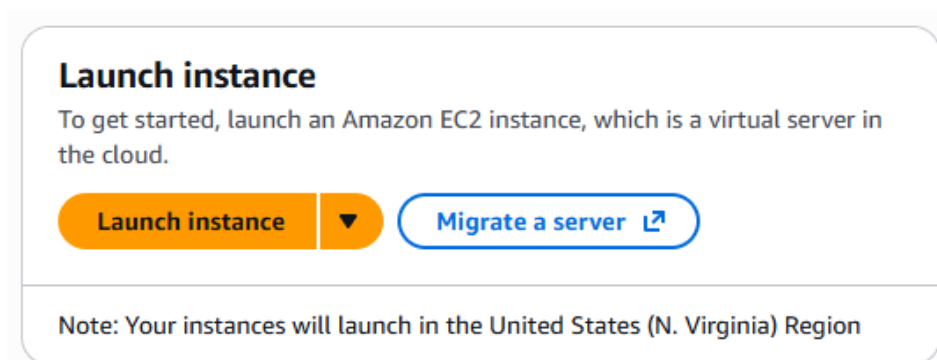
Multi-factor authentication (MFA) (1)				Remove	Resync	Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more						
Type	Identifier	Certifications	Created on			
<input type="radio"/> Virtual	arn:aws:iam::950298808068:mfa/Afeezdgr8	Not Applicable	Mon Jan 12 2026			

Setting up 2 EC2 instances

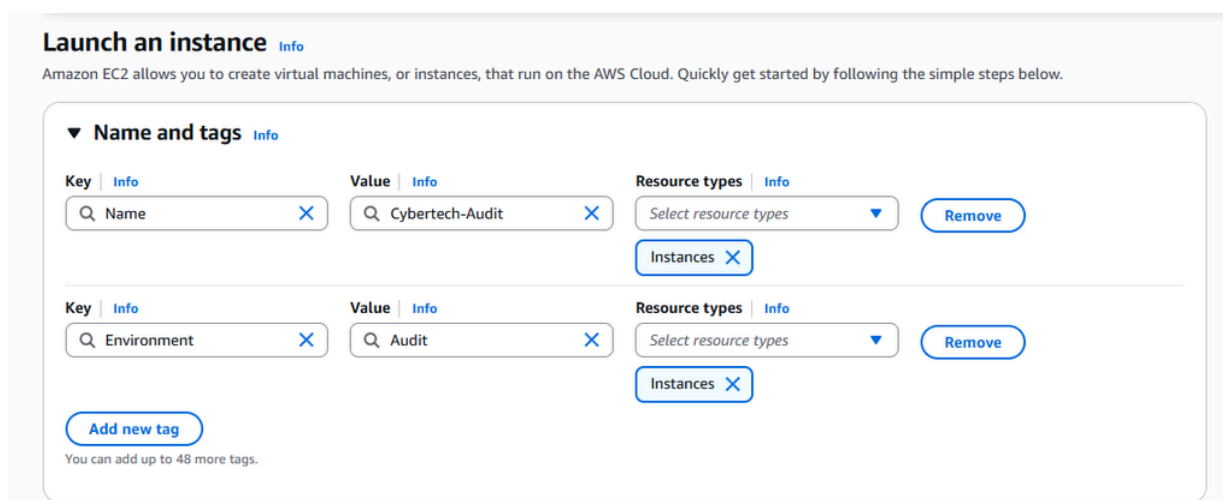
In order to be able to create the 2 EC2 (Audit & Sales) I clicked on the search bar and typed EC2. I selected the first one that says “Virtual Servers in the cloud”.



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.

▼ **Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux
aws

macOS
Mac

Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

SUSE Linux
SUSE

Debian
debian

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI
ami-07ff62358b87c7116 (64-bit (x86), uefi-preferred) / ami-059afa9e3a9c7af0c (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs Free tier eligible

Description

Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.10.20260105.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date	Username	
64-bit (x86)	uefi-preferred	ami-07ff62358b87c7116	2026-01-02	ec2-user	Verified provider

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.

▼ **Instance type** [Info](#) | [Get advice](#)

Instance type

t3.micro Free tier eligible

Family: t3 2 vCPU 1 GiB Memory Current generation: true

On-Demand Ubuntu Pro base pricing: 0.0139 USD per Hour On-Demand SUSE base pricing: 0.0104 USD per Hour

On-Demand Linux base pricing: 0.0104 USD per Hour On-Demand RHEL base pricing: 0.0392 USD per Hour

On-Demand Windows base pricing: 0.0196 USD per Hour

[Additional costs apply for AMIs with pre-installed software](#)

☐ All generations [Compare instance types](#)

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

EC2 > Instances

Instances (2) [Info](#)

Last updated 7 minutes ago Connect Instance state Actions Launch instances

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

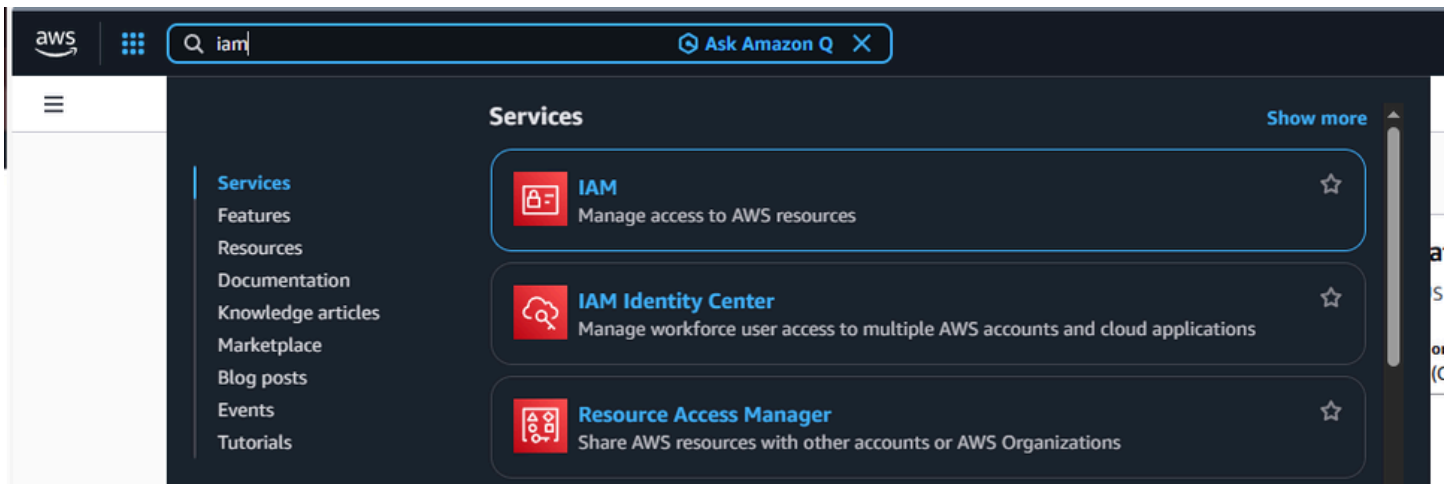
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input type="checkbox"/>	Cybertech-Audit	i-03c6bb9233f4075ee	Running	t3.micro	3/3 checks passed	View alarms	us-east-1c	ec2-54-196-148-24.co...	54.196.148.24	-
<input type="checkbox"/>	Cybertech-Sales	i-0bbd2e5de5fc8b6e9	Running	t3.micro	Initializing	View alarms	us-east-1c	ec2-54-221-188-144.co...	54.221.188.144	-

Creating an IAM Policy

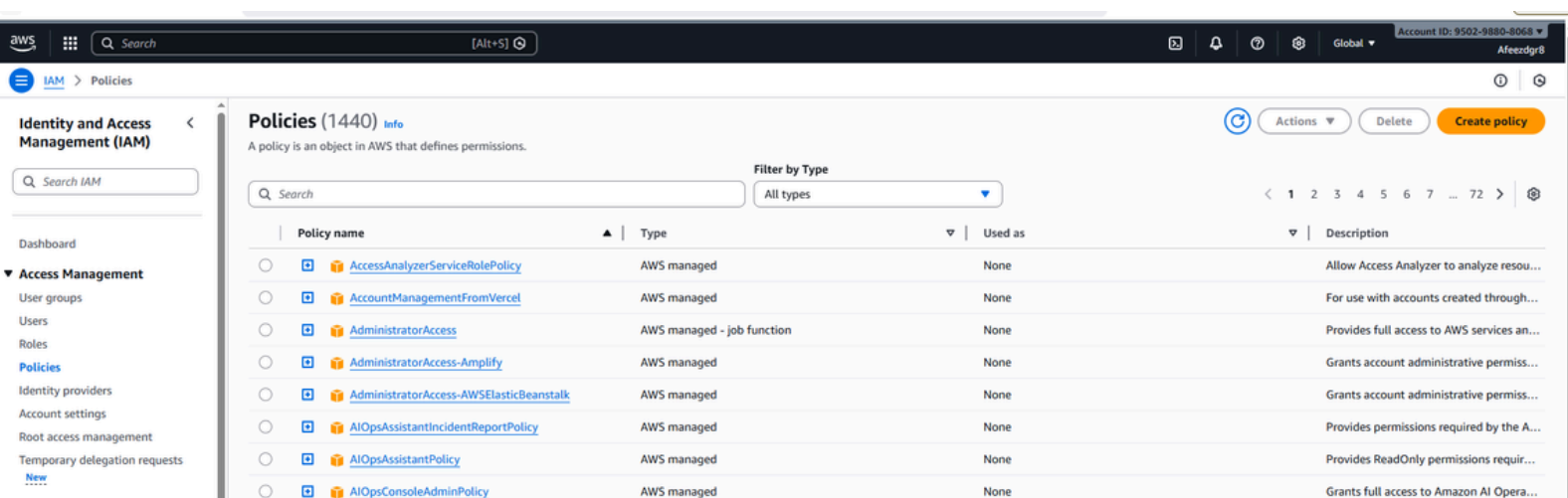
Moving on in the cloud security project, I want to create a policy.

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

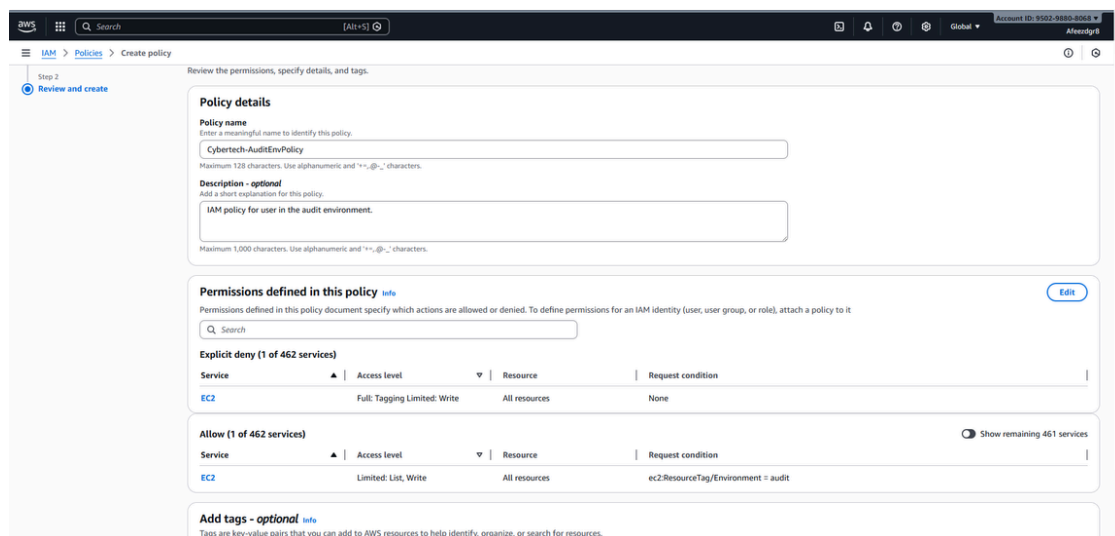
To do that, I will search for IAM in the search bar and select the first option.

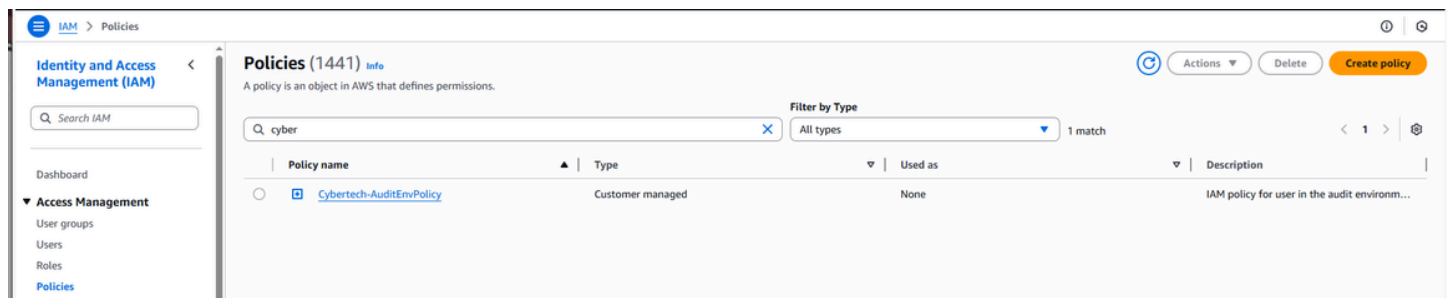


I navigate to policy and I click on “create policy” in order to create my own policy.



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

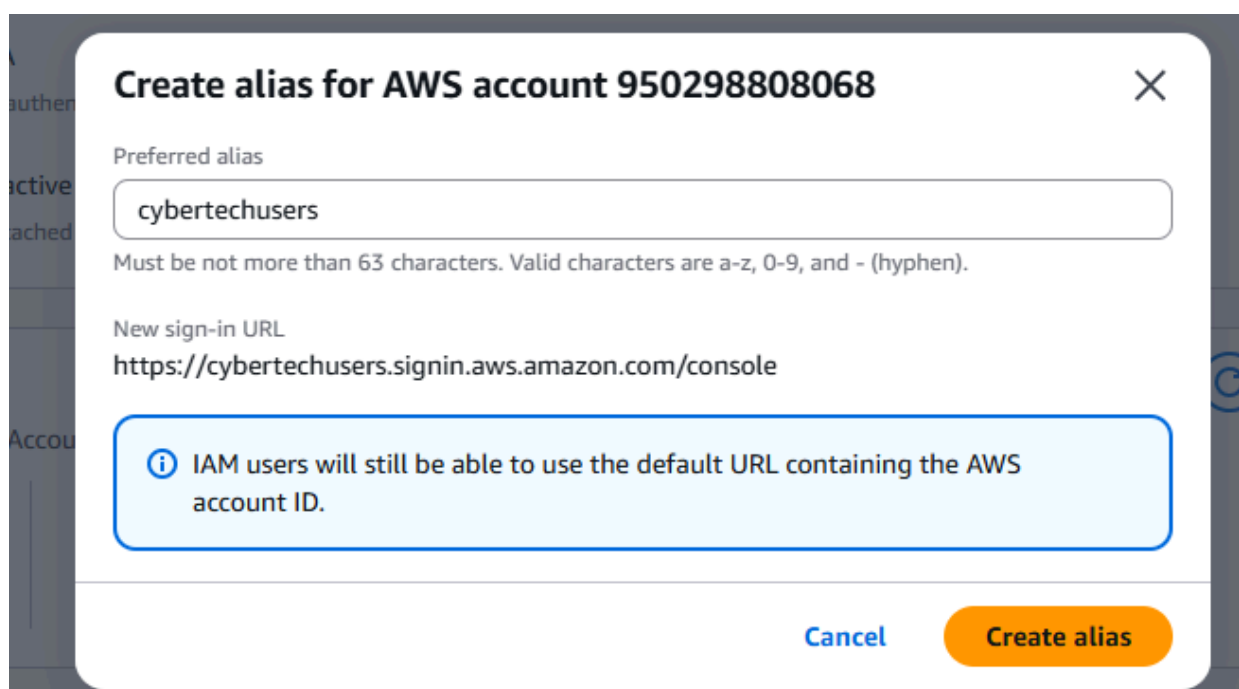
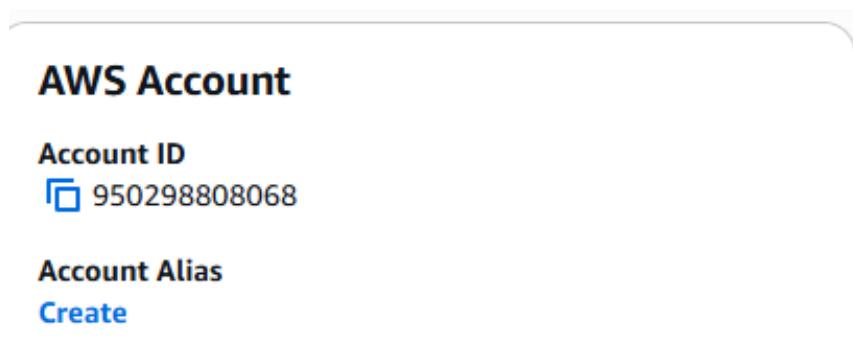




Creating an AW Alias

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.



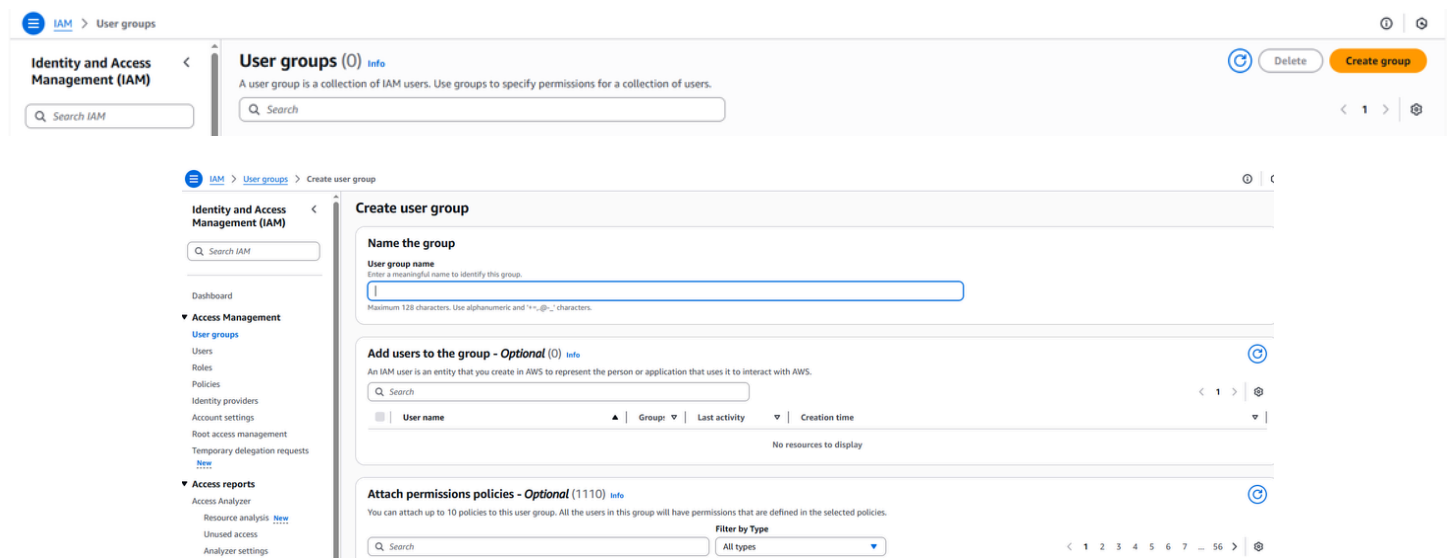
Creating IAM group & User

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

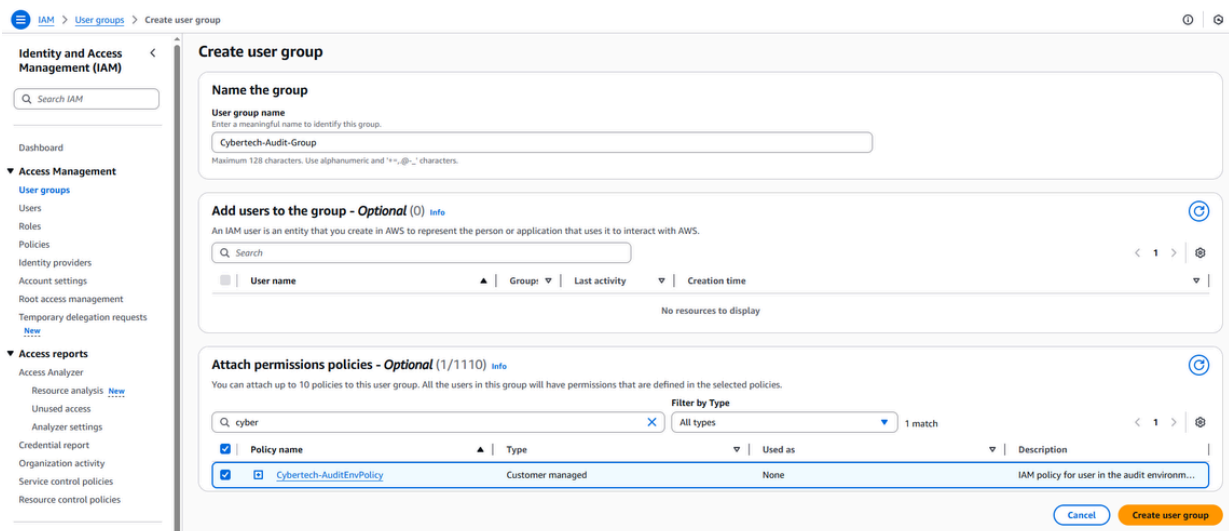
A group consist of different IAM users. The importance of creating a group is to make it easy when we want to apply a policy, it will affect all users in that group. Which makes it eaiser to assign policy to users.

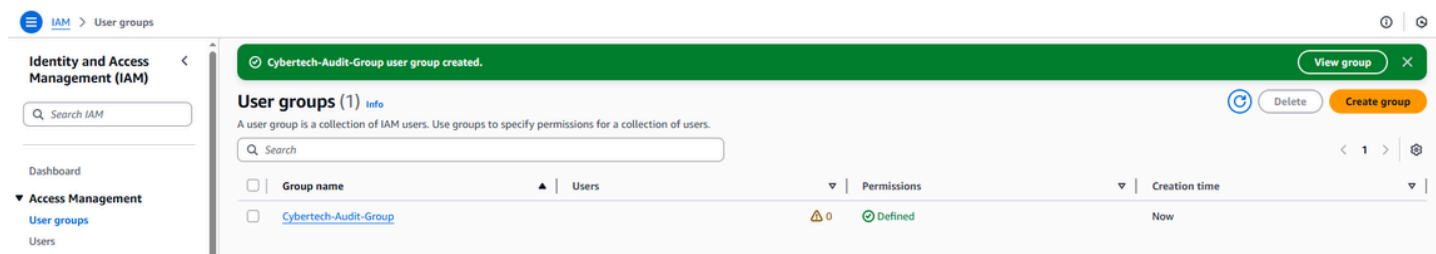
IAM user is a member of a group.

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

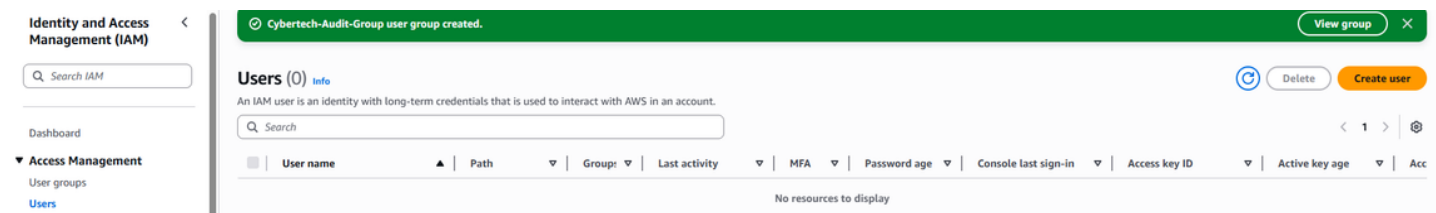


I gave my group a name and I attached the policy I previously created and I clicked on “create user group”.

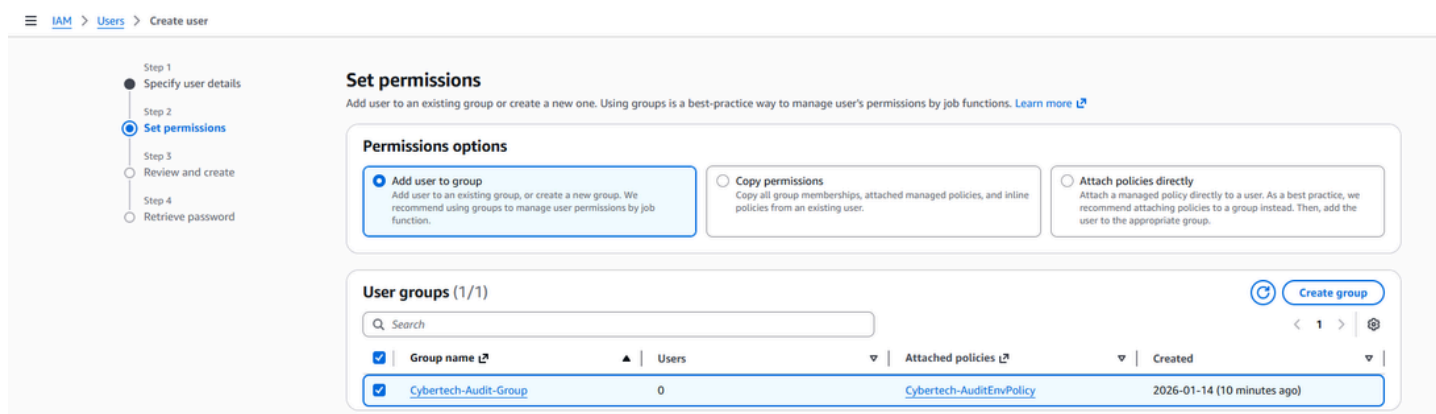




The next thing I want to do is to create user. In the same IAM tab, I clicked on “users”, then i clicked on create user.



I added the user to the group I previously created.



User created successfully and added to a group.

Identity and Access Management (IAM) > Users

Search IAM

Dashboard

Access Management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

[View user](#)

Users (1) [Info](#)

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

Search

<input type="checkbox"/>	User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age	Acc
<input type="checkbox"/>	Cybertech-Audit-Ali	/	1	-	-	1 minute	-	-	-	-

I signed in as the new user created.

aws

IAM user sign in ⓘ

Account ID or alias [\(Don't have?\)](#)

☐ Remember this account

IAM username

Password

☐ Show Password [Having trouble?](#)

[Sign in](#)

[Sign in using root user email](#)

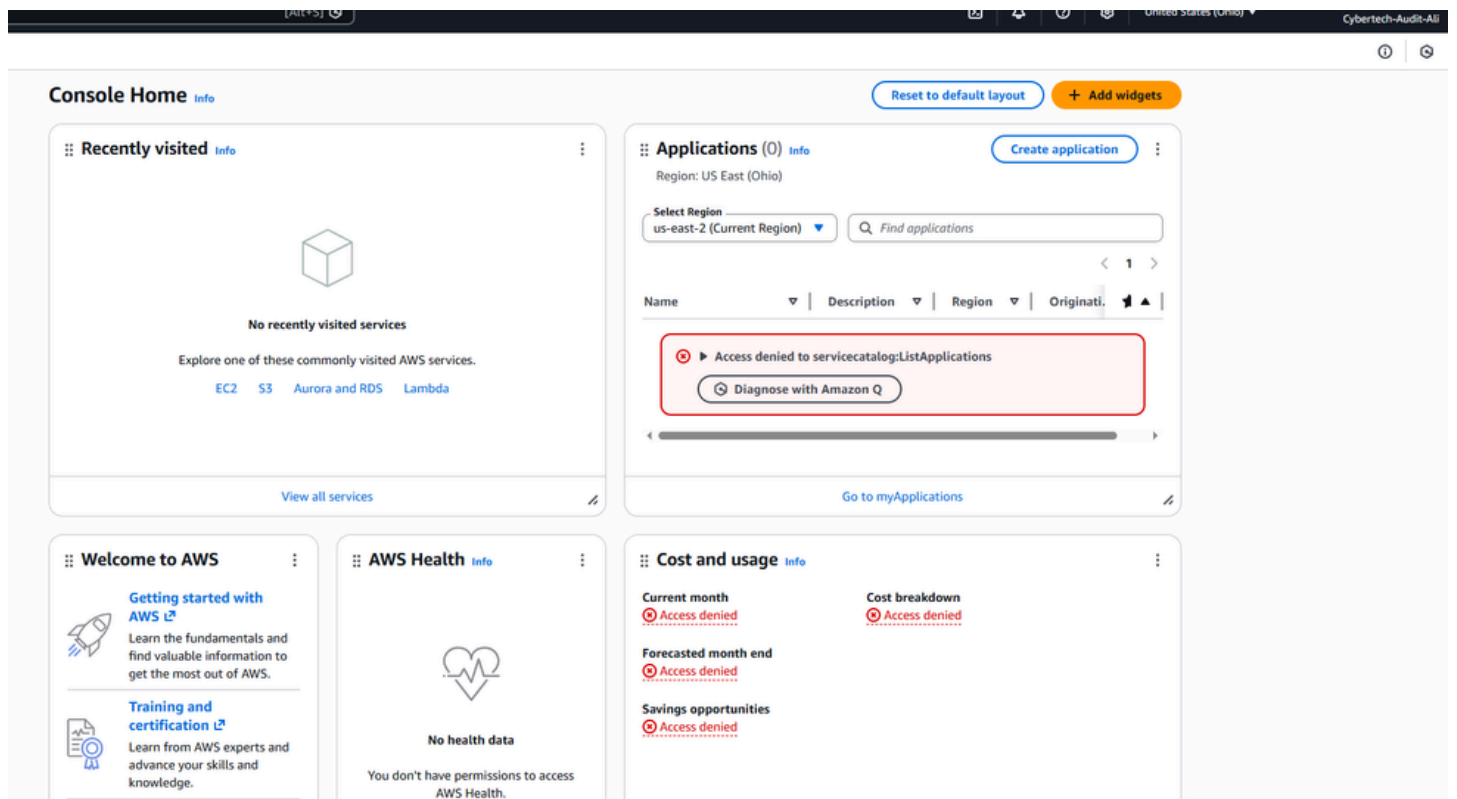
[Create a new AWS account](#)

By continuing, you agree to [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

Run models at scale with cost-effective chips

Our new AI chip, EC2 Trn3 UltraServer, delivers the best token economics for AI applications.

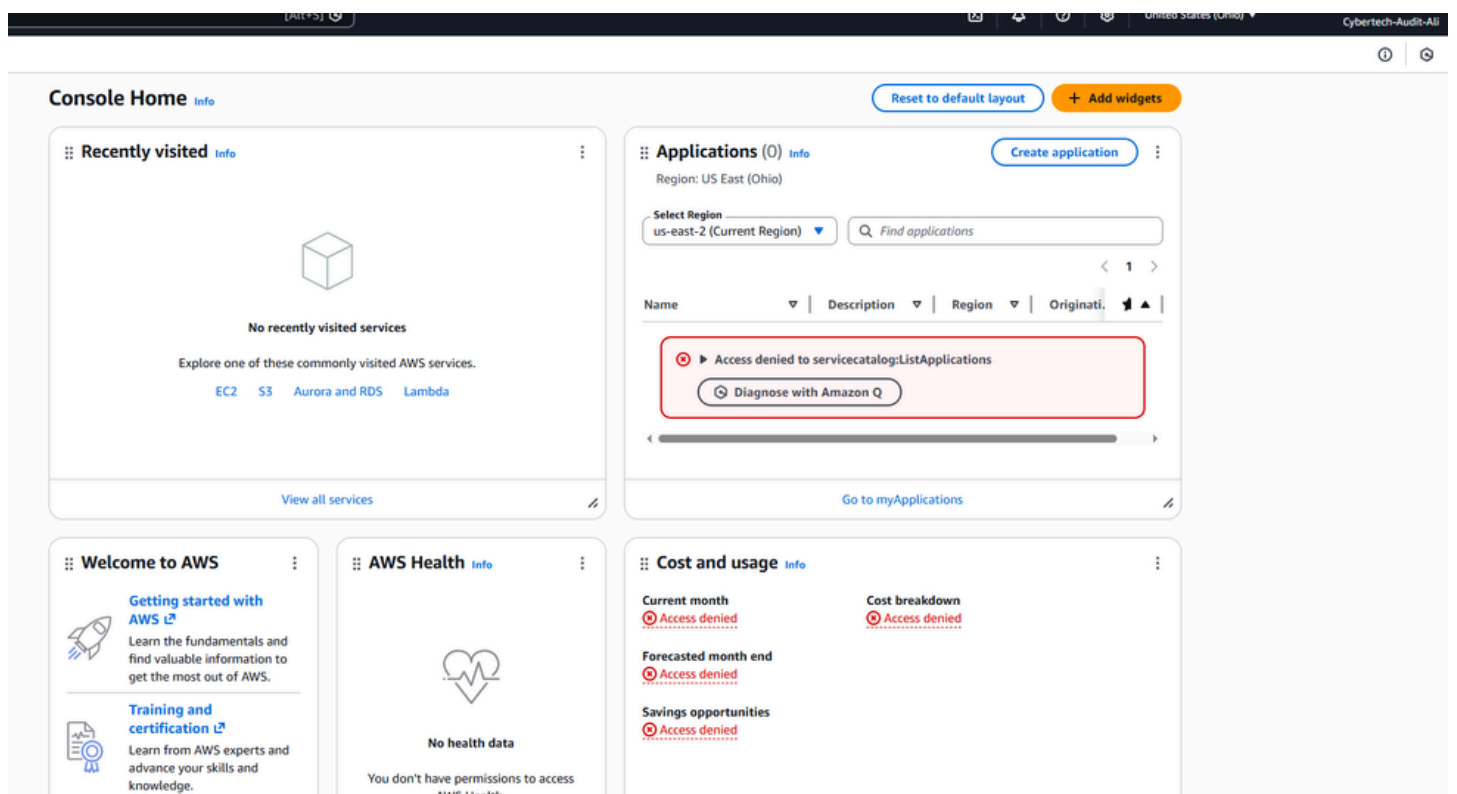
[Explore Trn3](#)



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

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.

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

[Additional information](#)