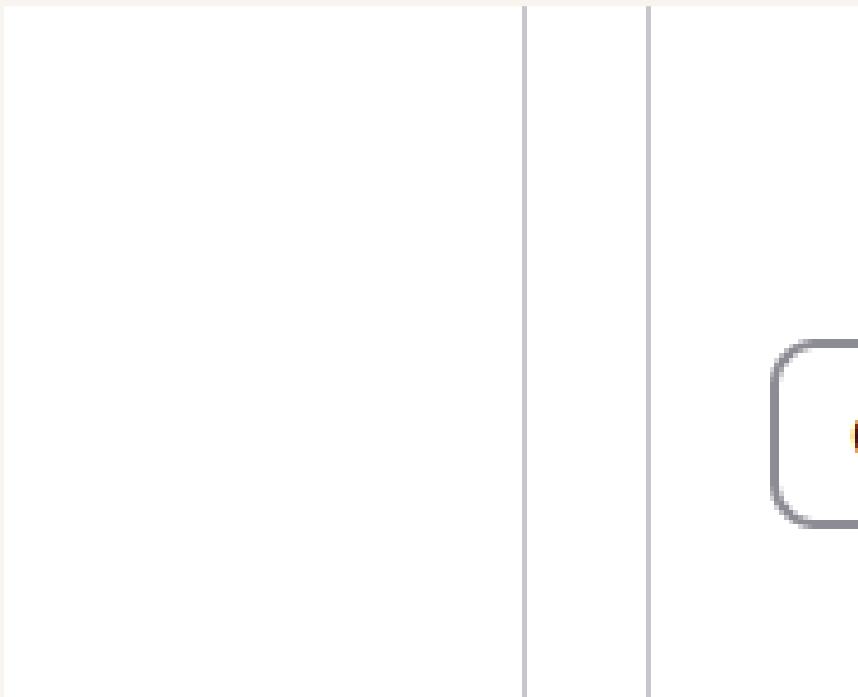


[nextwork.org](http://nextwork.org)

# Cloud Security with AWS IAM

LW

lwazi995@outlook.com



# Introducing today's project!

## What is AWS IAM?

AWS IAM are rules that help with Allow /Deny User/Resources permission to perform certain task/actions to my AWS Account.

## How I'm using AWS IAM in this project

I used AWS IAM to create two environments the development and production. We also created a group to assign new user as an intern, they were sent a link to their account with certain privileges restricted through my AWS Account

## One thing I didn't expect...

I didn't expect the development environment to allow the intern to be able to stop it completely. It came as a shock, nonetheless everything else was straight forward.

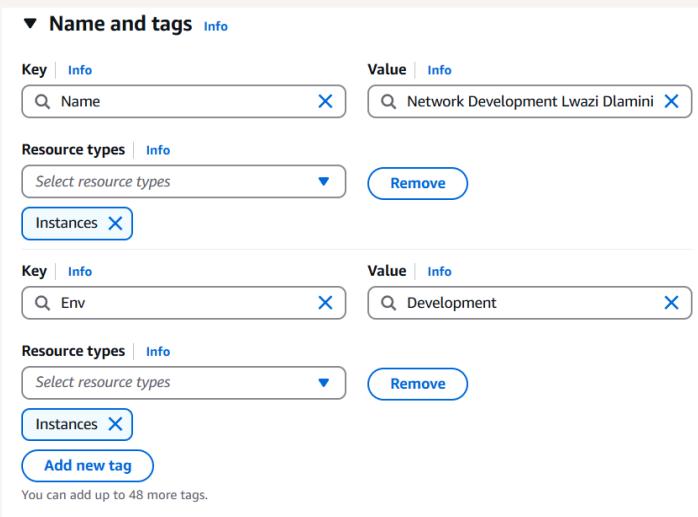
## This project took me...

It took me 2 hours.

# Tags

Tags are labels to help AWS Account users identify and manage their resources. The tags I've used on my EC2 is ENV. The value assigned for the instance production and development. This is the two environments that we building to release Nextwork app

The tag I've used on my EC2 instances is called ENV. The value I've assigned for my instance are production, and development.



# IAM Policies

IAM policies are rules that help to allow/deny users'/resources permissions to perform certain actions to my aws account resources.

## The policy I set up

For this project I've set up a policy using the JSON Editor I've created a policy that allows all EC2-related actions to all EC2 instances that have the environment ("Env")tag "development" but it also denies creating or deleting all EC2 instances

I've created a policy that allows all EC2 related actions to all EC3 instances that have the Environment ("Env")tag "development" and deleting tags for all EC2 instances

## When creating a JSON policy, you have to define its Effect, Action and Resource.

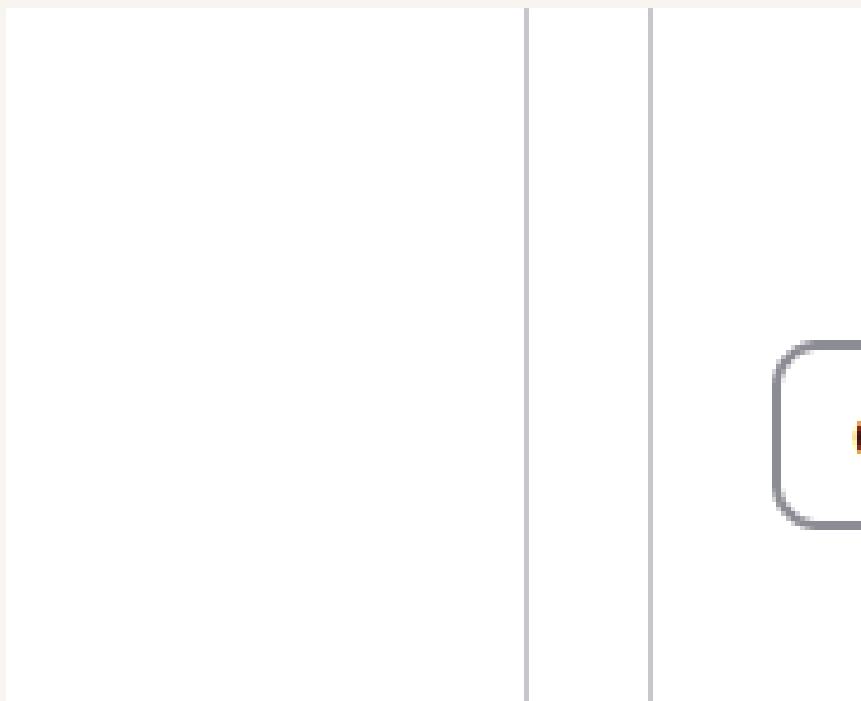
When writing JSON policy statements you have to specify the: 1. Effect i.e. Allow or Deny. 2. Action i.e. the specific action that we want to Allow or Deny. 3.Resource i.e. the specific/resource in my AWS account that this policy will take effect

LW

Iwazi995@outlook.com  
NextWork Student

NextWork.org

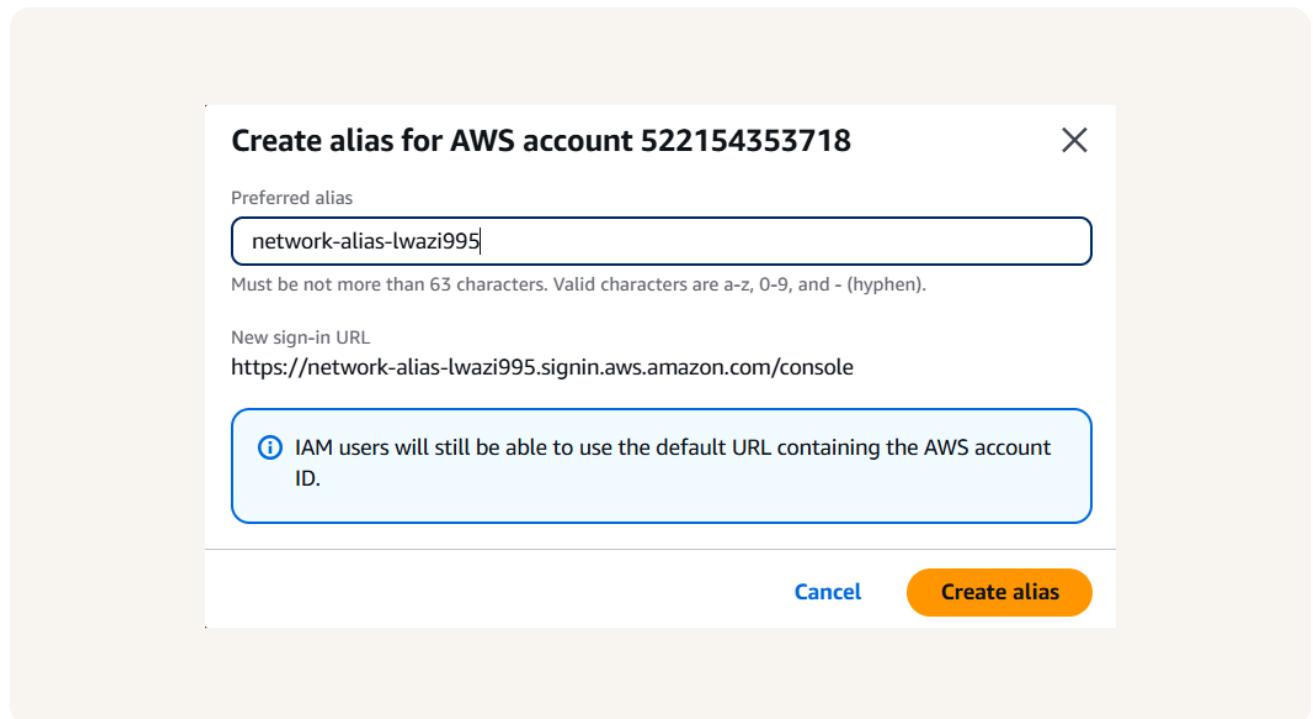
# My JSON Policy



# Account Alias

An account alias is a custom name that I can assign to my AWS Account. This custom name would replace my Account ID in my Account's log-in URL.

Creating an account alias took me less than a minute - Super quick flash! Now, my new AWS console sign-in URL is <https://network-alias-Iwazi995.signin.aws.amazon.com/console>



# IAM Users and User Groups

## Users

IAM users are other people who have access to my AWS Account these are created by myself using the AWS IAM service! I can designate my IAM user access to my AWS Accounts resources/services.

## User Groups

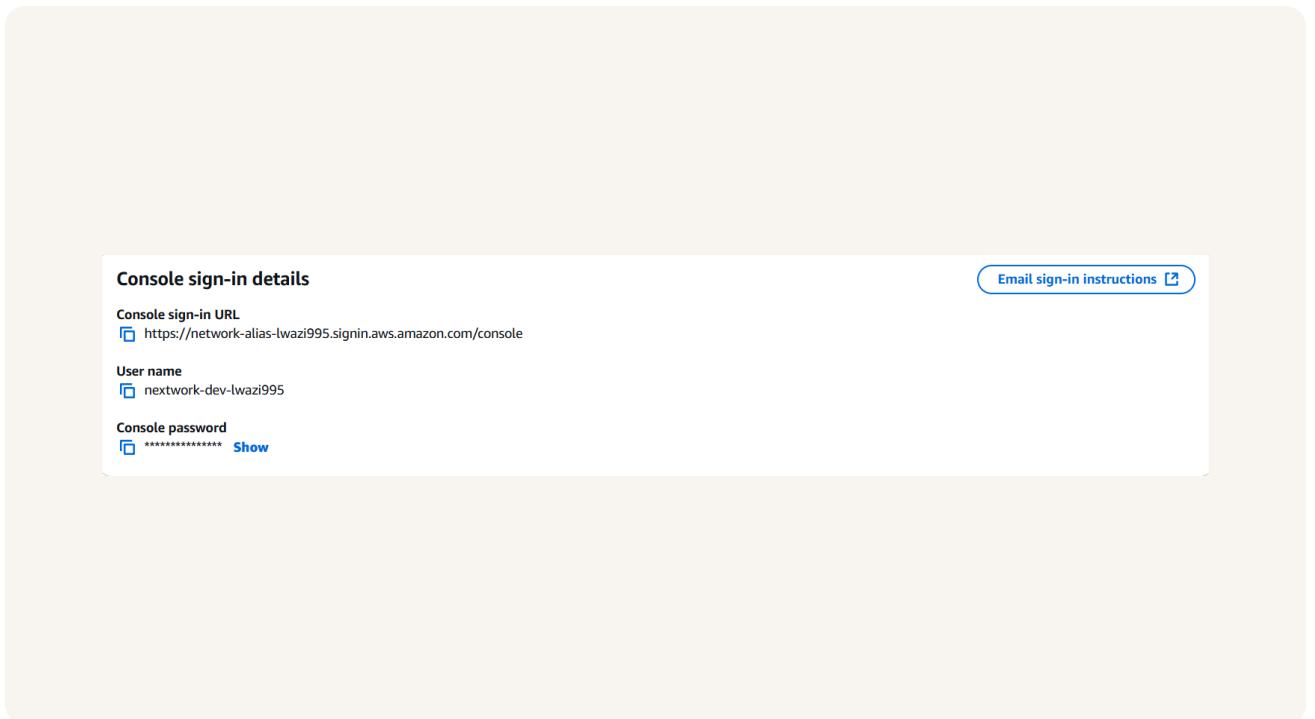
I AM Users are other log-ins/people who have access to my AWS account and these users are created by myself using the AWS IAM service! I can designate my users access to my AWS Account resources/services.

My user group is called nextwork-dev-group. I attached the Policy I created to this User Group, which means all users that are added to that user group will automatically inherit the user group's access permissions.

# Logging in as an IAM User

The first way is all the users that are added to the user group will automatically inherit the user groups access permissions. The second way is they will get a link sent to them and they will have access to that account in the group as an intern.

Once I logged in as my IAM user, I noticed that a lot of panels displayed access denied this was a clear difference to the dashboard that I usually see in my AWS Account where I wasn't denied any access.



# Testing IAM Policies

I tested my JSON IAM policy by to stop the development and production instances i.e. triggering the stop instance action.

## Stopping the production instance

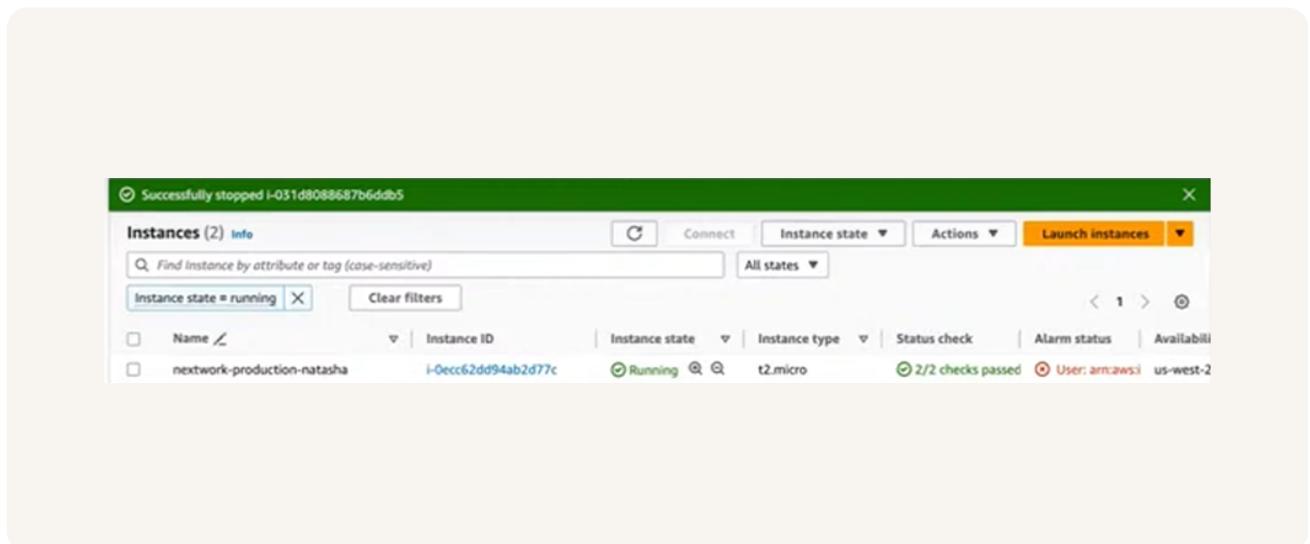
When I tried to stop the production instance I came accross a message stating that I am not authorized to commence with this action. Stopping the production incident.



# Testing IAM Policies

## Stopping the development instance

Next when I tried to stop the development instance it could be stopped this was because the policy I created and attached to the User group allowed all EC2 related actions to all EC2 instances/resources with the Env tag development





NextWork.org

# Everyone should be in a job they love.

Check out nextwork.org for  
more projects

