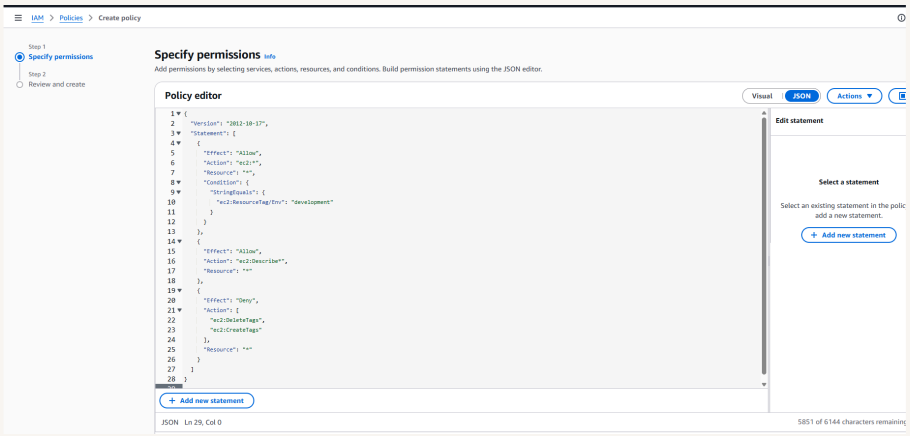
nextwork.org

Cloud Security with AWS IAM

Kiprono Yegon



Introducing Today's Project!

In this project, I will demonstrate using AWS IAM to control access to AWS services to specific users. I'm doing this project to learn more about cloud security and best practices if the cloud.

Tools and concepts

Services I used were Amazon EC2 and Amazon IAM. Key concepts I learnt include IAM users, policies, user groups and account aliases. I pearned how JSON policies worked.

Project reflection

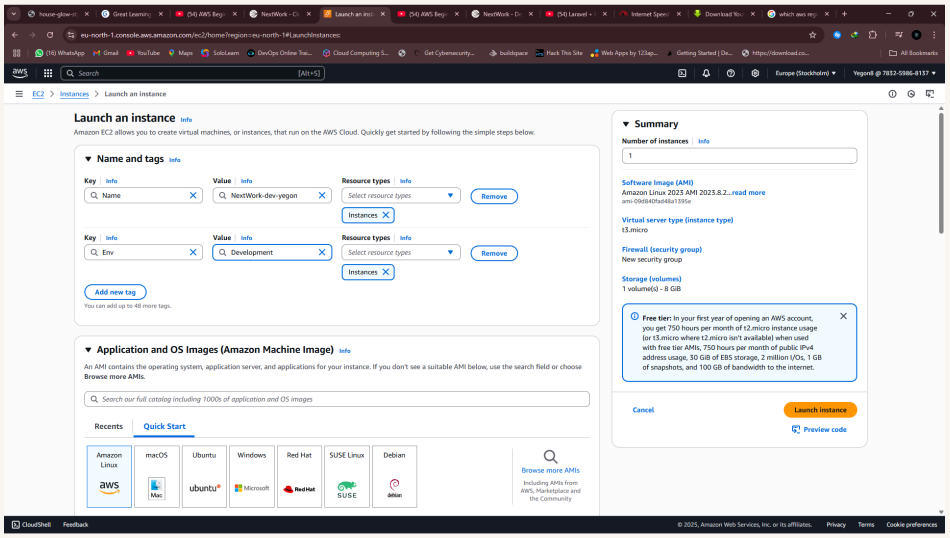
This project took me approximately one and a half hour to complete.The most challenging part was attaching policies. It was most rewarding to finally create instances and to delete them

Kiprono Yegon
NextWork Student

Tags

Tags are labels you attach to AWS resources for organization. I used the tag "Env" to label the production and development resources.

The tag I've used on my EC2 instances is called Environment (Env). The value I've assigned for my instances are development and production.



Kiprono Yegon
NextWork Student

IAM Policies

IAM Policies are rules for who can do what with given AWS resources. It gives permissions to IAM users, groups and roles and specify what changes they can do to specific AWS resources.

The policy I set up

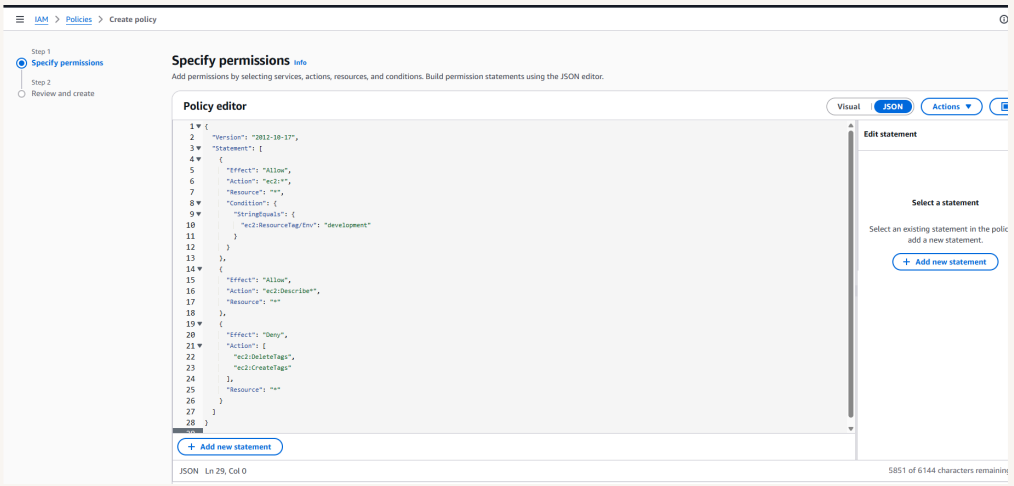
For this project, I've set up a policy using the JSON method.

I've created a policy that allows all actions on the EC2 instances

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

The Effect, Action, and Resource attributes of a JSON policy means; that the Effect can deny or allow a certain action and the action defines the list of actions that the policy allows or denies and the resource shows which resource the policy apply.

My JSON Policy

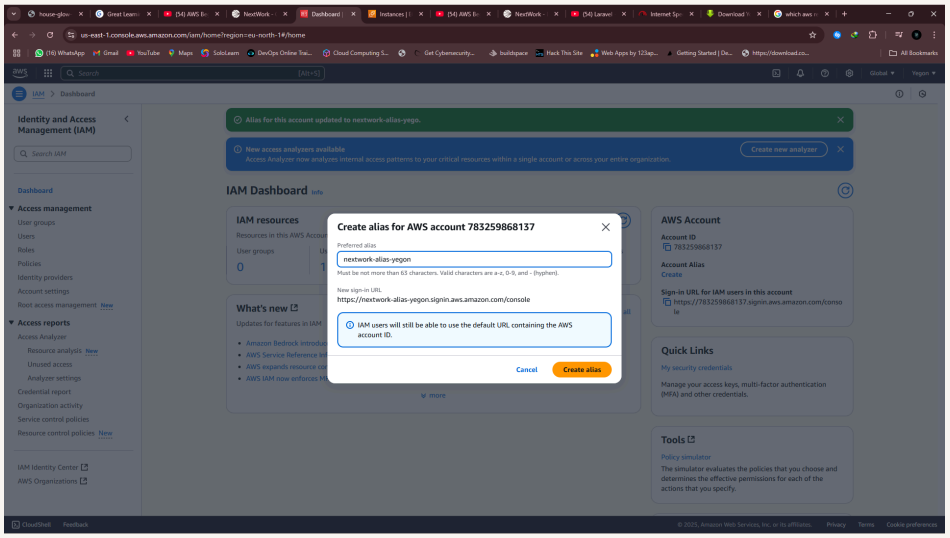


Kiprono Yegon
NextWork Student

Account Alias

An account alias is a unique user friendly name that you use for an account instead of the account ID to sign in to the AWS Management Console.

Creating an account alias took me less than two minutes. Now, my new AWS console sign-in URL is https://nextwork-alias-yegon.signin.aws.amazon.com/console



Kiprono Yegon
NextWork Student

IAM Users and User Groups

Users

IAM users are the people or accounts that will get to use the AWS resources that are specified. Users are given permissions to access the resources mentioned in the policy.

User Groups

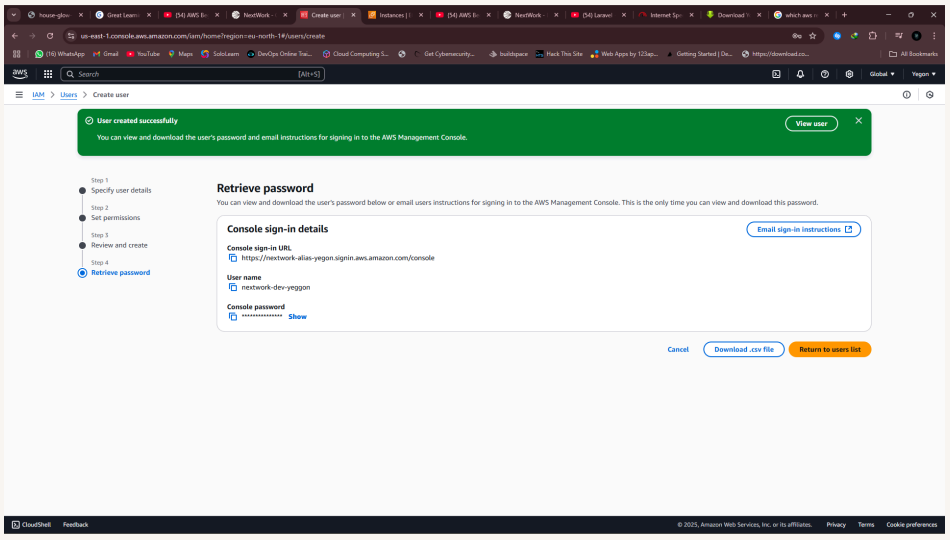
IAM user groups are colllection of IAM users that have the same permisiions to perform specific tasks to given resources.

I attached the policy I created to this user group, which means that the users in that group are given permissions by the policy on the resources they will work with

Logging in as an IAM User

The first way to share a user's sign in details is by downloading the csv file and sharing it with the new user or by emailing the sign in instructions to the user.

Once I logged in as my IAM user, I noticed that some of the dashboard panels are showing access deniedThis was because of the IAM policy that we gave to the user group that the user is in.

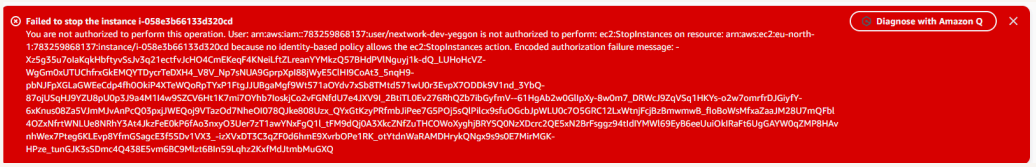


Testing IAM Policies

I tested my JSON IAM policy by trying to stop the two EC2 instances. The JSON IAM policy only allows the stopping of one EC2 instance policy; the development instance.

Stopping the production instance

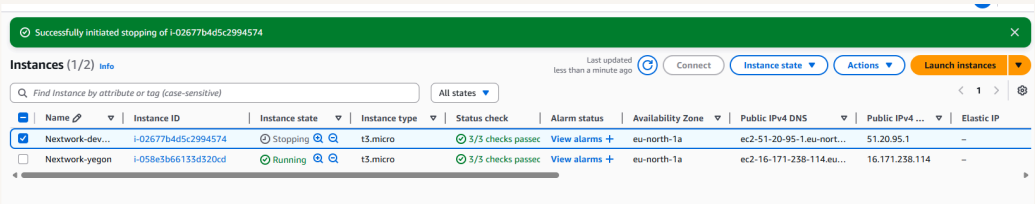
When I tried to stop the production instance there was a red banner that showed an error.This was because the intern does not have access to the production instance as stated in the IAM policy.



Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance it stopped. This was because the intern has access to manipulate the development instance according to the JSON IAM policy



The place to learn & showcase your skills

Check out nextwork.org for more projects