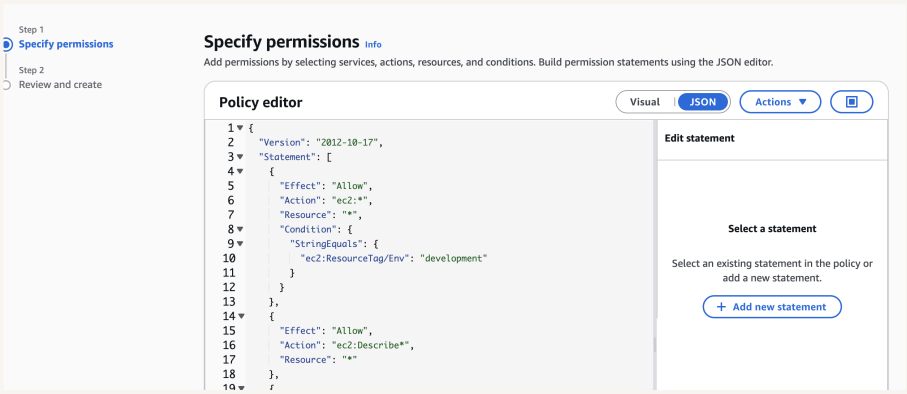
nextwork.org

Cloud Security with AWS IAM

Kehinde Abiuwa



Kehinde Abiuwa
NextWork Student

Introducing Today's Project!

In this project, I will demonstrate how to create EC2 instances, IAM Policies, IAM Users and User Groups, AWS Account Alias. I'm doing this project to learn Cloud Security with AWS IAM

Tools and concepts

Services I used were EC2 and IAM... Key concepts I learnt include launching ec2 instances, setting permissions on the instances, creating user policies and groups, creating a new IAM user and adding the user to the policy to test the permisions set for the ec2 instances

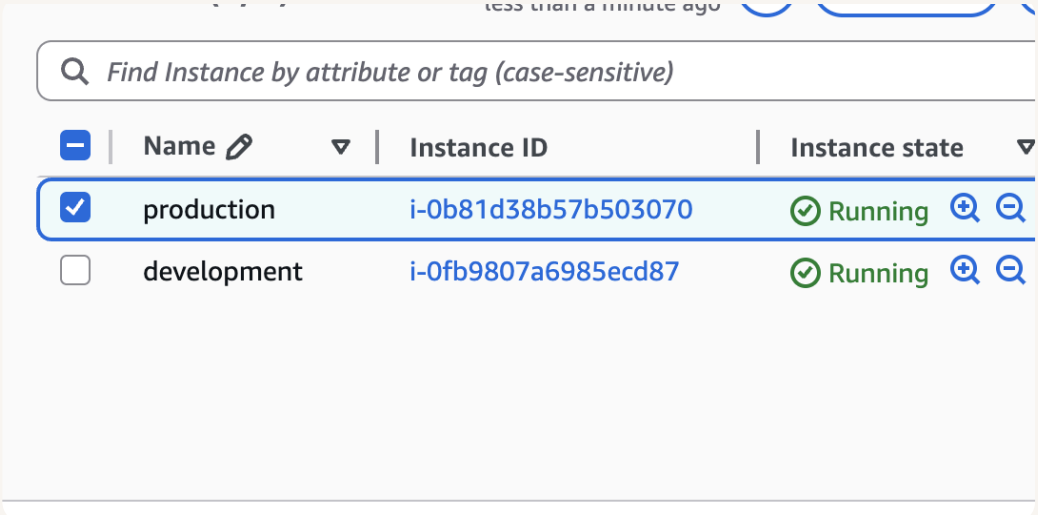
Project reflection

This project took me approximately 15minis

Tags

Tags are usefull for identifying all resources with the same tag at once

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



Kehinde Abiuwa
NextWork Student

IAM Policies

IAM Policies are are rules for who can do what within the aws resources

The policy I set up

For this project, I've set up a policy using the JSON in the IAM resource

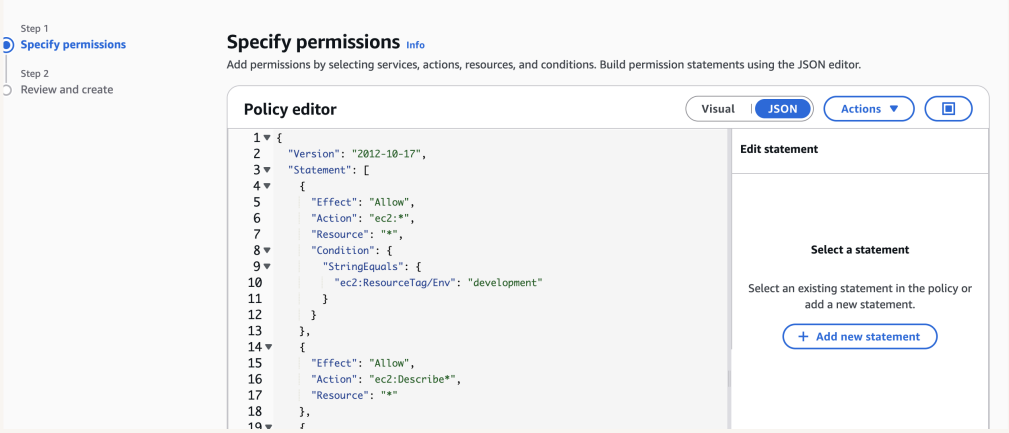
I've created a policy that allows some actions (like starting, stopping, and describing EC2 instances) for instances tagged with "Env = development" while denying the ability to create or delete tags for all instances

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

Effect This can have two values - either Allow or Deny - to indicate whether the policy allows or denies a certain action. Deny has priority. Looking at the first statement, "Effect": "Allow" means this statement is trying to allow for an action. Action A list of the actions that the policy allows or denies. In this case, "Action": "ec2:*" means all actions that you could possibly take on EC2 instances are allowed Resource Which resources does this policy apply to? Specifying "*" means all resources within the defined scope

Kehinde Abiuwa
NextWork Student

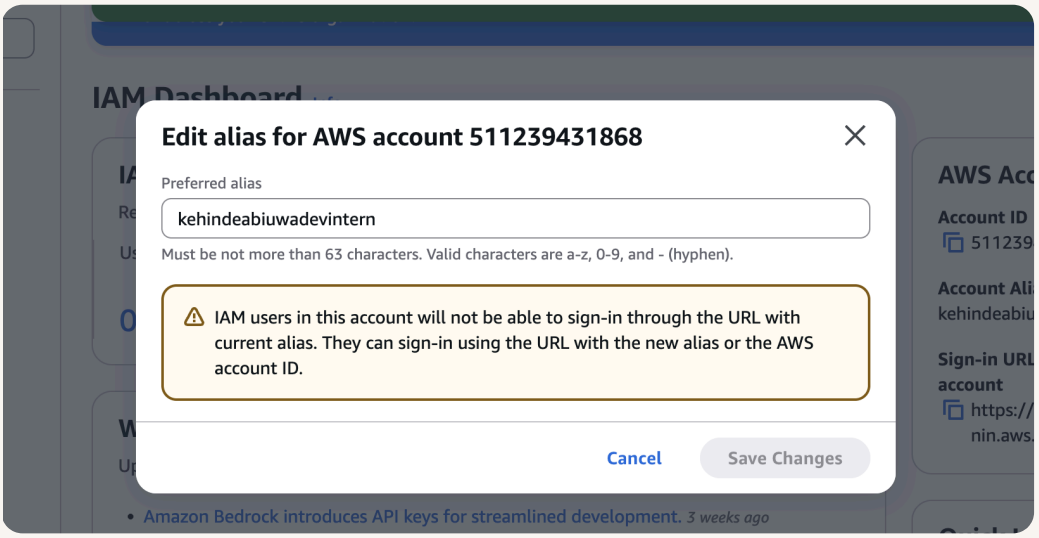
My JSON Policy



Account Alias

An Account Alias is a friendly name for your AWS account that you can use instead of your account ID to sign in to the AWS Management Console.

Creating an account alias took me 8mins Now, my new AWS console sign-in URL is https://kehindeabiuwadevintern.signin.aws.amazon.com/console



K
Kehinde Abiuwa
NextWork Student

IAM Users and User Groups

Users

IAM users are credentials given to other people to login to the AWS resources

User Groups

IAM user groups are groups used to manage permissions of a group of people from one place

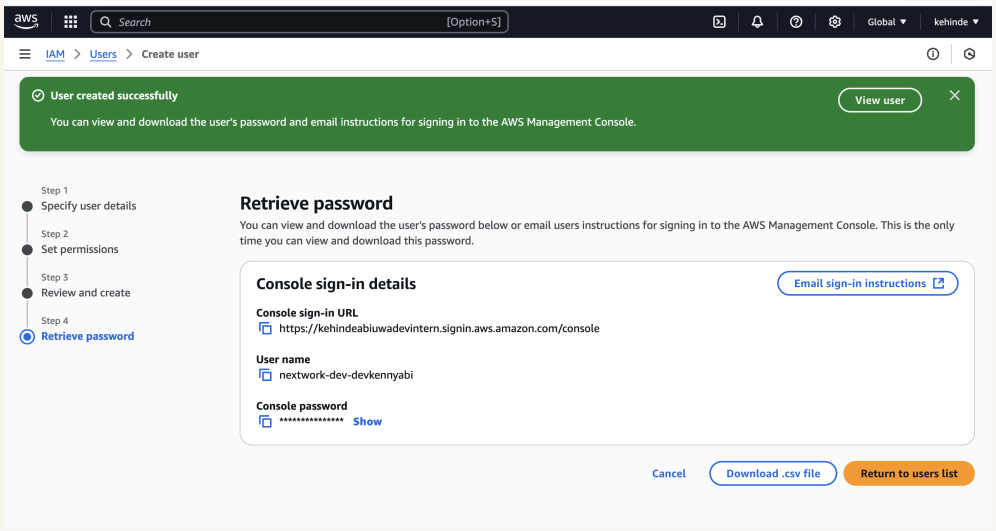
I attached the policy I created to this user group, which means that all the users in this group only have access to the development instace and not the production instance as the group is meant for our interns

Kehinde Abiuwa
NextWork Student

Logging in as an IAM User

The first way is email sign in notification, and the second is to download a .csv file

Once I logged in as my IAM user, I noticed that some of your dashboard panels are showing Access denied. This was because this IAM user is in the usergroup i created that is blocked from accessing the production instance



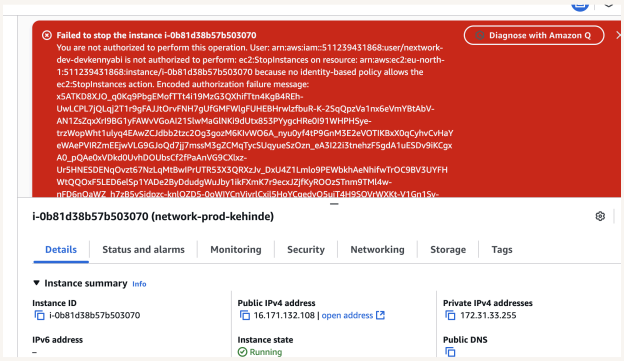
Kehinde Abiuwa
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by user the IAM user i added to my policy group to stop the dev instance and it stopped, I also tried to stop the production instance which rightfully returned an error.

Stopping the production instance

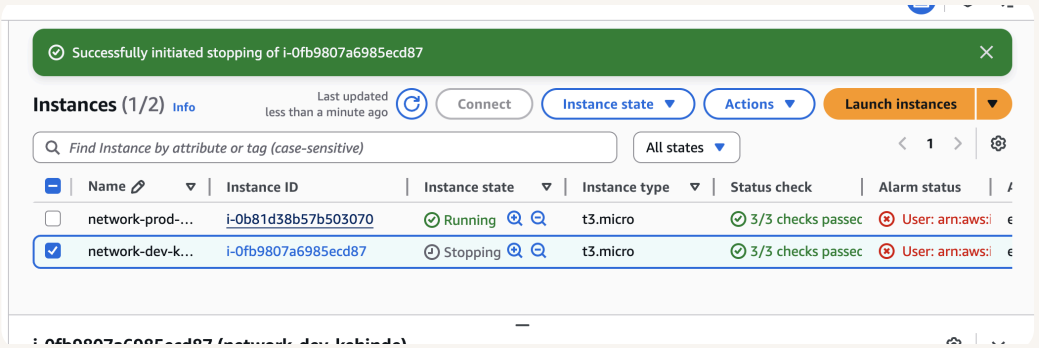
When I tried to stop the production instance I got an error message. This was because I dont have permission as this IAM user to stop the production instance



Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance it stopped because I have the permission to stop it



The place to learn & showcase your skills

Check out nextwork.org for more projects