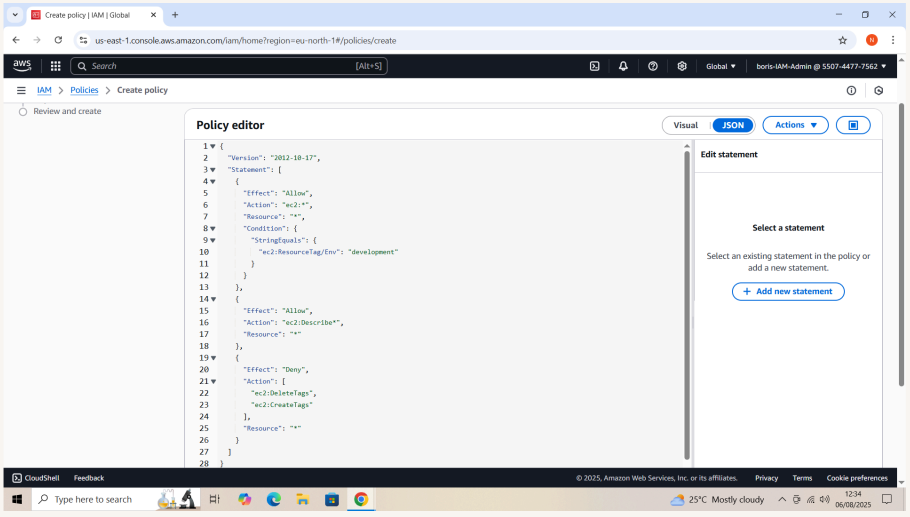
nextwork.org

Cloud Security with AWS IAM

Nchindo Boris



Nchindo Boris
NextWork Student

Introducing Today's Project!

Today, we'll be using the AWS Identity and Access Management (IAM) service to control who is authenticated (signed in) and authorized (has permissions) in your AWS account. We'll launch an EC2 instance, then control who has access to it

Tools and concepts

Services I used were; - EC2 - IAM and policy Key concepts I learnt include; - JSON policy for IAM users - Account Alias creation

Project reflection

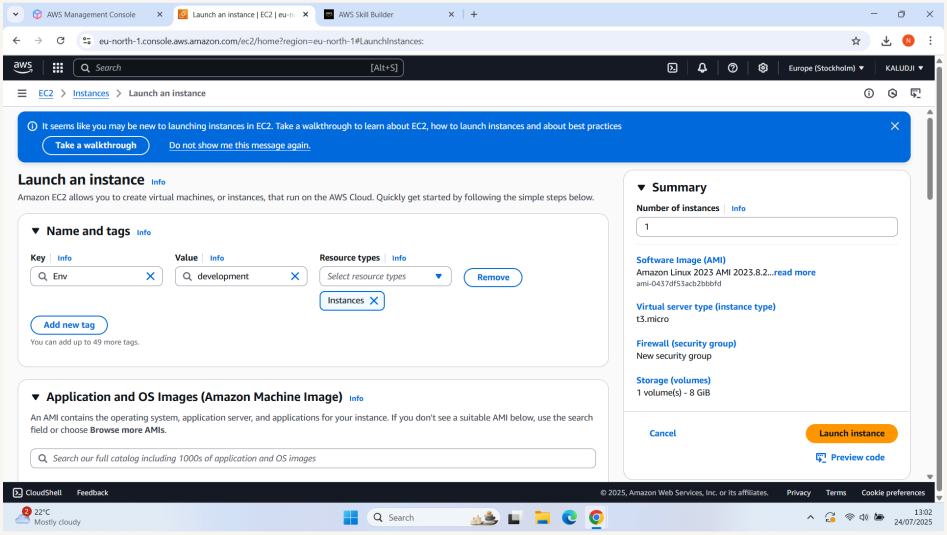
This project took me approximately 1hr 30mins. The most challenging part was to enfoce the security policies correctly. It was most rewarding to see the policies work effectively

Nchindo Boris
NextWork Student

Tags

Tags are like labels you can attach to AWS resources for organization. This tagging helps us with identifying all resources with the same tag at once

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



IAM Policies

IAM Policies are rules for who can do what with your AWS resources. It's all about giving permissions to IAM users, groups, or roles, saying what they can or can't do on certain resources, and when those rules kick in.

The policy I set up

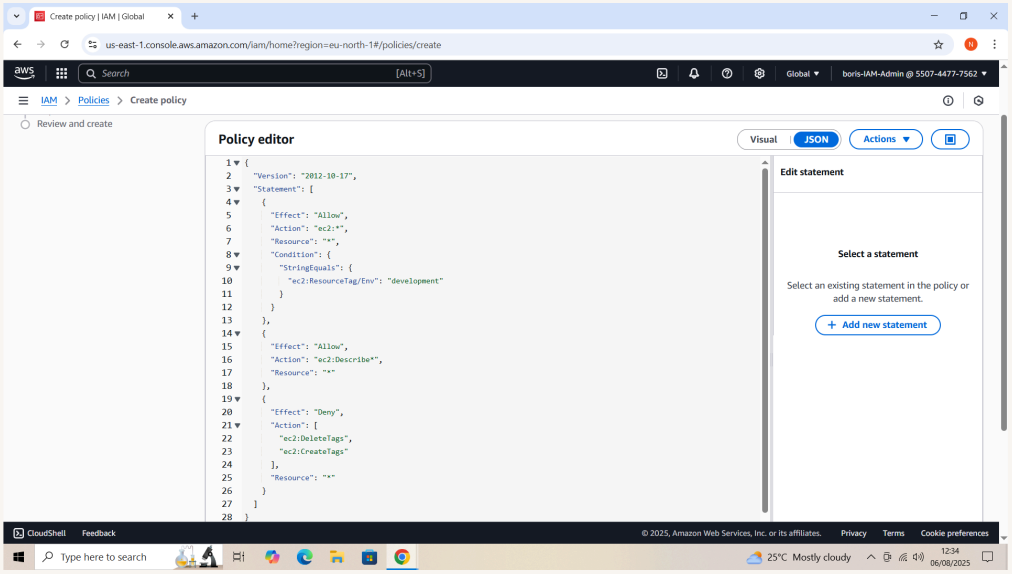
For this project, I've set up a policy using JSON

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.

The Effect, Action, and Resource attributes of a JSON policy mean; Effect = either Allow or Deny Action = A list of the actions that the policy allows or denies. Resource = Specifying "*" means all resources within the defined scope

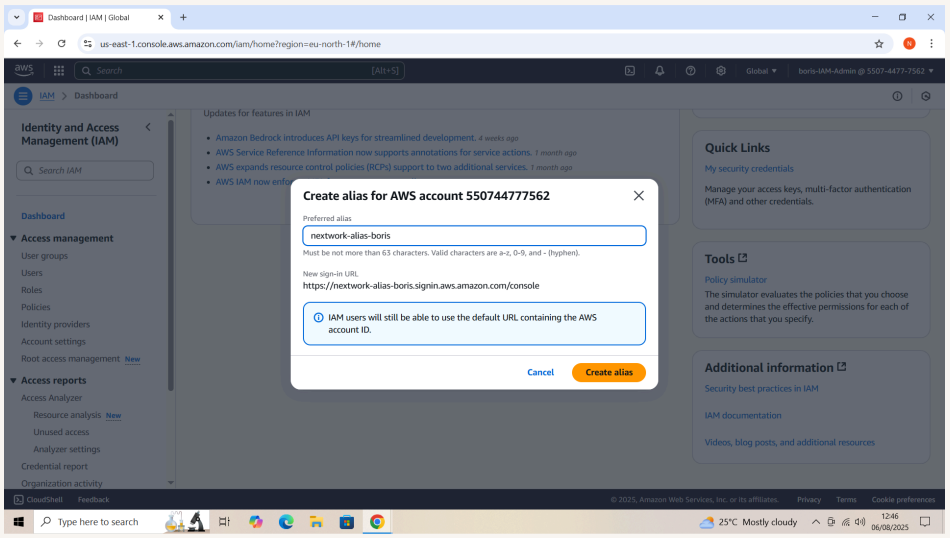
My JSON Policy



Account Alias

An account alias is a friendly name for your AWS account that you can use instead of your account ID (which is usually a bunch of digits) to sign in to the AWS Management Console.

Creating an account alias took me a minute. Now, my new AWS console sign-in URL is https://nextwork-alias-boris.signin.aws.amazon.com/console



Nchindo Boris
NextWork Student

IAM Users and User Groups

Users

IAM users are the people that will get access to your resources/AWS account

User Groups

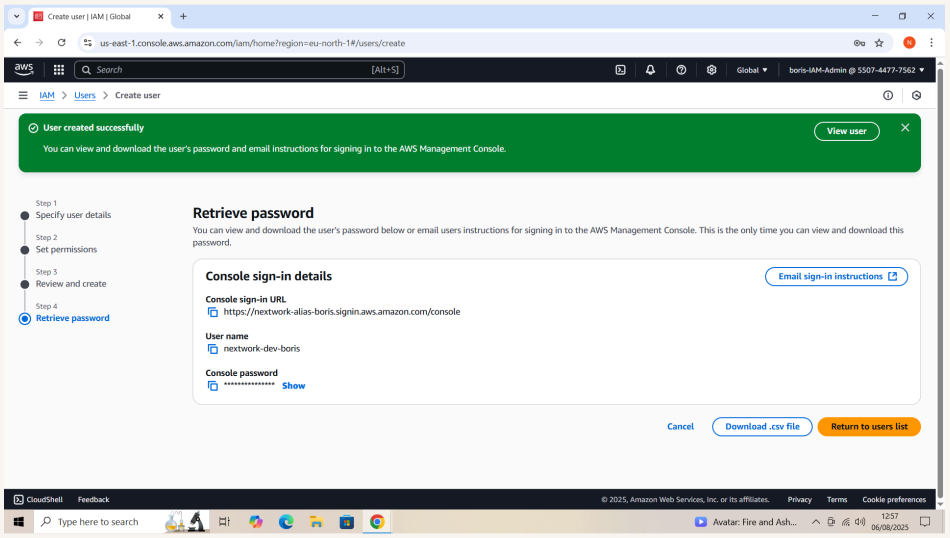
IAM user groups are collections/folders of IAM users. They allow me to manage permissions for all the users in my group at the same time by attaching policies to the group rather than individual users

I attached the policy I created to this user group, which means simplifying the management of permissions and ensures consistency across users who have similar access to AWS resources.

Logging in as an IAM User

The first way is to download the Credentials (.csv File) and manually send them. The second way is to email the sign-in instructions

Once I logged in as my IAM user, I noticed that some of my dashboard panels are showing Access denied already.



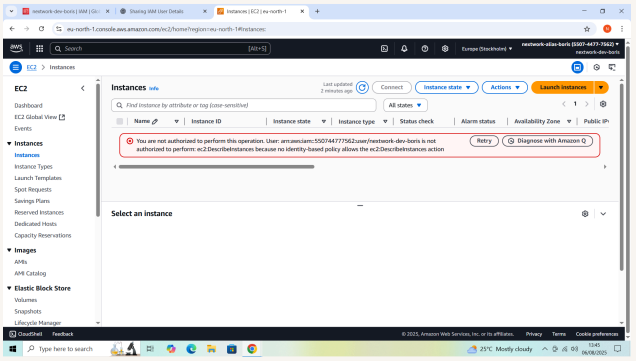
Nchindo Boris
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by trying to stop the EC2 Instances

Stopping the production instance

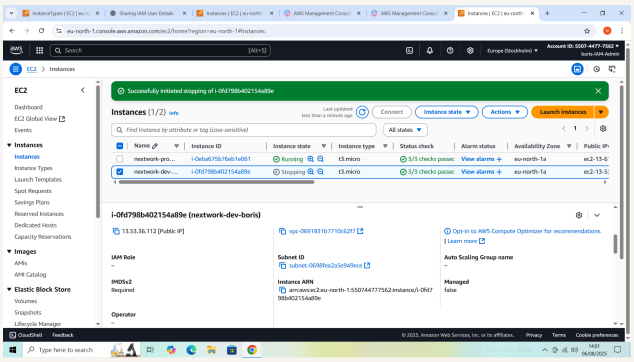
When I tried to stop the production instance I got an error message because this user is not authorized to perform this operation.



Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance it stopped. This was because the JSON policy allowed permission for that



The place to learn & showcase your skills

Check out nextwork.org for more projects