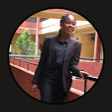
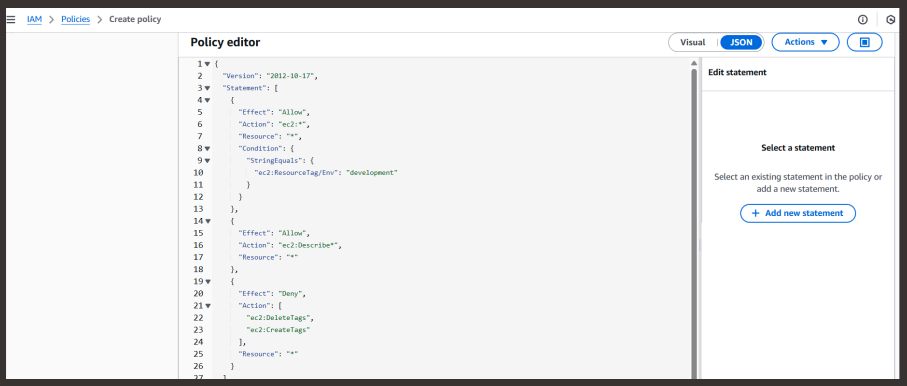
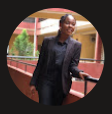
nextwork.org

Cloud Security with AWS IAM



Joba Amunigun
https://www.linkedin.com/in/dvoice




Joba Amunigun
NextWork Student

Introducing Today's Project!

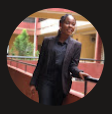
In this project, I will demonstrate how to use AWS Identity and Access Management (IAM) service to control who is authenticated (signed in) and authorized (has permissions) in my AWS account by creating some IAM policies and user groups . I'm doing this project to learn about cloud security from absolute foundations - every company thinks about access permissions- and there are even entire JOBS called IAM Engineers' focused on the skills i am about to build today :o

Tools and concepts

Services I used were Amazon EC2 and AWS IAM . Key concepts I learnt includes IAM users,policies,user groups and account aliases . I also learnt how to use Policy Simulator and how JSON policies work. How to launch Instances ,how to tag an instance and how to login as another user

Project reflection

This project took me approximately 2hours including Demo time .The most challenging part using the IAM Policy Simulator to test user access .It was most rewarding to see permission denied when the intern tried to delete the production instance - IAM access management was working

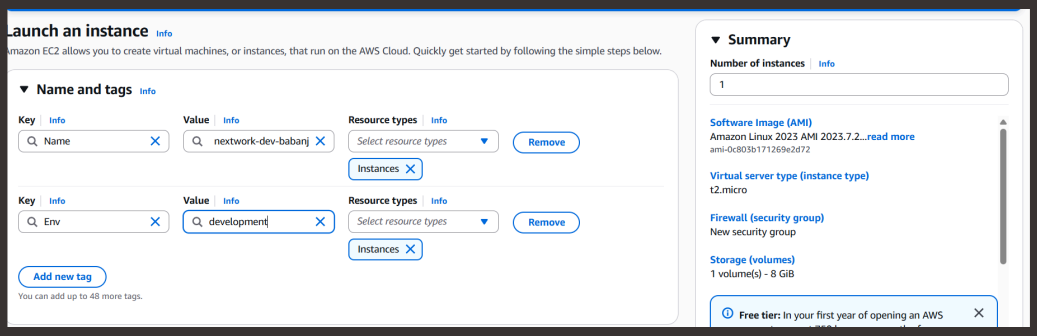


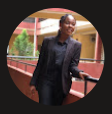
Joba Amunigun
NextWork Student

Tags

Tags are organisational tools that helps us label our resources. They are helpful for resources ,cost allocation and applying policies for all resources with the same tag

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




Joba Amunigun
NextWork Student

IAM Policies

IAM Policies are like rules that determines who can do what in our AWS account.I will be using policies today to control who can have access to the production /enviroment instance.

The policy I set up

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

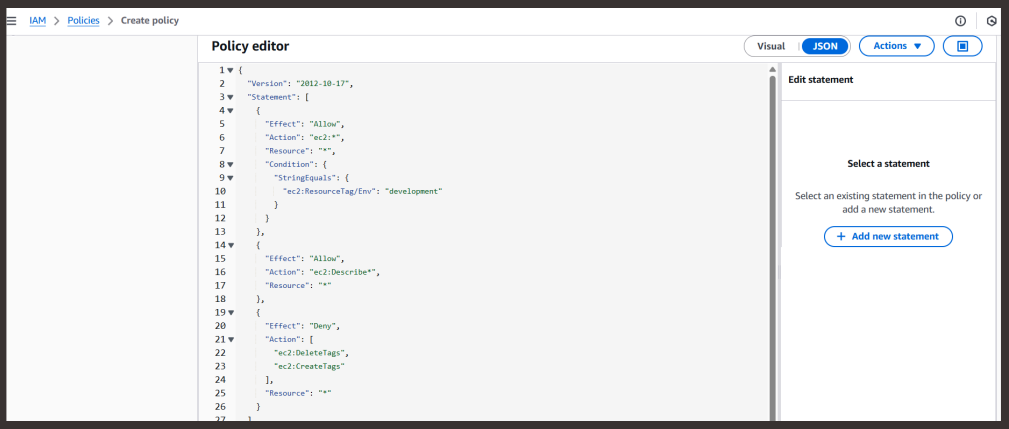
I've created a policy that allows the policy holder (i.e. the Intern) to do anything they want to any instance tag with "development" and they can also see information related to "production" but they are denied access to deleting or creating any tags for any instance as well.

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 whether or not the policy is "Denying" or "Allowing" action (i.e. Effect) ; What the policy holder can do or cannot do (i.e Action) ; and the specific AWS resources that the policy relates to (i.e resources)

Joba Amunigun
NextWork Student

My JSON Policy

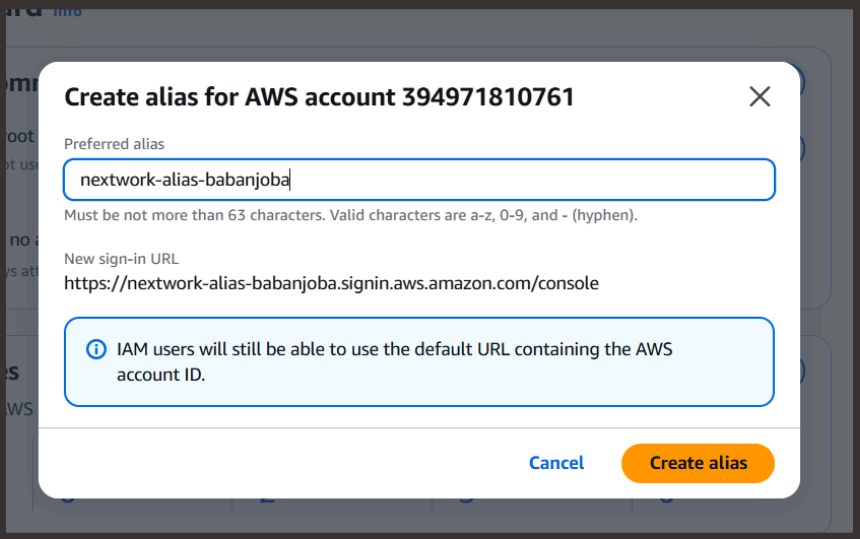


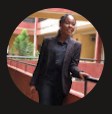
Joba Amunigun
NextWork Student

Account Alias

An account alias is a friendly name (Nickname) for your AWS account. Instead of a long account ID we can now refrence our account alias instead.

Creating an account alias took me about few seconds - it's a very simple Configuration in the IAM Dashboard. Now, my new AWS console sign-in uses the alias instead of the account ID




Joba Amunigun
NextWork Student

IAM Users and User Groups

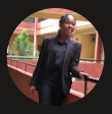
Users

IAM users are entities that have access or canlogin to your AWS account

User Groups

IAM user groups are like folders that collects IAM Users so that you can apply permission setting at the group level

I attached the policy I created to this user group, which means any user created inside this group will automatically get the permissions attached to the "NextWorkDevEnvironmentPolicy"

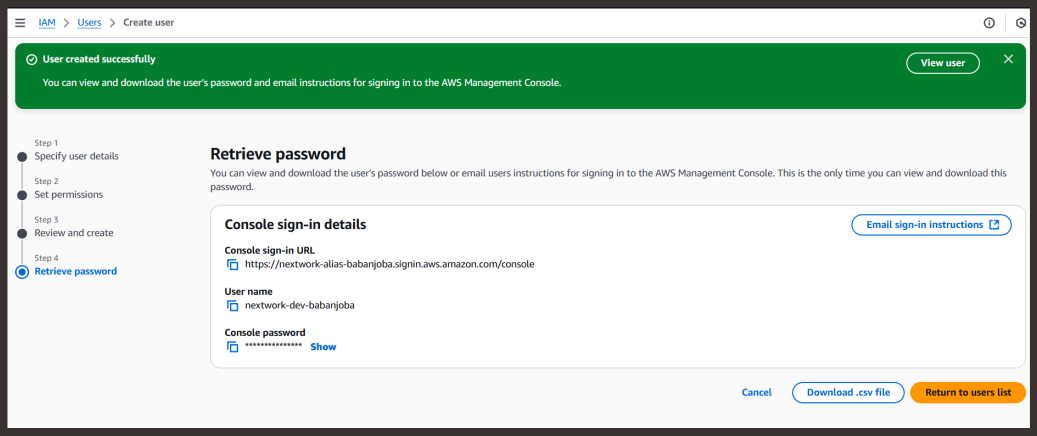


Joba Amunigun
NextWork Student

Logging in as an IAM User

The first way is to email users instructions for signing in to the AWS Management Console while the second way is to download the user's password as a CSV file

Once I logged in as my IAM user, I noticed that some of the dashboard panels are showing "Access denied" already. This was because i only set up the development EC2 instance so that the intern will not have access to something else and even see something else



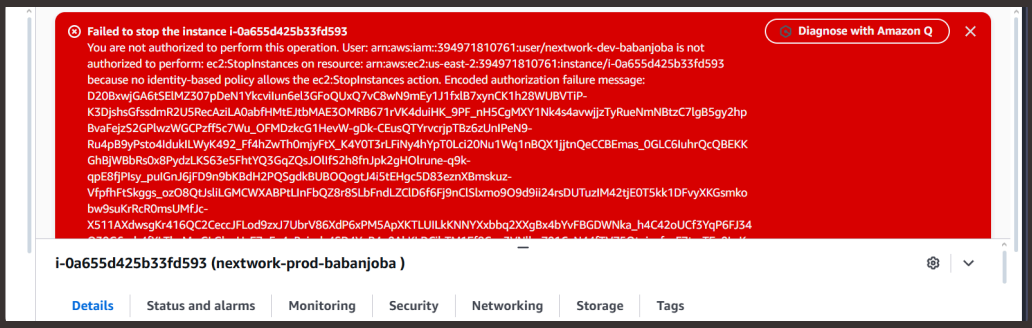
Joba Amunigun
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by attempting to stop both the development and production instances

Stopping the production instance

When I tried to stop the production instance - At the top of my page, an angry-looking banner indicated that the instance failed to stop .This was because the intern was not authorized and does not have the permission to stop any instance with the production tag - This is outside of the scope of his permission policy "Interns are only allowed to do things to the development instance"

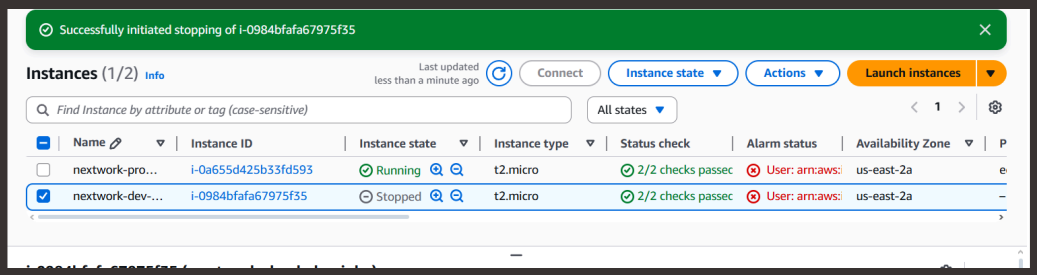


Joba Amunigun
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance i successfully saw the instance state change to "stopping" then eventually "stopped". This was because our permission policy allows the interns (i.e users in the nextwork-dev-group.)to stop instances.



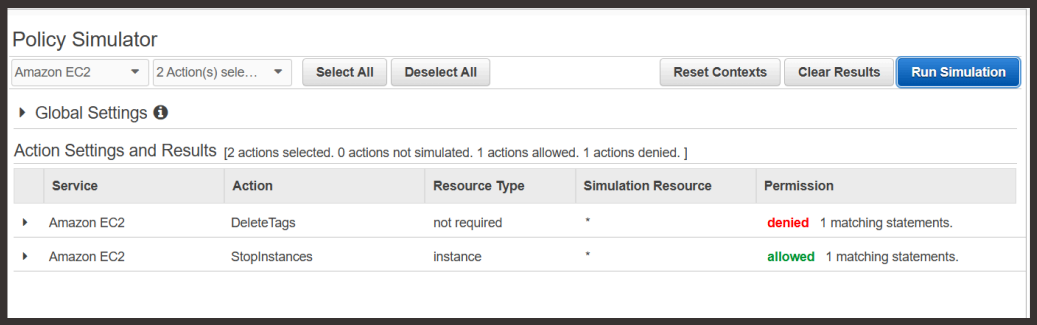
Joba Amunigun
NextWork Student

The IAM Policy Simulator

The IAM Policy Simulator is tool that lets us stimulates actions and test permission settings by defining defining a specific user,group and role. It's useful for saving time when testing permission setting no more logging into another user or stopping instances

How I used the simulator

I set up a simulation for whether the "dev user group" has permission to Stop instances or Delete tags.The results were denied for both so I had to adjust the scope of the EC2 instance to the ones that are tagged with "development". When i applied that tag permission was allowed



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects