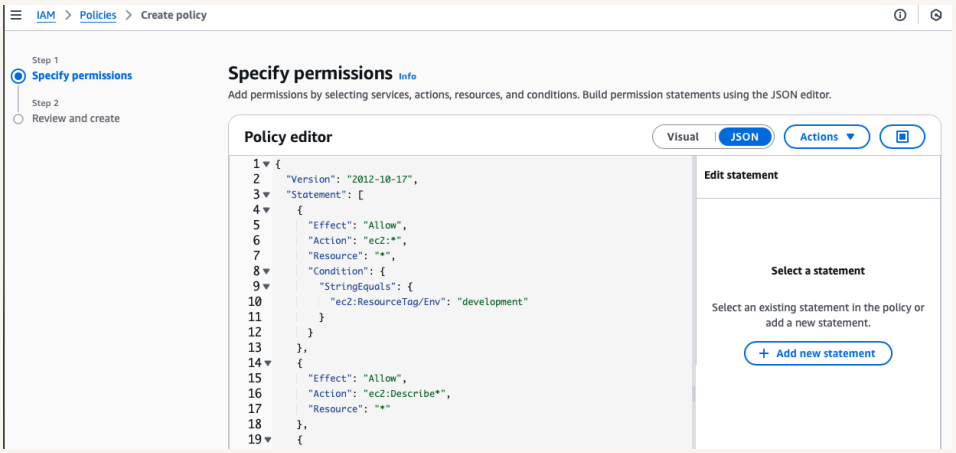
nextwork.org

Cloud Security with AWS IAM

Nigel Chitapi



Nigel Chitapi
NextWork Student

Introducing Today's Project!

Project overview

In this project, I will demonstrate how to use AWS IAM to control access and permission settings in my AWS account. I'm doing this project to learn cloud security from the basics and foundationtions. Every company thinks about access permissions, and there are even jobs called 'IAM Engineers" focused on these specifics security skills.

Tools and concepts

Services I used were EC2, IAM. Key concepts I learnt include IAM Users and Groups, IAM Policies, Instance creation, IAM Policy Simulator, Logging in as another user.

Project reflection

This project took me approximately 1.5hrs including demo time. The most challenging part was understand IAM JSON Policy structures and statement. It was most rewarding to see the IAM Policies work efficiently.

Nigel Chitapi
NextWork Student

Tags

What I did in this step

In this step, I will launch 2 EC2 instances because i need to boost NextWork's computing power. The company is expecting more users and traffic into their website for a period of time over the summer break.

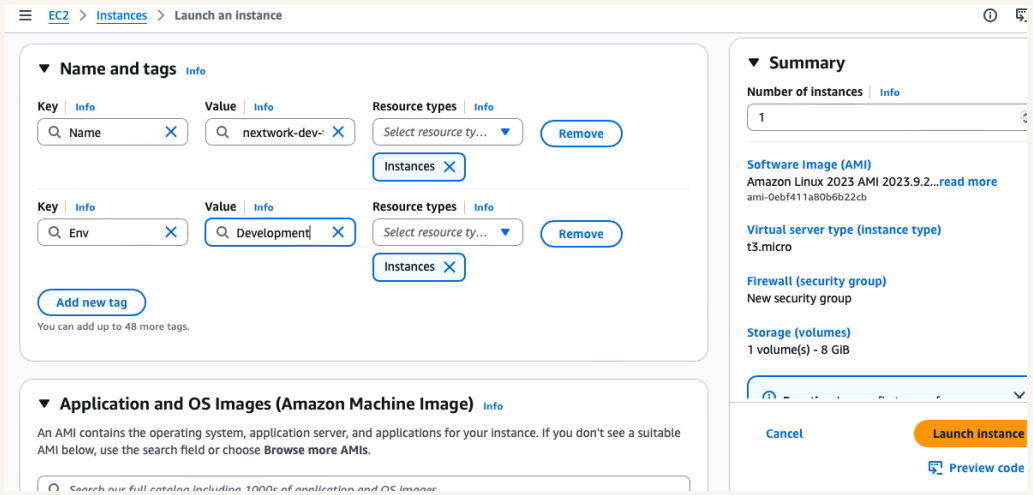
Understanding tags

Tags are organizational tools that enable us to label our resources.

My tag configuration

The tag I've used on my EC2 instances is called Environment. The values I've assigned for my instances are Production and Development.

Nigel Chitapi
NextWork Student



Nigel Chitapi
NextWork Student

IAM Policies

What I did in this step

In this step, I will use IAM Policies to control the access level of the newly hired intern. This is because they should only have access to the Development Environment and not the Production Environment.

Understanding IAM policies

IAM Policies are like rules that determine who can do what on AWS resources.

The policy I set up

For this project, I've set up a policy using JSON. I am using policies to control who has access to the production instance.

Policy effect

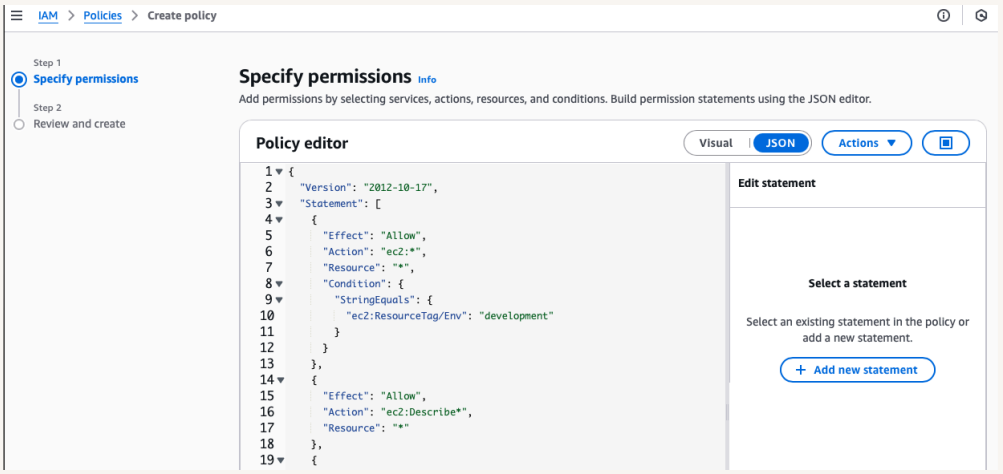
I've created a policy that allow the policy holder to have permission to do anything they want to any instance with the tag named "development". They can also see any information related to any instance however they can not delete or create tags for any instance

Understanding Effect, Action, and Resource

The Effect, Action, and Resource attributes of a JSON policy means whether or not the policy is allowing or denying action (effect), what the policy holder can and cannot do (action) and the specific AWS resources that the policy holder relates to (resource).

Nigel Chitapi
NextWork Student

My JSON Policy



Nigel Chitapi
NextWork Student

Account Alias

What I did in this step

In this step, I will setup an account alias which is like a nickname for an AWS account console log in. This is because an account alias makes it easy for our users to log-in

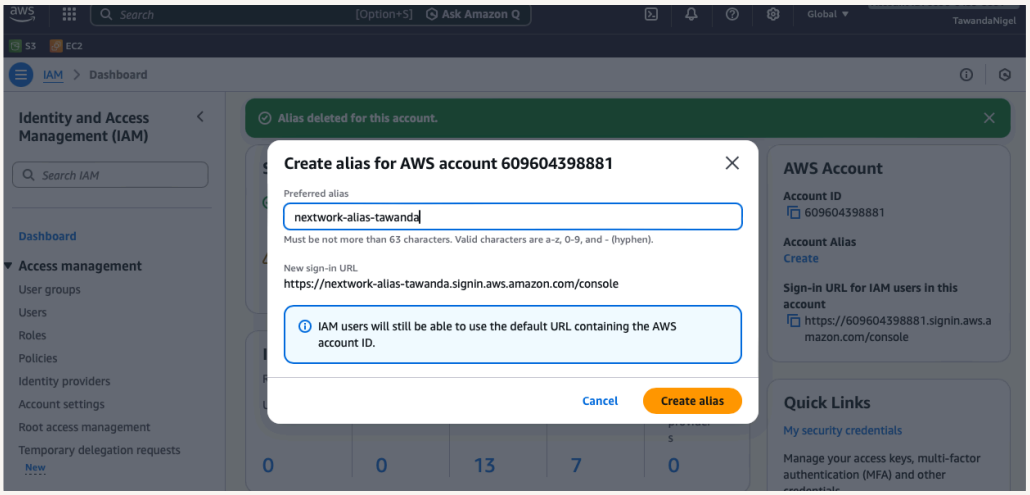
Understanding account aliases

An account alias is nickname for my AWS account instead of a long account ID we can now reference our account alias instead.

Setting up my account alias

Creating an account alias took me 15 seconds. Now, my new AWS console sign-in URL uses my alias and not my account ID.

Nigel Chitapi
NextWork Student



Nigel Chitapi
NextWork Student

IAM Users and User Groups

What I did in this step

In this step, I will setup 2 resources IAM Users and IAM groups. This is because IAM Users are like log-ins for people who want access to our AWS account and the IAM User Groups are like folders to manage users with the same level of access.

Understanding user groups

IAM user groups are like folders that contain IAM Users so that we can apply permission policies at the User Group

Attaching policies to user groups

I attached the policy I created to this user group, which means every user assigned to this group will be bound by the policies attached to the group

Understanding IAM users

IAM users are people or entities that can access or log into the AWS account.

Nigel Chitapi
NextWork Student

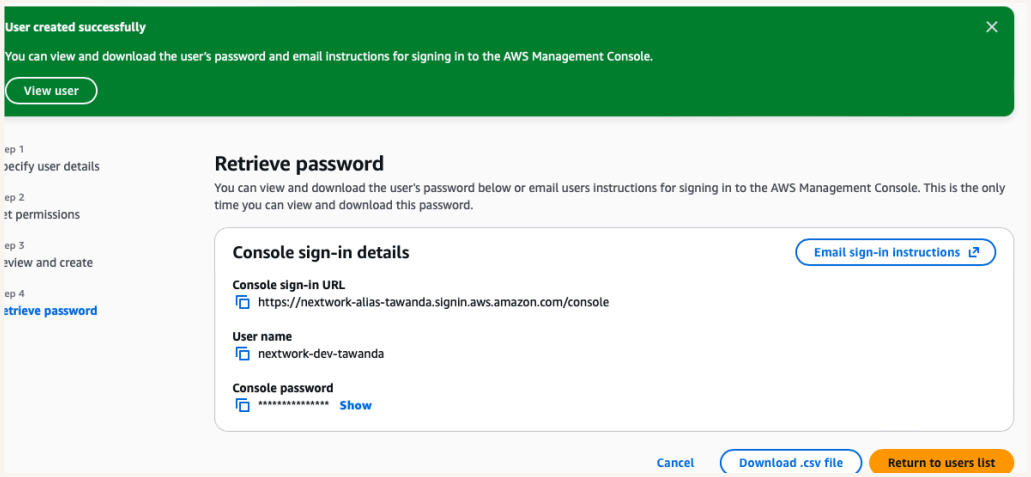
Logging in as an IAM User

Sharing sign-in details

The first way is email direct to the user or download the csv file

Observations from the IAM user dashboard

Once I logged in as my IAM user, I noticed that the intern user is denied access to panels on the main AWS Console dashboard. This was because we only setup permissions to the Development EC2 instance, so the intern would not have access to anything else of see anything else.



Nigel Chitapi
NextWork Student

Testing IAM Policies

What I did in this step

In this step, I will log into the AWS account as the intern and test access to the production and development instances because I need to ensure that the intern does not have the ability to do anything that might affect the production environment

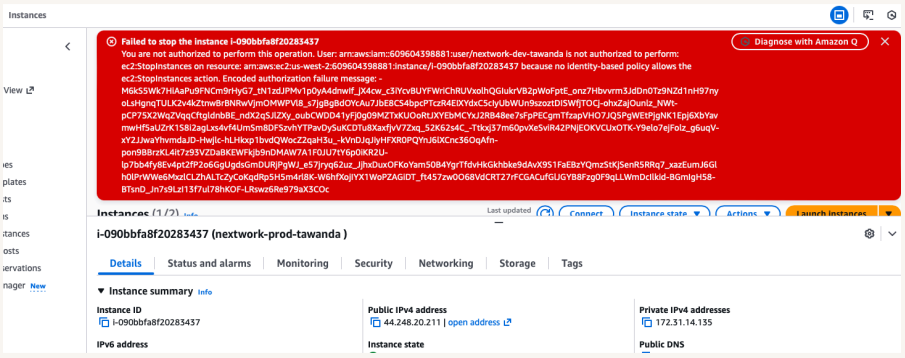
Testing policy actions

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

Stopping the production instance

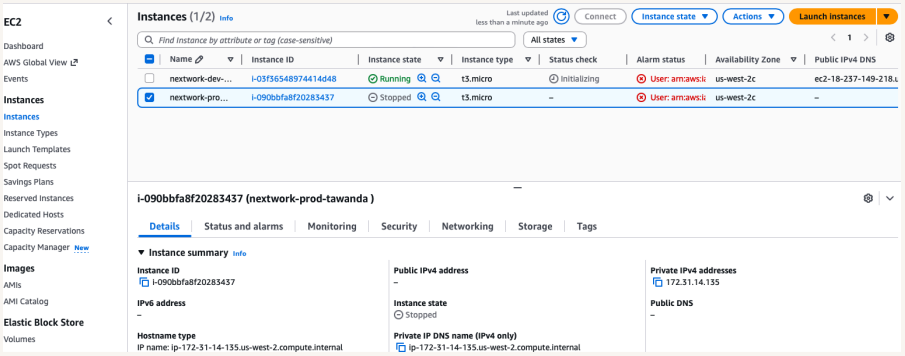
When I tried to stop the production instance i was met with an error. This was because the production instance is tagged with the production label which is outside of the production scope of the assigned policy.

Nigel Chitapi
NextWork Student



Stopping the development instance

Next, when I tried to stop the development instance i successfully saw the instance state stopping. This was because the permission policy allows users in the Dev Users to perform any action on the Development EC2 instance



Nigel Chitapi
NextWork Student

IAM Policy Simulator

To extend my project, I'm going to test the permission policies in a safer and more controlled way using a tool named IAM Policy Simulator. I'm doing this because having to stop instances and log into AWS accounts as other users in quite inefficient and can be disruptive.

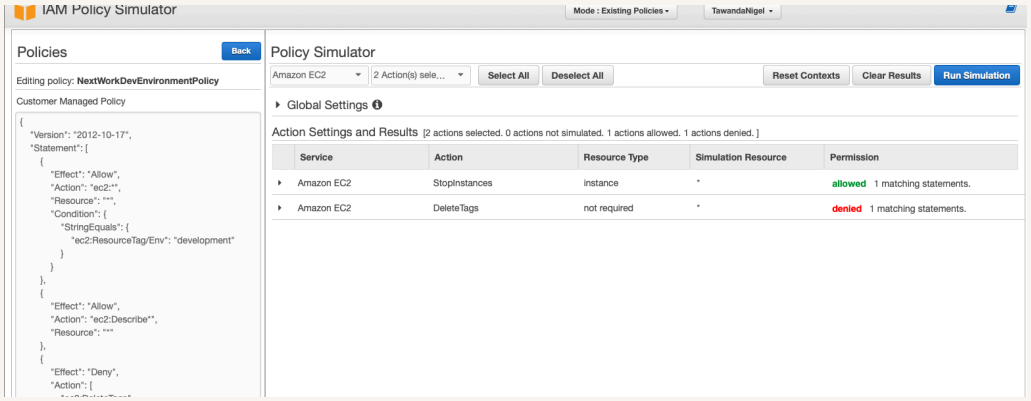
Understanding the IAM Policy Simulator

The IAM Policy Simulator is a tool that allows me to test permission settings by defining a specific users, group, role that i want to test for. It's useful for saving time time when testing permissions.

How I used the simulator

I set up a simulation for whether the Development user group had permission to stop instances or delete tags. The results were Denied! (which was great!) I had to adjust the scope of the EC2 instances to ones that are tagged development and this time around the the actions on the EC2 instances tagged Development were allowed.

Nigel Chitapi
NextWork Student



The place to learn & showcase your skills

Check out nextwork.org for more projects