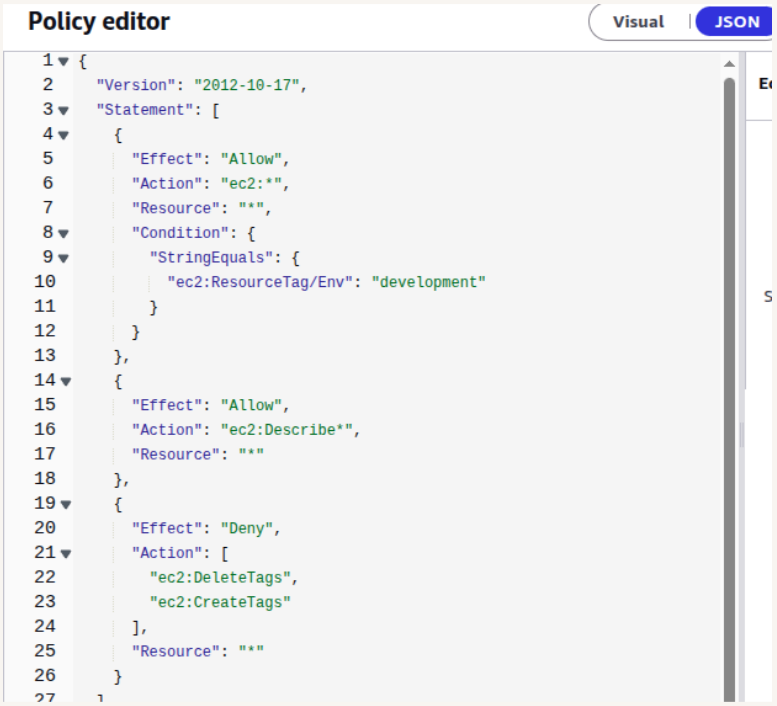
nextwork.org

Cloud Security with AWS IAM

Clive Maduke



Clive Maduke
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 to about cloud security from absolute foundations- every company has to think about access permissions, and there is even entire careers or jobs called IAM Engineers' focused on the skills I am demonstrating on this project today.

Tools and concepts

Services I used were Amazon EC2 and AWS IAM Key concepts I learnt include IAM users, policies, user groups and account aliases. I also learnt how to use policy simulator and how JSON policies work How to launch and tag an instance how to log in as another user

Project reflection

This project took me approximately 1 hours... The most challenging part was trying to figure out policies ... It was most rewarding was being able to see how the polies that were put in place will work for the user from using thier account to using the Policy simulator to...

Clive Maduke
NextWork Student

Tags

What I did in this step

In this step, I will be launching two EC2 instances because they will be needed to boost NextWork's computing power because NextWork will be expecting an influx of traffic over the Summer break!

Understanding tags

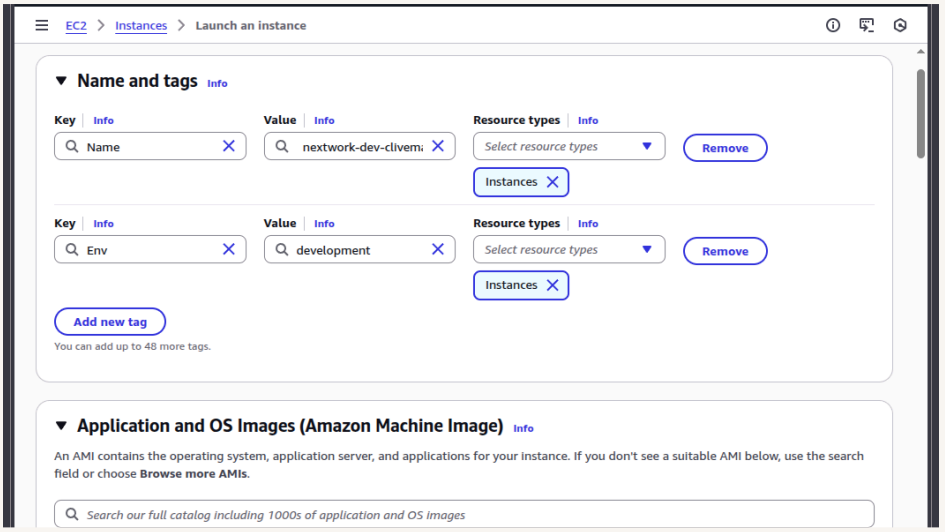
Tags are orgnisational tools that lets us label resources. They are useful for grouping resources, cost allocation and applying policies for all resources with tthe same tag

My tag configuration

The tag I have used on my EC2 instances is called Environment. The value I’ve assigned for my instances are production and development.

Clive Maduke
NextWork Student

nextwork.org



Clive Maduke
NextWork Student

IAM Policies

What I did in this step

In this step, I will use IAM policies to control the access level of a new NextWork intern because they should have access to the development environment(i.e the development environment) but NOT the production environment.

Understanding IAM policies

IAM Policies are rules that govern who can do what in our account. I will be using policies today to control who has access to our production or environment instance.

The policy I set up

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

Policy effect

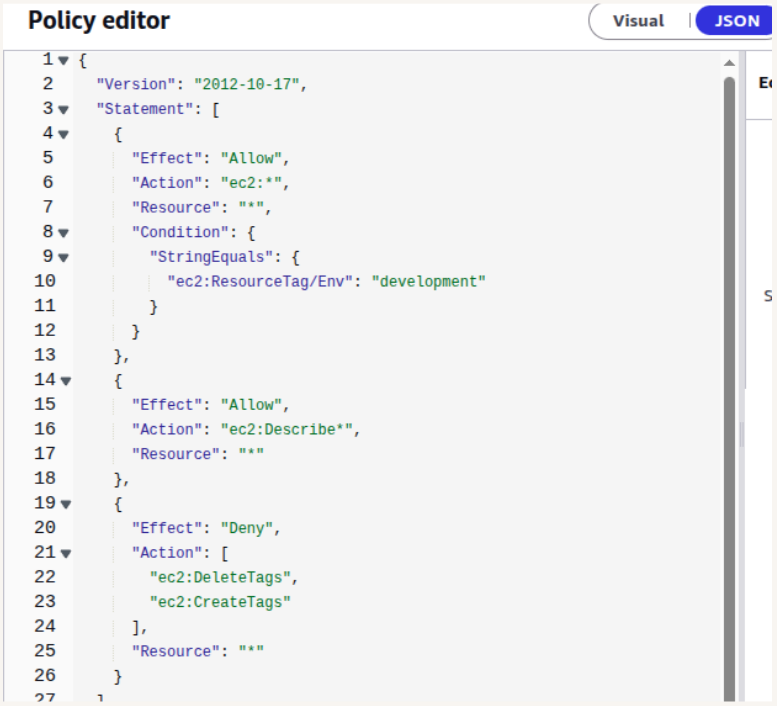
I've created a policy that allow the holder ie the intern to have permission to do anything they want to any instance tagged with "development". They can also see informationfor any instance, but there are denied access to deleting or creating tags for any instance

Understanding Effect, Action, and Resource

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

Clive Maduke
NextWork Student

My JSON Policy



Clive Maduke
NextWork Student

Account Alias

What I did in this step

In this step, I will set up an Account Alias, which is like a nickname for our AWS console's login. This because it makes it simple for the users loging easily.

Understanding account aliases

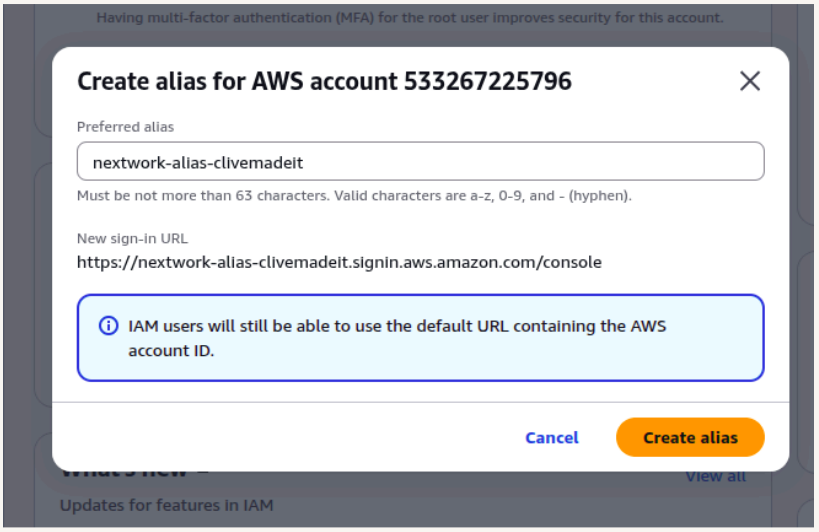
An account alias is a nick name for an AWS account instead of a long account ID, which means now I can reference my account instead.

Setting up my account alias

Creating an account alias took me less than a minute it was the simplest configuration. Now, my new AWS console sign-in URL uses the alias that I have created instead of my account ID

Clive Maduke
NextWork Student

nextwork.org



Clive Maduke
NextWork Student

IAM Users and User Groups

What I did in this step

In this step, I will set up two dedicated IAM resources IAM users, and IAM user groups. This is because IAM users are like logins for people that want access to our AWS account, while user groups are like folders to manage users that have the samw level of access.

Understanding user groups

IAM user groups are like folders that collect IAM users so that one can apply permission settings aat the group level.

Attaching policies to user groups

I attached the policy I created to this user group, which means any user created will automatically get the permissions our NextWorkDevEnvironment policy IAM Policy

Understanding IAM users

IAM users are people or entities that have or entities login to our AWS account.

Clive Maduke
NextWork Student

Logging in as an IAM User

Sharing sign-in details

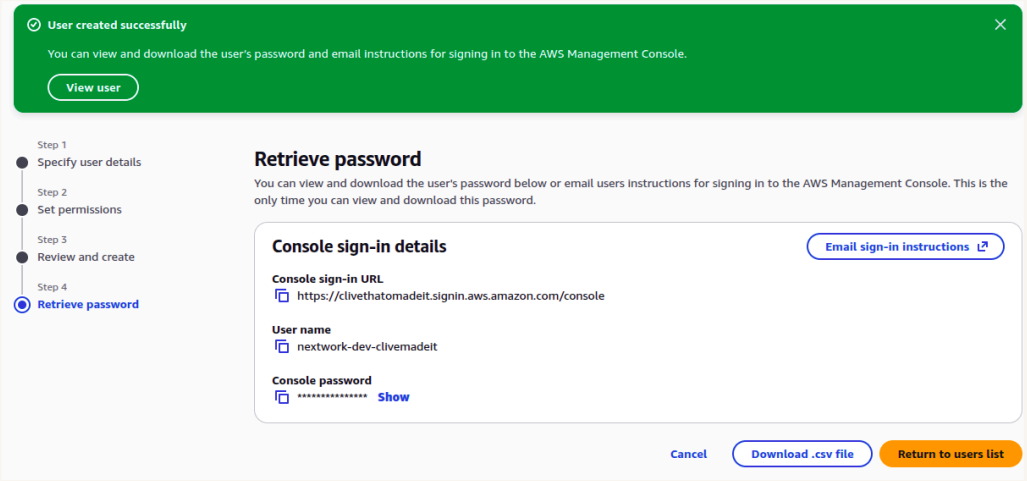
The first way is to email sign-in instructions to the user, while the second way is to download the .csv file with the sign details inside.

Observations from the IAM user dashboard

Once I logged in as my IAM user, I noticed that the user is already denied access to panels on the main AWS console dashboard. This was because the permissions have been set up to our development EC@ instance, so our intern will not be able to have access to the even see anything else

Clive Maduke
NextWork Student

nextwork.org



Clive Maduke
NextWork Student

Testing IAM Policies

What I did in this step

In this step, I will login to own AWS account as the intern and test access to the production and development instances because I have to make sure the intern has been given the right permissions and that the can not affect our production environment.

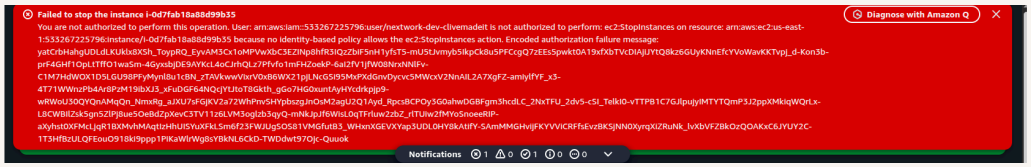
Testing policy actions

I tested my JSON IAM policy by attempting to stop both the development and [roduction instences

Stopping the production instance

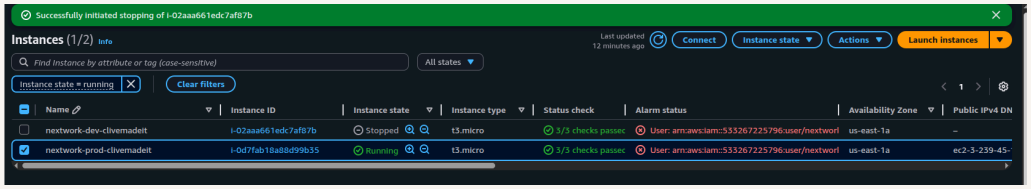
When I tried to stop the production instance I encountered an error. This was because our production instance is tagged with the production label which is out of the scope of our permission policy. interns are only allowed to do things to the development instances.

Clive Maduke
NextWork Student



Stopping the development instance

Next, when I tried to stop the development instance the stoppage was successfull as the instance state changed to stopping and then finally stopped. This this is due to the intern having permmission over at the development instance.



Clive Maduke
NextWork Student

IAM Policy Simulator

To extend my project, I'm going to test our permissions policies in safer and more controlled way using a tool called IAM poliy si,uater ... I'm doing this because... having to change accounts and stopping resources can be disruptive to other users

Understanding the IAM Policy Simulator

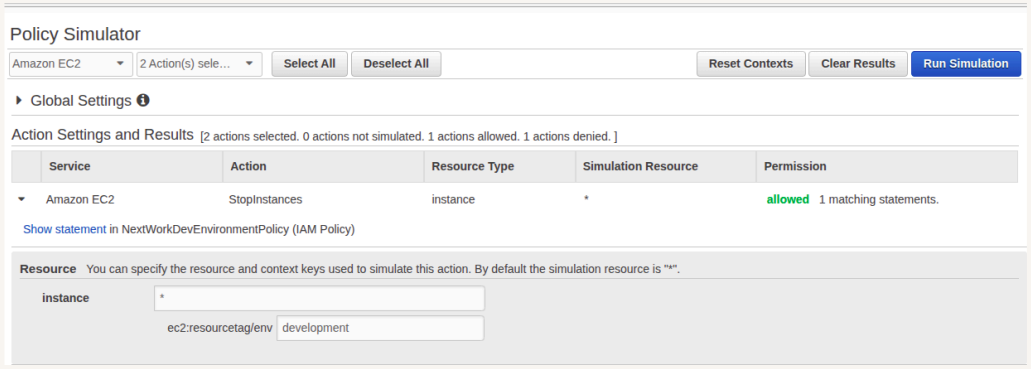
The IAM Policy Simulator is a tool that lets one simulat actions and test permission settings by defining a specific user, group or role and action we want to test for ... It's useful for saving time because one does not need to log in as another user to test out the permissions or stopping resources...

How I used the simulator

I set up a simulation for.whether our users can access certain permissions to stop instances and delete tags. The results were.. denied for both. I had to adjust the scope to EC2 instances to once that are tagged with development. Once we applied that tag, permission was allowed

Clive Maduke
NextWork Student

nextwork.org



The place to learn & showcase your skills

Check out nextwork.org for more projects