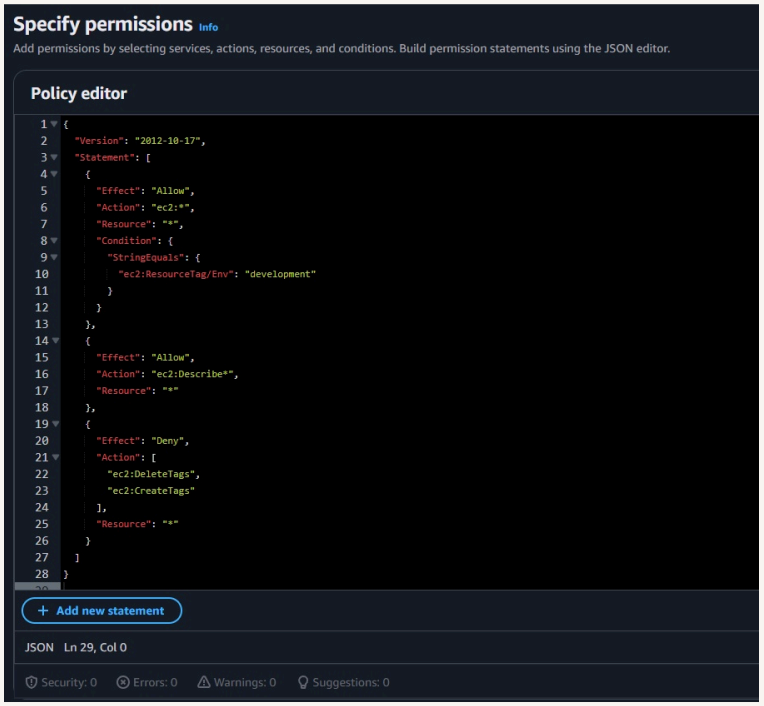
nextwork.org

Cloud Security with AWS IAM

B Bryce Cox



B
Bryce Cox
NextWork Student

Introducing today's project!

What is AWS IAM?

Services I used were EC2 and IAM. Key concepts I learned include IAM policy management, IAM groups, and IAM users. These concepts are essential to creating a productive and secure AWS environment.

How I'm using AWS IAM in this project

This project took me approximately one hour. The most challenging part was ensuring that the JSON policy was accurate. It was most rewarding to see my policy put into action and block the stoppage of the production instance.

One thing I didn't expect...

I chose to do this project today because I want to ensure that I understand the fundamentals of cloud and cloud security. Something that would make learning with NextWork even better is some of the pro features becoming free.

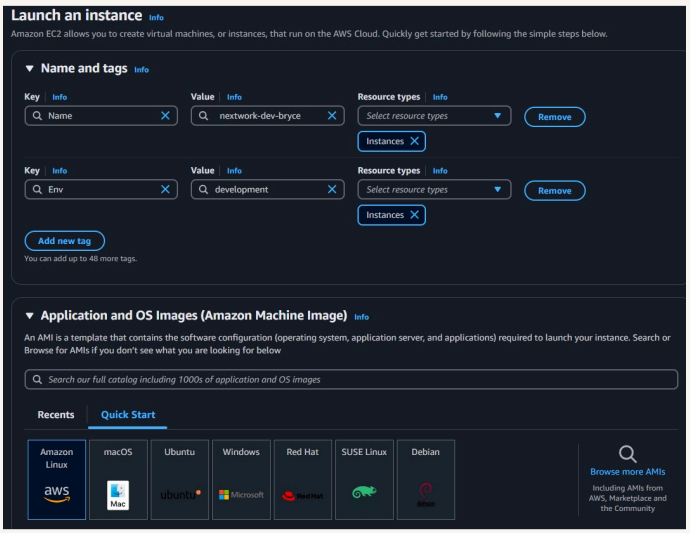
B

Bryce Cox
NextWork Student

Tags

Tags are useful for labeling instances for there use and being able to group them together in a search of multiple instances.

The tag I've used on my EC2 instances is called "Env" for environment. The values I've assigned for my instances are "production" and "development" which represent the which stage that instance is for.



B
Bryce Cox
NextWork Student

IAM Policies

IAM Policies are how we decide who can do what with our resources.

The policy I set up

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

I've created a policy that allows starting, stopping, and describing EC2 instances tagged "development," while denying the creation or deletion of tags on any resource.

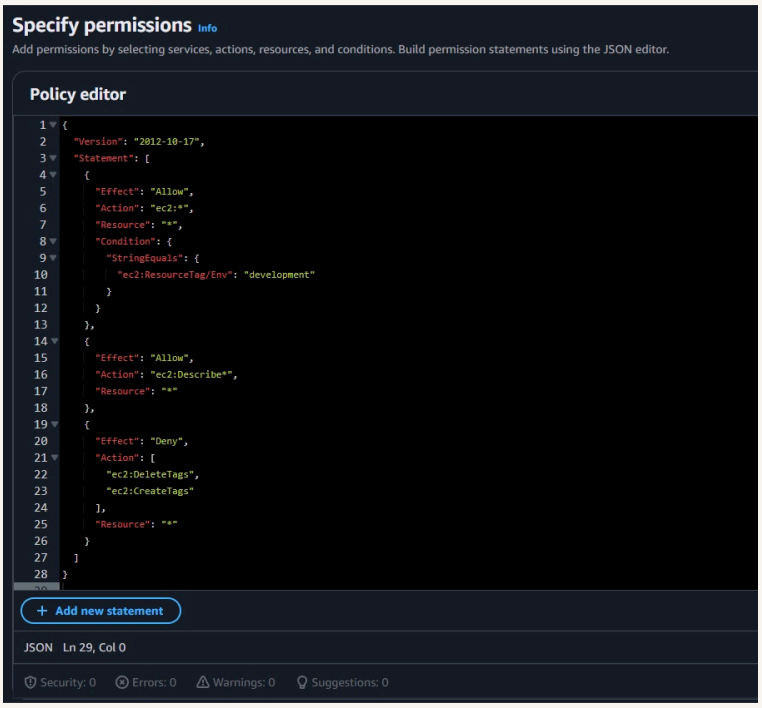
When creating a JSON policy, you have to define its Effect, Action and Resource.

The Effect, Action, and Resource attributes of a JSON policy means what we want to allow/block, what we want to do, and what resource we are refering to.

B

Bryce Cox
NextWork Student

My JSON Policy

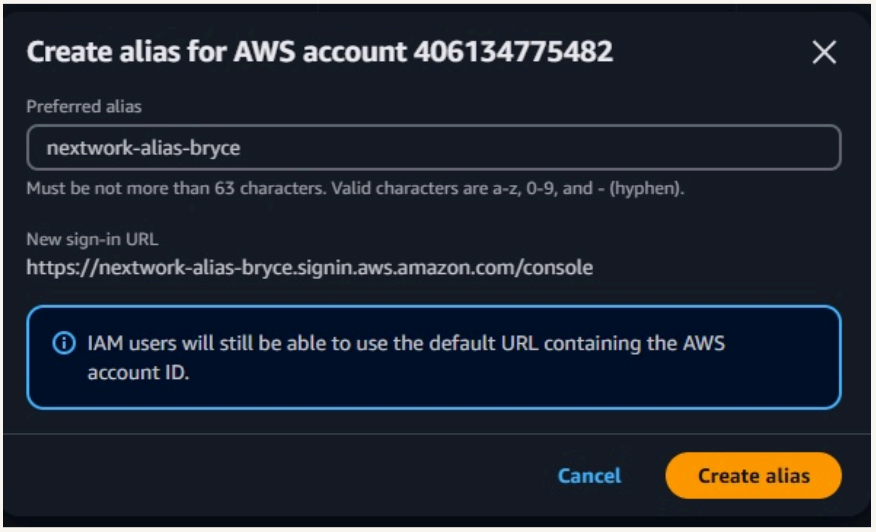


B
Bryce Cox
NextWork Student

Account Alias

An account alias is a name that you can use instead of the account ID, which simplifies the login process.

Creating an account alias took me 30 seconds. Now, my new AWS console sign-in URL is https://nextwork-alias-bryce.signin.aws.amazon.com/console. Much easier to use!



B
Bryce Cox
NextWork Student

IAM Users and User Groups

Users

IAM users are accounts with set permissions to do their role.

User Groups

IAM user groups are essentially a folder of users that allows you to manage all of their permissions at once. This is because users in an IAM group will have to have the same permissions.

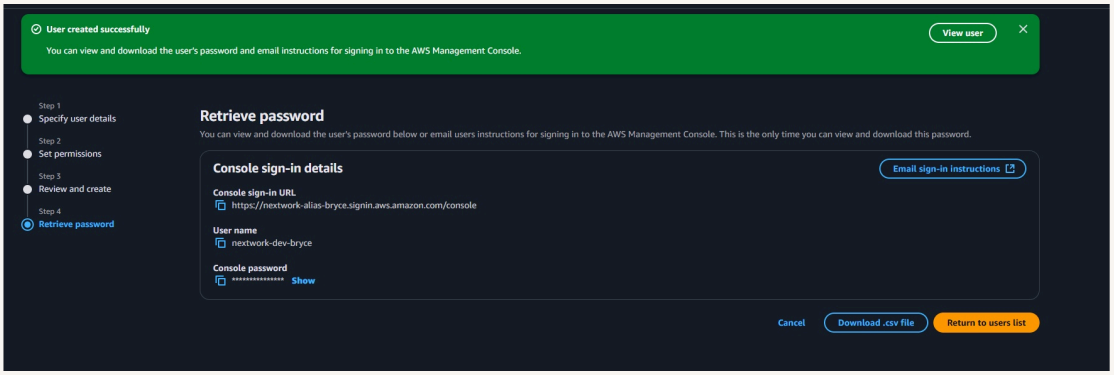
I attached the policy I created to this user group, which means they will be allowed to start, stop, and describe EC2 instances tagged "development," while being denied the creation or deletion of tags on any resource.

B
Bryce Cox
NextWork Student

Logging in as an IAM User

The first way is email sign-in instructions, the second way is to download the .csv file.

Once I logged in as my IAM user, I noticed some dashboard panels listed access denied. This was because of our IAM policy.



B

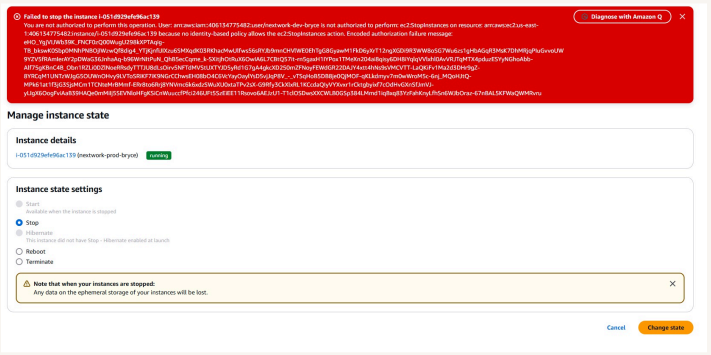
Bryce Cox
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by ensuring that the intern's user and that user group were not able to manipulate the production instance, but were still able to manipulate the development instance.

Stopping the production instance

When I tried to stop the production instance I was given a "Falied to stop instance" message. This was because our IAM policy does not allow the intern to perform these actions on the production instance.

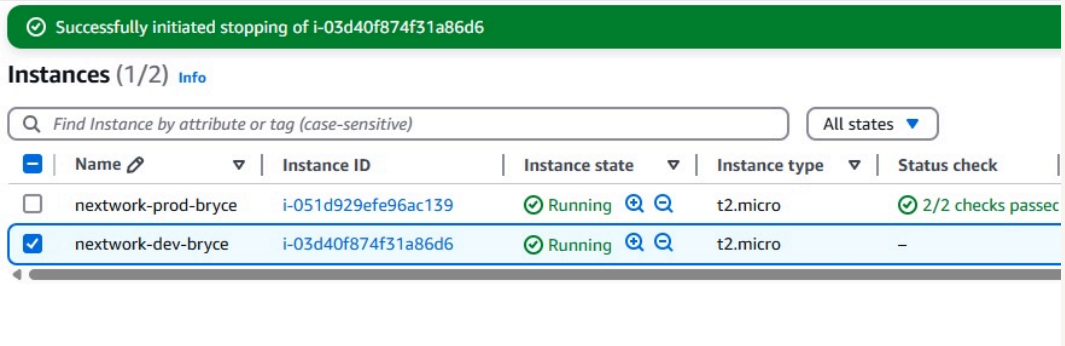


B
Bryce Cox
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance it allowed the intern to do so. This was because our IAM policy allows this action.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects