nextwork.org

Cloud Security with AWS IAM

Joseph Cole-Showers

Joseph Cole-Showers
NextWork Student

Introducing today's project!

What is AWS IAM?

Services I used were Amazon EC2, and AWS IAM. Key concepts I learnt include IAM users, role, user groups, policies, account alias, how to launch an instance, how to tag an instance, how to log in as another user.

How I'm using AWS IAM in this project

This project took me approximately 1hr 20 mins. The most challenging part was understanding the IAM policy written in JSON and it contained multiple statements. It was most rewarding to see "permission denied" when an intern tried to delete prod.

One thing I didn't expect...

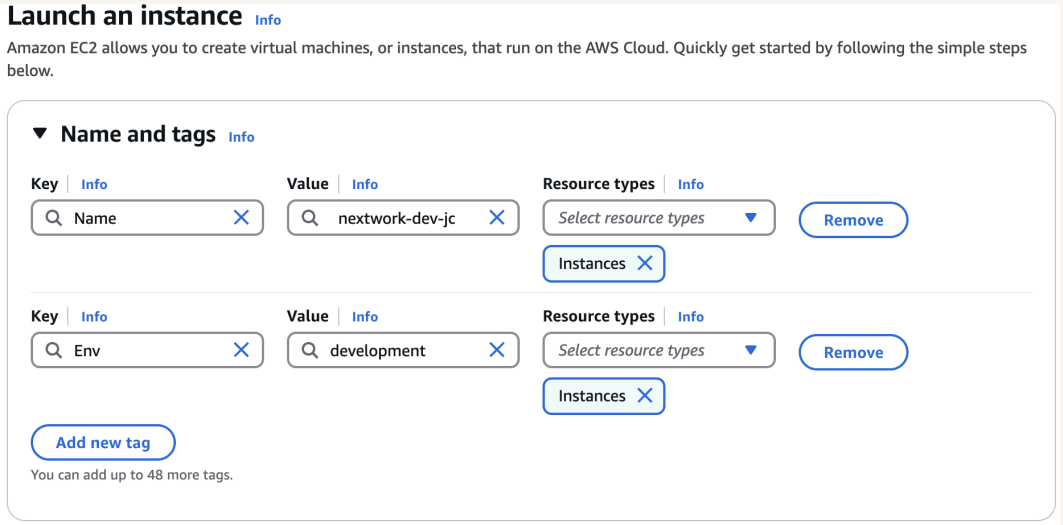
I chose to do this project today because IAM and Cloud security are key skills in Cloud computing.

Joseph Cole-Showers
NextWork Student

Tags

Tags are organizational tools that lets us to label our resources. They are helpful for grouping resources, applying policies for all resources with the same tag and cost allocation.

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



Joseph Cole-Showers
NextWork Student

IAM Policies

IAM Policies are like roles that determine who can do what in an AWS account. I'm using policies to control who has access to the production environment 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 to have permission to do anything they want with any instance tagged with dev. They can also see information related for any instance, but they are denied access to delete/create any instance

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 allowing or denying action (i.e Effect) What the policy hold can or cannot do (i.e Action) and the specific resources the policy relates to (resources).

Joseph Cole-Showers
NextWork Student

My JSON Policy

Policy editor

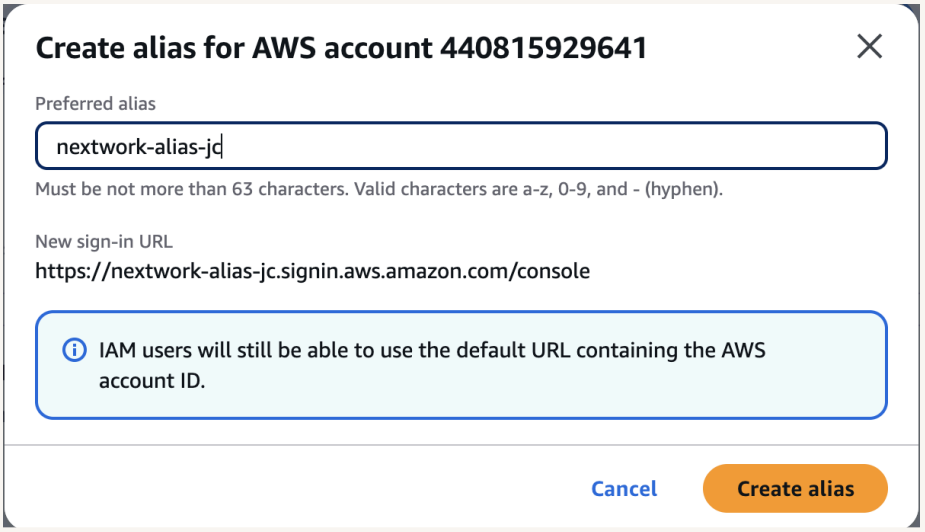
```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Action": "ec2:*",
7        "Resource": "*",
8        "Condition": {
9          "StringEquals": {
10           "ec2:ResourceTag/Env": "development"
11         }
12       }
13     },
14     {
15       "Effect": "Allow",
16       "Action": "ec2:Describe*",
17       "Resource": "*"
18     },
19     {
20       "Effect": "Deny",
21       "Action": [
22         "ec2:DeleteTags",
23         "ec2:CreateTags"
24       ],
25       "Resource": "*"
26     }
27   ]
28 }
```

Joseph Cole-Showers
NextWork Student

Account Alias

An account alias is simply a nickname for an AWS account. Instead of a log account ID, we can reference the account alias instead.

Creating an account alias took me 30 seconds. Now, my new AWS console sign-in URL uses the alias I created instead of my account ID.



Joseph Cole-Showers
NextWork Student

IAM Users and User Groups

Users

IAM users are people or entities that have access / login to your aws account.

User Groups

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

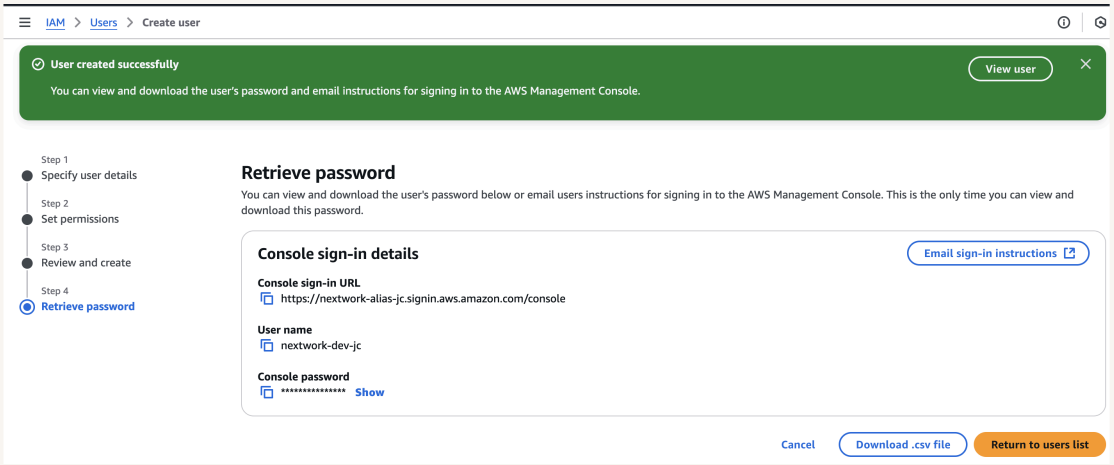
I attached the policy I created to this user group, which means any user created inside this group will automatically get the permissions attached to the policy

Joseph Cole-Showers
NextWork Student

Logging in as an IAM User

The first way is to email sign in instructions to the user, and the second way is to download the CSV file with the sign in details inside.

Once I logged in as my IAM user, I noticed that the user (intern) is already denied access to items under AWS dashboard. This was because I only setup permissions to our development EC2 instance.



Joseph Cole-Showers
NextWork Student

Testing IAM Policies

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

Stopping the production instance

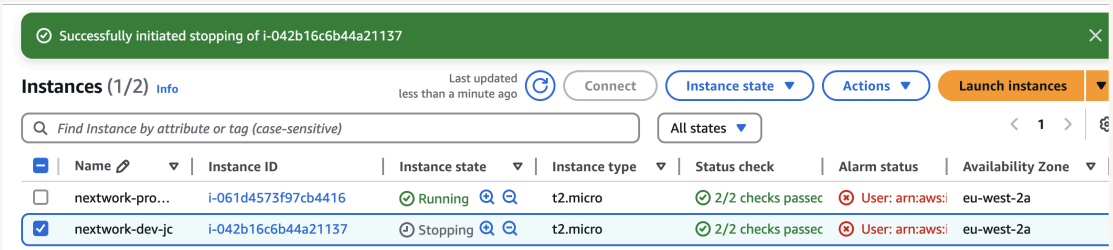
When I tried to stop the production instance I got an error. This was because the production instance is tagged with the production label which is outside of the scope of the permission policy. Interns are only allowed to do work in the dev instance.

Joseph Cole-Showers
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance I successfully saw the instance state changed to stopping and then stopped. This was because the permission policy I set allows the user in the dev group to stop instances.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects