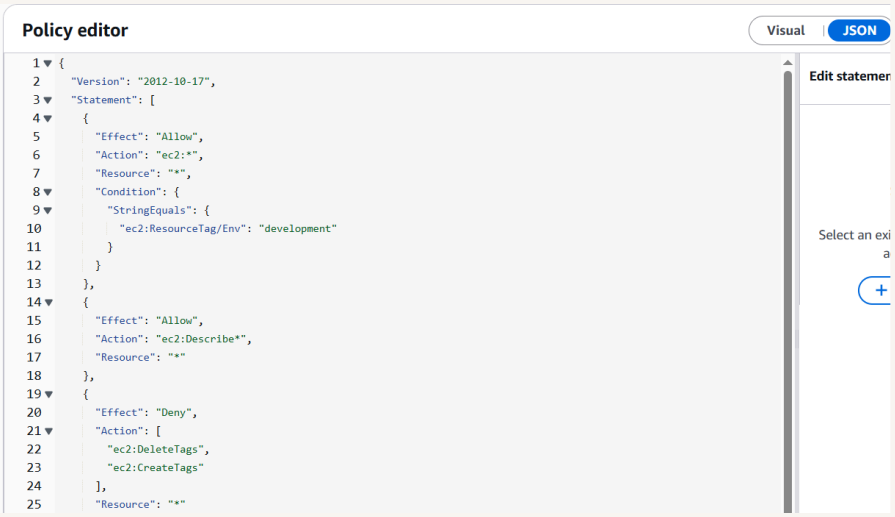
nextwork.org

Cloud Security with AWS IAM

MU muzyavida@gmail.com



Introducing Today's Project!

In this project, I will demonstrate how to use AWS IAM to control access and permission settings in our AWS account. I'm doing this project to learn about cloud security as every company thinks of access permissions and control of resources.

Tools and concepts

Services I used were Amazon EC2 and AWS IAM. Key concepts I learnt include IAM users, User groups,account aliases. I also (on the side) learnt how to use a policy simulator and how JSON policies work and how to launch and tagging an instance.

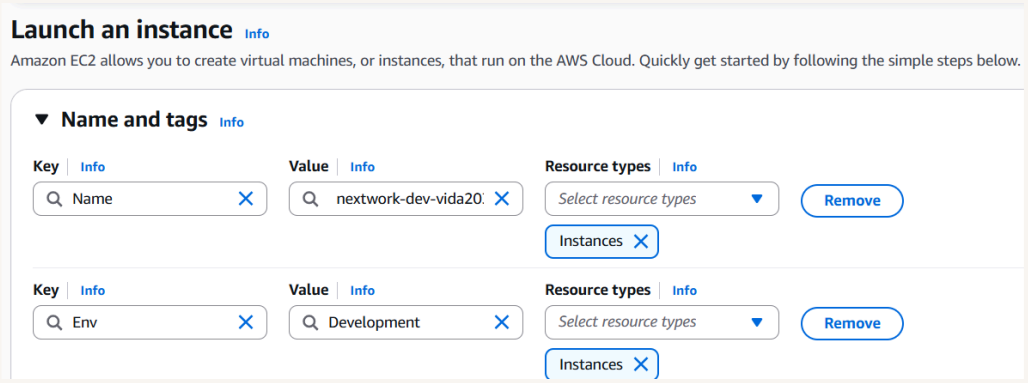
Project reflection

This project took me approximately 1.5 hours to finish. The most challenging part was understanding the IAM policy since it was written in JSON which had multiple statements. It was most rewarding to see permission denied meaning our policy worked.

Tags

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

The tag I've used on my EC2 instances is called Env, which stands for environment. The value I've assigned for my instances are production and development which represent the development stage or production stage in a the cycle.



IAM Policies

IAM Policies are like rules that determine who can do what in our AWS account. We are using policies today to control who has access to our production/development instances.

The policy I set up

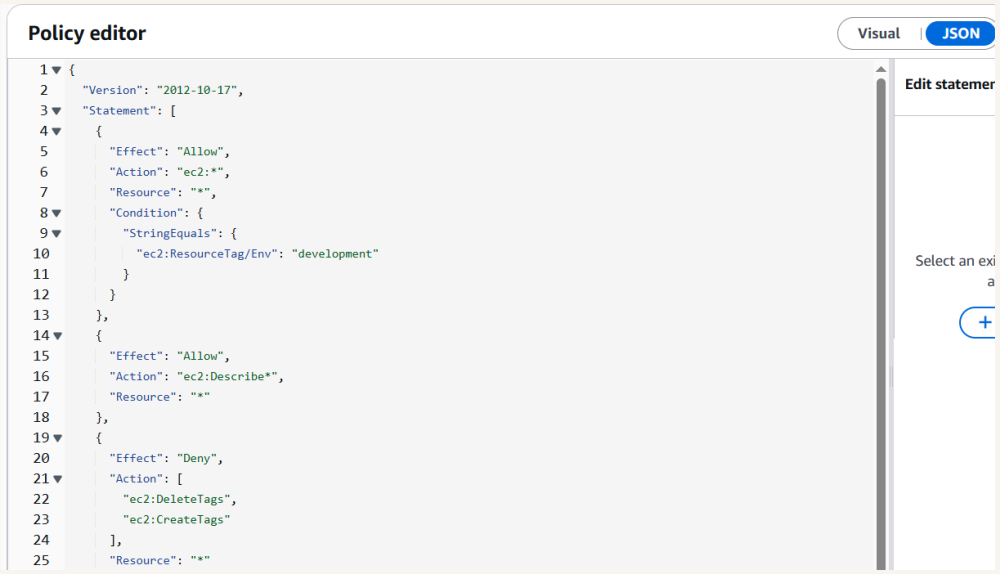
For this project, I've set up a policy using JSON.

I've created a policy that allows the user (i.e intern) to have permission to do anything in an the instance tagged "development". They can see info for any instance, but denied access to delete/create tags on any instances.

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 ot not the policy is allowing/denying(i.e effect), what the user can/cant do(i.e action),and the specific AWS resources the policy relates to (i.e resource)

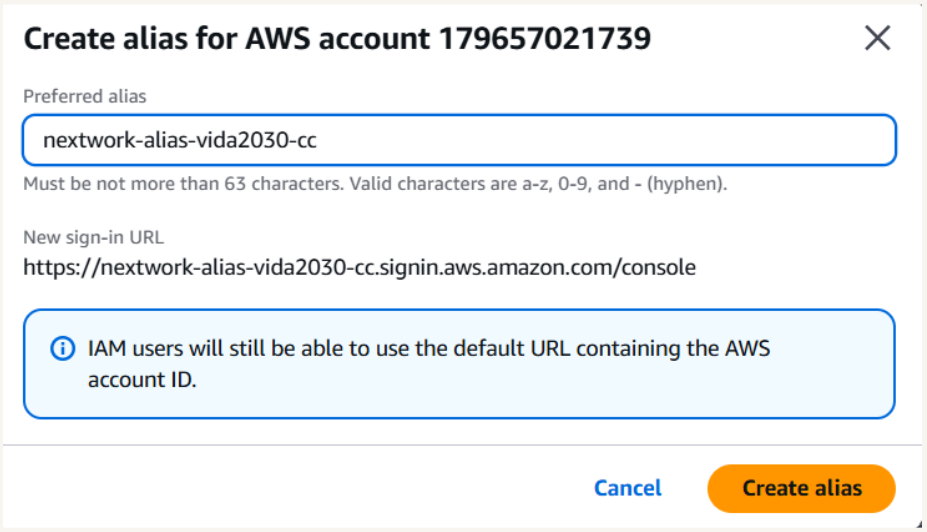
My JSON Policy



Account Alias

An account alias is simply a nicknamw for our AWS account. Instead of using a long account ID to login we can now reference our account alias instead.

Creating an account alias took me about 30 seconds. It is a simple configuration in the IAM dashboard.



IAM Users and User Groups

Users

IAM users are people/entities that have access to login to my AWS account.

User Groups

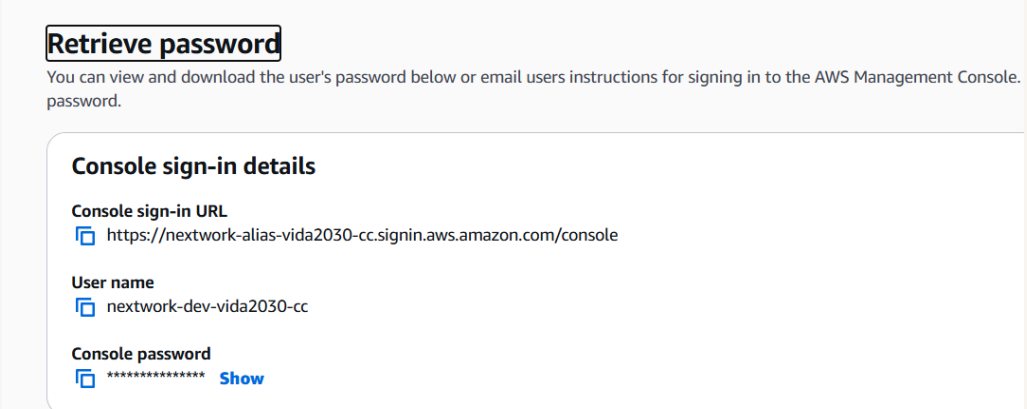
IAM user groups are like folders that collect IAM users so that you can apply permission settings at a group level.

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 our NextworkDevEnvironmentPolicy

Logging in as an IAM User

The first way is to email sign-in instructions to the user and the second is to download a .csv file with the login details.

Once I logged in as my IAM user, I noticed that our user is already denied access to panels on the main AWS console dashboard. This was because we only set up permissions to our development EC2 instance, so our intern cant see anything else.



Testing IAM Policies

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

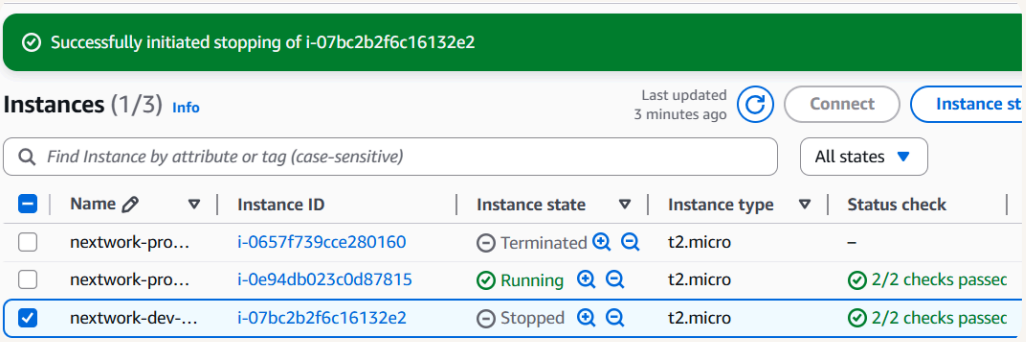
Stopping the production instance

When I tried to stop the prod instance,we were met with an error and its because our production instance is tagged with the 'production' label which is outside the scope of our permission policy-users only have access to the development instance.

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, we successfully saw the instance state change to stopping then stopped. This was because our permission policy allows the user to stop instances under the development environment not production.



The place to learn & showcase your skills

Check out nextwork.org for more projects