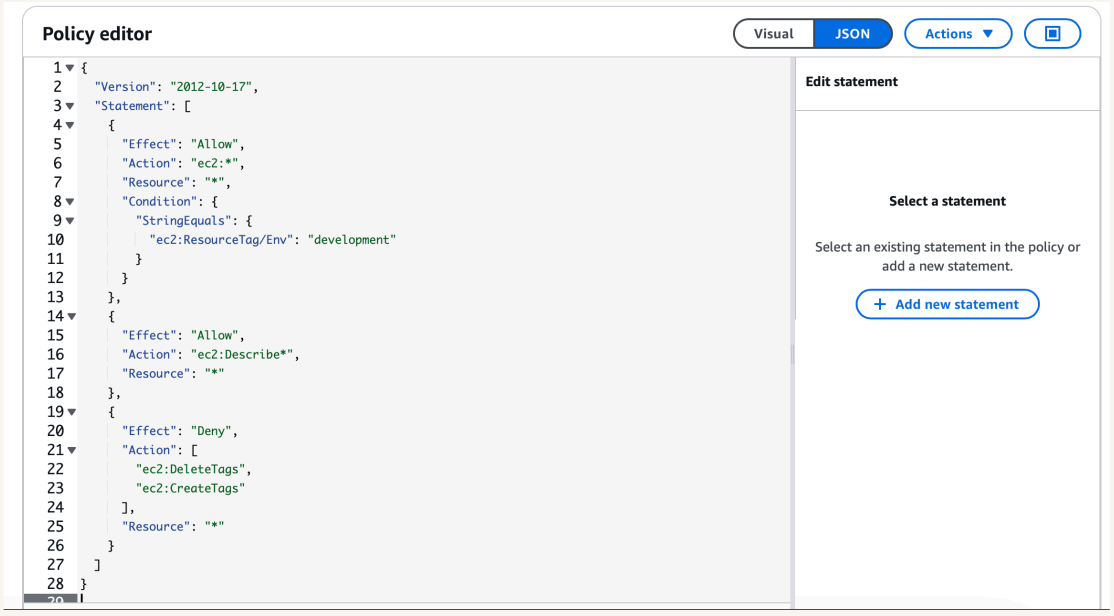
nextwork.org

Cloud Security with AWS IAM

CH chadhaswayam@gmail.com



CH
chadhaswayam@gmail.c...
NextWork Student

Introducing today's project!

What is AWS IAM?

AWS IAM is a web service for securely controlling access to AWS resources. It enables you to create and control services for user authentication or limit access to a certain set of people who use your AWS resources.

How I'm using AWS IAM in this project

I used IAM today to create policies and user groups, which allowed a certain user to only perform actions on designated EC2 instances.

One thing I didn't expect...

One thing I didn't expect was the huge error you get when the user tries to stop an EC2 instance he doesn't have the permission for.

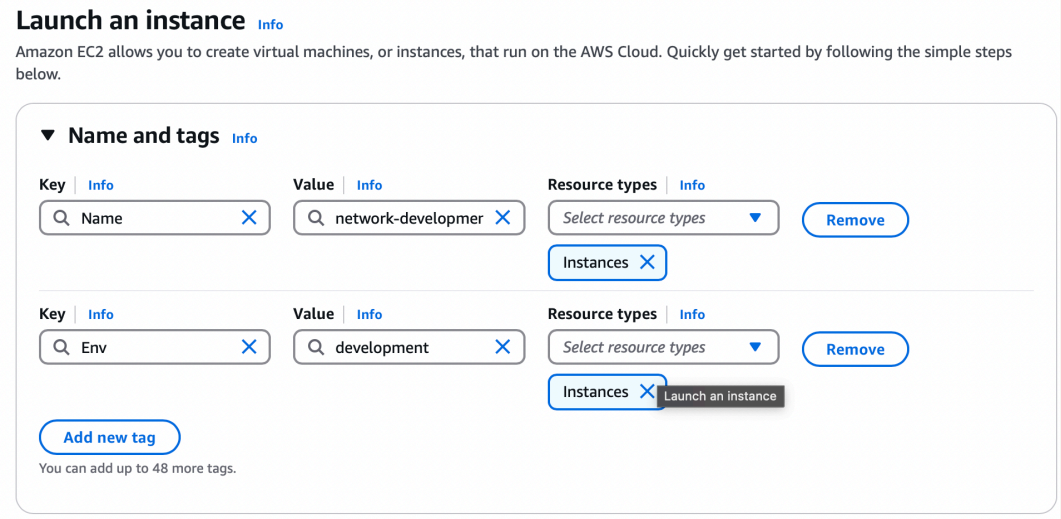
This project took me...

This project took me around an hour.

Tags

Tags are like labels you can attach to AWS resources for organization. This tagging helps us with identifying all resources with the same tag at once.

The tag I've used on my EC2 instances is called Env. The value I've assigned for my instances are production and development to differentiate between the two instances.



IAM Policies

IAM Policies are rules for who can do what with your AWS resources. It's about giving permissions to IAM users, groups, or roles, saying what they can or can't do on certain resources, and when those rules kick in.

The policy I set up

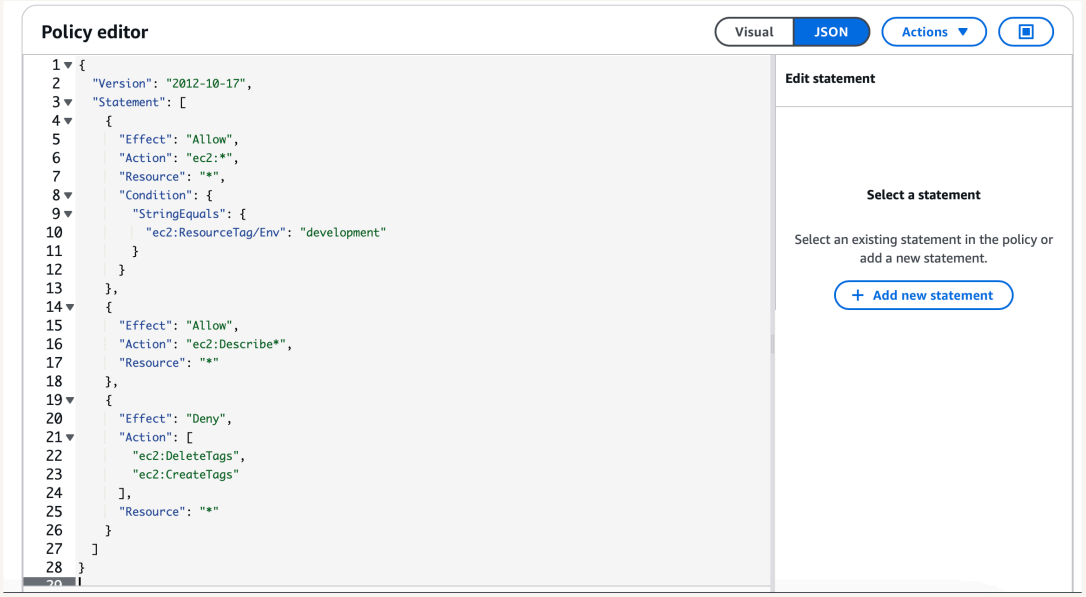
For this project, I've set up a policy using JSON.

I've created a policy that allows some actions (like starting, stopping, and describing EC2 instances) for instances tagged with "Env = development" while denying the ability to create or delete tags for all instances.

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

The Effect attribute of a JSON policy is whether a policy "allows" or "denies" a certain action, The Action attribute is a list of the actions allowed or denied and the Resource Attribute is which resources the policy applies to.

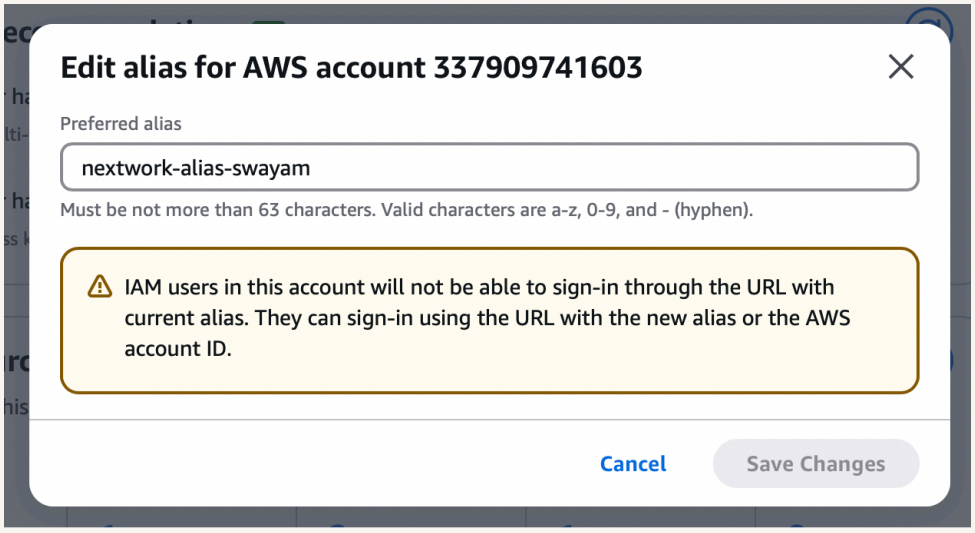
My JSON Policy



Account Alias

An account alias is a friendly name for your AWS-account that you can use instead of your account-id

Creating an account alias was really quick. Now, my new AWS console sign-in URL is https://nextwork-alias-swayam.signin.aws.amazon.com/console



IAM Users and User Groups

Users

IAM users are the people that will get access to your resources/AWS account.

User Groups

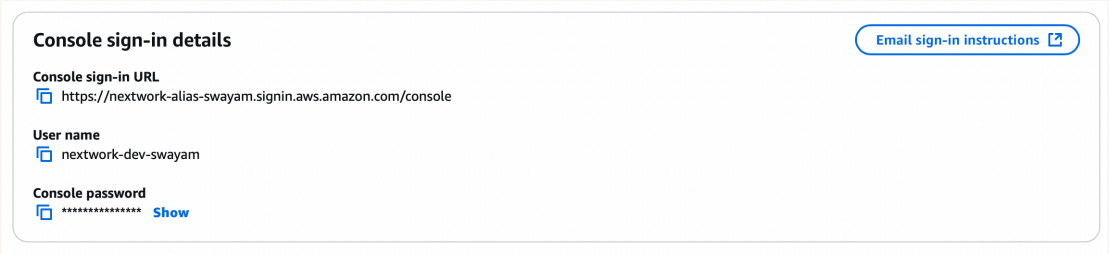
IAM user groups are a collection/folder of IAM users. It allows you to manage permissions for all the users in your group at the same time by attaching policies to the group rather than individual users.

I attached the policy I created to this user group, which means the users in this user group will now have the permissions associated with the Development Instance.

Logging in as an IAM User

The first way is to send an email with user login credentials and the second way is to share console Sign-in Link and Access Keys manually

Once I logged in as my IAM user, I noticed that some of my dashboard panels are showing Access denied already. This was because I can only access the resources I was given permission to.



Testing IAM Policies

'I tested my JSON IAM policy by first trying to stop my Production Instance. This was not possible because the JSON policy only allowed the user to make changes to the Development Instance.

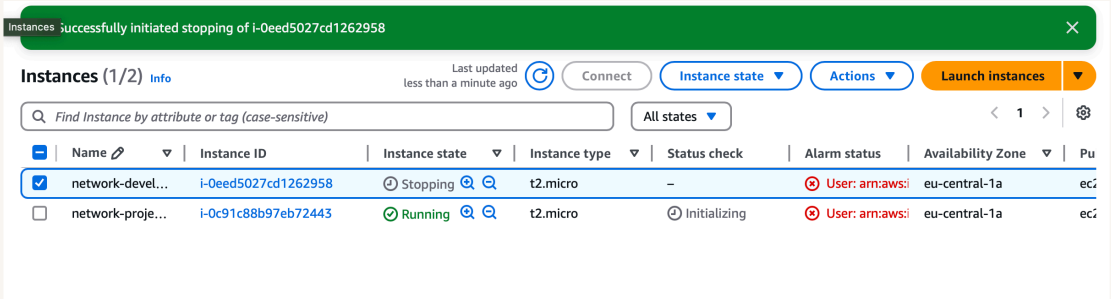
Stopping the production instance

When I tried to stop the production instance I recieved a huge error. This was because the user I created does not have the permission to stop the EC2 instance.

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance it was successfull. This was because the user had the permissions through the JSON ploicy to do so.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects