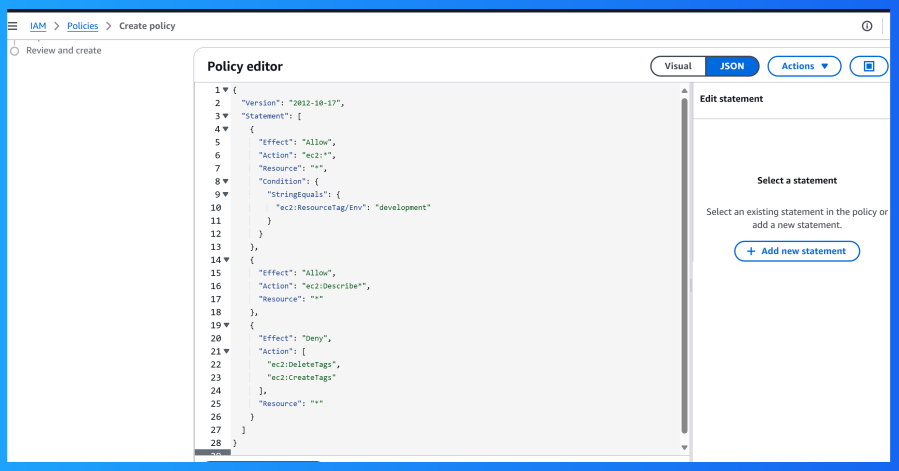
NextWork.org

Cloud Security with AWS IAM

MA mallangiharinathreddy727@gmail.com



MA
mallangiharinathreddy72...
NextWork Student
NextWork.org

Introducing today's project!

What is AWS IAM?

AWS IAM (Identity and Access Management) is a service provided by AWS to control who is authenticated (signed in) and authorized (has permissions) to use your account's resources.

How I'm using AWS IAM in this project

In today's project, I used IAM to create User Group,User and Policy for security purposes.

One thing I didn't expect...

one thing I didn't expect in this project was, when I am trying to stop the production instance, it thrown error.

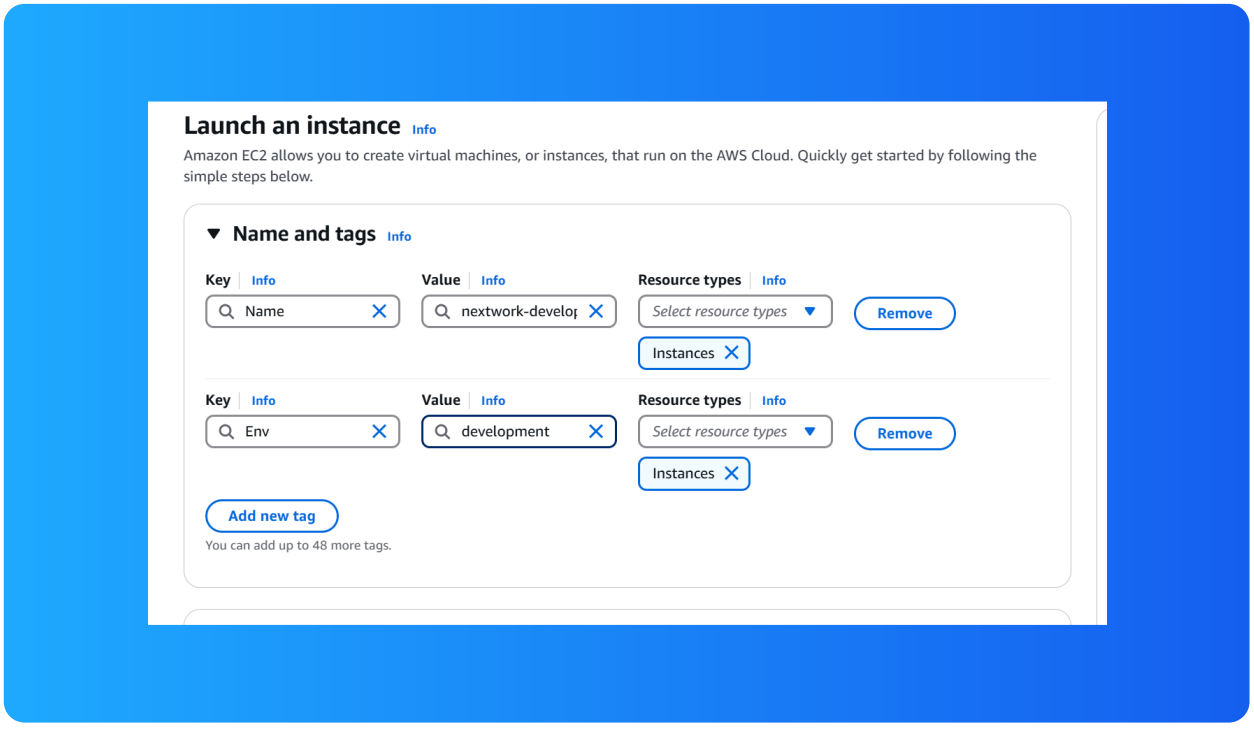
This project took me...

This project took me 2 Hours to complete include documentation.

Tags

Tags are Labels to help AWS Account users identify and manage their resources. Tags are useful for grouping, mass management and applying security policies.

The tag I've used on my EC2 instances is called Env.The value I've assigned for my instances are production, and development. This represents the two different environments that we are using to build and release the Nextwork App.



IAM Policies

IAM policies are rules for who can do what with your AWS resources. It's all 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 the JSON editor.

I've created a policy that allows all EC2 related actions to all EC2 instances that have the Environment("Env")tag "development".But it also denies creating and deleting tags for ALL EC2 instances.

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

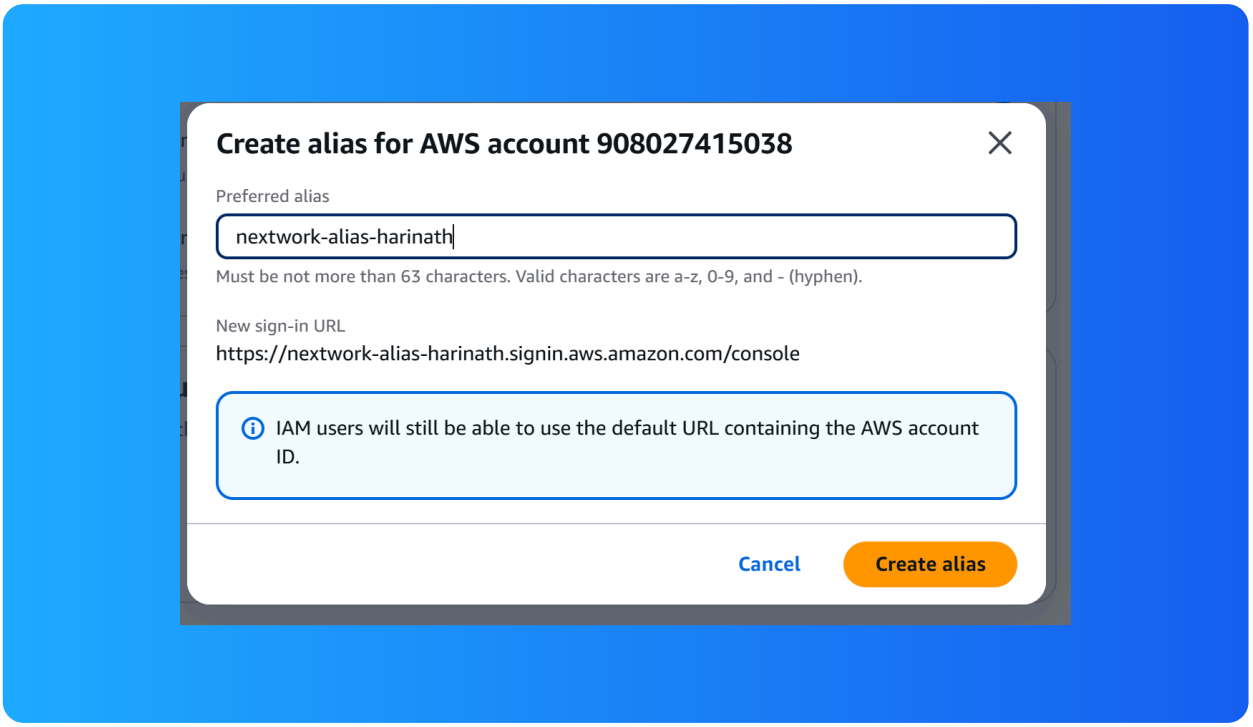
Effect: i.e. Allow or Deny. Action: i.e. The specific action that we are wanting to allow or deny. Resource: The specific resource/group of resources in my AWS Account that this policy will take effect on.

My JSON Policy

Account Alias

An account alias is a custom name that I can assign to my AWS account. This custom name would replace my ACCOUNT ID in my Account's log-in URL.

Creating an account alias took me less than a minute - super fast!. Now, my new AWS console sign-in URL is "https://nextwork-alias-harinath.signin.aws.amazon.com/console/"



IAM Users and User Groups

Users

IAM users are other log-ins/people who have access to my AWS Account. These users are created by myself using AWS IAM serivce! I can designate my user's access to my AWS Account's resources/services.

User Groups

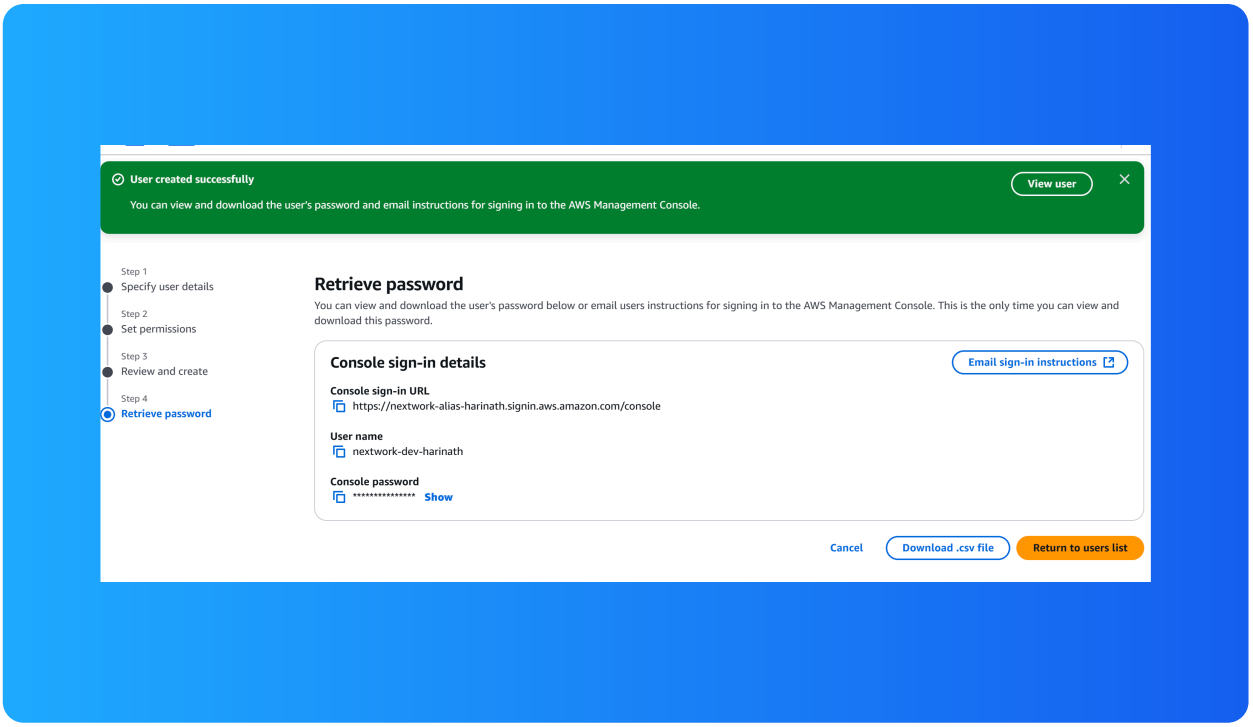
IAM user group is a collection/folder of IAM users. It allows you to manage permissions for all the users in your group at the same time by attaching policies to the group rather than individual users.

I attached the policy I created to this user group, which means all users that are added to that user group will automatically inherit the user group's access permissions.

Logging in as an IAM User

The first way is, Emailing sign-in instructions; second way is, Downloading.csv file.

Once I logged in as my IAM user,I noticed that a lot of panels displayed "Access Denied".This was the clear difference to the dashboard I usually see in my AWS account(where I had unrestricted access to resources and wasn't denied access to anything)

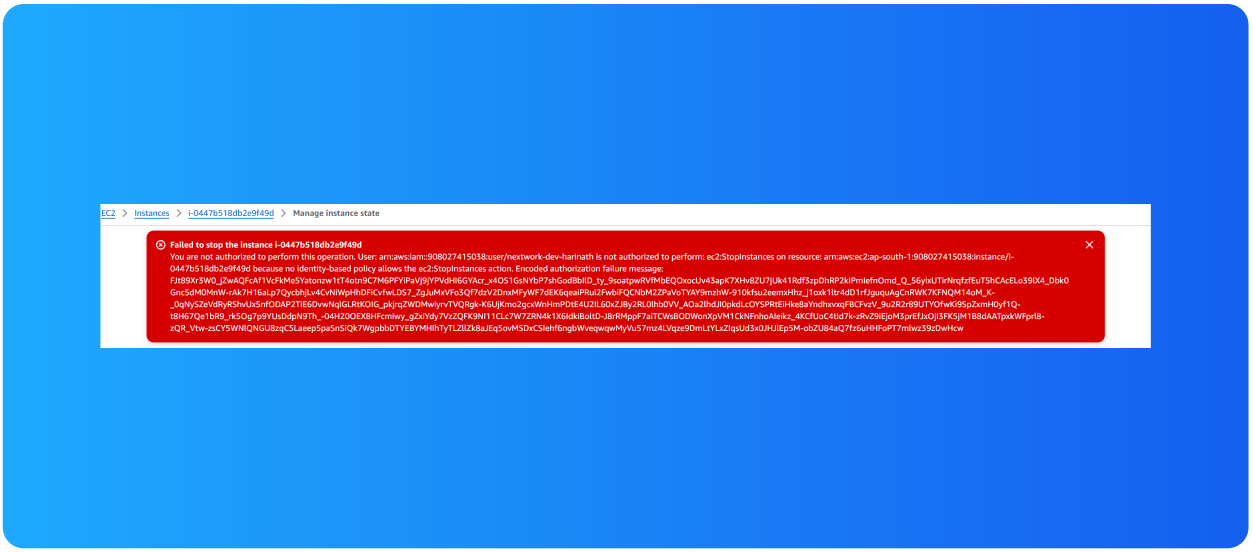


Testing IAM Policies

I tested my JSON IAM policy by trying to stop the development and production instances i.e. triggering the StopInstances action.

Stopping the production instance

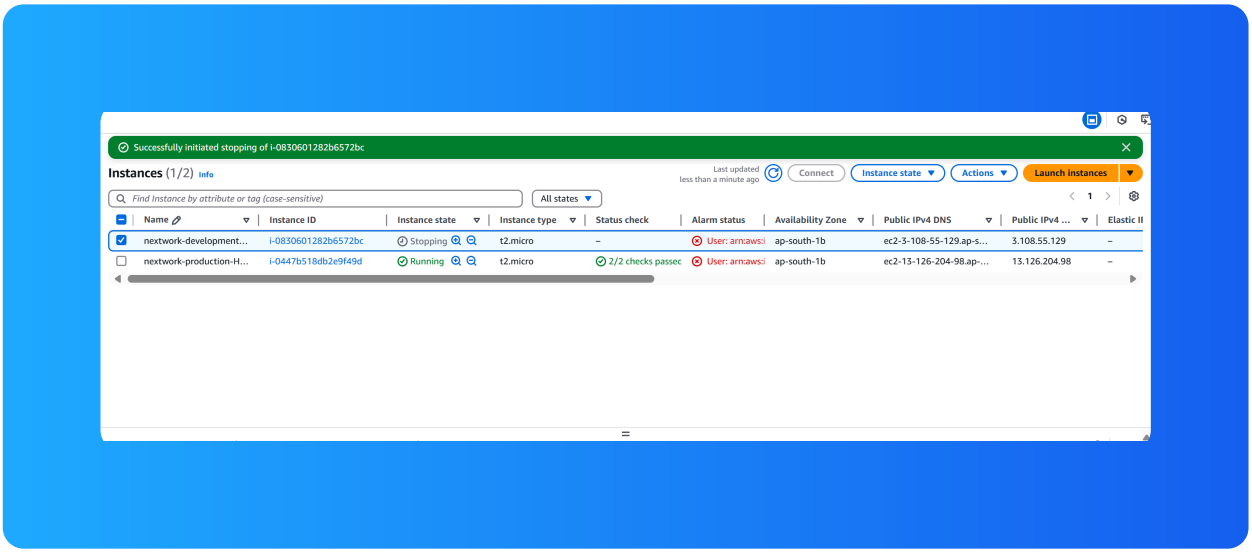
When I tried to stop the production instance an error message stopped me and explained that I am not authorized to stop the production instance.



Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, the development instance could be stopped! This was because the policy I created, allowed all EC2 related actions to all EC2 instances with/resources with the Env tag development.



Everyone should be in a job they love.

Check out nextwork.org for more projects