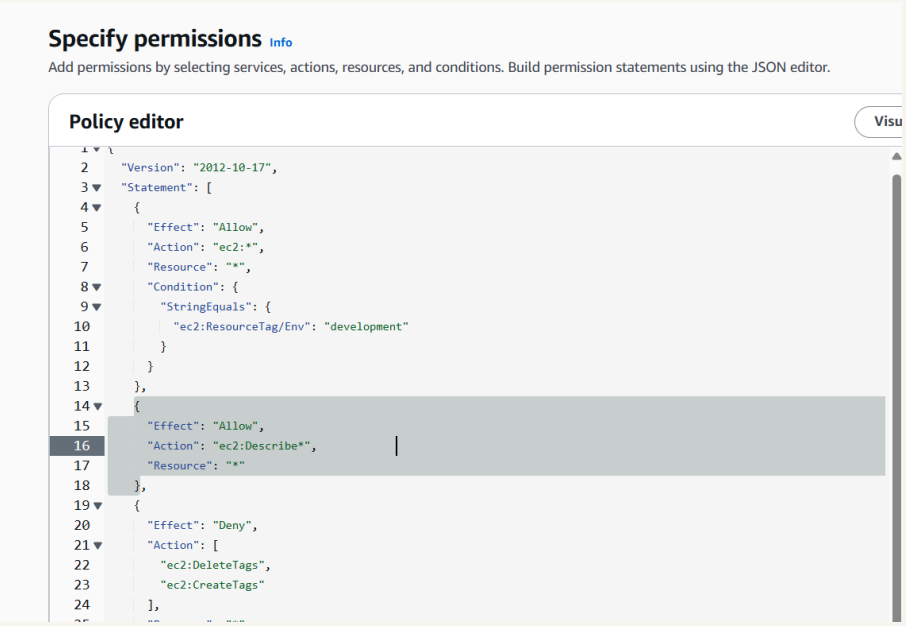
nextwork.org

Cloud Security with AWS IAM

DA davidramovichmandal@gmail.com



Introducing Today's Project!

In this project, I will demonstrate how to implement IAM policies and create user groups to control access to AWS resources. I'm doing this project to learn securing the AWS resources.

Tools and concepts

Services I used were EC2 and IAM. Key concepts I learnt include policy making , IAM user groups and roles , least privilege.

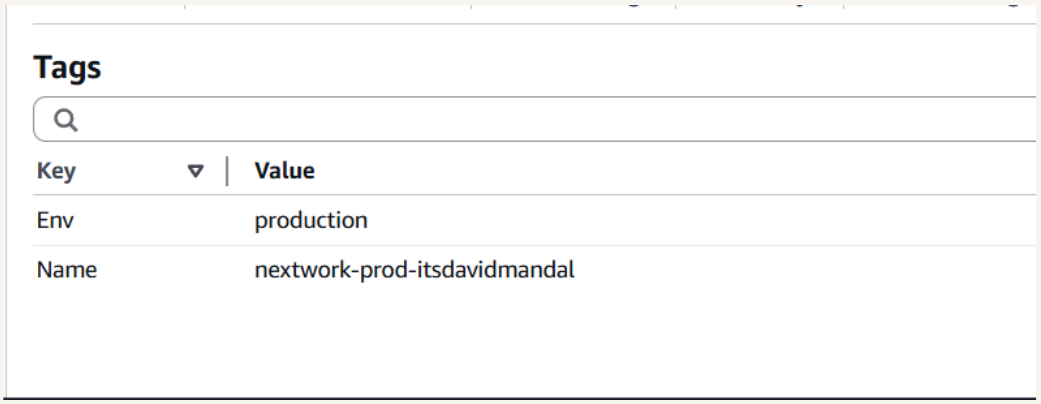
Project reflection

This project took me approximately 2 hrs.It was most rewarding to apply the theories studied into real world application.

Tags

Tags are metadata labels assigned to resources, such as EC2 instances, S3 buckets, or RDS databases which help organize, manage, and identify them. Each tag consists of a key and a value pair.

The tag I've used on my EC2 instances is called "Env" The value I've assigned for my instances are "production" and "dev"



IAM Policies

Policies in AWS define and enforce permissions for users, groups, or roles, controlling what actions they can perform on specific resources. Essentially, they answer the question, “Who can do what on which resources?"

The policy I set up

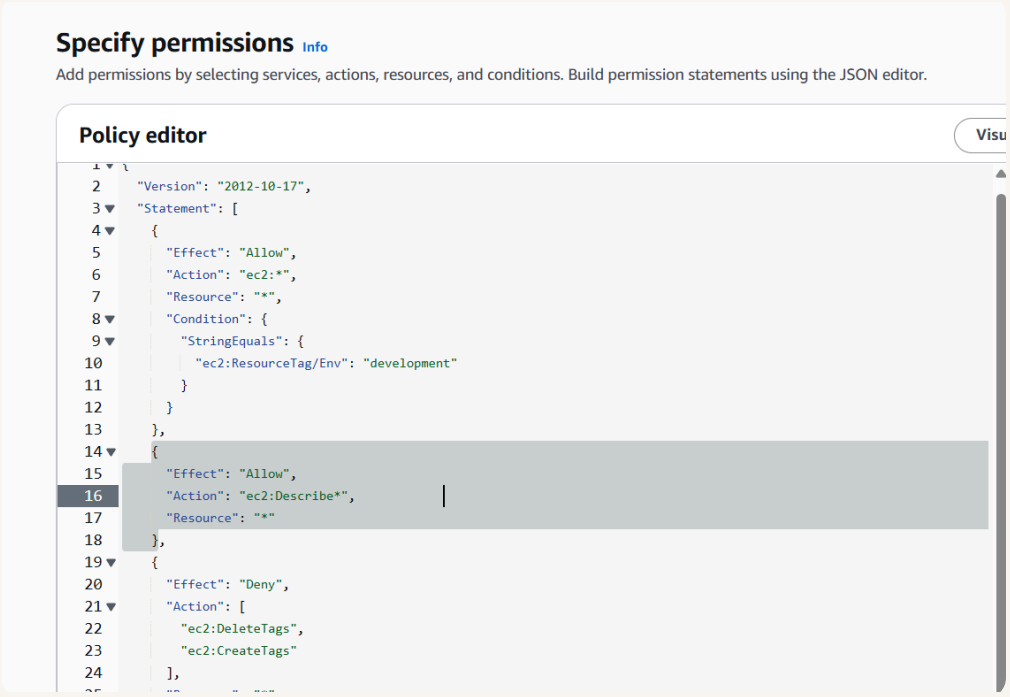
For this project, I’ve set up a policy using JSON

I’ve created a policy that lets the user fully manage EC2 instances tagged as development, view all EC2 resources, but prevents them from changing tags on any instance.policy that...

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

Effect specifies whether the policy allows or denies the actions listed. Action defines the specific operations that are permitted or denied. Resource identifies the AWS resources to which the actions apply, like a particular EC2 instance.

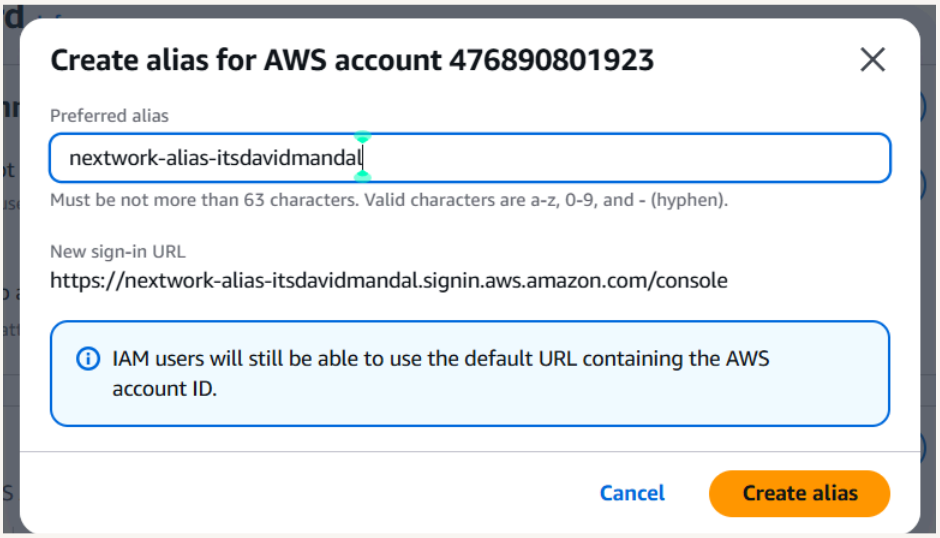
My JSON Policy



Account Alias

An account alias is a user-friendly name you can assign to your AWS account instead of using the default account ID, which is a long 12-digit number.

Creating an account alias took me just a minute. Now, my new AWS console sign-in URL is "https://nextwork-alias-itsdavidmandal.signin.aws.amazon.com/console"



IAM Users and User Groups

Users

An IAM user in AWS is an identity created within an AWS account to represent a person, application, or service that needs access to AWS resources.

User Groups

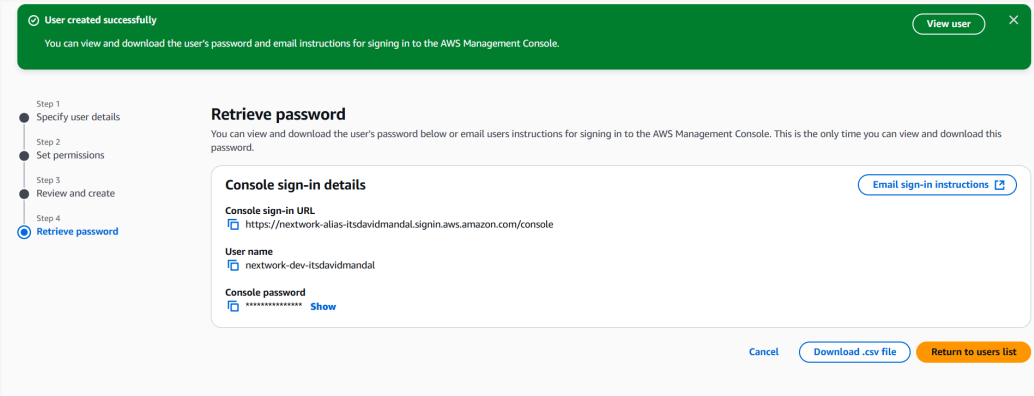
An IAM group is a collection of IAM users that allows you to manage permissions collectively rather than individually. Instead of assigning policies to each user separately, you attach policies to a group.

I attached the policy I created to this user group, which means that the users in this group can manage EC2 instances tagged as development, view all EC2 resources, but prevents them from changing tags on any instance.

Logging in as an IAM User

A new AWS IAM user's sign-in details can be shared in two main ways: via email or by providing a direct login URL with the username and temporary password.

Once I logged in as my IAM user, I noticed that some resources / functionalities were denied access. This was because of the policy inforcement.

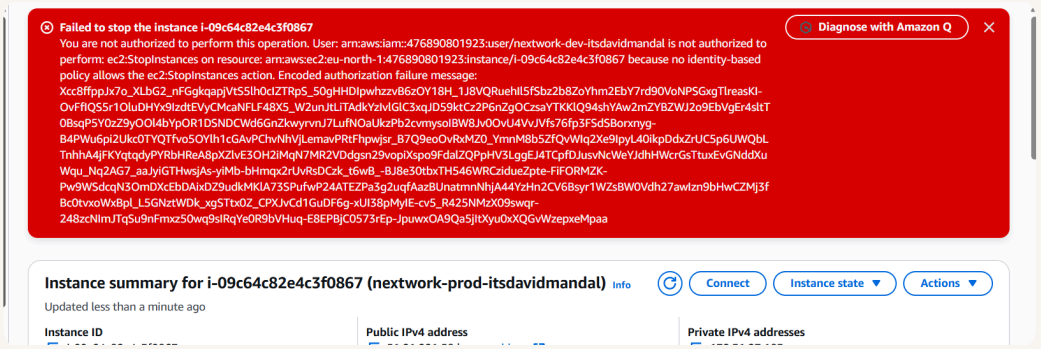


Testing IAM Policies

I tested my JSON IAM policy by trying to stop both the instances (prod and dev) . The instance with the tag Env=development was successfully deleted .

Stopping the production instance

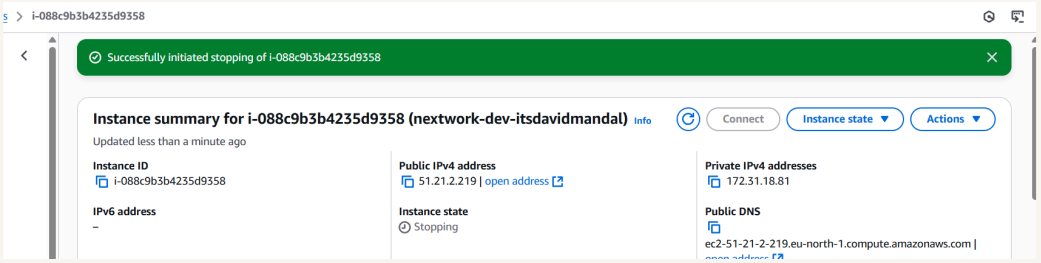
When I tried to stop the production instance I was stoped and given a warning. This was because the policy didn't allow me to stop the instances . The policy had mentioned that I can stop instances with the tag "Env=development"



Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance the instance with the tag Env=development was successfully deleted . This was because the policy has mentioned that I can delete instances with the tag Env=development



The place to learn & showcase your skills

Check out nextwork.org for more projects