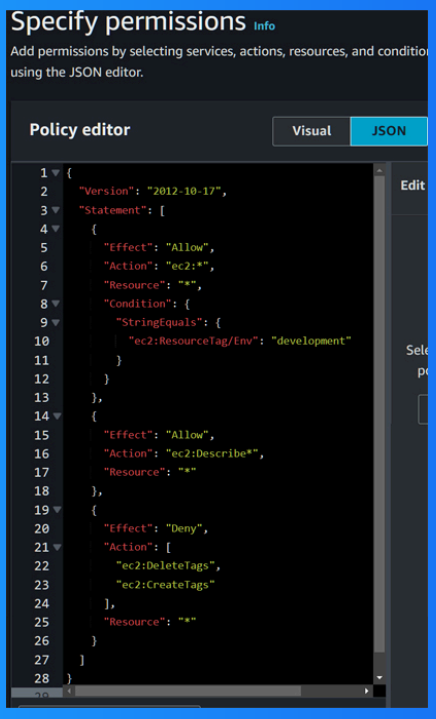
NextWork.org

Cloud Security with AWS IAM

EL elena@kroupkin.com



EL
elena@kroupkin.com
NextWork Student

Introducing today's project!

What is AWS IAM?

AWS IAM (Identity and Access Management) is a service that allows you to securely control access to AWS resources. It helps you manage users, groups, and permissions within your AWS account.

How I'm using AWS IAM in this project

I used AWS IAM to: 1.Create IAM groups 2.Create IAM user 3.Develop IAM policies 4.Attach policies to users and groups 5.Test IAM policies

One thing I didn't expect...

I didn't realize there was an IAM Policy Simulator. This tool would have been incredibly useful for testing policy outcomes without affecting live resources. It's definitely something to keep in mind for future projects.

This project took me...

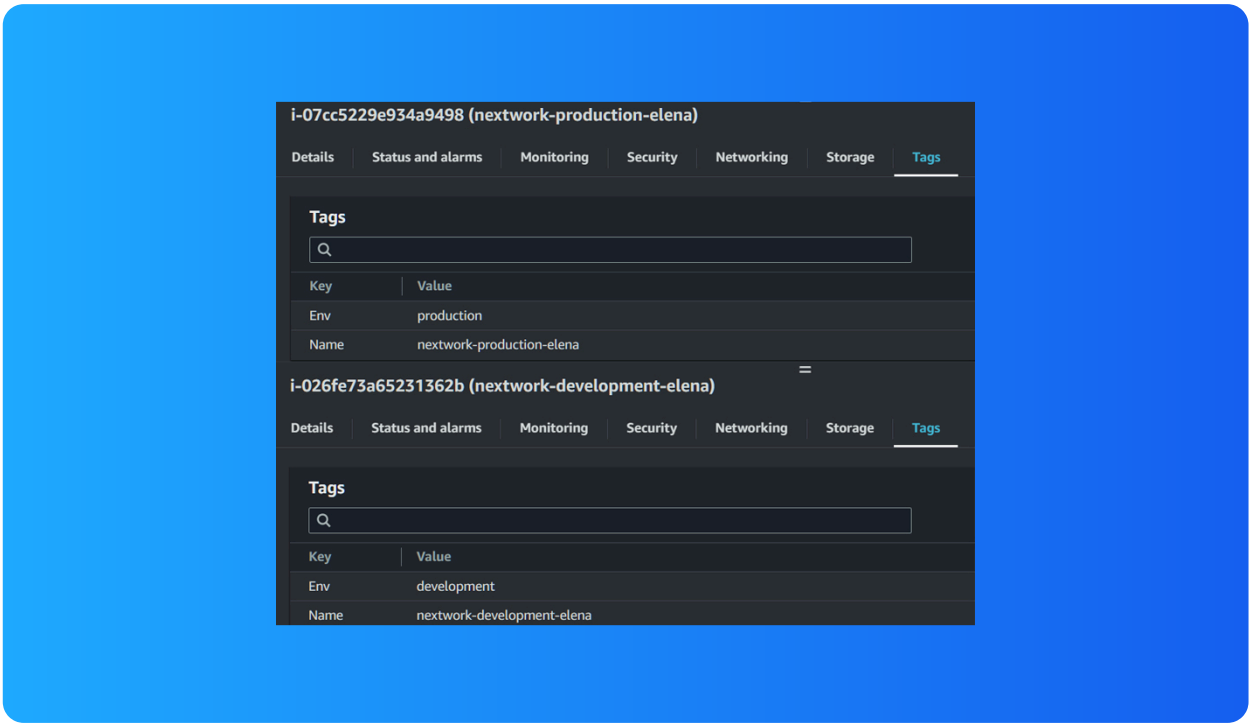
This project took approximately 2.5 hours to complete.

EL
elena@kroupkin.com
NextWork Student

Tags

Tags are user-defined key-value pairs that you can assign to AWS resources like EC2 instances, S3 buckets, and more. They're essentially metadata that you attach to your resources for better organization and management.

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



EL
elena@kroupkin.com
NextWork Student

IAM Policies

IAM Policies are the foundation of access control in AWS. They act as rules that dictate who can do what, and under which conditions, within your AWS environment.

The policy I set up

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

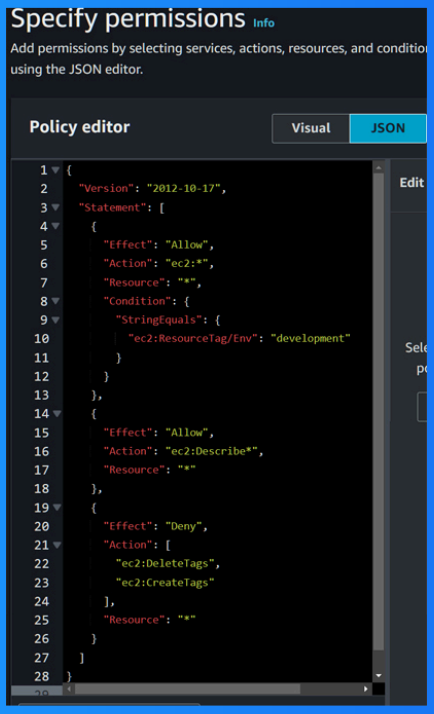
I've created a policy that provides broad EC2 permissions specifically for resources tagged as "development" while maintaining read-only access to all EC2 resources and protecting tags from modification.

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

Effect: allows or denies access. It can be either "Allow" or "Deny". Action: permits or prohibits action. In the format of "<service>:<action>", such as "ec2:StartInstances" or "s3:GetObject". Resource: Identifies the affected AWS resource(s).

EL
elena@kroupkin.com
NextWork Student

My JSON Policy



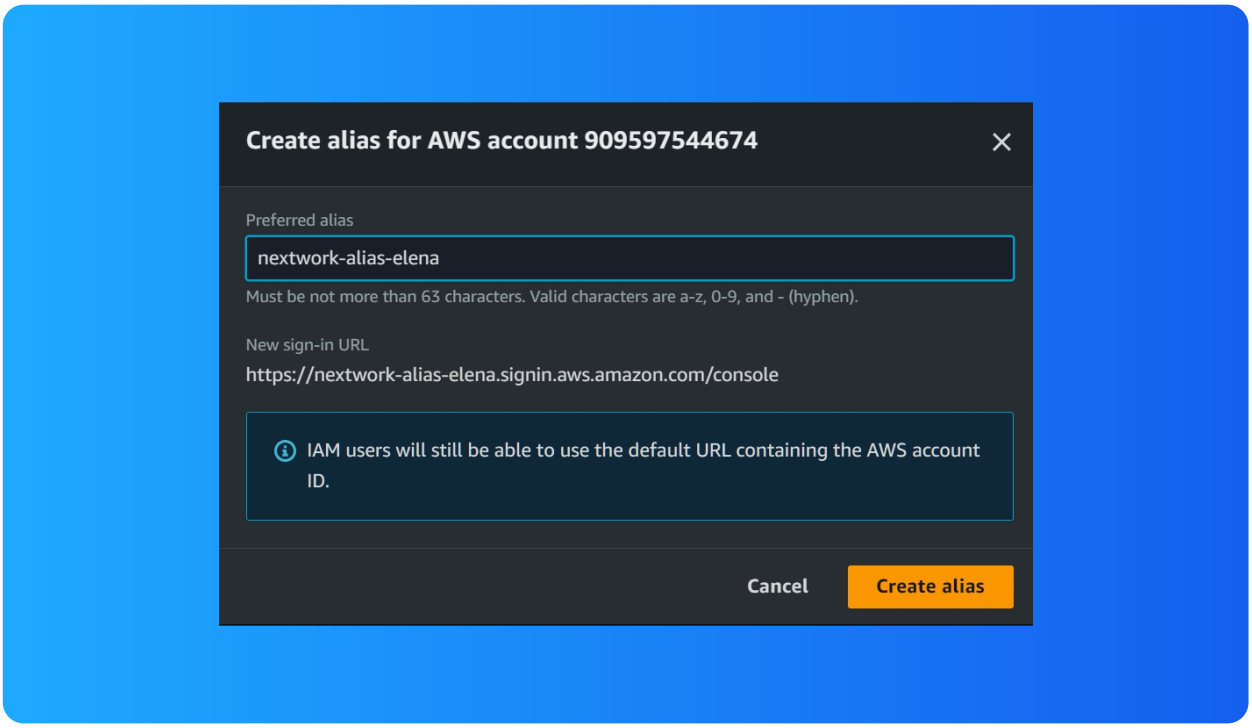
EL
elena@kroupkin.com
NextWork Student

Account Alias

An account alias is a user-friendly name assigned to a unique account number. It's like a nickname for your account, making it easier to identify and manage.

Creating an account alias took me one click. It's a quick and easy process.

Now, my new AWS console sign-in URL is https://nextwork-alias-elena.signin.aws.amazon.com/console



EL
elena@kroupkin.com
NextWork Student

IAM Users and User Groups

Users

IAM users are individual identities within an AWS account that can be used to access and manage AWS resources. They represent people or applications that need to interact with AWS services.

User Groups

IAM user groups are collections of IAM users that share common permissions. By assigning permissions to a group, you can efficiently manage access for multiple users without having to configure permissions individually.

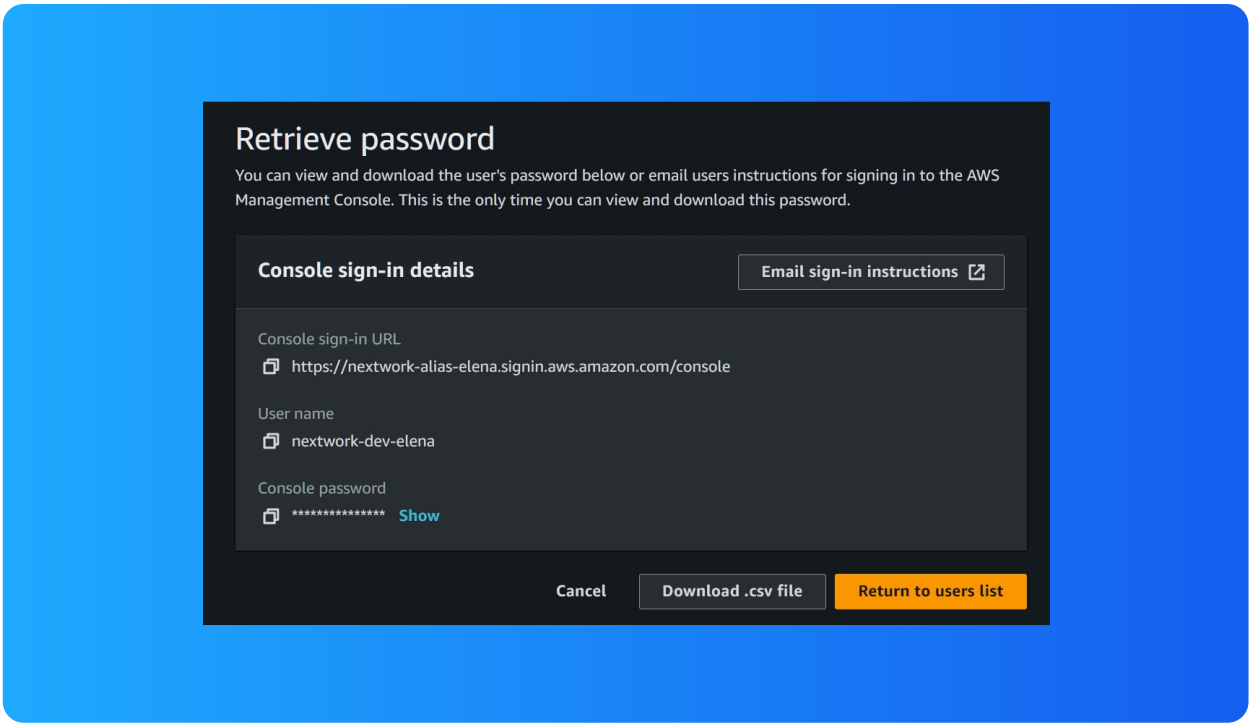
I attached the policy I created to this user group, which means all users within that group now have the permissions defined in the policy.

EL
elena@kroupkin.com
NextWork Student

Logging in as an IAM User

The first way is to generate a temporary password in the AWS Management Console. The second way is to send a secure email with sign-in credentials (less secure).

Once I logged in as my IAM user, I noticed a restricted dashboard with limited access. There were guides for using the main UI buttons, but many areas were inaccessible with "Access Denied" messages.



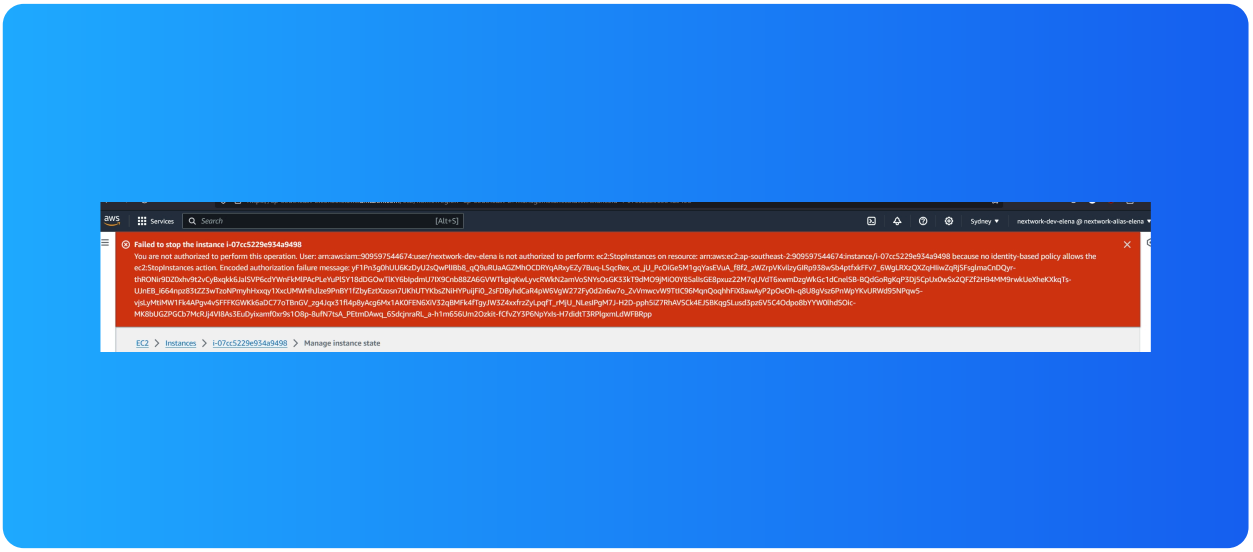
EL
elena@kroupkin.com
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by stopping the EC2 instance from the Production and Development environments

Stopping the production instance

When I tried to stop the production instance, an error message indicated insufficient permissions. This was expected, as my IAM policy only allows actions on EC2 instances tagged with "Env": "development".

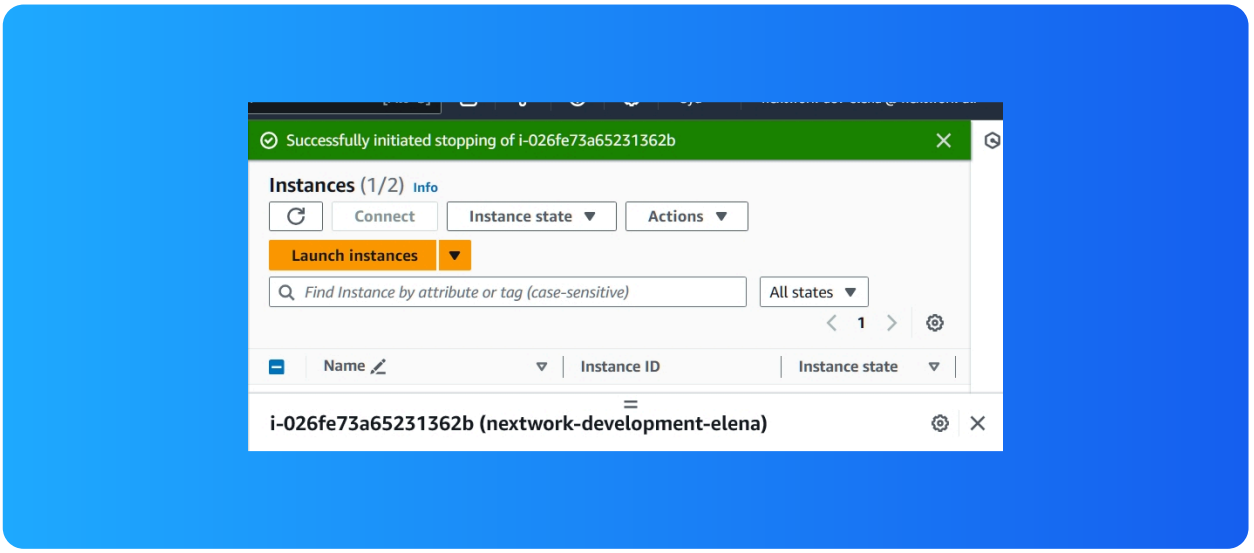


EL
elena@kroupkin.com
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, the Stop action worked as expected. This confirmed that the IAM policy was correctly granting permissions for EC2 instances tagged with "Env": "development".



Everyone should be in a job they love.

Check out nextwork.org for more projects