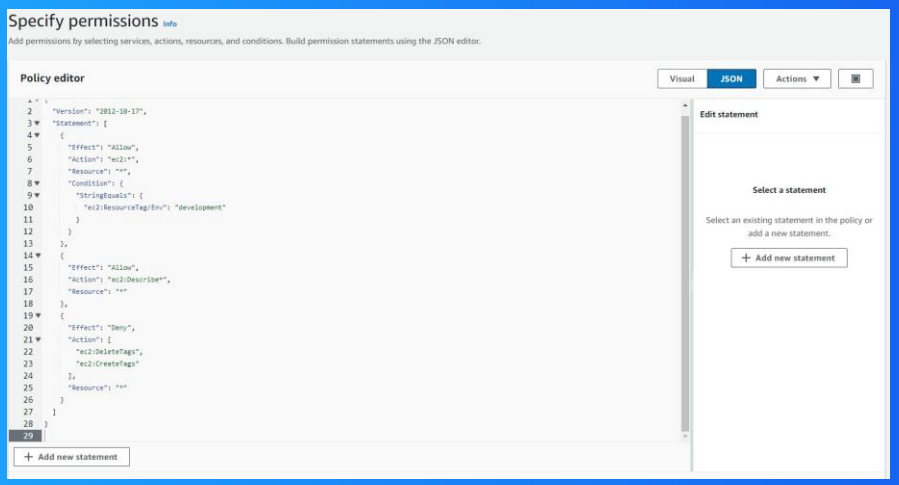
NextWork.org

Cloud Security with AWS IAM

James Francis Facistol



James Francis “Jae” Facistol
NextWork Student
NextWork.org

Introducing today's project!

What is AWS IAM?

AWS IAM is a service that enables you to manage users, permissions, and roles securely in AWS. It's useful for controlling access to resources, ensuring security, and following best practices for user management in cloud environments.

How I'm using AWS IAM in this project

In today’s project, I used AWS IAM to create user roles with specific permissions, ensuring secure access to resources. I configured policies to control access levels, enabling users to work effectively while maintaining security best practices.

One thing I didn't expect...

I didn't expect this project to be so easy. My background in Linux administration has really helped me grasp the concepts behind cloud services.

This project took me...

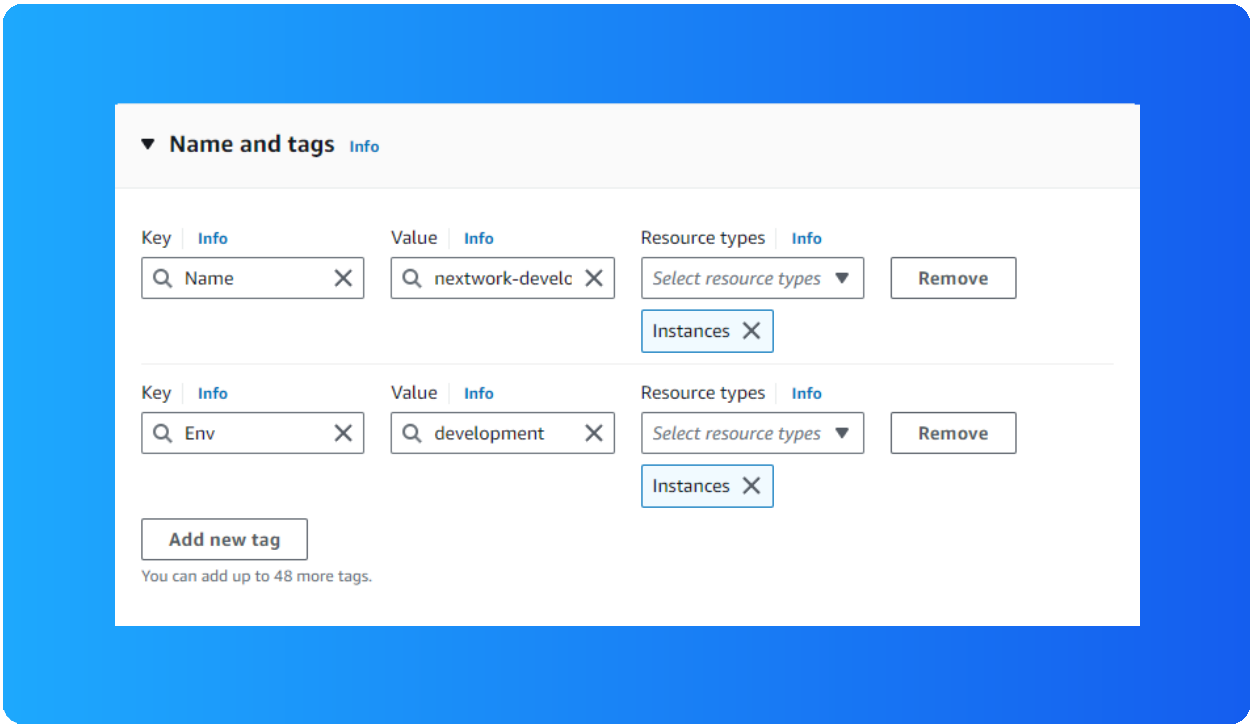
This project took me about an hour and a half as I focused on fully understanding the material.

James Francis “Jae” Facistol
NextWork Student

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.

I’ve tagged my EC2 instances with "Env," assigning the values "production" and "development" to represent the two environments for building and releasing our new app.



James Francis “Jae” Facistol
NextWork Student
NextWork.org

IAM Policies

IAM Policies are rules that help to allow/deny users'/resources' permissions to perform certain actions to my AWS Account's resources.

The policy I set up

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

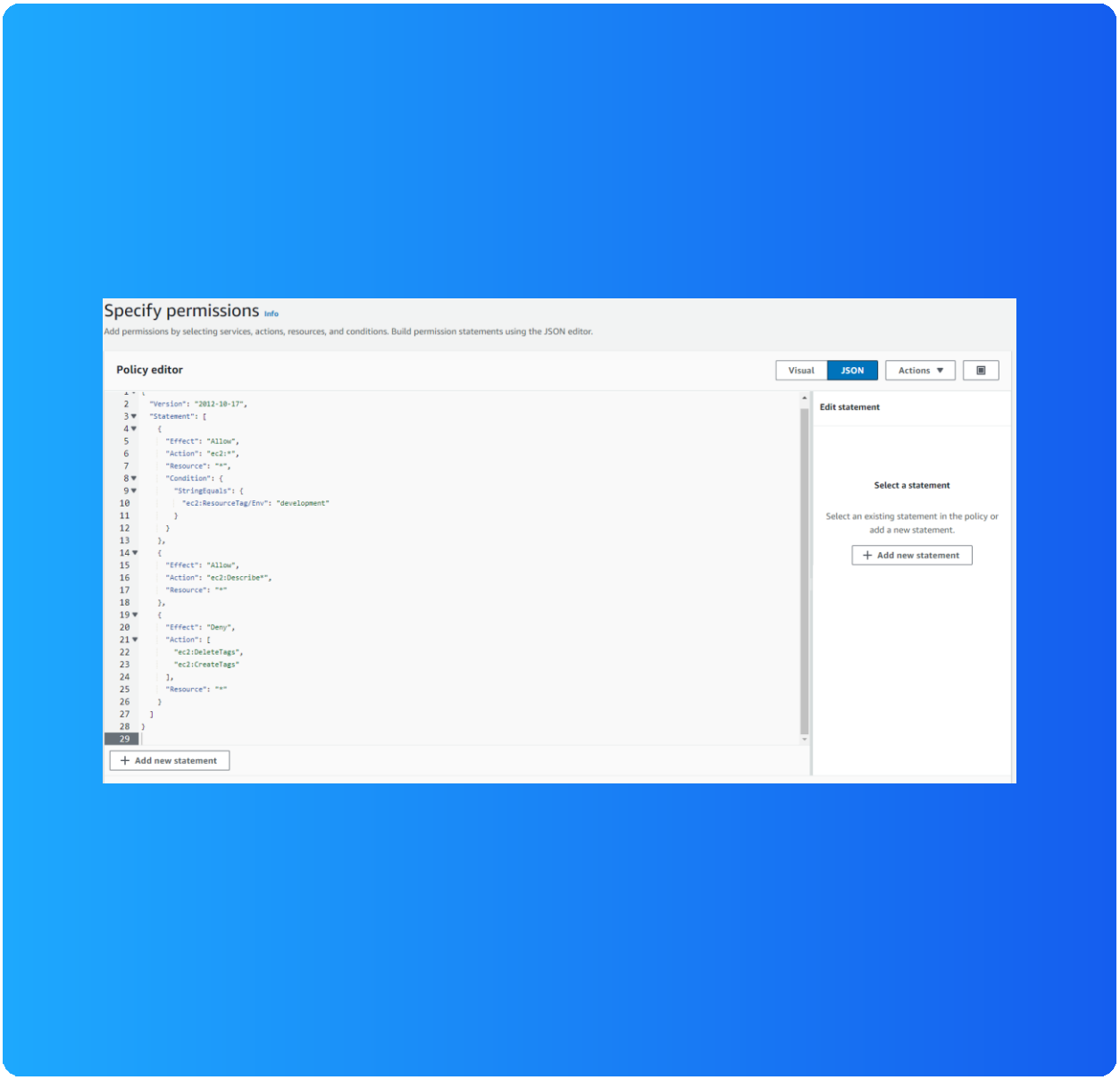
I’ve created a policy that allows all EC2-related actions for instances tagged with "Env" set to "development." Additionally, it denies the ability to create or delete tags for all EC2 instances.

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

JSON policy attributes are: Effect: Specifies if the action is allowed or denied. Action: Defines the specific action. Resource: Identifies the resource or group affected.

James Francis “Jae” Facistol
NextWork Student

My JSON Policy



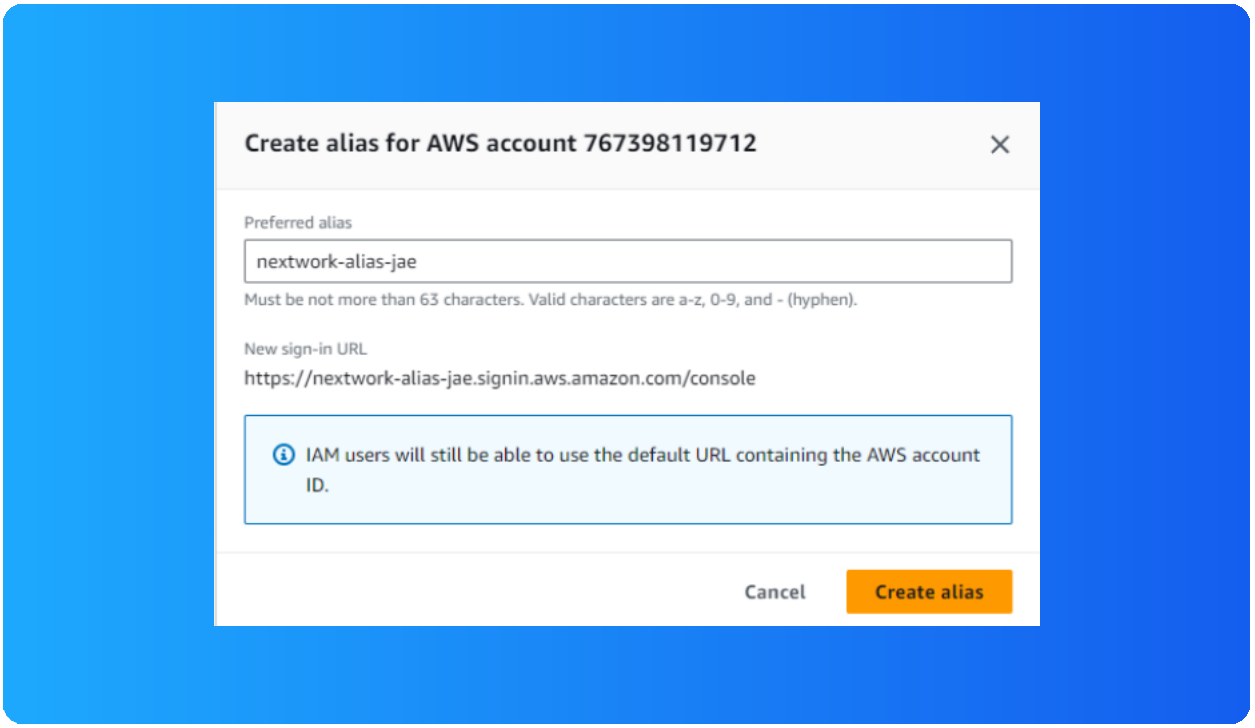
James Francis “Jae” Facistol
NextWork Student

Account Alias

An account alias is a custom name assigned to your AWS account that replaces the account ID in the login URL.

Creating an account alias took me less than a minute - it is really easy and super-fast.

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



James Francis “Jae” Facistol
NextWork Student
NextWork.org

IAM Users and User Groups

Users

IAM users are individual accounts within AWS Identity and Access Management (IAM) that enable users to securely access and manage AWS resources. Each IAM user has specific permissions and credentials.

User Groups

IAM user groups are collections of IAM users that allow you to manage permissions collectively. By assigning permissions to a group, you can easily control access for multiple users at once.

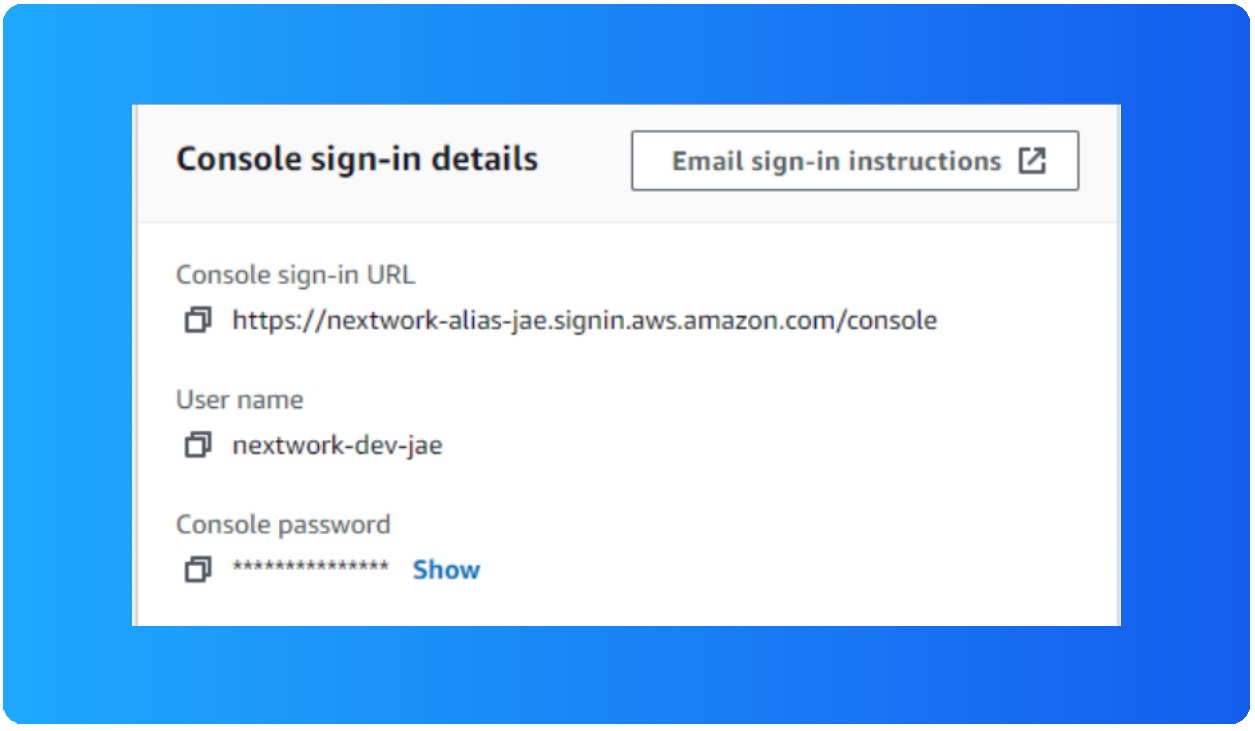
I attached the policy to this user group, so all members inherit its permissions. This simplifies management, as any changes to the policy automatically affect everyone in the group.

James Francis “Jae” Facistol
NextWork Student
NextWork.org

Logging in as an IAM User

The first way is to send the user an email containing their sign-in details securely. The second way is to provide the details via a secure messaging platform or a password manager that both you and the user have access to.

Once I logged in as my IAM user, I noticed that the dashboard was tailored to my permissions, providing access only to the resources relevant to my role. This made navigation easier and enhanced security by limiting exposure to unnecessary features.



Testing IAM Policies

I tested the JSON IAM policy I created by attempting to stop the development and production instances, specifically by triggering the StopInstances action.

Stopping the production instance

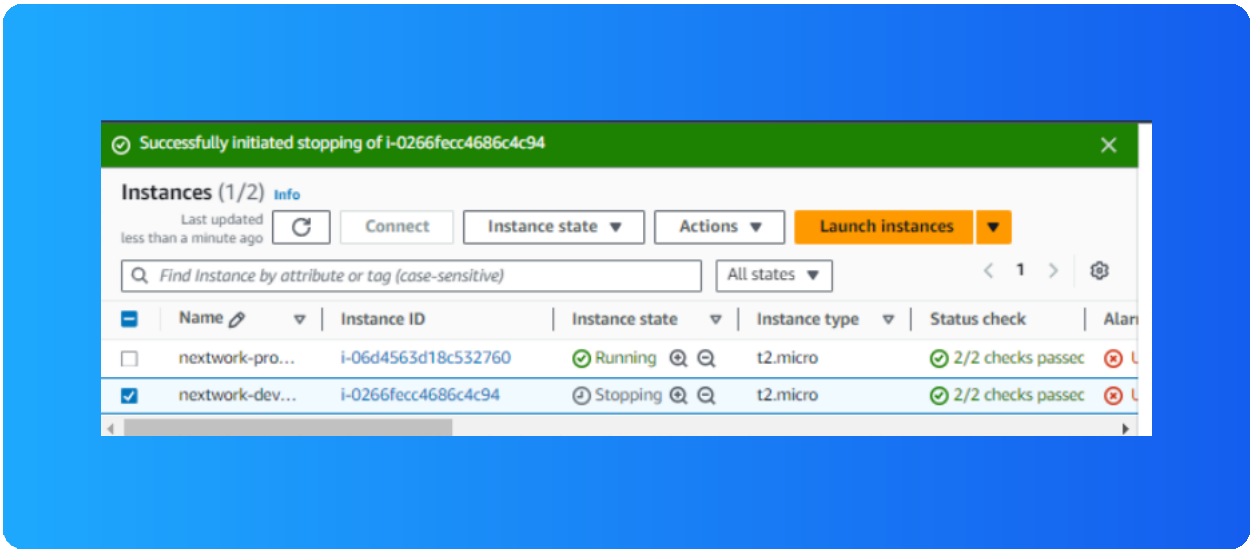
When I tried to stop the production instance, I got a permissions error, indicating my IAM policy didn’t grant the necessary access, so I wasn’t authorized to stop it.

James Francis “Jae” Facistol
NextWork Student

Testing IAM Policies

Stopping the development instance

I successfully stopped the development instance because my policy allowed all EC2 actions on instances tagged with "Env: development," which I attached to my user group.



Everyone should be in a job they love.

Check out nextwork.org for more projects