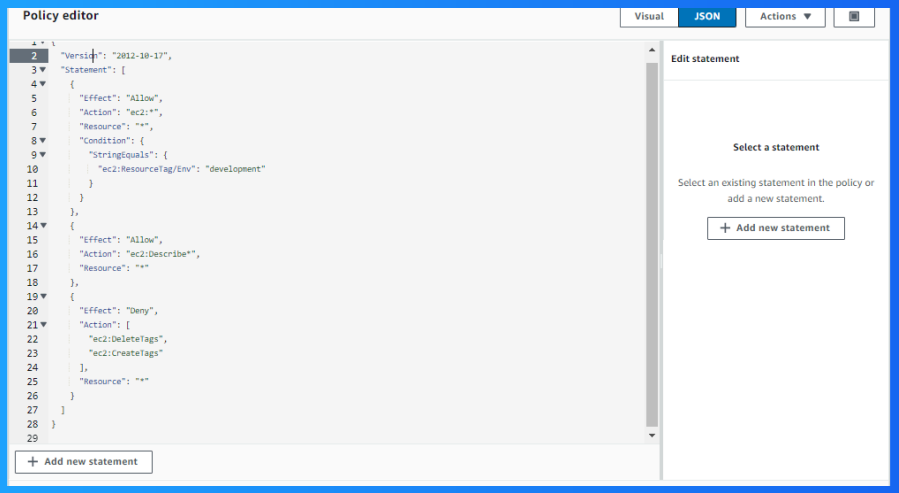
NextWork.org

Cloud Security with AWS IAM

Roshan Thomas



Roshan Thomas
NextWork Student

NextWork.org

Introducing today's project!

What is AWS IAM?

AWS IAM (Identity and Access Management) is your cloud bouncer! It controls who can do what in your AWS environment. By giving secure, granular access to AWS services, it keeps your data safe and ensures only the right folks have access.

How I'm using AWS IAM in this project

I used AWS IAM to create and manage user access policies, ensuring only authorized individuals can perform specific actions within our AWS environment. This included setting up roles and permissions for secure and efficient access management.

One thing I didn't expect...

One thing I didn't expect in this project was how granular and flexible the IAM policies can be. It allowed us to fine-tune access controls with precision, ensuring enhanced security and compliance effortlessly.

This project took me...

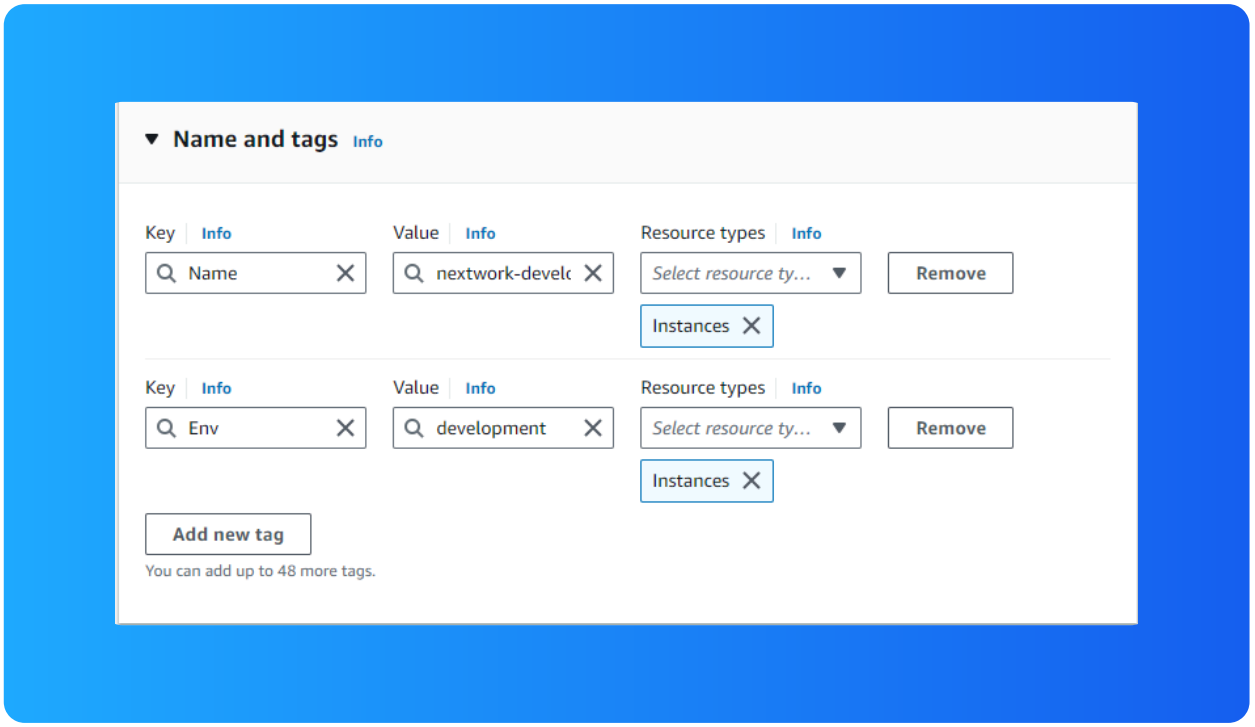
I took about 30 minutes

Roshan Thomas
NextWork Student

Tags

Tags are labels for AWS resources that aid in organization. They help identify resources with the same tag, manage cost allocation, and apply policies based on environment types.

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



Roshan Thomas
NextWork Student

IAM Policies

IAM Policies are rule 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 should be triggered.

The policy I set up

For this project, I've set up a policy using the JSON method. This setup makes resource management fun and efficient by ensuring proper tagging and policy application based on environment types, enhancing both security and organization.

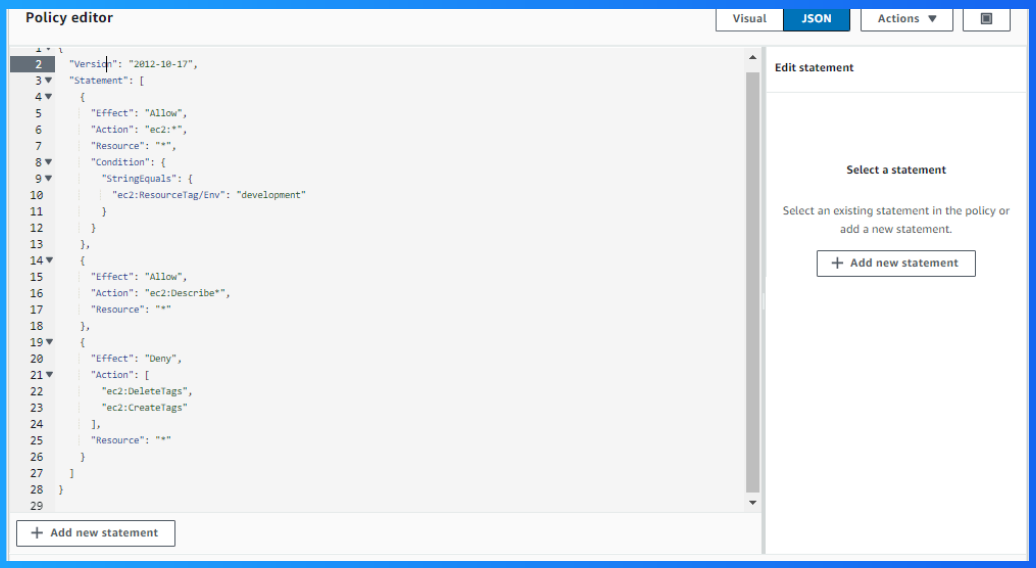
I've created a policy that allows all EC2 actions for resources tagged as "development," permits describing any EC2 resources, and denies the ability to create or delete tags on any resource. This ensures better control and organization.

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

The Effect, Action, and Resource attributes of a JSON policy specify what the policy does. "Effect" indicates allow or deny, "Action" defines what actions are permitted or denied, and "Resource" specifies the resources the policy applies to.

Roshan Thomas
NextWork Student

My JSON Policy



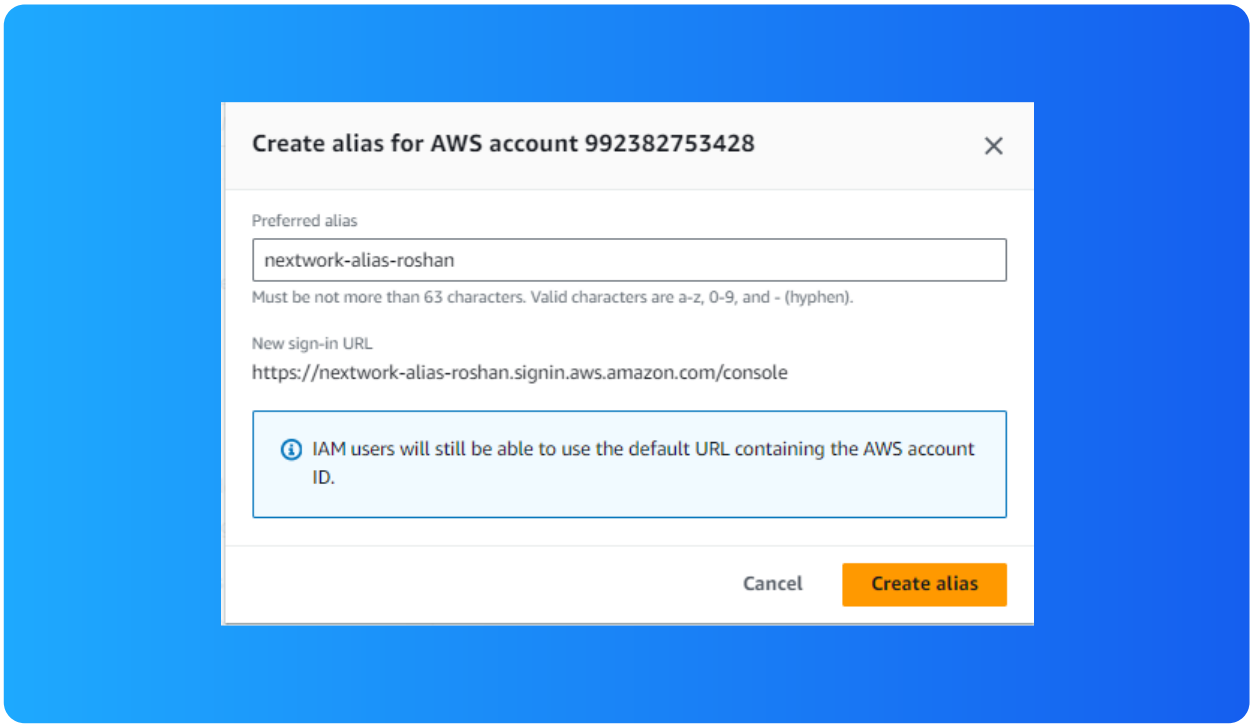
Roshan Thomas
NextWork Student

Account Alias

An account alias is a friendly name for your AWS account that replaces the numeric ID. It makes the login URL easier to remember and share like https://Your_Account_Alias.signin.aws.amazon.com/console/ ideal for team use such as welcoming new interns

Creating an account alias took me about 10 seconds.

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



Roshan Thomas
NextWork Student

IAM Users and User Groups

Users

IAM users are the VIPs of the cloud world, each with their own backstage pass! They control access to your AWS resources, making sure only the right people get to perform the right tasks.

User Groups

IAM user groups are like clubs for your cloud! They let you organize users and control their permissions, making sure only the right people get access to your precious resources.

Attaching the policy to your user group means I've just granted everyone in that group access to all the cool stuff the policy covers! It's like giving my squad the ultimate VIP pass

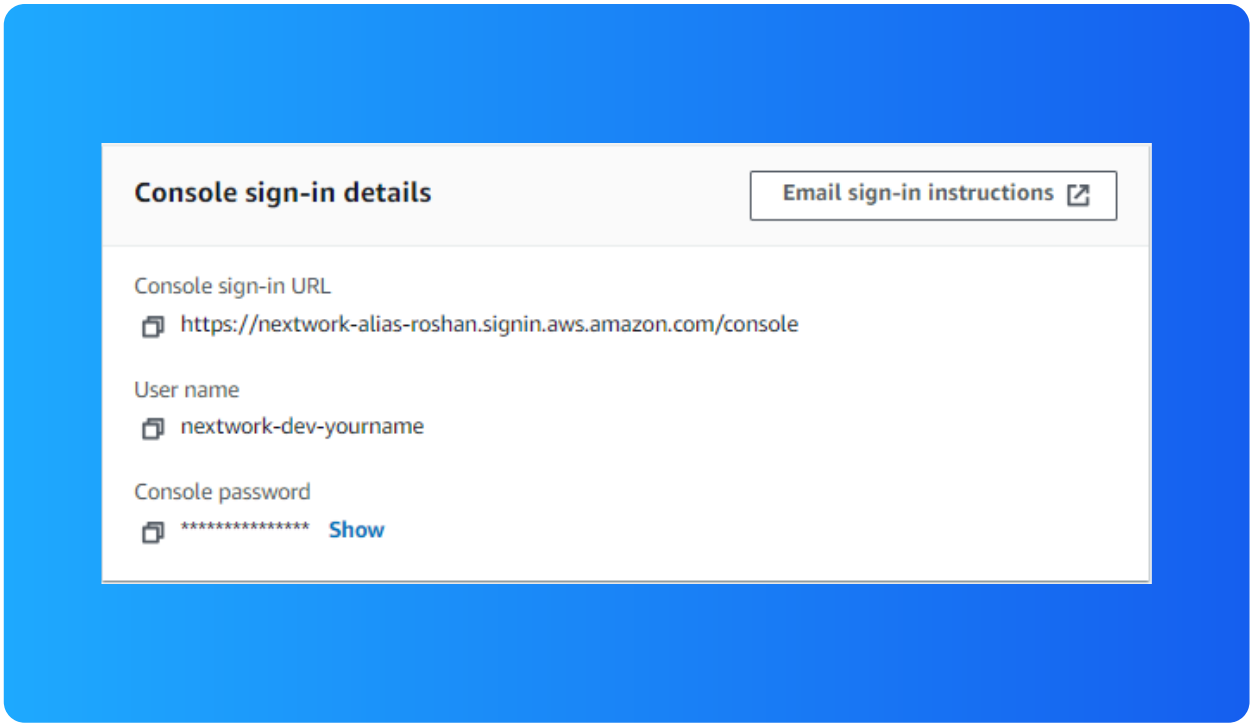
Roshan Thomas
NextWork Student

NextWork.org

Logging in as an IAM User

The first way is to email the user their sign-in details with a warm welcome message and instructions to get started. The second way is to provide the details through a secure messaging app, ensuring they receive it instantly and safely.

Once I logged in as my IAM user, I noticed that AWS console will treated me as someone that is starting from 0.



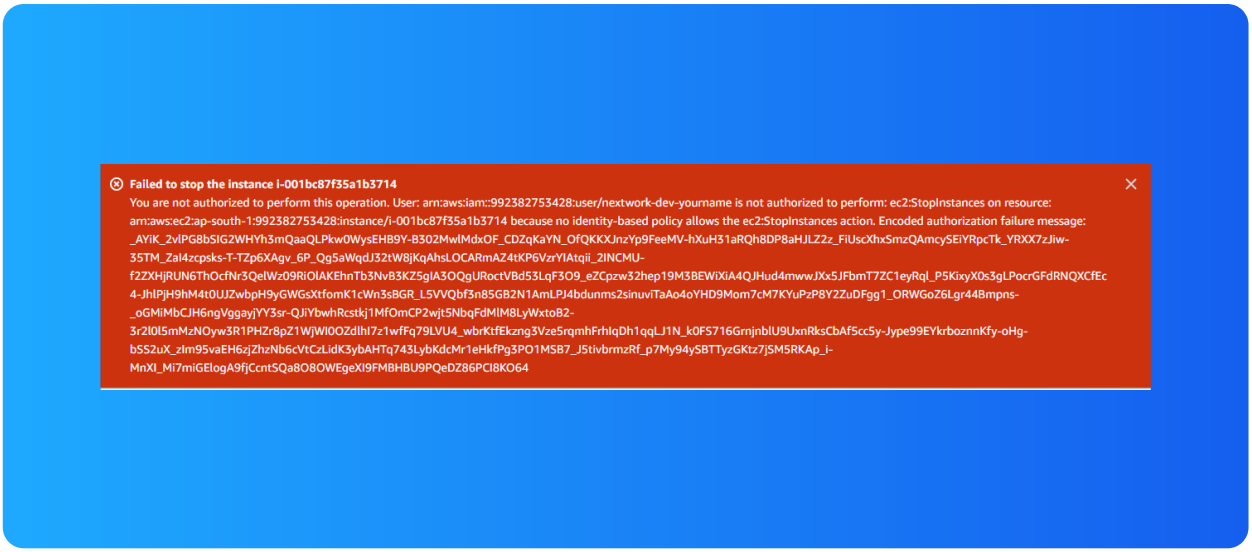
Roshan Thomas
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by trying to Stop the development and production instances i.e. triggering the StopInstance 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.

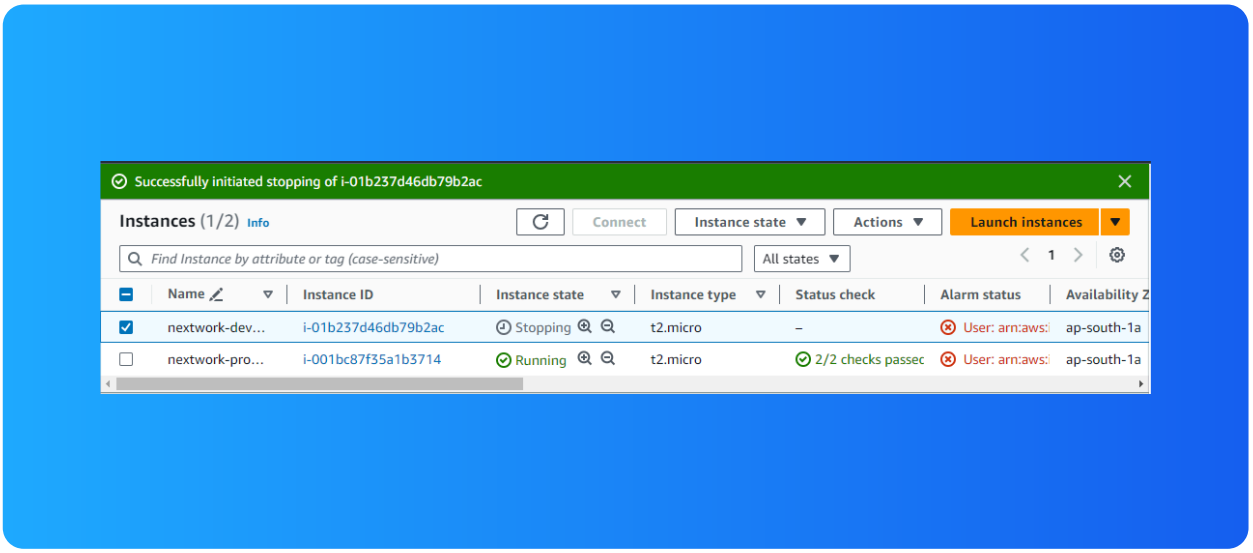


Roshan Thomas
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance could be stopped! This is because the Policy I created allowed all EC2 instance/resources with the Env tag development.



Everyone should be in a job they love.

Check out nextwork.org for more projects