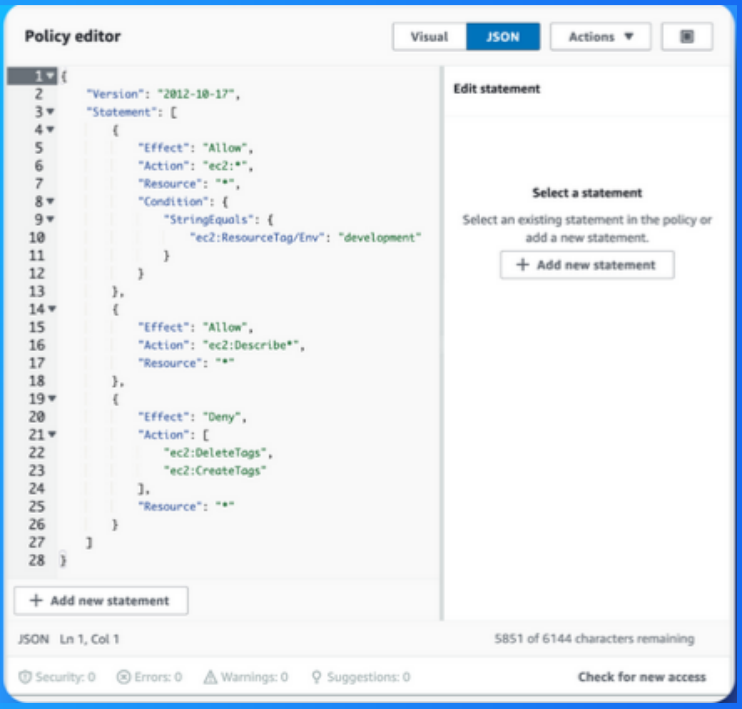
NextWork.org

Cloud Security with AWS IAM

Vishnu Kv



Vishnu Kv
NextWork Student

Introducing today's project!

What is AWS IAM?

IAM stands for Identity and Access Management. We can use AWS IAM to manage the access level that other users and services have to our resources.

How I'm using AWS IAM in this project

I used AWS IAM to simulate giving Access to a user to my instances, while restricting the user to not modify certain instances. This was useful to learn IAM and JSON IAM policies .

One thing I didn't expect...

I didn’t expect tags to be so useful—not just for organizing but also for managing costs and automating policies. It’s amazing how such a simple thing can make life easier!

This project took me...

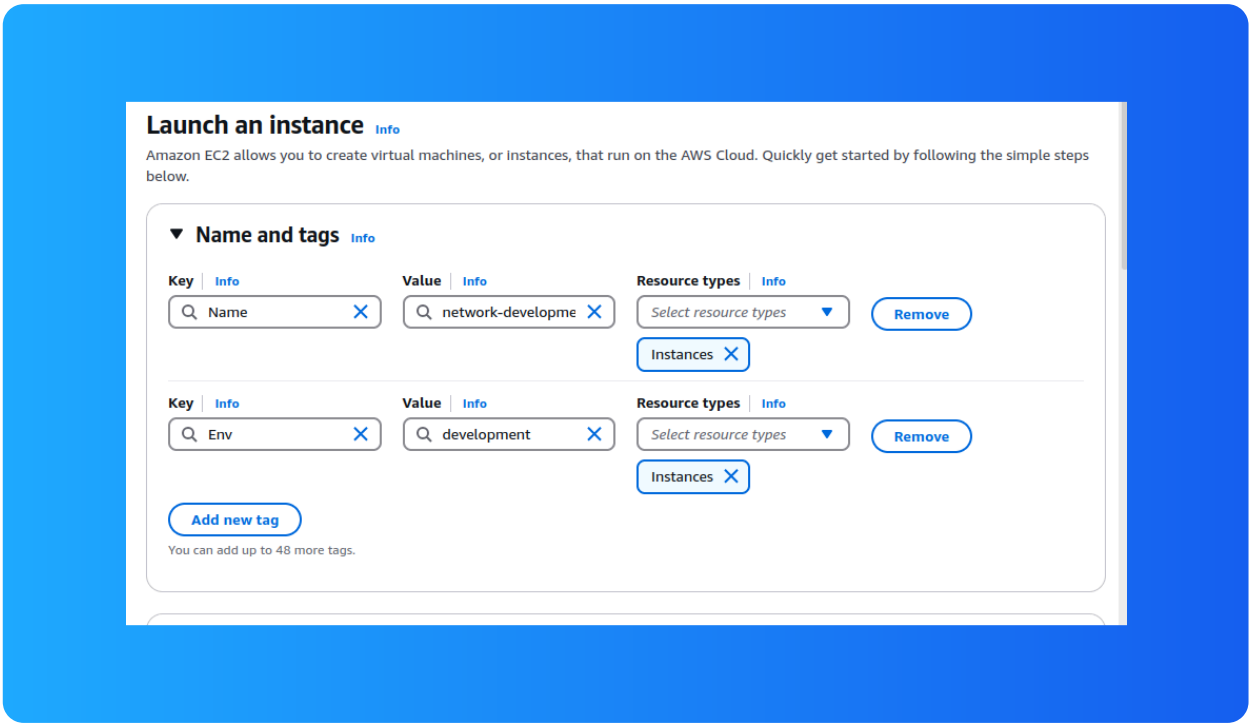
It did not take much of my time to finish the project, It only took around 1-1.5 or so

Vishnu Kv
NextWork Student

Tags

Tags in AWS are like labels you stick on resources to keep things organized. In this case, we're adding a tag called "Env" with values like "production" or "development" to easily tell apart instances used in different environments.

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



Vishnu Kv
NextWork Student

IAM Policies

An IAM policy is a 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 kick in.

The policy I set up

For this project, I've set up a policy using JSON polict editor in IAM Policies.

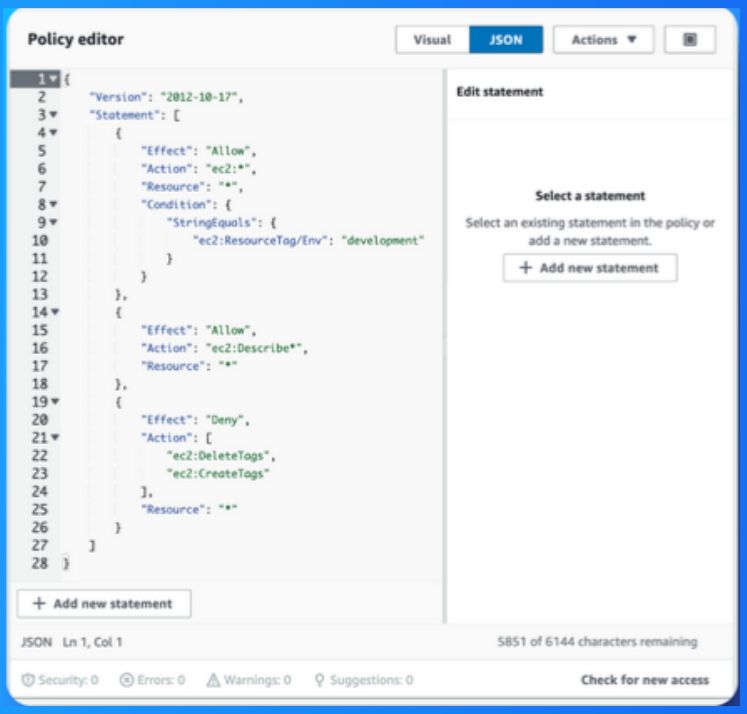
I've created a policy that allows actions like starting, stopping, and describing EC2 instances that are tagged with "Env": "development". At the same time, it denies the ability to create or delete tags on any EC2 instances.

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

Effect: Defines whether the policy allows or denies an action. Action: Specifies the actions that are allowed or denied (e.g., starting EC2 instances). Resource: Identifies which resources the policy applies to (e.g., all EC2 instances or specific on

Vishnu Kv
NextWork Student

My JSON Policy

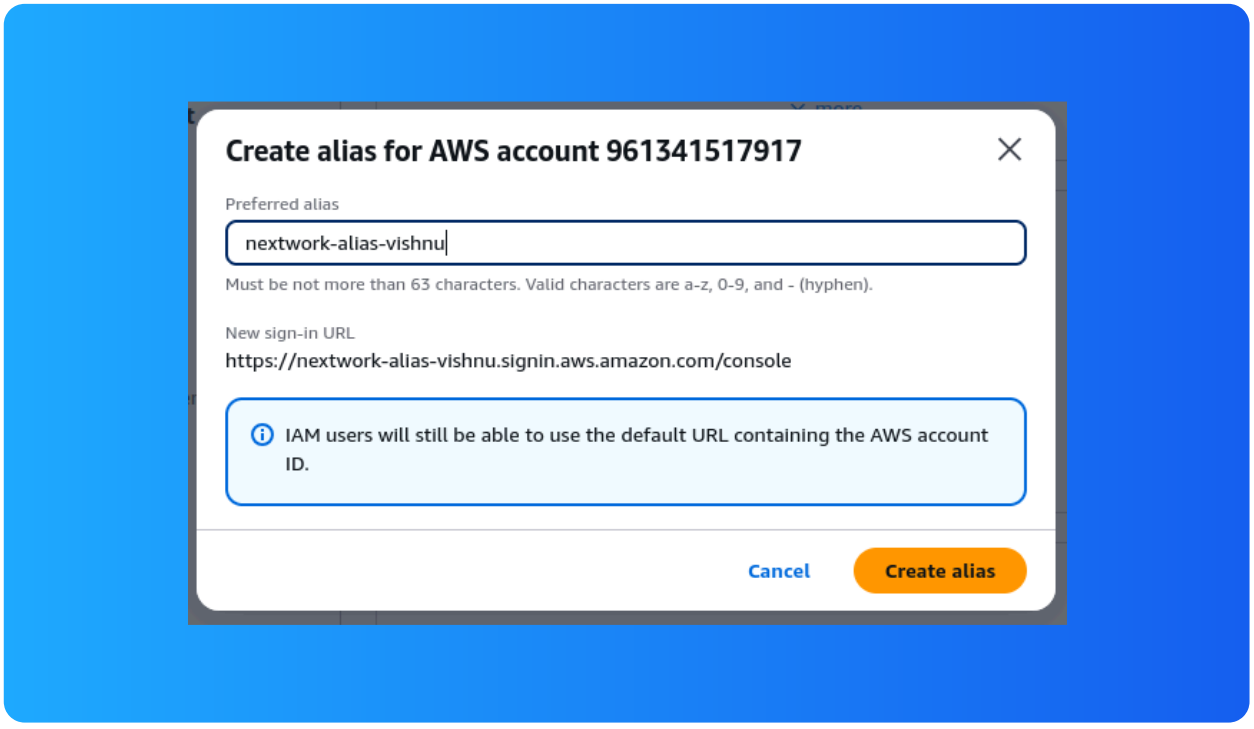


Vishnu Kv
NextWork Student

Account Alias

An Account Alias is a friendly name for your AWS account that you can use instead of your account ID to sign in to the AWS Management Console. with alias: https://Your_Account_Alias.signin.aws.amazon.com/console/ instead of numbers the alias present

Creating an Account alias will only take seconds and the new AWS console sign-in URL looks like : https://nextwork-alias-vishnu.signin.aws.amazon.com/console



Vishnu Kv
NextWork Student

IAM Users and User Groups

Users

IAM users are the people that will get access to your resources/AWS account, whereas user groups are the collections/folders of users for easier user management.

User Groups

An 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.

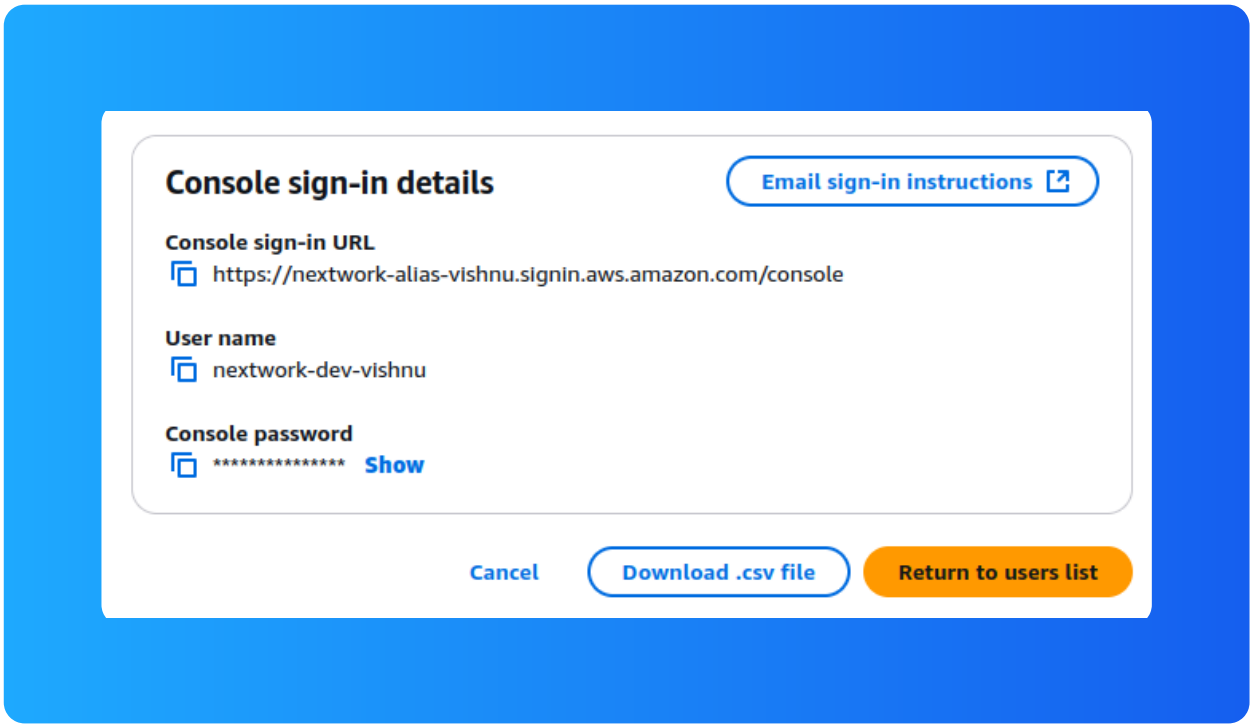
I attached the policy I created to this user group, which means it simplifies managing permissions and ensures consistency across users who have similar access to AWS resources.user groups are the collections/folders of users for easier user mgmt.

Vishnu Kv
NextWork Student

Logging in as an IAM User

The first way is to send the sign-in details via email, including the username and a temporary password for initial access. The second way is to share the details in a secure messaging platform or system, ensuring encryption and privacy.

Once I logged in as my IAM user, I noticed that I couldn't perform the `servicecatalog:ListApplications` action and received an "Access Denied" error. This was because the necessary permissions were not included in my IAM policy.



Vishnu Kv
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by trying to stop the development and production instance from the user (intern) account. The production instance showed error saying it can not be stopped meanwhile the development instance was stopped when tested.

Stopping the production instance

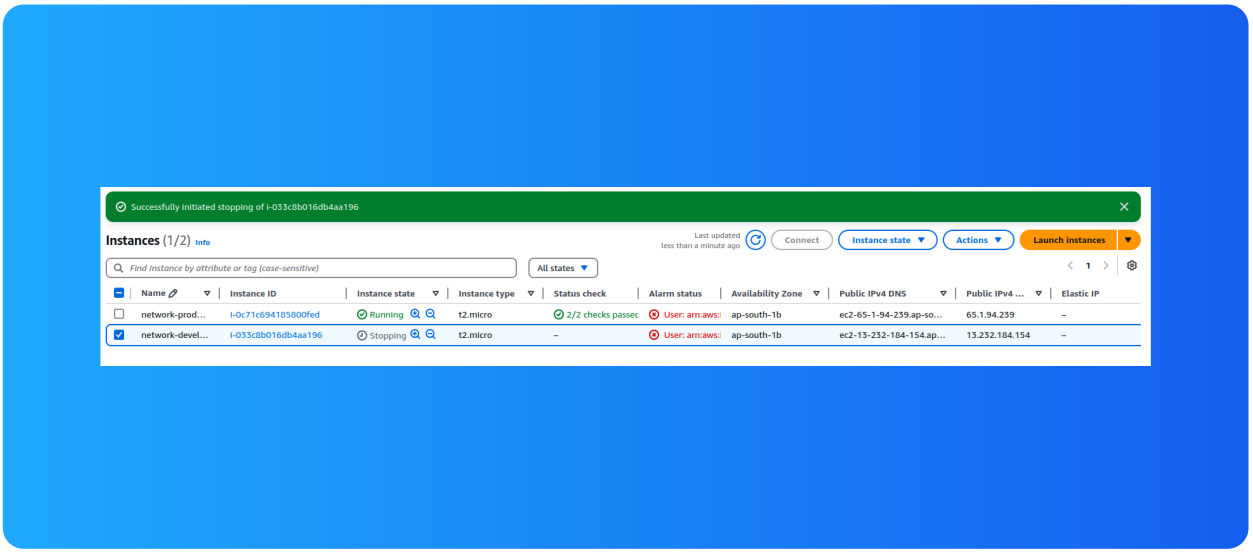
When I tried to stop the production instance it displayed "failed to stop instance" error with a red banner This was because the account i was logging in with didnt have permissions to stop the instance, hence the IAM policies that we applied

Vishnu Kv
NextWork Student

Testing IAM Policies

Stopping the development instance

When i tried to stop the development instance it stopped without errors because the intern had the access to stop or do operations with the development instance, which is specified in our JSON IAM policy



Everyone should be in a job they love.

Check out nextwork.org for more projects