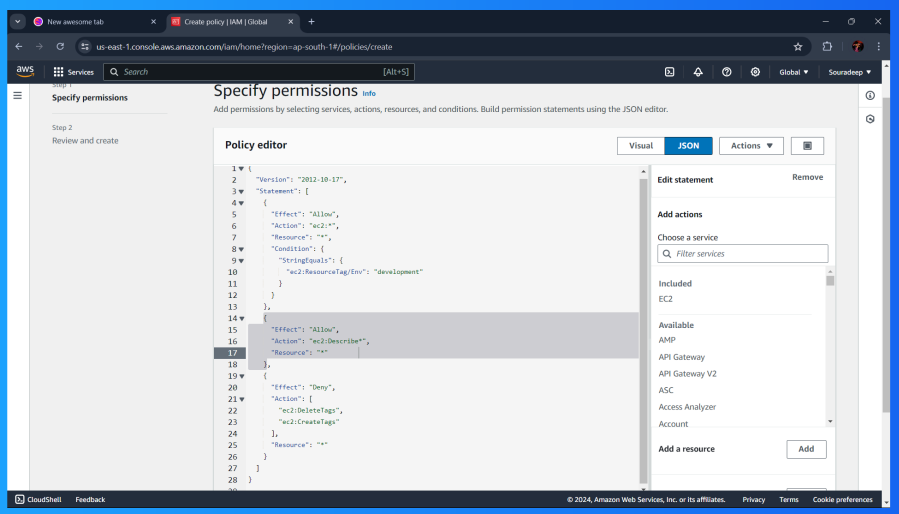
NextWork.org

# Cloud Security with AWS IAM

Souradeep Roy



**Souradeep Roy**
NextWork Student



# Introducing today's project!

## What is AWS IAM?

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, one can manage permissions that control which AWS resources users can access.

## How I'm using AWS IAM in this project

I used AWS IAM as a Service to control who is authenticated (signed in) and authorized (has permissions) to use my account's resources. IAM provides the infrastructure necessary to control authentication and authorization for AWS accounts.

## One thing I didn't expect...

I didn't expected to be such an easy task to handle the Authorization to my AWS Resources .....

## This project took me...

This project took me approximately 45 min to go through each and every feature and provide the infrastructure necessary to control the authentication and authorization of my AWS account.

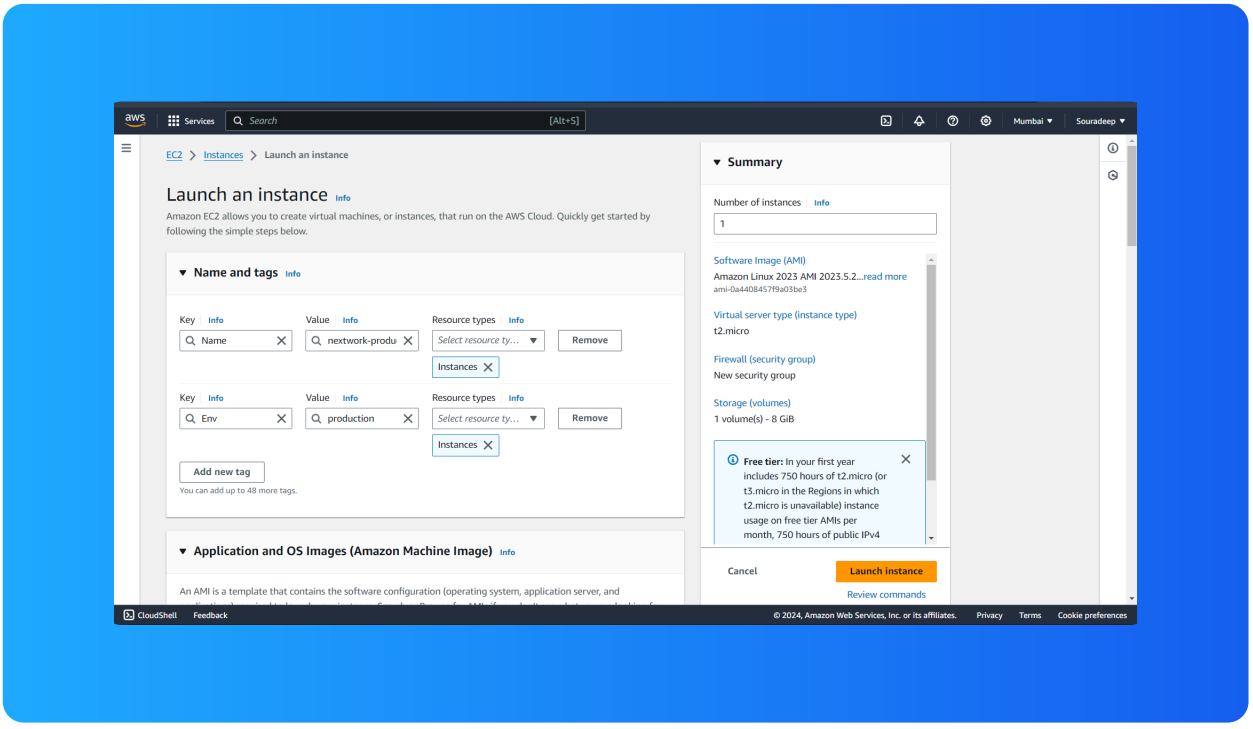
**Souradeep Roy**
NextWork Student



# Tags

Tags are like labels you can attach to AWS resources for organization. In this case, we're creating a tag called "Env" with a value of "production" or "development" to label the instances used in production vs development environments.

As mentioned above I tagged "Env" with a value of "production" and another instance "development" to label production and development environments separately.



**Souradeep Roy**
NextWork Student



# IAM Policies

"IAM Policies are a set of rules for who can do what with our 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 are being implemented"

## The policy I set up

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

'I've created a policy that allows some actions (like starting, stopping, and describing EC2 instances) for instances tagged with "Env = development" while denying the ability to create or delete tags for all instances. '

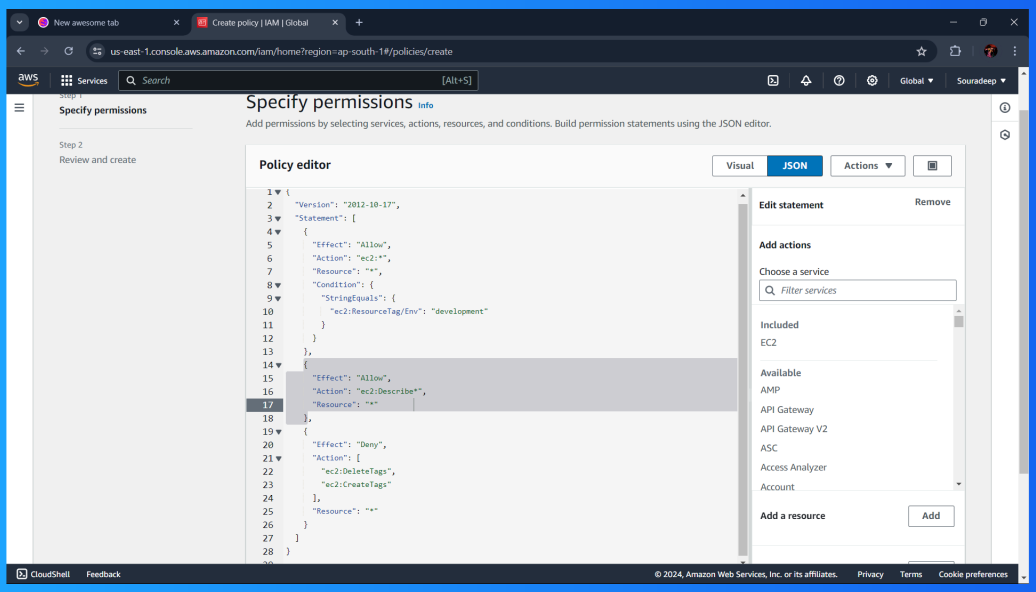
## When creating a JSON policy, you have to define its Effect, Action and Resource.

'The Effect, Action, and Resource attributes of a JSON policy means to indicate whether the policy allows or denies a certain action and A list of the actions that the policy allows or denies. Which resources does this policy apply to ! '

**Souradeep Roy**
NextWork Student



# My JSON Policy



**Souradeep Roy**
NextWork Student

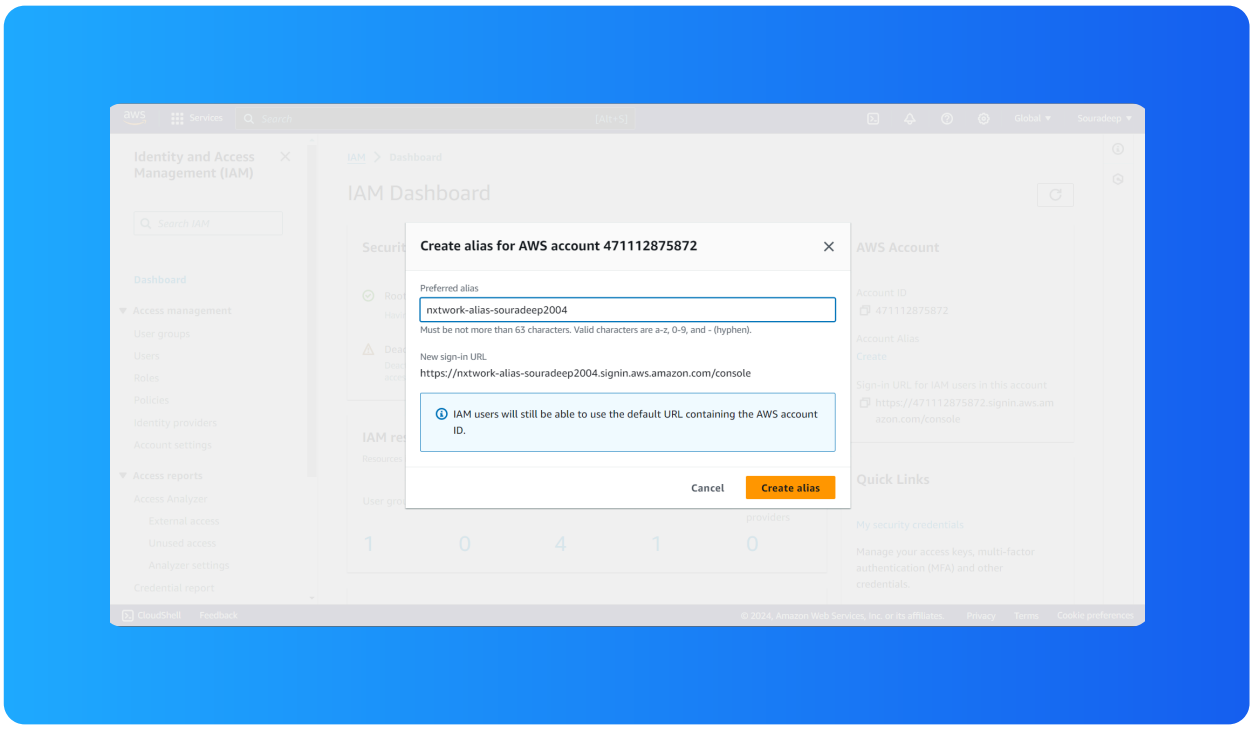


# Account Alias

'An account alias is a friendly name for your AWS account that you can use instead of your account ID (which is usually a bunch of digits) to sign in to the AWS Management Console. '

'Creating an account alias took me less than a 30 seconds ' ...

'Now, my new AWS console sign-in URL is https://nxtwork-alias-souradeep2004.signin.aws.amazon.com/console '.



**Souradeep Roy**
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 groups are a collection/folder of IAM users. It allows one to manage permissions for all the users in a 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 We're adding users to to grant them the permissions associated with that group. This simplifies managing permissions and ensures consistency across users who have similar access'....

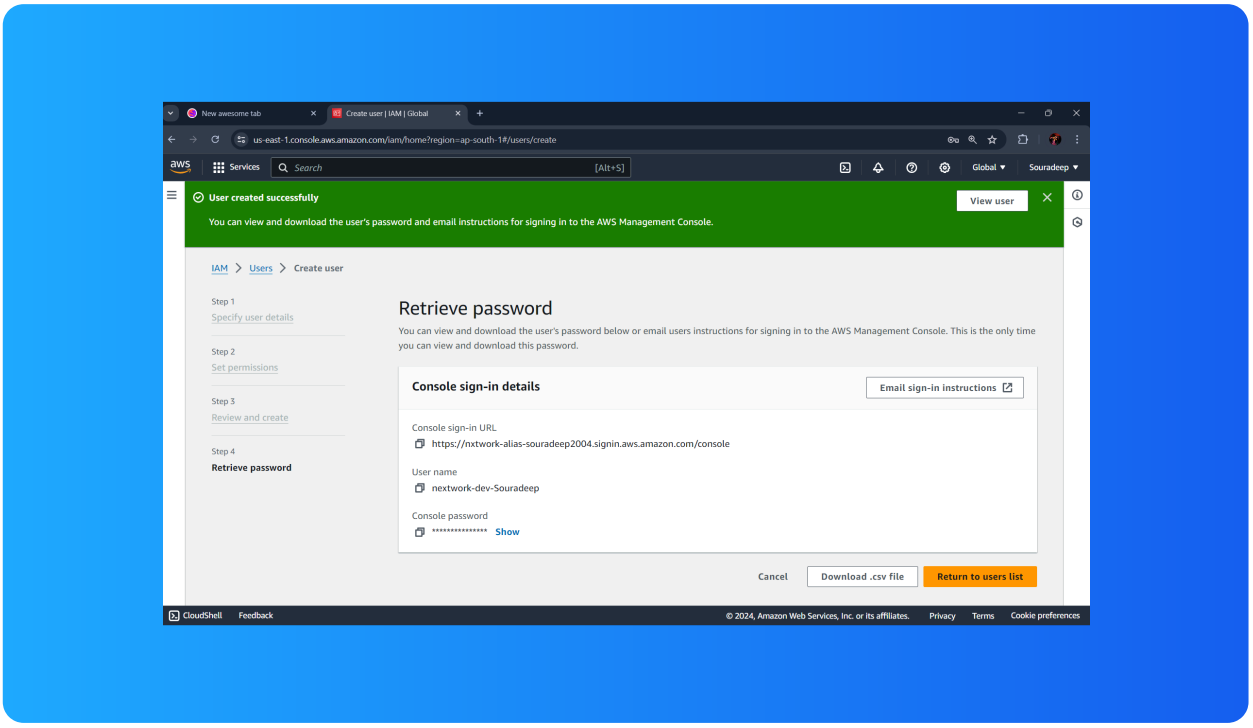
**Souradeep Roy**
NextWork Student



# Logging in as an IAM User

'The first way is one can view and download the user's password below or email users instructions for signing in to the AWS Management Console. '

'Once I logged in as my IAM user, I noticed that the full access to AWS console was not given so as far as I have noticed there were places were access was denied '...



**Souradeep Roy**
NextWork Student

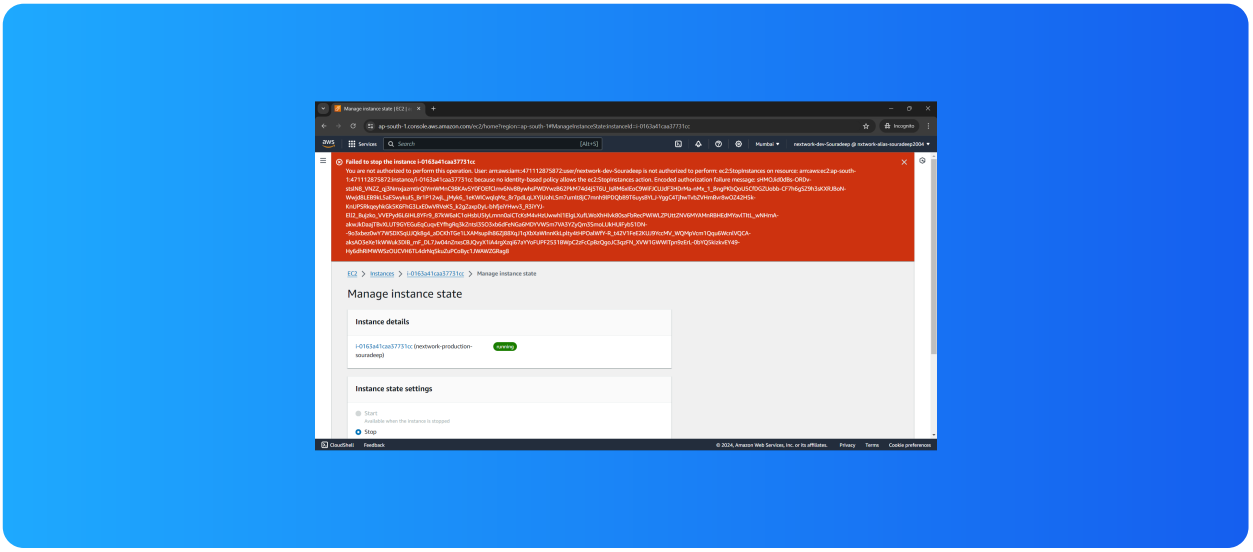


# Testing IAM Policies

'I tested my JSON IAM policy by trying to stop the production-LVL-instance which I was not supposed to stop AWS threw an error but The Development level instance stopped as it was mentioned/granted in the IAM Policy '...

## Stopping the production instance

'When I tried to stop the production instance AWS prevented the user to stop the instance as there was no permission granted to start/stop an instance of production-level '...



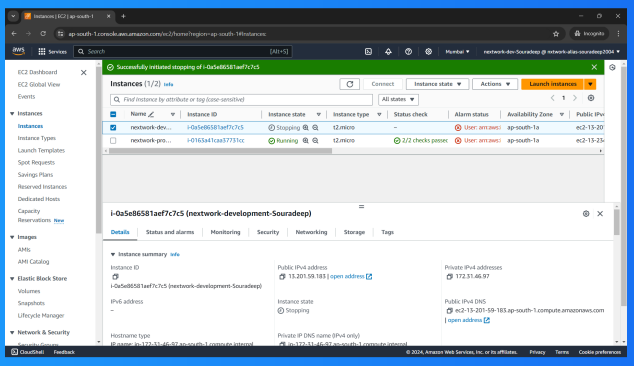
**Souradeep Roy**
NextWork Student



# Testing IAM Policies

## Stopping the development instance

'Next, when I tried to stop the development instance it stopped as we created an IAM policy which allows the user to start/stop the instances at development-level '...



# Everyone should be in a job they love.

Check out nextwork.org for more projects