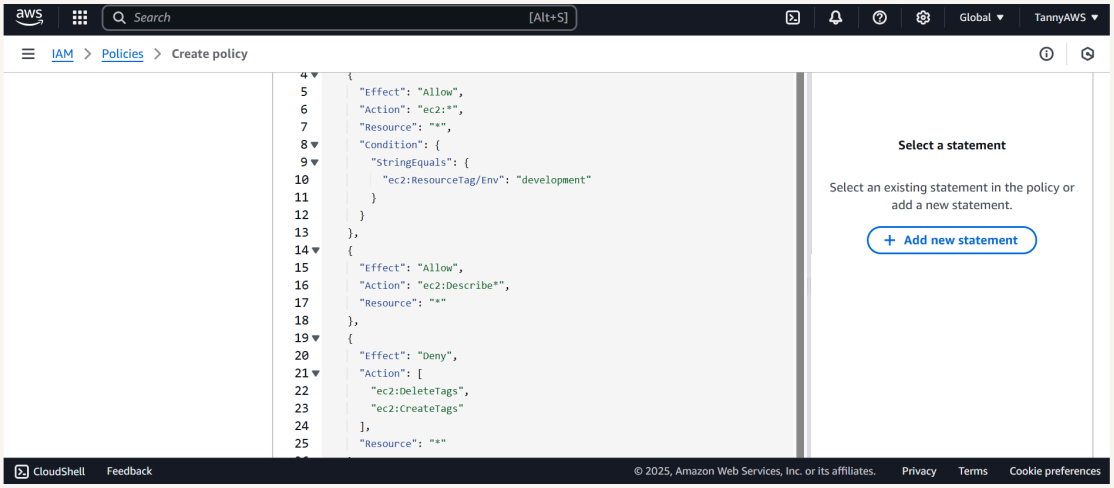
nextwork.org

Cloud Security with AWS IAM

Wachiraya Meevasana (Tanny)



Introducing today's project!

What is AWS IAM?

I learned how to use AWS IAM to create users and groups, attach policies, and manage permissions. I also practiced securing access with tags, console login, and create Alias account.

How I'm using AWS IAM in this project

This project took me approximately 3o mins.The most challenging part was create alias user. It was most rewarding to learn how ti create security group on my EC2 instances.

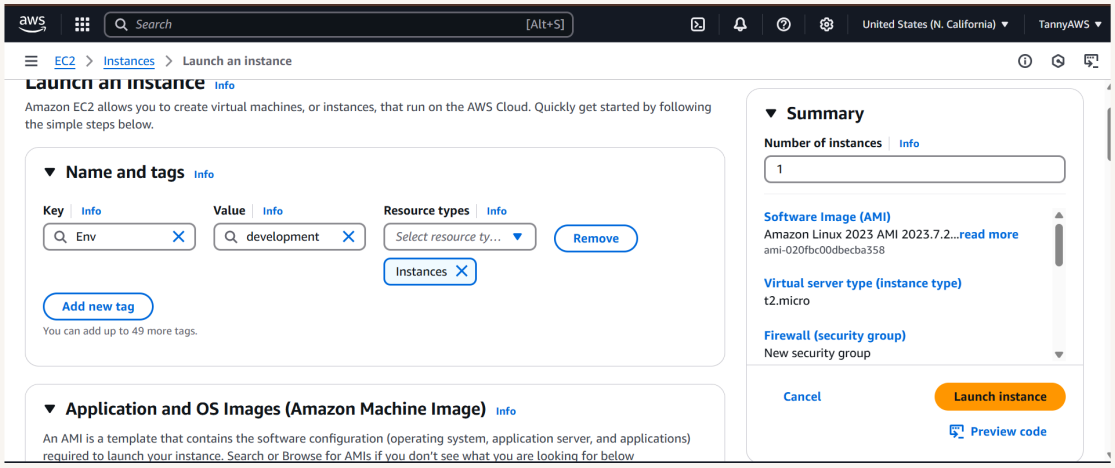
One thing I didn't expect...

I chose to do this project today because I want to keep learning on AWS services.

Tags

Tags are lebel that helps us with identifying all resources with the same tag at once (they are useful filters when we're searching for something), cost allocation, and applying 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.



IAM Policies

IAM Policies are the permissions to IAM users, groups, or roles, saying what they can or can't do on certain resources

The policy I set up

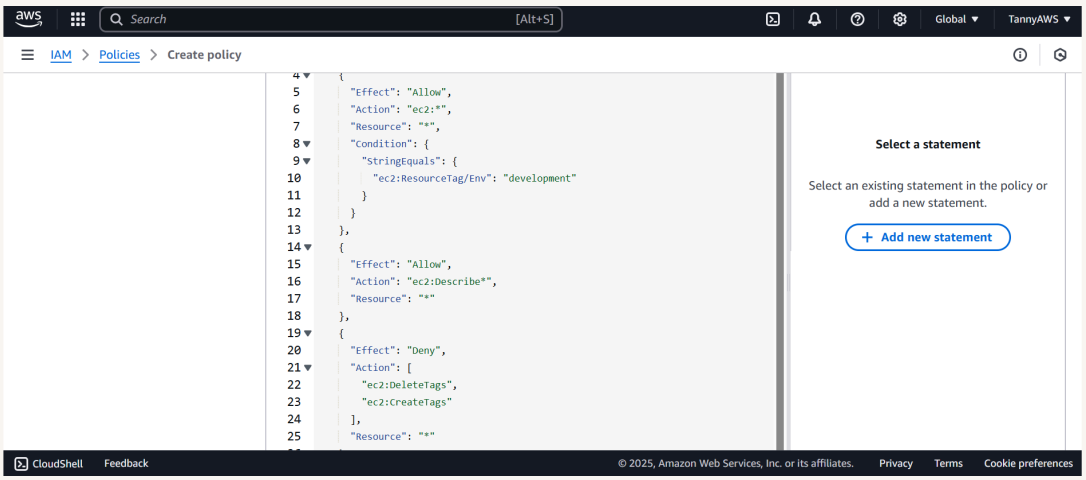
For this project, I've set up a policy using JSON

I've created a policy that the intern do everything EC2-related on resources tagged with Env=development and view (describe) all EC2 resources. But, he can't create or delete tags on any EC2 resources.

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

Effect: Specifies whether the action is allowed or denied (e.g., "Allow" or "Deny"). Action: Defines the specific AWS operation or service action (e.g., "ec2:StartInstances"). Resource: Specifies the AWS resources the action applies to.

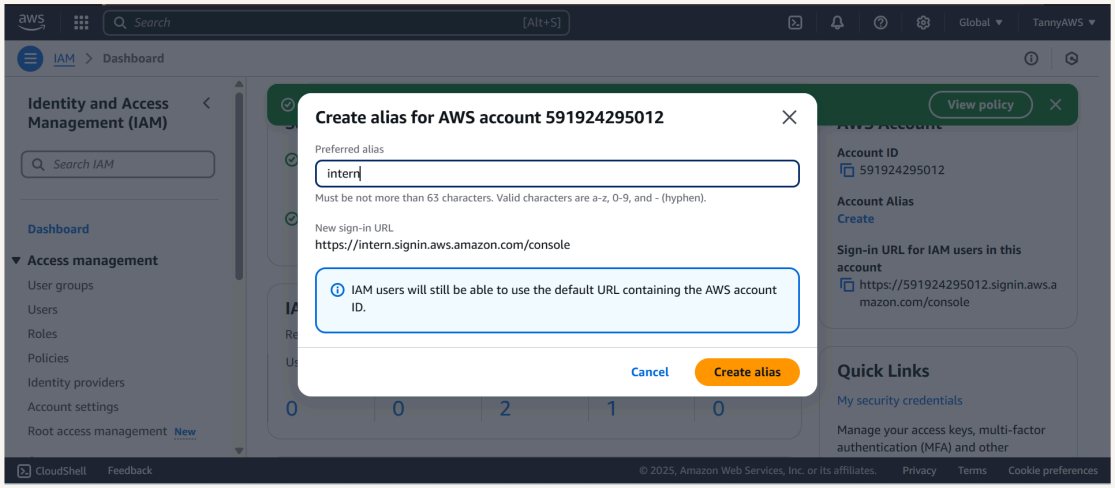
My JSON Policy



Account Alias

An account alias is a friendly name for your AWS account that I can use instead of my account ID to sign in to the AWS Management Console.

Creating an account alias took me 3 sec !. Now, my new AWS console sign-in URL is https://internacc1.signin.aws.amazon.com/console



IAM Users and User Groups

Users

IAM users are individual identities in AWS with credentials, used to access and manage resources based on assigned permissions.

User Groups

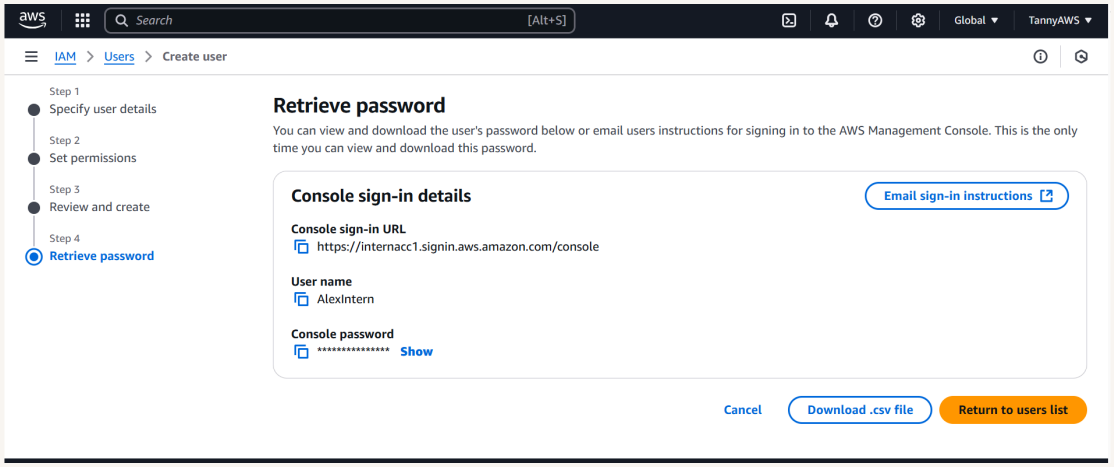
IAM user groups are collection of IAM users. Those allows me to manage permissions for all the users in the groups at the same time by attaching policies to the group rather than individual users

I attached the policy I created to this user group, which means this group have broad read access to EC2, limited control over "development"-tagged resources, and zero ability to tag anything.

Logging in as an IAM User

The first way is Email – Send login URL, username, and temporary password manually. Anoyher way is to download the .csv file with sign-in details and securely share it.

Once I logged in as my IAM user, I noticed the permission denied .This was because AWS console will treat me as someone that is starting from 0.



Testing IAM Policies

I tested my JSON IAM policy by stopping the instance.

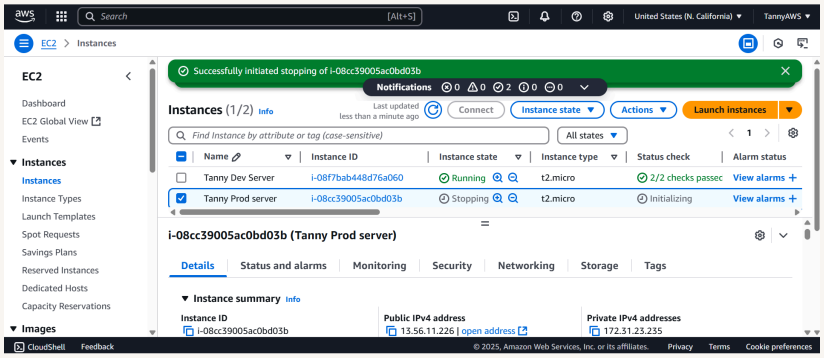
Stopping the production instance

When I tried to stop the production instance there was an error massge popped up, it's because we're not authorized. We don't have permission to stop any instance with the production tag.

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, it is successful. This was because I have permission to do it.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects