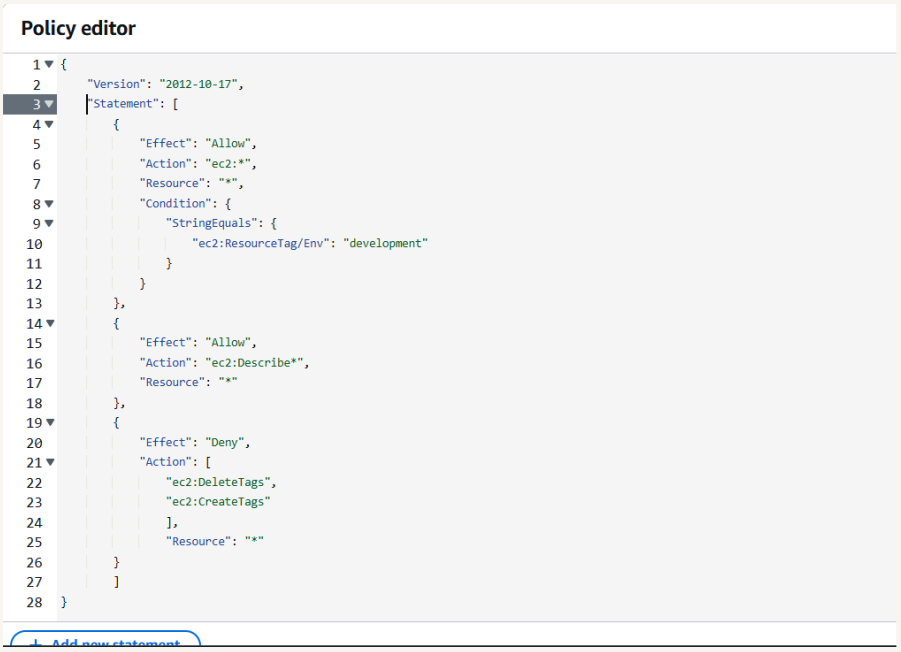
nextwork.org

Cloud Security with AWS IAM

CH chollangijagapathibabu@gmail.com



Introducing today's project!

What is AWS IAM?

Services I used were Amazon EC2, Amazon IAM. Key concepts I learnt include is IAM user, Policies, IAM User Groups and account aliases. I also leant about IAM Policy simulator which helps to identifies whether it has permission access or denied.

How I'm using AWS IAM in this project

This project took me approximately 1hour . The most challenging part was make changes for updating policy in JSON and make configurations so it has access to do certain tasks. It was most rewarding to verify the permission access to work correctly.

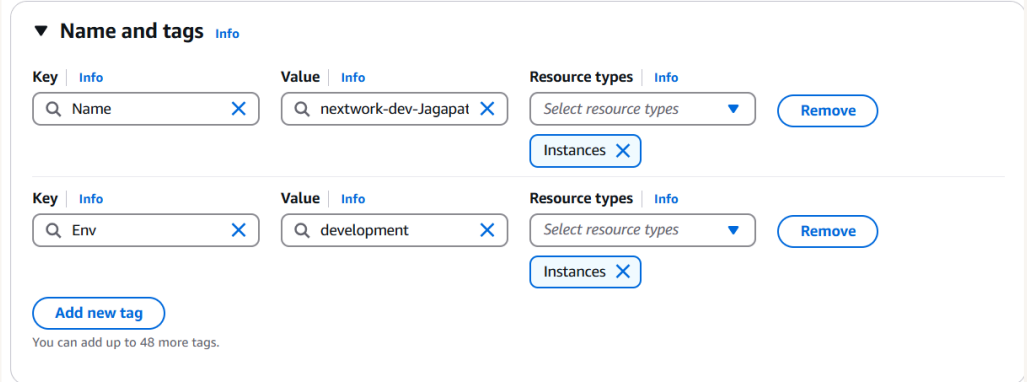
One thing I didn't expect...

I chose to do this project today because to Use IAM to configure IAM User and assigning to User Groups so this helps user to sign-in individual access. Something that would make learning with NextWork even better is doing hands-on experimentation.

Tags

Tags are tools that use for labelling our resources . They are used for grouping resources, cost allocation and applying policies for all resources with the same tag.

The tag i had used on my EC2 instances is called Env which is "Envionment". The value i have assigned for my instances are "production" and "development"



IAM Policies

IAM Policies are rules to determine , what users can do and users cannot do . In order execute or launch instance, do a task that individual service need to have a policy with permissions from IAM to get access.

The policy I set up

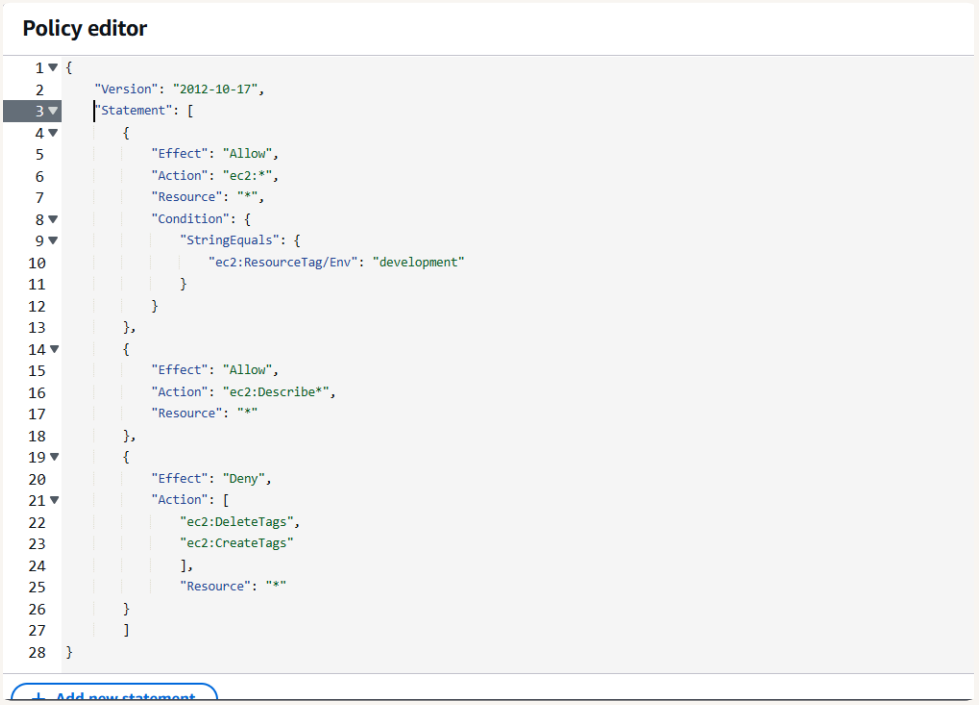
For this project, i had set a policy using JSON (JavaScript Object Notation), a lightweight, text-based open standard format for data representation.

I had created a policy that allows the policy holder to have permission to do anything to instance tagged with "development". they can view the information, but they dont have acess to delete or create new tags.

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 whether it is allowing or denying action is 'Effect' Allow or Deny. what the policy holder can or cannot do is 'Action' create or delete EC2 instance or tags. Resouce relates policy.

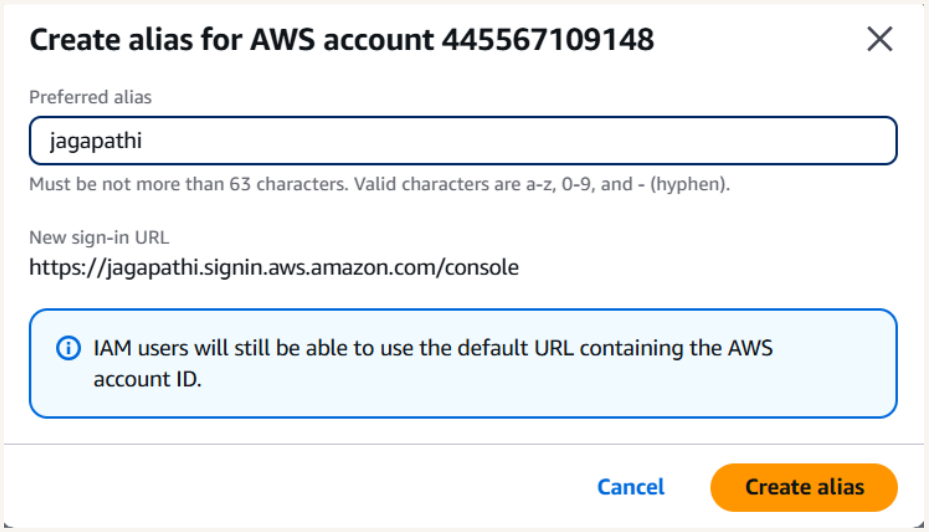
My JSON Policy



Account Alias

An account alias is a simple nickname for AWS account instead of a long AccountID number.

Creating an account alias took me 15 sec simple configuration creating a name on IAM. Now, my new AWS console sign-in URL uses alias instead of my account ID.



IAM Users and User Groups

Users

IAM users are people or entities that can access or login to AWS account . These are individual member they have certain set of required access to perform activities.

User Groups

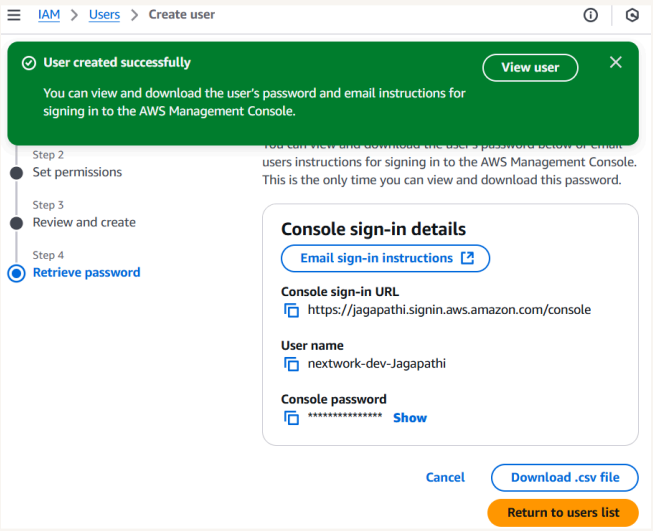
IAM user groups are set of permissions for IAM Users where every user have same type of access level. IAM is a folder in which it contain users to get access resouces permissions instead of applying individual User.

I attached the policy I created to this user group, which means any user inside this user group will automatically get permissions attached to DevEnvironment Policy.

Logging in as an IAM User

The first way is to email sign-in instructions to user. Second way is to download a .CSV file which has sign-in details like User name, Password, Console Sign-in Url.

Once I logged in as my IAM user, I noticed that user has access denied on panels on AWS Dashboard. This is because we set up premissions only for EC2 instance. This follows the Least privilege principle meaning, it gives only required access not all.

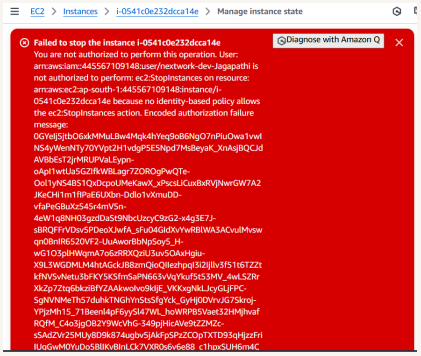


Testing IAM Policies

I tested my JSON IAM policy by stopping the development and production environment.

Stopping the production instance

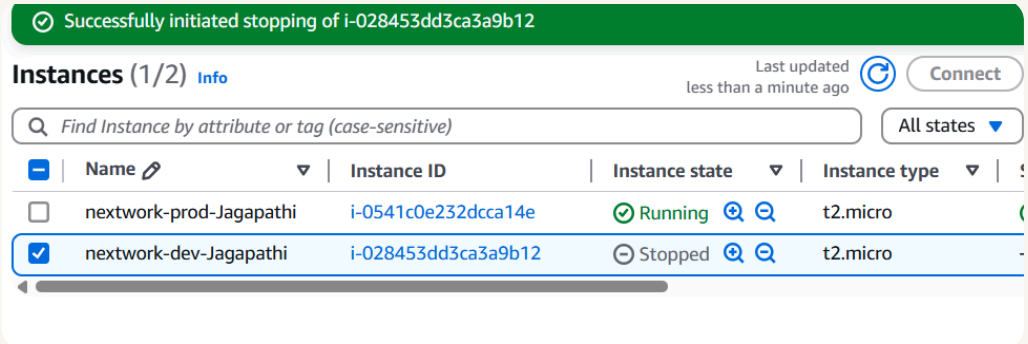
When I tried to stop the production instance it denies and we get an error. This is because our production is outside of the scope of permission policy which is "Dev Environment"only can launch EC2 and cannot delete or create resources of production.



Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance i had successfully stop the instance state. This was because policy allows the dev environment to stop insatnce.



The place to learn & showcase your skills

Check out nextwork.org for more projects