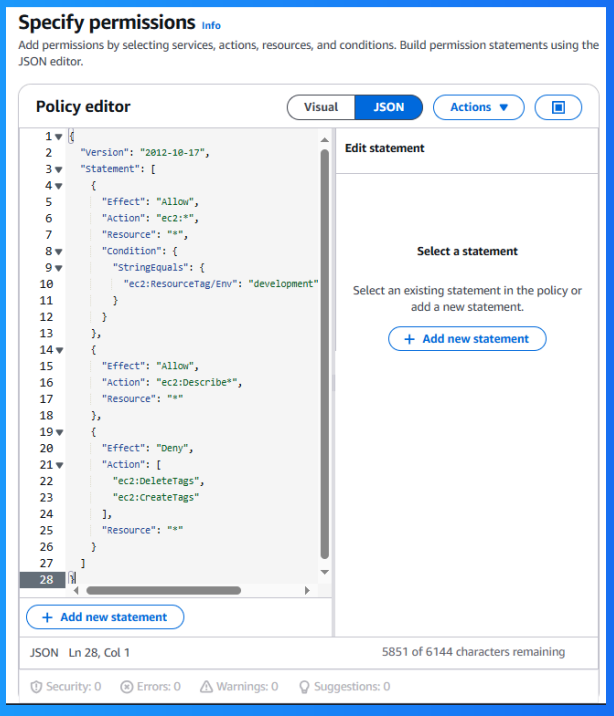
NextWork.org

Cloud Security with AWS IAM

IT itsbryantgonzalez@gmail.com



Introducing today's project!

What is AWS IAM?

AWS Identity Access Management is a tool that is most useful for creating and managing users and grouping them by departments to access certain workspaces or assets to carry out work tasks. This can be regulated thorugh security policies as well.

How I'm using AWS IAM in this project

I used AWS Identity Access Management to create users and user group that were assigned a custom security policy I created to allow all actions inside the development EC2 instance.

One thing I didn't expect...

One thing I didn't expect from this project was how easily accessible and intuitive the AWS platform is. This was my first project on AWS and I can happily say I'll be making many more projects on this platform.

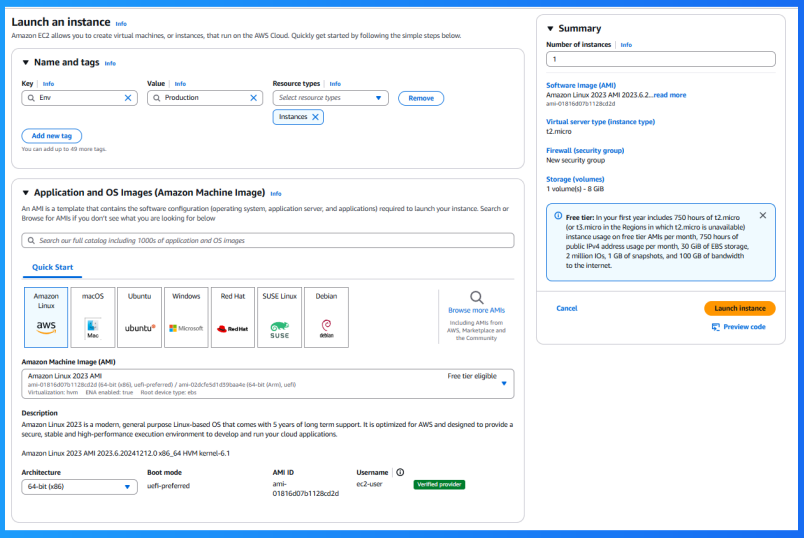
This project took me...

this project took me less than an hour in total.

Tags

Tags are labels we can add to our EC2 Instances to easily sort through and choose or assign the correct ones for users to gain access to. This also helps us know which policies are attached to which Instance.

The tag I've used on my EC2 Instances are called Env (A.K.A Environment) and Production.



IAM Policies

IAM Policies are strict rules for users dictating what they can and can't do to different assets inside AWS. This is to uphold the security principles of the CIA Triad and least privilege.

The policy I set up

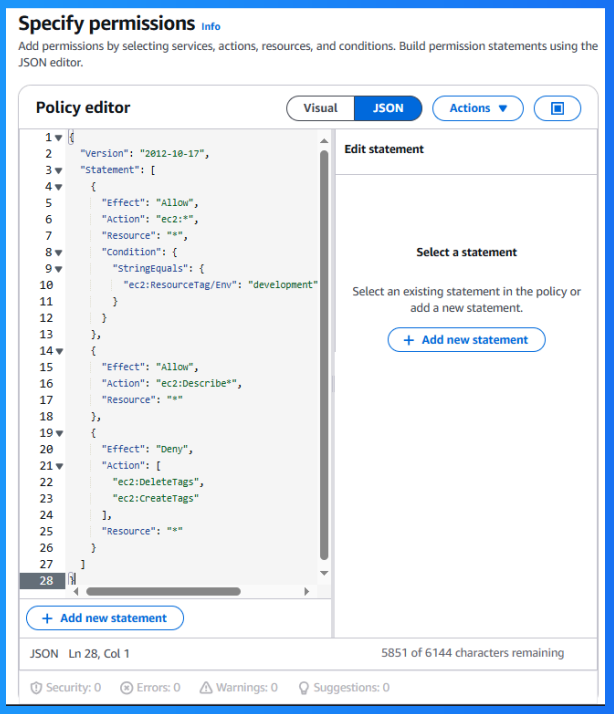
For this project, I've set up a policy using JSON.

I've created a policy that allows a user to perform all types of actions on all Instances with the "Development" tag.

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

The Effect, Action and Resource attributes of a JSON policy are controls that a user can or cannot make. For example the Effect = Allow; authorization, the Action = EC2; this is the service that can access, Resource = *; any.

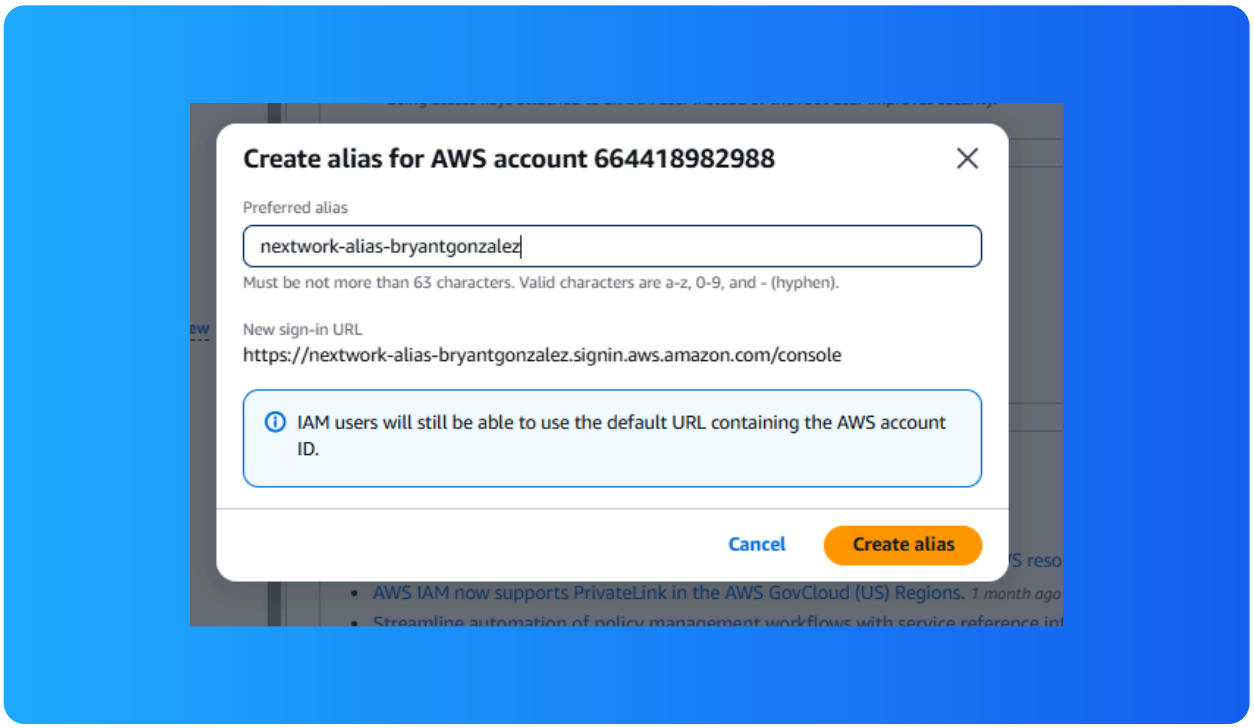
My JSON Policy



Account Alias

An account alias is a unique name you can use for your AWS account instead of your account ID.

Creating an account alias is super easy and is very useful for other in your organization to ID you.



IAM Users and User Groups

Users

IAM users are created and assigned to certain user groups to carry out different job functions on the AWS platform.

User Groups

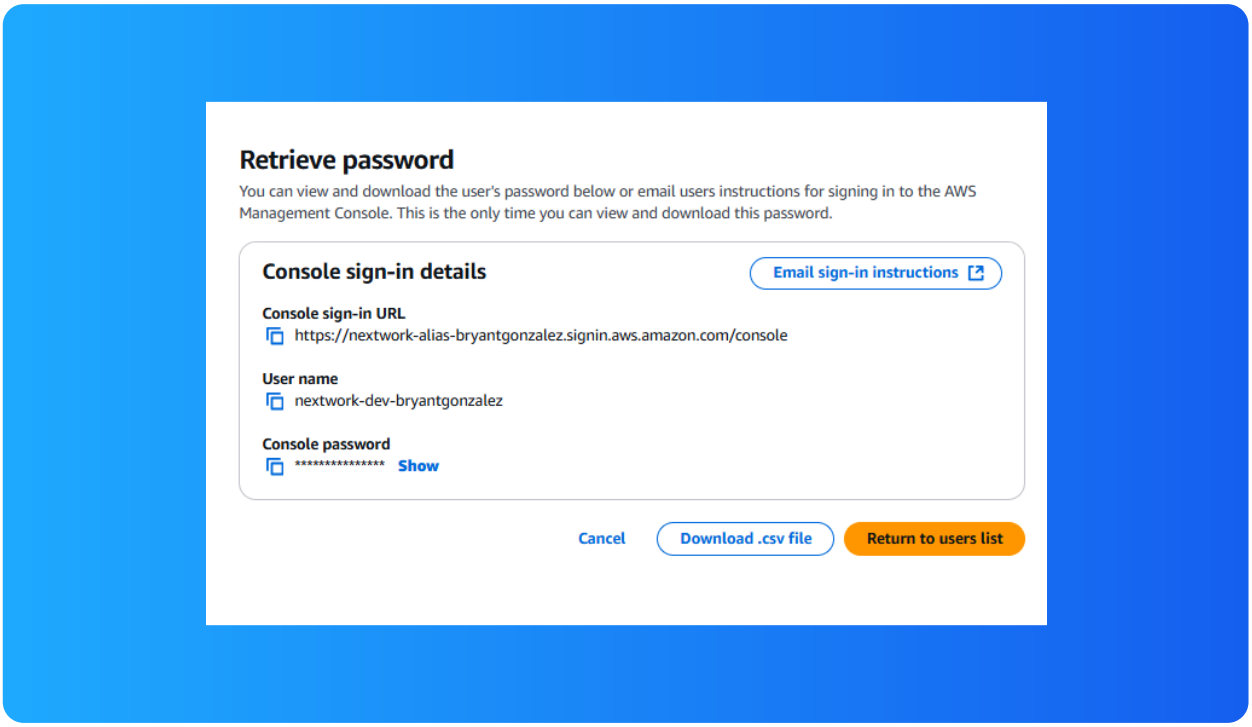
IAM user groups are equivalent to a folder of users that can be assigned policies and certain access.

I attached the policy I created to this user group which means these users now have access to the development instance and can freely take actions to edit inside the EC2 Instance.

Logging in as an IAM User

The first way to share a users sign-in details is by sharing a screenshot of the sign -in details or by emailing them the instructions directly.

Once I lgged in as my IAM user, I noticed certain stats of this instance were denied. For example I saw the cost analasys was denied to keep that information confidential.

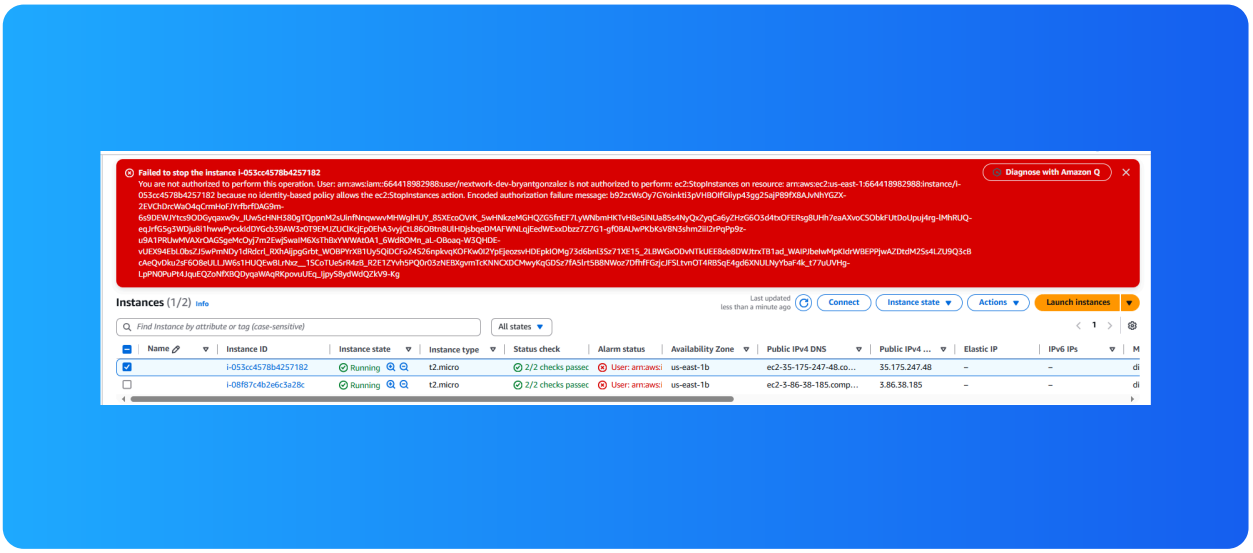


Testing IAM Policies

I tested my JSON IAM policy by attempting to stop the production instance with my root user and IAM user to test if these accounts were able to stop the instances. The root user was successful while the IAM user wasn not successful.

Stopping the production instance

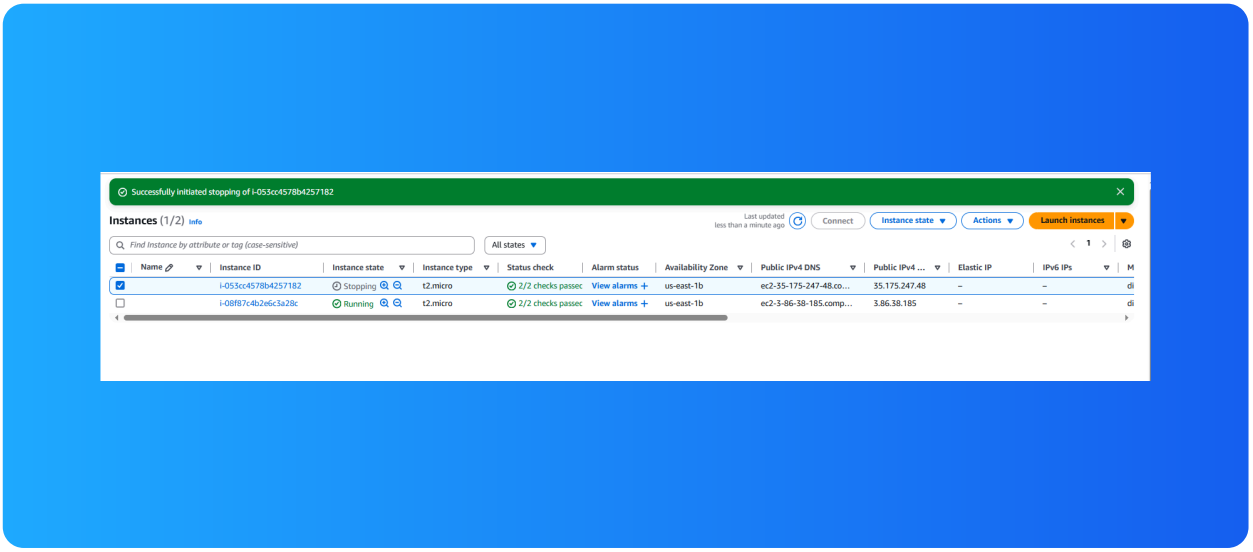
When i tried to stop the production instance I was shown an error that blocked me from stopping the production instance because I was logged in as a user with the least amount of privilege to carry out job functions.



Testing IAM Policies

Stopping the development instance

When I tried stopping the development instance with the root user I was successful because the root user has max priviliges.



Everyone should be in a job they love.

Check out nextwork.org for more projects