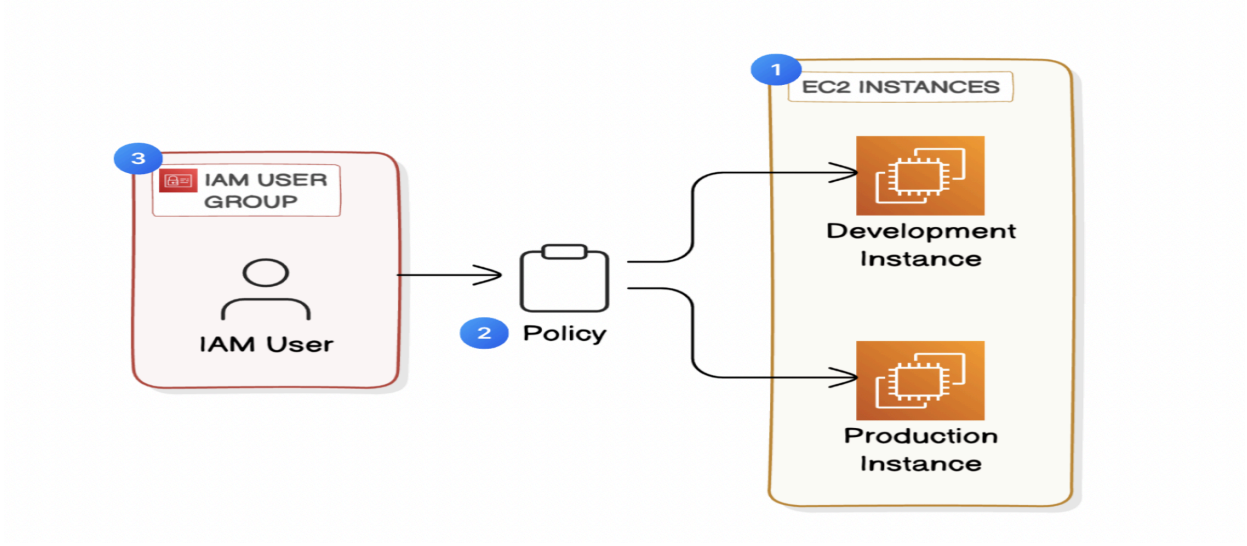
CLOUD SECURITY WITH AWS IAM

By Edikan Sam



PROJECT INTRODUCTION

WHAT IS AWS IAM?

AWS IAM (Identity and Access Management) is a service that securely manages user access to AWS resources. It helps control permissions, enhance security, and support compliance efforts.

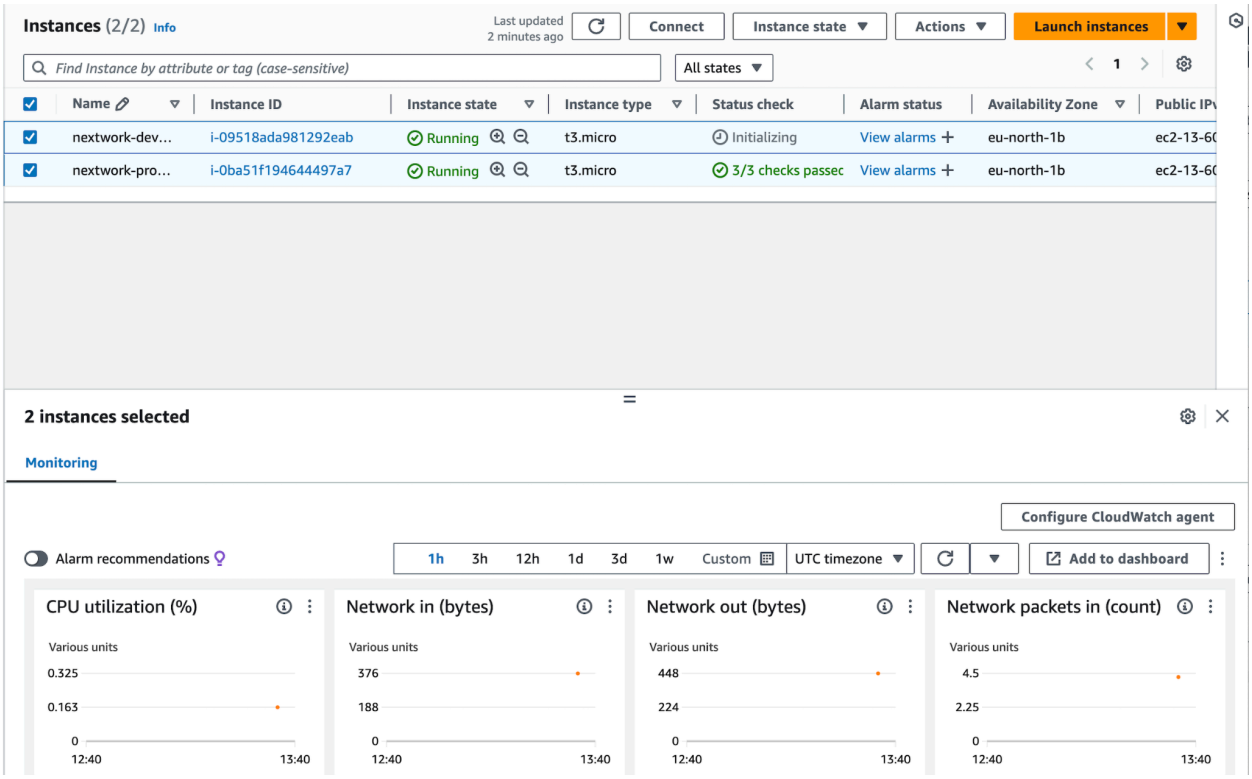
HOW I'M USING AWS IAM IN THIS PROJECT

I am using AWS IAM to create user groups, assign specific permissions to instances and attach policies.

One thing I didn't expect from this project was the intricate management of IAM policies and permissions, which demanded careful thought to provide users with appropriate access while maintaining security. This project took approximately 120 minutes to complete.

TAGS

EC2 tags function like labels that you can assign to your Amazon EC2 instances, which are virtual servers in the cloud. Each tag has a key and a value, making it easier to organize and manage your resources. For instance, you can use tags to indicate which instance is associated with a particular project, who oversees it, or its environment (such as development or production which I used on my EC2 instances). This simplifies the process of locating, sorting, and monitoring your servers, especially when you have numerous instances running in your AWS account.

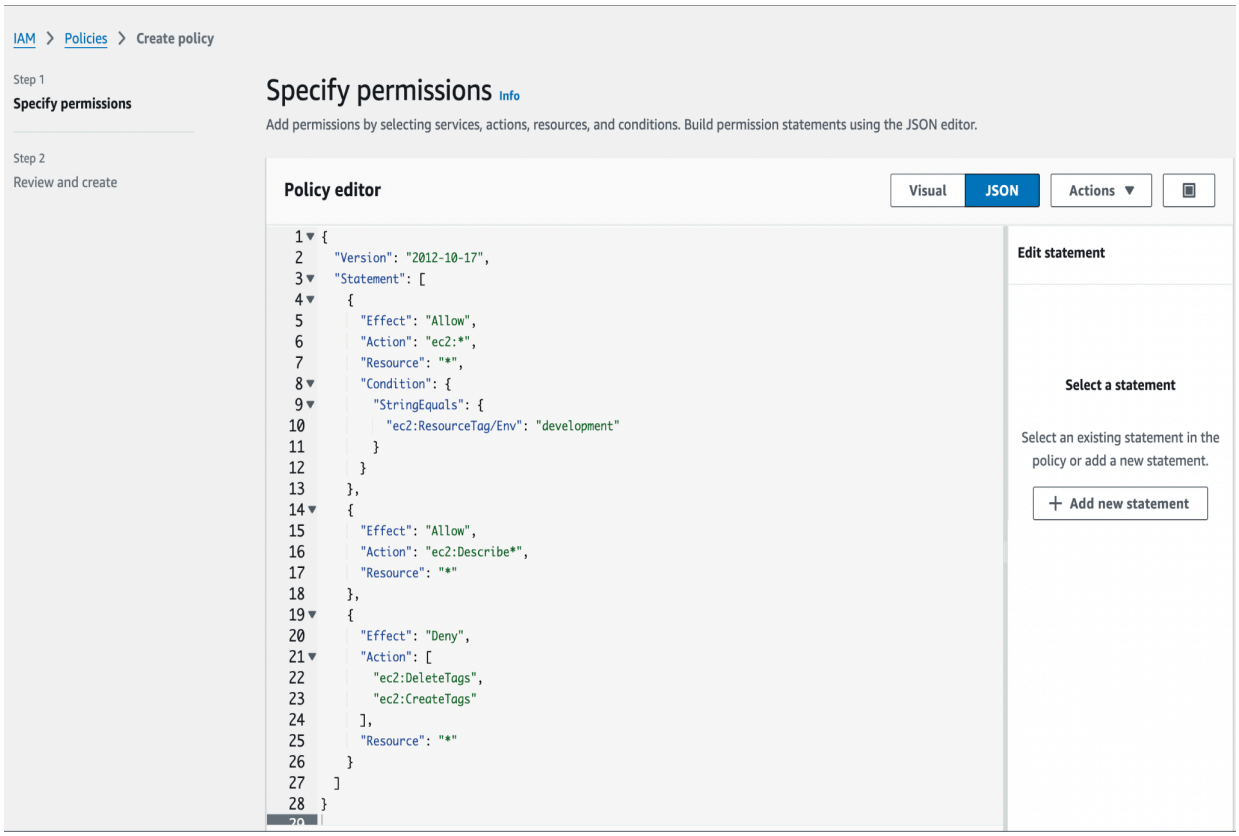


IAM POLICIES

IAM policy defines who gets access to AWS resources and what actions they can perform. It grants users, groups, or roles permissions, specifying what they are allowed or not allowed to do and when these rules apply.
For this project, I have set up a policy using JSON.
I have created a policy that grants full EC2 access to resources tagged Env=development, allows view-only access to all EC2 resources and prevents users from modifying resources tags.

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

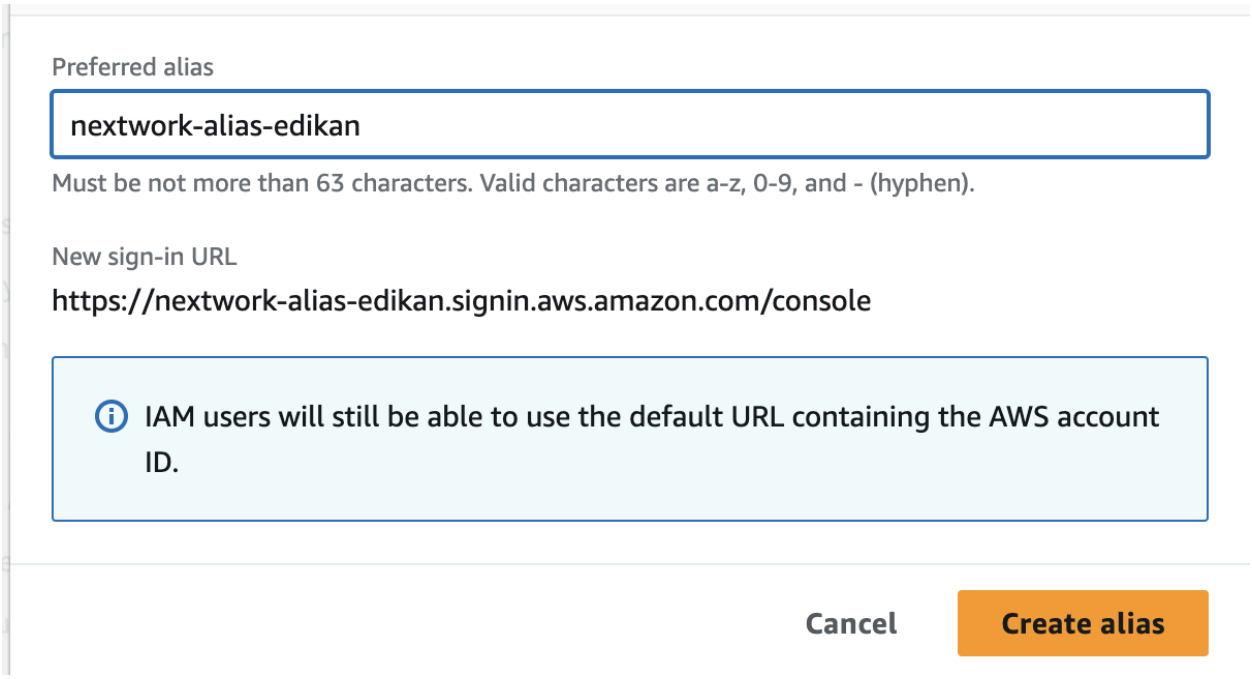
The Effect, Action and Resource attributes of a JSON policy mean that the Effect defines if permission is allowed or denied; the Action specifies the operations permitted; and the Resources identifies the AWS resources affected.



MY JSON POLICY

ACCOUNT ALIAS

An AWS Alias is a personalised name you use to replace the default account ID in your login URL. It takes less than a minute to create an account alias.
Now, my new AWS console sign-in URL is;
https://nextwork-alias-edikan.signin.aws.amazon.com/console



IAM USERS AND USER GROUPS

Users

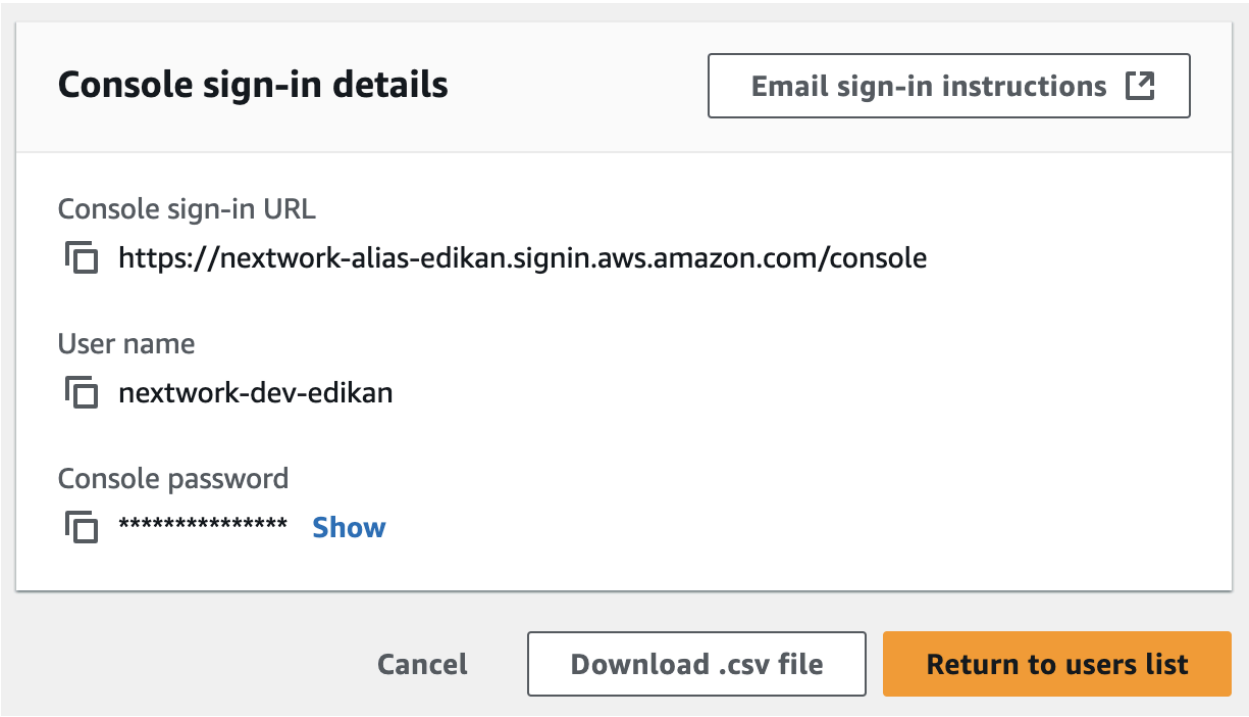
IAM users are like a login account for a person or application. Each has a name, password, and specific permissions, allowing them to access only certain AWS services perform actions you control, like read and write.

User Groups

An IAM user groups is a collection or grouping of IAM users. It enables you to manage permissions for all users within the group simultaneously by attaching policies to the group, instead of assigning them to each user individually.

I attached the policy I created to this user group, which means all users in the user group are granted the same permissions defined in the policy, simplifying access management.

Once I logged in as my IAM user, I noticed there were restrictions and i was denied access to IAM

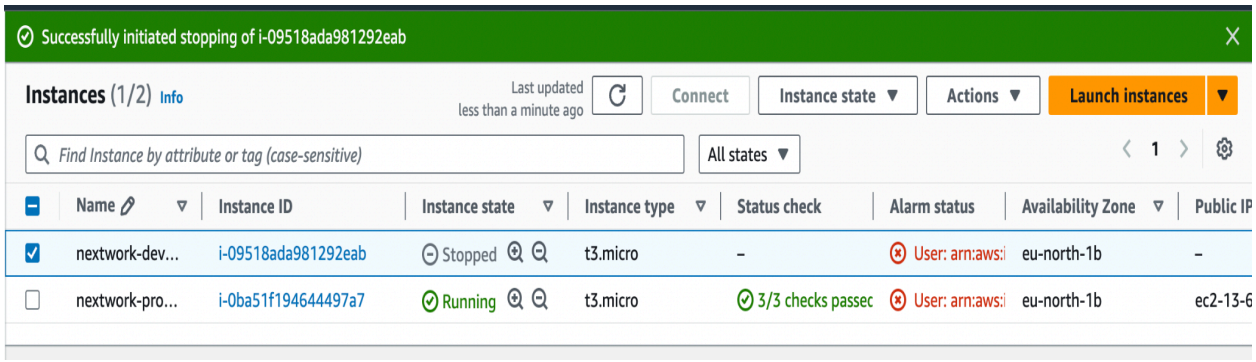


TESTING IAM POLICIES
I tested my JSON IAM policy by stopping the production and development instances.

Stopping the production instance
When I tried to stop the production instance, I got an error message because of a lack of authorisation to access the instance.

Stopping the development instance

Next, when I tried to stop the development instance, it successfully stopped on first attempt which wasn't the case for the production instance.



AWS IAM is crucial for ensuring cloud security. It efficiently manages user access, permissions, and identity control, safeguarding your cloud environment from unauthorised access and promoting secure resource usage. Whether you're just starting out or are an experienced cloud professional, mastering IAM is essential for creating a secure cloud infrastructure.