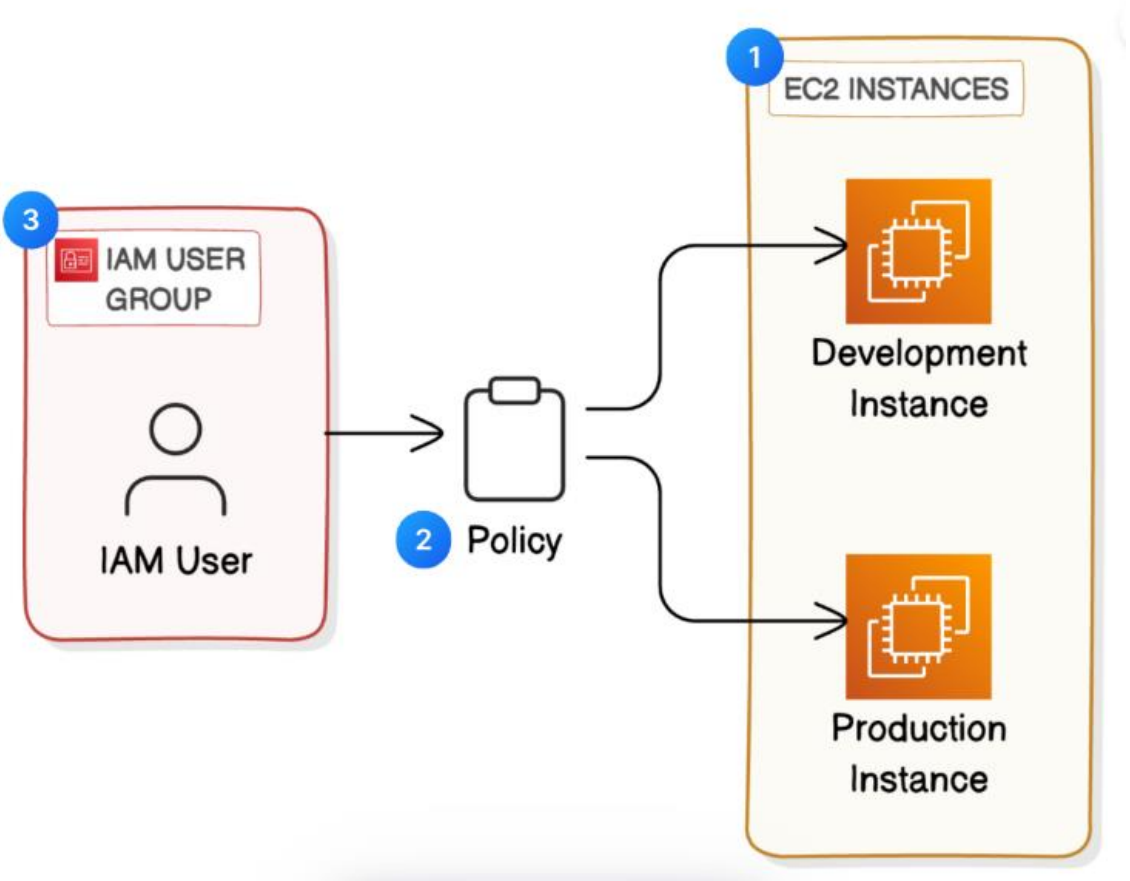
Cloud Securitywith AWS IAM

A Aviral Shukla



Introducing today's project!

What is AWS IAM?

AWS Identity and Access Management (IAM) is a service that helps you securely control access to AWS resources. It allows you to manage who can sign in (authentication) and what they can do (authorization) within your AWS account.

How I'm using AWS IAM in this project

Creating IAM Policies Setting Up IAM Users and Groups Testing Access Creating an Account aviral

One thing I didn't expect...

One thing that caught me off guard in this project was the unexpected error when trying to stop the development instance. It turned out that the instance was still configured to run a continuous integration process, which prevented it from stopping.

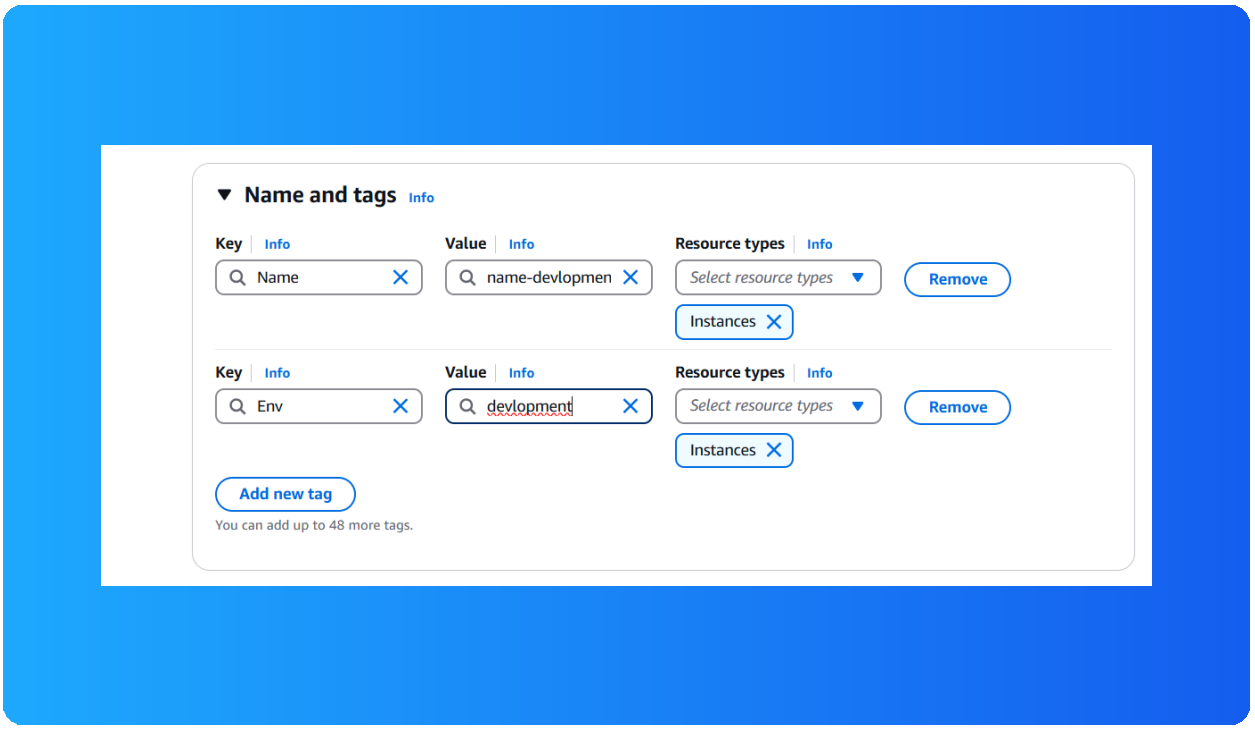
This project took me...

1 hour

Tags

Tags are labels to help AWS account user identify and manage their resources. Tags are useful for grouping mass mangement and applying security policies.

The tag I've used on my EC2 instances is called Env The value I've assigned for my instances are production and devlopment.



IAM Policies

IAM policies are rule that help to allow/deny users recources to perform certain action in my AWS account resources.

The policy I set up

I’ve set up a policy using JSON that allows all EC2 related action to all EC2 instances that have Environment ("Env") tag devlopment.

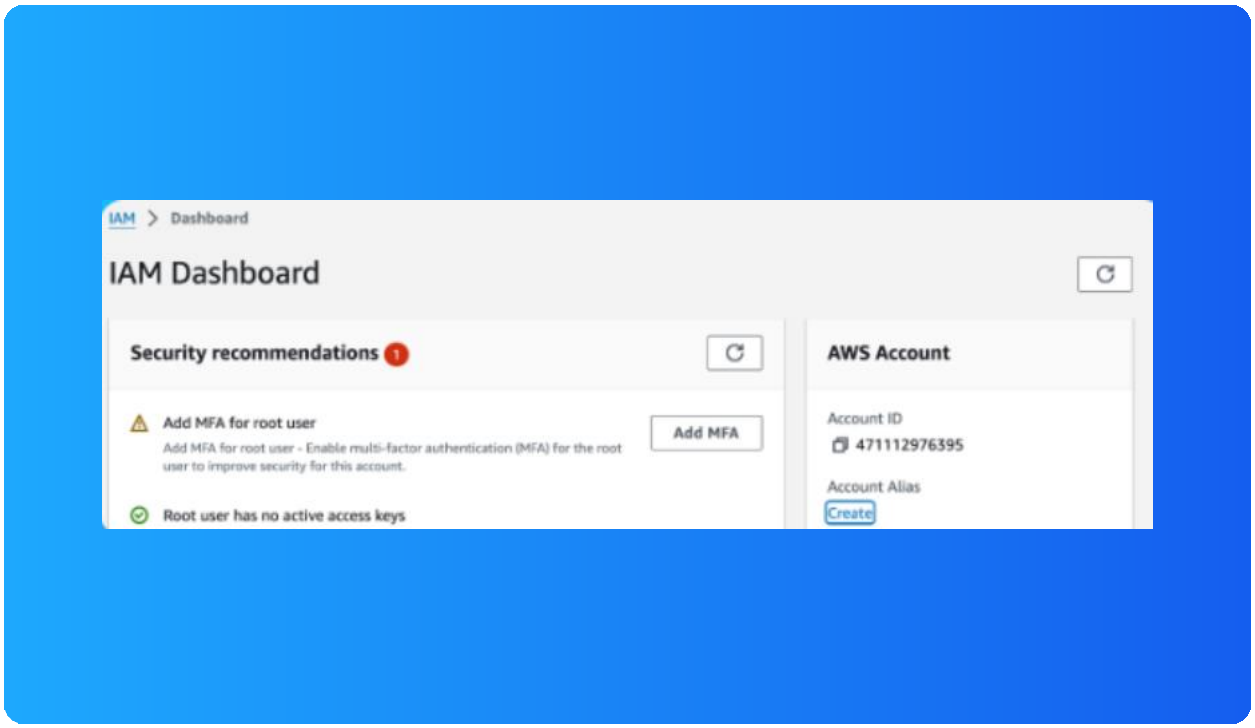
I’ve set up a policy using JSON that allows all EC2 related action to all EC2 instances that have Environment ("Env") tag "devlopment".But it also denies creating and deleting tags for all ec2 instances.

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

*Effect : allow /deny *Action : the specific action we want to allow or deny *Recources : the specific resources or group of resource/group in my AWS account that this policy will take effect on.

My JSON Policy

IAM dashboard



IAM Users and User Groups

Users

An IAM user is an entity that you create in your AWS account. The IAM user represents the human user or workload who uses the IAM user to interact with AWS resources. A IAM user consists of a name and credentials.

User Groups

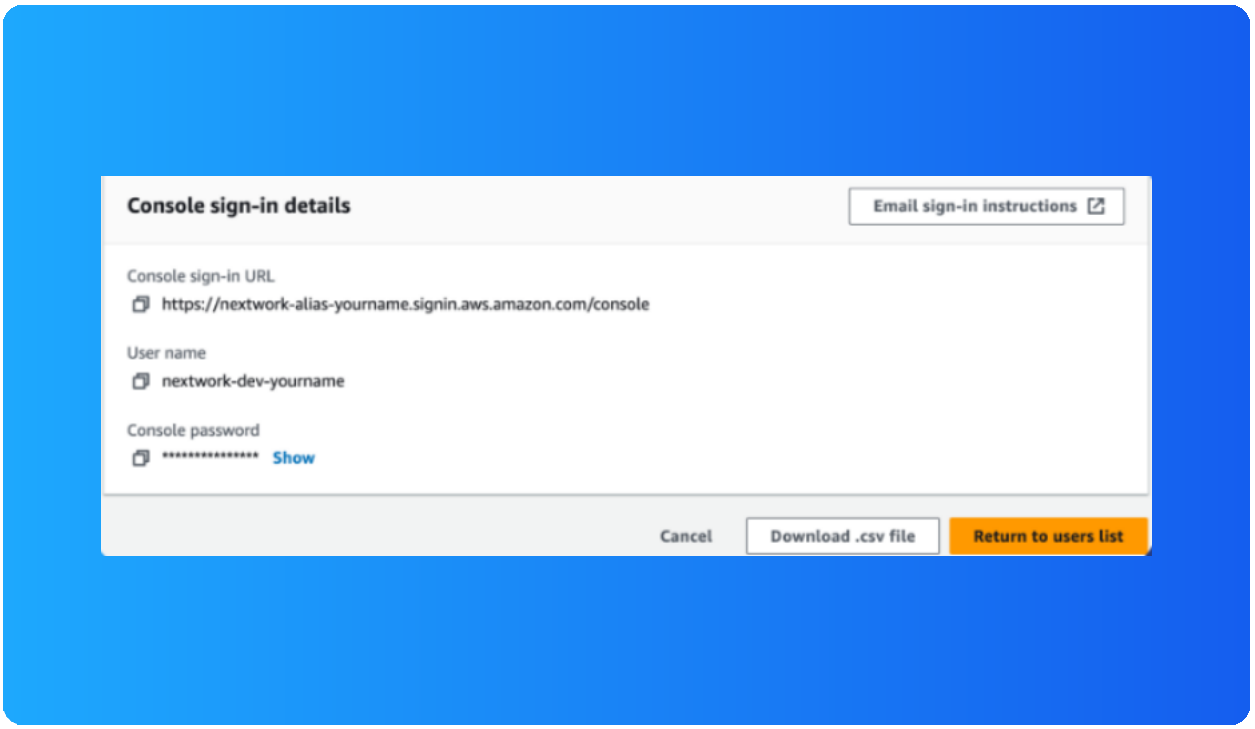
An IAM user group is a collection of IAM users. User groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users

Attaching your policy to a user group allows you to define permissions and access control for a group of users. This means that any changes you make to the policy will automatically apply to all users within the specified user group.

Logging in as an IAM User

1 : Direct sharing 2: Secure File Sharing

AWS Identity and Access Management Access Analyzer organizes external access and unused access findings into a visual summary dashboard. The dashboard helps you gain visibility into the effective use of permissions at scale and identify accounts .

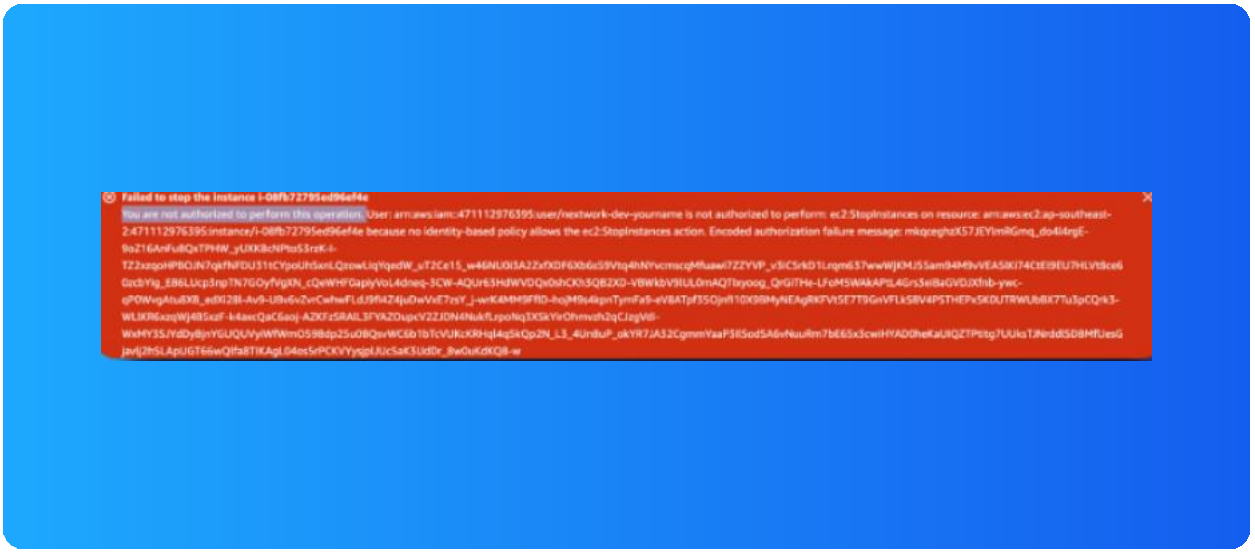


Testing IAM Policies

I tested my JSON IAM policy by launching two EC2 instances using the AWS CLI, one with the IAM role that has the policy attached and the other without. On the instance with the policy.

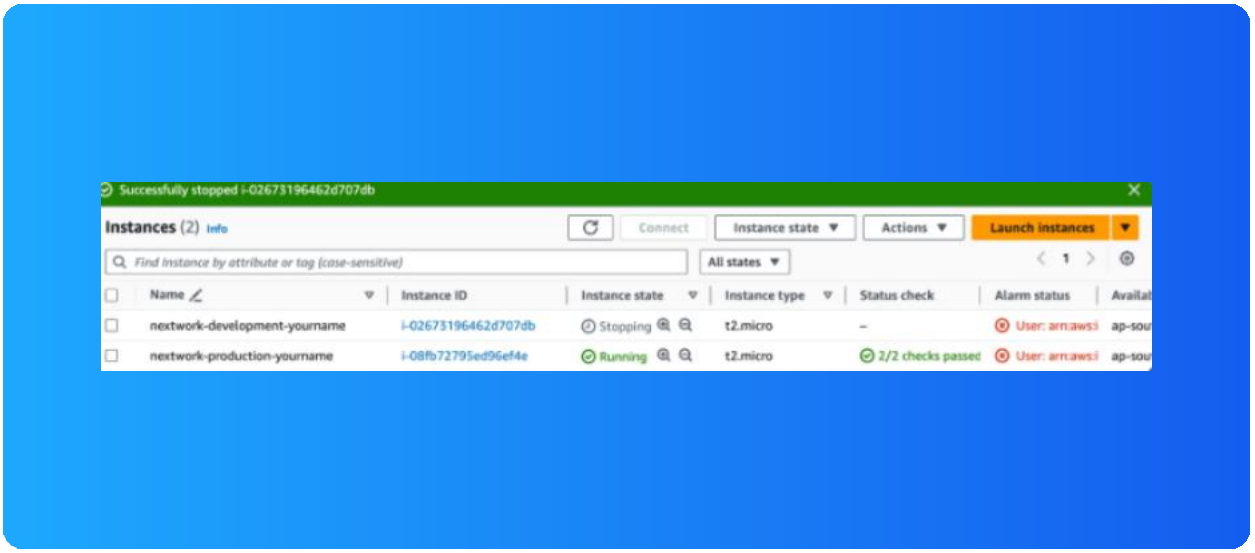
Stopping the production instance

When attempting to stop the production instance, I encountered an error. The instance was unable to be terminated due to an active connection to a dependent service. This is a common issue when trying to stop or terminate a production instance.



Testing IAM Policies

Stopping the development instance



Next, when I tried to stop the development instance, I encountered an error message indicating that the instance was in an "updating" state. This was because the development instance was still configured to run a continuous integration.

GitHub : https://github.com/aviralshukla12

Thank you !