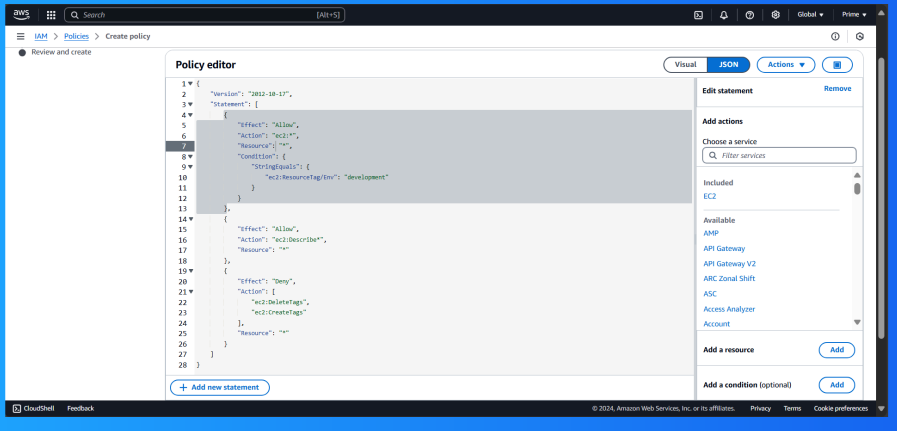
Cloud Security with AWS IAM

Unmilan Mukherjee



Introducing today's project!

What is AWS IAM?

AWS IAM stands for AWS Identity Access and Management. This allows us to attach policies/permissions to users to make sure that they only have access to the AWS resources that they need and nothing else.

How I'm using AWS IAM in this project

I used AWS IAM to create IAM groups and attach Policies to differentiate between development and production instances.

One thing I didn't expect...

I did not expect how robust and secure AWS has made user management on their platform. They have given us granular control over every user and resource.

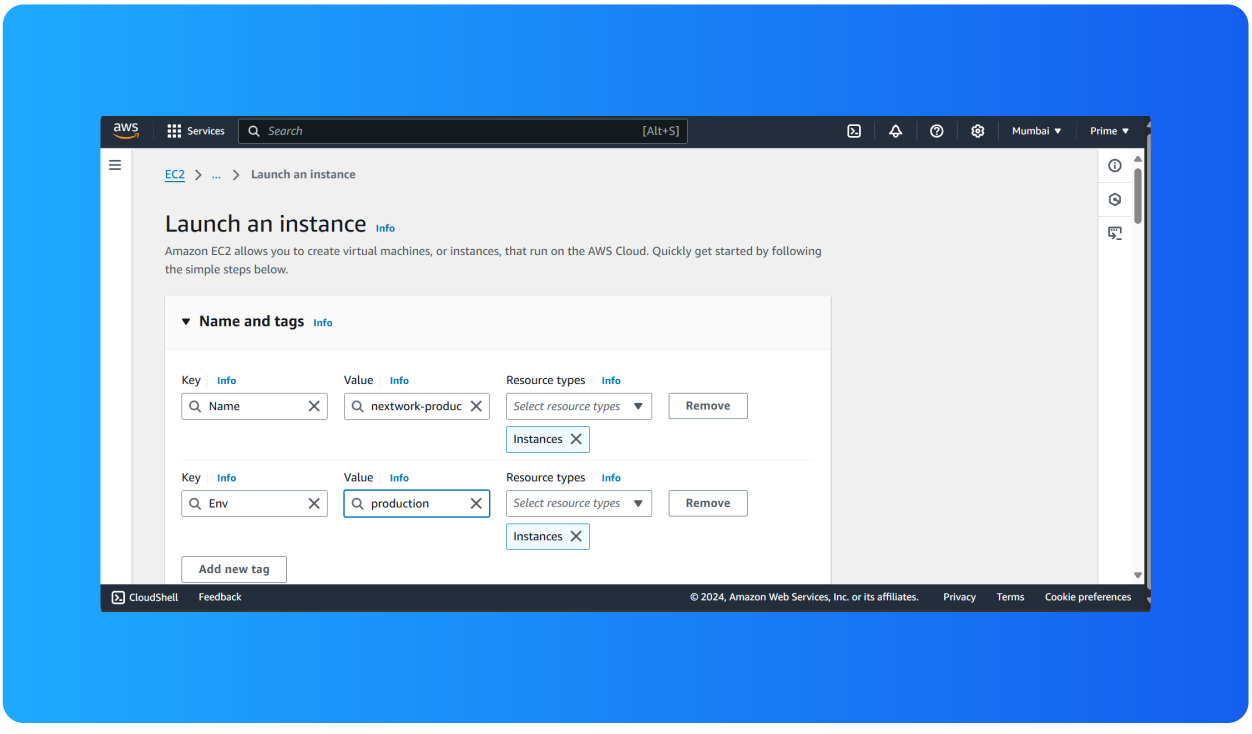
This project took me...

It took me 60 minutes to complete this entire project.

Tags

Tags are like labels for our instances. They allow us to easily identify what resource is for what purpose.

The tag I've used on my EC2 instances is called "Env". The value I've assigned for my instances are "development" and "production". These are for dev and prod environments respectively.



IAM Policies

IAM Policies are basically rules given to AWS that define who can do what on your AWS account. It allows you to give specific permissions to specific users.

The policy I set up

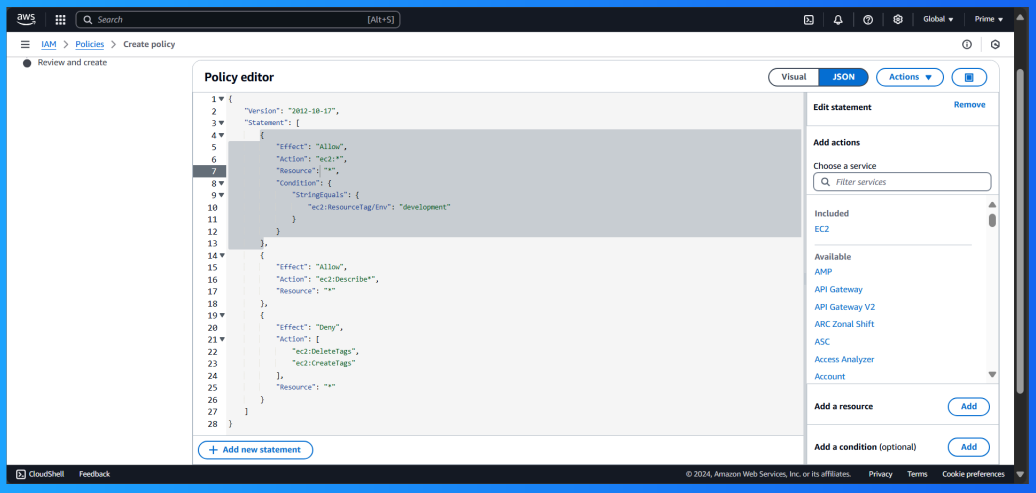
For this project, I've set up a policy using JSON.

I've created a policy that allows the user to create, start, stop, describe, etc EC2 instances when the instance has the Env=development tag while preventing the Creation or Deletion of Tags in that instance.

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 they allow/deny us an action(like create, delete, etc, etc) of an instance, in our case we use * for allowing all actions; Resource links these both to a particular resource on AWS.

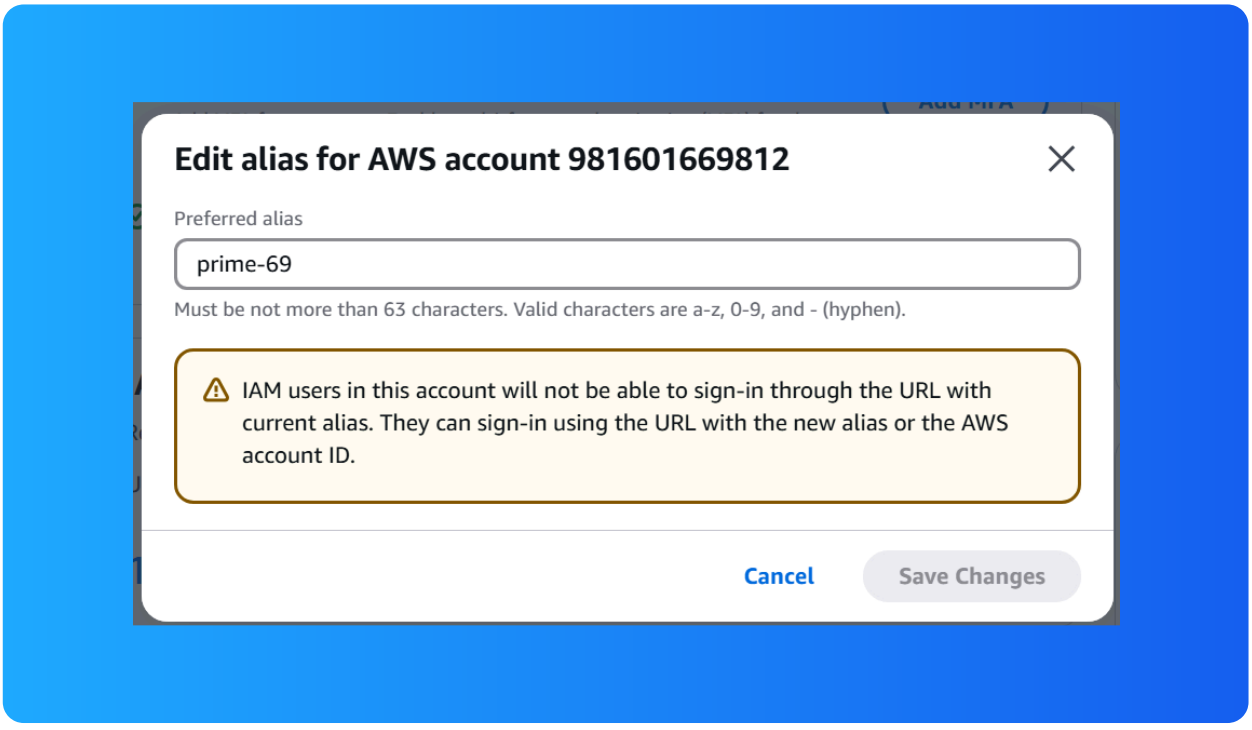
My JSON Policy



Account Alias

An account aliad is a friendly name for our AWS account(which is usually a bunch of random digits). This makes it easier to remember and share our console login.

It took me just 1 minute to create and set up my Account Alias. I had already created an alias so my popup is a warning rather than a creation page.



IAM Users and User Groups

Users

IAM users are users or employees of our companies with certain policies attached to them. This means that the permissions and actions they can perform on the AWS platform is controlled and limited to maintain heirarchy.

User Groups

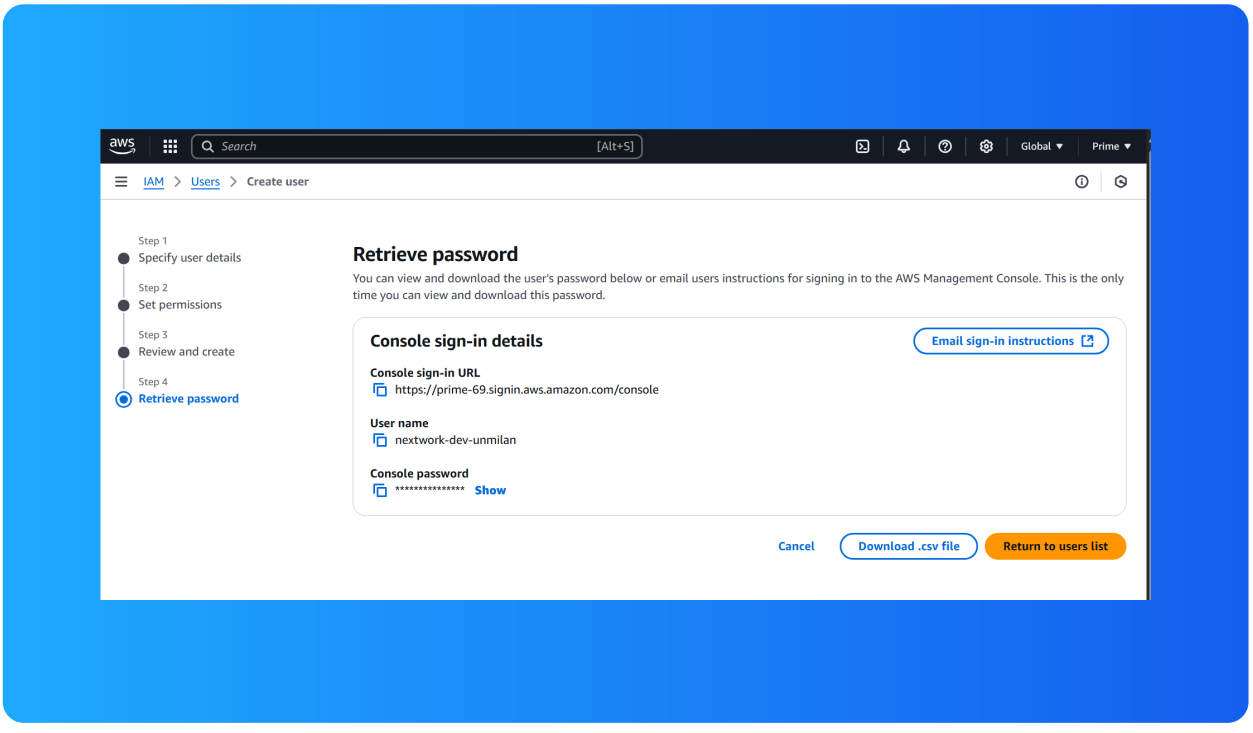
IAM user groups are basically a common set of policies and permissions attached to a group so that we can make it easier to manage permission among a huge team. So it allows us to grant different permissions to different departments in our workplace.

I attached the policy I created to this user group, which means that anybody in this IAM user group can do any EC2 action on a instance with Env=development tag minus creating/editing or deleting tags.

Logging in as an IAM User

The first way is to share it through an email. The second way is to download a .csv file with the login details.

Once I logged in as my IAM user, I noticed that the dashboard was completely empty and AWS gave me a quick guide of the UI. It also gave me some dashboard panels with Access denied warning as my IAM user is a new user with limited permissions.

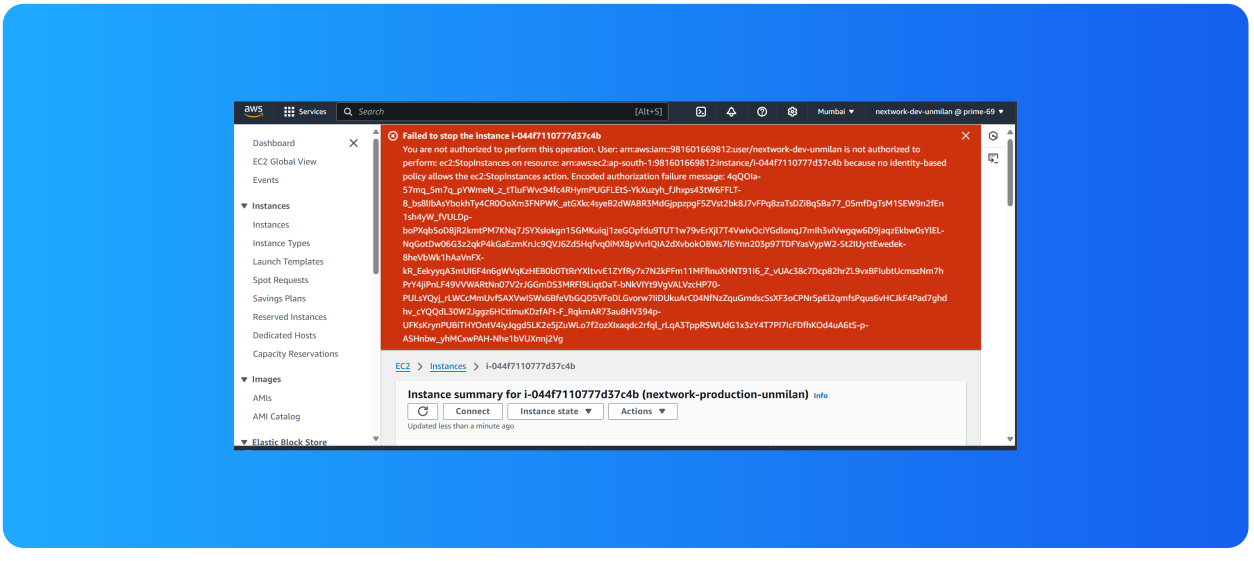


Testing IAM Policies

I tested my JSON IAM policy by trying to First: Stop the production instance; Second: Stop the development instance. The production instance gave me an error as expected.

Stopping the production instance

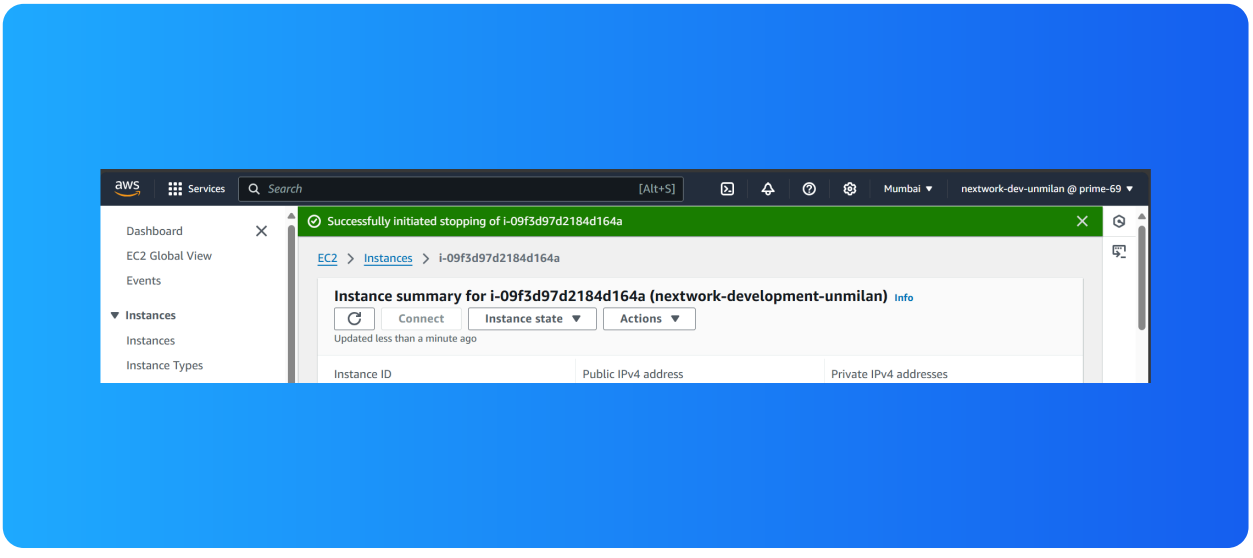
When I tried to stop the production instance, it gave me a error and blocked me from doing that action. This was because according to the Policies attached to the IAM group, it can only do actions in the Env=development tagged instances.



Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance it successfully allowed me to stop it. This was because according to the Policy in my IAM group, its users can do any action in the EC2 instances tagged with Env=development.



The IAM Policy Simulator

The IAM Policy Simulator is a service that allows us to test our IAM Policies. It's useful for testing if our policies are working without disrupting the other users or developers by manually interfering with the instances.

How I used the simulator

I set up a simulation for DeleteTags and StopInstances Actions. The results were denied. I had to adjust the instance type of the StopInstance Action from * to development and the tests returned positive.