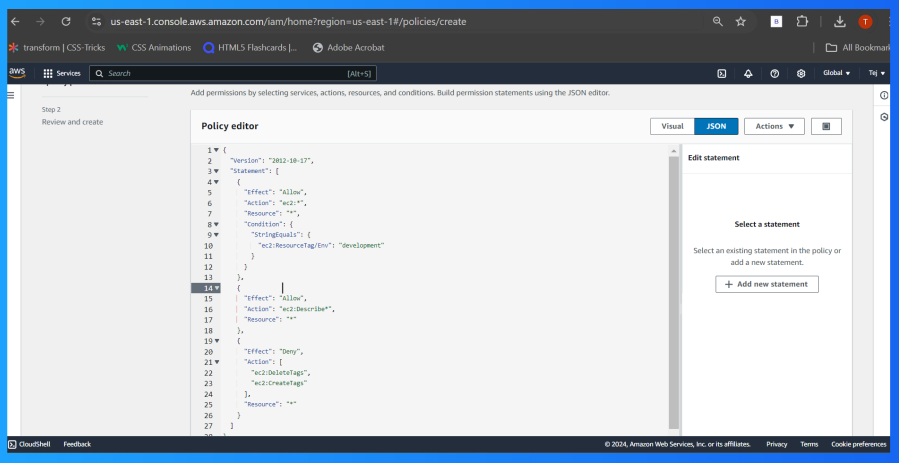
Cloud Security with AWS IAM

Tej Mandaliya



Tej Mandaliya

Introducing today's project!

What is AWS IAM?

AWS IAM (Identity and Access Management) is a service that enables you to securely manage access to AWS resources by creating and controlling user permissions, enhancing security and compliance.

How I'm using AWS IAM in this project

easily

One thing I didn't expect...

One thing I didn't expect in this project was the complexity of managing fine-grained permissions within IAM policies, which significantly impacts security and access control.

This project took me...

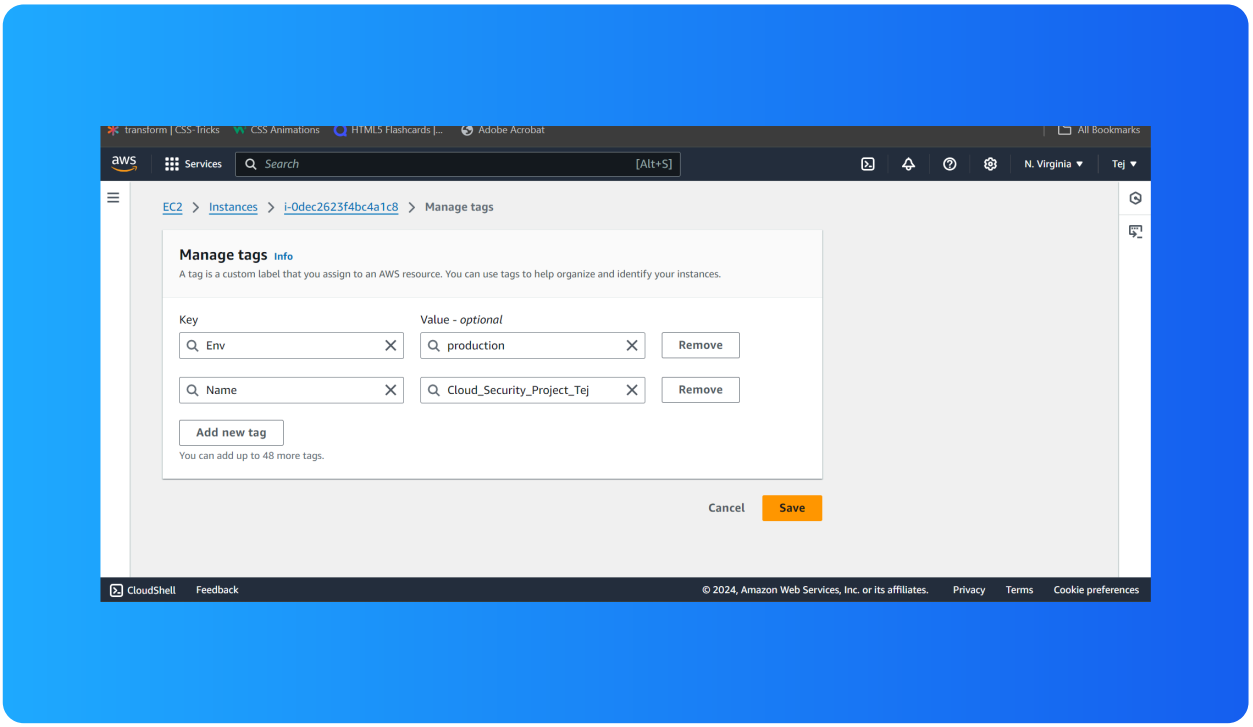
30 minutes

Tej Mandaliya

—

Tags are like labels you can attach to AWS resources for organization.

The tag I've used on my EC2 instances is called "Environment". The value I've assigned for my instances is "Production".



Tej Mandaliya

IAM Policies

An IAM policy is a rule for who can do what with your AWS resources. It's all about giving permissions to IAM users, groups, or roles, saying what they can or can't do on certain resources, and when those rules kick in.

The policy I set up

You can create and edit AWS policies in the visual editor or JSON. In this project, i have used the JSON method.

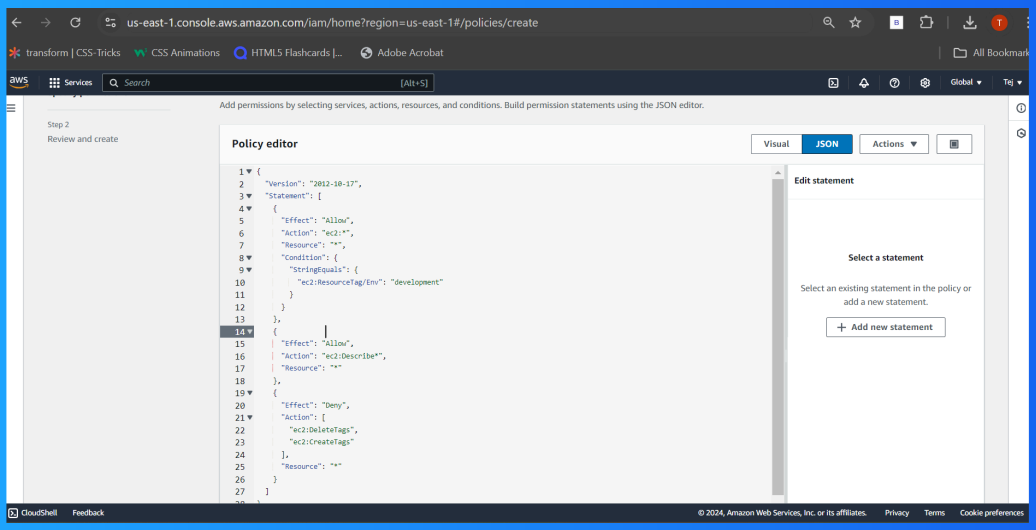
This policy allows some actions (like starting, stopping, and describing EC2 instances) for instances tagged with "Env = development" while denying the ability to create or delete tags for all instances

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

The attributes of a JSON policy mean: Effect: Defines whether the action is "Allow" or "Deny". Action: Specifies what actions (like ec2:StartInstances) are allowed or denied. Resource: Identifies the specific AWS resource affected

Tej Mandaliya

My JSON Policy



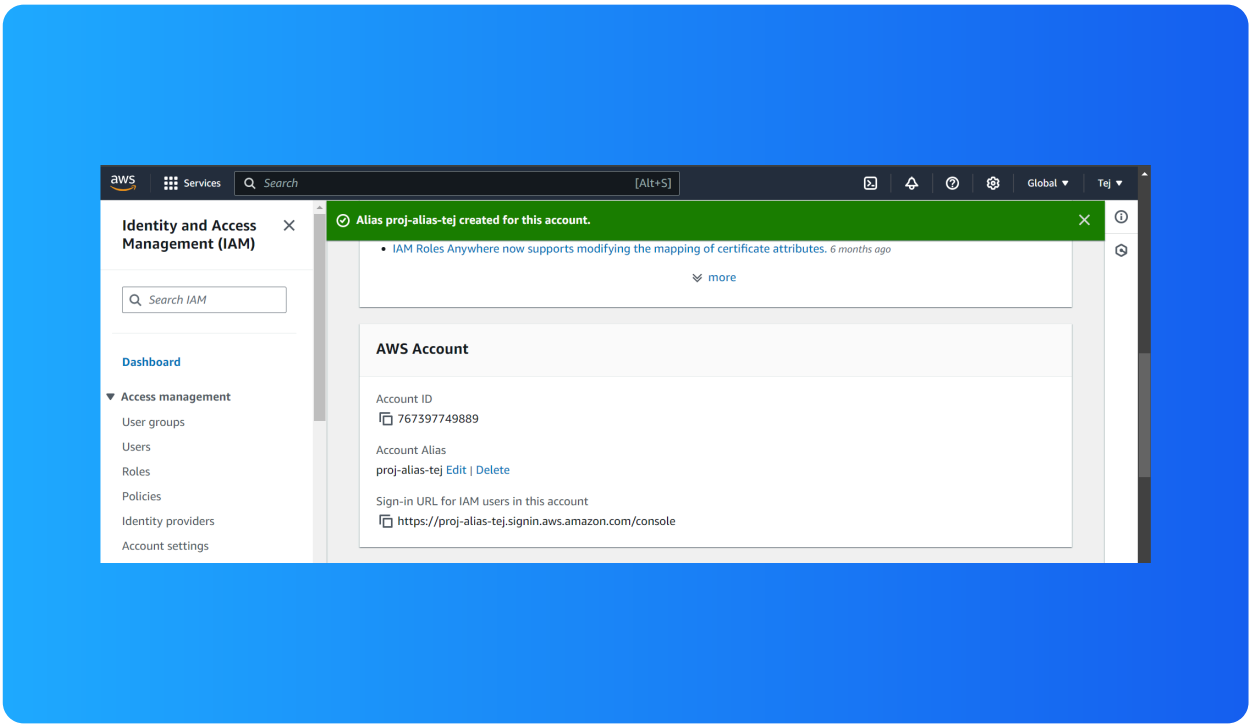
Tej Mandaliya

Account Alias

An Account Alias is a friendly name for your AWS account that you can use instead of your account ID (which is usually a bunch of digits) to sign in to the AWS Management Console.

Creating an account alias took me within 5 Minutes

Now, my new AWS console sign-in URL is https://proj-alias-tej.signin.aws.amazon.com/console



Tej Mandaliya

IAM Users and User Groups

Users

IAM users are individual identities in AWS that have specific permissions to access and manage AWS resources.

User Groups

An IAM user group is a collection/folder of IAM users. It allows you to manage permissions for all the users in your group at the same time by attaching policies to the group rather than individual users.

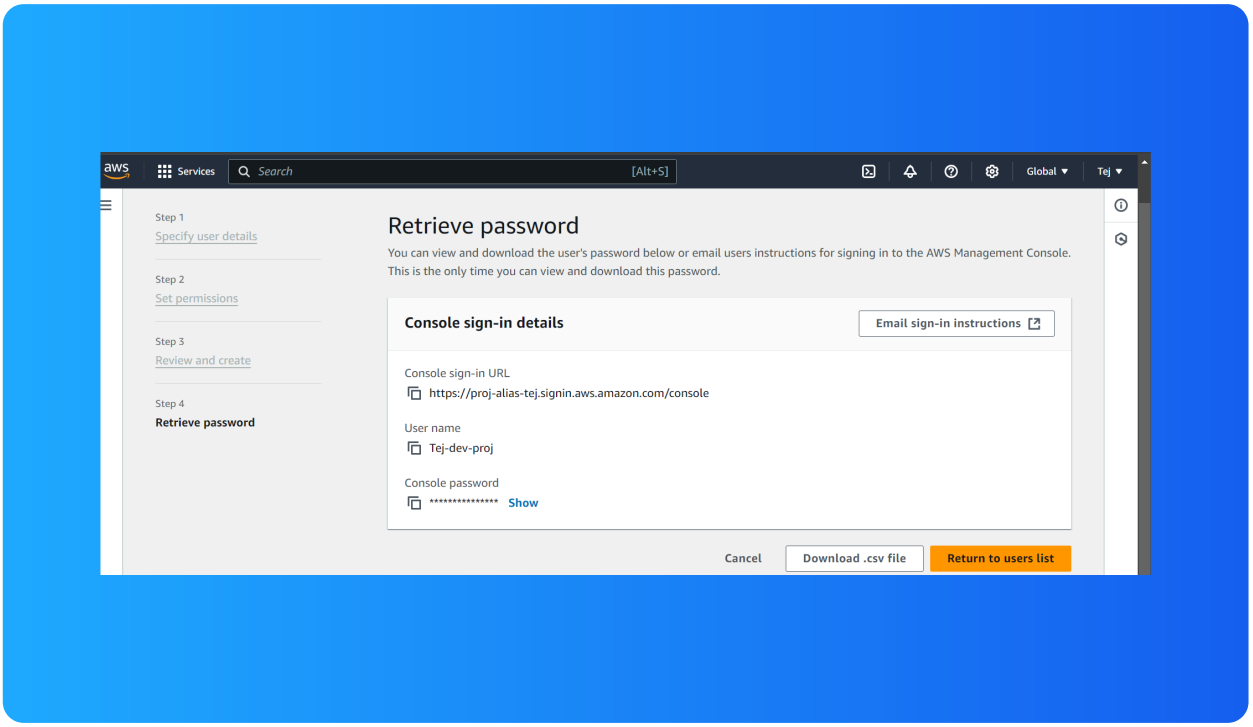
I attached the policy I created to this user group, which means all users in the group inherit the permissions defined in the policy.

Tej Mandaliya

Logging in as an IAM User

The first way is to send the sign-in URL and credentials via email, and the second way is to provide the information manually or through a secure method like a password manager.

Once I logged in as my IAM user, I observed limited access based on the permissions granted by the attached policies.



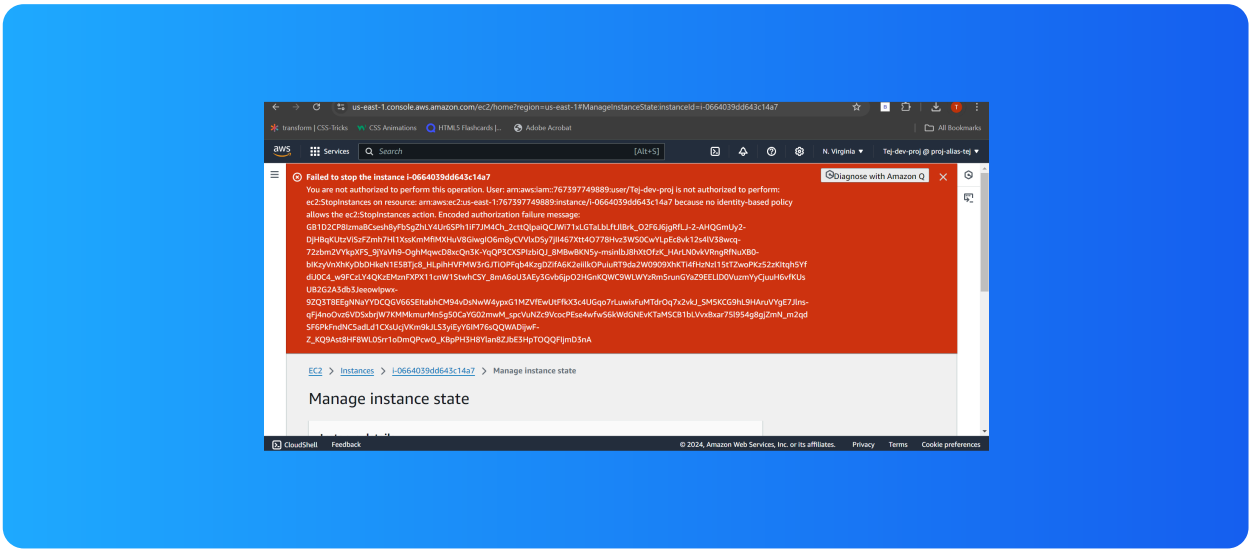
Tej Mandaliya
|

Testing IAM Policies

I tested my JSON IAM policy by starting and stopping my two EC2 instances.

Stopping the production instance

When I tried to stop the production instance, the action was denied due to the IAM policy restrictions.

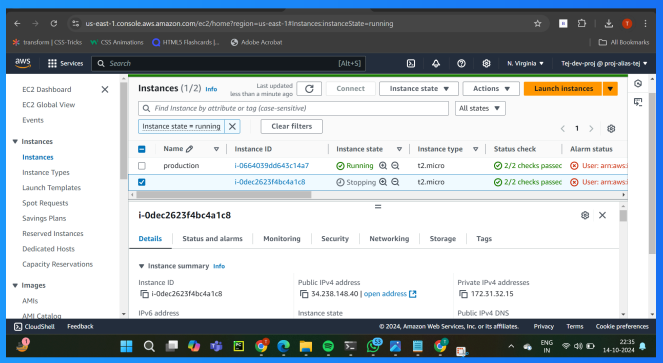


Tej Mandaliya

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, the action was successfully allowed.



END