NextWork.org

Cloud Security with AWS IAM

S Suyash Joshi

S

Suyash Joshi
NextWork Student

NextWork.org

Introducing today's project!

What is AWS IAM?

AWS IAM is a service for managing access to AWS resources. It's useful because it controls who can do what in your AWS environment, ensuring security and proper access management.

How I'm using AWS IAM in this project

I used AWS IAM in today's project to create and manage user access by setting up policies and user groups. This ensured that only authorized users could perform specific actions on our EC2 instances.

One thing I didn't expect...

One thing I didn't expect in this project was how straightforward it was to enforce granular permissions using IAM policies. It made managing access more efficient than I initially anticipated.

This project took me...

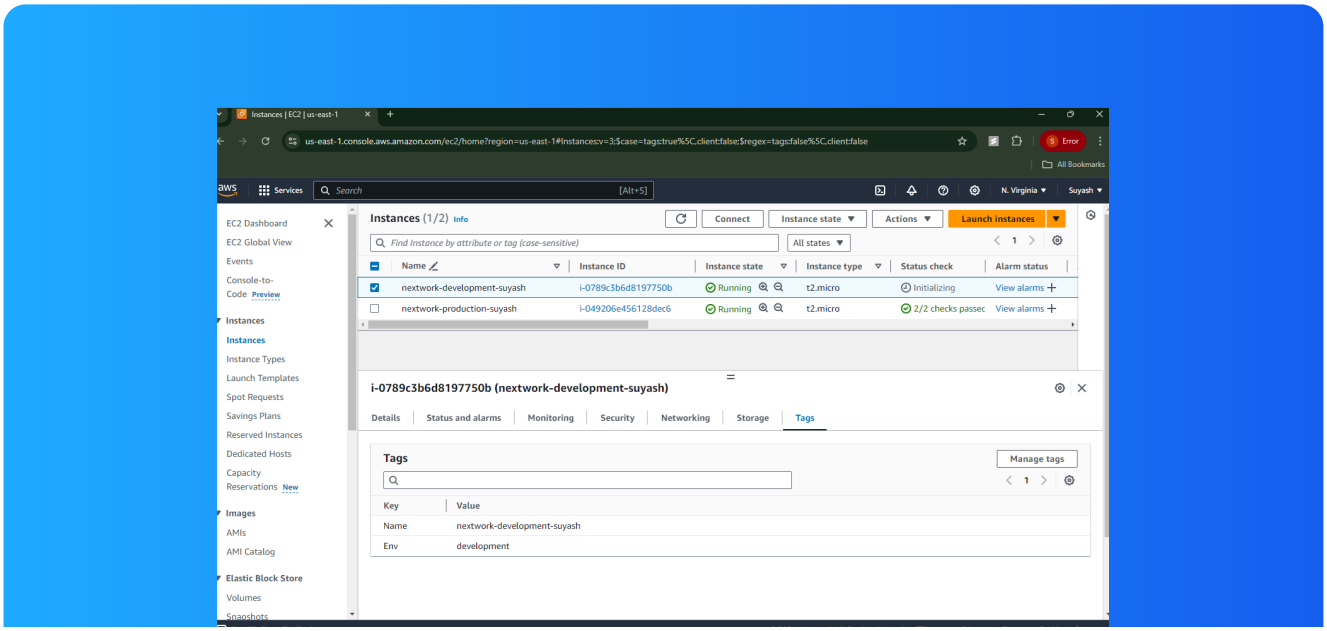
This project took me about 40 mins to complete.

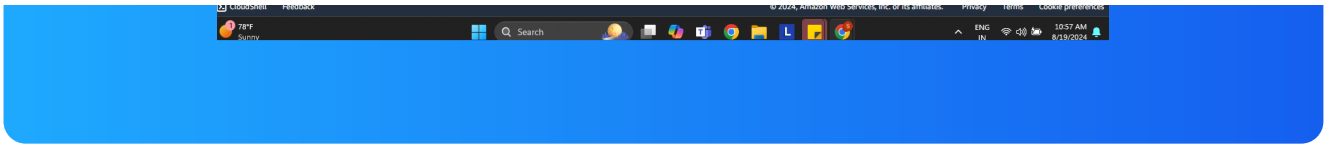
Suyash Joshi
NextWork Student
NextWork.org

Tags

Tags are labels that you attach to AWS resources, consisting of key-value pairs. They are useful for organizing, managing, and identifying resources, enabling easier filtering, cost allocation, and applying specific policies across your AWS env.

The tag I've used on my EC2 instances is called "Env." The values I've assigned for my instances are "production" for the first instance and "development" for the second instance.





S

Suyash Joshi
NextWork Student

NextWork.org

IAM Policies

IAM Policies are rules that control access to AWS resources. They define what actions users or services can or cannot perform.

The policy I set up

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

I've created a policy that allows actions on EC2 instances with the "development" tag and denies the ability to create or delete tags on any instance.

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

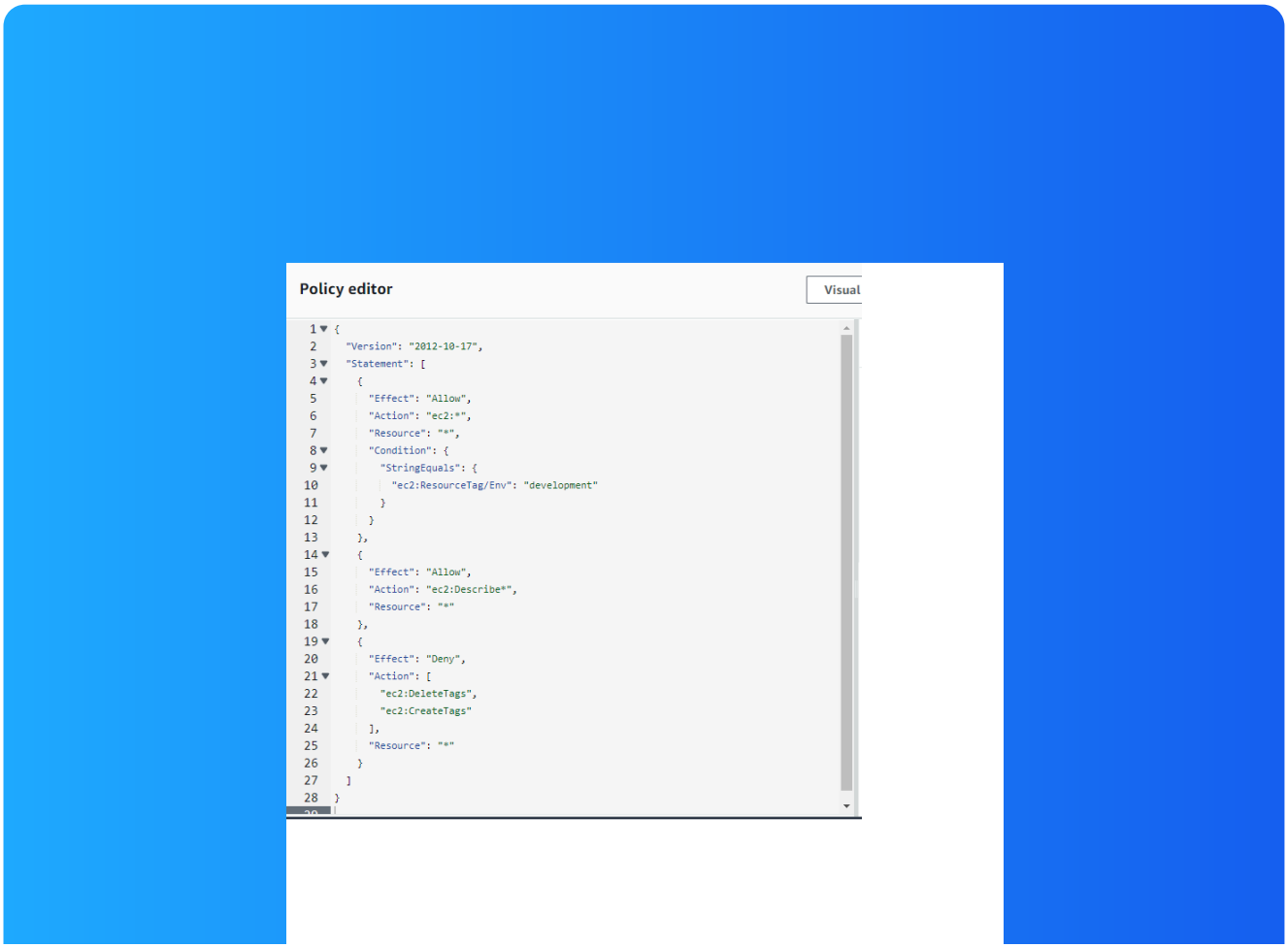
The Effect, Action, and Resource attributes define whether an action is allowed or denied, what the action is, and which resources it applies to.

S

Suyash Joshi
NextWork Student

NextWork.org

My JSON Policy



S

Suyash Joshi
NextWork Student

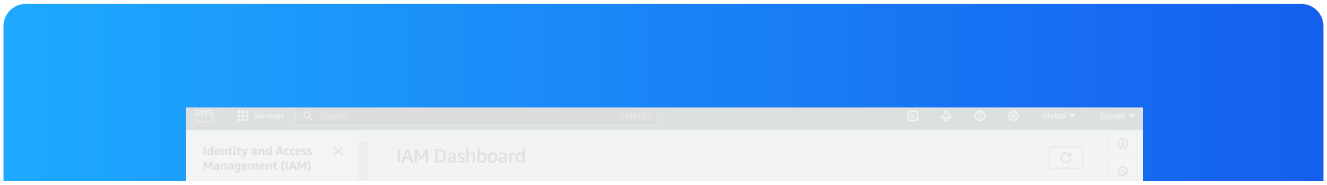
NextWork.org

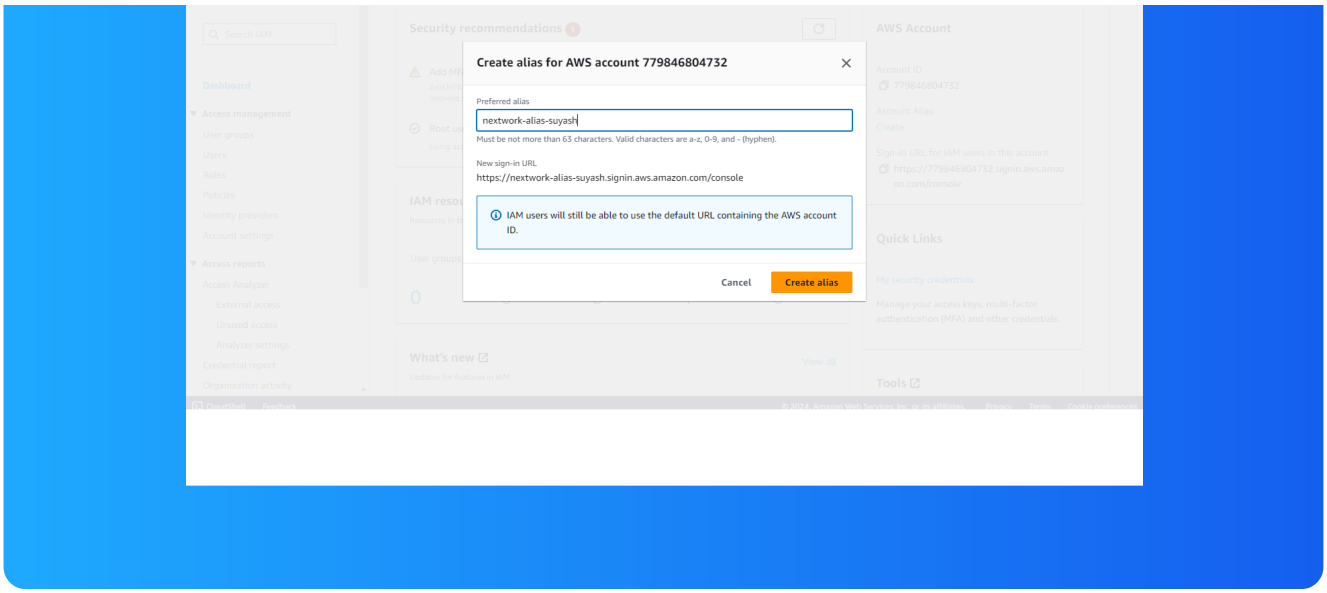
Account Alias

An account alias is a user-friendly name that you create to replace the default AWS account ID in your sign-in URL. This makes it easier to remember and share the login link with others.

Creating an account alias took me just a few minutes.

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





S

Suyash Joshi
NextWork Student

NextWork.org

IAM Users and User Groups

Users

IAM users are individual identities within your AWS account, each with unique credentials. They represent people or applications that need access to AWS resources.

User Groups

IAM user groups are collections of IAM users that allow you to manage permissions for multiple users simultaneously. They simplify administration by applying the same policies to all users within the group.

I attached the policy I created to this user group, which means all users in the group now have the permissions defined by the policy. This ensures consistent access control for everyone in the group.

S

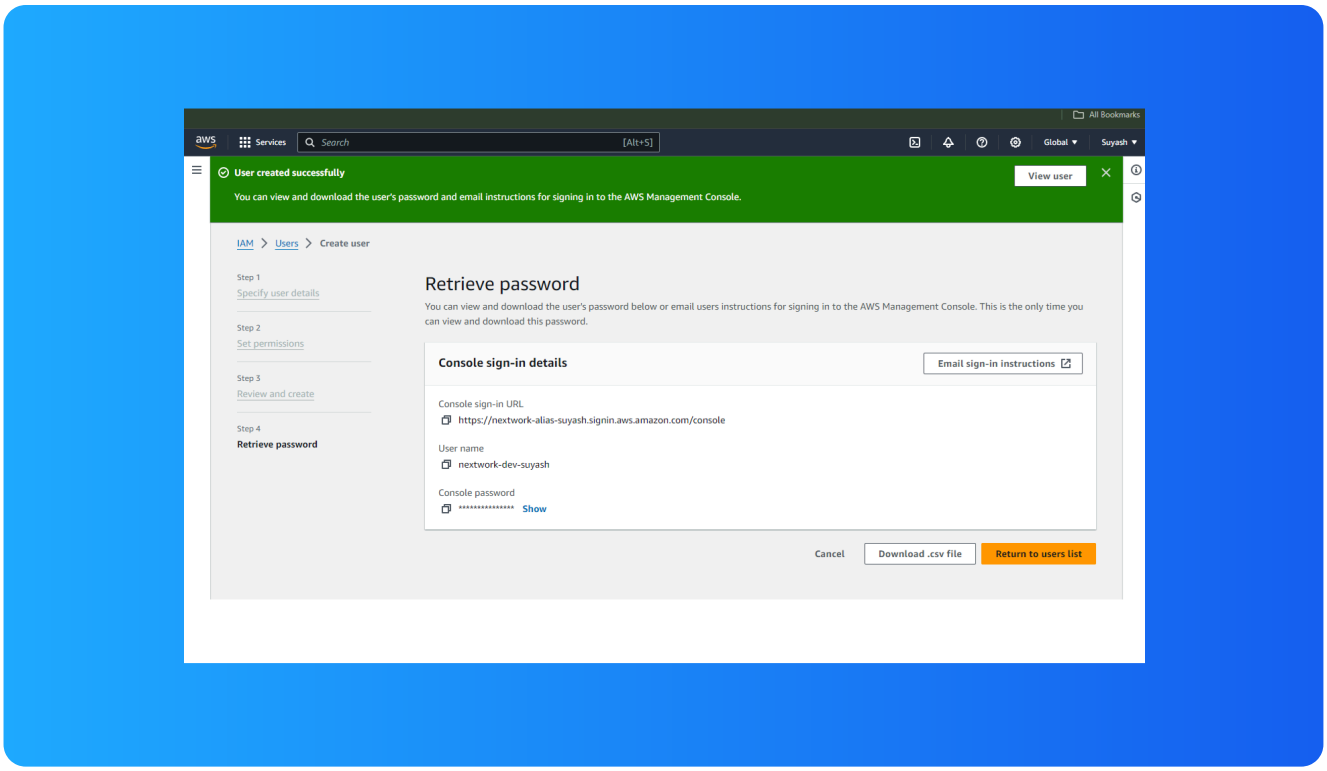
Suyash Joshi
NextWork Student

NextWork.org

Logging in as an IAM User

The first way is to download the user sign-in credentials as a CSV file. The second way is to send the sign-in URL directly to the new user via email.

Once I logged in as my IAM user, I noticed that some dashboard panels displayed "Access denied" due to the restricted permissions. This indicated that the user could only access specific resources allowed by the attached policy.



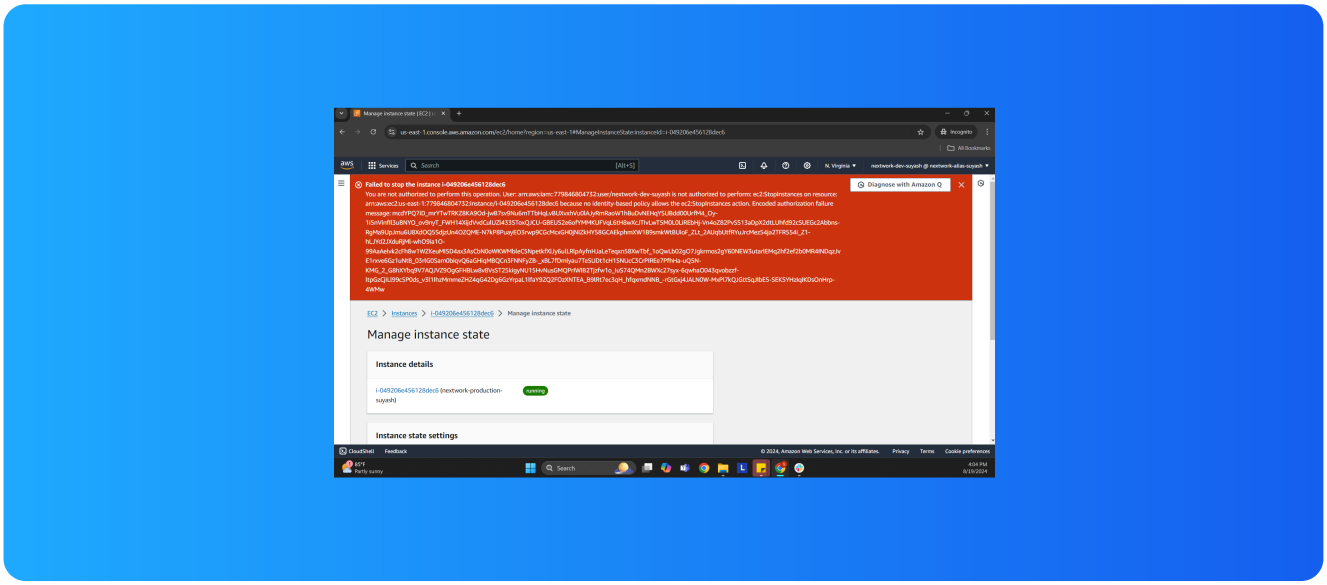
Suyash Joshi
NextWork Student
NextWork.org

Testing IAM Policies

I tested my JSON IAM policy by attempting to stop both EC2 instances. The policy correctly allowed me to stop the development instance while denying the stop action on the production instance.

Stopping the production instance

When I tried to stop the production instance, I received an "Access denied" error message. This was due to the policy restricting actions on instances tagged as production.



S

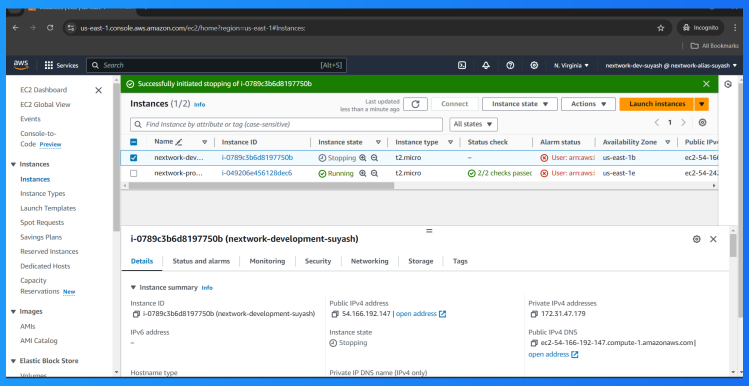
Suyash Joshi
NextWork Student

NextWork.org

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, the action was successful. The policy allowed this operation since the instance was tagged as development.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects