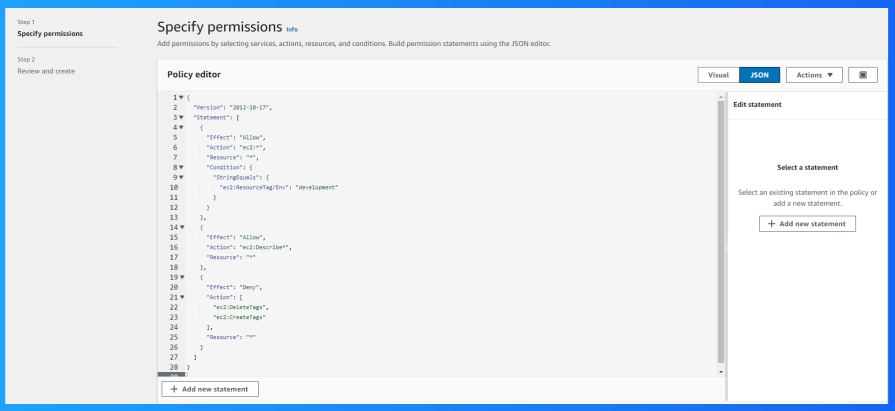
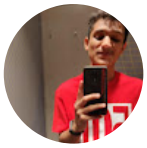
NextWork.org

Cloud Security with AWS IAM

Samarth Varu





Samarth Varu
NextWork Student

Introducing today's project!

What is AWS IAM?

AWS IAM (Identity and Access Management) controls access to AWS resources securely. It allows you to create users, groups, and roles with granular permissions manage temporary credentials.

How I'm using AWS IAM in this project

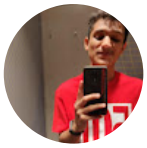
By using policy and attaching it to user group. Then creating a new IAM user and adding the user to user group. That way, I gave the IAM user the permission to stop only the development instance and also prevented from deleting any tags.

One thing I didn't expect...

The versatility of IAM.

This project took me...

It took me 25 mins to complete the project.

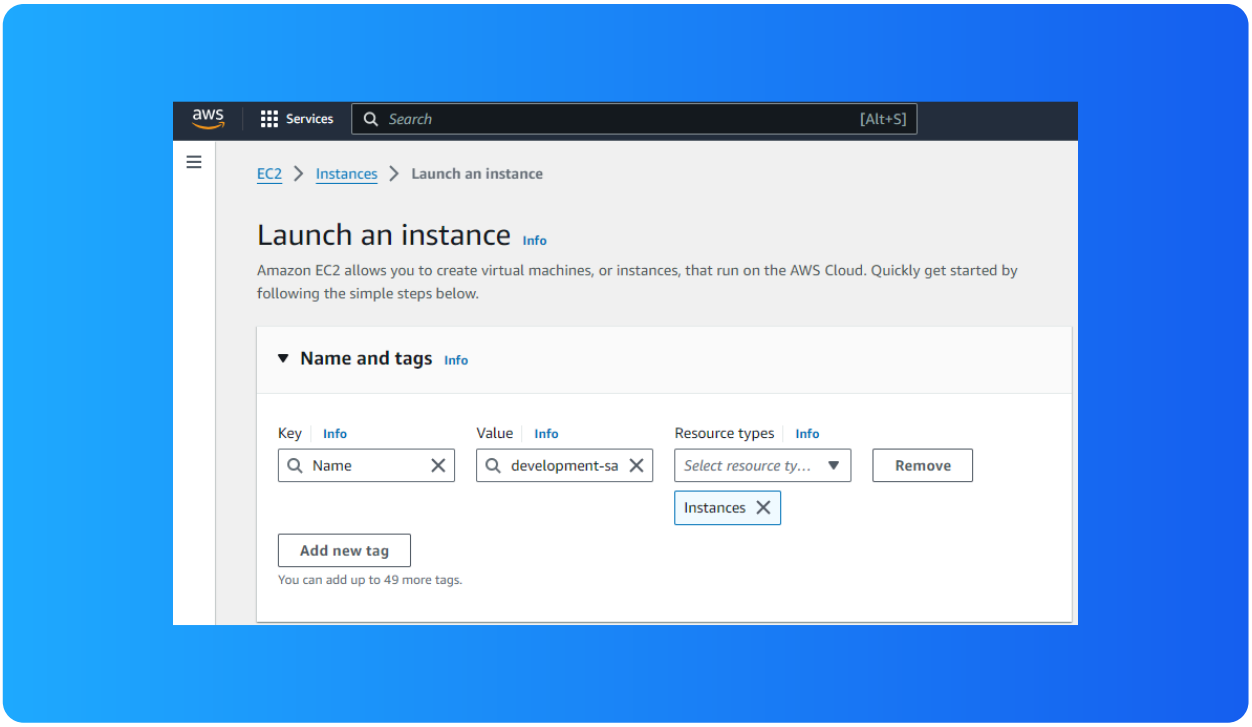


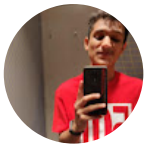
Samarth Varu
NextWork Student

Tags

ags are like labels you can attach to AWS resources for organization. In this case, we're creating a tag called "Env" with a value of "production" or "development" to label the instances used in production vs development environments.

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





Samarth Varu
NextWork Student

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

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

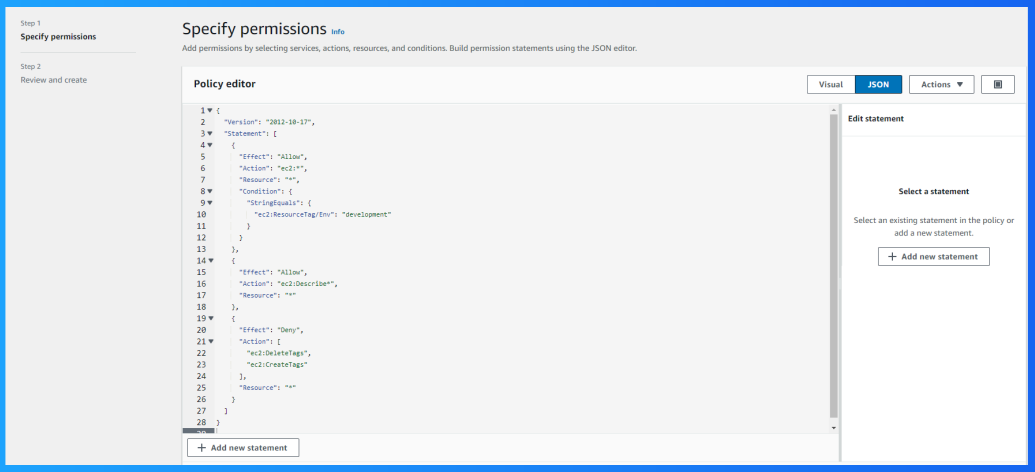
This policy allows some actions (like starting, stopping, and describing EC2 instances) for instances tagged with "Env = development" while denying the ability to create or delete tags for all instances.

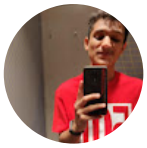
When creating a JSON policy, you have to define its Effect, Action and Resource.

Effect means Allow or Deny. Action means list of actions to allow or deny. Resource attributes specify the resource for this policy.

Samarth Varu
NextWork Student

My JSON Policy





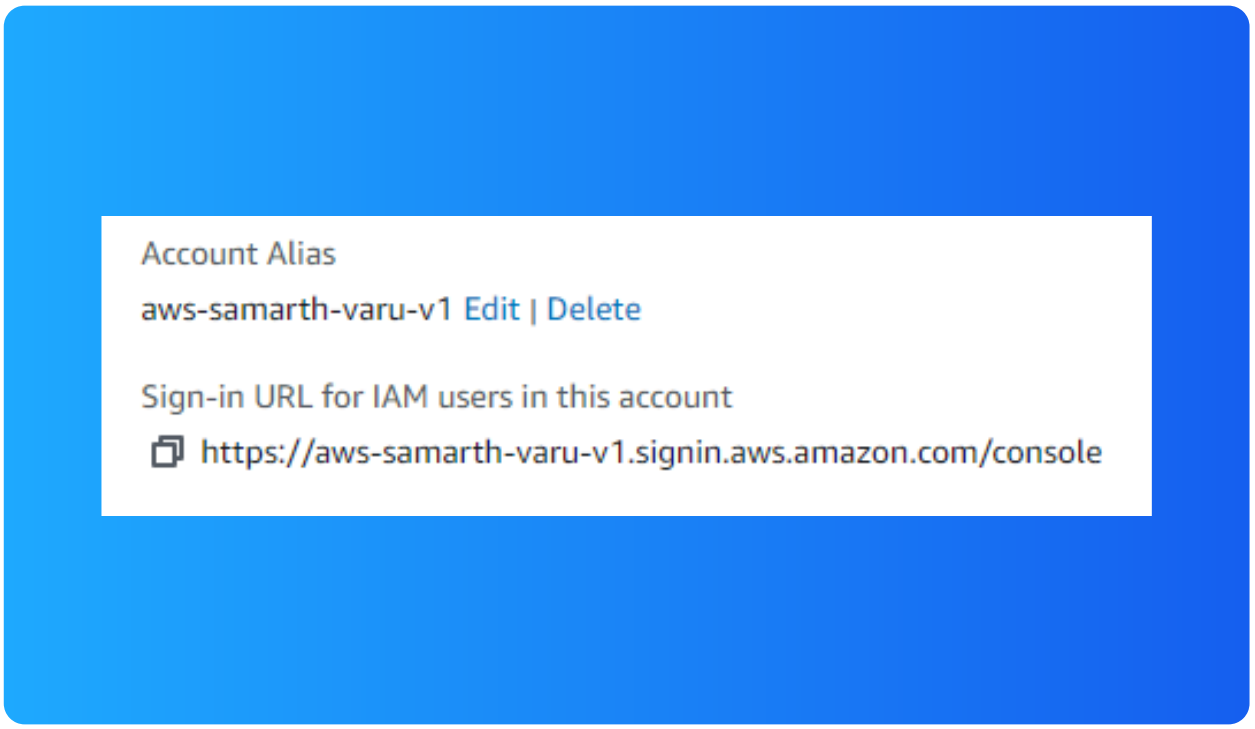
Samarth Varu
NextWork Student

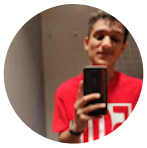
Account Alias

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 just took me 2 minutes.

Now, my new AWS console sign-in URL is https://aws-samarth-varu-v1.signin.aws.amazon.com/console





Samarth Varu
NextWork Student

IAM Users and User Groups

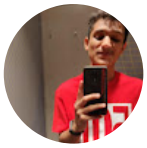
Users

IAM users are the people that will get access to your resources/AWS account, whereas user groups are the collections/folders of users for easier user management.

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.

This simplifies managing permissions and ensures consistency across users who have similar access to AWS resources.

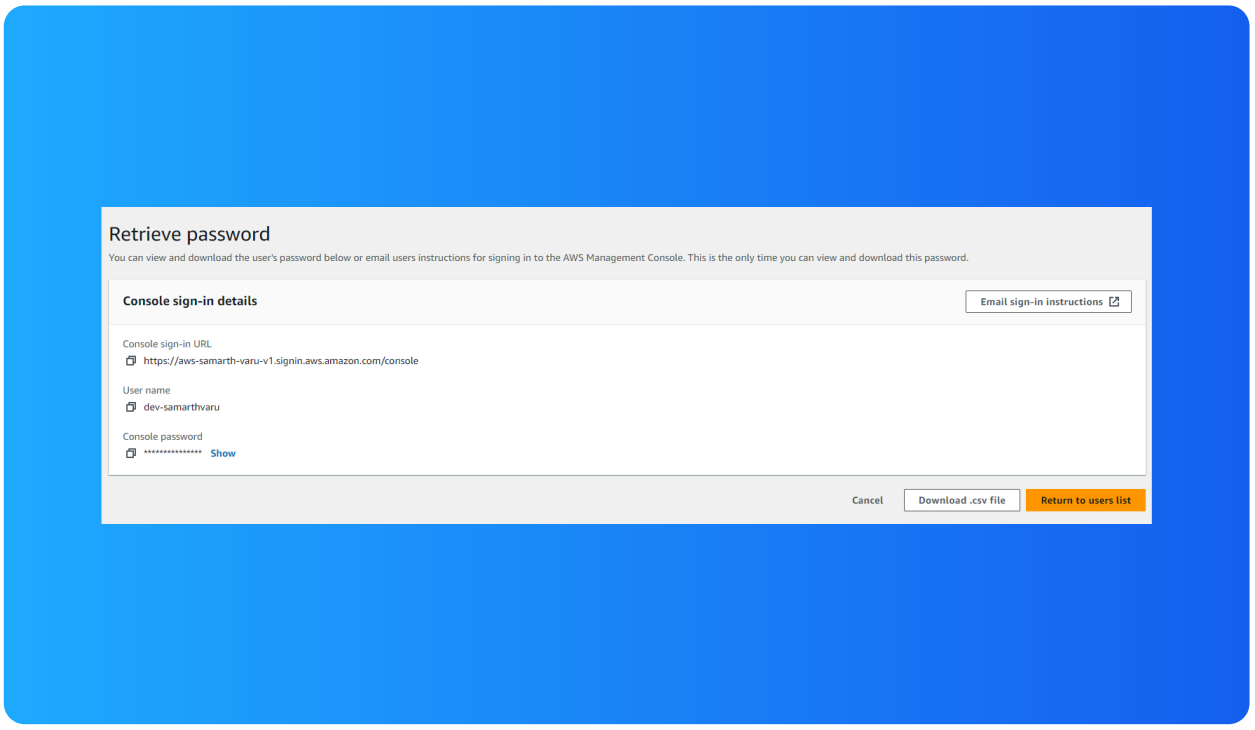


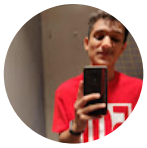
Samarth Varu
NextWork Student

Logging in as an IAM User

By giving them the temporary sign in url.

Once I logged in as my IAM user, I noticed I dont have access to most of the services.





Samarth Varu
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by trying to stop the production instance and development instance.

Stopping the production instance

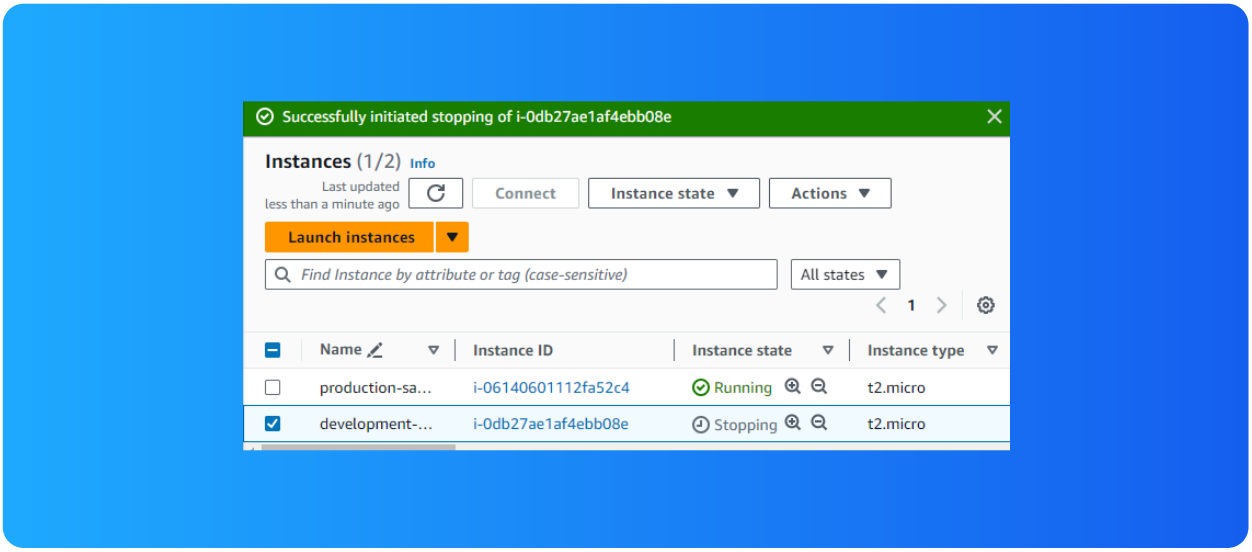
When I tried to stop the production instance, I got error, as I don't have permission to do it.

Samarth Varu
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, I was able to do it due to policy we defined earlier.



Everyone should be in a job they love.

Check out nextwork.org for more projects