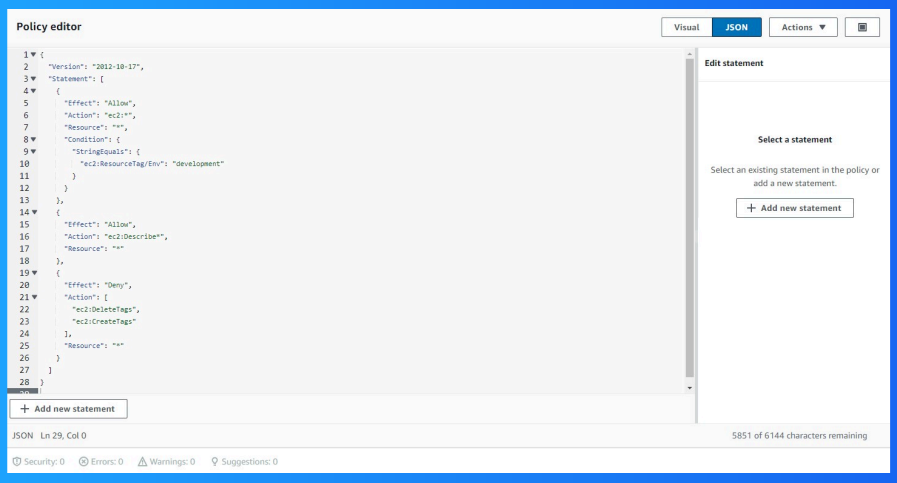
NextWork.org

Cloud Security with AWS IAM

Nikhil Bhan



N
Nikhil Bhan
NextWork Student
NextWork.org

Introducing today's project!

What is AWS IAM?

IAM stands for Identity Access Management. This AWS service is used to manage user access to AWS resources. It secures resources within an organization by controlling user access through permissions.

How I'm using AWS IAM in this project

In this project I used IAM to: - Create a Policy that restricted user access to EC2 instances by using tags - Create a User Group and assigned a policy to manage multiple users - Create a User and assigned them to a user group to grant permissions

One thing I didn't expect...

I wasn't expecting to learn how easy it was to use the IAM Policy Simulator to test permissions in my AWS environment. I found that useful and I'll use this when I develop my own projects.

This project took me...

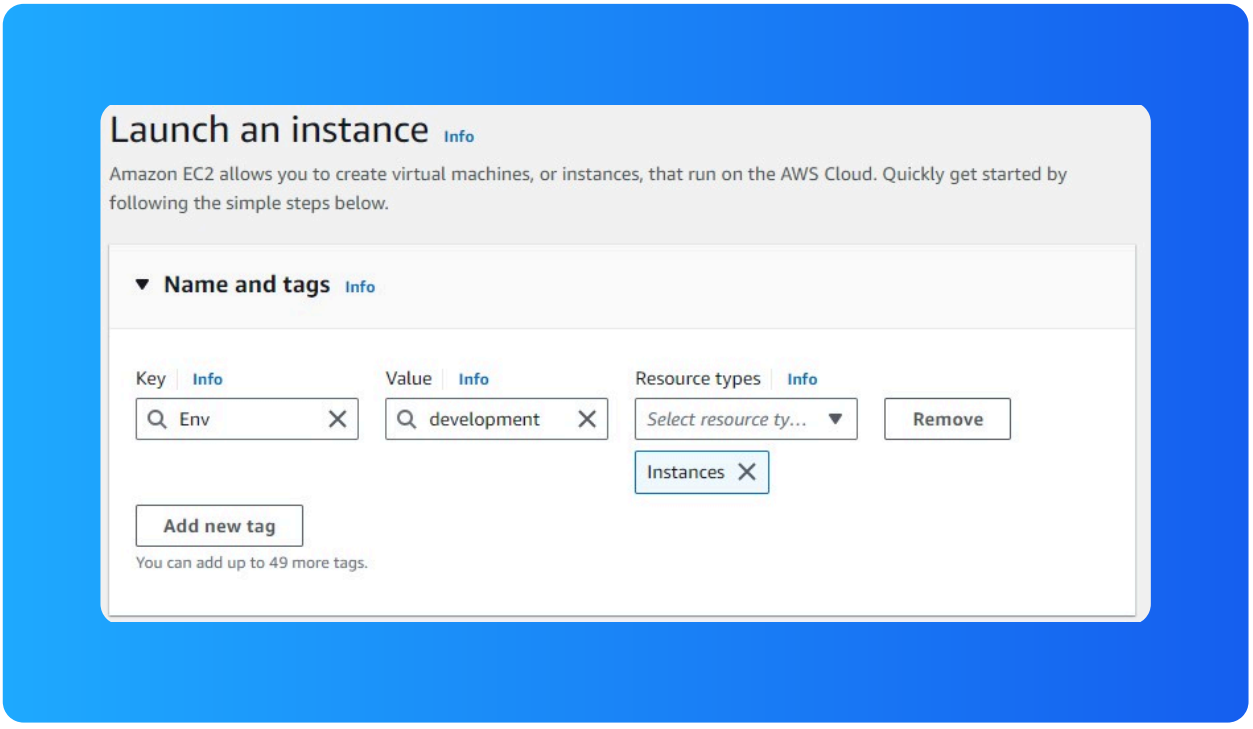
This project took me an hour to complete, which also included the time I needed to write my documentation.

Nikhil Bhan
NextWork Student

Tags

Tags are labels that you can attach to AWS resources for your organization; tagging is useful when you want to identify resources that have the same tag, as well as cost allocation and implementing policies depending on the type of environment

The tag I've used on my EC2 instances is called Env, which is short for environment. I've assigned two values, one for each EC2 instance I created. One value is called production and the other one is development.



N
Nikhil Bhan
NextWork Student

IAM Policies

IAM Policies are rules that define who and what can be done on your AWS resources in your account; these permissions are attached to IAM users, groups and roles, which will include Allow and Deny statements.

The policy I set up

For this project, I've set up a policy using the Policy Editor by clicking on the JSON button next to the Visual button; I copied the JSON code and pasted it into the editor to add the permissions to my IAM Policy.

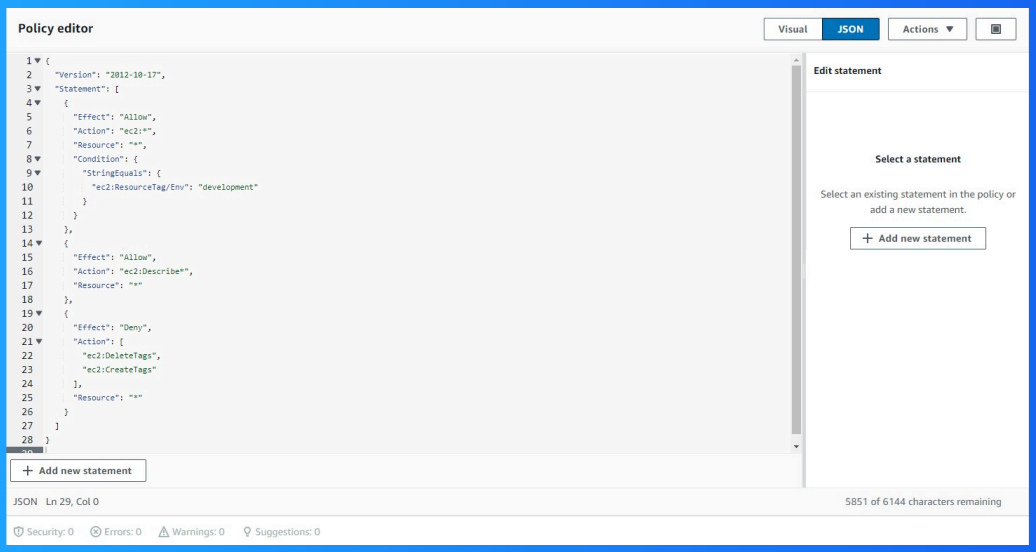
I've created a policy that will allow all resources to have full access to EC2 instances that are tagged with the key name "ENV" and the value of "Development"; at the same time all resources are denied the ability to create or delete tags.

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 the following. Effect shows if an action is Allowed or Denied. Action defines what specific action is Allowed or Denied. The Resource shows the resource the Action applies to.

Nikhil Bhan
NextWork Student

My JSON Policy



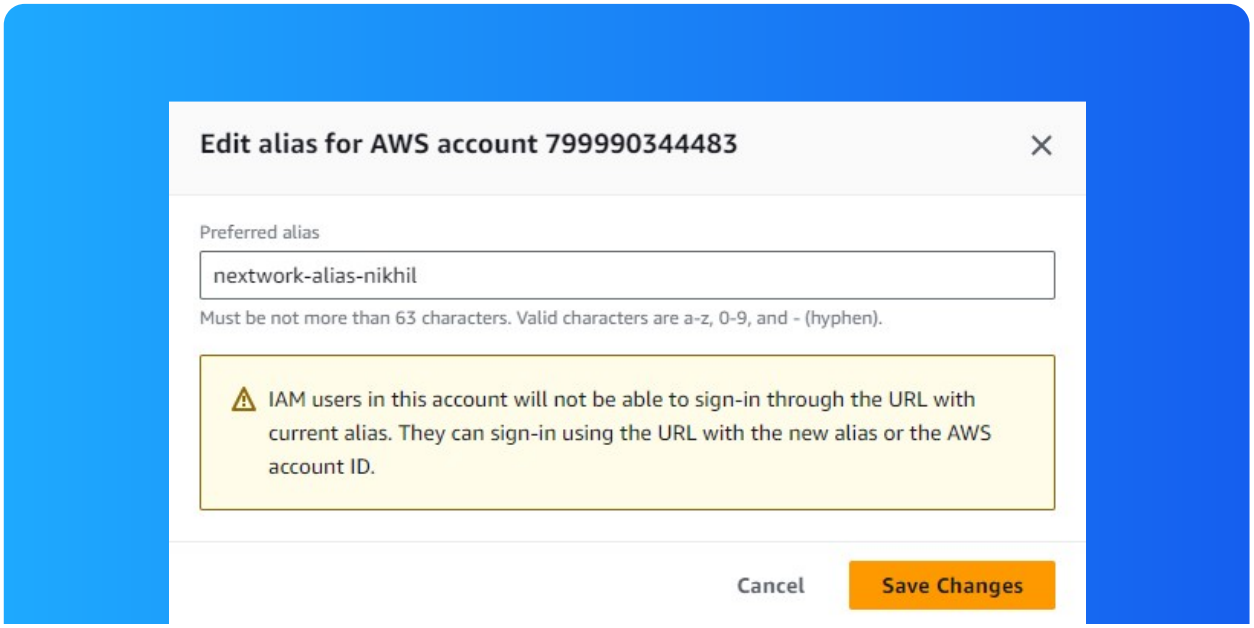
Nikhil Bhan
NextWork Student

Account Alias

An account alias is a friendly name you assign for your AWS account instead of using the account ID, which is used to sign in to the AWS Management Console. The alias is easier to remember and you'd be able to share the login URL with others.

Creating an account alias took me less than a minute to complete on my AWS Account. I used the IAM Dashboard to do this and the option to make an alias was on the right side, under AWS Account. If you already have an alias, you can change it.

Now, my new AWS console sign-in URL is https://nextwork-alias-nikhil.signin.aws.amazon.com/console This is the URL I would use to sign in and I wouldn't have to remember my Account ID.



N
Nikhil Bhan
NextWork Student
NextWork.org

IAM Users and User Groups

Users

IAM users are the people in an organization that will be given access to the AWS account and resources if they have the necessary permissions from the policies in the IAM service.

User Groups

IAM user groups are a collection of users and it makes it easier for user management. This is important for large organizations where there may be lots of people and user accounts to manage.

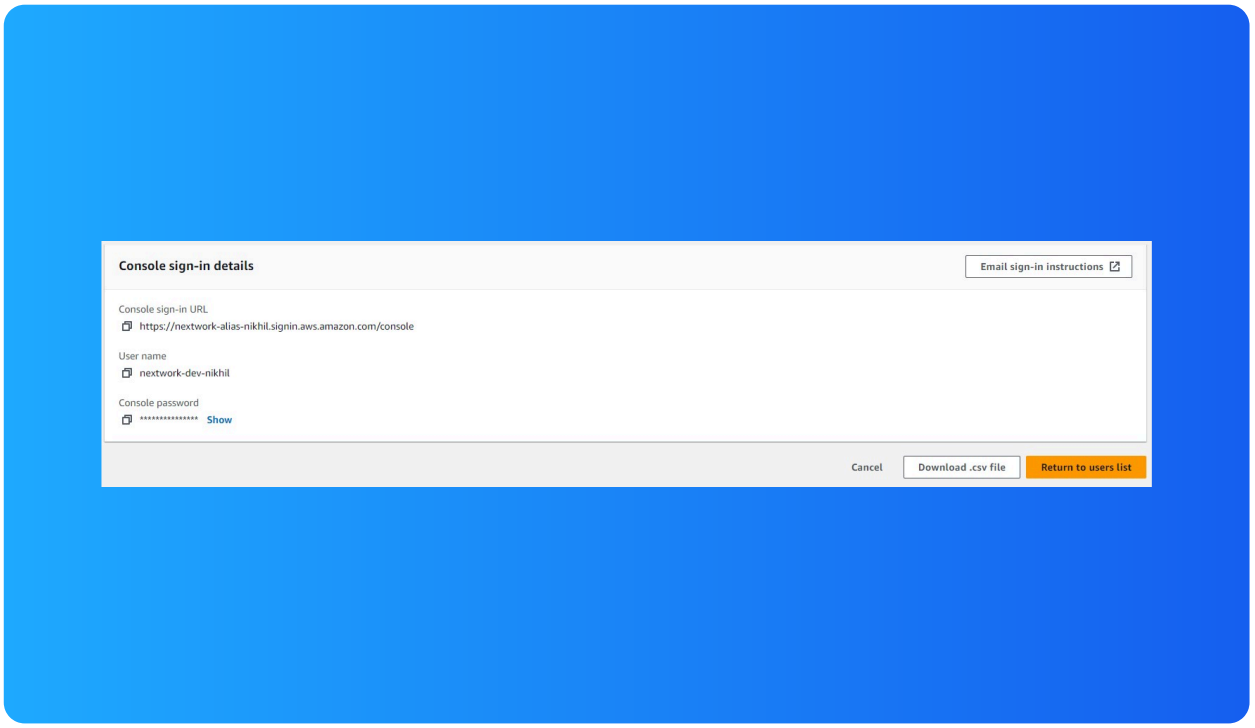
I attached the policy I created to this user group, which means that all current and future users assigned to the "network-dev-group" will inherit these permissions from the policy.

Nikhil Bhan
NextWork Student

Logging in as an IAM User

The first way is to download the user's sign-in details when that user is created; it's saved in a CSV formatted file. The other way to share that user's sign-in details is by using an account alias, which provide a unique sign-in URL to log in AWS.

Once I logged in as my IAM user, I noticed that my account was being denied access to some services and from seeing certain information. This is evidence that my user account didn't have the necessary permissions in AWS to perform these actions.



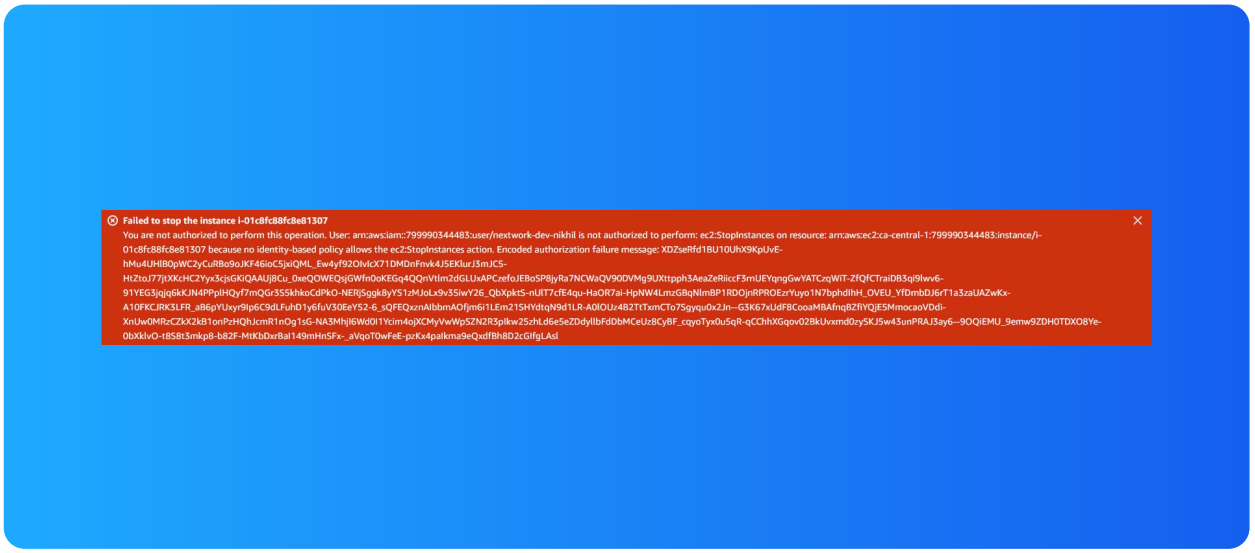
Nikhil Bhan
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by going to the EC2 service in my AWS account and clicking on Instances. My user account had access to these instances and I tested what would happen if I tried to stop these instances.

Stopping the production instance

When I tried to stop the production instance I encountered a red error message that stated that my user account was not authorized to stop the instance. This message also shows I need the permission 'ec2:StopInstances' to be able to stop instances.

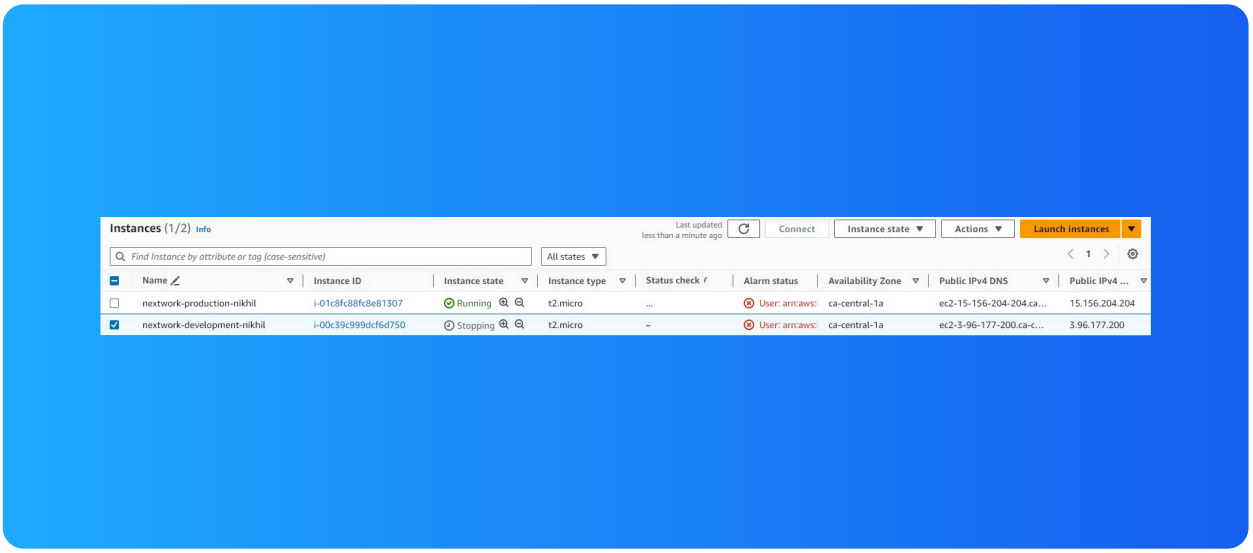


Nikhil Bhan
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance my user account was able to perform this action. This was because the policy permissions in my user group allowed my user account to perform any action on instances that had the 'development' tag.



Everyone should be in a job they love.

Check out nextwork.org for more projects