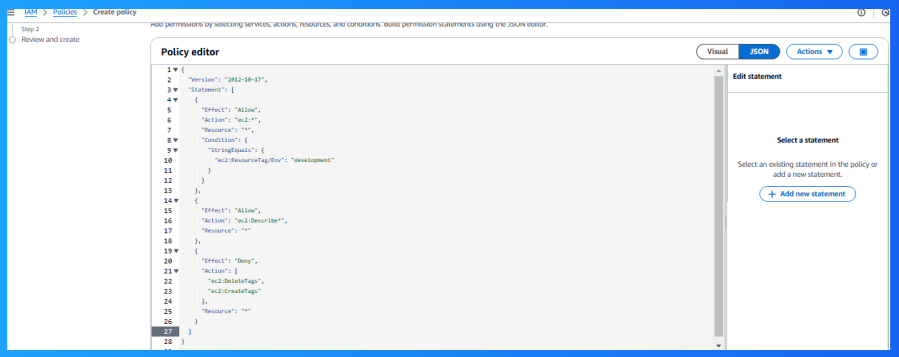
NextWork.org

Cloud Security with AWS IAM

Gloria



G
Gloria
NextWork Student

Introducing today's project!

What is AWS IAM?

AWS Identity and Access Management (IAM) is a service that enables you to securely control access to AWS resources. It is useful because it allows you to manage permissions for users, groups and roles, ensuring that only authorized people have access

How I'm using AWS IAM in this project

I used AWS IAM in today's project to manage access control for my AWS EC2 instances. Specifically, I created a custom IAM policy, attached it to a user group, and tested its effect on restricting or allowing actions, such as stopping EC2 instances.

One thing I didn't expect...

One thing I didn't expect in this project was how detailed and specific IAM policies can be, allowing precise control over actions for particular resources.

This project took me...

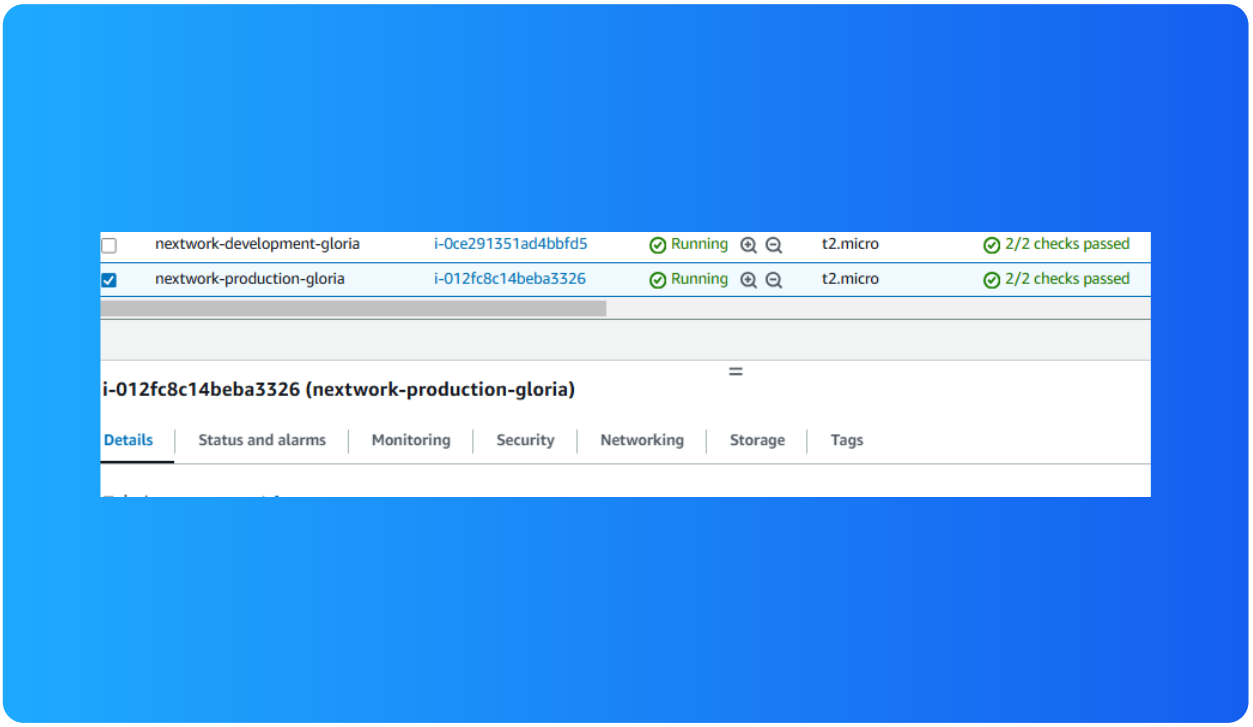
This project took me approximately 1 hour to complete, including setting up IAM policies, testing permissions on EC2 instances, creating users and creating aliases

Gloria
NextWork Student

Tags

Tags are key-value pairs that help you organize, manage, and categorize your AWS resources. Tags can be applied to almost all AWS resources, including EC2 instances, volumes, security groups, and more.

The tag I used on my EC2 instances is called Env and the value i assigned for my instances are production and development



G
Gloria
NextWork Student
NextWork.org

IAM Policies

IAM (Identity and Access Management) Policies define permissions for actions on AWS resources. They control what actions a user, group, or role can perform within an AWS account, ensuring that only authorized entities have access to specific service

The policy I set up

For this project , I did set up a policy using JSON that allows options like starting and stopping instances among other options .

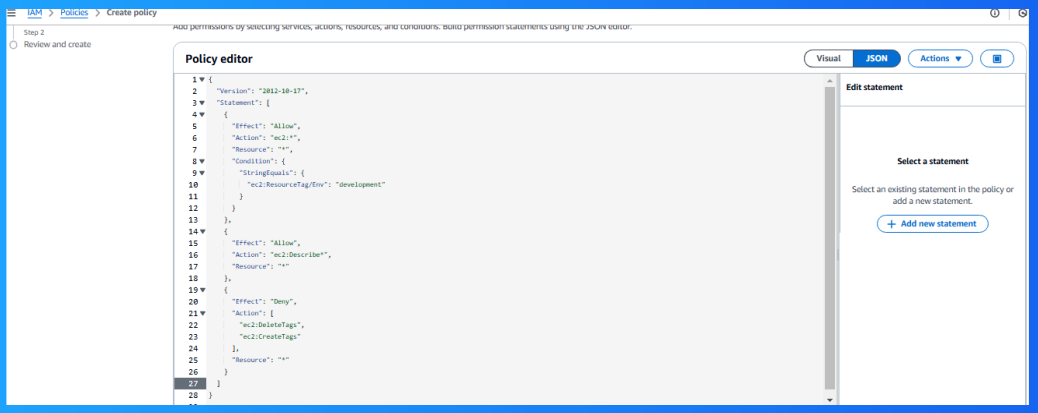
I've created a policy that grants full EC2 permissions only for resources tagged as "development," allows description actions for all EC2 resources, and explicitly denies the ability to create or delete tags on any EC2 resource.

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

The Effect, Action, and Resource attributes of a JSON policy mean: Effect specifies if the policy allow or deny, Action defines the permitted or denied operations and Resource limits the policy to specific AWS resources which the policy applies to.

Gloria
NextWork Student

My JSON Policy

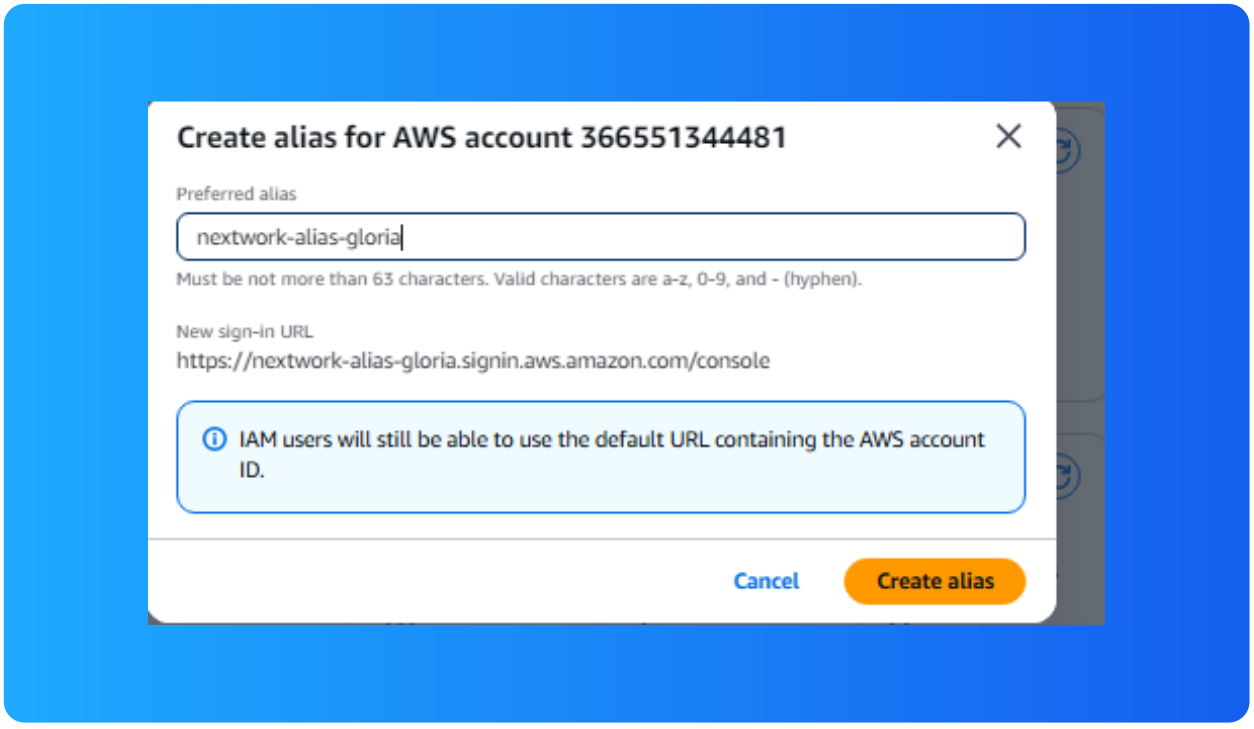


Gloria
NextWork Student

Account Alias

An account alias is a user-friendly name for your AWS account, replacing the default numerical account ID. It makes the AWS Management Console login URL easier to remember and share, making it more user friendly without affecting its functionality.

Creating an account alias took me only a minute. Now, my new AWS console sign-in URL is https://nextwork-alias-gloria.signin.aws.amazon.com/console.



G
Gloria
NextWork Student

IAM Users and User Groups

Users

IAM users are individual accounts within an AWS account that represent people or services. Each IAM user has unique credentials and can be assigned specific permissions to securely access AWS resources and perform actions based on assigned policies.

User Groups

IAM user groups are collections of IAM users that allow you to manage permissions for multiple users at once. By assigning policies to a group, all users within that group inherit the permissions, simplifying access management across your AWS account

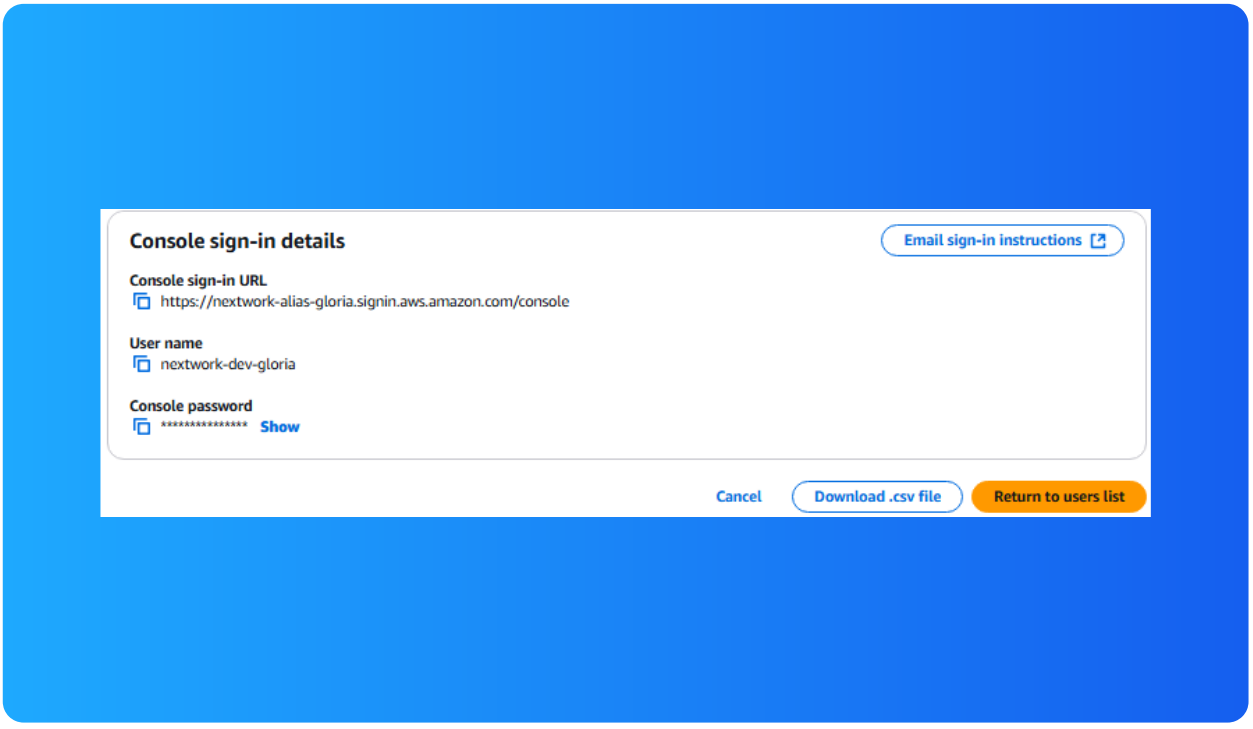
I attached the policy I created to this user group, which means all users in the group will inherit the permissions defined in the policy. This ensures uniform access controls, allowing or restricting specific actions on AWS resources based on policy

G
Gloria
NextWork Student

Logging in as an IAM User

The first way to share a new user's sign-in details is by directly emailing the credentials, including the username and temporary password. The second way is to provide the IAM user's sign-in URL and credentials manually.

Once I logged in as my IAM user, I noticed access denied to certain AWS services based on the permissions assigned to the user group. This was because the policy attached to the user group defined the allowed actions, resources, and conditions.



Gloria
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by attempting to stop the production instance which failed and successfully stopping the development instance. This demonstrated the policy's effectiveness in restricting unauthorized actions and allowing permitted ones.

Stopping the production instance

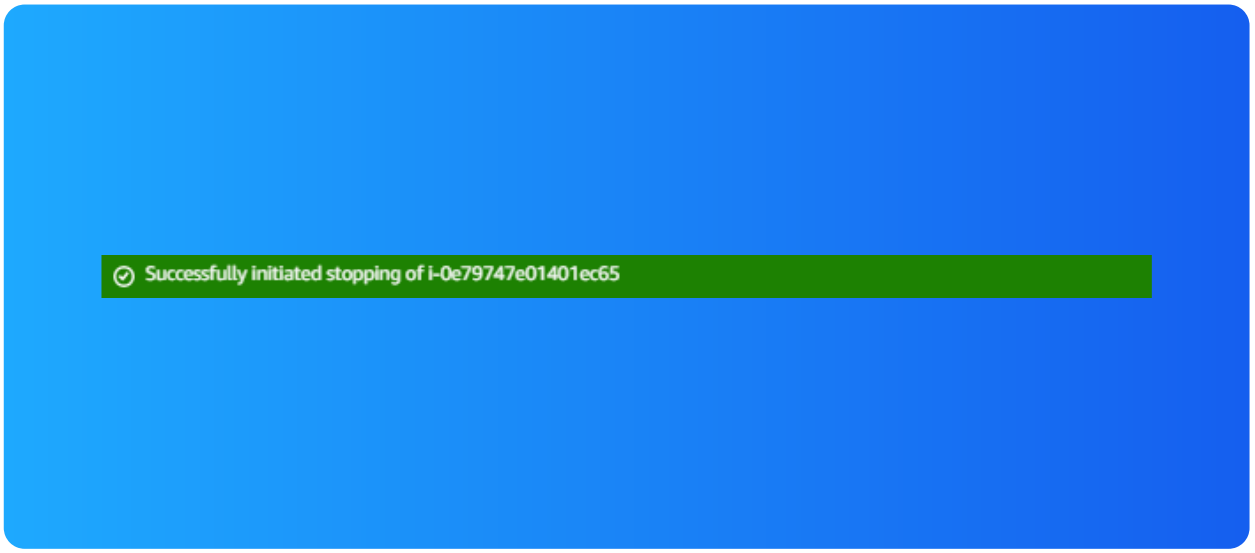
When I tried to stop the production instance, the action was denied. This was because the attached IAM policy explicitly restricted actions such as stopping instances in the production environment to prevent uncontrolled work related accidents

Gloria
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, the action was successful. This was because my JSON IAM policy allows stopping instances tagged with "development", which corresponds with the permissions listed



Everyone should be in a job they love.

Check out nextwork.org for more projects