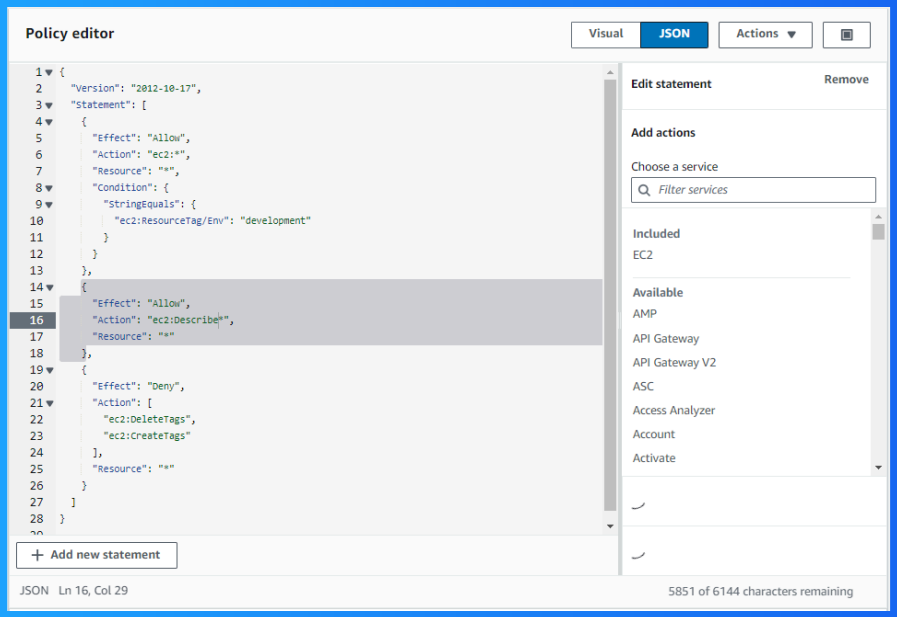
NextWork.org

Cloud Security with AWS IAM

sru anu



sru anu
NextWork Student

Introducing today's project!

What is AWS IAM?

AWS IAM manages access to AWS resources by creating users, groups, and roles with specific permissions, ensuring secure and controlled access.

How I'm using AWS IAM in this project

In today's project, I used AWS IAM to create user groups, assign policies, and manage permissions for accessing and controlling EC2 instances, ensuring secure operations.

One thing I didn't expect...

One thing I didn't expect in this project was the need to troubleshoot permission errors despite correctly setting up IAM policies and user groups.

This project took me...

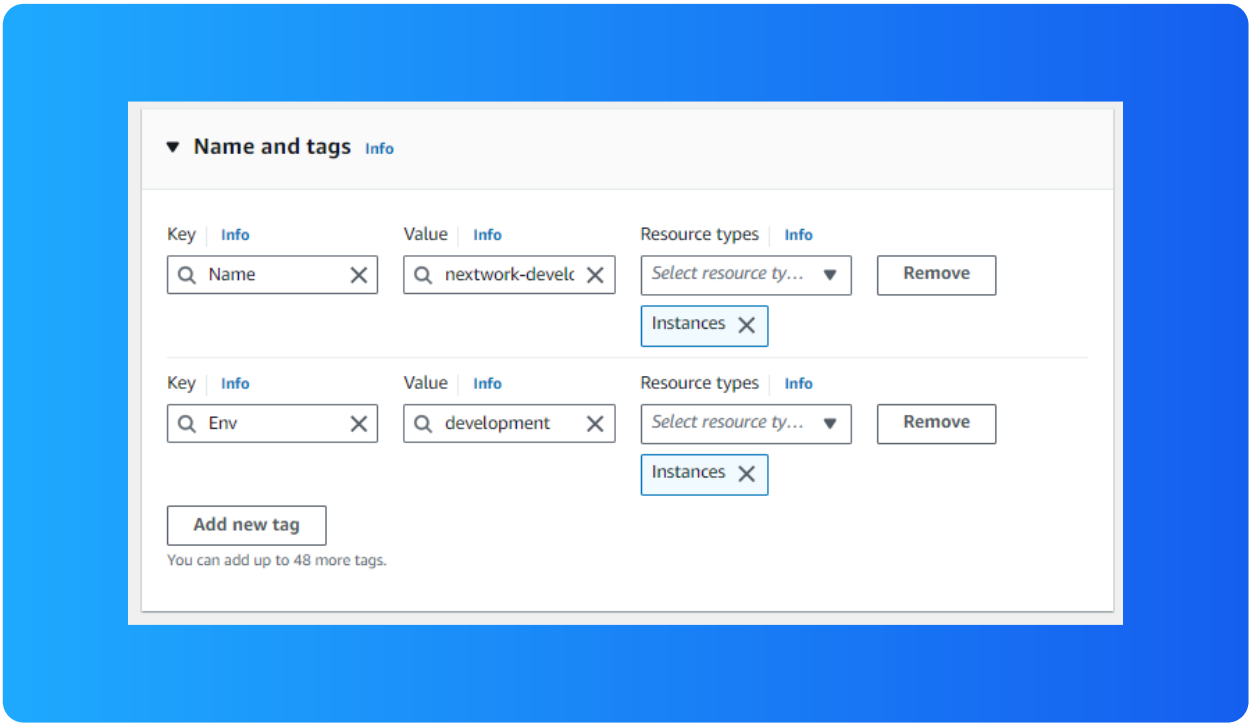
The project took me approximately 1 hour, with additional time spent on documentation.

sru anu
NextWork Student

Tags

Tags are key-value pairs that help categorize and organize AWS resources. They are useful for managing, tracking, and identifying resources, improving visibility for billing, automation, and access control across different projects or environments.

The tag I've used on my EC2 instances is called env. The values I've assigned for my instances are development for one instance and production for the other.



sru anu
NextWork Student

IAM Policies

IAM Policies are sets of permissions that define whether to allow or deny access to AWS resources. They control actions like creating, deleting, or making changes to instances and other services within AWS, ensuring proper access management.

The policy I set up

For this project, I've set up a policy using JSON to define the permissions and create the policy.

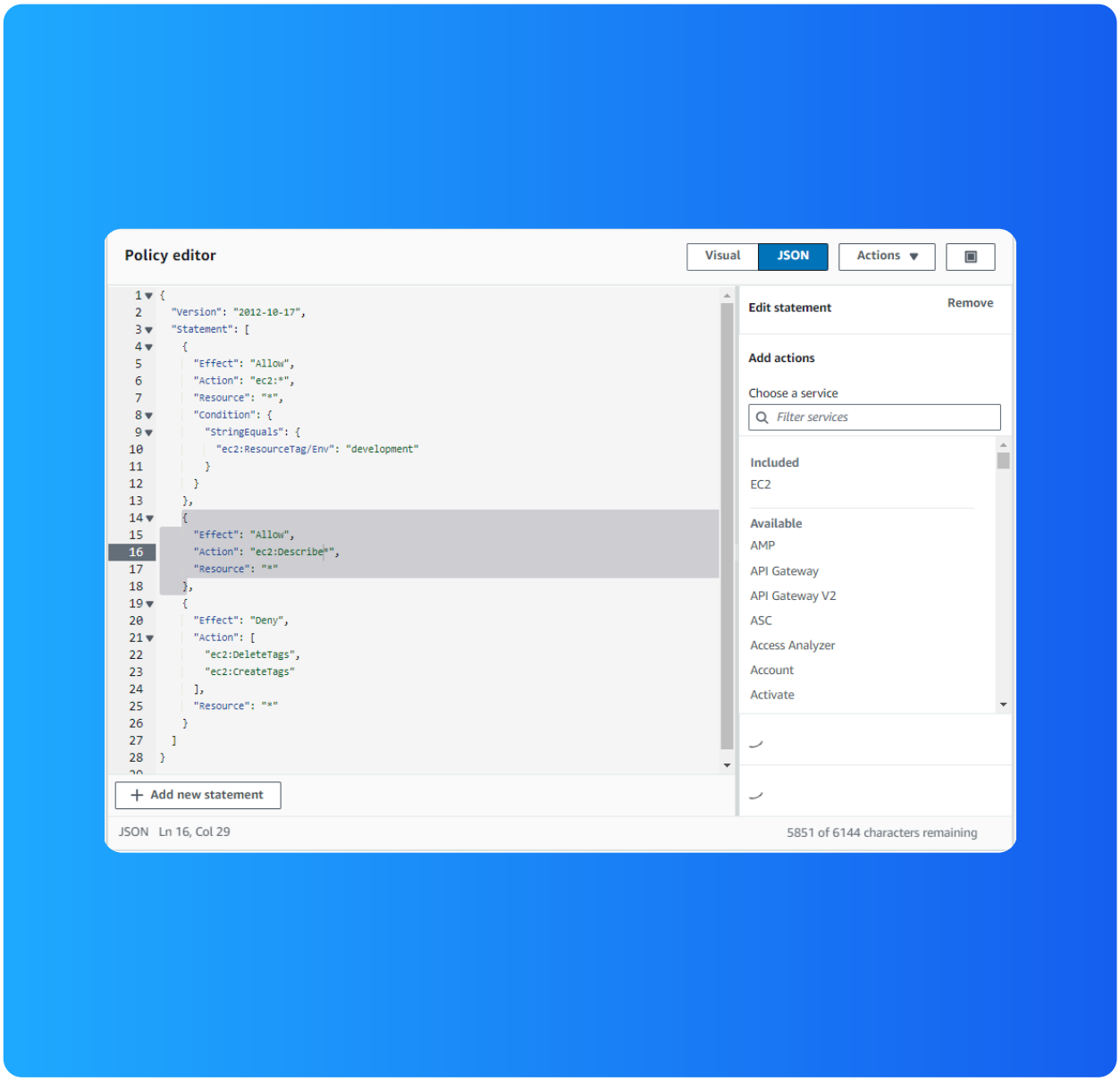
I created a policy that allows all EC2 actions on resources tagged with "Env=development," permits describing any EC2 resource, but denies the ability to create or delete tags across all EC2 resources.

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 the following: Effect specifies whether to allow or deny access, Action defines the specific AWS service operations, and Resource indicates the target AWS entities.

sru anu
NextWork Student

My JSON Policy



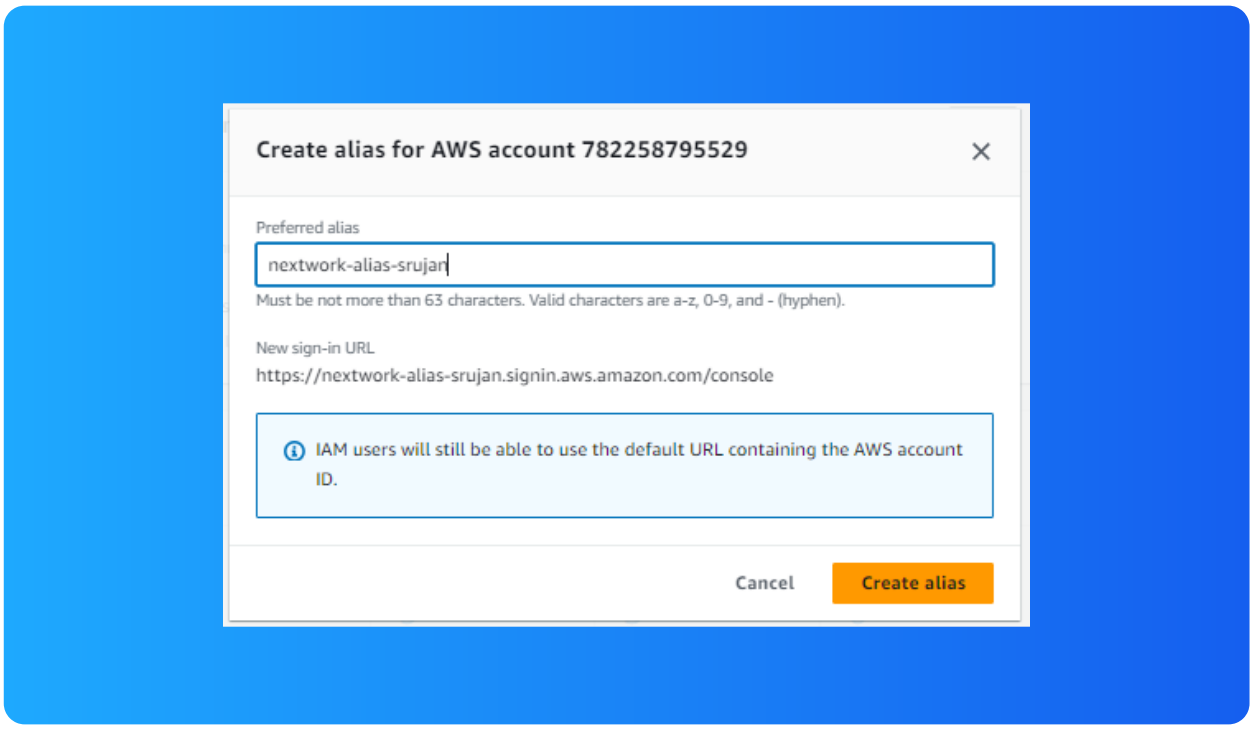
sru anu
NextWork Student

Account Alias

An account alias is a user-friendly name you assign to your AWS account, making it easier to identify instead of using the default numerical account ID.

An account alias is a user-friendly name you assign to your AWS account, making it easier to identify instead of using the default numerical account ID.

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



sru anu
NextWork Student

IAM Users and User Groups

Users

IAM users are individual identities created within AWS that allow access to AWS resources. Each user has a unique set of credentials and permissions, enabling them to perform specific actions based on assigned policies.

User Groups

IAM user groups are collections of IAM users that share the same permissions. By assigning policies to a group, you can manage permissions for multiple users at once, simplifying access control and management.

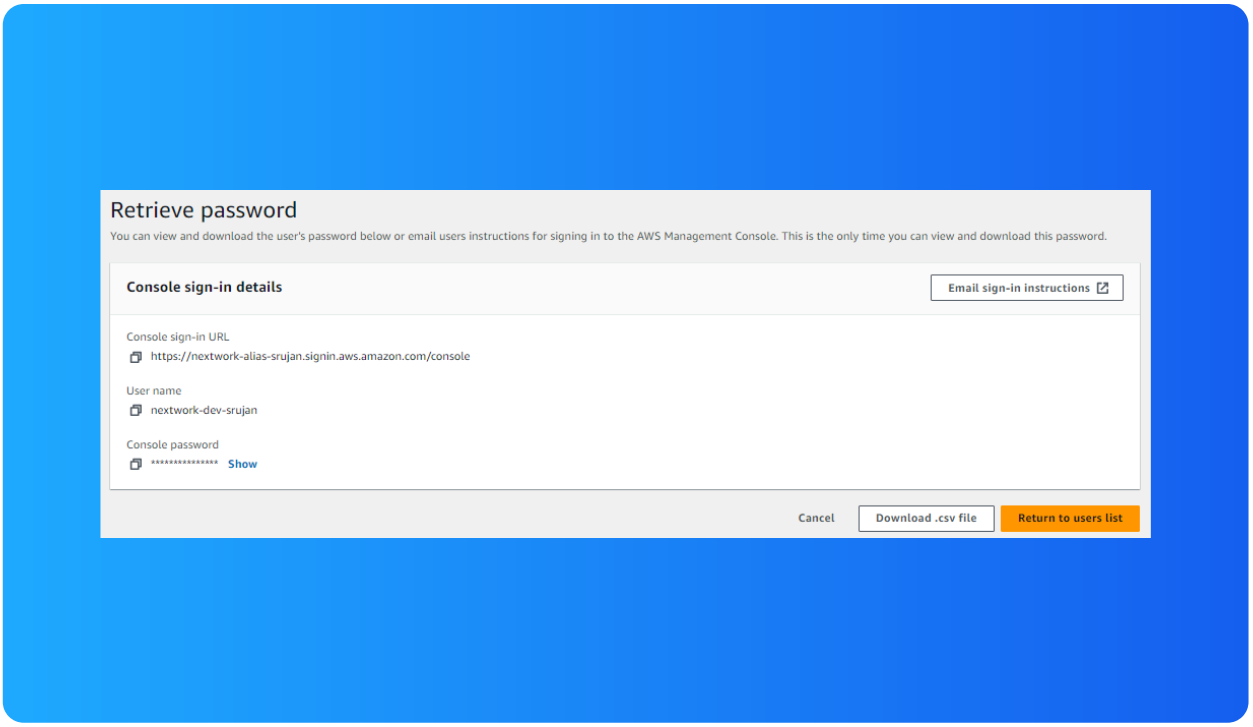
I attached the policy I created to this user group, which means all users in the group inherit the permissions defined in the policy, allowing them to perform the specified actions on AWS resources.

sru anu
NextWork Student

Logging in as an IAM User

I attached the policy I created to this user group, which means all users in the group inherit the permissions defined in the policy, allowing them to perform the specified actions on AWS resources.

Once I logged in as my IAM user, I noticed a denial of access to cost billing and current monthly cost features, as well as other restricted functions based on the assigned policy.



sru anu
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by trying to perform actions on my two EC2 instances, such as starting and stopping them, to ensure the policy's permissions and restrictions were applied correctly.

Stopping the production instance

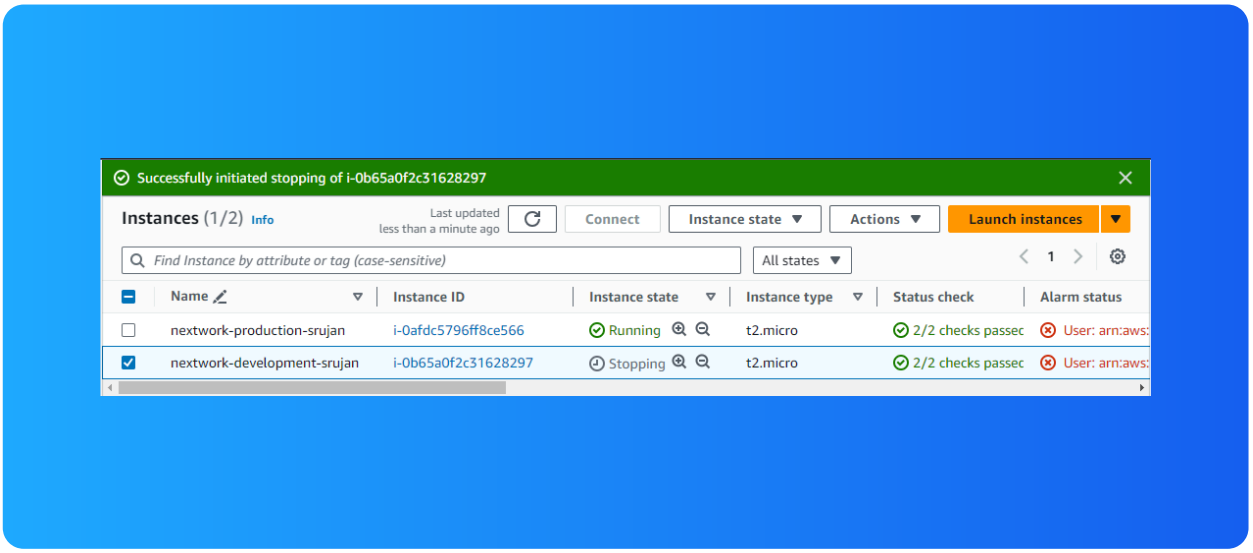
When I tried to stop the production instance, it showed a red error message indicating that the IAM user didn't have the permission to delete or stop the instance.

sru anu
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, the action was successful, confirming that the IAM policy allowed operations on instances tagged with "Env=development."



Everyone should be in a job they love.

Check out nextwork.org for more projects