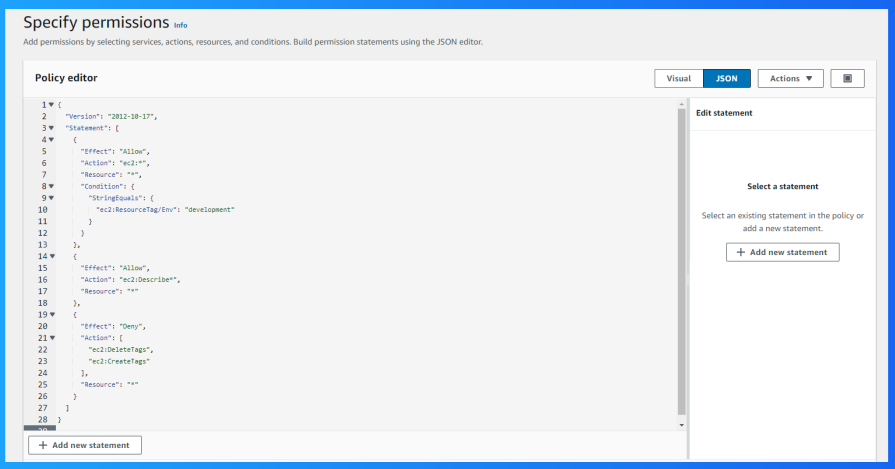
NextWork.org

Cloud Security with AWS IAM

Sai Prasanth Reddy



Sai Prasanth Reddy
NextWork Student

Introducing today's project!

What is AWS IAM?

AWS IAM (Identity and Access Management) is a service for securely managing access to AWS resources. It's useful for controlling who can access your resources and what actions they can take, providing enhanced security and compliance.

How I'm using AWS IAM in this project

I used AWS IAM in today's project to create users, set up a user group with specific permissions, and attach a custom policy to manage access to EC2 instances based on tags, ensuring secure and controlled resource management.

One thing I didn't expect...

One thing I didn't expect in this project was the strict enforcement of policy conditions, which prevented actions on instances without the correct tags, highlighting the precision needed in setting up IAM policies.

This project took me...

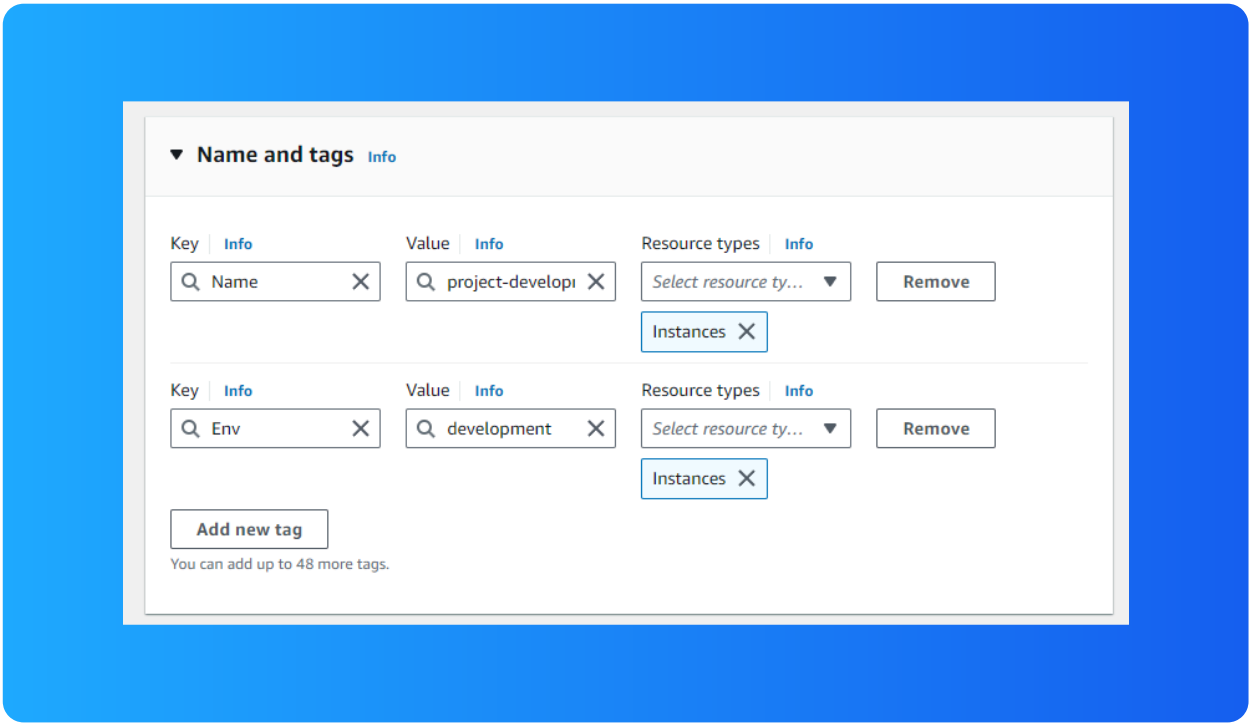
This project took me about an hour to complete, including setting up IAM users and groups, creating and testing the JSON policy, and verifying permissions on the EC2 instances.

Sai Prasanth Reddy
NextWork Student

Tags

Tags are labels you assign to resources in AWS, like EC2 instances, to help organize, manage, and search for resources. They are useful for tracking costs, applying policies, and maintaining clear resource management across your projects.

The tag I've used on my EC2 instances is called Name and Env. The values I've assigned for my instances are project-development-sai-reddy/project-production-sai-reddy for the Name tag and development/production for the Env tag.



Sai Prasanth Reddy
NextWork Student

IAM Policies

IAM Policies are documents that define permissions for users, groups, and roles in AWS, specifying what actions they can perform on which AWS resources, helping to manage access control and ensure security within your AWS environment.

The policy I set up

For this project, I've set up a policy using JSON to specify permissions for two EC2 instances, allowing precise control over the actions that can be performed on these instances.

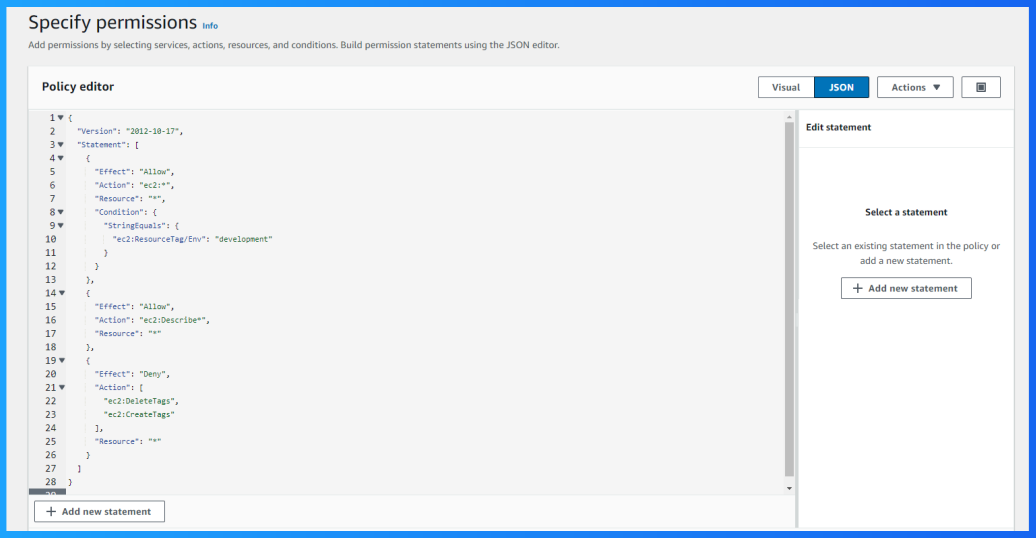
I've created a policy that allows all EC2 actions on resources tagged with **Env: development**, permits describing any EC2 instances, and denies the ability to create or delete tags on any EC2 resources.

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 defining whether to allow or deny access (Effect), specifying what actions can be performed (Action), and identifying which AWS resources the policy applies to (Resource).

Sai Prasanth Reddy
NextWork Student

My JSON Policy



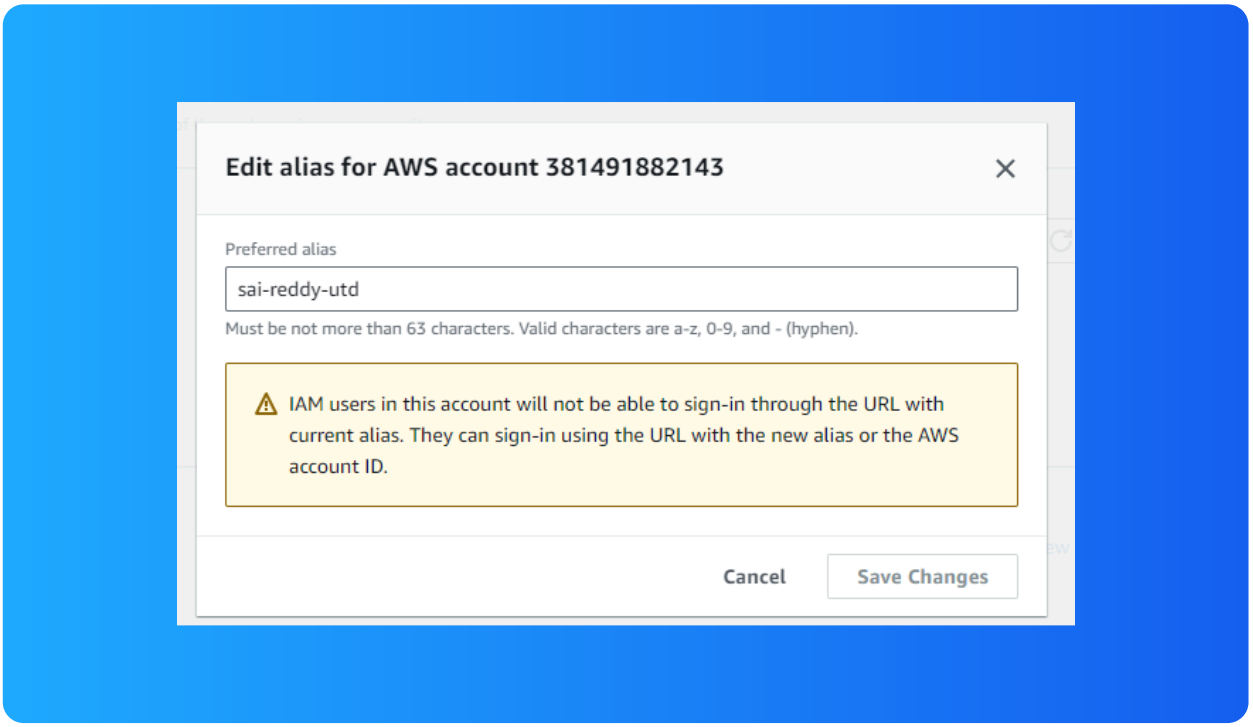
Sai Prasanth Reddy
NextWork Student

Account Alias

An account alias is a user-friendly name for your AWS account that replaces the default account ID in the sign-in URL, making it easier to remember and access your AWS management console.

Creating an account alias took me under a minute, as it only involved navigating to the IAM dashboard page in the AWS Management Console and entering a new alias.

Now, my new AWS console sign-in URL is `https://sai-reddy-utd.signin.aws.amazon.com/console`.



Sai Prasanth Reddy
NextWork Student

IAM Users and User Groups

Users

IAM users are entities you create in AWS to represent people or applications that need access to your AWS resources. Each IAM user has specific permissions and credentials to securely access and manage resources.

User Groups

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

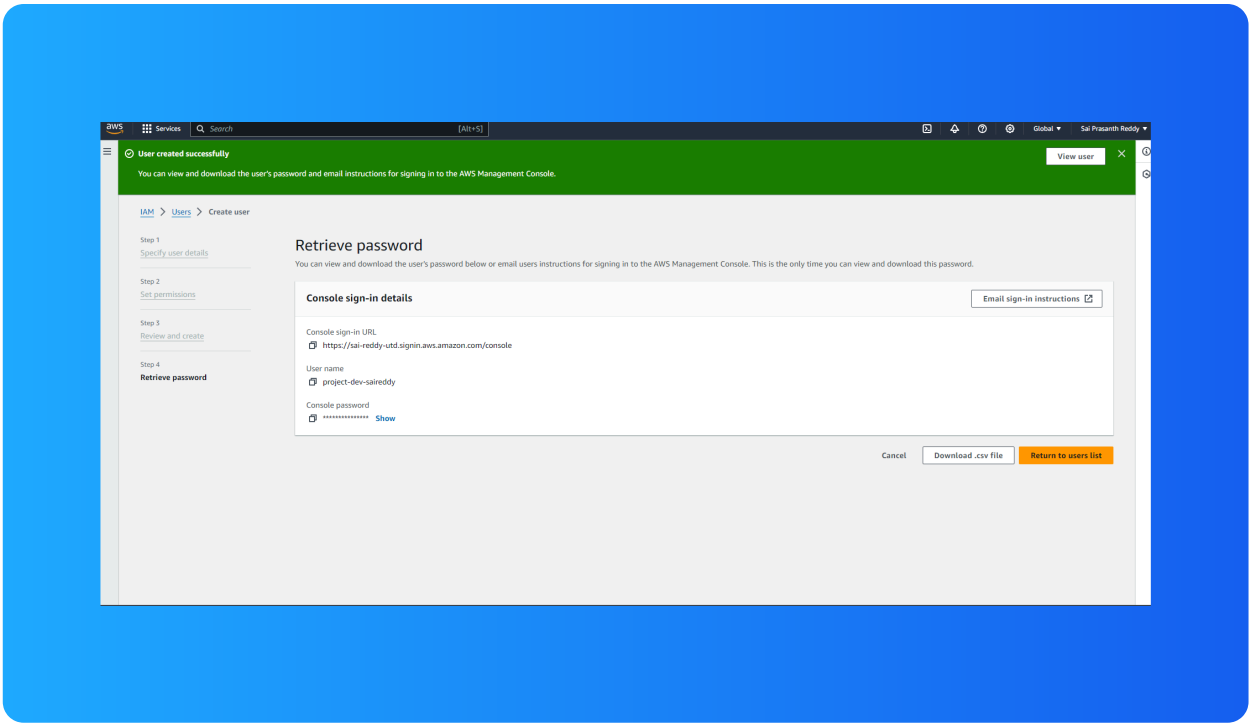
I attached the policy I created to this user group, which means all users in the group have the permissions defined in the policy, such as managing EC2 instances tagged with "development" and viewing all instances but not modifying tags.

Sai Prasanth Reddy
NextWork Student

Logging in as an IAM User

The first way is to email the sign-in details directly to the new user. The second way is to download the credentials and securely share them through a file or document that the user can access.

Once I logged in as my IAM user, I noticed limited access based on the assigned policies, with permissions only to manage EC2 instances tagged as "development" and view other resources without the ability to modify tags.



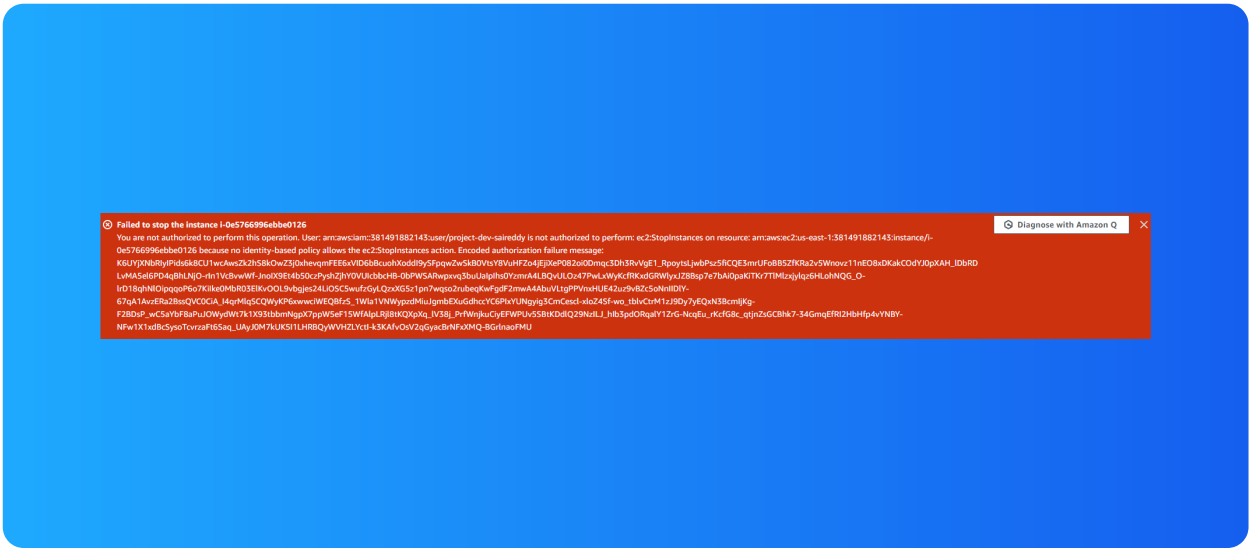
Sai Prasanth Reddy
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by trying to stop my two EC2 instances to ensure that the permissions allowed me to manage instances tagged with "development" as specified in the policy.

Stopping the production instance

When I tried to stop the production instance, the action was denied because my JSON IAM policy only allowed managing instances tagged with "development," not those tagged as production.

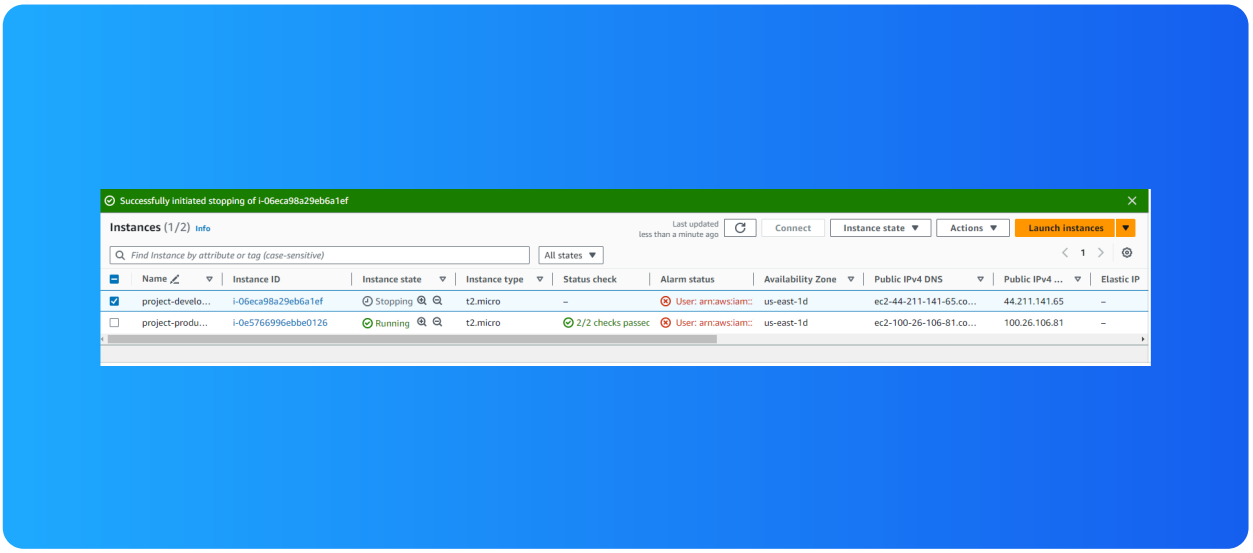


Sai Prasanth Reddy
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, the action was successful because my JSON IAM policy allowed all EC2 actions on instances tagged with "development."



Everyone should be in a job they love.

Check out nextwork.org for more projects