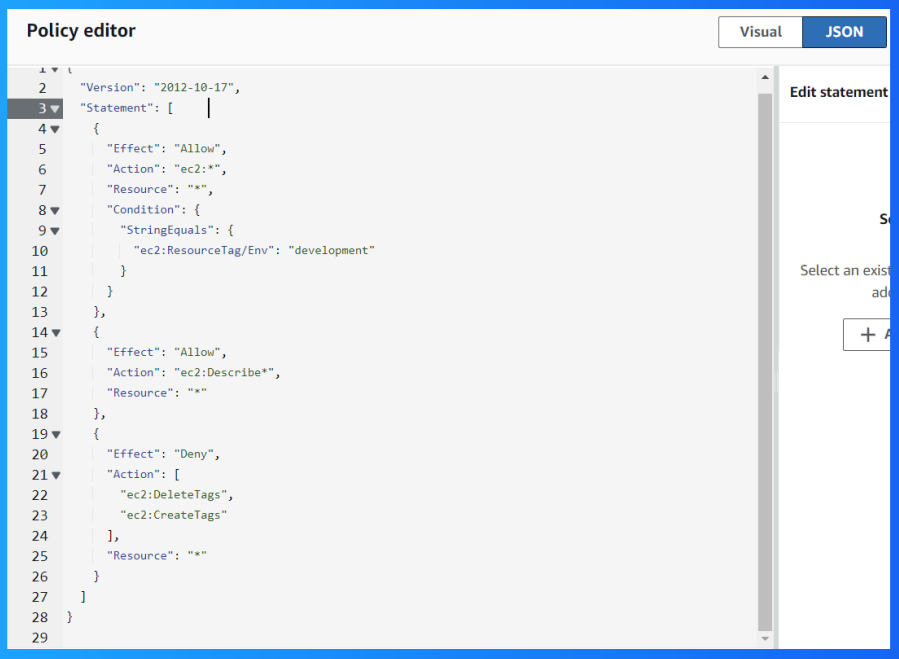
NextWork.org

Cloud Security with AWS IAM

AJ ajv.singh3107@gmail.com



AJ
ajv.singh3107@gmail.com
NextWork Student
NextWork.org

Introducing today's project!

What is AWS IAM?

AWS IAM is a service that allows you to manage access to AWS resources securely. It enables fine-grained control over user permissions, supports principle of least privilege, and integrates seamlessly with AWS ser, enhancing security and management.

How I'm using AWS IAM in this project

In today's project, I used AWS IAM to create user accounts and groups for team members, assigning specific permissions for secure access to resources. I implemented policies to control actions on EC2 instances and set up roles for secure API access.

One thing I didn't expect...

One thing I didn't expect in this project was the complexity of managing IAM policies. Ensuring each user had the correct access while maintaining least privilege required careful planning and testing.

This project took me...

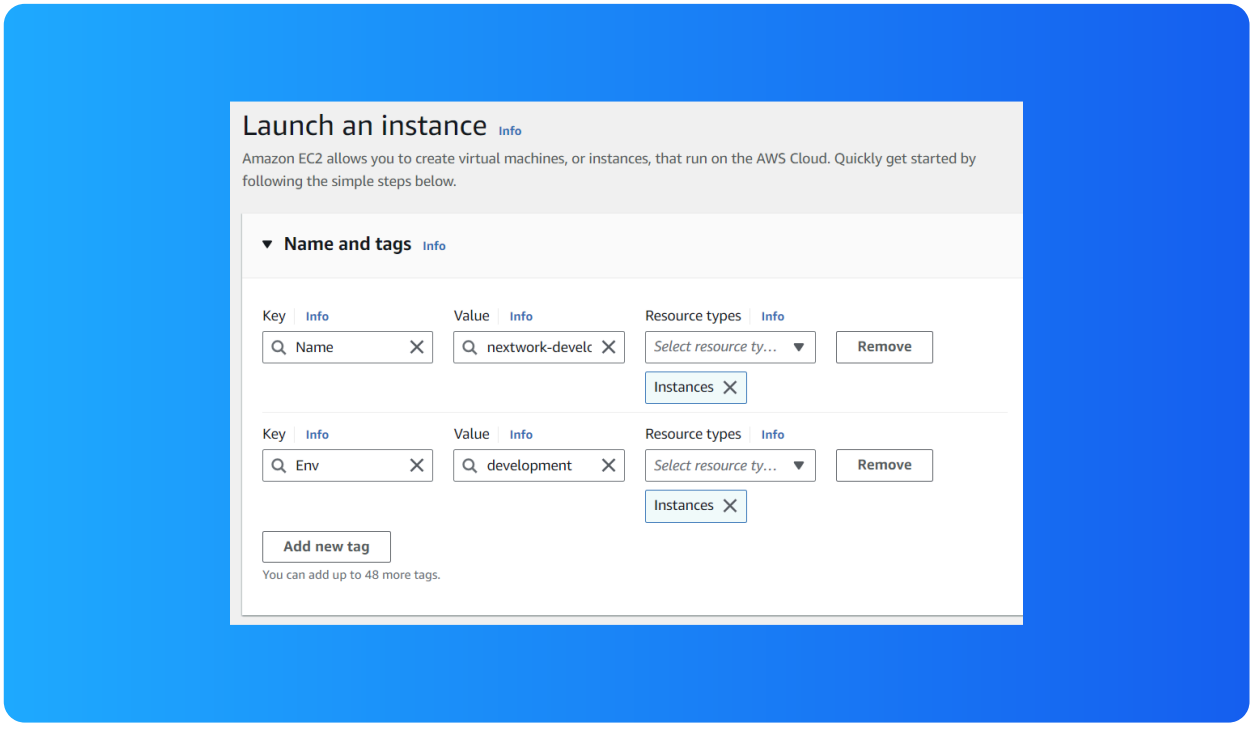
It took me 1 hr to complete the project with the documentation.

AJ
ajv.singh3107@gmail.com
NextWork Student
NextWork.org

Tags

Tags are labels assigned to AWS resources to categorize and organize them. They consist of key-value pairs and help in tracking usage, managing costs, and improving resource organization by enabling search and filtering in large cloud environments.

The tag I've used on my EC2 instances is called Environment. The values I've assigned for my instances are Production for one and Development for the other.



AJ
ajv.singh3107@gmail.com
NextWork Student
NextWork.org

IAM Policies

IAM Policies are documents that define permissions for AWS users, roles, or groups. They specify what actions are allowed or denied on AWS resources, ensuring secure and controlled access to manage cloud environments effectively.

The policy I set up

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

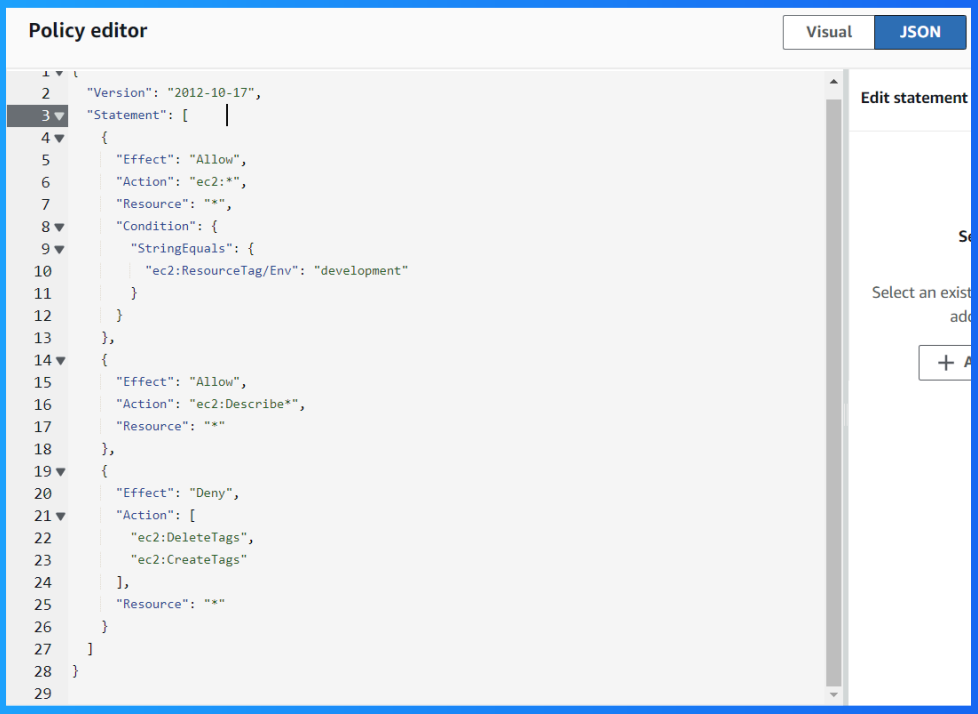
I've created a policy that allows full EC2 actions only for resources tagged with "Env: development," permits describing all EC2 resources, and denies the ability to create or delete tags on any EC2 resource, ensuring controlled resource management.

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: Allows or denies actions. - Action: Specifies what operations are permitted or denied. - Resource: Defines the AWS resources the actions apply to.

AJ
ajv.singh3107@gmail.com
NextWork Student

My JSON Policy



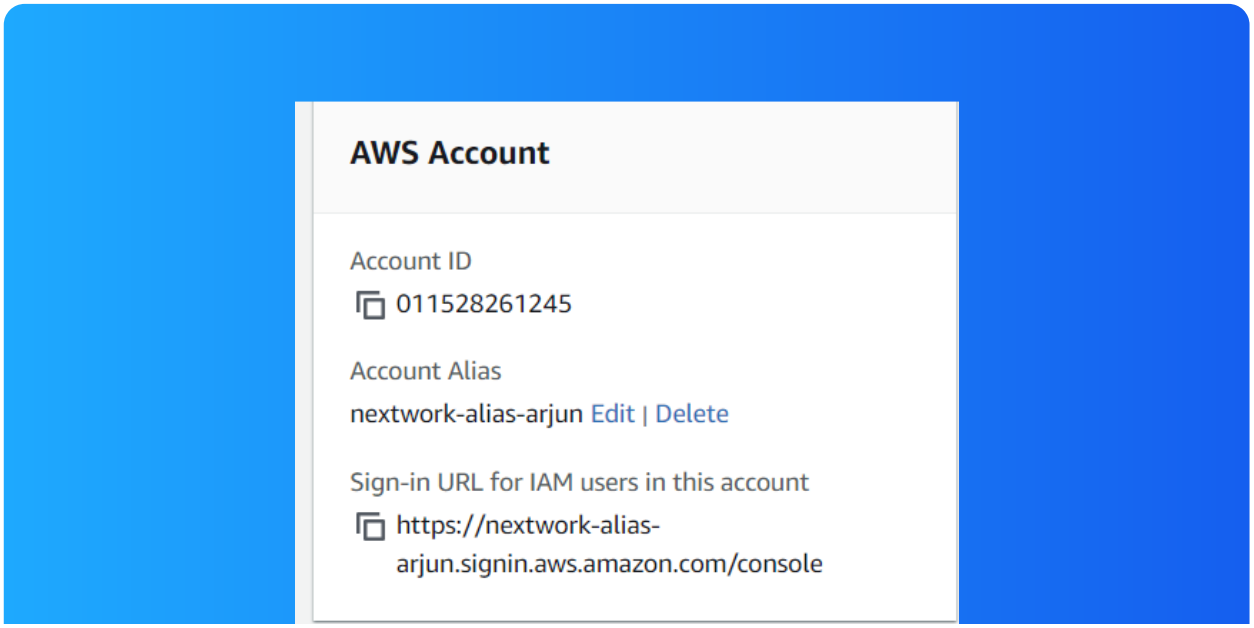
AJ
ajv.singh3107@gmail.com
NextWork Student

Account Alias

An account alias is a user-friendly name for your AWS account, replacing the default numeric account ID. It simplifies sign-in URLs and makes it easier to manage and identify accounts in multi-account environments.

Creating an account alias took me just a few minutes using the AWS Management Console. You simply navigate to the IAM dashboard, choose "Account Alias," and enter a unique name. It's a quick and straightforward process.

My new AWS console sign-in URL is `https://nextwork-alias-arjun.signin.aws.amazon.com/console`. This format indicates an account alias along with an organization prefix, allowing me to access my AWS resources conveniently.



AJ
ajv.singh3107@gmail.com
NextWork Student

IAM Users and User Groups

Users

IAM users are entities in AWS Identity and Access Management (IAM) that represent individual users or applications. Each IAM user has unique credentials, allowing access to AWS resources based on assigned permissions and policies for secure access ma

User Groups

IAM user groups are collections of IAM users that simplify management and permission assignment in AWS. By grouping users, you can apply policies to the entire group, ensuring consistent access controls and easier management of permissions.

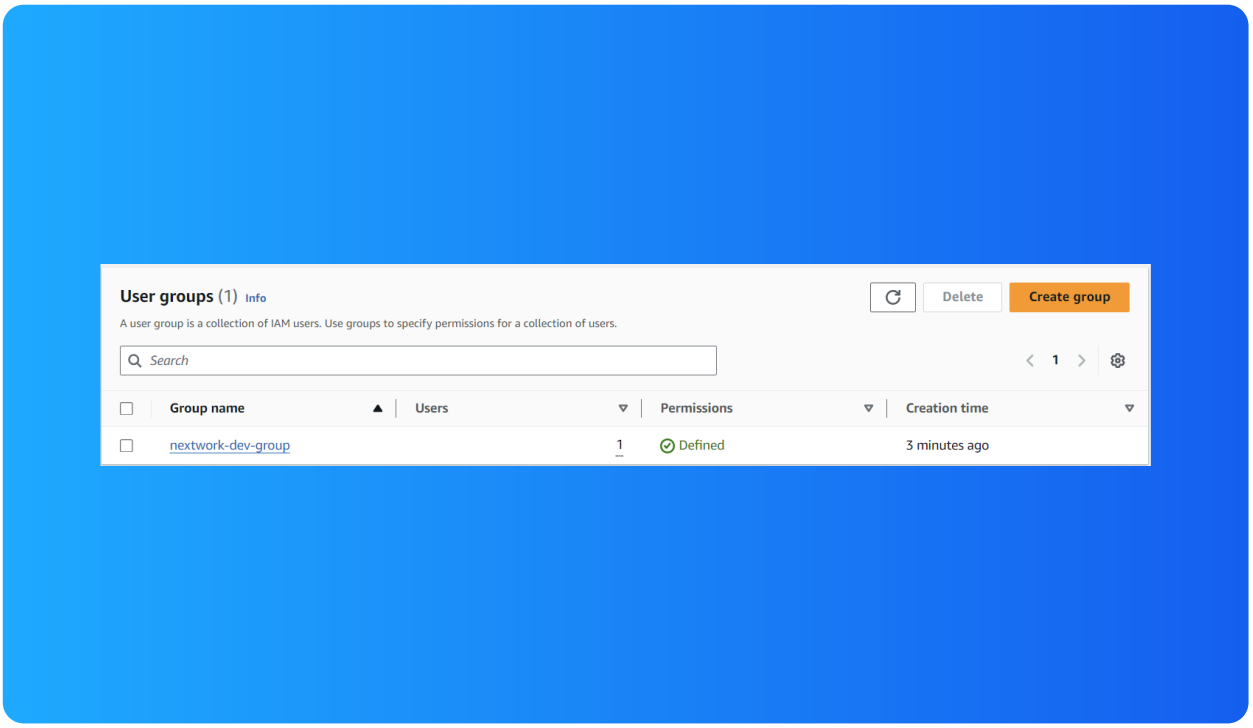
I attached the policy I created to this user group, which means all users in the group inherit the permissions defined in the policy. This ensures consistent access controls for the group, simplifying management and enhancing security across users.

AJ
ajv.singh3107@gmail.com
NextWork Student

Logging in as an IAM User

The first way to send the user's sign-in details via email, including their username and a temporary password. The second way is to use a secure messaging platform to share the details, ensuring that sensitive information remains protected.

Once I logged in as my IAM user, I noticed a simplified AWS dashboard with limited access compared to root account. It displayed only the services and permissions assigned to the IAM user, highlighting the principle of least privilege for security.



AJ
ajv.singh3107@gmail.com
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by attempting to stop the production EC2 instance, but it didn't work. However, I successfully stopped the development EC2 instance, confirming that the policy was correctly applied to my resources.

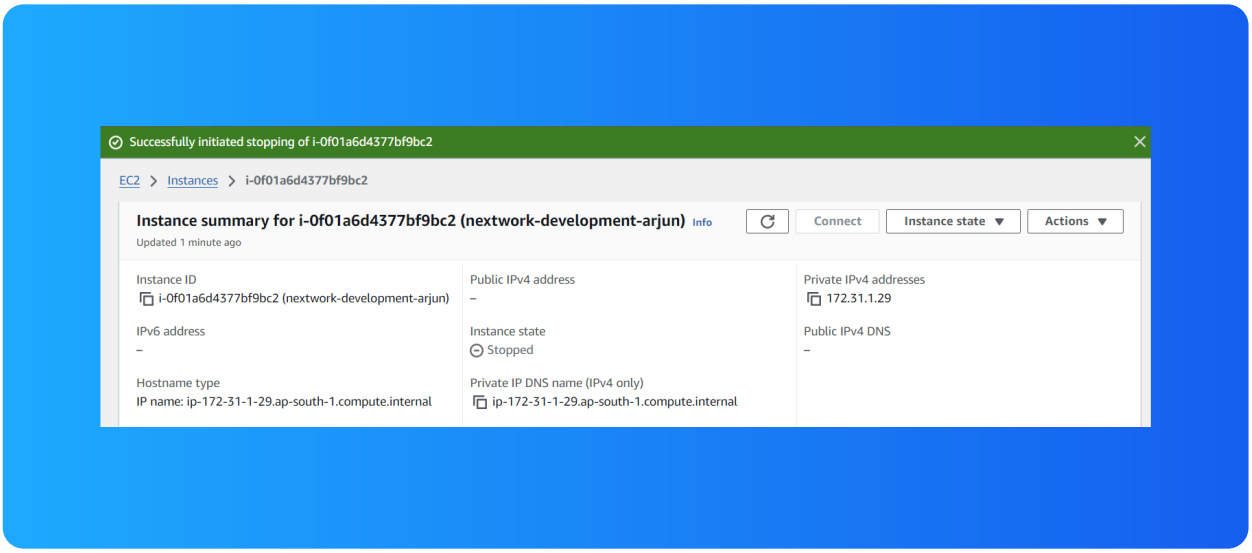
Stopping the production instance

When I tried to stop the production instance, the action was denied due to the permissions set in IAM policy. This outcome confirmed that the policy was effectively restricting access as intended, protecting critical resources from unintended changes

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, the action was successful. This confirmed that my IAM policy allowed the specified operations for resources tagged with "Env: development," enabling proper management of the development environment



Everyone should be in a job they love.

Check out nextwork.org for more projects