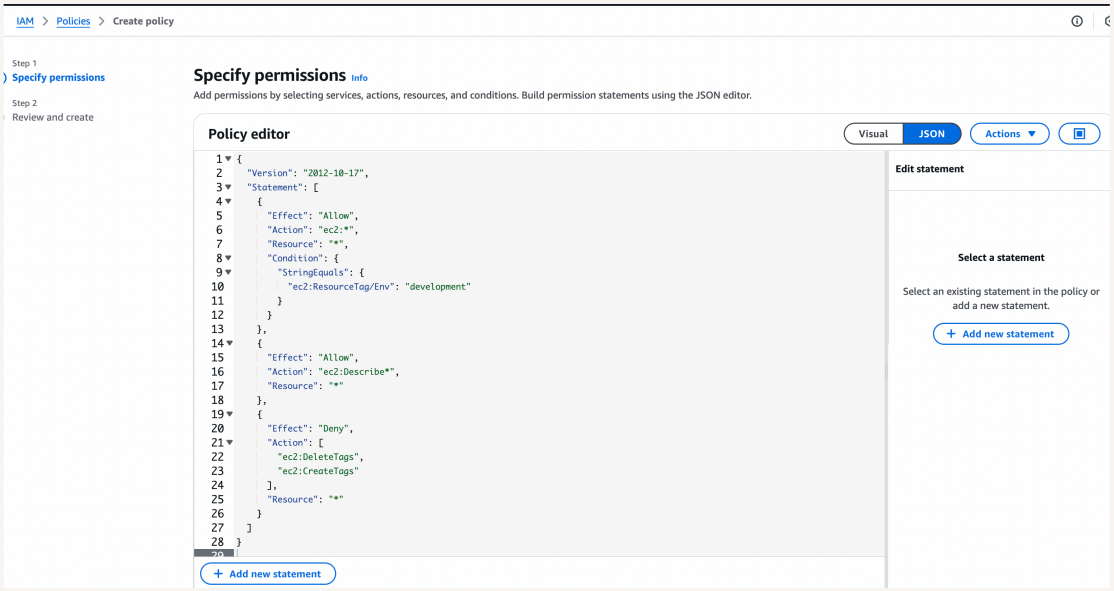
nextwork.org

# Cloud Security with AWS IAM

VA varshithmohang@gmail.com



# Introducing today's project!

## What is AWS IAM?

AWS Identity and Access Management (IAM) is a service that enables secure access control for AWS resources & allows you to manage users, groups, roles, policies to control who can access AWS services and resources and what actions they can perform.

## How I'm using AWS IAM in this project

Created IAM policies to grant only necessary permissions to users, roles, groups, assigned IAM roles to EC2 instances to allow secure access to AWS services without hardcoded credentials & enabled MFA for root users, IAM users for enhanced security.

## One thing I didn't expect...

AWS IAM evaluates policies in a specific order, and an explicit "Deny" in one policy can override multiple "Allow" permissions, causing unexpected access issues.In case using multiple IAM users, it is difficult to manage user access.

VA
**varshithmohang@gmail....**
NextWork Student

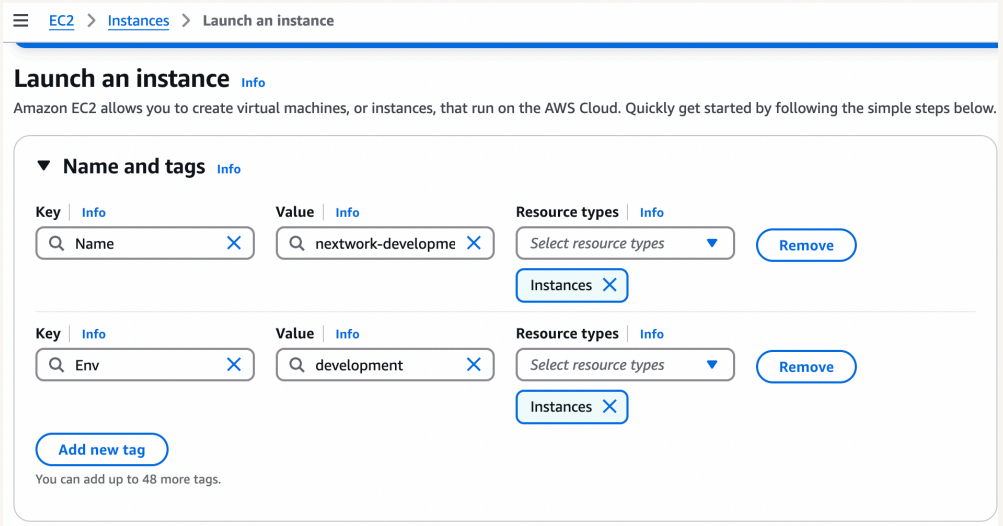

## This project took me...

Setting up IAM best practices (MFA, least privilege, logging) is a 1-2 hours, Automating IAM security compliance, and Integrating IAM into CI/CD pipelines will take significant time to ensure safe and secure prcatices.

# Tags

Tags are labels to help AWS Account users identify and manage their resources. Tags are useful for grouping, mass management and applying security policies within AWS environment.

The tag used on my EC2 instances is called Env. The values assigned for my instances are production, and development. They represent two different environments that we are using to build and release the NextWork app.



# IAM Policies

IAM (Identity and Access Management) policies are permissions, specify which actions users, groups, roles are allowed to perform on which AWS resources, ensuring secure and controlled access to the resources.

## The policy I set up

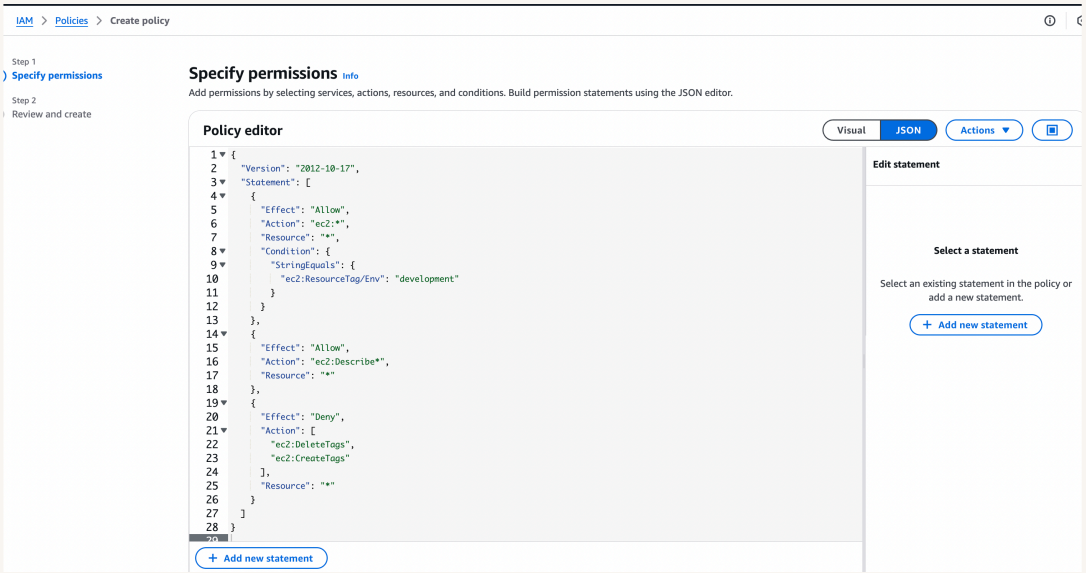
for this project I have set up a policy using JSON policy editor under create policy module.

I have created a policy that allows users to perform all EC2-related actions to all EC2 instances that have the Environment ("Env") tag with "development" and, it also denies or restricts creating and deleting tags for ALL EC2 instances.

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

The Effect: is to Allow or Deny. Actions: are the specific action that we are wanting to allow or deny. Resources: are the specific resource/group of resources in my AWS Account that this policy will take effect on.

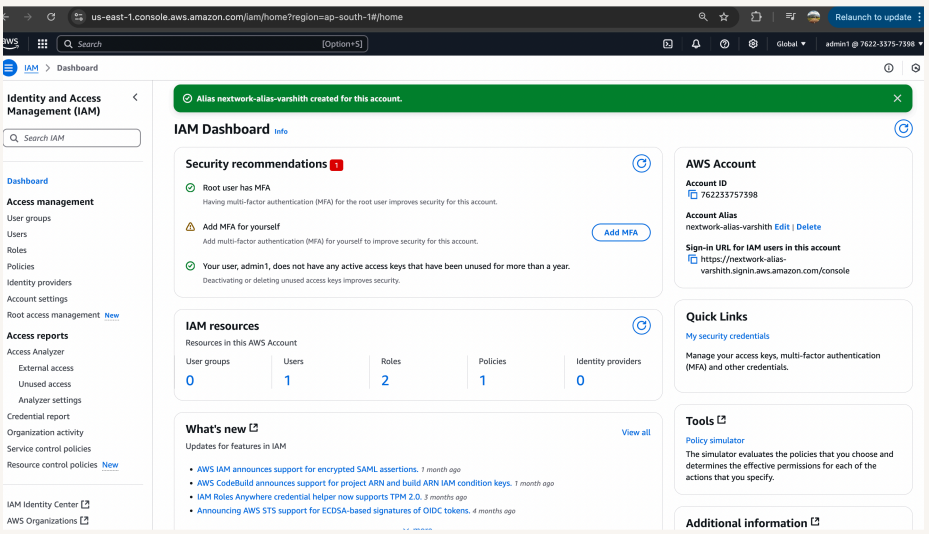
# My JSON Policy



# Account Alias

An account alias is a custom name that I can assign to my AWS IAM account, this name is used during log in to account instead of using AWS account ID. Usually this method can help new interns to do their work without affecting organizaton resources.

Creating an account alias is super quick, just unique ALIAS everytime you create alias account. Now my new AWS console sign in link is https://nextwork-alias-varshith.signin.aws.amazon.com/console it is easy to remember & share link with others.



# IAM Users and User Groups

## Users

IAM users are new employees that will get access to your resources/AWS account, where users are created by myself using AWS IAM service. This will allow new employees to acces AWS resources in a secure way, as they have limited permissions.

## User Groups

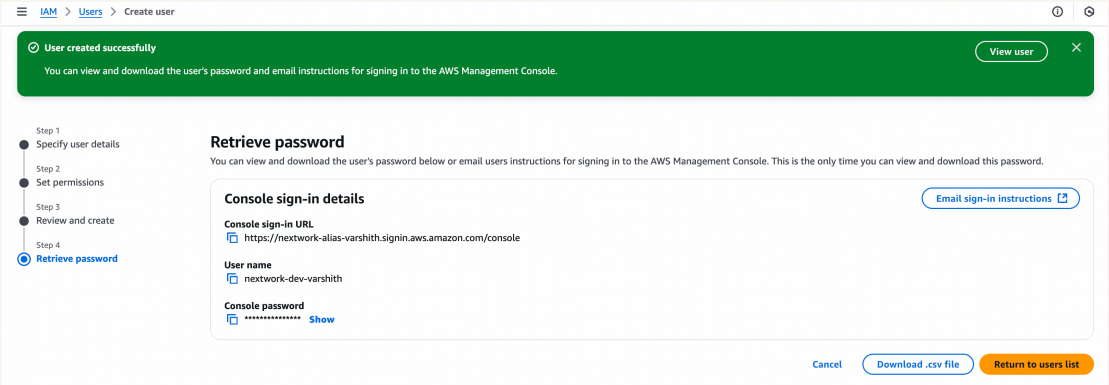
IAM user groups are new employees that will get access to your resources/AWS account, whereas user groups are the collections/folders of users for easier user management. I have created one user group, and granted the group with some permissions.

I attached the policy I created for this user group, this allows defined permissions in the policy to all users within that group, helps in user access management by enabling centralized control and easier to scale incase of large no of users.

# Logging in as an IAM User

After setting up new user, we can provide user signin details in two ways, one is we can a mail directly to user, second is download csv file of signin details and share with the respective user.

Once I logged in as my new (nextwork-dev-varshith)IAM user I noticed that permissions of few services, options, settings were denied,This is because i am a new user and my manager granted me only required permissions, actions subject to my work.

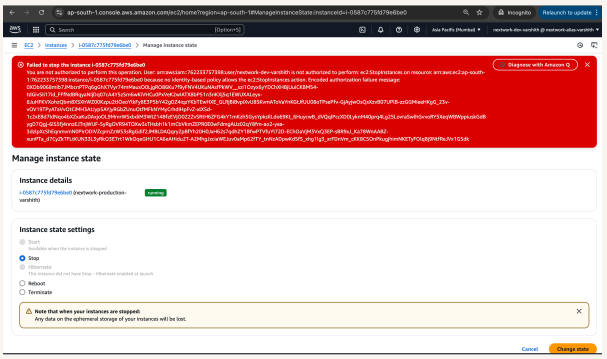


# Testing IAM Policies

I tested the JSON IAM policy by trying to stop the development and production instances by triggering the Stopinstances action under manage instance state panel.

## Stopping the production instance

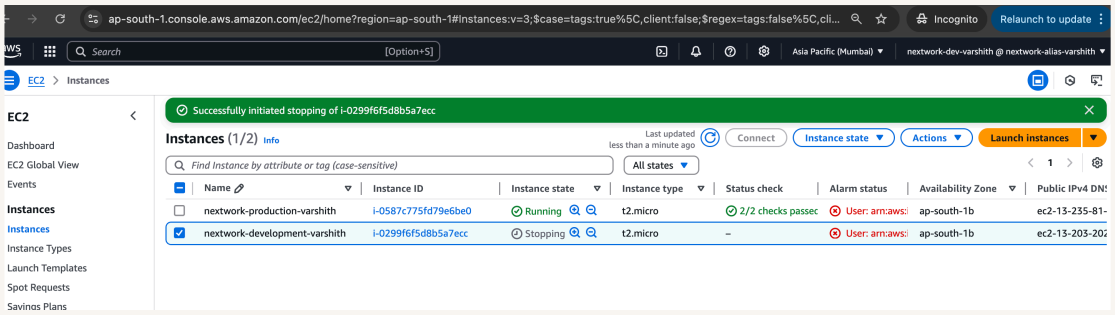
When I tried to stop the production instance, a red banner showed up saying you are not authorized to perform this operation. thanks to IAM, it helps new users to perform only certain actions, this explain new user cannot delete an instance.



# Testing IAM Policies

## Stopping the development instance

When I tried to stop the production instance, an error message stopped me and explained that I am not authorised to stop the production instance, but tried to stop production instance, it stopped successfully with out any error.





# Everyone should be in a job they love.

Check out nextwork.org for more projects