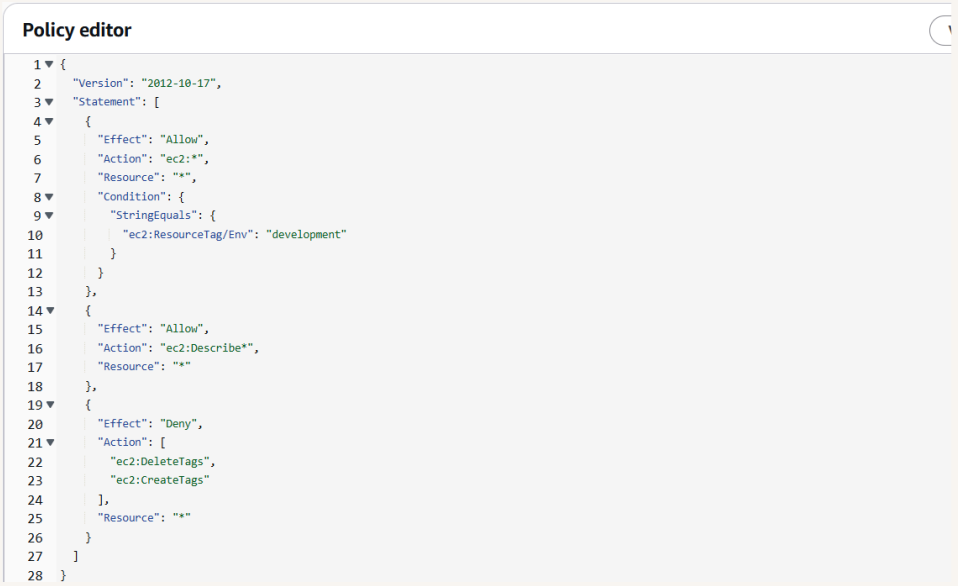
nextwork.org

Cloud Security with AWS IAM

Praveen Kambale



Praveen Kambale
NextWork Student

Introducing Today's Project!

Project overview

In this project, I demonstrate AWS Identity and Access Management (IAM). The goal of this project is to learn and understand IAM users, groups, policies, and account aliases.

Tools and concepts

In this project, I learned AWS IAM concepts, including users, groups, and policies to manage access. I also worked with account aliases and EC2 instances, gaining hands-on experience with permissions, access control, and secure resource management.

Project reflection

This project took me approximately 1.30 hours. The most challenging part was setting up IAM policies to restrict production access while allowing development access. The most rewarding part was seeing the intern safely use the development resources.

Praveen Kambale
NextWork Student

Tags

What I did in this step

In this step, I launch two EC2 instances to increase NextWork's computing power.

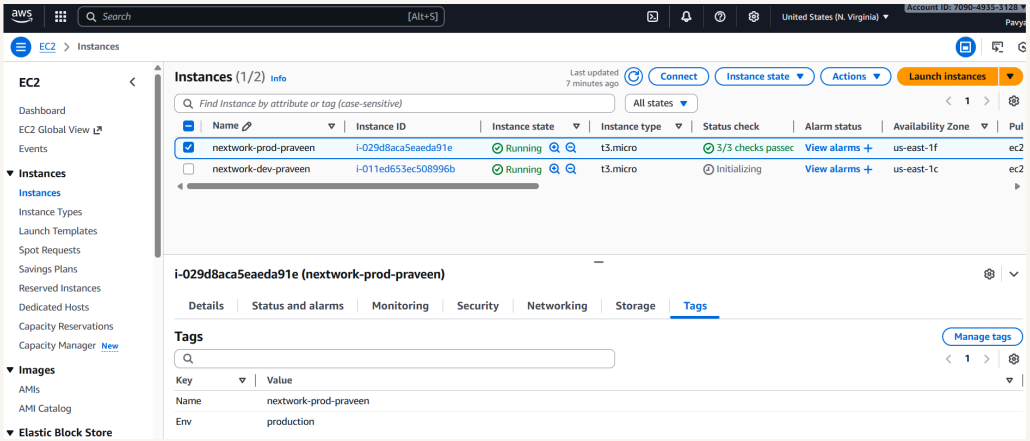
Understanding tags

ags are key value labels used to organize, manage, and track AWS resources efficiently.

My tag configuration

I assigned tags to my two EC2 instances to easily identify and manage them. The tags include Name (env), value (production & development)

Praveen Kambale
NextWork Student



Praveen Kambale
NextWork Student

IAM Policies

What I did in this step

I created IAM policies to allow the intern access only to the development EC2 instance, ensuring they can test safely without affecting the production environment.

Understanding IAM policies

IAM policies allow us to define and control permissions for EC2 resources by specifying who can access them and what actions they are allowed to perform, helping ensure secure and controlled resource usage.

The policy I set up

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

Policy effect

The effect of my policy is to allow the intern full access to EC2 instances tagged Env=development and view all instances, while denying tag changes, ensuring safe testing without affecting production.

Understanding Effect, Action, and Resource

In a JSON IAM policy, Effect specifies whether the policy allows or denies an action, with Deny taking priority. Action lists the operations the policy controls, and Resource defines which AWS resources the actions apply to.

Praveen Kambale
NextWork Student

My JSON Policy

Policy editor

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Env": "development"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource": "*"
    }
  ]
}
```

Praveen Kambale
NextWork Student

Account Alias

What I did in this step

In this step, we are creating an AWS Account Alias to simplify user login. By setting an account alias, users including our intern can log in using an easy to remember URL instead of the default AWS account ID.

Understanding account aliases

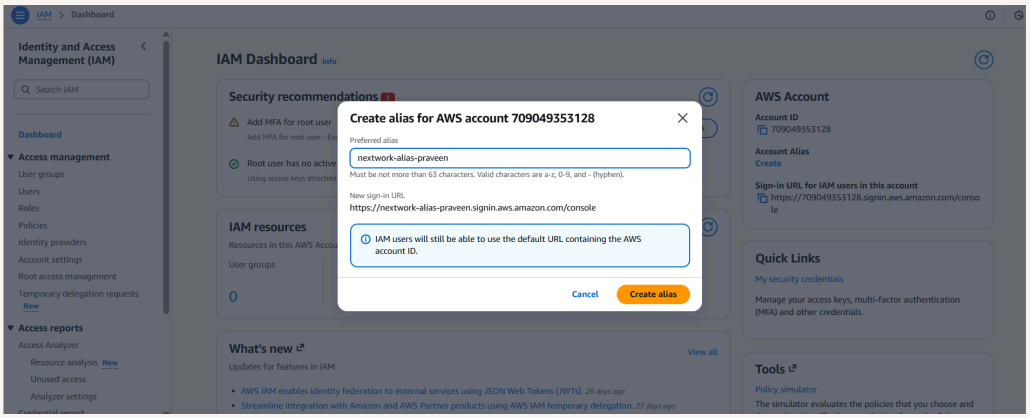
An AWS Account Alias is a custom name for your AWS account that replaces the numeric account ID in the login URL, making it easier for users to sign in while keeping all permissions and security intact.

Setting up my account alias

Setting up my AWS Account Alias took only a few minutes, as it is a simple process of creating a custom name to replace the default account ID in the login URL.Now, my new AWS console sign-in URL is nextwork-alias-praveen2000

Praveen Kambale
NextWork Student

nextwork.org



Praveen Kambale
NextWork Student

IAM Users and User Groups

What I did in this step

In this step, we are creating a dedicated IAM group for all NextWork interns to manage their permissions centrally, and setting up a new IAM user so the intern has a secure login to access AWS resources.

Understanding user groups

An IAM user group is a collection of IAM users that lets you manage permissions for all members at once. Policies attached to the group apply to every user, simplifying access control and ensuring consistent permissions.

Attaching policies to user groups

I attached the policy I created to the user group, which means all users in the group inherit the permissions. Interns can access development EC2 instances safely while being restricted from production.

Praveen Kambale
NextWork Student

Understanding IAM users

IAM users are individual identities in an AWS account that represent people or applications. Each user has unique credentials and can be assigned permissions directly or via groups for secure and controlled access to AWS resources.

Praveen Kambale
NextWork Student

Logging in as an IAM User

Sharing sign-in details

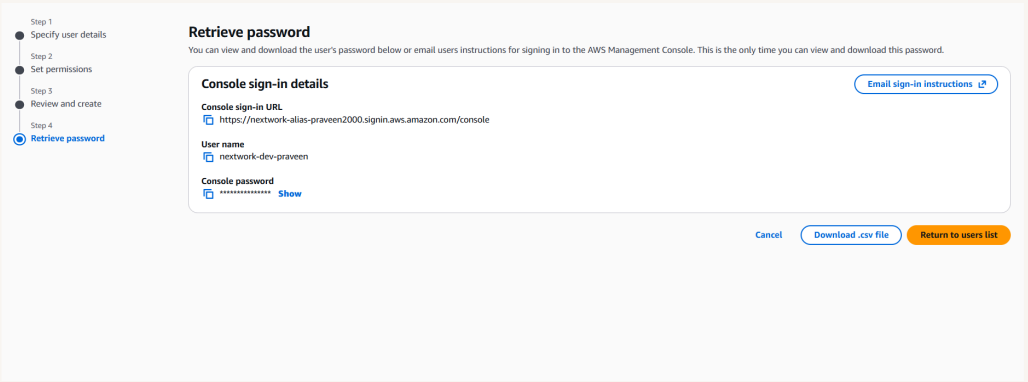
There are two ways to share a new IAM user’s sign-in details: provide the login URL, username, and temporary password directly, or send the credentials securely via email so the user can log in and set their own password.

Observations from the IAM user dashboard

As a new IAM user, some dashboard panels show "Access denied" because their permissions are restricted. They can access development resources but are blocked from production.

Praveen Kambale
NextWork Student

nextwork.org



Praveen Kambale
NextWork Student

Testing IAM Policies

What I did in this step

In this step, we log in using the intern’s IAM user credentials to test their access, ensuring they can work on the development EC2 instance but cannot access the production instance.

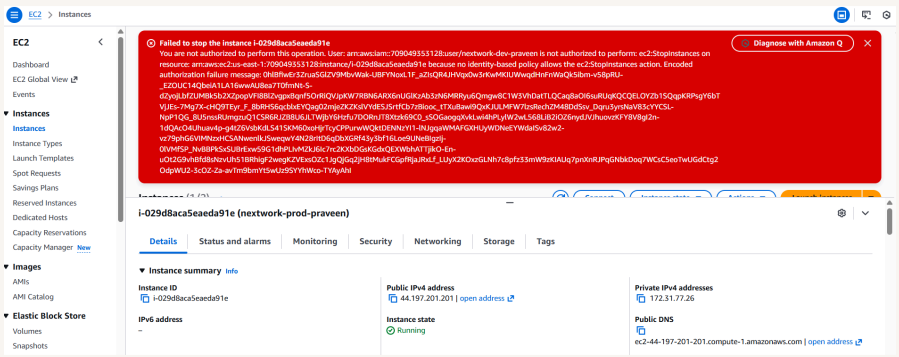
Testing policy actions

The actions I performed on the two EC2 instances were: starting and stopping the development instance to test access and verify permissions, while attempting to stop the production instance, which was denied due to restricted permissions.

Stopping the production instance

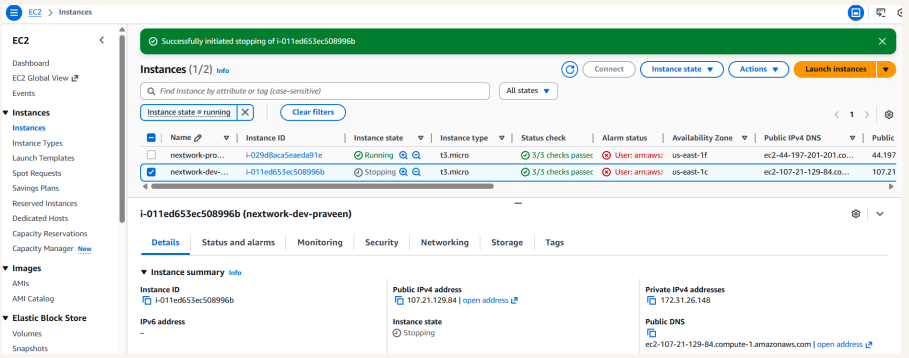
When I tried to stop the production instance using the intern’s IAM user, the action was denied because the policy restricts access, preventing any accidental changes to production.

Praveen Kambale
NextWork Student



Stopping the development instance

When I tried to stop the development instance using the intern's IAM user, the action was allowed, as the policy grants full access to EC2 instances tagged for development, enabling safe testing and management.



The place to learn & showcase your skills

Check out nextwork.org for more projects