NextWork.org

Cloud Security with AWS IAM

Uday Atla

Uday Atla
NextWork Student

Introducing today's project!

What is AWS IAM?

IAM stands for Identity and Access Management. You'll use AWS IAM to manage the access level that other users and services have to your resources.

How I'm using AWS IAM in this project

I used AWS IAM to manage the access level that other users and services have to my resources.It's all about giving permissions to IAM users, groups, or roles,

One thing I didn't expect...

The one thing I did not expect in this project is the ease of setting up the security to your cloud.

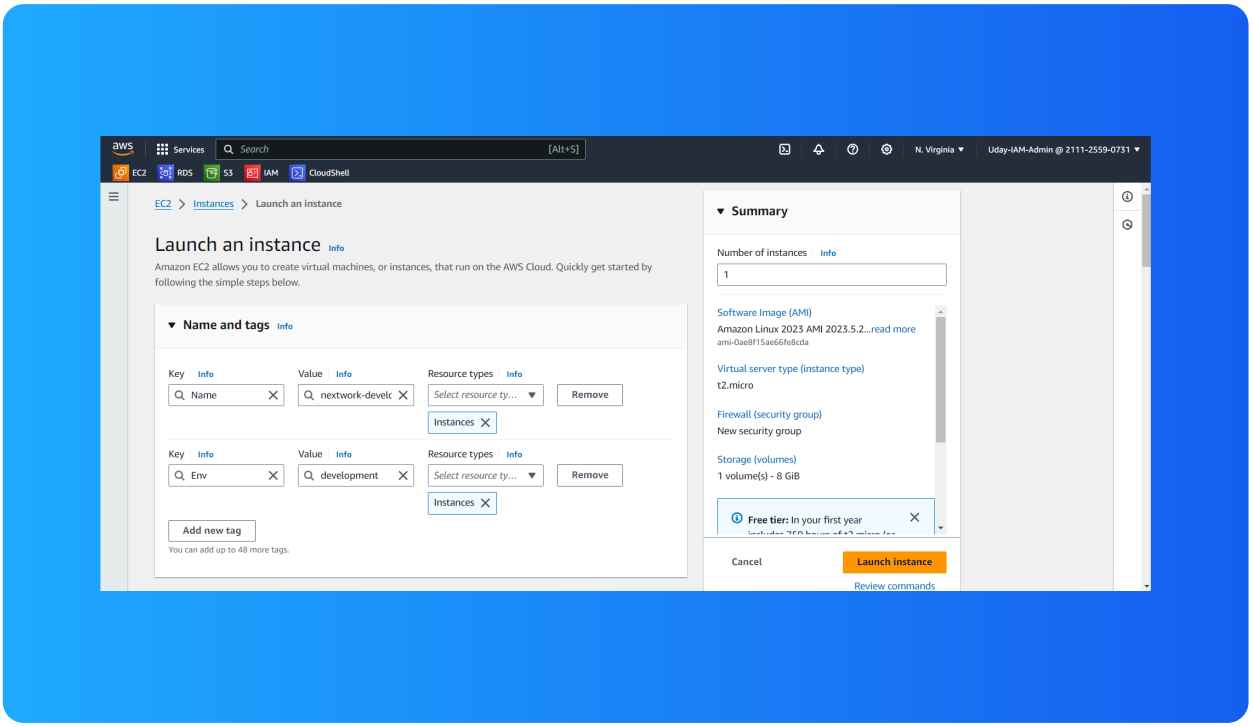
This project took me...

Continuous dedication and understanding of each service took me about 1.5 hrs but it's worth learning.

Tags

Tags are like labels you can attach to AWS resources for organization. This tagging helps us with identifying all resources with the same tag at once cost allocation and applying policies based on environment types.

The tag I've used on my EC2 instances is called ENV as in 'Environment'. The values I've assigned for my instances are Production and Development.



Uday Atla
NextWork Student

IAM Policies

IAM Policy is a rule for who can do what with your AWS resources. It's all about giving permissions to IAM users, groups, or roles.

The policy I set up

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

I've created a policy that can have two values - either Allow or Deny - to indicate whether the policy allows or denies a certain action.

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

When writing a JSON policy statement,you have to specify that: EFFECT: Allow or Deny ACTION: the specific action we want to deny. RESOURCES: the specific resource/group of resources in my AWS account that this policy will take effect on.

Uday Atla
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": "*"
        }
    ]
}
```

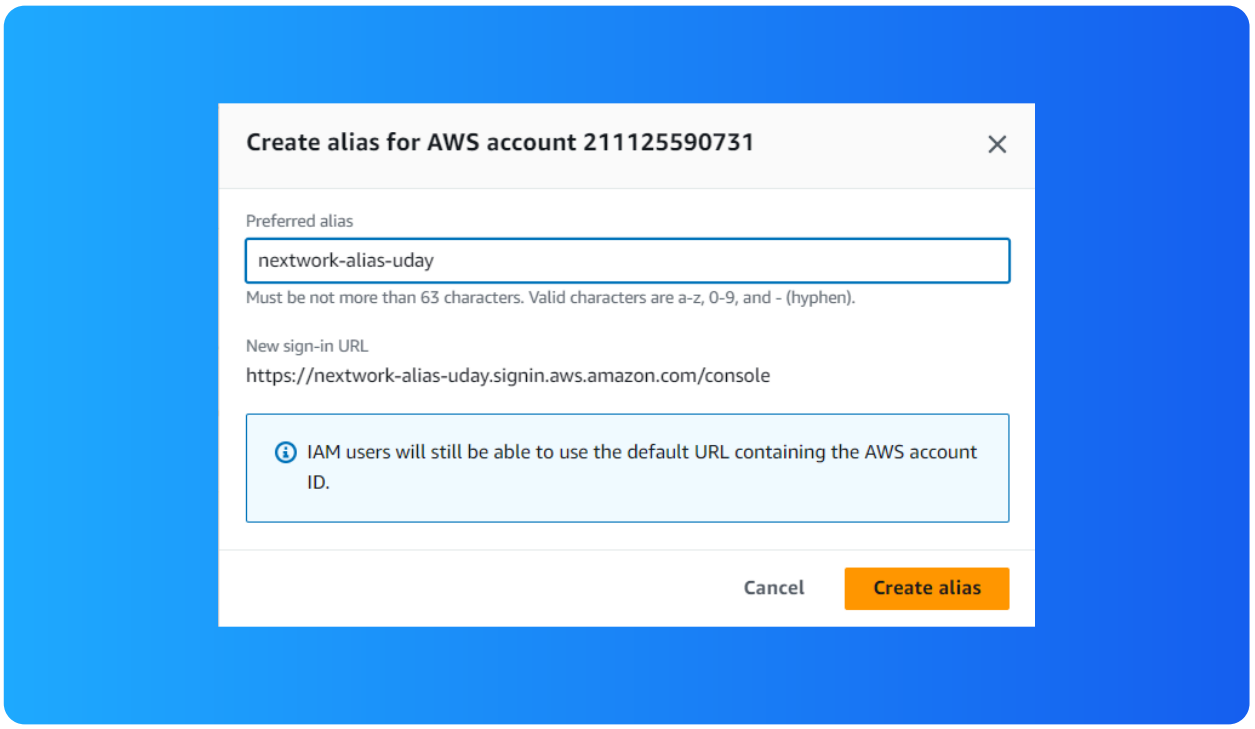
Uday Atla
NextWork Student

Account Alias

An account alias is a friendly name for your AWS account that you can use instead of your account ID (which is usually a bunch of digits) to sign in to the AWS Management Console.

Creating an account alias took me less than 5 min.

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



Uday Atla
NextWork Student

IAM Users and User Groups

Users

IAM users are the people who will get access to your resources/AWS account, whereas user groups are the collections/folders of users for easier user management.

User Groups

IAM user groups are a collection/folder of IAM users. It allows you to manage permissions for all the users in your group at the same time by attaching policies to the group rather than individual users.

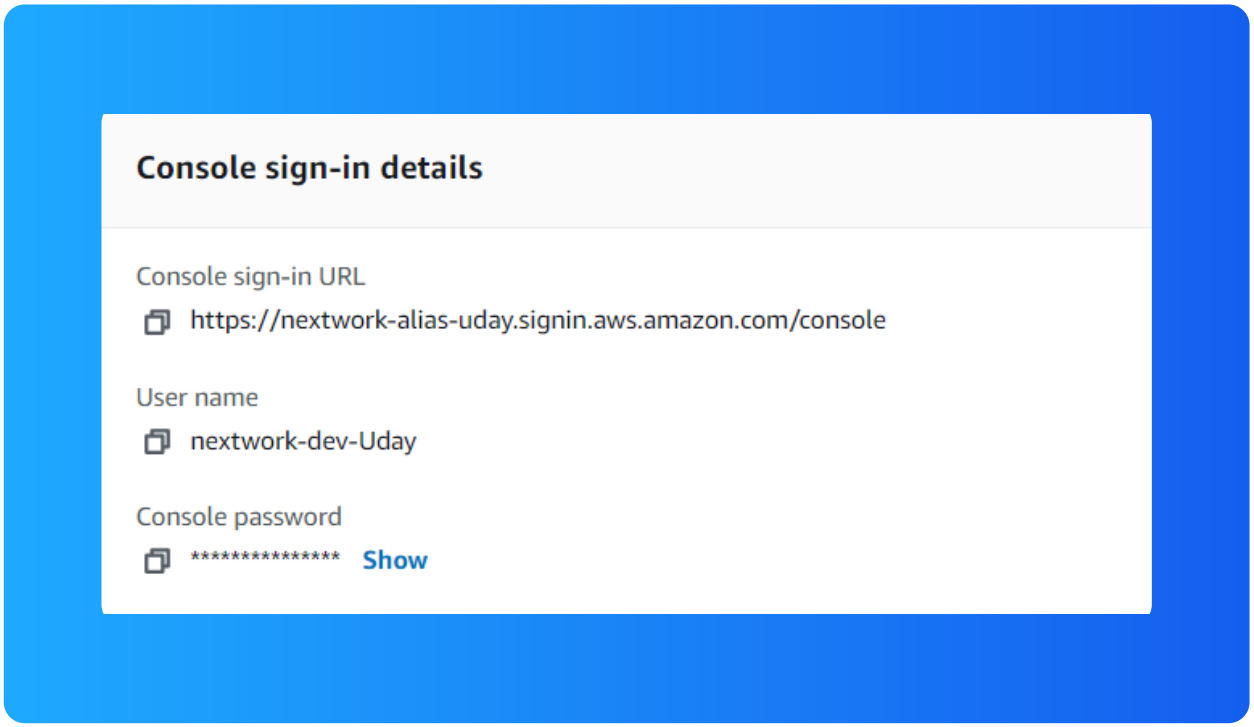
I attached the policy I created to this user group, which means all users that are added to the user group will automatically inherit the user group access permission.

Uday Atla
NextWork Student

Logging in as an IAM User

The first way is to email sign-in instructions; secondly, download a CSV. file.

Once I logged in as my IAM user, I noticed As a new user, I noticed that some of my dashboard panels were showing Access Denied Already!



Uday Atla
NextWork Student

Testing IAM Policies

tested my JSON IAM policy by I set up by trying to stop the development and production instances, i.e. triggering the Stop instances action.

Stopping the production instance

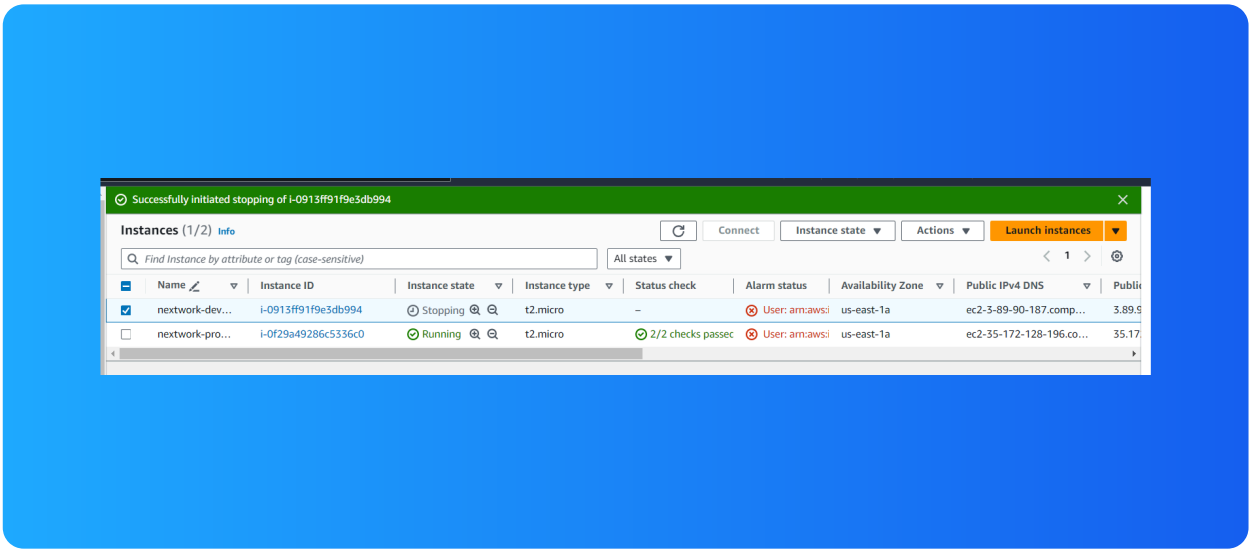
When I tried to stop the production instance an error message stopped me and explained that i was not and authorized to stop the production instacnce

Uday Atla
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, the development instance could be stopped! This was because the policy I created allowed all EC2-related action to all EC2 instances/resources with the ENV tag development.



Everyone should be in a job they love.

Check out nextwork.org for more projects