NextWork.org

Cloud Security with AWS IAM

NI nikhil7_94@hotmail.com

```
{
  "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": "*"
    }
  ]
}
```

NI
nikhil7_94@hotmail.com
NextWork Student
NextWork.org

Introducing today's project!

What is AWS IAM?

AWS IAM is used to manage access level to user to the AWS resources. It is useful to control who can do what in the AWS services.

How I'm using AWS IAM in this project

Today I used AWS IAM to create user groups, users and IAM policies to learn how each of them works.

One thing I didn't expect...

I didnt expect there was a tool called policy simulator that evaluates the policies created for this project.

This project took me...

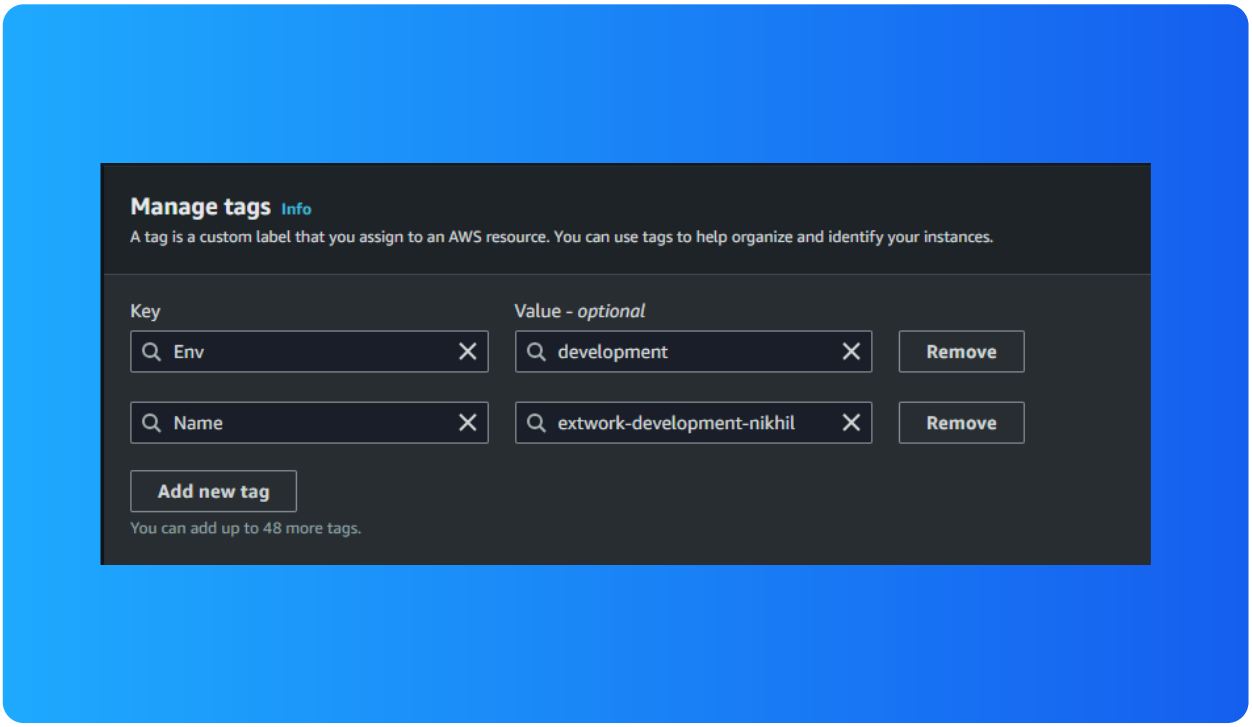
I took around 1 hour with this project.

NI
nikhil7_94@hotmail.com
NextWork Student

Tags

Tags are like labels you can attach to AWS resources for organization.

The tag I've used on my EC2 instances is called "Env" for both instaces. The value I've assigned for my instances are for one of the EC2 instance "production" and the other instance "development"



NI
nikhil7_94@hotmail.com
NextWork Student
NextWork.org

IAM Policies

IAM stands for Identity and Access Management. It used to manage the access level of the users to the services.

The policy I set up

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

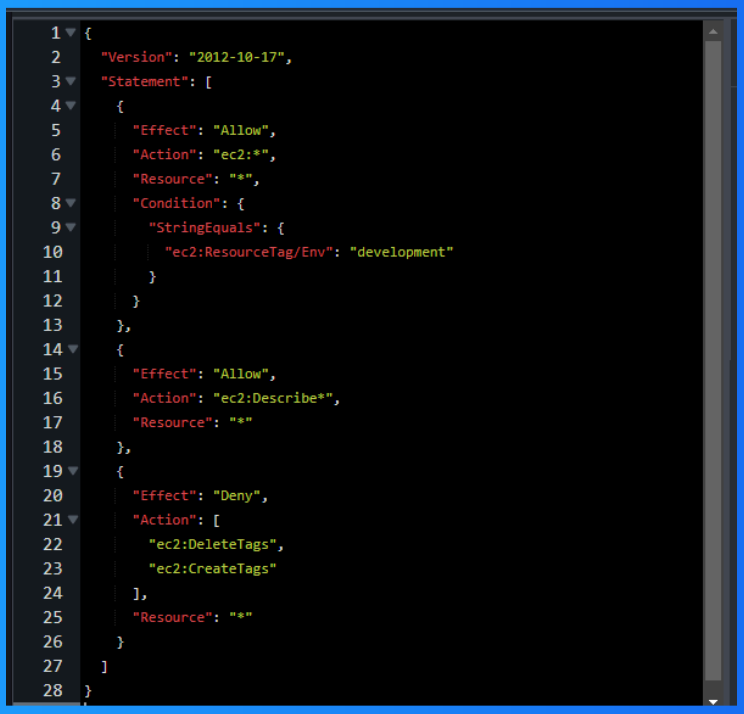
I've created a policy that allows some actions like starting, stopping, and describing EC2 instances for instances tagged with "Env = development" while denying the ability to create or delete tags for all instances.

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

The Effect, Action, and Resource attributes of a JSON policy means if you are allowed or dennied to an action which means all the actions in the EC2 instanceand to which resources.

NI
nikhil7_94@hotmail.com
NextWork Student

My JSON Policy



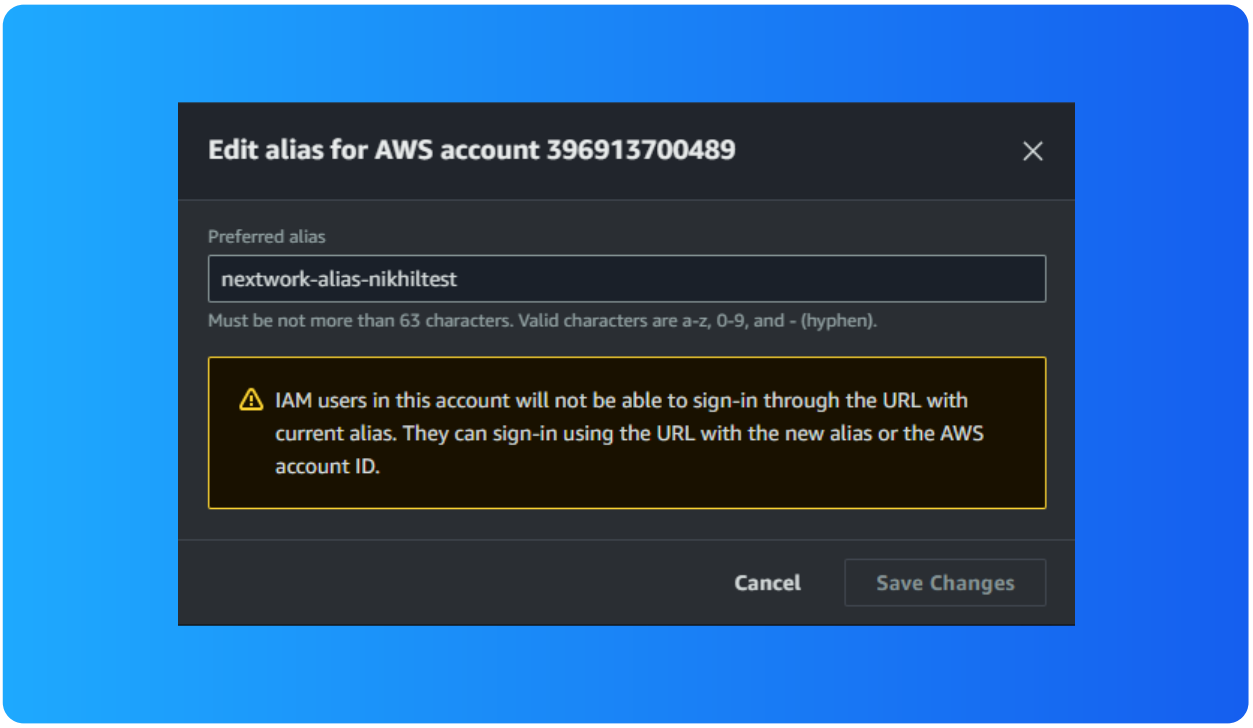
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Env": "development"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",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

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 1 minute.

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



NI
nikhil7_94@hotmail.com
NextWork Student
NextWork.org

IAM Users and User Groups

Users

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

User Groups

An IAM user group is 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.

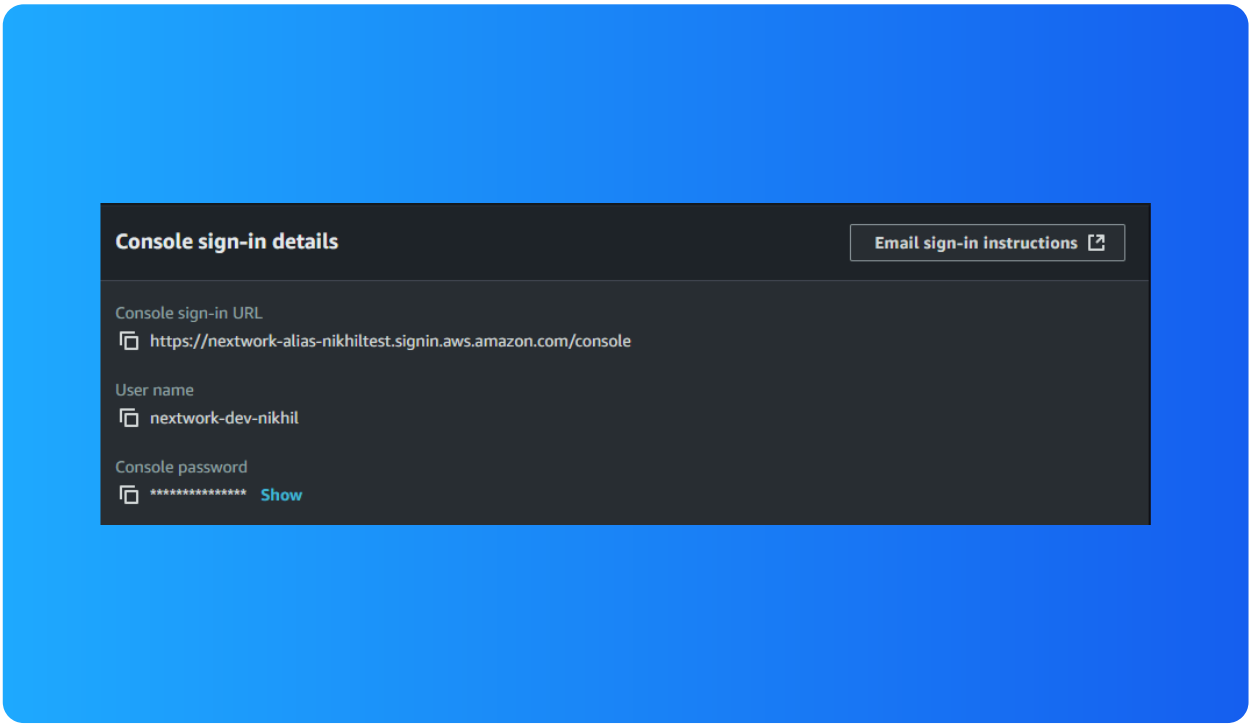
I attached the policy I created to this user group, which means this user group has certain permissions to do some indicated tasks.

NI
nikhil7_94@hotmail.com
NextWork Student

Logging in as an IAM User

The first way is by the console sign-in details and the second way is by .csv file.

Once I logged in as my IAM user, I noticed that the AWS console will treat you as someone that is starting from 0 again.



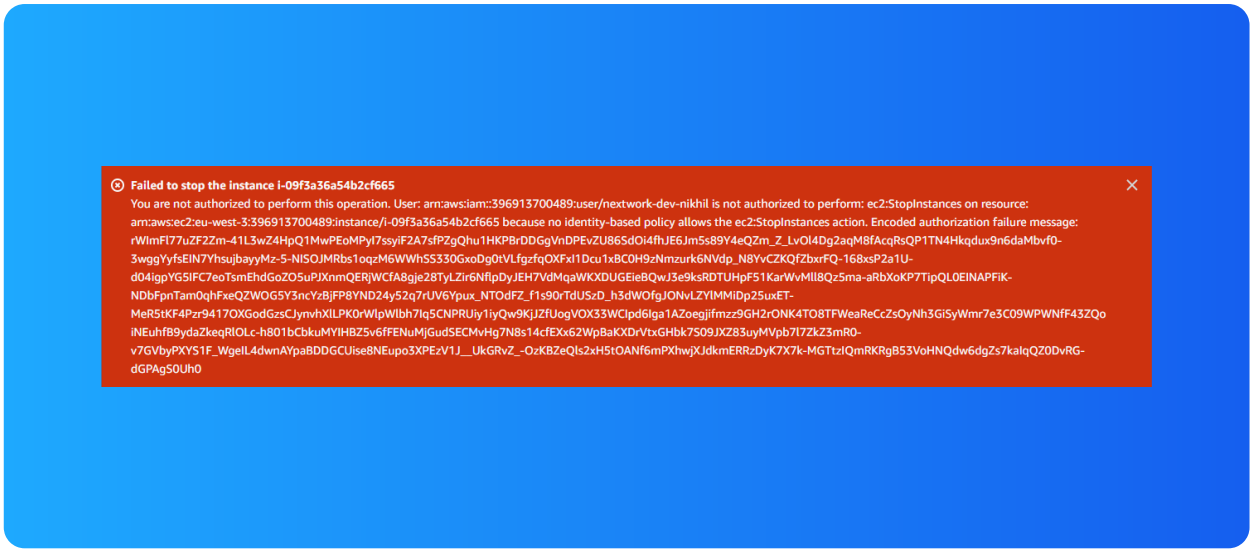
NI
nikhil7_94@hotmail.com
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by accessing to AWS console from incognito window and trying to stop both instances.

Stopping the production instance

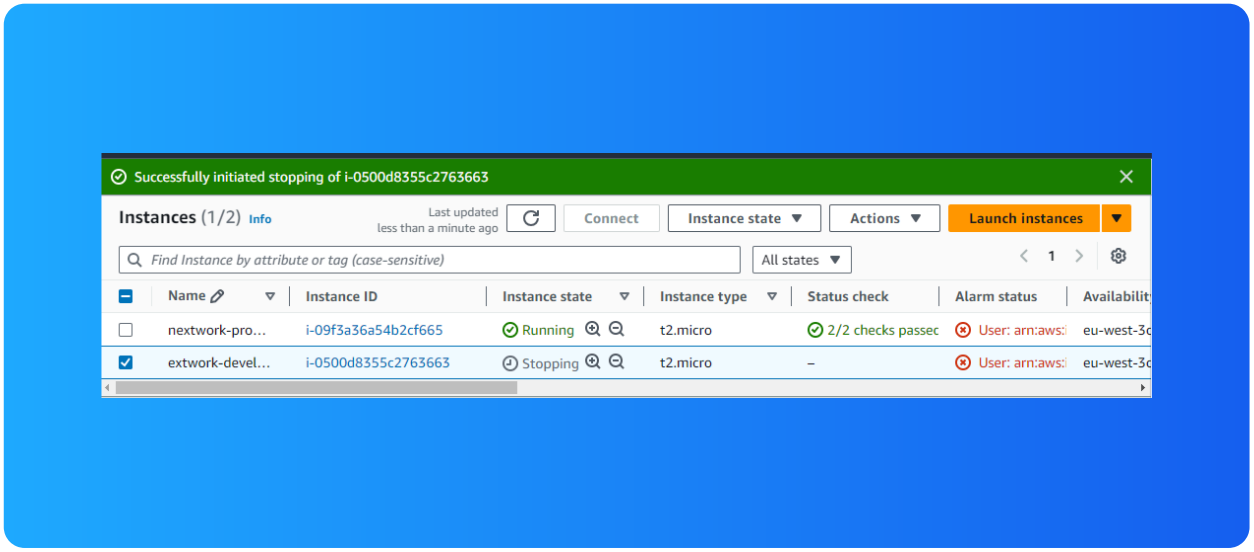
When I tried to stop the production instance I got an error message as I dont have the permission to stop that instance.



Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance and it worked because in this case I did have the right permissions.



Everyone should be in a job they love.

Check out nextwork.org for more projects