nextwork.org

Cloud Security with AWS IAM

Muhammad Abbas

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": "*"
    }
  ]
}
```

Muhammad Abbas
NextWork Student

Introducing Today's Project!

In this project, I will demonstrate how to use AWS IAM to control access and permission settings in my AWS account. I'm doing this project to learn about cloud security from the absolute foundations - every company thinks about access permissions, and there are even entire jobs called 'IAM Engineers' focused on the skills I am about to build today.

Tools and concepts

Services I used were today were Amazon EC2 and AWS IAM! Key concepts I learnt include IAM users, policies, user groups and account aliases. I also learn how to use the Policy Simulator and how JSON policies work. How to launch an instance, how to tag an instance, how to log in as another user.

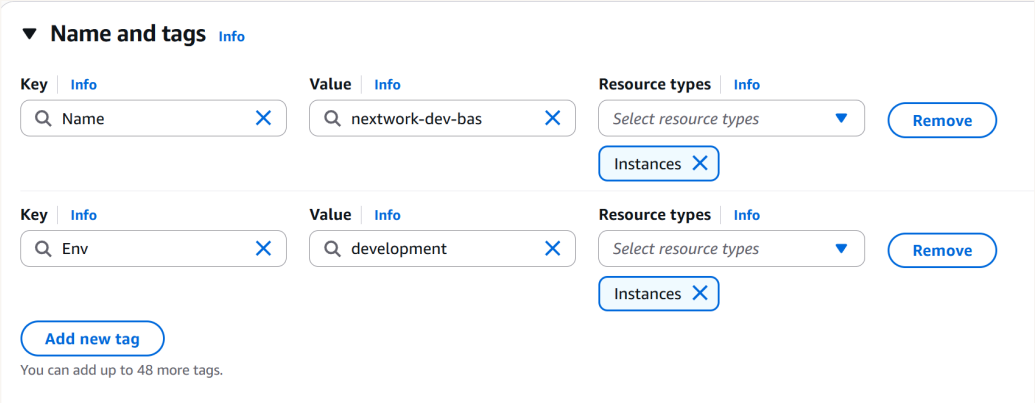
Project reflection

This project took me approximately 1 hour 15 mins. The most challenging part was understanding the IAM policy since It was written in JSON and it contained multiple statements. It was most rewarding to see the permission denied when the intern tried to delete the production instance - my IAM access management set up is working:)

Tags

Tags are organizational tools that let's me label my resources. They are helpful for grouping resources, cost allocation and applying policies for all resources with the same tag.

The tag I've used on my EC2 instances is called Env, which stands for environment. The value I've assigned for my instances are production and development!



Muhammad Abbas
NextWork Student

IAM Policies

IAM Policies are are like rules that determine who can do what in my AWS account. I am using policies today to control who has access to my production/enviroment instance.

The policy I set up

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

I've created a policy that allows the policy holder (i.e. the interns to have permission to do anything they want to any instance tagged with "development". They can also see information for any instance, but they're denied access to deleting/creating tags for any instance as well.

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 whether or not the policy is allowing/denying action (i.e. Effect); what the policy holder can or cannot do (i.e. Action): and the specific AWS resources that the policy relates to (i.e. Resourse).

My JSON Policy

Policy editor

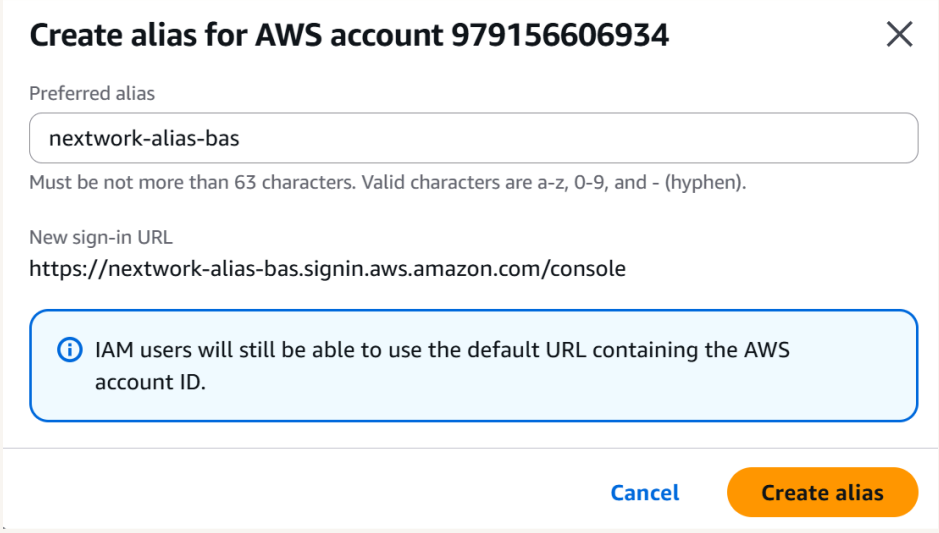
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Env": "development"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",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

Muhammad Abbas
NextWork Student

Account Alias

An account alias is simply a nickname for my AWS account! Instead of a long account ID, I can now reference my account alias instead.

Creating an account alias took me 30 seconds - it's a simple configuration in the IAM dashboard. Now, my new AWS console sign-in URL used the alias instead of my account ID.



Muhammad Abbas
NextWork Student

IAM Users and User Groups

Users

IAM users are people or entities that have access/can login to my AWS account.

User Groups

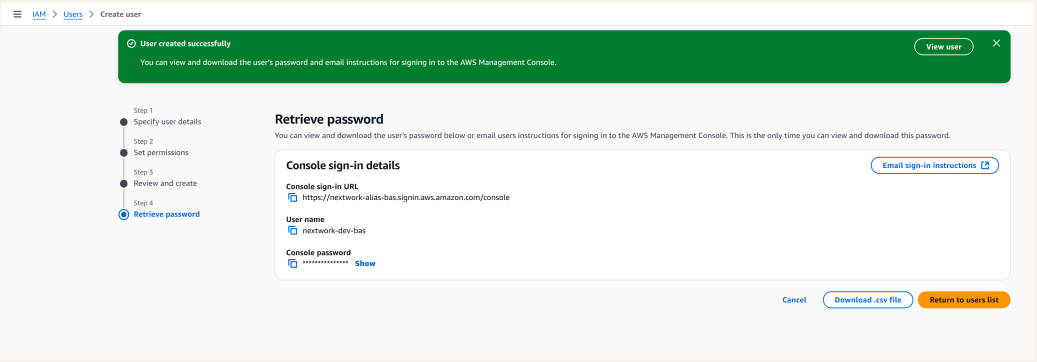
IAM user groups are like folders that collect IAM users so that I can apply permission settings at the group level.

I attached the policy I created to this user group, which means any user created inside this group will automatically get the permissions to the NextWorkDevEnvironmentPolicy IAM policy.

Logging in as an IAM User

The first way is to email sign-in instructions to the user, while the second way is to download a /.csv file with the sign-in details inside.

Once I logged in as my IAM user, I noticed that the user is already denied access to panels on the main AWS console dashboard. This was because I only set up permissions to the development EC2 instances, so that the intern wouldn't have access to even see anything else.



Testing IAM Policies

I tested my JSON IAM policy by attempting to stop both development and the production instances.

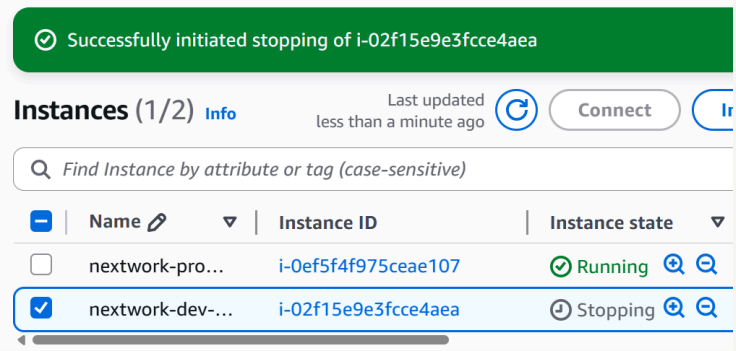
Stopping the production instance

When I tried to stop the production instance, we were met with an error! This was because the production instance is tagged with the 'production' label, which is outside of the scope of the permission policy - interns are only allowed to do things to development instances.

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, I successfully saw the instance state change to Stopping and then Stopped. This was because my permission policy allows the intern (i.e. users in the network-dev-group) to stop instances.

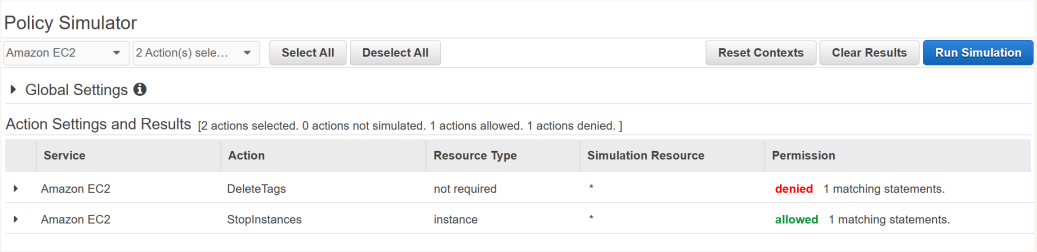


The IAM Policy Simulator

The IAM Policy Simulator is is tool that let's me simulate actions and test permission settings by defining a specific user/group/role and the actions wewant to test for. It's useful for saving time when testing permission settings! No more logging into another user or actually stopping resources.

How I used the simulator

I set up a simulation for whether the dev user group has permission to Stopinstances or DeleteTags. The results were denied for both - I had to adjust the scope of the EC2 instances to ones that are tagged with "development". Once I applied that tag, permission was allowed.



The place to learn & showcase your skills

Check out nextwork.org for more projects