nextwork.org

Cloud Security with AWS IAM

GS gsweaponx@gmail.com

Introducing Today's Project!

In this project, I will demonstrate how to use AWS IAM to control access and permission settings in our AWS account. I'm doing this project to learn about Cloud Security

Tools and concepts

Services I used were Amazon EC2 and AWS IAM. Key concepts I learnt include IAM users, roles, policies, user groups and alias. We also learnt how to use policy simulator.

Project reflection

This project took me approximately 1hour today including demo time. The most challenging part was unserstanding and writing IAM policy in JSON. It was most rewarding to see my IAM access management working with the denied and successful message.

Tags

Tags are organisational tools that lets us label our resources. They are helpful for grouping resources, cost allocation and applying policies for all resources of the same tag.

The tag I've used on my EC2 instances is called Env (Environment). The value I've assigned for my instances are production and development.

IAM Policies

IAM Policies are rules that deteermine who can do what in our AWS account. We are using policies today to control who has access to our production and development instance.

The policy I set up

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

I've created a policy that allows the policy holder (in this case the intern) to have permission to do anything they want to any instance with tag as development. They can also see information for any instance but denied access to deleteing tags.

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 policy is allowing or denying something i.e. the effect. What policy holder can & can't do is i.e. the action. And the specific AWS resources that the policy relates to

My JSON Policy

Account Alias

An account alias is just a nice name for our account instead of a long account ID we can now refrence our account alias instead.

Creating an account alias took me 30 seconds. Now, my new AWS console sign-in URL uses alias instead of my account ID.

IAM Users and User Groups

Users

IAM users are poeple or entities that have access/can login to your AWS account.

User Groups

IAM user groups are the collections/folders of users for easier user management.

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

Logging in as an IAM User

The first way is to email the instructions to the user while the second way is to download the CSV file with login credentials

Once I logged in as my IAM user, I noticed that our user is already denied access to items/services on main AWS dashboard This was because we only set up permissions to only our developed EC2 instances.

Testing IAM Policies

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

Stopping the production instance

When I tried to stop the production instance we were met with an error. This was because our production instance is tagged with the productipn label which is outside the scope of our intern access policy.

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance we successfully saw the instance state to stopping and stopped. This was because our permission policy allowed the intern to stop development instances.

nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects