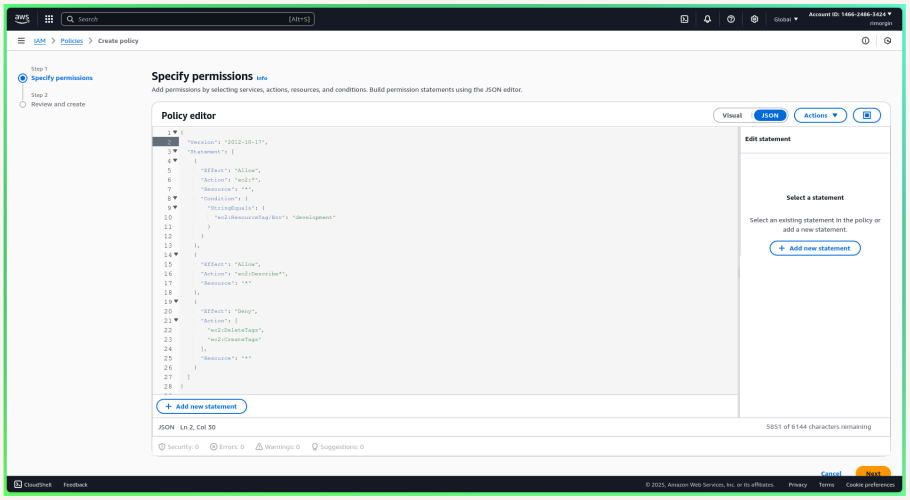
nextwork.org

Cloud Security with AWS IAM

Sean Calderon



Sean Calderon
NextWork Student

Introducing Today's Project!

In this project, I will demonstrate how to spin up virtual servers or EC2 instances. Next up, creating policies and applying it to a certain identity or group using IAM. I'm doing this project to learn about IAM access control and user management.

Tools and concepts

Services I used were EC2 and IAM. Key concepts I learnt include applying policies on users or groups allows me to have access control in which case limiting certain access on EC2 instances only and specifying which actions are permitted on instances.

Project reflection

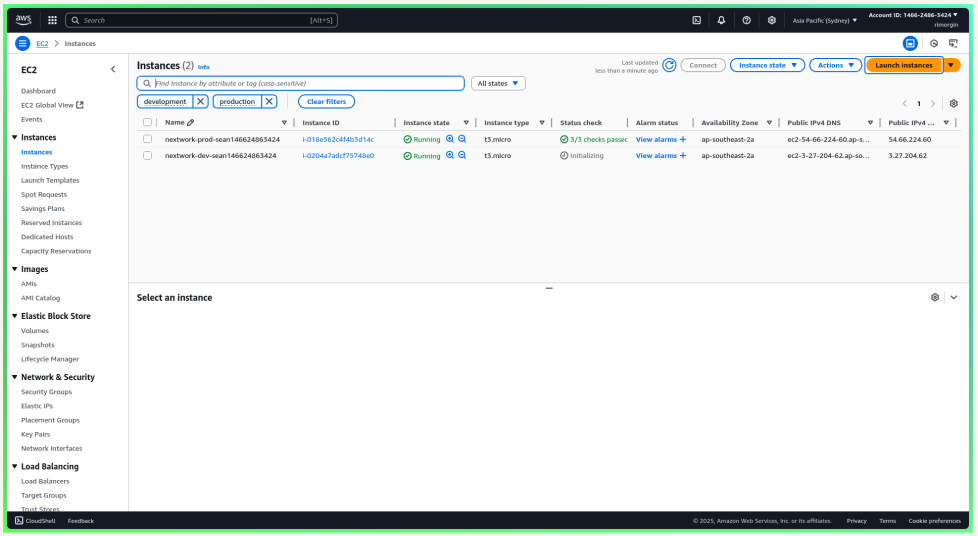
This project took me approximately 30 minutes. It was most rewarding to see access control and user management taking in effect when I test it myself.

Sean Calderon
NextWork Student

Tags

Tags are labels that are attached to AWS resources and are helpful for quick searches and filtering results, allowing you to find instantly the resources that you need.

The tag I've used on my EC2 instances is called "Env" key and the value I've assigned separately for my two instances are "development" and "production". Note that tag consist of key-value pair.



Sean Calderon
NextWork Student

IAM Policies

IAM Policies are a set of rules and permissions that define access control to users, groups, or roles specifying what they can or can't do on certain AWS Resources

The policy I set up

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

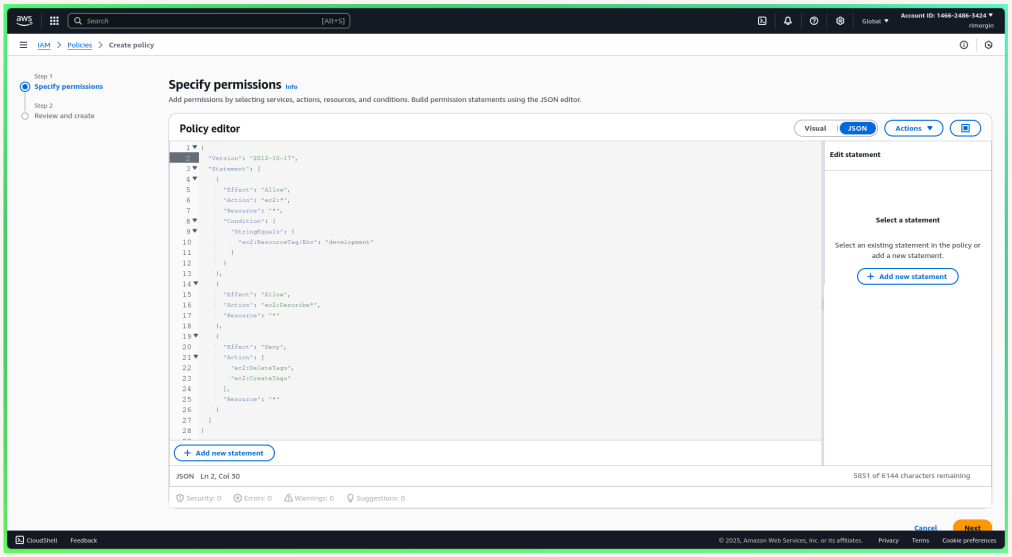
I've created the first policy to allow every action to perform however the condition states that it is only applied on a certain resources with a development tag. The second allows to list all instances and the third denies creating and deleting tag.

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 defining a structured set of permissions that specifies permit or deny, which actions are doable, and which resource the rule applies to.

Sean Calderon
NextWork Student

My JSON Policy

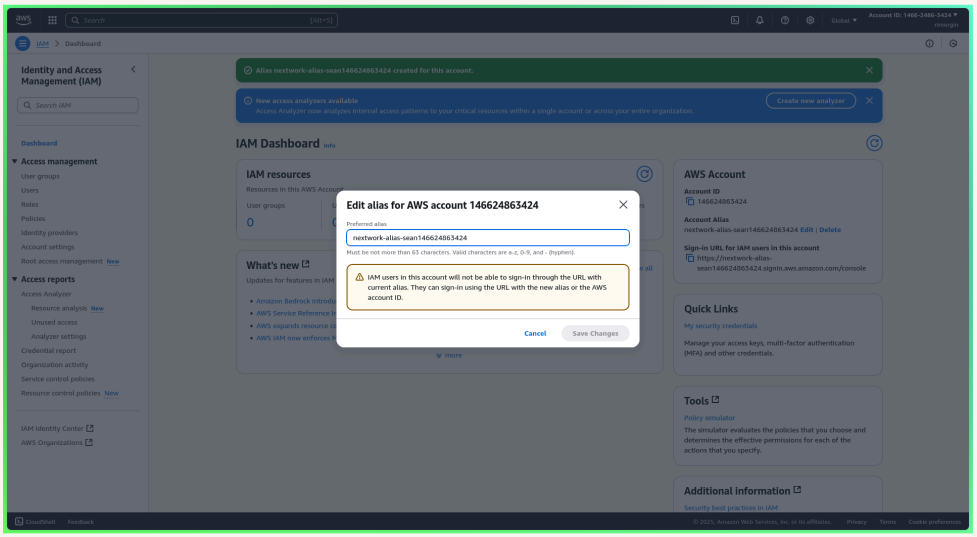


Sean Calderon
NextWork Student

Account Alias

An account alias is a friendly name for AWS account and is used for simplicity and making user-friendly sign-in page.

Creating an account alias took me a few clicks. Now, my new AWS console sign-in URL is https://nextwork-alias-sean146624863424.signin.aws.amazon.com/console...



Sean Calderon
NextWork Student

IAM Users and User Groups

Users

IAM users are entities that have predefined policies attached to them which dictates their access to the resources. IAM Users can be applied to IAM User Groups in order to share the same policies.

User Groups

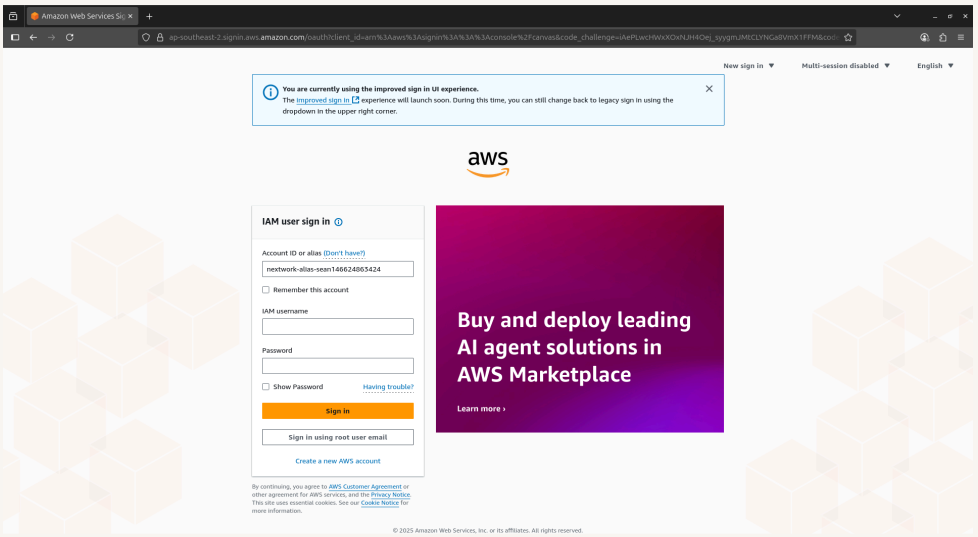
IAM user groups are collection of IAM Users which makes for administrator to have easier user management and access control.

I attached the policy I created to this user group, which means the policy is propagated across all users on the group.

Logging in as an IAM User

The first way is send the the link for sign-in page and then email them their access credentials.

Once I logged in as my IAM user, I noticed errors of access denied everywhere on the AWS management console dashboard. This was because I applied a policy limited to EC2 instances only.



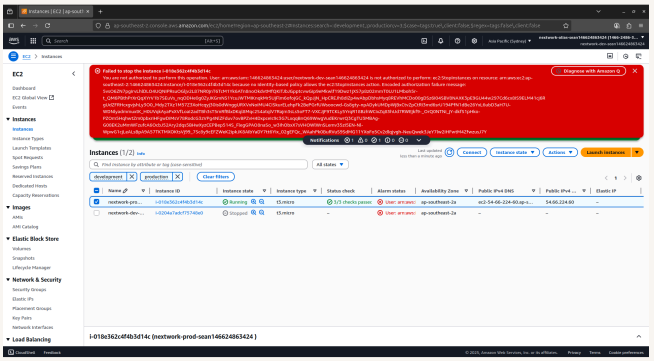
Sean Calderon
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by on my newly created IAM user and performed actions such as starting and stopping both the development and production instance.

Stopping the production instance

When I tried to stop the production instance the error access denied occur and only the development instance can be stopped. This was because the policy is limited to development instance only, and thereby prohibiting actions on production instance.

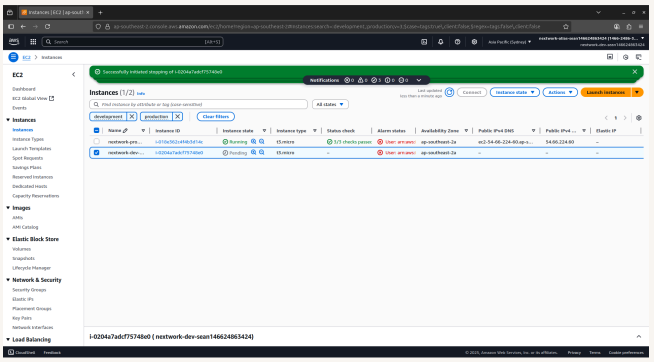


Sean Calderon
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, its successfully stopped. Since the policy is permitting such action.



The place to learn & showcase your skills

Check out nextwork.org for more projects