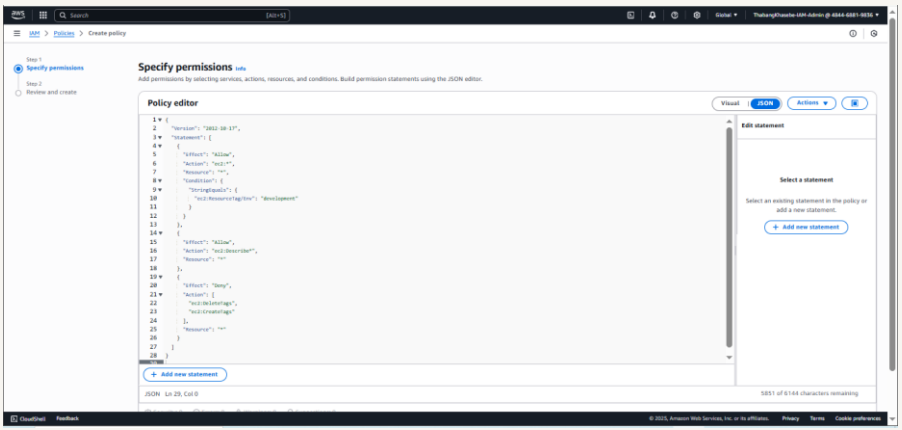
Cloud Security with AWS IAM

Thabang Khasebe



Thabang Khasebe

Introducing Today's Project!

In this project, I will demonstrate how to launch an EC2 instance and use IAM to manage access. I'm doing this to learn how AWS handles authentication, authorization, and secure resource management.

Tools and concepts

I used AWS EC2 to launch servers and IAM to manage user access. I learned how to create IAM policies, user groups, and users, control permissions with tags, and securely restrict access to resources like development and production instances.

Project reflection

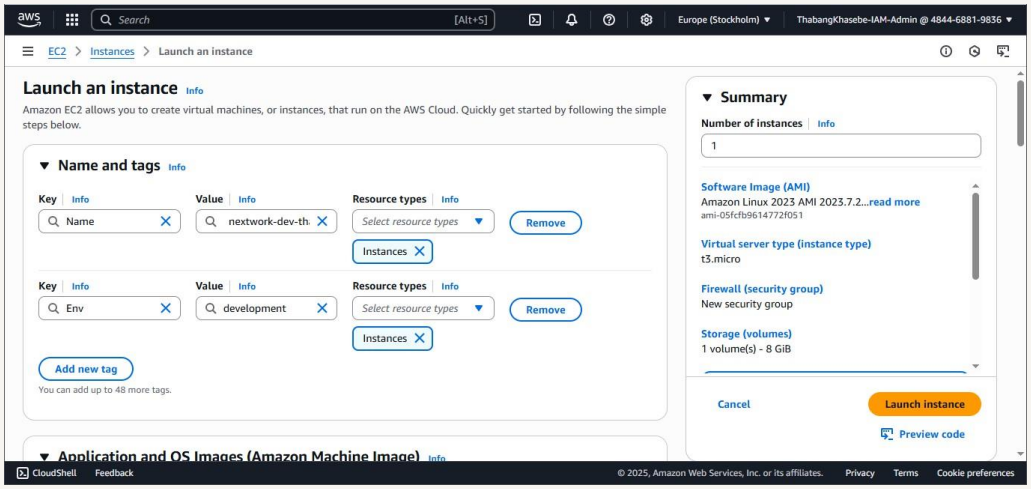
This project took me approximately 2 hours. The most challenging part was setting precise IAM policies to restrict access correctly. It was most rewarding to see the intern securely access only the development instance without affecting production.

Thabang Khasebe

Tags

Tags are key-value pairs that you can assign to AWS resources. They are useful for organizing, identifying, and managing resources by grouping them based on purpose, owner, environment (e.g., dev, test, prod), or department.

The tag I've used on my EC2 instances is called Env. The values I've assigned are production for nextwork-prod-thabangkhasebe and development for nextwork-dev-thabangkhasebe.



Thabang Khasebe

IAM Policies

IAM Policies are documents that define permissions for AWS users, groups, or roles. They specify what actions are allowed or denied on which AWS resources, helping control and secure access within an AWS account.

The policy I set up

For this project, I've set up a policy using JSON to have more precise control over the permissions granted to the intern.

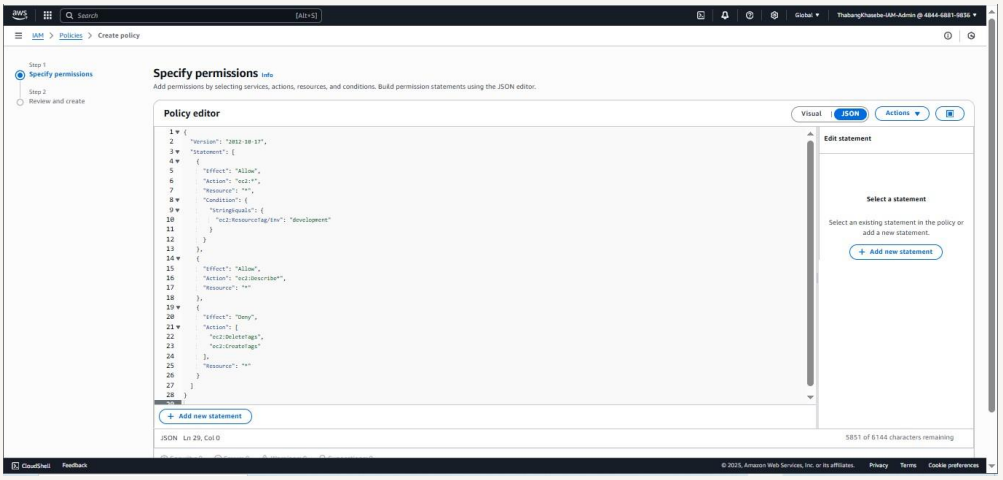
I've created a policy that allows the intern to start, stop, and describe EC2 instances tagged with "Env = development," while denying them permission to create or delete tags on any instances.

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

The Effect, Action, and Resource attributes of a JSON policy mean: Effect decides allow or deny, Action lists what operations are allowed or denied, and Resource specifies which AWS resources the policy applies to.

Thabang Khasebe

My JSON Policy

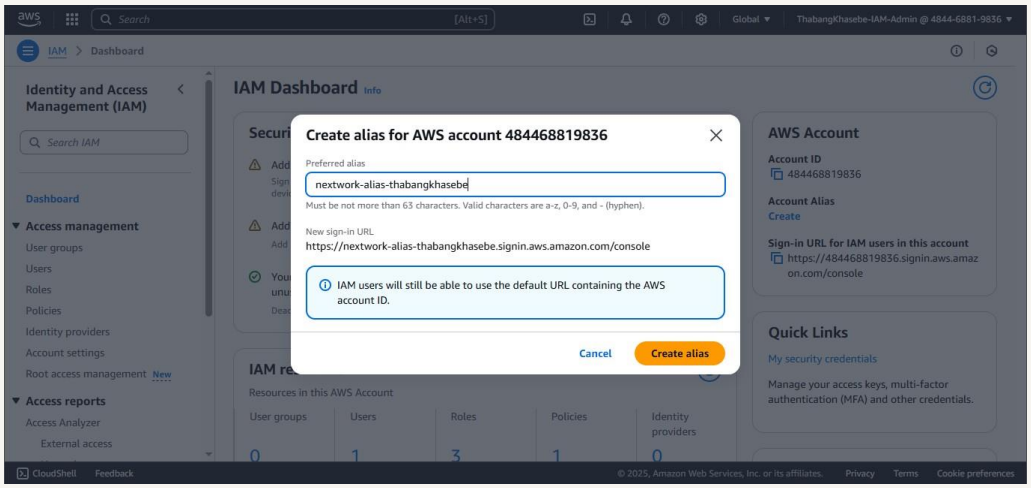


Thabang Khasebe

Account Alias

An account alias is a custom name that replaces the default AWS account ID in the login URL, making it easier to remember and use when signing in to the AWS Management Console.

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



Thabang Khasebe

IAM Users and User Groups

Users

IAM users are individual identities within an AWS account that represent people or applications. Each user has unique credentials and permissions to securely access AWS resources according to assigned policies.

User Groups

IAM user groups are collections of IAM users that share the same permissions. They make it easier to manage access by allowing you to assign policies to the group instead of configuring each user individually.

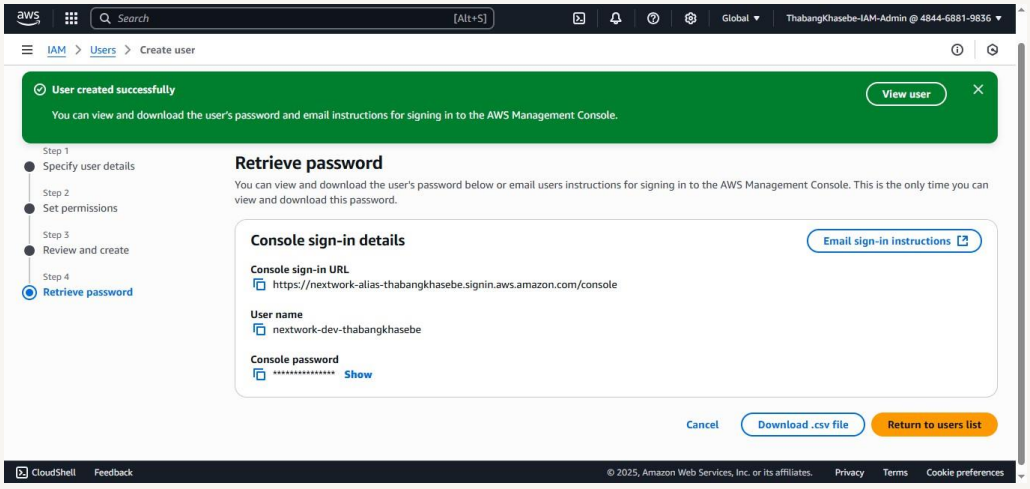
I attached the policy I created to this user group, which means all users in the group, including the intern,will have permission to access only the development EC2 instance while being restricted from modifying tags or accessing production resources

Thabang Khasebe

Logging in as an IAM User

The first way is to share the AWS login URL with the username and temporary password for console access. The second way is to provide access keys for programmatic access via the AWS CLI or APIs.

Once I logged in as my IAM user, I noticed some dashboard panels showed "Access denied." This was because my permissions are restricted to only the development EC2 instance, preventing access to production and other resources.



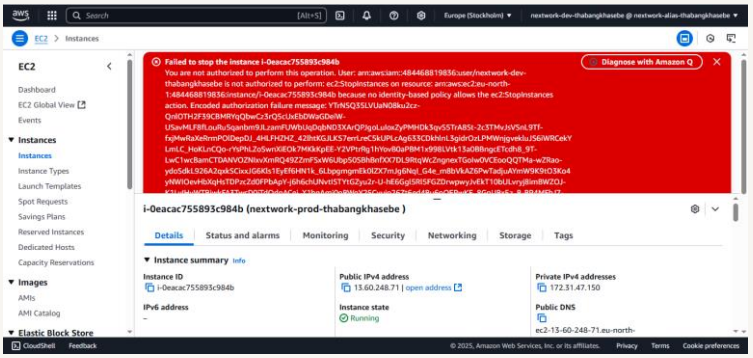
Thabang Khasebe

Testing IAM Policies

I tested my JSON IAM policy by trying to stop both EC2 instances. I was denied permission when stopping the production instance but was able to successfully stop the development instance.

Stopping the production instance

When I tried to stop the production instance, I received an error message saying I was not authorized to perform this action. This was because my IAM policy restricts access to production instances to prevent accidental changes.



Thabang Khasebe

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, the action succeeded without any errors. This was because my IAM policy grants me permission to manage instances tagged with "Env = development."