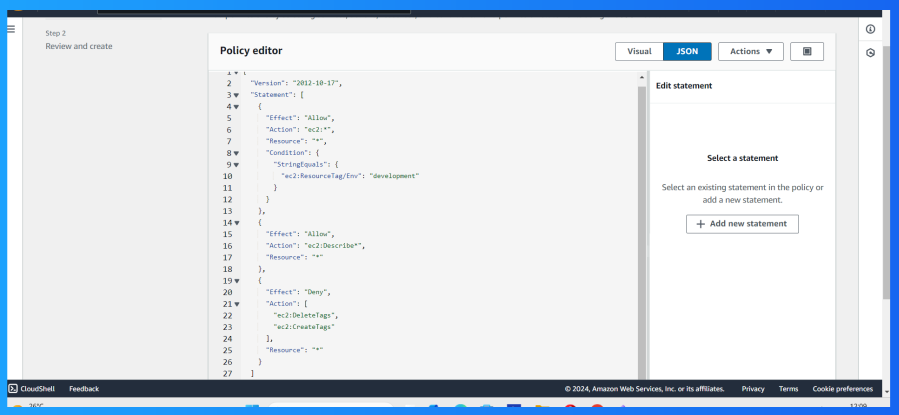
NextWork.org

Cloud Security with AWS IAM

Dora Klobučar



D
Dora Klobučar
NextWork Student

Introducing today's project!

What is AWS IAM?

AWS Identity and Access Management (IAM) is a service that helps you securely control access to AWS services and resources. With IAM, you can manage who is authenticated (signed in) and authorized (has permissions) to use resources in your AWS accoun

How I'm using AWS IAM in this project

For creating users and groups

One thing I didn't expect...

Having so much fun

This project took me...

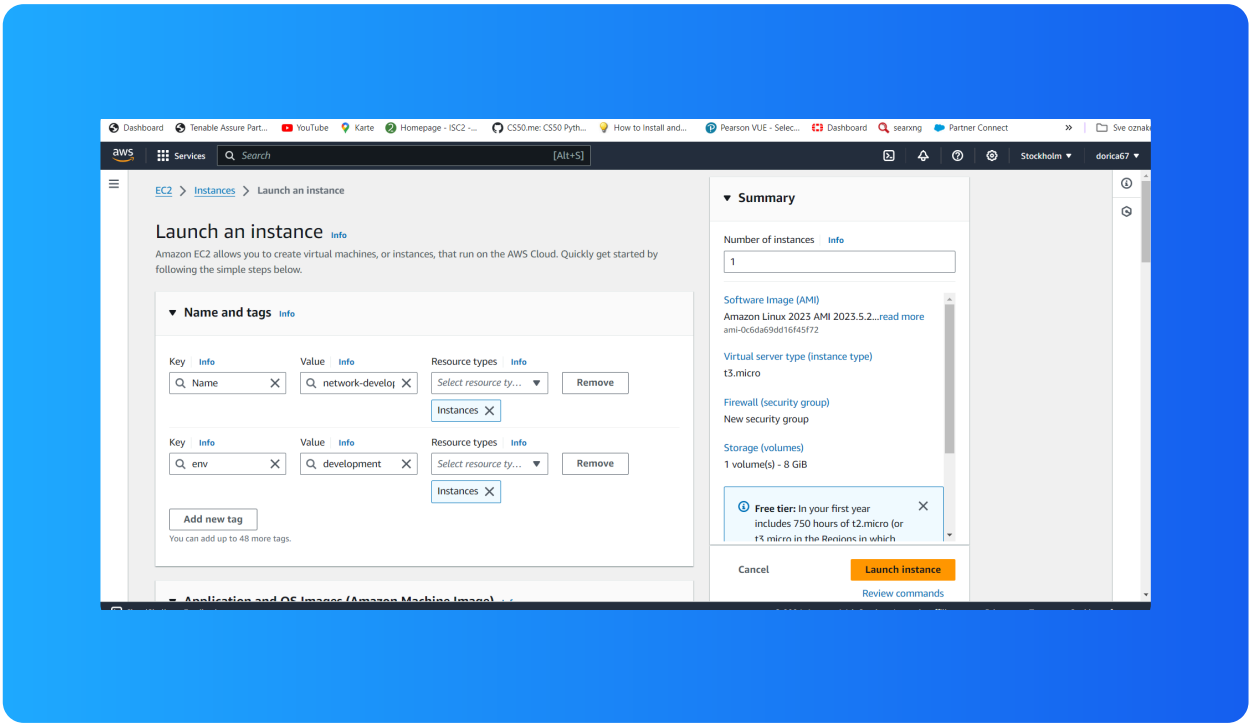
1 h

Dora Klobučar
NextWork Student

Tags

Tags are labels to help AWS Account users to manage and identify resources. Tags are useful for mass managemnet and applying security policies.

The tag I used on my EC2 instance is called Env. The value I assigned for my instances are development and production. This represents the two different environments that we are using to build and release the NextWork app.



D
Dora Klobučar
NextWork Student

IAM Policies

IAM Policies are rules that help to allow/deny user resources and premission to perform certain actions to my AWS Accounts resources.

The policy I set up

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

I've created a policy that allows all EC2 related actions to all EC2 instances that have the Environment ("Env") tag "development". But it also denies creating and deleting tags for all EC2 instances.

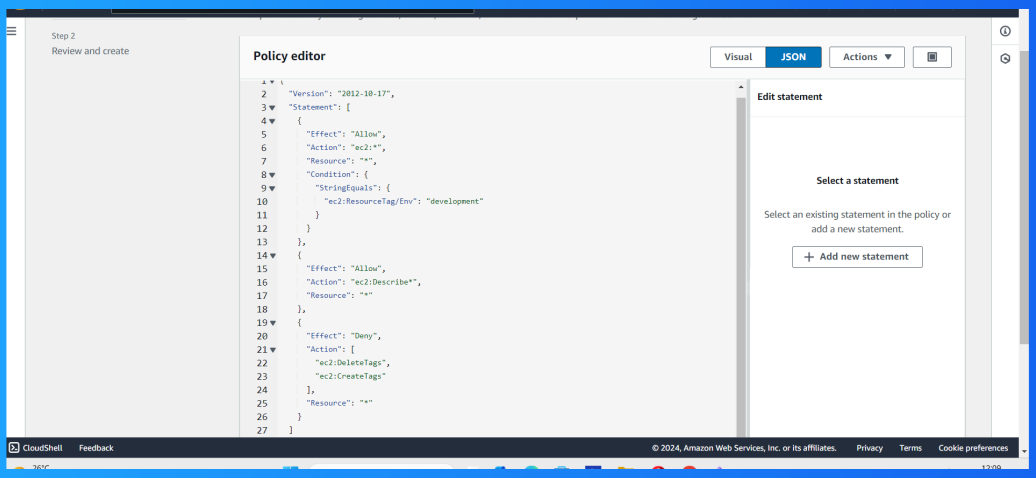
When creating a JSON policy, you have to define its Effect, Action and Resource.

When wiritng JSON policy statements, you have to write: -Effect: ie. Allow or deny - Action: the specific action that we are wanting to allow or deny - Resource: the specific resource/group of resources in my AWS account

D

Dora Klobučar
NextWork Student

My JSON Policy



D

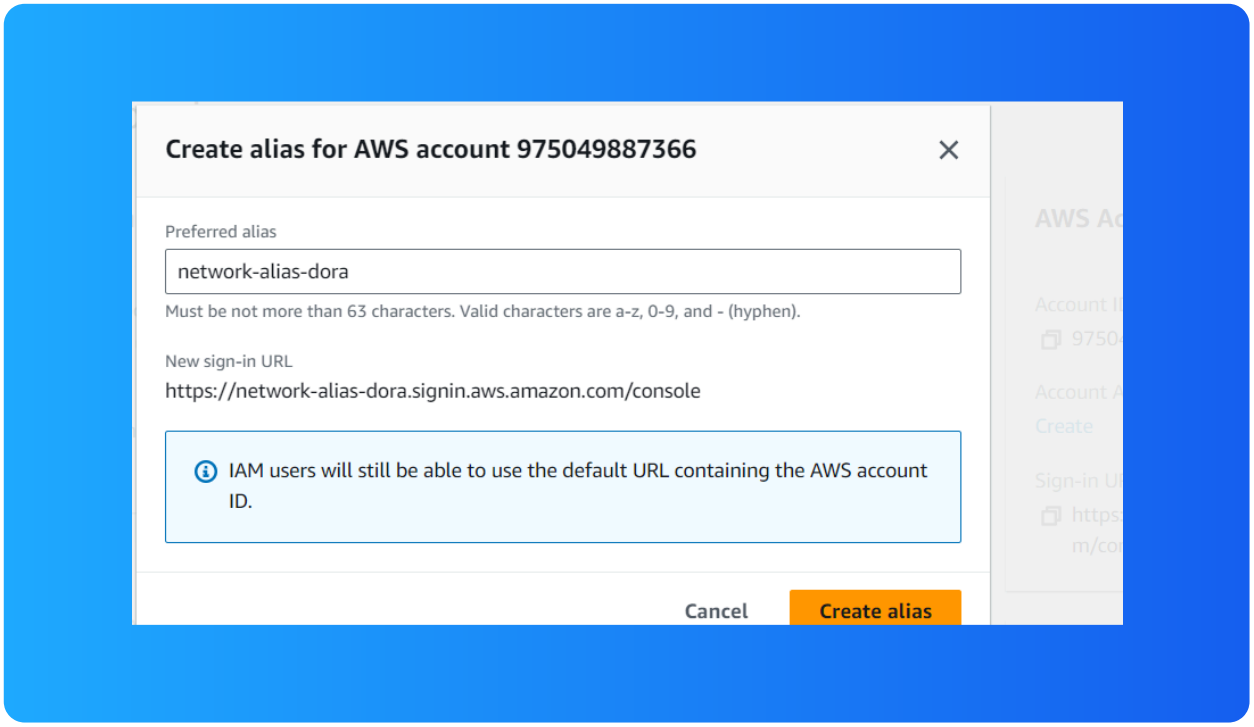
Dora Klobučar
NextWork Student

Account Alias

An account alias is a custom name that I can assign to my AWS account. This custom name would replace my Account ID, in my account's log-in URL.

Creating an account alias took me less then a minute-super fast!

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



D
Dora Klobučar
NextWork Student

IAM Users and User Groups

Users

IAM user are other logins/people who have access to my AWS account. These users are created by myself using AWS IAM service. I can designate my IAM users access to my AWS account resources/services.

User Groups

User groups are used for managing and grouping user's premissions at group level. They act similary to folders when it comes to assigning premission/policies at mass level.

I attached the policy I created to this user group, which means which means all users that are added to that user group wil automatically inherit the user's group access premissions.

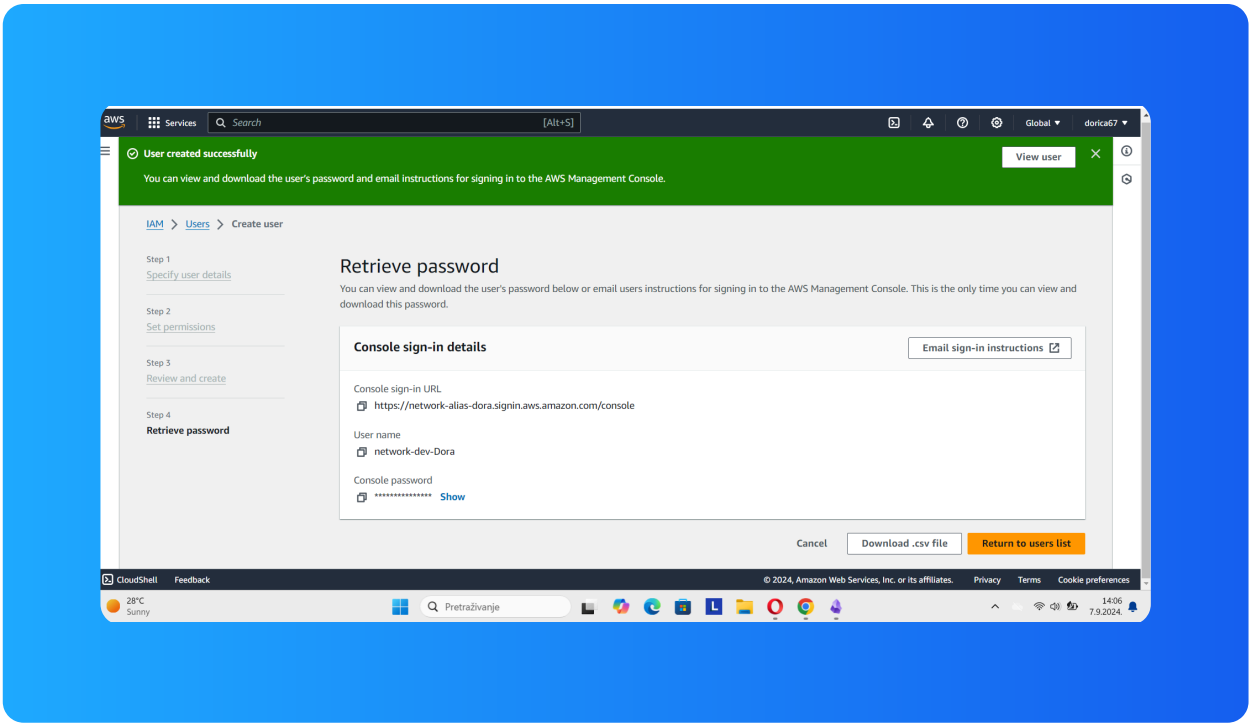
D

Dora Klobučar
NextWork Student

Logging in as an IAM User

The first way is emailing sign-in instructions and other way is downloading .csv file

Once I logged in as my IAM user, I noticed that a lot of panels displayed "Acess denied". That was a clear difference that I usually see in my AWS account (where I had unlimited access to resources and wasn't denied access to anything)



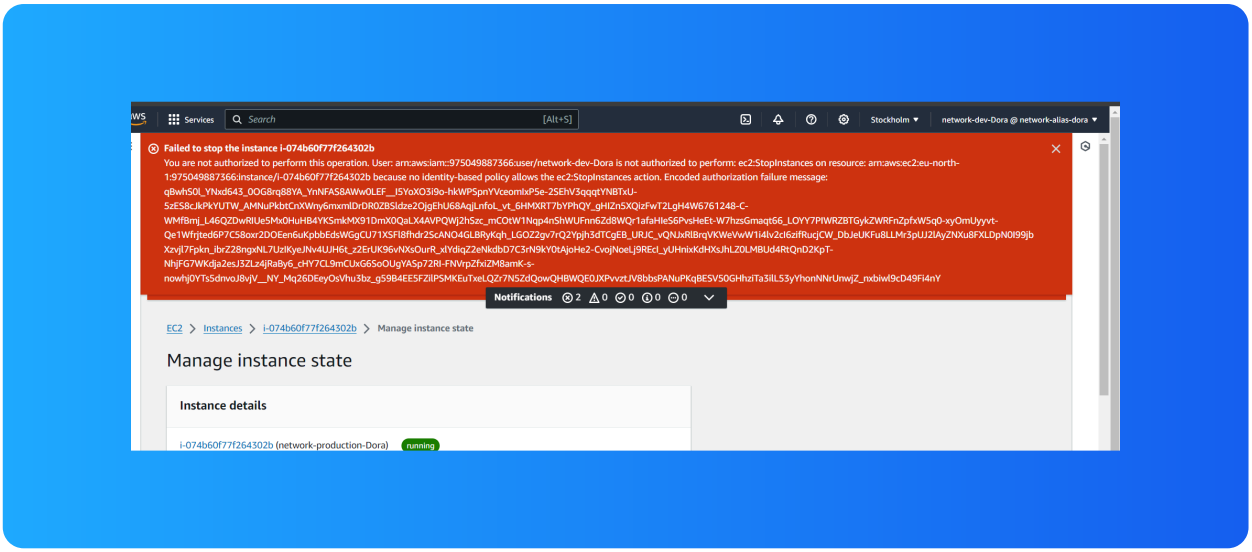
Dora Klobučar
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by trying to stop production and development instances, ie triggering StopInstaces action.

Stopping the production instance

When I tried to stop the production instance an error message stopped me and explained I am not authorized to stop the production instance.



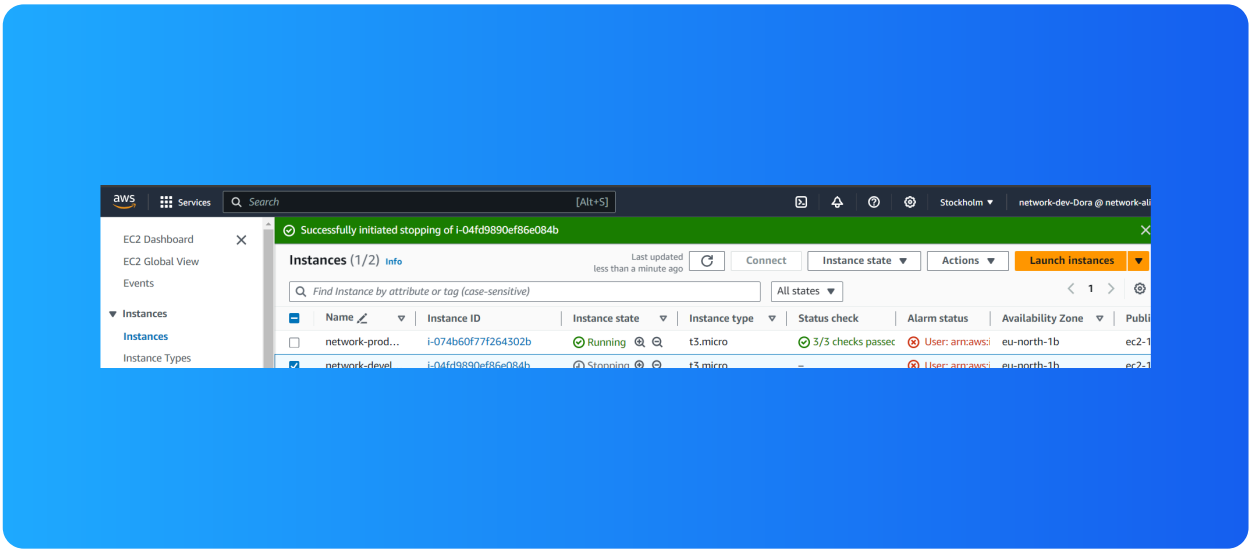
D

Dora Klobučar
NextWork Student

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance the development instance could be stopped. This was beacuse polivy I created(and attached to User Group that my User is part of) allowed all EC2 related actions to all EC2 instances/resources with



Everyone should be in a job they love.

Check out nextwork.org for more projects