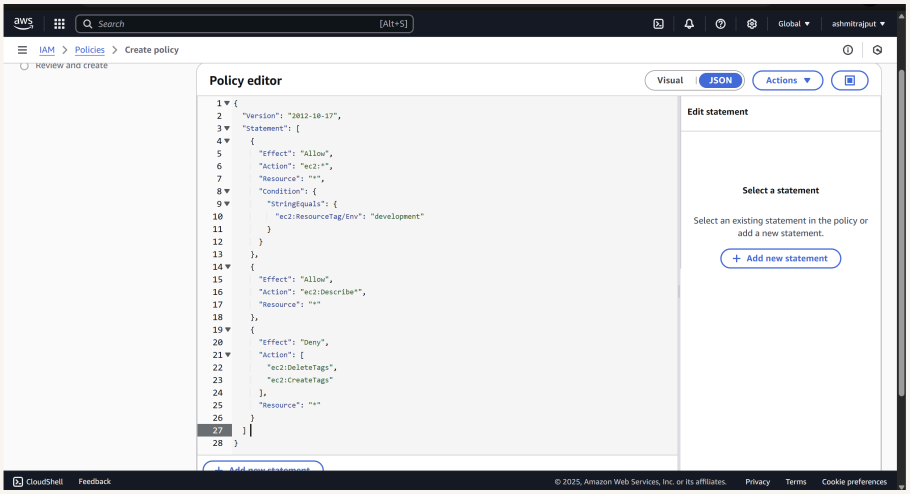
nextwork.org

Cloud Security with AWS IAM

A Ashmit Rajput



Introducing Today's Project!

In this project, I will demonstrate how to create EC2 instances, IAM groups and policies to access those EC2 Instances. I'm doing this project to learn more about creating EC2 Instances and working with IAM policies for security and accessibility.

Tools and concepts

Services I used were EC2, IAM. Key concepts I learnt include how to setup EC2 instances, name tags for resources, writing policy for users, creating user groups in IAM, creating users and adding them to the group, signing in using an Alias or user.

Project reflection

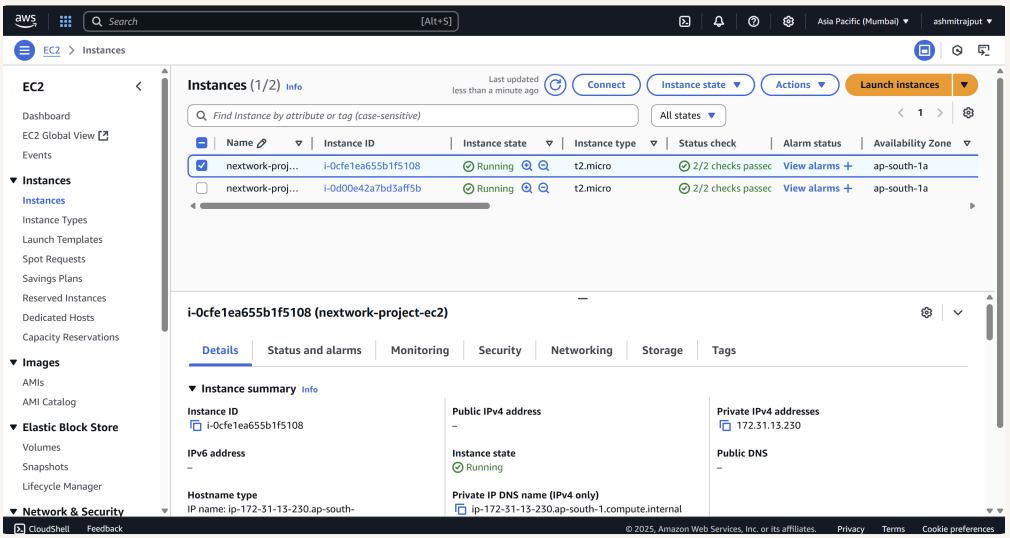
This project took me approximately 1.5 hours to complete & learn about all the concepts, while learning about new concepts and implementing them in the AWS console I realized most challenging was to explore AWS, Subnets, EC2 in depth on my own.

Ashmit Rajput
NextWork Student

Tags

Tags are additional information we add to our resources which makes them easier to classify and filter when we search for them. Tags can help label our resources or services into different categories or environments, and make it more organized.

The tag I've used on my EC2 instances is called "env", short for environment as i wanted to classify the instances on the basis of their phase of development. The value I've assigned for my instances are "Production" and "Development".



IAM Policies

IAM Policies are basically a script in JSON that defines what kind of access we give different users, roles or groups to different resources. It lays out different features of a resource and the effect we want on it i.e. Allow or deny, for any user.

The policy I set up

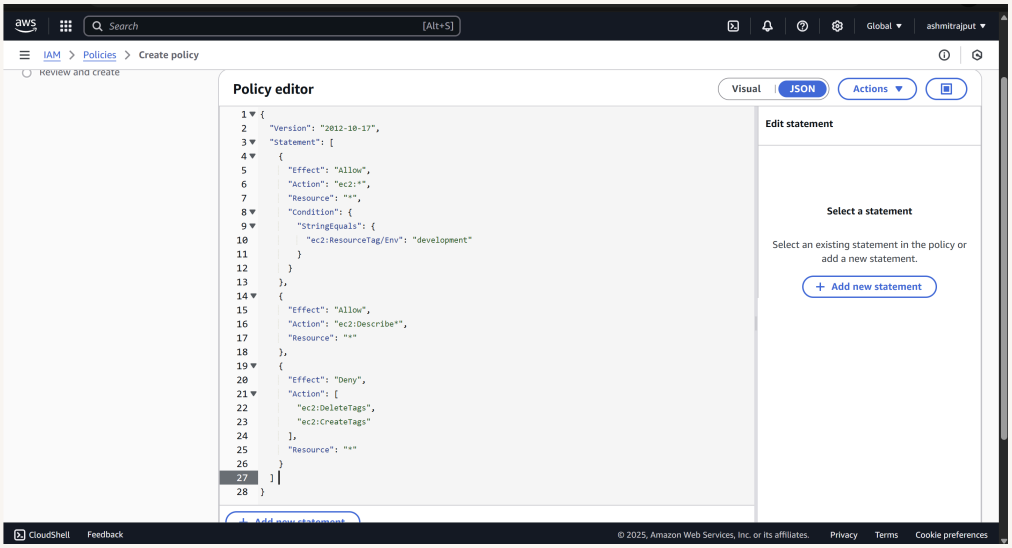
For this project, I've set up a policy using JSON, where I specified the rules for accessing different EC2 instances that I created for a user, in this case say an Intern, where He/She is only allowed to access EC2 of Development Environment.

I've created a policy that allows access to all the features of the EC2 instances that have Tag with name "env", value set as "Development". It also denies the user to create or delete tags over all resources, so user doesn't alter the tag values.

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 that whether this statement is going to Allow or Deny permissions to the user, Action describes all the functionalities user can access in the resource, here "*" means all.

My JSON Policy

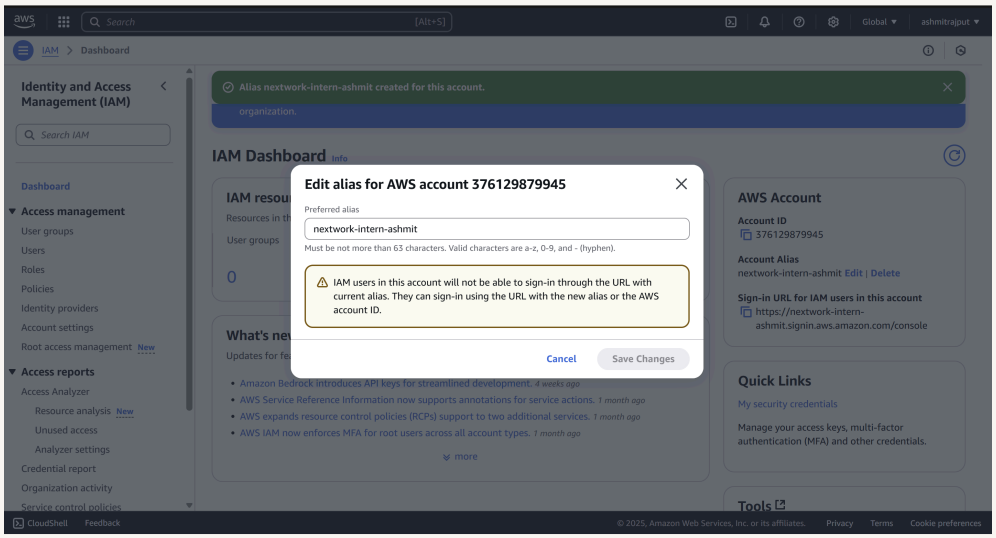


Ashmit Rajput
NextWork Student

Account Alias

An account alias is a way for multiple users to use the same AWS account by using different names and different login URL's generated for that alias specifically, it is helpful when a team has to work on specific resources together.

Creating an account alias took me literally two minutes as it is a very easy process and right on the dashboard on IAM service of AWS. Now, my new AWS console sign-in URL is https://nextwork-intern-ashmit.signin.aws.amazon.com/console.



IAM Users and User Groups

Users

IAM users are basically new branches to our account, here we get new sign-in information for every new user, by which new users can access the AWS account but with slightly different permissions which we can manage using groups and policies in IAM.

User Groups

IAM user groups are a collection/folder that contain several users with similar authority and require similar permissions/accessibility. So, we can club users ex. interns, in a group and grant them similar permissions and add new interns easily in it

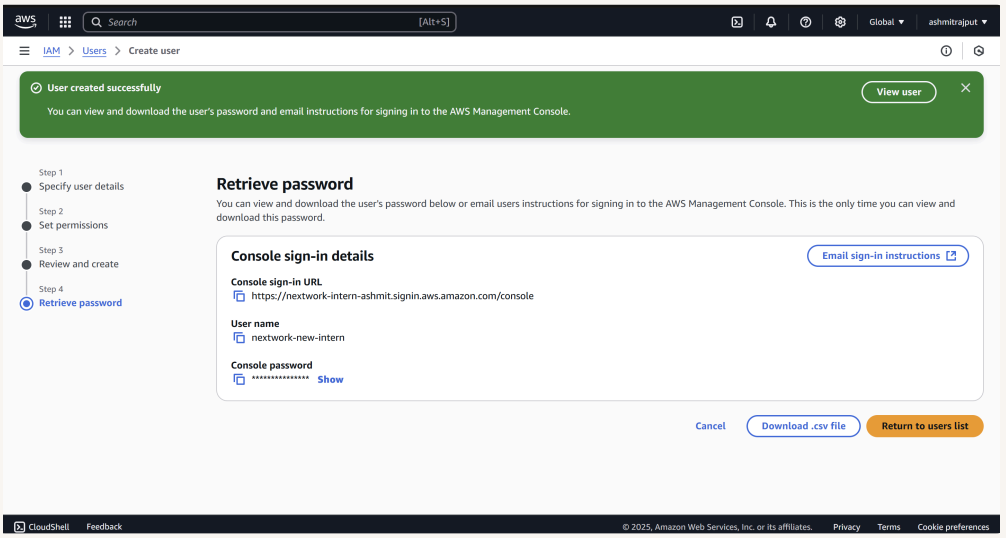
I attached the policy I created to this user group, which means that any user who is added to this group will have the permissions mentioned in the policy, same as other users, in this case, they won't have access to the EC2 instance in production.

Ashmit Rajput
NextWork Student

Logging in as an IAM User

The first way is by sharing a Console Sign-in URL, directly give access to the user without having to share a username and password. Second way is by sharing the username and password given by IAM to that specific user, passwords can be changed later

Once I logged in as my IAM user, I noticed that AWS treated me like a completely new user and started showing pop-ups related to settings and menu. This was because I came as an intern in the console, I also saw access denied in various services.



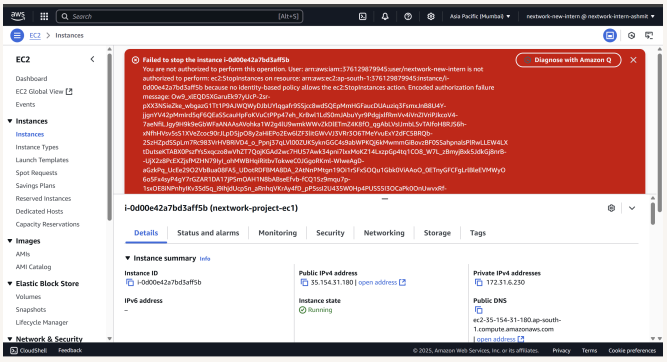
Ashmit Rajput
NextWork Student

Testing IAM Policies

I tested my JSON IAM policy by logging in as a user of the Inten-User-Group to which my policy was attached, and then tested it by trying to stop the production instance (which was clearly denied in the policy), and as expected I could not. Tested!

Stopping the production instance

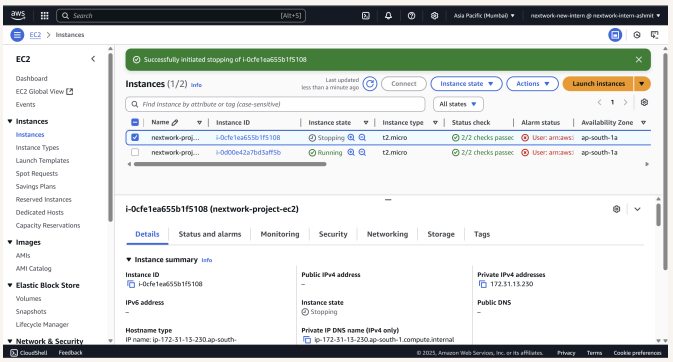
When I tried to stop the production EC2 instance, a red banner popped on my screen and alerted me that I (as an intern) am not authorized to stop this instance. This was because it was what we mentioned in the policy attached to the intern user group



Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance I could easily stop the instance and I was not denied by any policy as I had permission to all actions of development instance according to the JSON script. This was a clear test of the policy.



The place to learn & showcase your skills

Check out nextwork.org for more projects