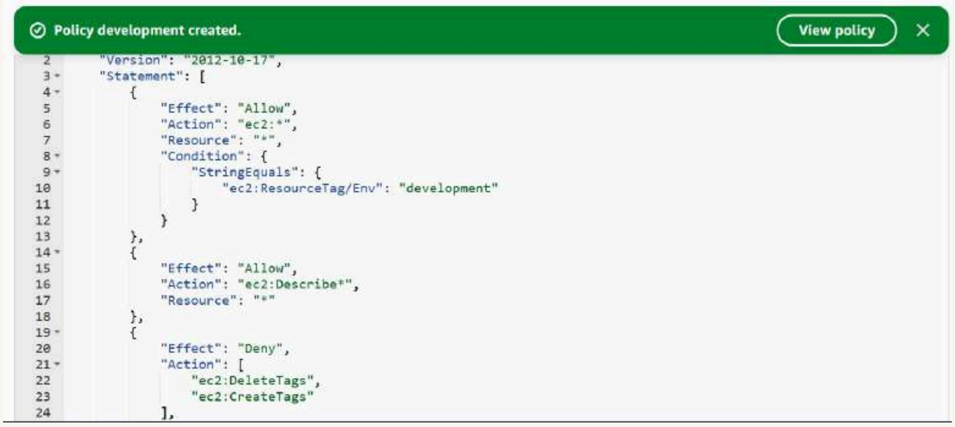
Cloud Security with AWS IAM

GA Mohamed Galole



Policy development created.

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Env": "development"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DeleteTags",
                "ec2:CreateTags"
            ],
```

Introducing Today's Project!

In this project, I will demonstrate EC2 instances, IAM Policies, IAM Users/User Groups, AWS Account Alias. I'm doing this project to learn how to use the AWS Identity and Access Management (IAM) service to control who is authenticated and authorized.

Tools and concepts

Services I used were IAM Policy, IAM groups, IAM Users Key concepts I learnt include testing IAM Policy how it affects users and permissions.

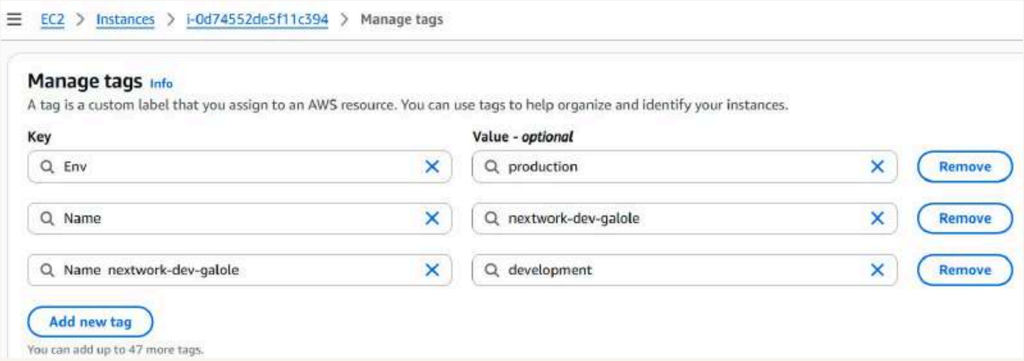
Project reflection

This project took me approximately one hour The most challenging part was getting errors when tried to stop production instance It was most rewarding to learn key skills of IAM Policy,Users and Groups.

Tags

Tags are short keywords or labels that describe the content, skills, or technologies related to a project.

The tag I’ve used on my EC2 instances is called prod The value I’ve assigned for my instances are production



Manage tags Info

A tag is a custom label that you assign to an AWS resource. You can use tags to help organize and identify your instances.

Key	Value - *optional*
Env	production
Name	nextwork-dev-galole
Name nextwork-dev-galole	development

You can add up to 47 more tags.

IAM Policies

IAM Policies are rules for who can do what with your AWS resources. It's all about giving permissions to IAM users, groups, or roles, saying what they can or can't do on certain resources.

The policy I set up

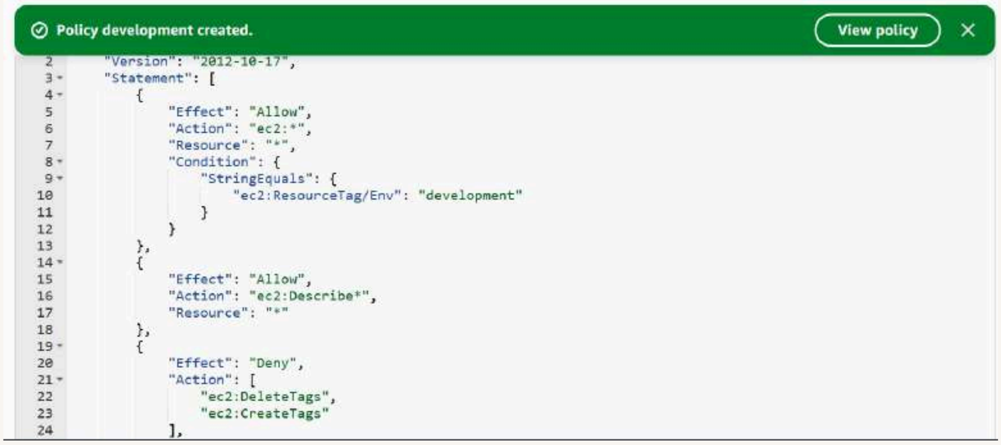
For this project, I’ve set up a policy using JSON

I’ve created a policy that follows tag-based access control (a best practice). It separates development vs production resources safely. It prevents privilege escalation via tag editing.

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 define what permissions are granted, to which AWS services/resources, and whether they’re allowed or denied.

My JSON Policy

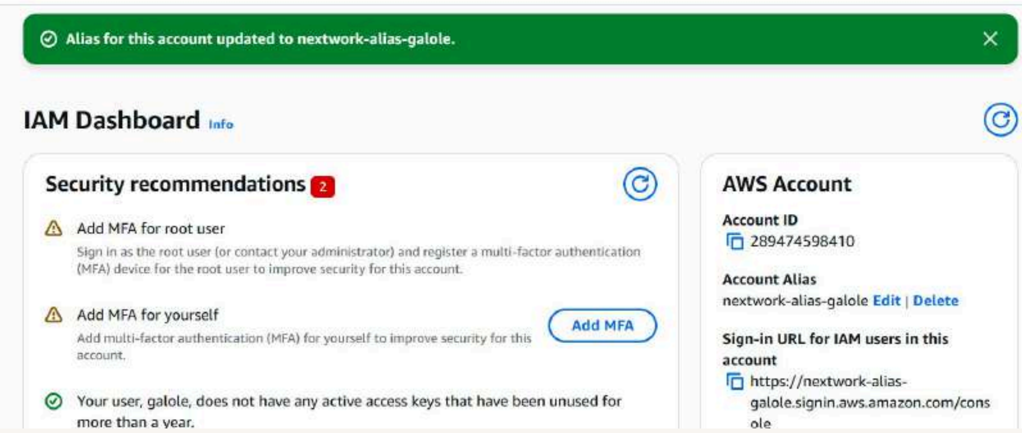


```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Env": "development"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DeleteTags",
                "ec2:CreateTags"
            ],
```

Account Alias

An Account Alias is simply a custom name that you assign to your AWS account to make your sign-in URL easier to remember and share.

Creating an account alias took me one minute Now, my new AWS console sign-in URL is https://nextwork-alias-galole.signin.aws.amazon.com/console



Alias for this account updated to nextwork-alias-galole.

IAM Dashboard Info

Security recommendations 2

Add MFA for root user

Sign in as the root user (or contact your administrator) and register a multi-factor authentication (MFA) device for the root user to improve security for this account.

Add MFA for yourself

Add multi-factor authentication (MFA) for yourself to improve security for this account.

Your user, galole, does not have any active access keys that have been unused for more than a year.

AWS Account

Account ID
289474598410

Account Alias
nextwork-alias-galole Edit | Delete

Sign-in URL for IAM users in this account
https://nextwork-alias-galole.signin.aws.amazon.com/console

IAM Users and User Groups

Users

IAM users represents an individual person or application that needs access to your AWS account.

User Groups

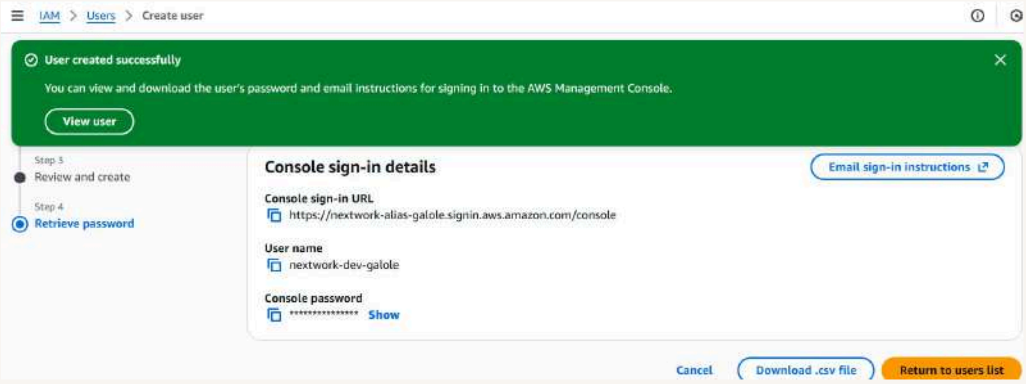
IAM user groups in AWS are a collection of IAM users that share the same set of permissions.

I attached the policy I created to this user group, which means every user inside that group automatically inherits all the permissions defined in that policy.

Logging in as an IAM User

The first way is Share the Console Sign-In URL and Password second one is Share Access Keys (for Programmatic Access)

Once I logged in as my IAM user, I noticed some errors This was because least priviledge.



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Console sign-in details

Console sign-in URL
https://nextwork-alias-galole.signin.aws.amazon.com/console

User name
nextwork-dev-galole

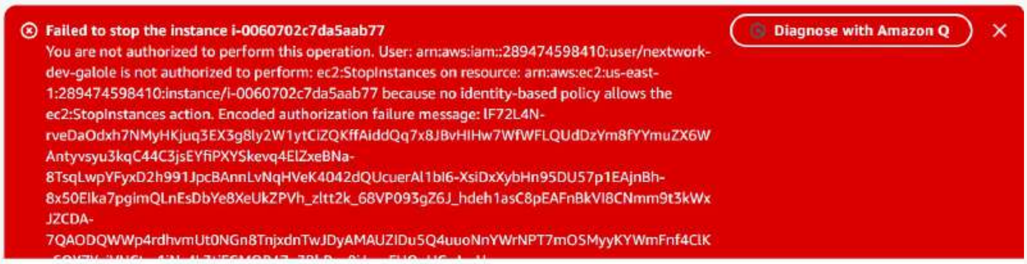
Console password
*************** Show

Testing IAM Policies

I tested my JSON IAM policy by trying to stop the instance using the dev new user and got denied.

Stopping the production instance

When I tried to stop the production instance You are not authorized to perform this operation, Access Denied This was because limited Access.



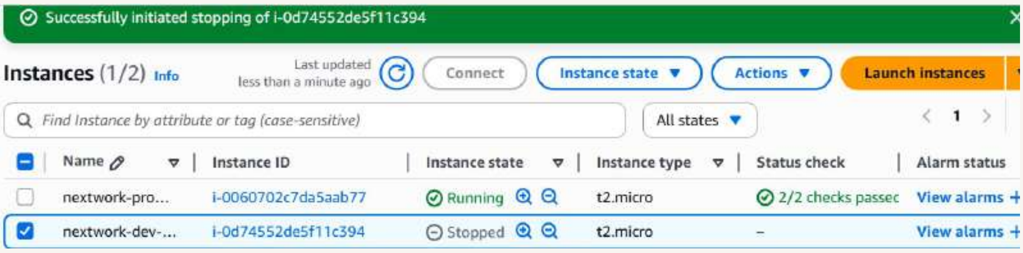
Failed to stop the instance i-0060702c7da5aab77

```
You are not authorized to perform this operation. User: arn:aws:iam::289474598410:user/nextwork-
dev-galole is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-
1:289474598410:instance/i-0060702c7da5aab77 because no identity-based policy allows the
ec2:StopInstances action. Encoded authorization failure message: lF72L4N-
rveDaOdxh7NMyHKjuq3EX3g8ly2W1ytCiZQKffAiddQq7x8JBvHIHw7WfWFLQUdDzYm8fYYmuZX6W
Antyvsyu3kqC44C3jsEYfiPXYSkevq4ElZxeBNa-
8TsqLwpYFyxD2h991JpcBAnnLvNqHVeK4042dQUcuerAl1bl6-XsiDxXybHn95DU57p1EAjnBh-
8x50Elka7pgimQLnEsDbYe8XeUkZPVh_zltt2k_68VP093gZ6J_hdeh1asC8pEAFnBkVI8CNmm9t3kWx
JZCDA-
7QAODQWWp4rdhvmUt0NGn8TnjxdnTwJDyAMAUZIDu5Q4uuoNnYWrNPT7mOSMyyKYWmFnf4ClK
```

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance got denied This was because of the policy atteched to the user.



Successfully initiated stopping of i-0d74552de5f11c394

Instances (1/2) Info

Last updated less than a minute ago

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☐	nextwork-pro...	i-0060702c7da5aab77	Running	t2.micro	2/2 checks passec	View alarms +
☑	nextwork-dev-...	i-0d74552de5f11c394	Stopped	t2.micro	–	View alarms +

The place to learn & showcase your skills

Check out nextwork.org for more projects