



Cloud Security with AWS IAM



Ivan Delgadillo Fernandez

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor Visual **JSON** Actions ▾

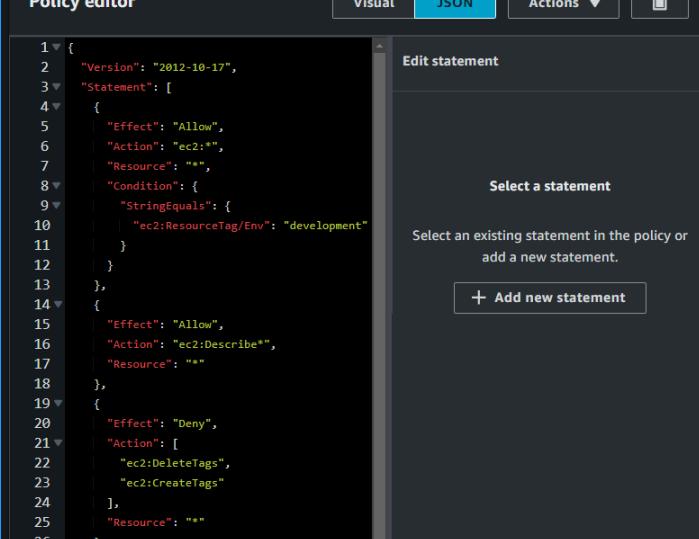
1 `{`
2 `"Version": "2012-10-17",`
3 `"Statement": [`
4 `{`
5 `"Effect": "Allow",`
6 `"Action": "ec2:*`
7 `"Resource": "",`
8 `"Condition": {`
9 `"StringEquals": {`
10 `"ec2:ResourceTag/Env": "development"`
11 `}`
12 `},`
13 `{`
14 `"Effect": "Allow",`
15 `"Action": "ec2:Describe*",`
16 `"Resource": "*"`
17 `},`
18 `{`
19 `"Effect": "Deny",`
20 `"Action": [`
21 `"ec2:DeleteTags",`
22 `"ec2:CreateTags"`
23 `],`
24 `"Resource": "*"`
25 `}`
26 `,`
27 `]`

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement





Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

Introducing today's project!

What is AWS IAM?

AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS resources

How I'm using AWS IAM in this project

I've created a policy to access two environments.

One thing I didn't expect...

I didn't expect use a policy editor

This project took me...

60 minutes



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

Tags

Tags are like labels you can attach to AWS resources for organization.

The tag I've used on my EC2 instances is called "Env" the value I've assigned for my instances are "production and development"

Request to manage tags has succeeded.					
Instances (2) Info		Last updated 2 minutes ago	C	Connect	Instance state ▾
<input type="text"/> Find Instance by attribute or tag (case-sensitive)				All states ▾	
<input type="checkbox"/>	Name 🔗	Instance ID	Instance state ▾	Instance type ▾	
<input type="checkbox"/>	DevelopmentEC2-IvanDelgadillo	i-0e98915dd33d502e9	Running Q Q	t2.micro	
<input type="checkbox"/>	ProductionEC2-IvanDelgadillo	i-0aef40e60bb90fb8d	Running Q Q	t2.micro	



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

IAM Policies

IAM stands for Identity and Access Management. You'll use AWS IAM to manage the access level that other users and services have to your 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 some actions (like starting, stopping, and describing EC2 instances) for instances tagged with "Env = development" while denying the ability to create or delete tags for all 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 means to indicate whether the policy allows or denies a certain action



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

My JSON Policy

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual **JSON** Actions ▾

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": "ec2:*",  
7       "Resource": "*",  
8       "Condition": {  
9         "StringEquals": {  
10            "ec2:ResourceTag/Env": "development"  
11          }  
12        }  
13      },  
14      {  
15       "Effect": "Allow",  
16       "Action": "ec2:Describe*",  
17       "Resource": "*"  
18     },  
19     {  
20       "Effect": "Deny",  
21       "Action": [  
22         "ec2:DeleteTags",  
23         "ec2>CreateTags"  
24       ],  
25       "Resource": "*"  
26     }  
27   ]  
}
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement



Ivan Delgadillo Fernandez

NextWork Student

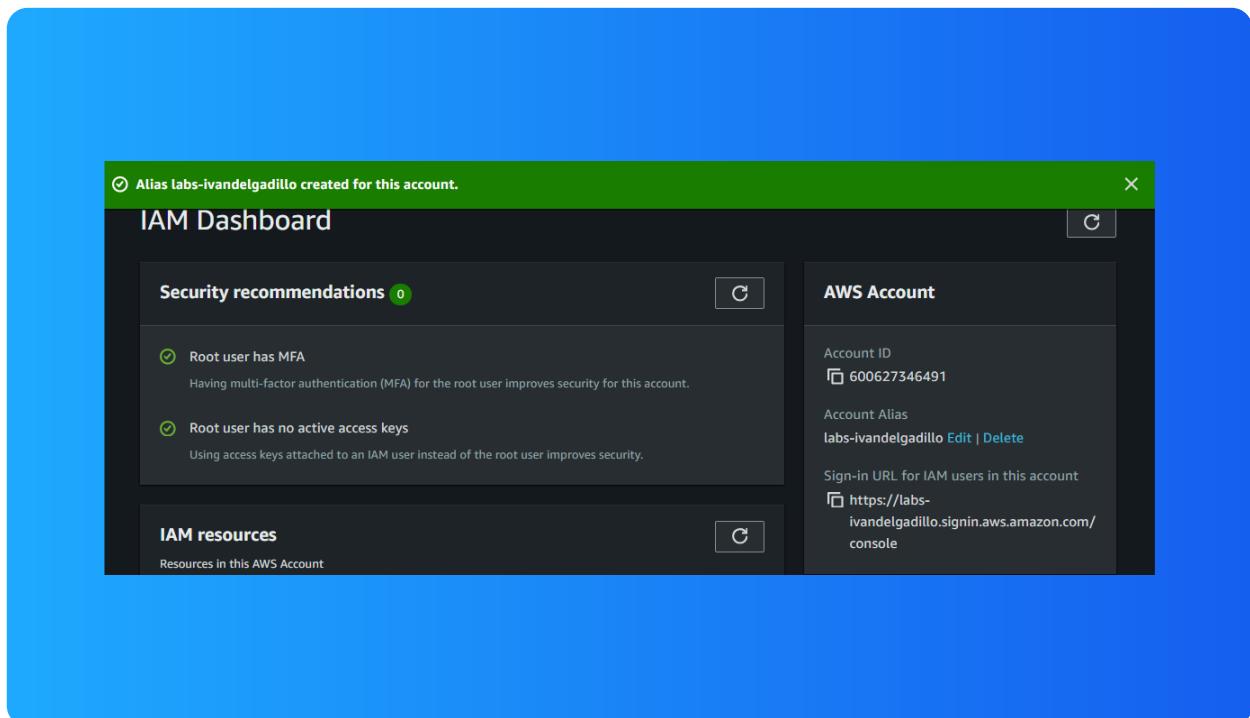
NextWork.org

Account Alias

An Account Alias is a friendly name for your AWS account that you can use instead of your account ID (which is usually a bunch of digits) to sign in to the AWS Management Console.

Creating an account alias took me 2 minutes

Now, my new AWS console sign-in URL is [labs-ivandelgadillo](https://labs-ivandelgadillo.signin.aws.amazon.com/console)





Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

IAM Users and User Groups

Users

A user is an entity that you create in AWS.

User Groups

An IAM user group is a collection/folder of IAM users.

I attached the policy I created to this user group, which means the user has access to resources on AWS.



Ivan Delgadillo Fernandez

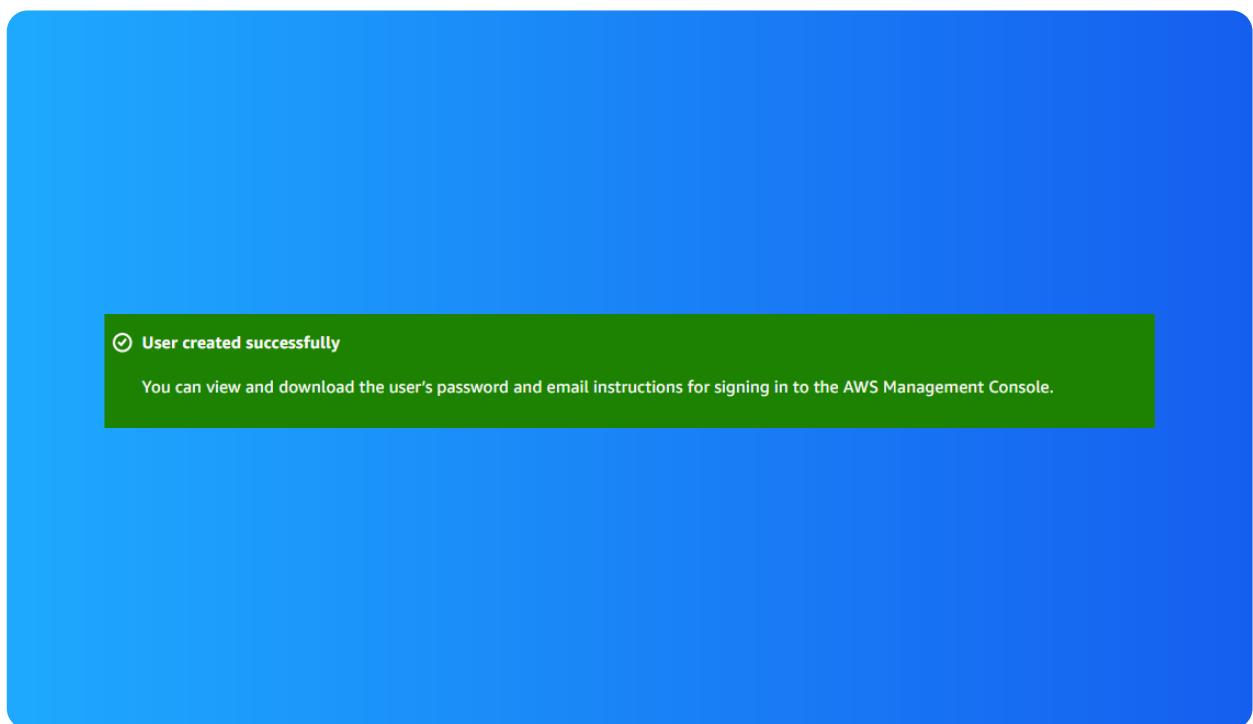
NextWork Student

NextWork.org

Logging in as an IAM User

The first way is specify with Identity Center and second way is create user and password.

Once I logged in as my IAM user, I noticed that I can't access different sections





Ivan Delgadillo Fernandez

NextWork Student

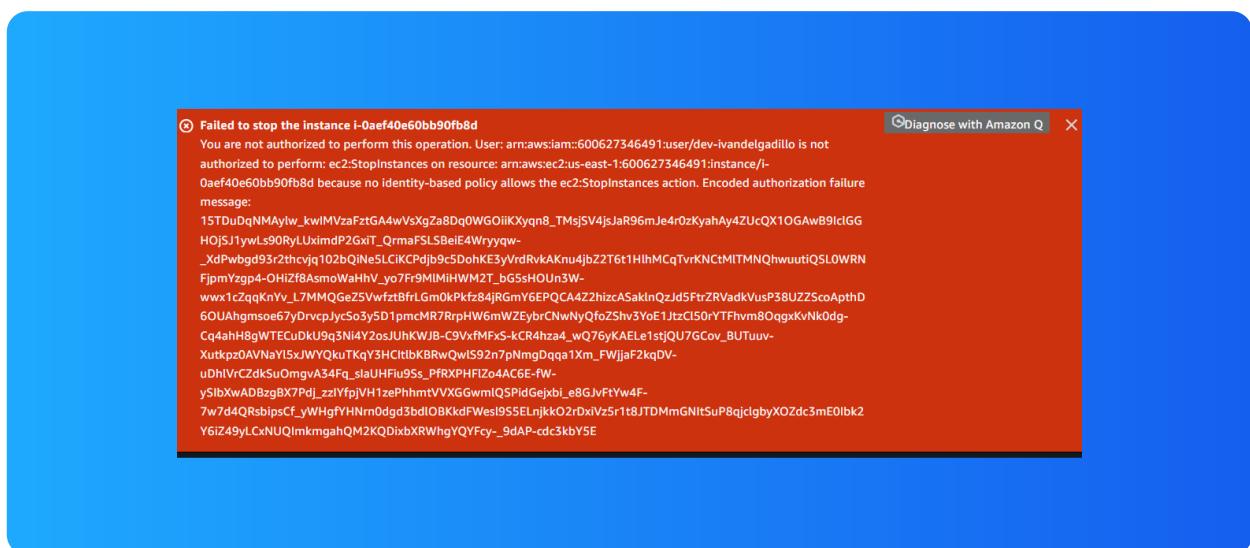
NextWork.org

Testing IAM Policies

I tested my JSON IAM policy by stop production instance and development instance

Stopping the production instance

When I tried to stop the production instance, show the error message





Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, the show message has Successfully

The screenshot shows the AWS EC2 Instances page. At the top, a green banner displays the message: "Successfully initiated stopping of i-0e98915dd33d502e9". Below the banner, the heading "Instances (1/2) Info" is visible. A toolbar includes "C" (Create), "Connect", "Instance state ▾", "Actions ▾", "Launch instances", and a dropdown menu. A search bar says "Find Instance by attribute or tag (case-sensitive)" and a filter says "All states ▾". The main table lists two instances:

Name	Instance ID	Instance state	Instance type
DevelopmentEC2-IvanDelgadillo	i-0e98915dd33d502e9	Stopping	t2.micro
ProductionEC2-IvanDelgadillo	i-0aef40e60bb90fb8d	Running	t2.micro



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

