



NextWork.org

Cloud Security with AWS IAM



mmoorej24@gmail.com

Policy editor

```
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 | ]
28 | ]
    ^
    |
    + Add new statement
JSON Ln 28, Col 1
```



mmoorejr24@gmail.com
NextWork Student

NextWork.org

Introducing today's project!

What is AWS IAM?

AWS Identity and Access Management (IAM), is a service you can specify who or what can access services and resources in AWS, centrally manage fine-grained permissions, and analyze access to refine permissions across AWS.

How I'm using AWS IAM in this project

I used it to create a new user with specific permissions to demonstrate user and access management.

One thing I didn't expect...

I didn't expect the process to be this straight forward. Although I would like to experiment on the level of granular control that you can grant to a user group.

This project took me...

This project took me an hour and ten minutes to complete.



mmoorejr24@gmail.com
NextWork Student

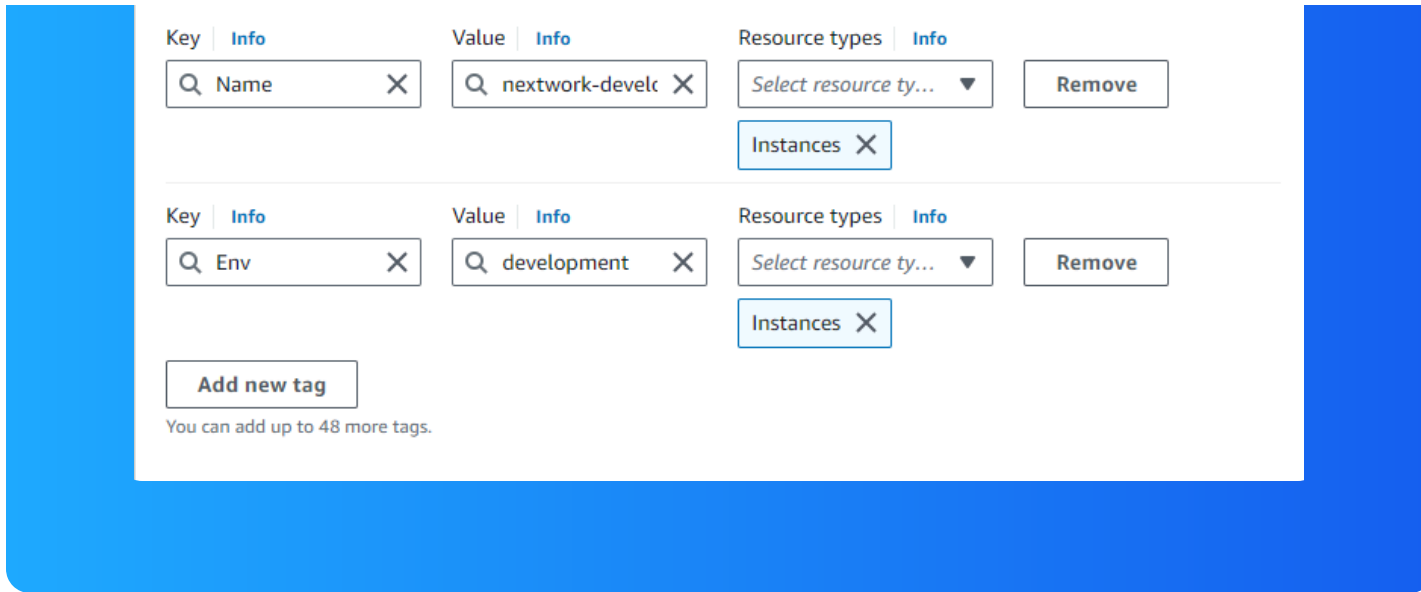
NextWork.org

Tags

Tags are labels to help AWS Account users identify and manage their resources. Tags are useful for grouping, mass management, and applying security policies.

The tag I've used on my EC2 instances is called Env. The values I've assigned for my instances are production, and development. This represents the two different environments that are used to build and release the Nextwork app.

▼ Name and tags [Info](#)



Key | Info Value | Info Resource types | Info

Q Name X Q nextwork-develc X Select resource ty... Remove

Instances X

Key | Info Value | Info Resource types | Info

Q Env X Q development X Select resource ty... Remove

Instances X

Add new tag

You can add up to 48 more tags.



mmoorej24@gmail.com

NextWork Student

NextWork.org

IAM Policies

IAM Policies are rules that help to allow/deny users or resources permissions to perform certain actions to my AWS Account's resources.

The policy I set up

For this project, I've set up a policy using the 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, also denies creating and deleting tags for All EC2 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: * Effect: i.e. Allow or Deny. * Action: i.e. the specific action that we are wanting to allow or deny. * Resource: specific resources in my AWS Account that policies be effected on.



mmoorej24@gmail.com
NextWork Student

NextWork.org

My JSON Policy

Policy editor

```
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 ]
28 ]
29 ]
```

[+ Add new statement](#)

JSON Ln 28, Col 1



mmoorej24@gmail.com

NextWork Student

NextWork.org

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 than a minute - hooray! Super fast!

Now, my new AWS console sign-in URL is <https://nextwork-alias-mitchell.signin.aws.amazon.com/console>

Create alias for AWS account 088535984191



mmoorejr24@gmail.com

NextWork Student

NextWork.org

IAM Users and User Groups

Users

IAM users are other log-ins people who have access to my AWS Account. These users were created by myself using the AWS IAM service. I can designate my user's access to my AWS Account resources/services.

User Groups

IAM user groups are useful for grouping and managing user's permissions at a group level. They act similarly to folders when it comes to assigning permission/policies at a mass level.

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



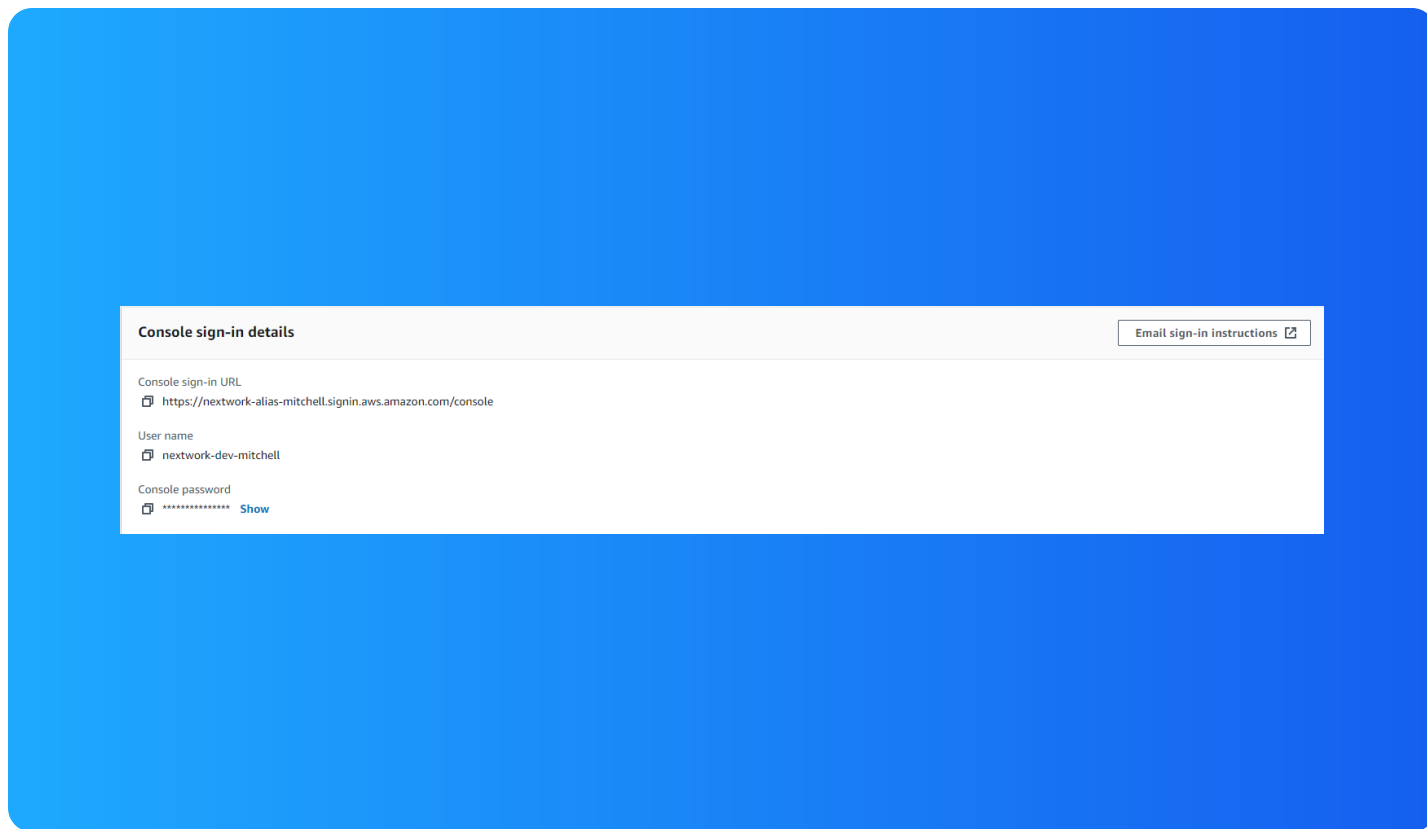
mmoorejr24@gmail.com
NextWork Student

NextWork.org

Logging in as an IAM User

The first way is emailing sign-in instructions. The second is downloading a .csv file.

Once I logged in as my IAM user, I noticed that a lot of the panels displayed "Access denied". This was a clear difference to the dashboard I usually see in my AWS Account.





mmoorejr24@gmail.com
NextWork Student

NextWork.org

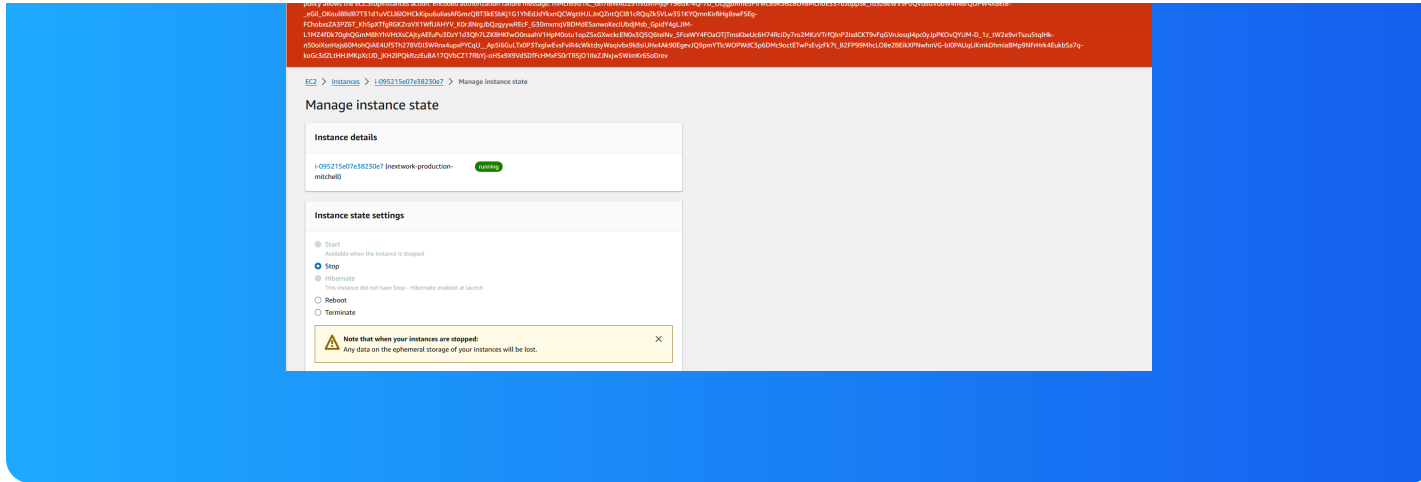
Testing IAM Policies

I tested my JSON IAM policy by logging in as the new user.

Stopping the production instance

When I tried to stop the production instance, I received a big fat error message letting me know that I was denied that action.

Failed to stop the instance i-0952156d783229c7
You are not authorized to perform the operation. User: arn:aws:iam::38855984191:user/network-dev-mitchell is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-west-1:38855984191:instance/i-0952156d783229c7 because no identity-based



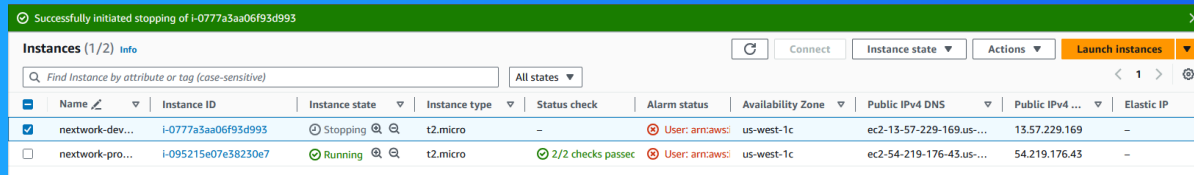
mmoorej24@gmail.com
NextWork Student

NextWork.org

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, I received a green success banner.





NextWork.org

**Everyone
should be in a
job they love.**

Check out nextwork.org for more projects

