



# Cloud Security with AWS IAM



auliaarifin89@gmail.com

> Create policy

**Specify permissions** Info

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

Policy editor

```
1 var [
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "ec2:Describe",
7       "Resource": "*",
8       "Condition": {
9         "StringEquals": {
10           "ec2:ResourceTag/Env": "development"
11         }
12       }
13     },
14     {
15       "Effect": "Allow",
16       "Action": "ec2:DeleteTags",
17       "Resource": "*"
18     },
19     {
20       "Effect": "Deny",
21       "Action": [
22         "ec2:DeleteTags",
23         "ec2:CreateTags"
24       ],
25       "Resource": "*"
26     }
27   ]
28 ]
```

Visual JSON

Edit statement

Select an existing add a

+ Add

Add new statement



auliaarifin89@gmail.com

NextWork Student

[NextWork.org](http://NextWork.org)

---

# Introducing today's project!

## What is AWS IAM?

AWS IAM is a user management for AWS resources

## How I'm using AWS IAM in this project

I use to rule control the AWS EC2 instance for new user

## One thing I didn't expect...

AWS IAM is so good for user management, so detail on the policy

## This project took me...

i take around 1 hour to under standing AWS IAM policy



auliaarifin89@gmail.com

NextWork Student

[NextWork.org](http://NextWork.org)

# Tags

Tags are like labels you can attach to AWS resource for organization

In this case, we're creating a tag called "Env" with a value of "production" or "development" to label the instances used in production vs development environments.

The image displays two side-by-side screenshots of the AWS EC2 'Manage tags' interface. Both screenshots show a list of tags for a specific instance, with the ability to add new tags.

**Screenshot 1 (Left):** Shows tags for instance `i-09670c0a53f7c1db8`. It lists two tags:

- Key: Env, Value: development
- Key: Name, Value: network-development-auliaarifin

**Screenshot 2 (Right):** Shows tags for instance `i-01372ce53d2127fb`. It lists two tags:

- Key: Env, Value: production
- Key: Name, Value: network-production-auliaarifin

Both interfaces include fields for 'Add new tag' and 'Save' buttons.



auliaarifin89@gmail.com

NextWork Student

[NextWork.org](http://NextWork.org)

---

# IAM Policies

IAM Policies are a rule what you can do with AWS resources. is all about giving permissions to IAM users

## The policy I set up

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

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 a part of policy structure and define a list permissions



auliaarifin89@gmail.com

NextWork Student

[NextWork.org](http://NextWork.org)

# My JSON Policy

Create policy

### Specify permissions Info

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

Policy editor

```
1 w [ ]  
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

Visual    **JSON**

Edit statement

Select an existing statement  
+ Add new statement



auliaarifin89@gmail.com

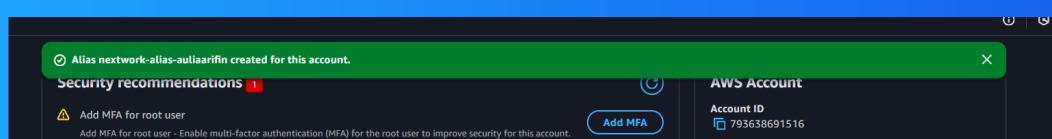
NextWork Student

[NextWork.org](http://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 under 5 mintutes. Now my new AWS console sign-in URL is <https://nextwork-alias-auliaarifin.signin.aws.amazon.com/console>





auliaarifin89@gmail.com

NextWork Student

[NextWork.org](http://NextWork.org)

---

# IAM Users and User Groups

## Users

IAM users are services to manage users for using AWS resources

## User Groups

IAM user groups are the people that will get access to your resources/AWS account, whereas user groups are the collections/folder of users for easier user management.

I attached the policy I created to this user group which means to grant user to nextwork-dev-group for permission associated with that group



auliaarifin89@gmail.com

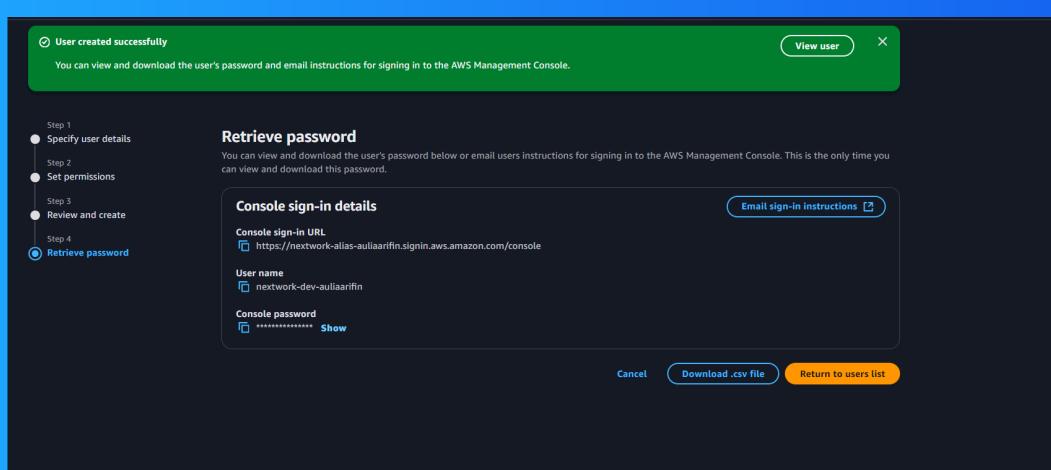
NextWork Student

[NextWork.org](http://NextWork.org)

# Logging in as an IAM User

The first way is create IAM users and give a policy for user to manage/uses AWS resources

Once I logged in as my IAM user, I noticed the list application on ec2 instance acces denied, this was becasue i dont give a permission to ec2 list application





auliaarifin89@gmail.com

NextWork Student

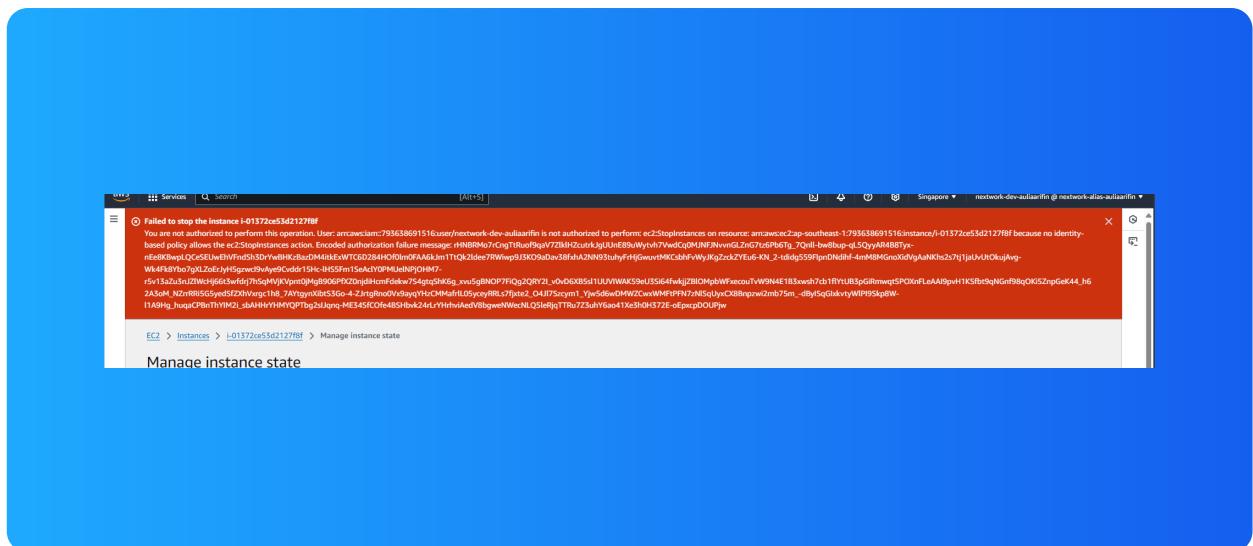
[NextWork.org](http://NextWork.org)

# Testing IAM Policies

I tested my JSON IAM policy by stop instance, when stop the production i have an error and when stop the development production is successfully stoped

## Stopping the production instance

When I tried to stop the production instance eror pop up appear, this was because the user didnt have a permission to the production instance





auliaarifin89@gmail.com

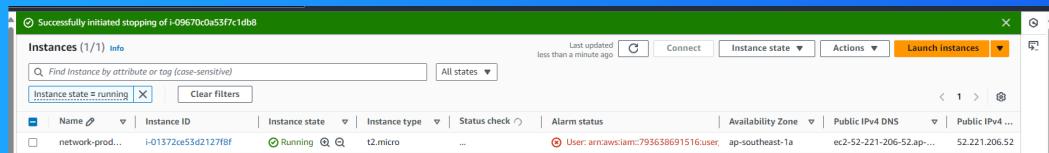
NextWork Student

[NextWork.org](http://NextWork.org)

# Testing IAM Policies

## Stopping the development instance

Next, when I tried to stop the development instance i have to check my user policy this was becasue the policy is powerfull to manage a user





NextWork.org

# Everyone should be in a job they love.

Check out nextwork.org for  
more projects

