



NextWork.org

Cloud Security with AWS IAM



James La

The screenshot shows the AWS IAM Policy editor interface. At the top, there are tabs for "Visual", "JSON" (which is selected), and "Actions". Below the tabs, the JSON code for a policy is displayed:

```
1 ▼ {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Effect": "Allow",
6             "Action": "ec2-*"
}
```

To the right of the JSON code, there is a "Edit statement" button.

```
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 }
```

Select a statement

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

+ Add new statement



James La
NextWork Student

[NextWork.org](https://www.nextwork.org)

Introducing today's project!

What is AWS IAM?

AWS IAM is a service that helps you control access to your AWS resources. This is useful because it significantly reduces security risks and operational overhead in our AWS operations.

How I'm using AWS IAM in this project

In today's project, I used AWS IAM to create policies and give users and user groups specific access to specific resources.

One thing I didn't expect...

I didn't expect to be able to create accounts that can access and manage my resources, so easily.

This project took me...

This project took me around 1 hour to complete.



James La
NextWork Student

[NextWork.org](https://www.nextwork.org)

Tags

Tags are labels we can add to instances to make it easier to organize our instances.

The tag I've used on my EC2 instances is called "Env". The value I've assigned for my instances are "production" and "development". This will allow me to use the "Env" tag to filter between instances that are designed for production or development.

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

▼ Name and tags [Info](#)

| Key Info | Value Info | Resource types Info |
|---|--|---|
| <input type="text" value="Name"/> X | <input type="text" value="nextwork-develc"/> X | <input type="button" value="Select resource ty..."/> Remove |
| Instances X | | |
| Key Info | Value Info | Resource types Info |
| <input type="text" value="Env"/> X | <input type="text" value="development"/> X | <input type="button" value="Select resource ty..."/> Remove |
| Instances X | | |
| Add new tag | | |
| You can add up to 48 more tags. | | |



James La
NextWork Student

[NextWork.org](#)

IAM Policies

IAM Policies are a set of rules that defines who can do what with my AWS resources.

The policy I set up

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

I've created a policy that allows any action to be taken on EC2 instances with a "Env - Development" tag, anyone to get information on EC2 instances, and it also denies users from deleting and creating tags.

When creating a JSON policy, you have to define its Effect, Action and Resource.

The Effect, Action, and Resource attributes of a JSON policy are key components that define the permissions granted or denied by that policy.



James La
NextWork Student

[NextWork.org](https://www.nextwork.org)

My JSON Policy

Policy editor

Visual **JSON** Actions ▾

```
1 ▼ {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": "s3:ListBucket"
6       "Resource": "arn:aws:s3:::nextwork-public"
7     }
8   ]
9 }
```

Edit statement

```
1
2
3
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}
```

Select a statement

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

+ Add new statement



James La
NextWork Student

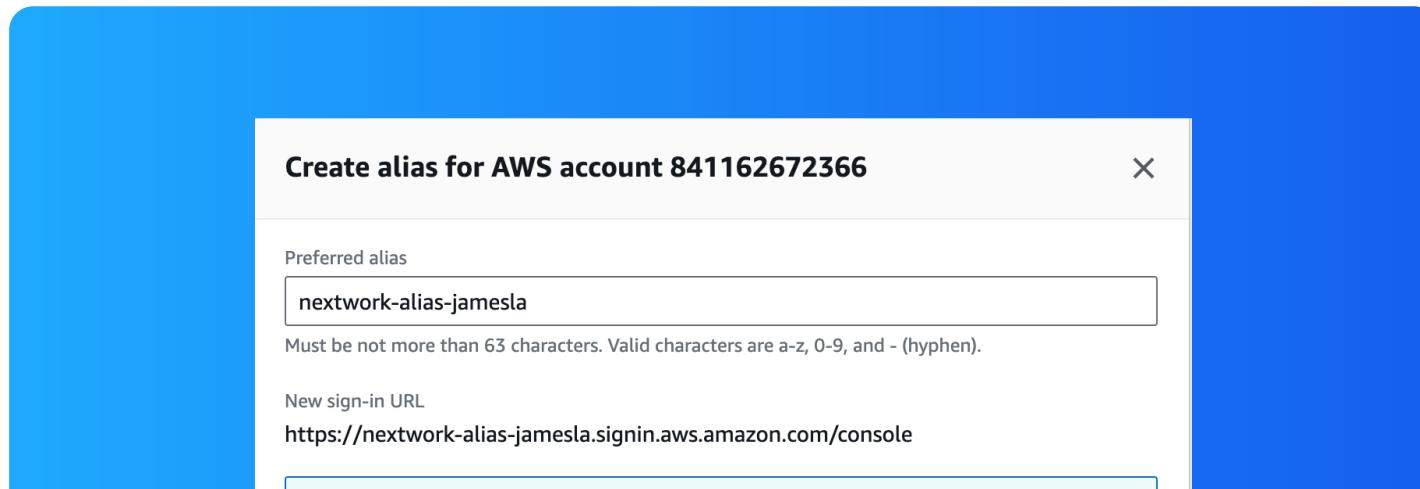
[NextWork.org](https://www.nextwork.org)

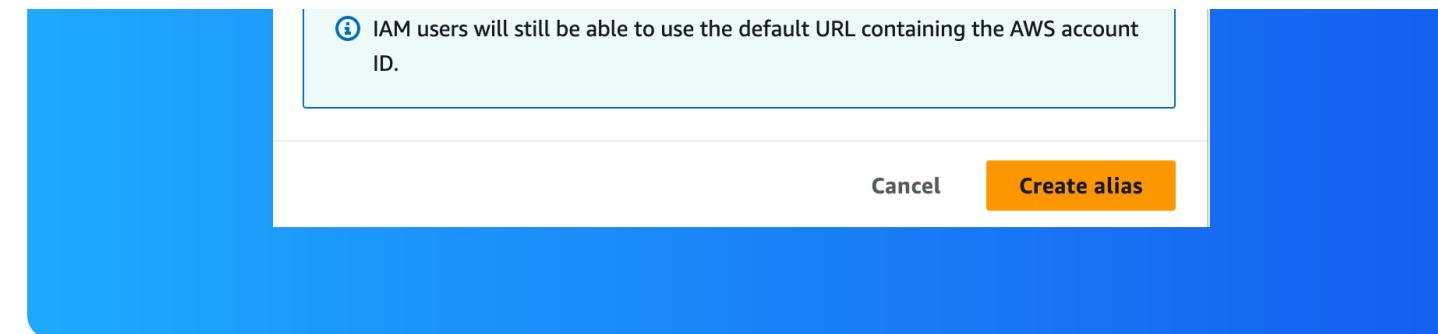
Account Alias

An account alias is name for my AWS account that I can use to sign in to the AWS Management console instead of using my Account ID.

Creating an account alias took me 5 seconds. It was as simple as clicking a button, setting a title, and clicking "create alias".

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





James La
NextWork Student

[NextWork.org](https://www.nextwork.org)

IAM Users and User Groups

Users

IAM users are users or services that can interact with AWS resources.

User Groups

IAM user groups are collections or folders of IAM users. IAM user groups allow us to collectively manage users without having to manage each and every user individually.

I attached the policy I created to this user group, which means all users in the selected group all follow the given policy.



James La
NextWork Student

[NextWork.org](https://www.nextwork.org)

Logging in as an IAM User

The first way is to email the sign-in instructions to the user through a button when you create the user, and the second way is to download a provided csv file, with the details, and directly send it to the user.

Once I logged in as my IAM user, I noticed many of the dashboard panels were showing "Access denied"!

A screenshot of the AWS IAM User Details page. A large blue rectangular overlay covers the top portion of the page. Within this overlay, there is a white rectangular box containing the following text:

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Below this text are two buttons:

Console sign-in details

Email sign-in instructions

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

User name
 [nextwork-dev-james](#)

Console password
 ***** [Show](#)



James La
NextWork Student

[NextWork.org](#)

Testing IAM Policies

I tested my JSON IAM policy by stopping both the production and development EC2 instances.

Stopping the production instance

When I tried to stop the production instance, I got a big error saying that it failed to stop the instance.





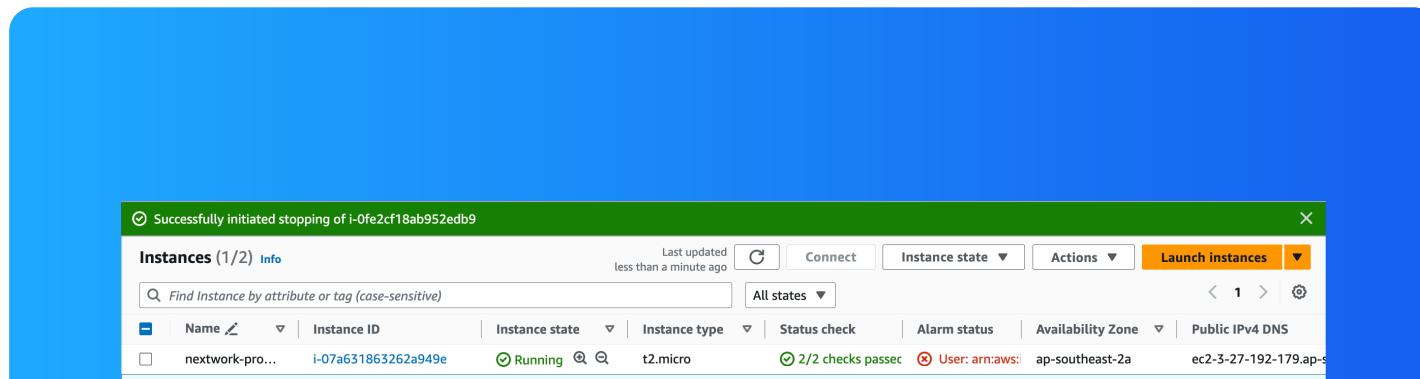
James La
NextWork Student

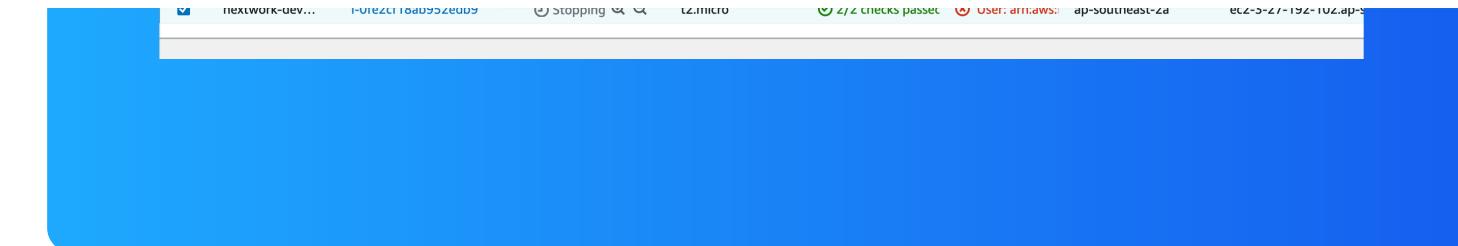
[NextWork.org](https://www.nextwork.org)

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, I got a notification saying it successfully stopped the instance.





[NextWork.org](https://learn.nextwork.org/heartsfelt_navy_zesty_moray_eel/projects/aws-security-iam/document.html)

Everyone should be in a job they love.

Check out nextwork.org for
more projects

