



Cloud Security with AWS IAM



otite.timothy@yahoo.com

Step 2
Review and create

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 {
16   "Effect": "Allow",
17   "Action": "ec2:Describe*",
18   "Resource": "*"
19 },
20 {
21   "Effect": "Deny",
22   "Action": [
23     "ec2:DeleteTags",
24     "ec2:CreateTags"
25   ],
26   "Resource": "*"
27 ]
28 }
```

+ Add new statement

Edit statement

Select a statement

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

+ Add new statement



otite.timothy@yahoo.com

NextWork Student

NextWork.org

Introducing today's project!

What is AWS IAM?

AWS Identity and Access Management (IAM) is a service that enables you to securely manage access to AWS services and resources. It allows you to create and control user accounts, assign permissions, and enforce security policies.

How I'm using AWS IAM in this project

Creating Users and Groups: I set up IAM users and grouped them based on their roles. Assigning Policies: I attached specific policies to users and groups, granting them the necessary permissions to access and manage AWS resources like EC2 instances.

One thing I didn't expect...

I didn't expect this project to provide robust security steps without being technically difficult. In light of completing this project, It was straightforward and didn't not come at the cost of sacrificing security

This project took me...

2 hours



otite.timothy@yahoo.com

NextWork Student

NextWork.org

Tags

Tags are like unique label identifiers attach to AWS resources for organisation. This tagging helps us with identifying all resources with the same tag at once

The tag I've used on my EC2 instances are called nextwork-development-Otite and nextwork-production-Otite. The value I've assigned for my instances are' called 'Env production' and 'Env Environment'

The screenshot shows the 'Name and tags' configuration section for a Lambda function. It displays two existing tags and a button to add a new one.

Key	Value	Resource types
Name	nextwork-develc	Select resource ty... Instances
Development	Enter value	Select resource ty... Instances

Add new tag
You can add up to 48 more tags.



otite.timothy@yahoo.com

NextWork Student

NextWork.org

IAM Policies

IAM Policies enable robust control for who has permitted access to use specific 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 as it can be easily configured with an existing template provided in the JSON Policy 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 These attributes together control access by defining what can be done, on which resources, and whether it is allowed or denied.



otite.timothy@yahoo.com

NextWork Student

NextWork.org

My JSON Policy

Step 2
Review and create

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    ]
28 }
```

Edit statement

Select a statement

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

+ Add new statement

+ Add new statement

**otite.timothy@yahoo.com**

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

Creating an account alias took me 2 minutes to create

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

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with various navigation options like 'Dashboard', 'Access management', 'Access reports', and 'Tools'. The main area is titled 'IAM Dashboard' and contains sections for 'Security recommendations', 'AWS Account' (with account ID 497538590872), 'Quick Links' (including 'My security credentials'), and 'What's new'. A central modal window is open, titled 'Edit alias for AWS account 497538590872'. It has a 'Preferred alias' input field containing 'nextwork-alias-otite' and a note below it stating: 'Must be no more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen)'. Below the note is a warning message: 'IAM users in this account will not be able to sign-in through the URL with current alias. They can sign-in using the URL with the new alias or the AWS account ID.' At the bottom of the modal are 'Cancel' and 'Save Changes' buttons.



otite.timothy@yahoo.com

NextWork Student

NextWork.org

IAM Users and User Groups

Users

IAM users are the people that will get access to your resources/AWS account

User Groups

IAM user groups are groups are the collections/folders of users for easier user management.

I attached the policy I created to this user group, which means that every user in the group inherits the permissions specified in the policy. This allows for centralised management of permissions

**otite.timothy@yahoo.com**

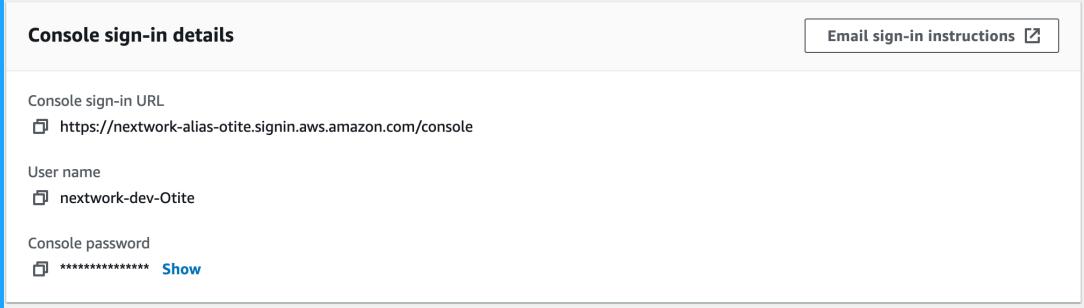
NextWork Student

NextWork.org

Logging in as an IAM User

The first way is download a CSV file containing the user's access key ID, secret access key, and other sign-in details. The second way is emailing the Sign-In Link AWS provides includes the account ID or alias

Once I logged in as my IAM user, I noticed that some of your dashboard panels are displaying restrictive access



A screenshot of the AWS IAM console showing sign-in details. The interface has a blue header and a white body. At the top left is the heading "Console sign-in details". At the top right is a button labeled "Email sign-in instructions". Below these are three sections: "Console sign-in URL" with a link to "https://nextwork-alias-otite.signin.aws.amazon.com/console", "User name" with the value "nextwork-dev-Otite", and "Console password" with a redacted value followed by a "Show" link.



otite.timothy@yahoo.com

NextWork Student

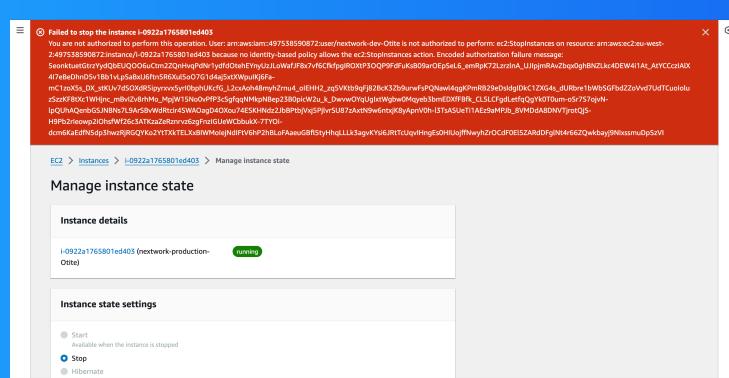
NextWork.org

Testing IAM Policies

I tested my JSON IAM policy by trying to stop the development and production instances i.e. triggering the StopInstance action.

Stopping the production instance

When I tried to stop the production instance, an error message stopped me and explained that I am not authorised to stop the production instance.





otite.timothy@yahoo.com

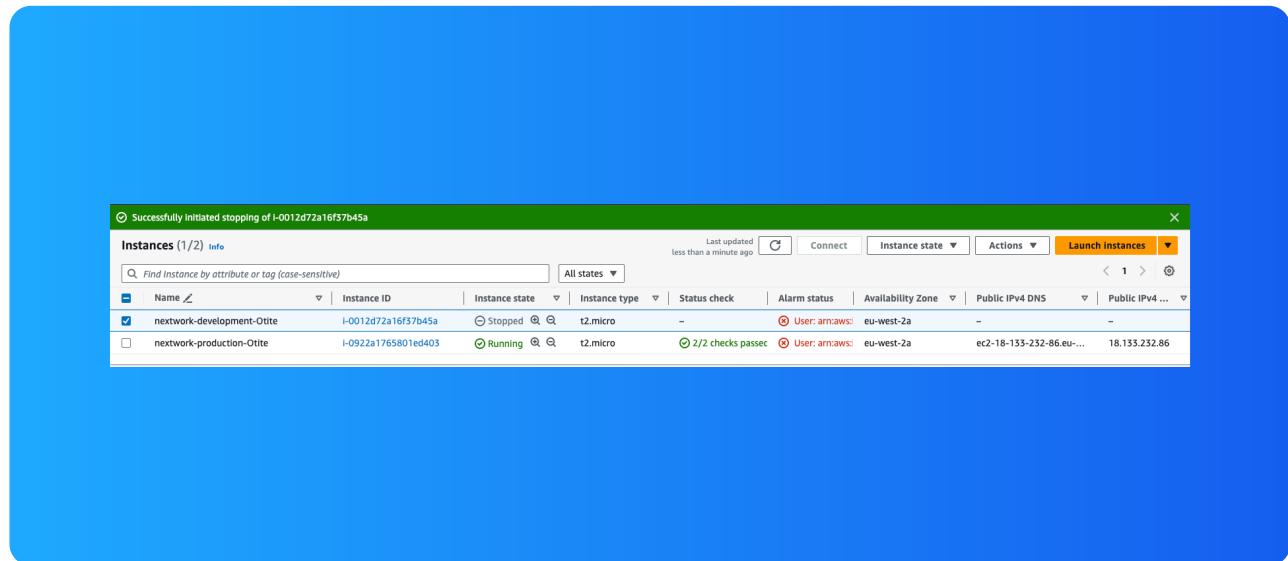
NextWork Student

NextWork.org

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, it successfully stopped





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

Everyone should be in a job they love.

Check out nextwork.org for
more projects

