



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

# Cloud Security with AWS IAM



Ogun Tari Joseph

The screenshot shows the AWS IAM Policy Editor interface. The top navigation bar includes the AWS logo, a search bar, and tabs for IAM, Policies, and Create policy. Below the navigation, a breadcrumb trail shows IAM > Policies > Create policy. A progress bar indicates Step 1: Specify permissions is selected. The main area is titled "Specify permissions" with a "Info" link. It contains a note: "Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor." The "Policy editor" section displays the following JSON code:

```
1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Effect": "Allow",
5         "Action": "ec2:Describe",
6         "Resource": "*",
7         "Condition": {
8             "StringEquals": {
9                 "ec2:ResourceTag/Env": "development"
10            }
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    }
26]
```

The right side of the interface features a "Select a statement" panel with a "Edit statement" button, a "Select a statement" dropdown, and a "+ Add new statement" button.



# Introducing Today's Project!

In this project, I will demonstrate connecting EC2 instances to an IAM policy. I'm doing this project to learn more about cloud security

## Tools and concepts

Services I used were AWS IAM and EC2. Key concepts I learnt include user creation, cloud security, and user permissions.

## Project reflection

This project took me approximately 20 minutes. The most challenging part was setting up the IAM user, but it was enjoyable for me.



# Tags

Tags are used for classifying and organizing AWS resources, and this is to ensure the purpose of similar AWS resources are not mixed up.

The tag I've used on my EC2 instances is called Env, which stands for the environment the instances are in. The value I've assigned for my instances are production and development, which are the two environments available.

The screenshot shows the AWS EC2 'Launch an instance' wizard. In the 'Name and tags' section, a tag named 'Env' with the value 'development' is selected. The 'Summary' sidebar on the right shows the instance configuration: 1 instance, AMI 'Amazon Linux 2023.7.2...', instance type 't3.micro', and 1 volume (8 GiB). A tooltip for the 'Free tier' is visible, stating: 'In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where # of cores isn't multiplied when used with free tier)'.



# IAM Policies

IAM Policies are JSON documents that permit select actions, resources and so on.

## The policy I set up

For this project, I've set up a policy using JSON, which is the standard format the policies are in.

I've created a policy that allows certain actions to be carried out the instances I created that are tagged with the tags I made.

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

The Effect, Action, and Resource attributes of a JSON policy mean the allowing or denying the action, the details of the action, and the resources that will be affected by said action.



# My JSON Policy

The screenshot shows the AWS IAM 'Create policy' interface. The 'Specify permissions' step is selected. The 'Policy editor' section displays the following JSON policy:

```
1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Effect": "Allow",
5         "Action": "ec2:*",
6         "Resource": "*",
7         "Condition": {
8             "StringEquals": {
9                 "ec2:ResourceTag/Env": "development"
10            }
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    }
]
```

The right side of the screen shows a modal titled 'Edit statement' with the sub-section 'Select a statement'. It contains the instruction 'Select an existing statement in the policy or add a new statement.' and a blue button labeled '+ Add new statement'.



# Account Alias

An account alias is an alternative and easier name to access the AWS management console.

Creating an account alias took me less than a minute. Now, my new AWS console sign-in URL is <https://nextwork-alias-tariogun.sigin.aws.amazon.com/console>

The screenshot shows the AWS IAM Dashboard. A modal window titled "Create alias for AWS account 440744216547" is open. In the "Preferred alias" field, the value "nextwork-alias-tariogun" is entered. Below the field, a note states: "Must be no more than 63 characters. Valid characters are a-z, 0-9, and -(hyphen)." Under "New sign-in URL", the URL "https://nextwork-alias-tariogun.sigin.aws.amazon.com/console" is displayed. A note below it says: "IAM users will still be able to use the default URL containing the AWS account ID." At the bottom right of the modal is a yellow "Create alias" button. The background of the dashboard shows the IAM resources section with 0 User groups, 0 Users, 3 Roles, 5 Policies, and 0 Identity providers. To the right, there's a sidebar for "AWS Account" with the account ID "440744216547" and a link to the sign-in URL. There are also "Quick Links" for "My security credentials" and "Manage your access keys, multi-factor authentication (MFA) and other credentials".



# IAM Users and User Groups

## Users

IAM users are people who are granted access to an AWS console and are restricted by set policies, which makes them unable to take any actions other than the ones they intend to do.

## User Groups

IAM user groups are a collection of IAM users that share similar permissions and these groups are used for better organization.

I attached the policy I created to this user group, which means every member of said group is subject to the policy.



# Logging in as an IAM User

The first way is by copying it and sending it to the user. The second way is to set up the user's email to be a recipient of the details from the console.

Once I logged in as my IAM user, I noticed I was denied access to certain things. This was because I had not been granted permission for those things.

The screenshot shows the AWS Management Console interface for creating a new IAM user. The top navigation bar includes the AWS logo, search bar, and user profile 'jtari6'. The main title is 'IAM > Users > Create user'. A green success message box at the top states 'User created successfully' and 'You can view and download the user's password and email instructions for signing in to the AWS Management Console.' Below this, a sidebar on the left lists the steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password), with Step 4 currently selected. The main content area is titled 'Retrieve password' and contains the following information:

- Console sign-in details**:
  - Console sign-in URL: <https://nextwork-alias-tariogun.siginin.aws.amazon.com/console>
  - User name: nextwork-dev-tariogun
  - Console password:  [Show](#)
- [Email sign-in instructions](#)

At the bottom of the page are buttons for 'Cancel', 'Download .csv file' (disabled), and 'Return to users list'.

Page footer: https://eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1  
© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

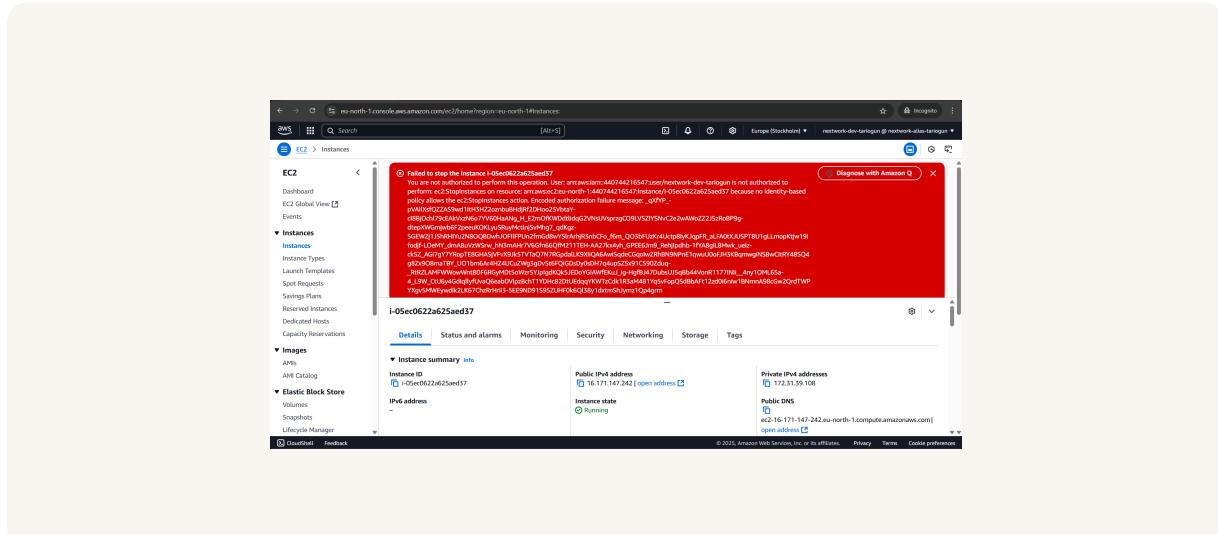


# Testing IAM Policies

I tested my JSON IAM policy by stopping both instances, and I was only able to stop one, which was what the policy stated I had permission to do.

## Stopping the production instance

When I tried to stop the production instance, a large red notification popped up which said I did not have permission to stop the instance. This was because in the policy, I was only granted permission to stop the development instance.

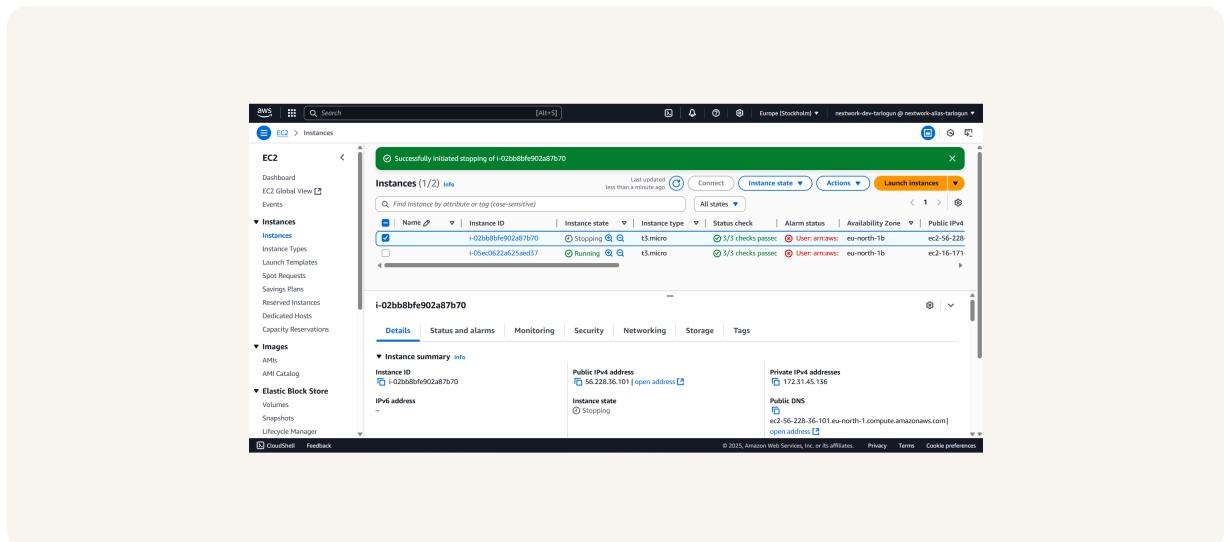




# Testing IAM Policies

## Stopping the development instance

Next, when I tried to stop the development instance, it was successful, since I had permission to do that.





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

# The place to learn & showcase your skills

Check out [nextwork.org](https://nextwork.org) for more projects

