



nextwork.org

Cloud Security with AWS IAM



Wachiraya Meevasana (Tanny)

The screenshot shows the AWS IAM 'Create policy' page. The left pane displays a JSON policy document with line numbers 5 through 25. The right pane contains a sidebar with the heading 'Select a statement' and a button '+ Add new statement'.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Env": "development"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:Describe",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource": "*"
    }
  ]
}
```



Wachiraya Meevasana (T...

NextWork Student

NextWork.org

Introducing today's project!

What is AWS IAM?

I learned how to use AWS IAM to create users and groups, attach policies, and manage permissions. I also practiced securing access with tags, console login, and create Alias account.

How I'm using AWS IAM in this project

This project took me approximately 30 mins. The most challenging part was create alias user. It was most rewarding to learn how to create security group on my EC2 instances.

One thing I didn't expect...

I chose to do this project today because I want to keep learning on AWS services.



Tags

Tags are labels that help us with identifying all resources with the same tag at once (they are useful filters when we're searching for something), cost allocation, and applying policies based on environment types

The tag I've used on my EC2 instances is called ENV. The values I've assigned for my instances are Production and Development.

The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. In the 'Name and tags' section, a tag named 'Env' with the value 'development' is selected. The 'Summary' panel indicates 1 instance will be launched. The 'Software Image (AMI)' section shows 'Amazon Linux 2023 AMI 2023.7.2...' with a 'read more' link. The 'Virtual server type (instance type)' is set to 't2.micro'. The 'Firewall (security group)' dropdown shows 'New security group'. At the bottom right are 'Cancel', 'Preview code', and a large orange 'Launch instance' button.



IAM Policies

IAM Policies are the 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

I've created a policy that the intern do everything EC2-related on resources tagged with Env=development and view (describe) all EC2 resources. But, he can't create or delete tags on any EC2 resources.

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

Effect: Specifies whether the action is allowed or denied (e.g., "Allow" or "Deny").

Action: Defines the specific AWS operation or service action (e.g.,

"ec2:StartInstances"). Resource: Specifies the AWS resources the action applies to.



My JSON Policy

The screenshot shows the AWS IAM 'Create policy' interface. The left pane displays a JSON policy document with line numbers 4 through 25. The right pane contains a sidebar with the heading 'Select a statement' and a button '+ Add new statement'. At the bottom, there are links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

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

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)



Account Alias

An account alias is a friendly name for your AWS account that I can use instead of my account ID to sign in to the AWS Management Console.

Creating an account alias took me 3 sec !. Now, my new AWS console sign-in URL is <https://internacc1.signin.aws.amazon.com/console>

The screenshot shows the AWS IAM 'Create alias' dialog box over a blurred background of the IAM dashboard. The dialog box has the following fields:

- Preferred alias:** intern
- New sign-in URL:** <https://intern.signin.aws.amazon.com/console>
- Note:** IAM users will still be able to use the default URL containing the AWS account ID.

At the bottom right of the dialog box are two buttons: **Cancel** and **Create alias**. The **Create alias** button is highlighted with a yellow border. In the background, the IAM dashboard shows a list of users and roles, and a sidebar with navigation links like Dashboard, Access management, Policies, and Identity providers.



IAM Users and User Groups

Users

IAM users are individual identities in AWS with credentials, used to access and manage resources based on assigned permissions.

User Groups

IAM user groups are collection of IAM users. Those allows me to manage permissions for all the users in the groups at the same time by attaching policies to the group rather than individual users

I attached the policy I created to this user group, which means this group have broad read access to EC2, limited control over "development"-tagged resources, and zero ability to tag anything.



Logging in as an IAM User

The first way is Email – Send login URL, username, and temporary password manually. Another way is to download the .csv file with sign-in details and securely share it.

Once I logged in as my IAM user, I noticed the permission denied. This was because AWS console will treat me as someone that is starting from 0.

aws Search [Alt+S]

IAM > Users > Create user

Step 1
● Specify user details
Step 2
● Set permissions
Step 3
● Review and create
Step 4
● **Retrieve password**

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.

Console sign-in details

Console sign-in URL
 https://internacc1.signin.aws.amazon.com/console

User name
 AlexIntern

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

[Email sign-in instructions](#)

[Download .csv file](#) [Return to users list](#)

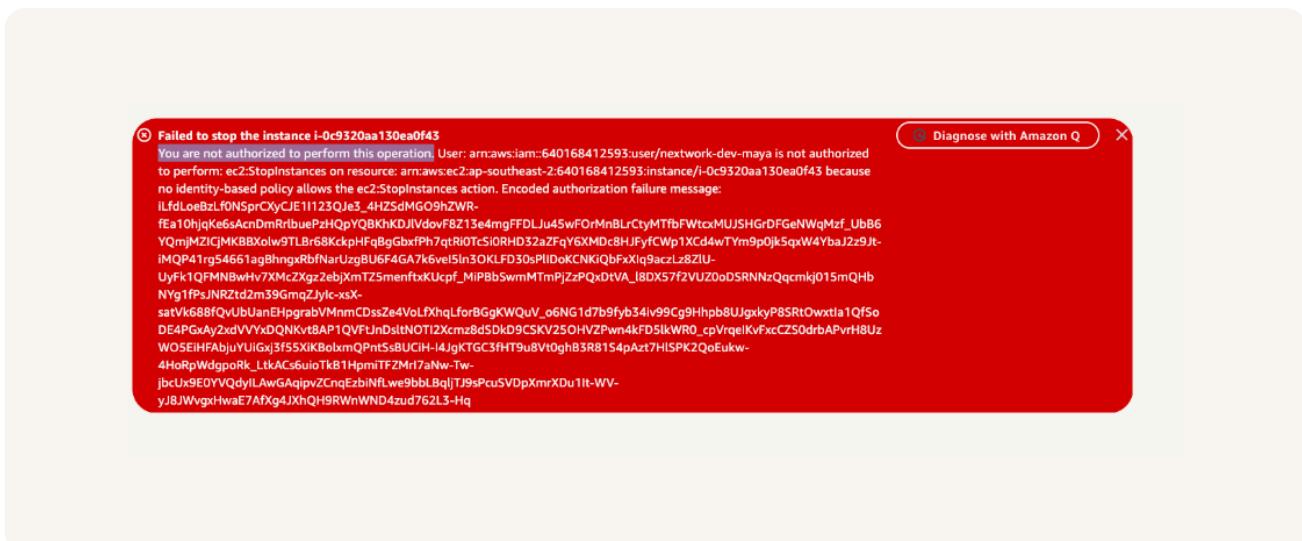


Testing IAM Policies

I tested my JSON IAM policy by stopping the instance.

Stopping the production instance

When I tried to stop the production instance there was an error message popped up, it's because we're not authorized. We don't have permission to stop any instance with the production tag.





Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance, it is successful. This was because I have permission to do it.

The screenshot shows the AWS EC2 Instances page. At the top, there is a green notification bar stating "Successfully initiated stopping of i-08cc39005ac0bd03b". Below this, the main interface displays two instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
Tanny Dev Server	i-087bab448d76a060	Running	t2.micro	2/2 checks passed	View alarms +
Tanny Prod server	i-08cc39005ac0bd03b	Stopping	t2.micro	Initializing	View alarms +

The "Tanny Prod server" instance is currently stopping. The page also includes sections for Instance summary, Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

