



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

# Cloud Security with AWS IAM

KU

kushwanthchowdary990@gmail.com

Policies > Create policy

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

create

Policy editor

Visual    **JSON**

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 {  
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 ]

Edit statement

Select an existing statement  
Add new statement

+ A

# Introducing today's project!

## What is AWS IAM?

Services I used were... Key concepts I learnt include IAM, groups user and alias and policy simulator and how JSON policy works

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

This project took me approximately 1 hour... The most challenging part was figuring out the denied of Ec2 instance It was most rewarding to do

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

I chose to do this project today because i have no idea how to do IAM setting for new users... Something that would make learning with NextWork even better is learning about Cloud Security

# Tags

Tags are organisational which are useful to label on what bases we are creating Ec2 instance

for ec1 tags are key: Env value: production for ec2 tags: key: Env value:Development

## ▼ Name and tags [Info](#)

[Key](#) | [Info](#)

Name

[Value](#) | [Info](#)

nextwork-dev-kush

[Key](#) | [Info](#)

Env

[Value](#) | [Info](#)

Development

# IAM Policies

IAM Policies are determine who can do what in AWS for this project use JSON to control who has access to what

## The policy I set up

For this project, I've set up a policy using JSON to give access to only development for only interns

I've created a policy that a policy holder who can do anything with development tag

## 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 whether a policy is allowing or deny the action, what the policyholder can do or cannot do and specific resources can access to policy holders only

# My JSON Policy

Policies > Create policy

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

create

Policy editor

Visual    **JSON**

```
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 {
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 ]
```

Edit statement

Select an existing statement or add a new one

+ A

# Account Alias

An account alias is simply a nickname to our AWS account instead of our long AWS ID we use this alias account as reference

Creating an account alias took me 30 secsNow, my new AWS console sign-in URL is <https://nextwork-alias-kush.signin.aws.amazon.com/console>

## Create alias for AWS account 021891614188

Preferred alias

Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL

<https://nextwork-alias-kush.signin.aws.amazon.com/console>

i IAM users will still be able to use the default URL containing the AWS account ID.

[Cancel](#)

[Create alias](#)

# IAM Users and User Groups

## Users

IAM users are people that access to your AWS login account

## User Groups

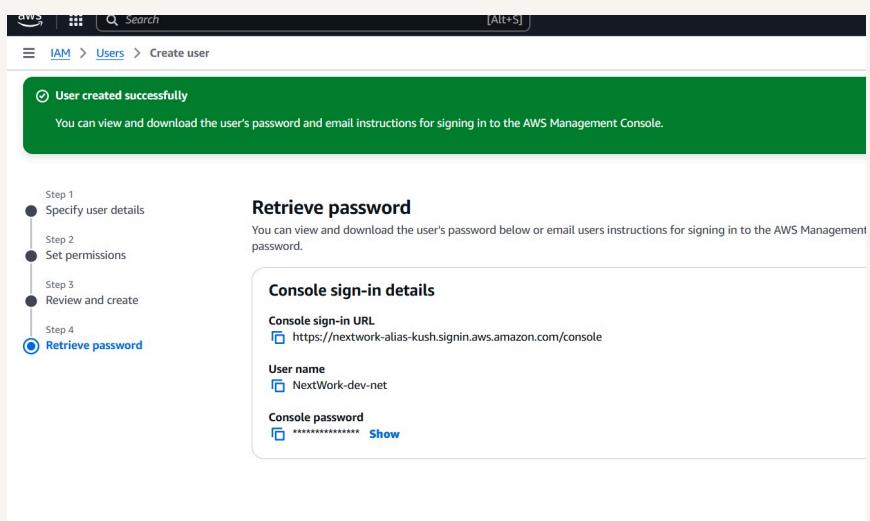
IAM user groups are like folders that collect IAM users that apply permission settings in group level

I attached the policy I created to this user group, which means any user inside this folder can access the development environment

# Logging in as an IAM User

The first way is downloading .csv file another and another way instructions to the users

Once I logged in as my IAM user, I noticed my root user was logout This was because i hva etried to another login in the same broswer



# Testing IAM Policies

I tested my JSON IAM policy by JSON format to manage actions on two Amazon EC2 instances.

## Stopping the production instance

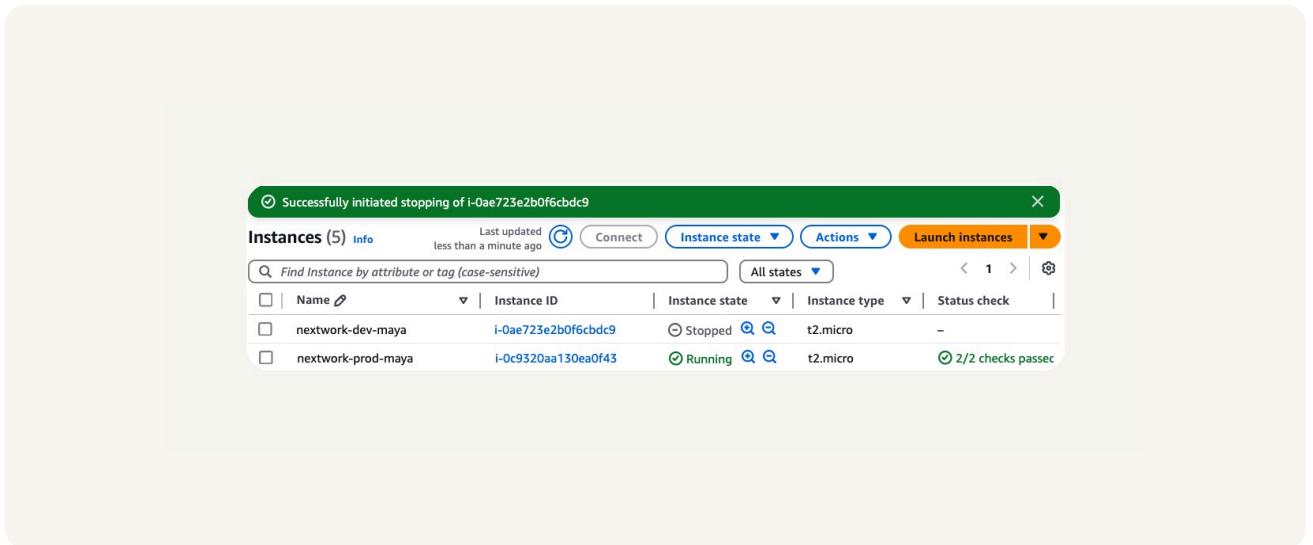
Ensure that your IAM user or role has the necessary permissions to stop EC2 instances. The required action is ec2:StopInstances. Without this permission, attempts to stop an instance will be denied.

```
Failed to stop the instance i-0c9320aa130ea0f43
You are not authorized to perform this operation. User: arn:aws:iam::640168412593:user/nextwork-dev-maya is not authorized
to perform: ec2:StopInstances on resource: arn:aws:ec2:ap-southeast-2:640168412593:instance/i-0c9320aa130ea0f43 because
no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message:
iLfdLoeBzLf0NSprCXyCJE1I123QJe3_4HZSdMGO9hZWR-
fEa10hjqKe6sAcnDmRlbluePzHQpYQBKhKDjlvdovF8Z13e4mgFFDLJu45wForMnBLrCtyMTfbFWttxMUIJSHGrDFGeNWqMzf_UbB6
YQmjMzICjMKBBXolw9TLBr68KckpHFqBgGbxPh7qtRiOTci0RHd32aZfqY6XMDc8HJFycCWP1Xcd4wTYm9p0jk5gxW4YbaJ2z9Jt-
iMQP41rg54661agBhngxRbfNarUzgBU6F4GA7k6veI5ln3OKLFD30sPlIDoKCNKiQbFxXlq9aczLz8ZIU-
UyFk1QFMNBwhhv7XMcZXqz2ebjXmT25menftxKUcpf_MiPBbSwmMTmPjZzPQxDtVA_18DX57f2VUZoDSRNNzQqcmkj015mQHb
NYg1fPsJNRZtd2m39GmqZJylc-xsX-
satV688fQvUbUanEHppgrabVMnmCDssZe4VoLfXhqLforBggKWQuV_o6NG1d7b9fyb34iv99Cg9HhpB8UJgxkyP8SRtOwxtla1QfSo
DE4PGxAy2xdVVYxDQNkvt8AP1QVFjnDsItNOTI2Xcmz8dSDk9CSKV250HVZPwn4kFD5lkWR0_cpVrqelKvFxcCZS0drbAPvrH8Uz
W0SEiHFaibuYUIGxj3f55XIKBolxmQPrntSsBUCiH-l4JgKTGc3fHT9u8Vt0ghB3R8154pAzt7HiSPK2QoEukw-
4HoRpWdgpoRk_LtkACs6uoTkB1HpmiTfZMrI7aNw-Tw-
jbcUx9E0YVQdylLAwGAqipvZCnqEzbiNflwe9bbLBqljTJ9sPcuSVDPxmrXDu1lt-WV-
yJ8JWvgxHwaE7AfXg4JXhQH9RWnWND4zud762L3-Hq
```

# Testing IAM Policies

## Stopping the development instance

Next, when I tried to stop the development instance, I encountered a permission error. This was because the IAM policy attached to my user account did not include the necessary `ec2:StopInstances` permission for that specific instance.





NextWork.org

# **Everyone should be in a job they love.**

Check out nextwork.org for  
more projects

