

nextwork.org

Cloud Security with AWS IAM



Arun Kumar

The screenshot shows the AWS IAM Policy editor interface. The top navigation bar includes the AWS logo, search bar, and global navigation links. The main area is titled "Policy editor" and displays a JSON-based policy document. The policy defines two statements: one allowing EC2 actions with a condition based on resource tags, and another denying specific EC2 actions. The right side of the interface features a sidebar with options to "Edit statement", "Select a statement", and "Add new statement".

```
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 }
```



Arun Kumar
NextWork Student

NextWork.org

Introducing today's project!

What is AWS IAM?

IAM users (Identity and Access Management users) are individual identities created within AWS IAM (Identity and Access Management) that represent a person or service interacting with your AWS resources.

How I'm using AWS IAM in this project

creatd the iam user and created group policy and add new user to the user group

One thing I didn't expect...

the sudden paid sumilator

This project took me...

i wasted because i felt bore so i take like 50mins



Arun Kumar
NextWork Student

NextWork.org

Tags

tag are the shortcuts to the resources where they make things easier to access them when we needed in this the tags are Env production and Env development so these can tag to the file

In this case, we're creating a tag called "Env" with a value of "production" or "development" to label the instances used in production vs development environments.

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links like Dashboard, EC2 Global View, Events, Instances (selected), Instances Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, and Images. The main content area has a header 'Instances (2) Info' with filters for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Pub. Below this is a table with two rows:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Pub
nextwork-pro...	i-0a7e63e100bade7e8	Running	t2.micro	2/2 checks passed	View alarms +	ap-southeast-2b	ec2...
nextwork-dev...	i-0c4085ab1ecb6ab41	Running	t2.micro	2/2 checks passed	View alarms +	ap-southeast-2b	ec2...

At the bottom, there's a section labeled 'Select an instance' with a dropdown menu.



IAM Policies

An IAM policy is a rule for who can do what with your 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, and when those rules kick in.

The policy I set up

I've set up a policy using'... json

This policy 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.

effect it means it can have two actions either allow or deny action this give list of options to allow or deny in this "ec2:*" means all actions that you could possibly take on EC2 instances are allowed Resource '*' means all resource in the scope



Arun Kumar
NextWork Student

NextWork.org

My JSON Policy

```
aws IAM Policies Create policy [Option+5] Global Arun
Policy editor
Visual JSON Actions ▾
Edit statement
Select a statement
+ Add new statement
+ Add new statement
1 v {
2   "Version": "2012-10-17",
3 v   "Statement": [
4 v     {
5       "Effect": "Allow",
6       "Action": "ec2:*",
7       "Resource": "*",
8 v       "Condition": {
9 v         "StringEquals": {
10          "ec2:ResourceTag/Env": "development"
11        }
12      },
13    },
14 v    {
15      "Effect": "Allow",
16      "Action": "ec2:Describe*",
17      "Resource": "*"
18    },
19 v    {
20      "Effect": "Deny",
21 v      "Action": [
22        "ec2:DeleteTags",
23        "ec2:CreateTags"
24      ],
25      "Resource": "*"
26    }
27  ]
28 }
```



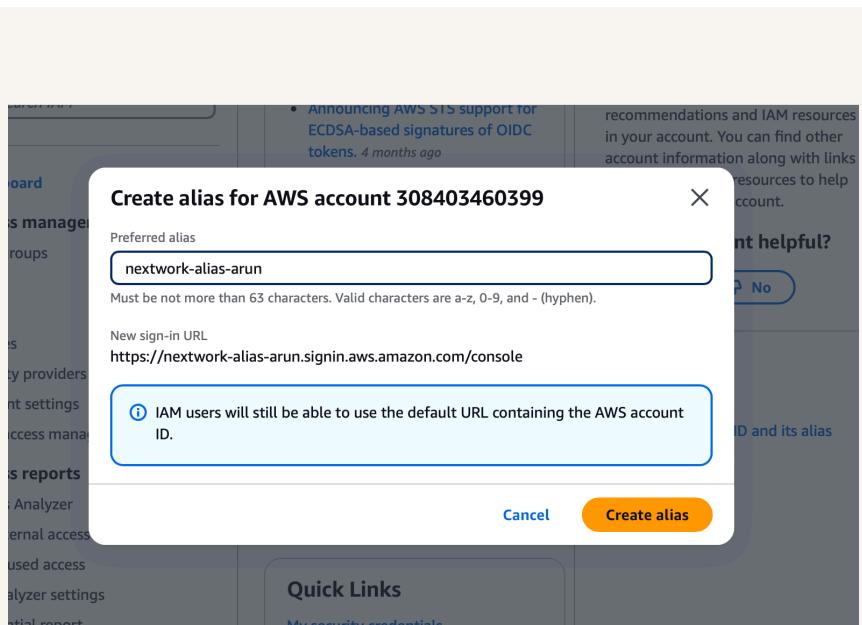
Arun Kumar
NextWork Student

NextWork.org

Account Alias

An Account Alias is a friendly name for your AWS account that you can use instead of your account ID (which is usually a bunch of digits) to sign in to the AWS Management Console.

'Creating an account alias took me less then 30 seconds ... Now, my new AWS console sign-in URL is'...nextwork-alias-arun





Arun Kumar
NextWork Student

NextWork.org

IAM Users and User Groups

Users

IAM users (Identity and Access Management users) are individual identities created within AWS IAM (Identity and Access Management) that represent a person or service interacting with your AWS resources.

User Groups

An IAM user group is a collection/folder of IAM users. It allows you to manage permissions for all the users in your group at the same time by attaching policies to the group rather than individual users.

i attached the policy i created to the user group it make easier to update allows you to manage permissions for all the users in your group at the same time by attaching policies to th



Logging in as an IAM User

1. Email or Secure Messaging the Credentials Manually
2. Download the .csv File

As a new user, you'll notice that some of your dashboard panels are showing Access denied already. As a new user, the AWS console will treat you as someone that is starting from 0 again.

The screenshot shows the AWS IAM 'Create user' process at Step 4: Retrieve password. A green success message box at the top right says 'User created successfully' and provides instructions to view and download password and email instructions. To the left, a vertical navigation bar lists steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password, which is highlighted). On the right, under 'Retrieve password', there's a 'Console sign-in details' section containing a 'Console sign-in URL' (https://nextwork-alias-arun.sigin.aws.amazon.com/console), 'User name' (nextwork-dev-arun), and 'Console password' (a masked password). Buttons for 'Email sign-in instructions' (with a link icon), 'Download .csv file', and 'Return to users list' are at the bottom.



Arun Kumar
NextWork Student

NextWork.org

Testing IAM Policies

'I tested my JSON IAM policy by trying to stop the production and development instances so i have no access to stop the production instances

Stopping the production instance

'When I tried to stop the production instance... it pops up a warning banner. This was because i dont have access to it

The screenshot shows a browser window for the AWS EC2 Instances page. The URL is [EC2 > Instances > i-0a7e63e100bade7e8 > Manage instance state](#). A red error message box is displayed, containing the following text:

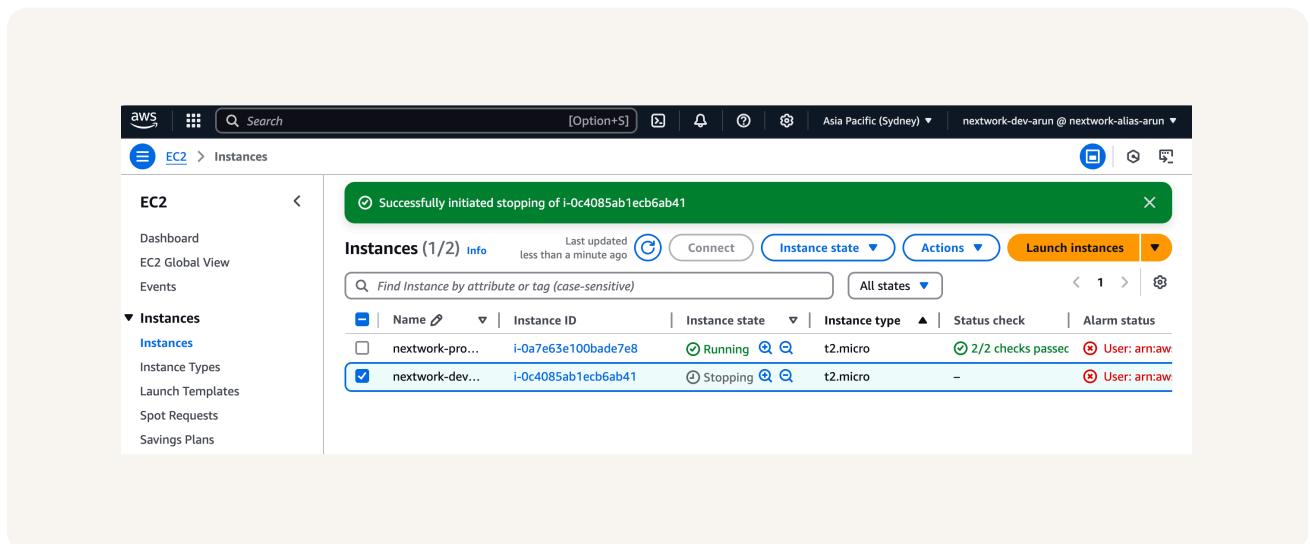
```
Failed to stop the instance i-0a7e63e100bade7e8
You are not authorized to perform this operation. User: arn:aws:iam::308403460399:user/nextwork-dev-arun is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:ap-southeast-2:308403460399:instance/i-0a7e63e100bade7e8 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: p3w5nV8m-vfSSnfBxlnfGm18plaGR78SgOOBgytZ6ndlDa_IkxD2wp5TO12cXdhq44u-bgxPwXlmQsyoN64qxHmDng643pkSXggGQxL_RicKDDE1VWwdVdOoyhu148RcUrvCh024TAzK2zpAdbzYuBx_n1b09LY87GI4gPwj0JY-Gz-gaqZE56_wq_ZxCQDZwvTEpso9QZeh1selrESI72tjusHTgx4yeNiNNIB_vEjStwdYp4qGOURR80O2L_xkagGuHN3Hgc-p5bWgbhOyLcqH1gzGTrmSi-lbVILsdGDIpmQLH5rcCaMAYagy_-Hm79jY7pNz-6qk6Z2ZGOpuQDyJaLMKcJ_3AvjhUbJ2wMjEjMjhGOFQtSe26lMDEHf2_BxZBuXQcijKLujJPVDBLY0hRFU6-OI2aeuhQWrINk6ehsuQ8WUf_cf2AQHsrb7ArvxjyZI461GlvL-w2plfE7q0A8RClykUFp_rjDpRY_Y_Dd8pV1_S2GxQwTYAxs9eOyQYj02m-efeuusUqM7H40fHUtC3tIepmVwEV6cDsLkokwQJTL7sLs-eg3VNb6hsUV_rTbvXsg8CWV7zsvEchibEloshWluxZfSvnf3g5DFY0EkmhsG35-fjQYeTmHdDuUN3tw4RF43HDzdht3VDDmFJwc-p8moQdlzMijcJtmsKORilkcvjNrHj6i7avkAvdge7mSP7fbsvjMF9sw1LmfTH3CxAcGE2kWropeh3ie-s_QoHxz2ENU0-TA2l9s3n5sDzK7n6f_pRVBSscQyzaMkOaqM3djdtkOy9MjlC-0TM42w-16e8ZYk-XplvA-sjm3byhof564-r7QERpljX18n04UsckjQBNlbGdwrgLGRO_FteiGn
```



Testing IAM Policies

Stopping the development instance

when I tried to stop the development instance it was successfully deployed. This was because I have the complete access to the development instance.





NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

