



Cloud Security with AWS IAM



Ronson Lobo

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

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": [

```

Edit statement Remove

Add actions

Choose a service

Included

EC2

Available

AMP

API Gateway

API Gateway V2

ASC



Ronson Lobo
NextWork Student

NextWork.org

Introducing today's project!

What is AWS IAM?

AWS Identity and Access Management (IAM) is a free web service that allows you to control access to AWS resources and services. It's a key tool for securing your AWS account by helping you: Manage permissions Create and manage roles etc

How I'm using AWS IAM in this project

I used AWS IAM by creating a new user and granting the permission to that user to perform specific action via JSON policy

One thing I didn't expect...

I wasn't expecting the policy will run

This project took me...

I was able to complete this project in 1 hour of time



Ronson Lobo
NextWork Student

NextWork.org

Tags

In AWS, tags are labels or attributes that you can attach to resources to help you manage, identify, and organize them:

The tag I've used on my EC2 instances is called production and development

Instances (1/2) Info					
Last updated less than a minute ago					
		Actions		Launch instances	
Name	Instance ID	Instance state	Instance type	Status check	Alarm status
<input type="checkbox"/> production	i-012a38dc82cd68f70	Running	t2.micro	Initializing	View alarm
<input checked="" type="checkbox"/> development	i-0149ffdfa28bca7a4	Running	t2.micro	Initializing	View alarm



IAM Policies

IAM policies define permissions for users, groups, and roles in an AWS account, and regulate access to AWS resources. They are a key part of any solution built on AWS-managed services.

The policy I set up

For this project, I've set up a policy using JSON

'I've created a policy that Allow or Deny on mentioned keywords

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

In AWS, a policy is a JSON document that defines permissions and resource access rules. Action is a rule to be performed on a resource and a resource in JSON policy is the target

Ronson Lobo
NextWork Student

NextWork.org

My JSON Policy

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

Policy editor

Visual	JSON	Actions ▾	□
Edit statement			
Remove			
Add actions			
Choose a service			
<input type="text"/> Filter services			
Included			
EC2			
Available			
AMP			
API Gateway			
API Gateway V2			
ASC			

```
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": [
```

Ronson Lobo
NextWork Student

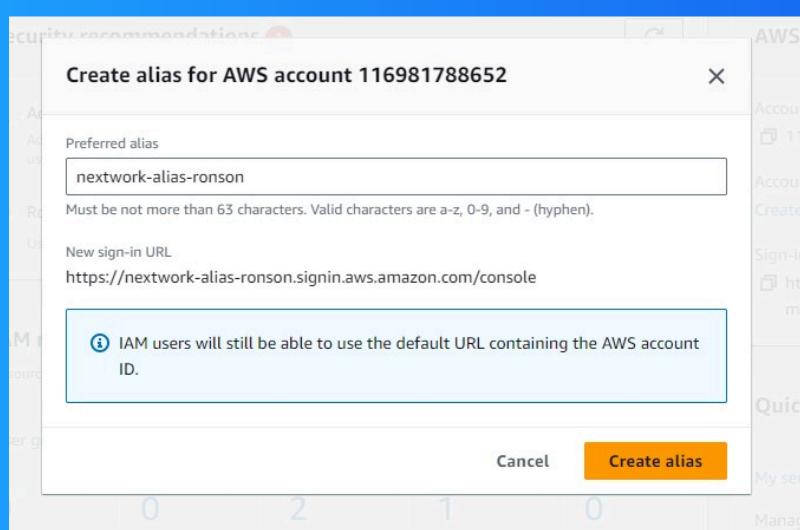
NextWork.org

Account Alias

An account alias is an alternate name for an account number, and is used to more easily identify an account when performing a transaction.

Creating an account alias took me a minute

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





IAM Users and User Groups

Users

An IAM user is an entity in an AWS account that represents a person or application that interacts with AWS resources. IAM stands for AWS Identity and Access Management, which is a security measure that controls access to AWS resources.

User Groups

In Amazon Web Services (AWS), an IAM user group is a collection of IAM users that can be managed as a single entity. IAM user groups allow you to:

- Specify permissions for multiple users
- Make it easier to manage permissions
- Define what actions

I attached the policy I created to this user group, which means set of rules are define in JSON



Logging in as an IAM User

The first way is to share the user url name and user id password and ask him to change the password later and second option is create a user and provided the username and url and click on option Users must create a new password at next sign-in -

Once I logged in as my IAM user, I noticed Access Denied for

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	Email sign-in instructions
Console sign-in URL https://nextwork-alias-ronson.signin.aws.amazon.com/console	
User name nextwork-dev-ronson	
Console password Yq#Vz6j6 Hide	



Ronson Lobo
NextWork Student

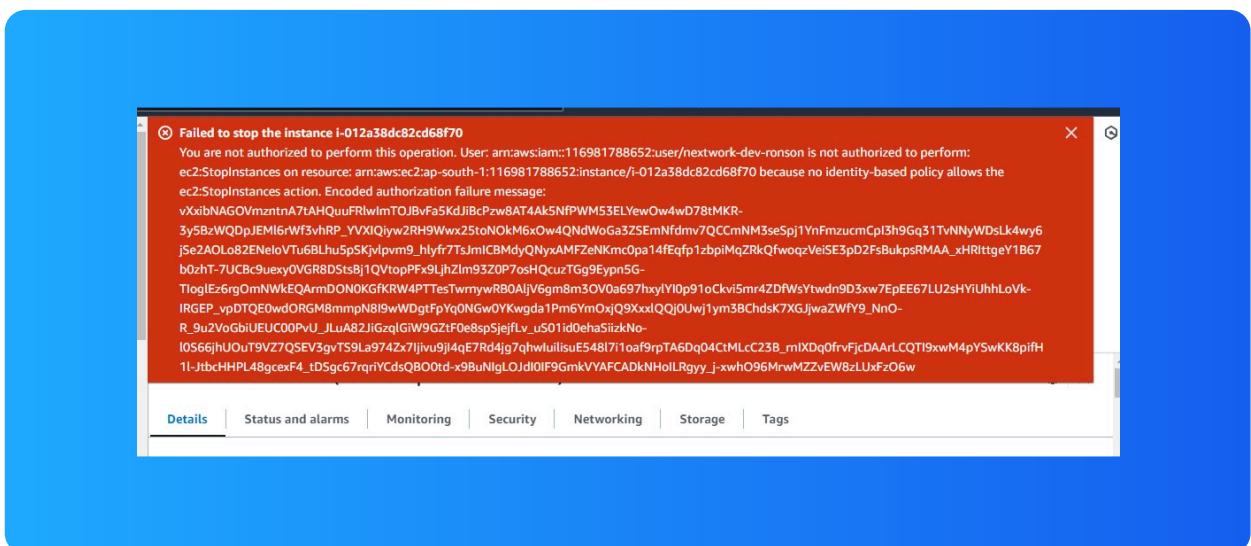
NextWork.org

Testing IAM Policies

I tested my JSON IAM policy by stopping the development EC2 instance as it was pre-described. I was able to stop development instance but i was not able to stop the production instance

Stopping the production instance

When I tried to stop the production instance i got a big error on the screen. We don't have permission to stop any instance with the production tag.





Ronson Lobo
NextWork Student

NextWork.org

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance i was able to stop the instance immediately without any error

The screenshot shows the AWS EC2 Instances page with the following details:

Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP
Running	t2.micro	Initializing	User: arn:aws:iam::123456789012:root	ap-south-1a	ec2-43-205-136-112.ap...	43.205.136.112
Running	t2.micro	2/2 checks passed	User: arn:aws:iam::123456789012:root	ap-south-1a	ec2-13-232-87-161.ap...	13.232.87.161



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

