

Cloud Security with AWS IAM

Erik Gonzalez

Policy editor

Visu

```
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 }
29
```

Introducing Today's Project!

In this project, I'll show how to use AWS IAM to manage user access and permissions in an AWS account, building a foundation-level understanding of cloud security and how identities are securely controlled in the cloud.

Tools and concepts

Services I used were Amazon EC2 and AWS IAM. Key concepts I learnt include IAM users, policies, user groups, account aliases. I also learned how to use a policy simulator and how JSON policies work. How to launch and tag an instance.

Project reflection

This project took me approximately 2 hours. The most challenging part was understanding the IAM policy since it was written in JSON and it contained multiple statements. It was most rewarding to see permission denied as the intern. Policy worked!

Tags

Tags are organizational tools that let us label our resources. They are helpful for grouping resources, cost allocations, and applying policies for all real resources with the same tag.

The tag I've used on my EC2 instances is called Env, which stands for environment. The values I've assigned for my instances are production and development.

Launch an instance [Info](#)
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

▼ Name and tags [Info](#)

Key [Info](#)

Q Name X

Value [Info](#)

Q nimbus-dev-eg X

Resource types [Info](#)

Select resource types ▼

Instances X

Remove

Key [Info](#)

Q Env X

Value [Info](#)

Q development X

Resource types [Info](#)

Select resource types ▼

Instances X

Remove

Add new tag

You can add up to 48 more tags.

IAM Policies

IAM policies are rules that can determine who can do what in an AWS account. To control who has access to my production/environment instance.

The policy I set up

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

Made a policy that allows the policy holder (i.e. the intern) to have permission to do anything they desire to any instance tagged with "development." They can also see information for any instance, but they're denied access to deleting/creating tags

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 or not the policy is allowing or denying actions (i.e. effect); what the policy holder can or cannot do (i.e. the action) and specific AWS resources that the policy relates to.

My JSON Policy

Policy editor

Visu

```
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 }
29
```

Account Alias

An account alias is simply a nickname for the AWS account. Instead of a long account ID, we can now reference the account alias instead.

Creating an account alias took me less than a minute. The console login uses is <https://cloud-strife.signin.aws.amazon.com/console>

Create alias for AWS account 312831649097

Preferred alias

cloud-strife

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

New sign-in URL

https://cloud-strife.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 or entities that have access/can login to the AWS account.

User Groups

IAM user groups are like folders that collect IAM users so that you can apply permission settings at the group level.

I attached the policy I created to this user group, which means any user created inside this group will automatically get the permissions attached to our Nimbus Dev Environment IAM policy.

Logging in as an IAM User

The first way is to email the instructions, the second way is to download a .csv file with the sign-in details inside.

Once I logged in as my IAM user, I noticed that the intern user is already denied access to panels on the main AWS console dashboard. This was because we set up permissions in the EC2 instance to follow as such

The screenshot shows the AWS IAM console interface. At the top is the AWS navigation bar with the logo, a search bar, and utility icons. Below it is a breadcrumb trail: IAM > Users > Create user. A green success banner at the top of the main content area states 'User created successfully' and provides a 'View user' button. To the left is a vertical step indicator with four steps: 'Specify user details', 'Set permissions', 'Review and create', and 'Retrieve password' (which is the active step, indicated by a blue circle). The main content area is titled 'Retrieve password' and includes a sub-header 'Console sign-in details'. It displays the 'Console sign-in URL' as 'https://cloud-strifee.signin.aws.amazon.com/console', the 'User name' as 'Nimbus-dev-eg', and the 'Console password' as a masked string with a 'Show' link. On the right side of the 'Console sign-in details' box is an 'Email sign-in instructions' button. At the bottom right of the main content area are 'Cancel' and 'Download .csv file' buttons.

aws [Search] [Option+S]

IAM > Users > Create user

✔ User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View 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 password.

Console sign-in details

Email sign-in instructions

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

User name
Nimbus-dev-eg

Console password
***** Show

Cancel Download .csv file

Testing IAM Policies

I tested my JSON IAM policy by attempting to stop both the development and the production instances.

Stopping the production instance

When I tried to stop the production instance., I was met with an error. This was because the production instance is tagged with the 'production' label which is outside of the scope of the intern's permission policy. Intern is only granted development.

Failed to stop the instance i-06b8ce51e2bd0de82

 Diagnose with Amazon Q

















You are not authorized to perform this operation. User: arn:aws:iam::312831649097:user/Nimbus-dev-eg is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:312831649097:instance/i-06b8ce51e2bd0de82 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: DpIPQmA72z_XvsjbaAma9hldll2w9QMFI_GtQvIrHP5ZKGIT_Dd6CX5VnR9_azpzULCaCNvbLUXW965PyPuXXMMMPqQ0Et8Ga3-1xQtPa1ZH1CIJ7VAO7Pslpmgct29cZIAZgzfMtE9WDTw_1Vjp2yS-DQjqUXCKR7OBDAeOHZdNXvkn6bA7xeH2lNoV7Jgf1O55Wuv7Eeg1k5tASJfO0kwrbl6s7UH2vbJaYBkQ4TTZqkTaQMMTqaYUJi-dRZGUGwZyF09aPlu0x4wl41GBK8TJncoix-w8AU-C8ofdhsO7HGB2zOgl_2CR92tKK_tZC4kKM72qaBniNRdqLUIAXS7NgjfZSivVELwjthHqzWI_78m8rYSghEL8-DOoMMIV557t_H9ZcfEwCEXhNNhP_UrWt-Q6xTFb154XQVPJ8j2QPQBJp_JFnw-OvzSGZWeoeVqj9vLb57ali21UP11uZKgFiozzHm-1z7H3cOkDx5J6VKG_CR9pVdkwv3ps87nYTHwg7h12Ud4FhB1jniKEQsnYh6s9GbT6mGXJjfx6EuxFI_R95fsWMIM-cbURGG0JznixN79nVs4k5ctVMTdewEjyulKwMJs131HizpiOSkrvg_GkaaspL9R40XSgv8kqgzKZNaJxAl4cor6JxAO8Zbp7hgTqJWLcpnQ615P0_6_pTO6am-TkpxamovS2U74x3xavsF6a1UN4tFm6EY2r-yen3FQ56cYg3HcRLC7OCPW6Td7vJMDf5QHW7bf6A0zPs0XFDI_RkT_ZI75EZ4C4zUBfdJP5FcbzG0yW3IDYcNPvcttJ-hdKmgK7rbC7aDk2xtQHpg1q5xsTNat4OGGv0v7nYROWNA0A07E1wssg75tvPcY5-OfCwSTfHg

Testing IAM Policies

Stopping the development instance

Next, when I tried to stop the development instance I successfully saw the instance state change to Stopping and then Stopped. This was because our permission policy allows the intern (users in dev group)) to stop instances.

Instances	Name 	Instance ID	Instance state 	Instance type 	Status check	Alarm status	Availability Zone 
<input checked="" type="checkbox"/>	nimbus-dev-eg	i-0b07d155188e95526	 Stopping  	t2.micro	 2/2 checks passed	 User: arn:aws:iam::123456789012:user:dev	us-east-1c
<input type="checkbox"/>	Nimbus-prod-eg	i-06b8ce51e2bd0de82	 Running  	t2.micro	 2/2 checks passed	 User: arn:aws:iam::123456789012:user:dev	us-east-1c

IAM Policy Simulation

Why would you use the IAM Policy Simulator?

The IAM policy simulator is a tool that lets us simulate actions and test permission settings by defining a specific user/group/role and the action we want to test for. It's useful for saving time when testing permission settings. No more logging in into another user or actually stopping resources.

What were the simulation results for the development instance?

We set up a simulation for whether our dev group has permission to StopInstances or DeleteTags. The results were denied for both - we had to adjust the scope of the EC2 instances to ones that are tagged with “development”. Once we applied the tag, permission was allowed.

Policy Simulator

Amazon EC2

2 Action(s) sele...

Select All

Deselect All

Reset Contexts

Clear Results

Run Simulation

▸ Global Settings ⓘ

Action Settings and Results [2 actions selected. 0 actions not simulated. 1 actions allowed. 1 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
▸ Amazon EC2	StopInstances	instance	*	allowed 1 matching statements.
▸ Amazon EC2	DeleteTags	not required	*	denied 1 matching statements.