

```
→ ssh git:(master) × ssh ec2-user@18.133.189.86
The authenticity of host '18.133.189.86 (18.133.189.86)' can't be established.
ECDSA key fingerprint is SHA256:haqt+kC+krpX8UpH2uQ4d1TZZfxrXXAJU+QjKf3tsUA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '18.133.189.86' (ECDSA) to the list of known hosts.
ec2-user@18.133.189.86: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
→ ssh git:(master) × ssh ec2-user@18.133.189.86 -i LondonKey.pem
```

```
__|__|__| )
_| ( / Amazon Linux 2 AMI
---|\\---|---
```

```
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-15-102 ~]$
```

The screenshot shows the AWS Management Console interface. On the left, there's a navigation sidebar with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, and LOAD BALANCING. The main content area displays the 'MyCLIEC2' EC2 instance. A context menu is open over the instance, showing options like 'Connect', 'Create Template From Instance', 'Launch More Like This', 'Instance State', 'Instance Settings', 'Image', 'Networking', and 'CloudWatch Monitoring'. The 'Instance Settings' submenu is expanded, showing options like 'Add/Edit Tags', 'Attach to Auto Scaling Group', 'Attach/Replace IAM Role' (which is highlighted), 'Change Instance Type', 'Change Termination Protection', 'View/Change User Data', 'Change Shutdown Behavior', 'Change T2/T3 Unlimited', 'Get System Manager', 'Modify Instance Profile', and 'Modify Instance Maintenance Settings'. A yellow text box overlay reads: 'Update: Select the EC2 Instance and go under 'Actions,' 'Security,' and then "Modify IAM role.''

Below the instance details, there's a table showing the instance's configuration:

Instance: i-0709e7992269990e (MyCLIEC2)		Public DNS: ec2-52-56-196-80.eu-west-2.compute.amazonaws.com
<b>Description</b>		
Instance ID	i-0709e7992269990e	Public DNS (IPv4)
Instance state	running	ec2-52-56-196-80.eu-west-2.compute.amazonaws.com
Instance type	t2.micro	IPv4 Public IP
Elastic IPs		52.56.196.80
Availability zone	eu-west-2a	IPv6 IPs
		-
		Private DNS
		ip-172-31-25-137.eu-west-2.compute.internal
		Private IPs
		172.31.25.137

aws

Services

Search for services, features, marketplace products, and docs

[Option+S]

linghuang

Global

Support

Identity and Access Management (IAM)

Policies > AdministratorAccess

Summary

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

AWS account ID:

156507964004

Policy ARN

arn:aws:iam::aws:policy/AdministratorAccess

Description

Provides full access to AWS services and resources.

Permissions

Policy usage

Policy versions

Access Advisor

Policy summary

{ } JSON

1 {

2 "Version": "2012-10-17",

3 "Statement": [

4 {

5 "Effect": "Allow",

6 "Action": "\*",

7 "Resource": "\*"

8 }

9 ]

10 }

read-only

```
+ ssh git:(master) x ssh ec2-user@18.133.189.86 -i LondonKey.pem
Last login: Sat Jul 10 23:07:52 2021 from pool-72-79-56-92.nwrknj.east.verizon.net

 _ _ _ _ _
| | | | |
|_|_|_|_|_| Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-15-102 ~]$ sudo su
[root@ip-172-31-15-102 ec2-user]# l
bash: l: command not found
[root@ip-172-31-15-102 ec2-user]# ls
[root@ip-172-31-15-102 ec2-user]# aws s3 ls
2021-06-14 00:33:04 ling-version-control-demo123
2021-06-13 23:18:37 linghuang-20210613
2021-06-18 15:13:13 myreplicationbucket-ling
2021-06-20 20:08:30 scubasyndrome20210620
2021-07-10 23:14:57 testbucket-lingh
[root@ip-172-31-15-102 ec2-user]# cd ~
[root@ip-172-31-15-102 ~]# l
bash: l: command not found
[root@ip-172-31-15-102 ~]# ls -lah
total 20K
drwxr-x--- 4 root root 115 Jul 10 23:11 .
drwxr-xr-x 18 root root 257 Jul 10 23:03 ..
drwxr-xr-x 2 root root 39 Jul 10 23:11 aws
-rw-r--r-- 1 root root 18 Oct 18 2017 .bash_logout
-rw-r--r-- 1 root root 176 Oct 18 2017 .bash_profile
-rw-r--r-- 1 root root 176 Oct 18 2017 .bashrc
-rw-r--r-- 1 root root 108 Oct 18 2017 .cshrc
drwx----- 2 root root 29 Jul 10 23:03 .ssh
-rw-r--r-- 1 root root 129 Oct 18 2017 .tcshrc
[root@ip-172-31-15-102 ~]# rm -rf aws
[root@ip-172-31-15-102 ~]# aws s3 ls
2021-06-14 00:33:04 ling-version-control-demo123
2021-06-13 23:18:37 linghuang-20210613
2021-06-18 15:13:13 myreplicationbucket-ling
2021-06-20 20:08:30 scubasyndrome20210620
2021-07-10 23:14:57 testbucket-lingh
[root@ip-172-31-15-102 ~]# cd .aws
bash: cd: .aws: No such file or directory
[root@ip-172-31-15-102 ~]#
```

- Roles are more secure than storing your access key and secret access key on individual EC2 instances.
- Roles are easier to manage.
- Roles can be assigned to an EC2 instance after it is created using both the console & command line.
- Roles are universal — you can use them in any region.