

Services → IAM →

aws Services Resource Groups

Search IAM

Welcome to Identity and Access Management

AM users sign-in link: <https://673164704829.signin.aws.amazon.com/console>

Groups: 1 Roles: 6

Users: 1

Customer Managed Policies: 0

Security Status 3 out of 5 complete.

- ✓ Delete your root access keys
- ⚠ Activate MFA on your root account
- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- ⚠ Apply an IAM password policy

Search IAM

Users > Developer1

Summary

User ARN: am:aws:iam::673164704829:user/Developer1

Path: /

Creation time: 2018-06-05 10:07 UTC+0100

Permissions Groups (1) Security credentials Access Advisor

Add permissions Attached policies: 1

Policy name Policy type

Attached from group

Administrator Access

AWS managed policy from group Developers

Add inline policy

Search IAM

Add user Delete user

Find users by username or access key

Showing 1 result

User name	Groups	Access key age	Password age	Last activity	MFA
Developer1	Developers	Today	None	None	Not enabled

aws Services Resource Groups

Search IAM

User ARN: am:aws:iam::673164704829:user/Developer1

Path: /

Creation time: 2018-06-05 10:07 UTC+0100

Permissions Groups (1) Security credentials Access Advisor

Sign-in credentials

Console password Disabled Manage password

Console login link N/A

Last login None

Assigned MFA device No

Signing certificates None

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. Learn more

Create access key

Access key ID	Created	Last used	Status
AKIAIMJAO3INFPDGHFA	2018-06-05 10:19 UTC+0100	N/A	Active

SSH keys for AWS CodeCommit

Use SSH public keys to authenticate access to AWS CodeCommit repositories. Learn more

Upload SSH public key

SSH key ID	Uploaded	Status
------------	----------	--------

Creating Roles

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Entropy on keys

1

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles

Create role

Delete role

Showing 6 results

Role name	Description	Trusted entities
<input type="checkbox"/> aws-codestar-service-role		AWS service: codestar
<input type="checkbox"/> aws-serverless-repository-alexaskilskitowto...		AWS service: lambda
<input type="checkbox"/> aws-serverless-repository-alexaskilskitodej...		AWS service: lambda
<input type="checkbox"/> aws-serverless-repository-alexaskilskitodej...		AWS service: lambda
<input type="checkbox"/> AWSServiceRoleForElasticLoadBalancing	Allows ELB to call AWS services on your behalf.	AWS service: elasticloadbalancing (Service-...

2

Create role

Select type of trusted entity

AWS service

Another AWS account

Web identity

SAML 2.0 federation

Choose the service that will use this role

EC2

Lambda

API Gateway

AppSync

Application Auto Scaling

Auto Scaling

Batch

CloudFormation

CloudHSM

CloudWatch Events

CodeBuild

CodeDeploy

Config

DMS

Data Pipeline

DeepLens

Directory Service

DynamoDB

EC2

EC2 - Fleet

EMR

ElastiCache

Elastic Beanstalk

Elastic Container Service

Elastic Transcoder

ElasticLoadBalancing

Glue

Greengrass

GuardDuty

Inspector

IoT

Kinesis

Lambda

Lex

Machine Learning

MediaConvert

OpsWorks

RDS

Redshift

Rekognition

S3

SMS

SNS

SWF

SageMaker

Service Catalog

Step Functions

Storage Gateway

* Required

Cancel

Next: Permissions

3

Create role

Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Refresh

Filter: Policy type

Showing 4 results

Policy name	Attachments	Description
<input type="checkbox"/> AmazonDMSRedshiftS3Role	0	Provides access to manage S3 settings for Redshift endpoint...
<input checked="" type="checkbox"/> AmazonS3FullAccess	0	Provides full access to all buckets via the AWS Management...
<input type="checkbox"/> AmazonS3ReadOnlyAccess	0	Provides read only access to all buckets via the AWS Manag...
<input type="checkbox"/> QuickSightAccessForS3StorageManagement...	0	Policy used by QuickSight team to access customer data pr...

Policies > AmazonS3FullAccess

Summary

Policy ARN

Description

Permissions

Attached entities (0)

Policy versions

Access Advisor

Policy summary

{JSON}

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": "s3:*",
7-       "Resource": "*"
8-     }
9-   ]
10- }
```

* Required

aws

Services

Resource Groups

A Cloud Guru 2018

Create role

123

Review

Provide the required information below and review this role before you create it.

Role name*

MyS3AdminAccess

Use alphanumeric and '+, @, _' characters. Maximum 64 characters.

Role description

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+, @, _' characters.

Trusted entities

AWS service: ec2.amazonaws.com

Policies

AmazonS3FullAccess

* Required

aws

Services

Resource Groups

A Cloud Guru 2018

Global

Support

Create roleDelete role

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Search

Showing 7 results

Role name	Description	Trusted entities
<input type="checkbox"/> aws-codestar-service-role		AWS service: codestar
<input type="checkbox"/> aws-serverless-repository-alexaskitsho...		AWS service: lambda
<input type="checkbox"/> aws-serverless-repository-alexaskitnodej...		AWS service: lambda
<input type="checkbox"/> aws-serverless-repository-alexaskitnodej...		AWS service: lambda
<input type="checkbox"/> AWSServiceRoleForElasticLoadBalancing	Allows ELB to call AWS services on your behalf.	AWS service: elasticloadbalancing (Service-...
<input type="checkbox"/> myLambdaRole	Allows Lambda functions to call AWS services on your behalf.	AWS service: lambda
<input type="checkbox"/> MyS3AdminAccess	Allows EC2 instances to call AWS S3 on your behalf.	AWS service: ec2

aws Services Resource Groups

Launch Instance

Filter by tags and attributes or search

Actions

- Connect
- Get Windows Password
- Launch More Like This
- Instance State
 - Instance Settings
 - Add/Edit Tags
 - Attach to Auto Scaling Group
 - Attach/Replace IAM Role
 - Change Instance Type
 - Change Termination Protection
 - View/Change User Data
 - Change Shutdown Behavior
 - Change T2 Unlimited
 - Get System Log
 - Get Instance Screenshot
 - Modify Instance Profile
- Image
- Networking
- CloudWatch Monitoring

Name	Instance ID	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
	i-04931d2ef877c108f	us-east-1c	running	2/2 checks ...	None	ec2-35-153-184-58.co...	35.153.184.58	-

Instance: i-04931d2ef877c108f Public DNS: ec2-35-153-184-58.compute-1.amazonaws.com

Description Status Checks Monitoring Tags

Property	Value	Property	Value
Instance ID	i-04931d2ef877c108f	Public DNS (IPv4)	ec2-35-153-184-58.compute-1.amazonaws.com
Instance state	running	IPv4 Public IP	35.153.184.58
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs	-	Private DNS	ip-172-31-36-54.ec2.internal
Availability zone	us-east-1c	Private IPs	172.31.36.54
Security groups	MyWebDMZ, view inbound rules	Secondary private IPs	-

Attaching IAM role to EC2 instance

Instances > Attach/Replace IAM Role

Attach/Replace IAM Role

Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM console. If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID i-04931d2ef877c108f ⓘ

IAM role* MyS3AdminAccess ⓘ Create new IAM role ⓘ

Cancel Apply

1

```
[root@ip-172-31-36-54 ec2-user]# aws s3 ls

An error occurred (InvalidAccessKeyId) when calling the ListBuckets operation: The AWS Access key id you provided does not exist in our records.
[root@ip-172-31-36-54 ec2-user]# aws s3 ls

An error occurred (InvalidAccessKeyId) when calling the ListBuckets operation: The AWS Access Key Id you provided does not exist in our records.
[root@ip-172-31-36-54 ec2-user]# cd ~/.aws
[root@ip-172-31-36-54 .aws]# ls
config  credentials
[root@ip-172-31-36-54 .aws]# rm credentials
rm: remove regular file 'credentials'? y
[root@ip-172-31-36-54 .aws]# rm config
rm: remove regular file 'config'? y
[root@ip-172-31-36-54 .aws]# ls
[root@ip-172-31-36-54 .aws]# cd /
[root@ip-172-31-36-54 /]#
```

Throws error because it has invalid keys
Deleting config and credentials from the root directory will help in accessing the s3 again
Accessing S3 using roles instead of access and secret key

2

```
[root@ip-172-31-36-54 /]# aws s3 ls
2018-06-05 09:09:28 acloudguru1234-rk
[root@ip-172-31-36-54 /]# aws s3 ls s3://acloudguru1234-rk
2018-06-05 09:10:35      18 hello.txt
[root@ip-172-31-36-54 /]# echo "Hello Cloud Gurus 2" > hello2.txt
[root@ip-172-31-36-54 /]# aws s3 cp hello2.txt s3://acloudguru1234-rk
upload: ./hello2.txt to s3://acloudguru1234-rk/hello2.txt
[root@ip-172-31-36-54 /]# aws s3 ls s3://acloudguru1234-rk
2018-06-05 09:10:35      18 hello.txt
2018-06-05 10:50:08     20 hello2.txt
[root@ip-172-31-36-54 /]#
```

AWS Documentation » AWS Command Line Interface » User Guide » Configuring the AWS CLI » Configuration and Credential Files

Configuration and Credential Files

The CLI stores credentials specified with `aws configure` in a local file named `credentials` in a folder named `.aws` in your home directory. Home directory location varies but can be referred to using the environment variables `%UserProfile%` in Windows and `$HOME` or `~` (tilde) in Unix-like systems.

For example, the following commands list the contents of the `.aws` folder:

Linux, macOS, or Unix

```
$ ls ~/.aws
```

Windows

```
> dir "%UserProfile%\aws"
```


EXAM TIPS



- Roles allow you to not use Access Key ID's and Secret Access Keys
- Roles are preferred from a security perspective
- Roles are controlled by policies
- You can change a policy on a role and it will take immediate affect
- You can attach and detach roles to running EC2 instances without having to stop or terminate these instances