

IAM Roles

aws

Search

[Alt+S]

United States (N. Virginia)

Account ID: 7057-3373-8044

Pratik AWS

EC2 > Instances

EC2

Dashboard

EC2 Global View

Events

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

CloudShell

Feedback

Instances (1/3) Info

Find Instance by attribute or tag (case-sensitive)

All states

Connect

Instance state

Actions

Launch instances

< 1 >

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	linux	i-0bd758a4c24188863	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1c
<input type="checkbox"/>	WebHostingSe...	i-084874d7d7479be4e	Stopped	t2.micro	-	View alarms +	us-east-1c
<input type="checkbox"/>	MigrationInsta...	i-02415f6e40c315dc7	Stopped	t2.micro	-	View alarms +	us-east-1c

i-0bd758a4c24188863 (linux)

IAM Role

Role1

Subnet ID

subnet-0bdb91041a0b80bad

Instance ARN

arn:aws:ec2:us-east-1:705733738044:instance/i-0bd758a4c24188863

Auto Scaling Group name

-

Managed

false

Learn more

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search

[Alt+S]

Global

Account ID: 7057-3373-8044

Pratik AWS

IAM > Roles

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

CloudShell

Feedback

Roles (1/3) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

< 1 >

	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
<input checked="" type="checkbox"/>	Role1	AWS Service: ec2	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

Manage

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search

[Alt+S]

Global

Account ID: 7057-3373-8044

Pratik AWS

IAM > Roles > Role1

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

CloudShell

Feedback

Creation date

September 12, 2025, 12:58 (UTC+05:30)

ARN

arn:aws:iam:705733738044:role/Role1

Instance profile ARN

arn:aws:iam:705733738044:instance-profile/Role1

Last activity

-

Maximum session duration

1 hour

Permissions

Trust relationships

Tags

Last Accessed

Revoke sessions

Permissions policies (1/2) Info

You can attach up to 10 managed policies.

Filter by Type

Search

All types

< 1 >

	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	1
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	1

Permissions boundary (not set)

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences