

IDENTITY ACCESS MANAGEMENT

AWS IAM (Identity and Access Management) is a service that helps you securely control access to AWS services and resources. It allows you to manage users, groups, roles, and permissions to ensure that only authorized users can perform specific actions.

EC2 INSTANCES

Amazon EC2 (Elastic Compute Cloud) is a service that lets you run virtual servers in the cloud, giving you flexible, scalable computing power. You can quickly launch and manage instances to meet your needs and only pay for the resources you use.

STEP 1 Launch EC2 instance – Amazon Linux

The screenshot shows the 'Launch an instance' page in the AWS Management Console. The page is divided into two main sections: configuration on the left and a summary on the right.

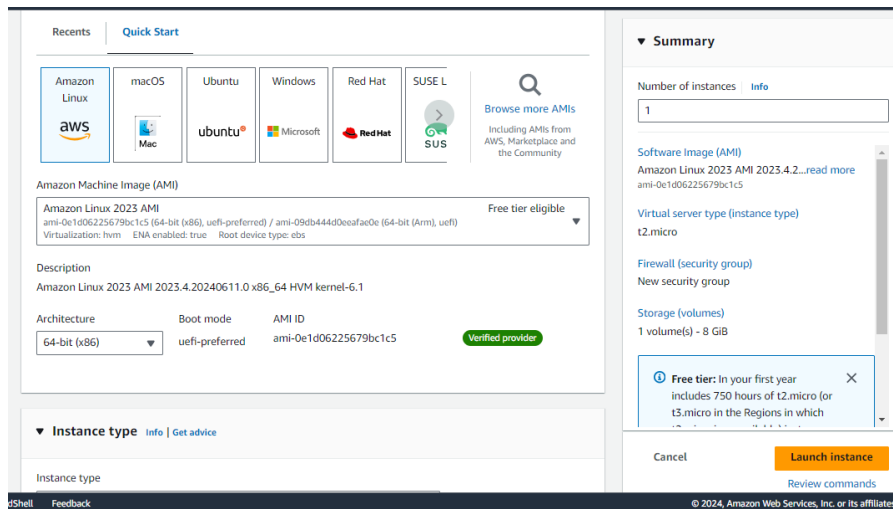
Left Section: Launch an instance

- Name and tags:** A text box contains 'iam pri'. A link 'Add additional tags' is to the right.
- Application and OS Images (Amazon Machine Image):** A search bar with the placeholder text 'Search our full catalog including 1000s of application and OS images'. Below the search bar are 'Recents' and 'Quick Start' tabs.

Right Section: Summary

- Number of instances:** A dropdown menu set to '1'.
- Software Image (AMI):** 'Amazon Linux 2023 AMI 2023.4.2...read more' with the ID 'ami-0e1d06225679bc1c5'.
- Virtual server type (instance type):** 't2.micro'.
- Firewall (security group):** 'New security group'.
- Storage (volumes):** '1 volume(s) - 8 GiB'.
- Free tier:** A blue box with a close button (X) stating: 'Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which...)'.
- Buttons:** 'Cancel' and 'Launch instance' (in orange). A link 'Review commands' is below the 'Launch instance' button.

Footer: '© 2024, Amazon Web Services, Inc. or its affiliates.'



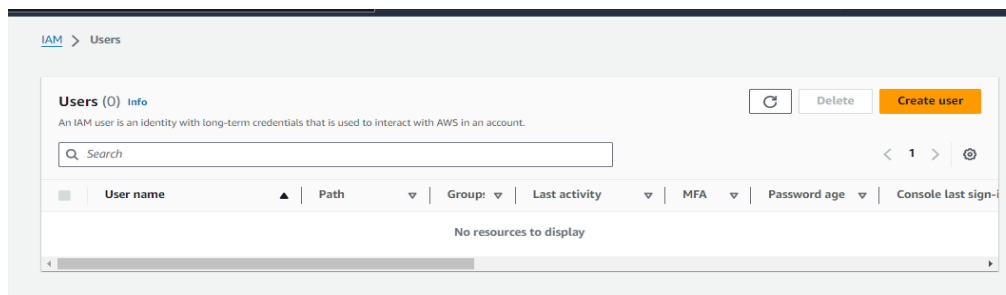
STEP 2 successfully created

Instances (1/1) Info							
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/> All states < 1 > ⓘ							
<input checked="" type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	iam pri	i-0d5376bca06588084	Running	t2.micro	-	View alarms	ap-south-1a

USER

In AWS IAM, a user is an entity that represents a person or service needing access to AWS resources. Users are assigned permissions through policies, allowing them to perform specific actions within AWS.

STEP 1 create user



[CloudShell](#)
[Feedback](#)

 © 2024, Amazon Web Services, Inc. or its affiliates.
 [Privacy](#)
[Terms](#)
[Cookie preferences](#)

cloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

[budShell](#)
[Feedback](#)

[© 2024, Amazon Web Services, Inc. or its affiliates.](#)
[Privacy](#)
[Terms](#)
[Cookie preferences](#)

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

IAM > Users > Create 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 view and download this password.

Console sign-in details

Email sign-in instructions

Console sign-in URL

https://637423530978.signin.aws.amazon.com/console

User name

ram

Console password

***** Show

Cancel

Download .csv file

Return to users list

STEP 2 let's try to login using IAM user



Sign in as IAM user

Account ID (12 digits) or account alias

637423530978

IAM user name

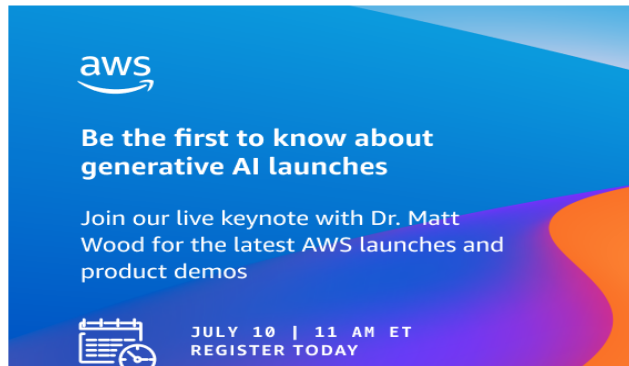
ram

Password

☒ Remember this account

Sign in

Sign in using root user email



Services

Search

[Alt+S]

Mumbai

ram @ 6374-2353-0978

Console Home

Recently visited

Billing and Cost Management

S3

IAM

EC2

View all services

Applications (0)

Region: Asia Pacific (Mumbai)

ap-south-1 (Current Region)

Find applications

Name

Description

Region

Access denied

Go to my Applications

Welcome to AWS

AWS Health

Cost and usage

Account

Organization

Service Quotas

Billing and Cost Management

Security credentials

Switch role

Sign out

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

STEP 1 connect the EC2 instance using ssh client



IAM > Users > ram

ramInfoDelete

Summary

ARN
arn:aws:iam::637423530978:user/ram

Created
June 13, 2024, 15:08 (UTC+05:30)

Console access
Enabled without MFA

Console sign-in
Today

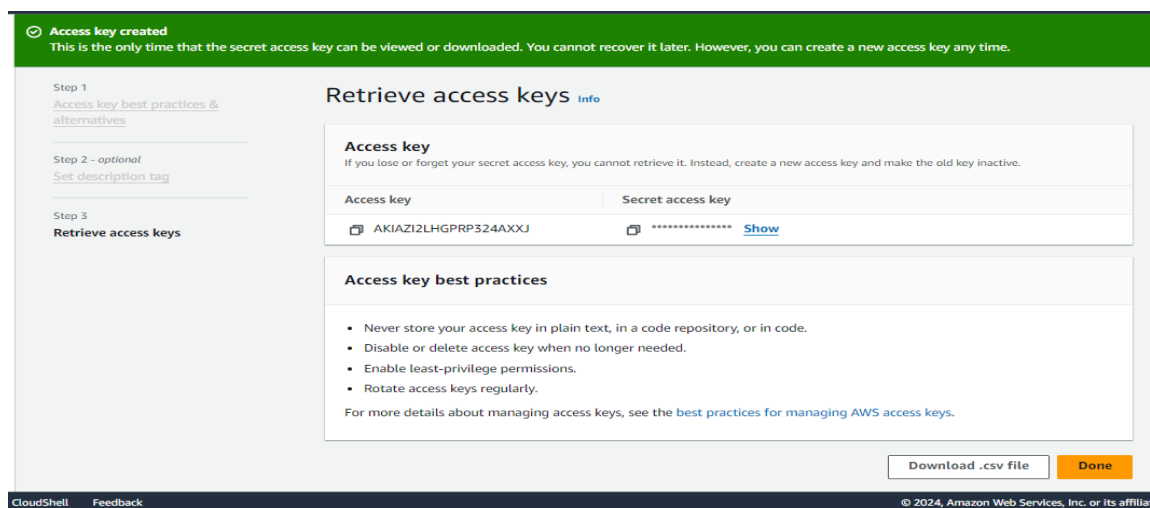
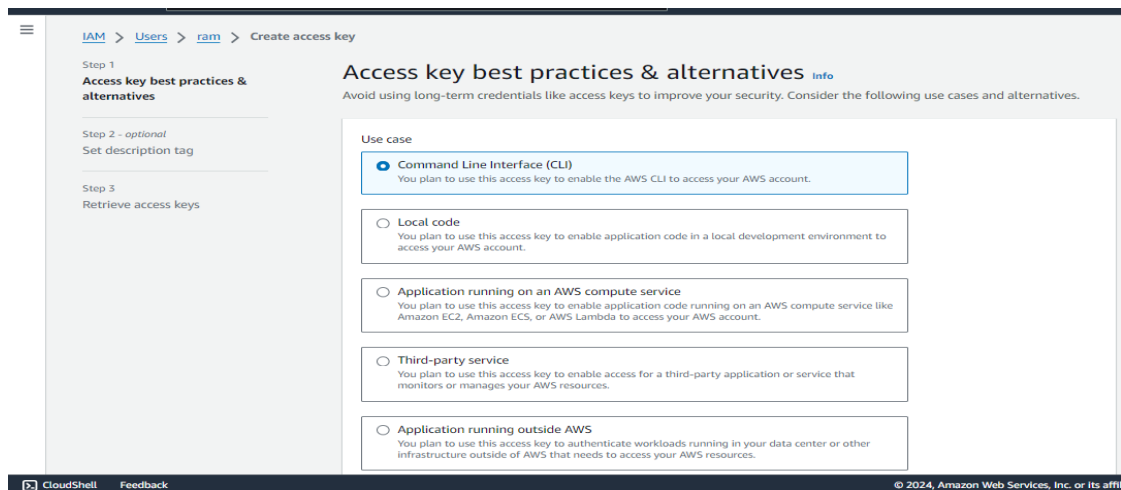
Access key 1
Create access key

Permissions | Groups | Tags | Security credentials | Access Advisor

Console sign-inManage console access

Console sign-in link
https://637423530978.signin.aws.amazon.com/console

Console password
Updated 4 minutes ago (2024-06-13 15:08 GMT+5:30)
Last console sign-in
3 minutes ago (2024-06-13 15:09 GMT+5:30)



```
[ec2-user@ip-172-31-37-100 ~]$ aws configure
AWS Access Key ID [None]: AKIAZI2LHGPRP324AXXJ
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: json
[ec2-user@ip-172-31-37-100 ~]$
```

User Groups

In AWS IAM, a user group is a collection of IAM users that you can manage as a single unit. By assigning permissions to a user group, all users in the group inherit those permissions, simplifying access management.

STEP 1 create user group

[IAM](#) > [User groups](#) > Create user group

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+','=','_' characters.

Add users to the group - *Optional* (1/1) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

< 1 >

☒ User name [?](#)

Groups

Last activity

Creation time

☒ ram

0

10 minutes ago

11 minutes ago

Attach permissions policies - *Optional* (928) [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

© 2024, Amazon Web Services, Inc. or its affiliates.

[Privacy](#)

[Terms](#)

[Cookie preferences](#)

developer user group created.

[View group](#)

[IAM](#) > [User groups](#)

User groups (1/1) [Info](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

< 1 >

☒ Group name

Users

Permissions

Creation time

☒ developer

1

Defined

Now

Add or remove users

[IAM](#) > [User groups](#) > developer

developer [Info](#)

Summary

User group name

Creation time

ARN

developer

June 13, 2024, 15:20 (UTC+05:30)

arn:aws:iam::637423530978:group/developer

Users (1)

Permissions

Access Advisor

Users in this group (1/1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

< 1 >

☒ User name [?](#)

Groups

Last activity

Creation time

☒ ram

1

12 minutes ago

13 minutes ago

© 2024, Amazon Web Services, Inc. or its affiliates.

[Privacy](#)

[Terms](#)

[Cookie preferences](#)

Roles

In AWS, roles are a way to grant permissions to entities like EC2 instances, Lambda functions, or users, allowing them to perform specific actions on AWS resources. They use temporary security credentials and can be assumed by trusted entities, enabling secure and controlled access.

STEP 1 create role

The image shows two screenshots from the AWS IAM console. The top screenshot displays the 'Roles' page, which lists existing roles and provides options to create a new role. The bottom screenshot shows the 'Select trusted entity' step of the role creation process, where the user selects the trusted entity type and the use case.

Roles (5)

Role name	Trusted entities	Last activity
aws-ec2-spot-fleet-tagging-role	AWS Service: spotfleet	8 days ago
AWSServiceRoleForEC2Spot	AWS Service: spot (Service-Linked Role)	-
AWSServiceRoleForEC2SpotFleet	AWS Service: spotfleet (Service-Linked Role)	8 days ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-

Roles Anywhere

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

Access AWS from your non AWS | X.509 Standard | Temporary credentials

Select trusted entity

Trusted entity type

- ☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case:

Choose a use case for the specified service.

Use case: ☒ **EC2**

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

Permissions policies (3/928) Info

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

Filter by Type

All types

< 1 2 3 4 5 6 7 ... 47 > ⚙

<input type="checkbox"/>	Policy name <small>🔗</small>	Type	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	Provides full access to AWS services an...
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	Grants account administrative permis...
<input type="checkbox"/>	AdministratorAccess-AWSElasticBean...	AWS managed	Grants account administrative permis...
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	Provide device setup access to AlexaFo...
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	Grants full access to AlexaForBusiness ...
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	Provide gateway execution access to A...
<input type="checkbox"/>	AlexaForBusinessLifsizeDelegatedAc...	AWS managed	Provide access to Lifesize AVS devices
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAcces...	AWS managed	Provide access to Poly AVS devices

oudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and "+-.,@_:" characters.

Description

Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: "_+,:@-./\[\]{}\$%&'\"`<>`

Step 1: Select trusted entities

Edit

Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": {  

```

oudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Role teamleader created. View role ✕

Roles (1/6) Info

🔄 Delete Create role

< 1 > ⚙

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
<input checked="" type="checkbox"/>	teamleader	AWS Service: ec2	-

AWS S3

Amazon S3 (Simple Storage Service) is a scalable cloud storage service that allows you to store and retrieve large amounts of data at any time. It offers secure, durable, and highly available object storage, ideal for backups, data archiving, and content distribution.

STEP 1 S3 - bucket - create bucket

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region
Asia Pacific (Mumbai) ap-south-1

Bucket name Info

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ ACLs disabled (recommended) ☐ ACLs enabled

cloudShell Feedback

☑ Successfully created bucket "priyabucket1203"

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

[View details](#)

Amazon S3 > Buckets

► Account snapshot - updated every 24 hours All AWS Regions

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)

General purpose buckets | Directory buckets

General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

< 1 > ⌕

Name	AWS Region	IAM Access Analyzer	Creation date
priyabucket1203	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 13, 2024, 15:25:52 (UTC+05:30)

EC2- Modify IAM Role

STEP 1 modify IAM role

The screenshot shows the AWS Management Console 'Instances' page. A table lists instances, with 'iam pri' (ID: i-Od5376bca06588084) in a 'Running' state. The 'Actions' dropdown menu is open, showing options like 'Connect', 'View details', and 'Modify IAM role', which is highlighted.

The screenshot shows the 'Modify IAM role' page. It displays the instance ID 'i-Od5376bca06588084' and the current IAM role 'teamleader'. There is a 'Create new IAM role' link and an 'Update IAM role' button.

The screenshot shows a green success message: 'Successfully attached teamleader to instance i-Od5376bca06588084'. Below the message, the instance table is visible, showing the instance 'iam pri' with the 'teamleader' role.

STEP 2 Open command prompt

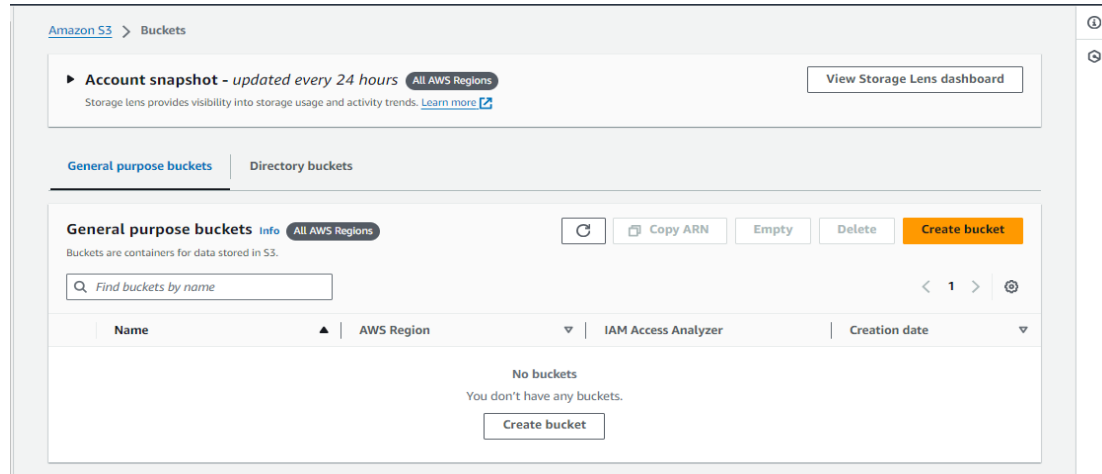
```
[ec2-user@ip-172-31-37-100 ~]$ aws configure
AWS Access Key ID [*****AXXJ]: AKIAZI2LHGPRP324AXXJ
AWS Secret Access Key [*****Lpdk]: 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
Default region name [ap-south-1]: ap-south-1
Default output format [json]: json
[ec2-user@ip-172-31-37-100 ~]$ sudo yum install awscli
Last metadata expiration check: 0:26:20 ago on Thu Jun 13 09:36:30 2024.
Package awscli-2.2.15.30-1.amzn2023.0.1.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-172-31-37-100 ~]$

[ec2-user@ip-172-31-37-100 ~]$ aws s3 ls
2024-06-13 09:55:53 priyabucket1203
[ec2-user@ip-172-31-37-100 ~]$
```

STEP 3 Removing bucket through commands

```
[ec2-user@ip-172-31-37-100 ~]$ aws s3 rb s3://priyabucket1203
remove_bucket: priyabucket1203
[ec2-user@ip-172-31-37-100 ~]$
```

STEP 4 open AWS S3 to check the bucket whether removed or not



After, completing the task terminate the instance

