

## **AWS MODULE**

Submitted by -ADESH ARUN ADHAV

Submitted to- VIKUL SIR

Batch no.-Devops SA2409031

DATE- 18/10/2024

L2 -Login to AWS Console and Create IAM User, Role, and Group

### **Step 1: Log in to the AWS Management Console**

1. Open the AWS management console.
2. Create your account in aws console by providing your details.
3. Enter your root account credentials to log in.

### **Step 2: Create an IAM User**

- 1.navigate the IAM service in aws console
- 2.click on add on user.
- 3.enter username detail and give the access to the user  
(for eg. Ec2 full access)

### **Step 3: Create a Group**

- 1.Clik on create group
2. Give group name
- 3.After creating group open the group and add the user to the group

### **STEP 4 : Create an IAM Role**

- 1.navigate to role services
- 2.clik on create the role
- 3.Attach policies to the role by giving permission

- Login to console

## Sign in

☒ **Root user**

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**

User within an account that performs daily tasks. [Learn more](#)

**Root user email address**

adeshadhav8484@gmail.com

**Next**

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

— New to AWS? —

**Create a new AWS account**

## Generative AI on Amazon SageMaker deep dive series

Learn how to scale foundation model development using purpose-built tools and infrastructure

**Watch now ›**

- Login credintial

 **Try the new sign in UI**

See our new improved Amazon Web Services sign in experience before we officially launch.

**Enable new sign in**



### Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

**Email address:** adeshadhav8484@gmail.com

**MFA code**

009810

**Submit**

[Troubleshoot MFA](#)

[Cancel](#)



## AWS Cloud Institute

Classes start January 6, 2025

**Enroll today >>**



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

English ▼

- IAM DASHBOARD

AWS

Services

Search

[Alt+S]

Global ▾

ADESH ADHAV ▾

EC2

Identity and Access Management (IAM)

X

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

IAM > Dashboard

IAM Dashboard

Refresh

Security recommendations 0

Refresh

Root user has MFA

Having multi-factor authentication (MFA) for the root user improves security for this account.

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

Refresh

User groups	Users	Roles	Policies	Identity providers
0	1	10	0	0

AWS Account

Account ID  
120569631866

Account Alias  
[Create](#)

Sign-in URL for IAM users in this account  
<https://120569631866.signin.aws.amazon.com/console>

Quick Links

[My security credentials](#)

Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

[Policy simulator](#)

The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Additional information

[Security best practices in IAM](#)

[IAM documentation](#)

[Videos, blog posts, and additional resources](#)

CloudShell Feedback

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

Updates for features in IAM

AWS IAM Access Analyzer now offers policy checks for public and critical resource access. 4 months ago

AWS IAM Access Analyzer now offers recommendations to refine unused access. 4 months ago

AWS Launches Console-based Bulk Policy Migration for Billing and Cost Management Console Access. 5 months ago

IAM Roles Anywhere now supports modifying the mapping of certificate attributes. 6 months ago

more

- CREATE USER

Set permissions

Step 3  
Review and create

Step 4  
Retrieve password

User name

ADESH

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ \_ - (hyphen)

☒ Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

**Are you providing console access to a person?**

User type

☐ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☐ Autogenerated password

You can view the password after you create the user.

☒ Custom password

Enter a custom password for the user.

\*\*\*\*\*

\* Must be at least 8 characters long

CloudShell Feedback

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

☐ Show password

☒ Users must create a new password at next sign-in - Recommended

Users automatically get the `IAMUserChangePassword` policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel

Next

User details		
User name	Console password type	Require password reset
ADESH	Custom password	Yes



- PERMISSION TO THE USER

Permissions policies (1/1241)

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

ec2

Filter by Type

All types

43 matches

	Policy name	Type	Attached entities
<input type="checkbox"/>	<a href="#">AmazonEC2ContainerRegistryFullA...</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2ContainerRegistryPowe...</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2ContainerRegistryPullO...</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2ContainerRegistryRead...</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2ContainerServiceAutosc...</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2ContainerServiceEvents...</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2ContainerServiceforEC2...</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2ContainerServiceRole</a>	AWS managed	0
<input checked="" type="checkbox"/>	<a href="#">AmazonEC2FullAccess</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2RoleforAWSCodeDeploy</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2RoleforAWSCodeDeplo...</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2RoleforDataPipelineRole</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2RoleforSSM</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2RolePolicyForLaunchWi...</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2SpotFleetAutoscaleRole</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonEC2SpotFleetTaggingRole</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonElasticMapReduceforEC2Role</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AmazonSSMManagedEC2InstanceD...</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AWSApplicationAutoscalingEC2Spo...</a>	AWS managed	0

► Set permissions boundary - optional

Cancel

Previous

Next

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

ADESH Info

Delete

Summary

ARN  
arn:aws:iam::120569631866:user/ADESH

Console access  
Enabled without MFA

Access key 1  
Create access key

Created  
October 18, 2024, 11:55 (UTC+05:30)

Last console sign-in  
Never

Permissions Groups Tags Security credentials Last Accessed

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
  - External access
  - Unused access
  - Analyzer settings

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type  
All types

Policy name	Type	Attached via
AmazonEC2FullAccess	AWS managed	Directly
IAMUserChangePassword	AWS managed	Directly

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

Generate policy

No requests to generate a policy in the past 7 days.

• CREATE GROUP

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

Create user group

Name the group

User group name  
Enter a meaningful name to identify this group.

aaaa

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

Add users to the group - *Optional* (2/3) [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.

Q Search

< 1 >

	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	<a href="#">aadesh</a>	0	None	56 minutes ago
<input checked="" type="checkbox"/>	<a href="#">ADESH</a>	1	None	1 hour ago
<input checked="" type="checkbox"/>	<a href="#">adhav</a>	1	None	1 hour ago

Attach permissions policies - *Optional* (955) [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.

[Alt+S]



Global ▾

ADESH ADH

<input type="checkbox"/>	Policy name	Type	Used as	Description
<input type="checkbox"/>	<a href="#">AdministratorAccess</a>	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services an...
<input type="checkbox"/>	<a href="#">AdministratorAccess-A...</a>	AWS managed	None	Grants account administrative permissi...
<input type="checkbox"/>	<a href="#">AdministratorAccess-A...</a>	AWS managed	None	Grants account administrative permissi...
<input type="checkbox"/>	<a href="#">AlexaForBusinessDevic...</a>	AWS managed	None	Provide device setup access to AlexaFor...
<input type="checkbox"/>	<a href="#">AlexaForBusinessFullA...</a>	AWS managed	None	Grants full access to AlexaForBusiness r...
<input type="checkbox"/>	<a href="#">AlexaForBusinessGate...</a>	AWS managed	None	Provide gateway execution access to AL...
<input type="checkbox"/>	<a href="#">AlexaForBusinessLifesi...</a>	AWS managed	None	Provide access to Lifesize AVS devices
<input type="checkbox"/>	<a href="#">AlexaForBusinessPoly...</a>	AWS managed	None	Provide access to Poly AVS devices
<input type="checkbox"/>	<a href="#">AlexaForBusinessRead...</a>	AWS managed	None	Provide read only access to AlexaForBu...
<input type="checkbox"/>	<a href="#">AmazonAPIGatewayA...</a>	AWS managed	None	Provides full access to create/edit/delet...



Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

aaaa Info

Delete

Summary

Edit

User group name

aaaa

Creation time

October 18, 2024, 12:03 (UTC+05:30)

ARN

arn:aws:iam::120569631866:group/aaaa

Users

Permissions

Last Accessed

Users in this group (2)

Remove

Add users

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

Search

< 1 >

☐

User name

Groups

Last activity

Creation time

☐

[ADESH](#)

1

None

44 minutes ago

☐

[adhav](#)

1

None

37 minutes ago

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

IAM

User groups

aaaa

aaaa Info

Delete

Summary

Edit

User group name

aaaa

Creation time

October 18, 2024, 12:03 (UTC+05:30)

ARN

arn:aws:iam::120569631866:group/aaaa

Users

Permissions

Last Accessed

Permissions policies (2)

Info

Simulate

Remove

Add permissions

You can attach up to 10 managed policies.

Search

Filter by Type

All types

< 1 >

☐

Policy name

Type

Attached entities

☐

[AmazonS3FullAccess](#)

AWS managed

1

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

Privacy

Terms

Cookie preferences

## • ROLE

### 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

EC2

Choose a use case for the specified service.

Use case

☒ **EC2**

Allows EC2 instances to call AWS services on your behalf.

☐ **EC2 Spot Fleet - AWS managed**

☐ **EC2 Spot Fleet Role**

Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

☐ **EC2 Spot Fleet Auto Scaling**

[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.

aaa

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

Description

Add a short explanation for this role.

Allows EC2 instances to call AWS services on your behalf.

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": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "sts:AssumeRole"
8       ],
9       "Principal": {
10        "Service": "ec2.amazonaws.com"
11      }
12    }
13  ]
14 }
```

aws

Services

Search

[Alt+S]

Global

ADESH ADHAV

EC2

15 }
16 }

Step 2: Add permissions

Edit

Permissions policy summary

Policy name	Type	Attached as
<a href="#">AdministratorAccess</a>	AWS managed - job function	Permissions policy

Step 3: Add tags

Add tags - optional

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create role

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

THANK YOU

