

[Home](#) / [AWS](#) / [Guided Lab](#) / [Creating IAM Roles](#)

Creating IAM Roles

Level: **Fundamental**

Identity And Access Management Amazon Web Services

Required Points

10

Lab Duration


00:30:00


Average Start time


Less than a minute

Start Lab →

Need help?

 How to use Hands on Lab


 Troubleshooting Lab


 FAQs

Submit Feedback

Share

Lab Overview

 Cloud Administrator

 Security

Lab Details:

1. This lab walks you through the steps to Create IAM Roles.
2. Duration: **30 minutes**

3. AWS Region: **US East (N. Virginia) us-east-1**

Introduction :

What is AWS IAM role ?

AWS IAM (Identity and Access Management) role is a security feature provided by Amazon Web Services (AWS) that enables you to manage access to AWS services and resources securely. IAM roles are used to delegate permissions to entities within your AWS environment, such as users, services, or applications, instead of using long-term access keys like usernames and passwords.

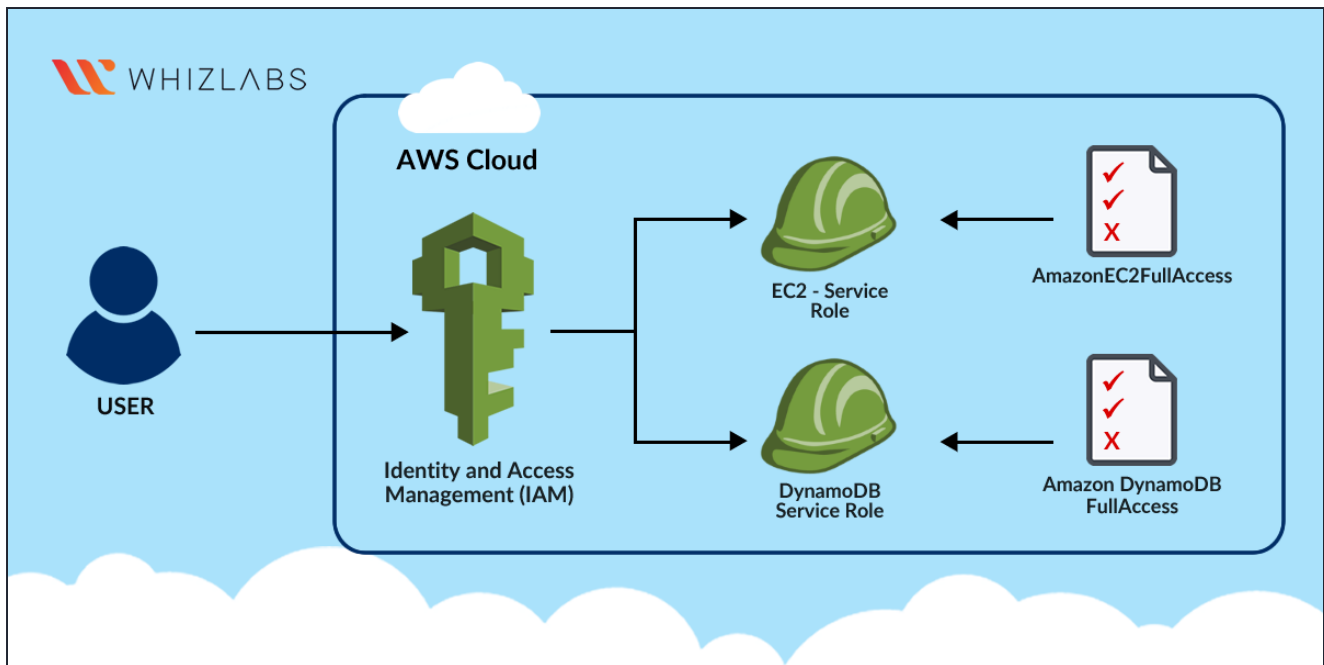
- IAM roles define a set of permissions that determine what actions can be performed on AWS resources. These permissions can be associated with AWS services, such as EC2 instances, Lambda functions, or S3 buckets, as well as with other AWS accounts. By assigning roles to entities, you can control their level of access and limit the need for sharing credentials.

IAM roles have several advantages over using access keys:

- Temporary credentials: IAM roles provide temporary security credentials that can be assumed by entities. These credentials have an expiration time, reducing the risk of unauthorized access.
- Least privilege access: You can assign fine-grained permissions to IAM roles, granting only the necessary access required for a specific task or service. This principle of least privilege enhances security by minimizing potential damage if credentials are compromised.
- Flexibility: IAM roles can be easily associated with multiple entities, allowing for centralized access management and reducing administrative overhead.
- Trust relationships: IAM roles can establish trust relationships with other AWS accounts or services, enabling cross-account or cross-service access. This is useful when you need to grant permissions to external entities or to enable services to access resources on your behalf.

Architecture Diagram:





Task Details:

1. Sign in to AWS Management Console
2. Create an IAM Role for EC2 service
3. Create an IAM Role for DynamoDB service.
4. Validation of the lab

Launching Lab Environment

1. To launch the lab environment, Click on the **Start Lab** button.
2. Please wait until the cloud environment is provisioned. It will take less than a minute to provision.
3. Once the Lab is started, you will be provided with **IAM user name, Password, Access Key, and Secret Access Key.**

Note : You can only start one lab at any given time

[About Us](#) [Subscription](#) [Instructions and Guidelines](#) [FAQ's](#) [Contact Us](#)



© 2024, Whizlabs Software Pvt. Ltd.

