

Introduction to AWS Identity Access Management (IAM)

Lab Details:

This lab will walk you through creating IAM users and adding them into IAM Groups.

Introduction

What is IAM?

- Stands for Identity and Access Management.
- Web Service that helps the user securely control access to AWS resources.
- Used to control who is authenticated and authorized to use AWS resources.
- Primary resources in IAM are users, groups, roles, policies, and identity providers.

Tasks:

- Log into AWS Management Console
- Create 4 IAM Users
- Create 2 IAM Groups
- Add IAM Users to different IAM Groups
- Attach IAM policies to the IAM Groups

Lab Steps:

Create New IAM User:

1. Click on Services and select IAM under the Security, Identity & Compliance section.
 2. Click Users in left panel and click Add User to create IAM user.
 3. In Add User section:
 - User Name: Sachin
 - Click on another user and provide: Saurav
- In Select AWS Access Type:
 - AWS Management Console access: **Check**
 - Programmatic access: **Uncheck**
 - Require password reset: Uncheck
 - Console password:
 - Auto Generated password: Uncheck
 - Check Custom password and Enter *****

Click on Next until you see Review tab and click on Create Users. (Ignore the error message and close). Similarly, add 2 more users let's say Karthik and Satya.

Create New IAM Group:

1. Select the Groups in left panel, and click on Create New Group.
2. Set Group Name as “Dev-Team” and click on Next Step.
3. Attach two policies: **AWS CodeDeployFullAccess & AWSCodeDeployRole**
4. Click on next step, review all the details and click on Create Group.
5. Follow the same steps and create new group as “HR-Team”.
6. Attach the Policy **Billing** to it and create the Group.

Adding an IAM User to an IAM Group:

1. Go to Groups and click on Dev-Team:
Click on Users and now click on “Add users to group” and select Sachin and Saurav
Repeat the same step to add Karthik and Satya to “HR-Team”