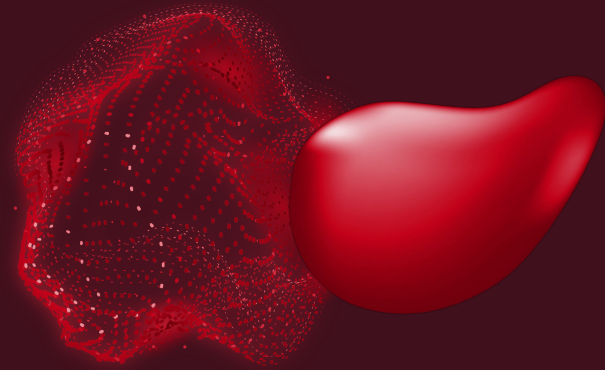


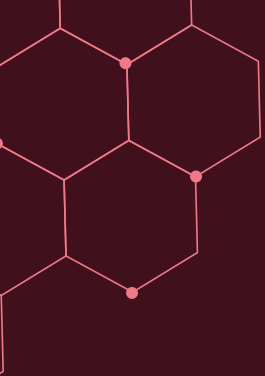
Identity and Access

Management (IAM)

Overview

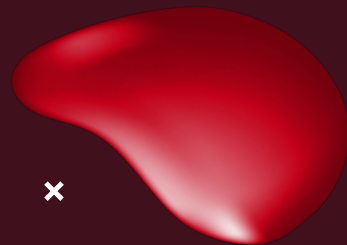
Securely managing access to AWS resources





x

TABLE OF CONTENTS



x

- 01** **Introduction**
- 02** **Key Features**
- 03** **Core Components**
- 04** **MFA**
- 05** **Best Practices**
- 06** **Hands-on Lab**

01

Introduction

What is IAM





Introduction

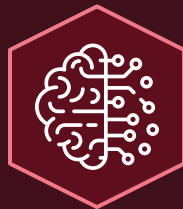
A web service that helps you securely control access to AWS resources for your users. IAM enables you to manage permissions and access control for AWS services and resources. With IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

Importance of IAM in Cloud Security



Centralized Access Control

IAM enables centralized management of access permissions, ensuring consistent application of security policies across all AWS resources.



Principle of Least Privilege

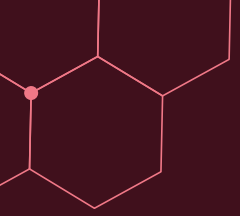
IAM allows you to grant only the necessary permissions to users and applications, reducing the risk of unauthorized access



Identity Federation

IAM supports integration with external identity providers, allowing seamless and secure access for users from external systems without the need to manage separate AWS credentials.





Opening Console

1)

AWS Console

2)

AWS CLI

3)

AWS SDKs



Access Keys

Access Key ID is the Username

Private Access Key ID is the Password

Protect CLI & SDKs



02

Key Features

Core functionalities and benefits

Key Features

- Centralized Control of AWS Account
- Granular Permissions
- Multi-Factor Authentication (MFA)
- Secure Access to AWS Resources
- Integration with Other AWS Services
- Temporary Security Credentials
- Identity Federation
- Auditing and Compliance





03

Core Components

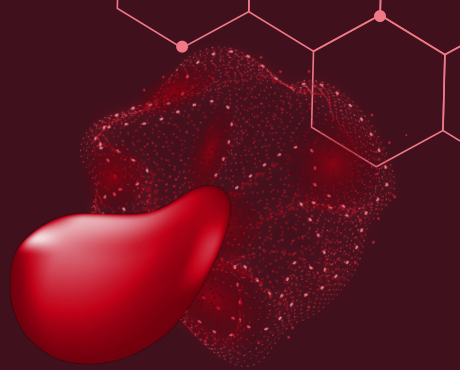
What can we do in IAM



x

Core Components

x



Unique identities for
individuals or applications

Users



Collections of users with
shared permissions

Groups



JSON documents
defining permissions

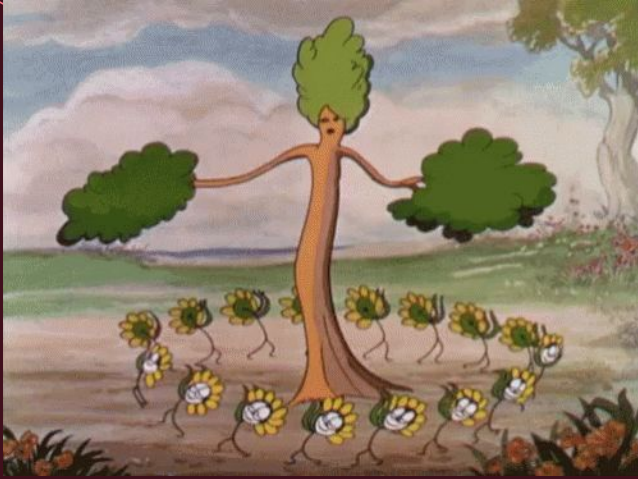
Policies



Temporary permissions
for access without
sharing credentials

x
Roles

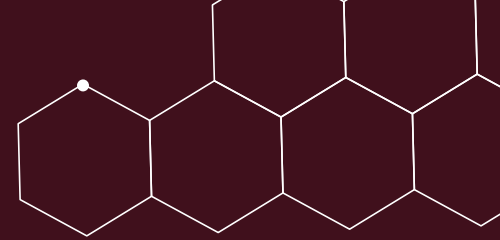




IAM Policy Inheritance

Users can belong to multiple groups, so the users can inherit the permissions from the groups they're in

```
{
  "Id": "Policy1721502044882",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1721502041403",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket/*",
      "Principal": "*"
    }
  ]
}
```



IAM Policy Structure



04

MFA

MFA Overview

Multi Factor Authentication



x

x

MFA

Extra layer of security using a
second authentication factor

For users with administrative
or high-privilege access

**Multi Factor
Authentication**
x

05

Best Practices

Best practices in Cloud Security



Best Practices

- Least Privilege Principle
- Use Groups to Assign Permissions
- Enable MFA for Privileged Users
- Regularly Review and Rotate

Credentials

- Use Roles for Applications
- Monitor and Audit IAM Activity





Best Practices

x

Least Privilege Principle

Granting the minimum necessary permissions

Using Groups and Roles

Simplifying permission management with groups

Monitoring and Auditing

Using AWS CloudTrail for auditing



Fine-Grained Permissions

who can access what resources and what actions they can perform

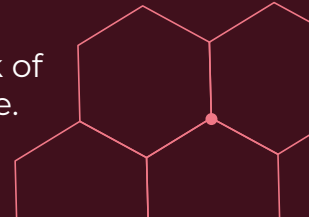
Enhanced Security Posture

organizations can significantly enhance their security posture, reducing the likelihood of security incidents

x

Temporary Credentials

reducing the exposure of long-term credentials and minimizing the risk of credential leakage.



x



06

Hands-on Lab

Open your AWS Console

Thank you!

Q/A Session

