



AWS IAM



Table of Contents



- ▶ Introduction to IAM
- ▶ IAM - Users
- ▶ IAM - Policies
- ▶ IAM - User Groups
- ▶ IAM - Roles



1

Introduction to IAM

Introduction to IAM

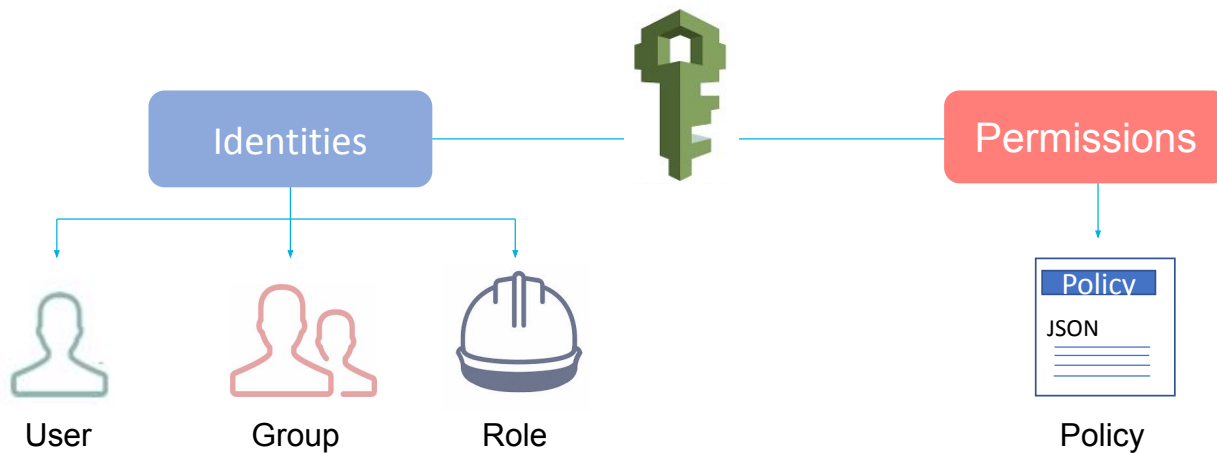
What is IAM?



- IAM stands for **Identity & Access Management**,
- IAM is the primary service that **handles authentication and authorization** processes within AWS environments.

Introduction to IAM

Categorizing IAM Components



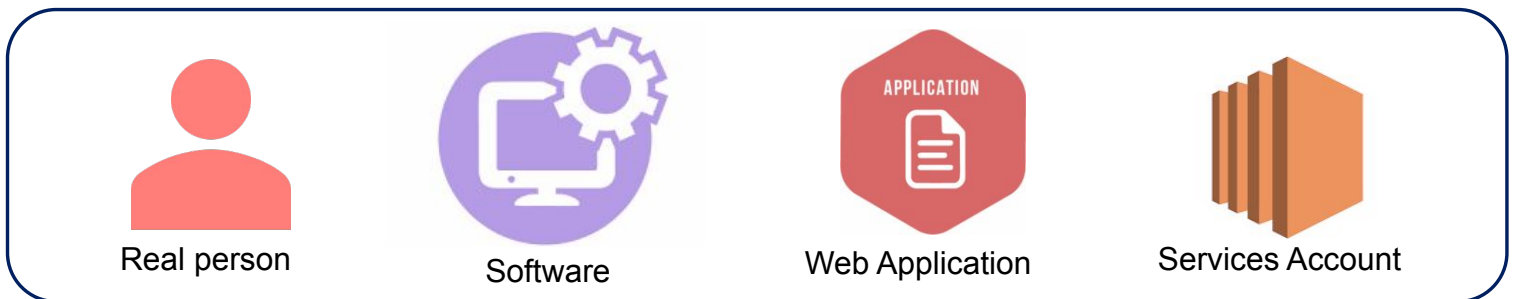
- IAM components can be mainly categorized under two terms; **Identities** and **Permissions**.

2 IAM Users

IAM Users

What is IAM User?

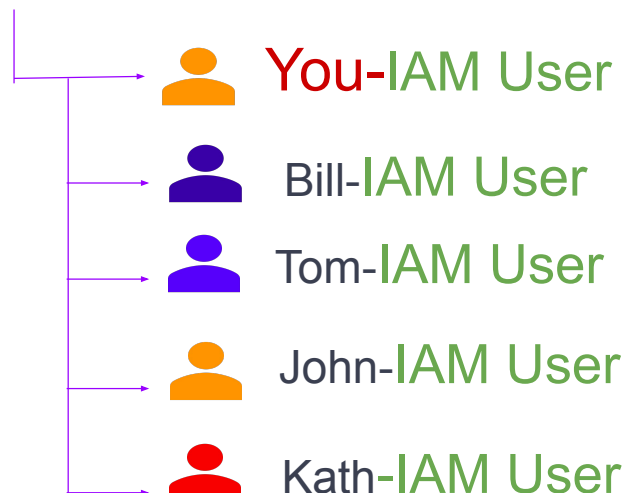
- An IAM user represents the person or service who uses AWS
- Who can be an IAM User? There are 4 types of user:



IAM Users

What is Root User and IAM User.

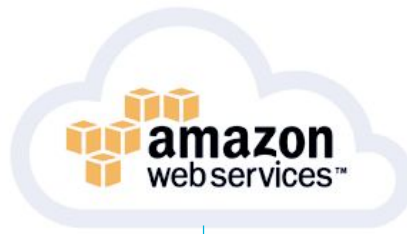
AWS Account Owner - Root User (you)



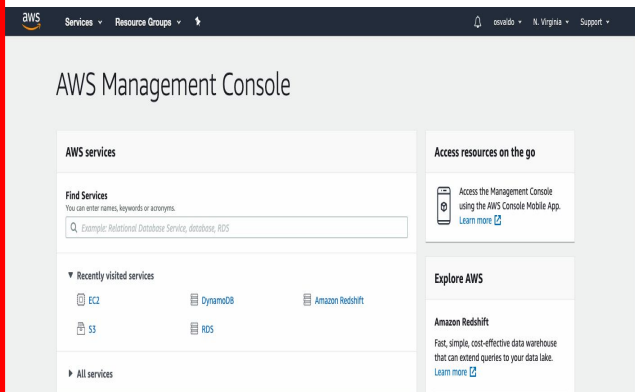
- Root User is a special user
- Username is **email** used to create account
- Generally, **cannot limit permissions** of Root User
- **Cannot delete** Root User
- Best practices:
 - **Enable MFA** for Root User
 - Don't use Root User for **day-to-day work**
 - Keep **password** in a secure location

IAM Users

Access Types

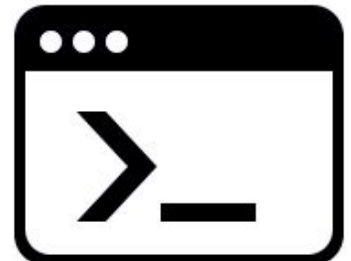


AWS Management Console



ROOT USER
IAM USER.

Programmatic Access



IAM Users

Sign in with Root User- AWS Management Console Access

aws

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

osvaldo@clarusway.com

Next



E-mail
Password

aws

Root user sign in

Email: osvaldo@clarusway.com

Password [Forgot password?](#)

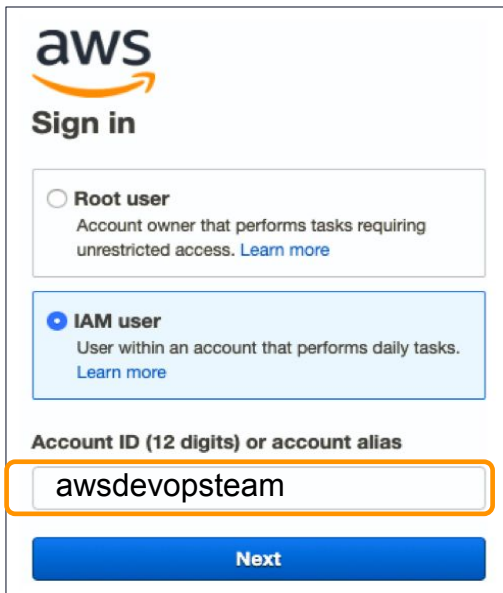
Sign in

[Sign in to a different account](#)

[Create a new AWS account](#)

IAM Users

Sign in with IAM User- AWS Management Console Access



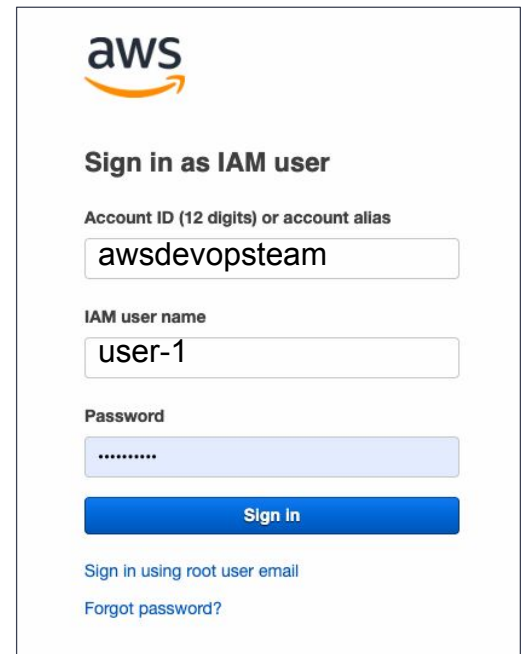
The AWS Sign in page shows two options: Root user and IAM user. The IAM user option is selected. Below the options is a text input field for the Account ID (12 digits) or account alias, containing 'awsdevopsteam'. A blue 'Next' button is at the bottom.



Account ID/Alias

User name

Password

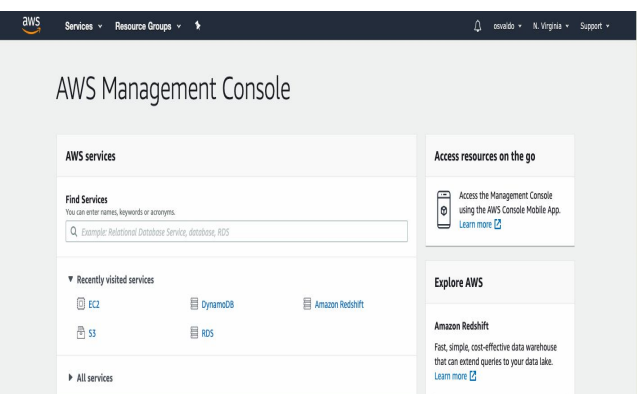


The 'Sign in as IAM user' page shows the same account alias 'awsdevopsteam' in the first field. The second field is for the IAM user name, containing 'user-1'. The third field is for the password, shown as dots. A blue 'Sign in' button is at the bottom.

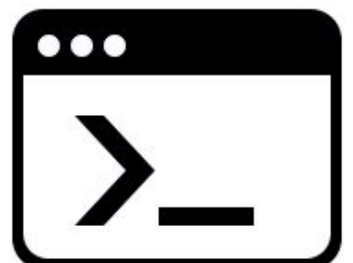
CLARUSWAY
WAY TO REINVENT YOURSELF



AWS Management Console



Programmatic Access



IAM Users

Sign in with IAM User- Programmatic Access

SDKs



Android



iOS



Java



JavaScript



.NET



Node.js



PHP



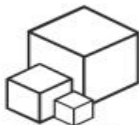
Python (boto)



Ruby



Xamarin



AWS CLI



AWS Toolkit
for Eclipse



AWS Toolkit
for Visual Studio



AWS Tools
for Windows
PowerShell

CLARUSWA
WAY TO REINVENT YOURSELF.

IAM Users

Sign in with IAM User- Programmatic Access

```
Last login: Fri Apr 24 22:44:56 on ttys000
Clarusway-MacBook-Air:- user$

Access Key ID !!!!

Secret Access Key !!!!
```



****ROOT USER**

IAM USER.

IAM Users

Sign in with IAM User- AWS CLI



YOUR TERMINAL



SECRET ACCESS KEY
ACCESS KEY ID



AWS CLI

3 IAM Policies

IAM Policies

What is a Policy?



- A policy is an object used to define the **permissions** of an identity or resource in AWS
- Permissions in the policies determine whether the request is **allowed** or **denied**.
- Policies are stored in AWS as **JSON** documents.

Policy Structure - E-PARC

Version

Specifies the version of the policy document so IAM knows how to parse it.

Statement

A list of statements with the elements below.

Effect

Either Allow or Deny.

Principal

The AWS principal associated with the policy.

Action

A list of valid actions defined by the permission.

Resource

The specific resource(s) associated with this permission.

Condition

Conditions associated with this permission.

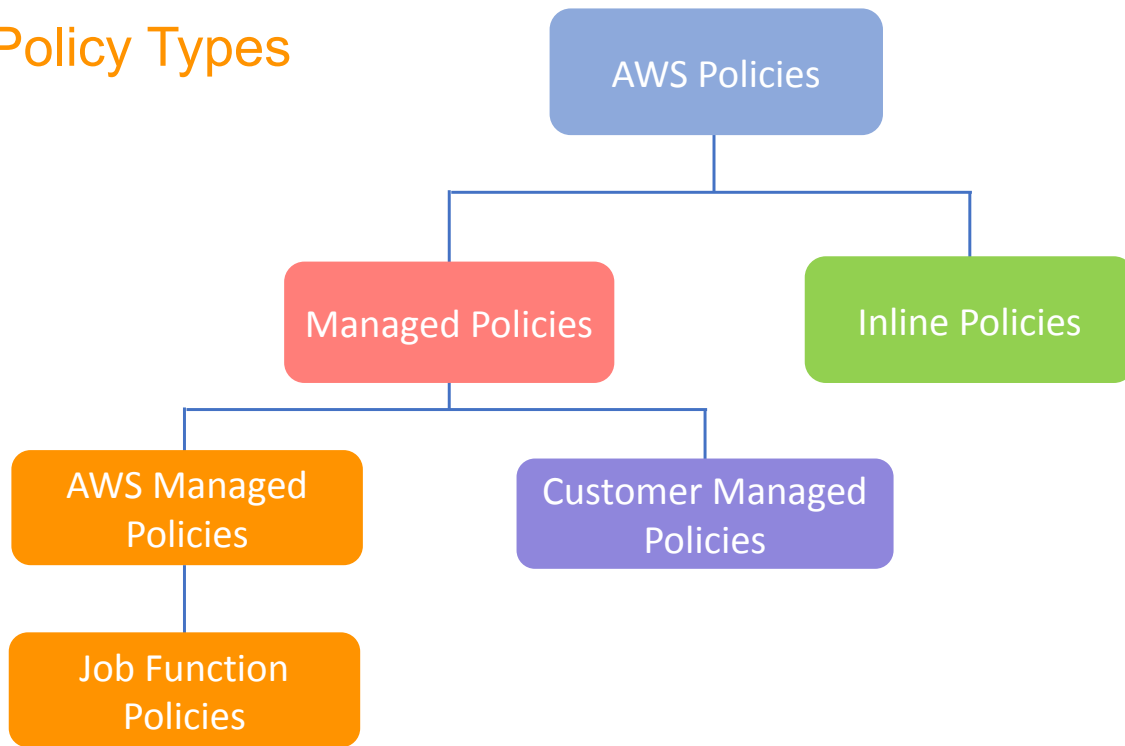


```
{  
  Version  
  Statement  
  [  
    Effect  
    Principal  
    Action  
    Resource  
    Condition  
  ]  
}
```

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AddCannedAcl",  
      "Effect": "Allow",  
      "Principal": { "AWS": [ "arn:aws:iam::111122223333:root" ] },  
      "Action": [ "s3:PutObject", "s3:PutObjectAcl" ],  
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",  
      "Condition": { "StringEquals": { "s3:x-amz-acl": [ "public-read" ] } }  
    }  
  ]  
}
```

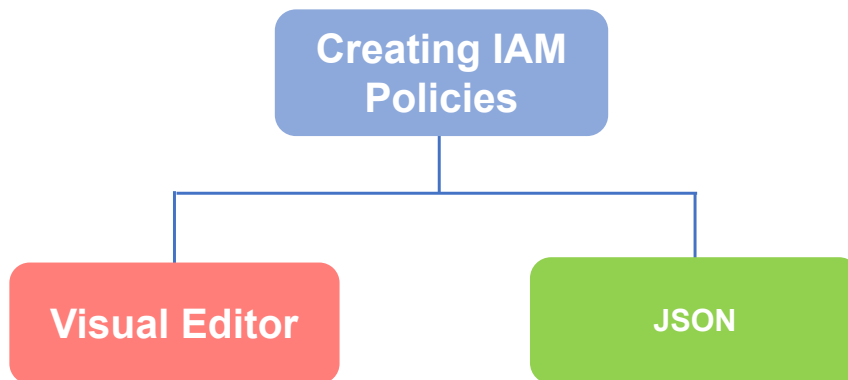
IAM Policies

IAM Policy Types



IAM Policies

Creating IAM Policies



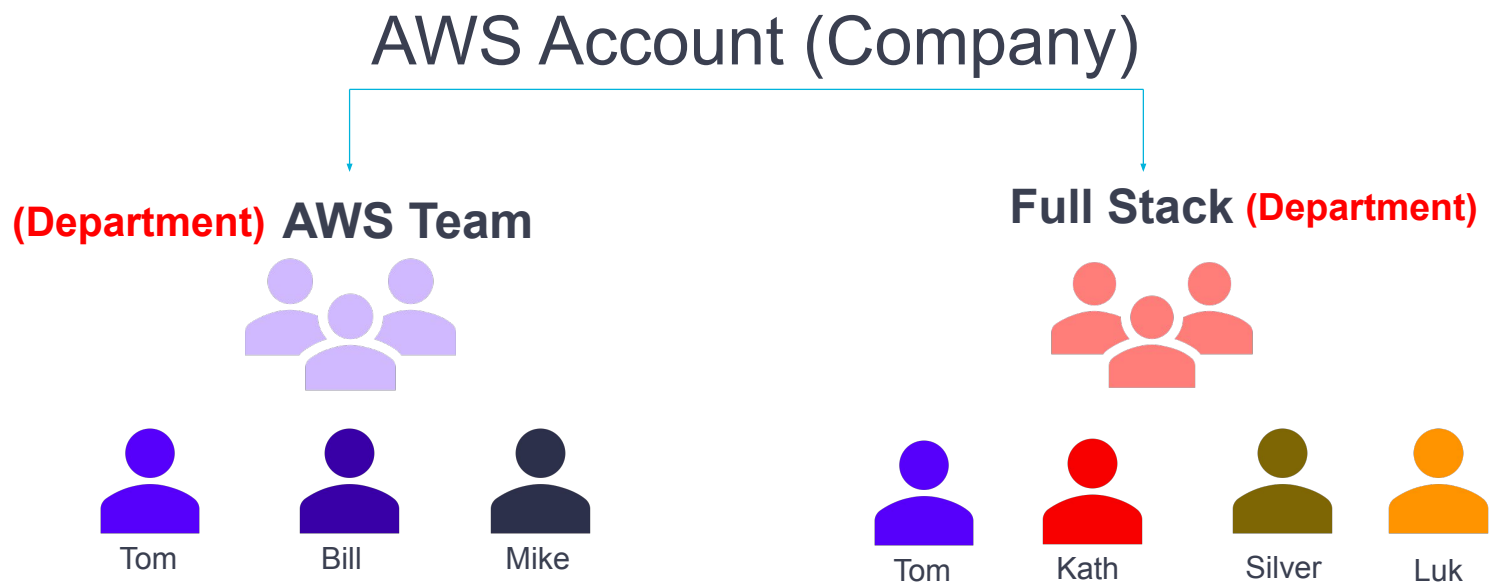


4 IAM Groups

CLARUSWAY
WAY TO REINVENT YOURSELF

IAM Groups

What is Group in AWS?



CLARUSWAY
WAY TO REINVENT YOURSELF

IAM Groups

IAM Group Features

Managed IAM policies can be attached to groups

Inline IAM policies can be added to groups

The limit of IAM users in a group is equal to 5000

User can be a member of 10 different IAM groups



5 IAM Roles

IAM Roles

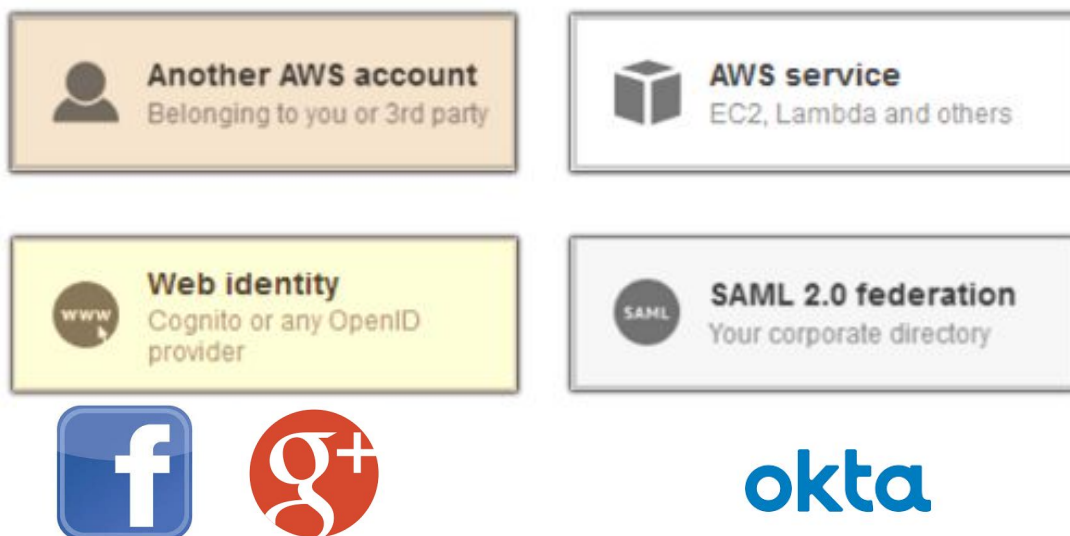
What is a Role in AWS?



- The authorization system where we determine how an identity can **access the AWS resources**.
- An IAM role, similar to an IAM user, is an IAM identity that **has specific permissions** that you can create in your account.

IAM Roles

Who can assume an IAM Role?



IAM Roles

What does IAM ROLE do ?

www.e-commerce...

What if you sold something?



Record:
-Customer info



IAM Roles

Anatomy of a Role



Trusted Entity

Use case

Permission Policy



AWS service
EC2, Lambda and others





Let's get our hands dirty!



THANKS!

Any questions?

You can find me at:

- @osvaldo
- osvaldo@clarusway.com

