

AWS IAM

CLARUSWAY
WAY TO REINVENT YOURSELF



▶ Introduction to IAM

What is IAM?

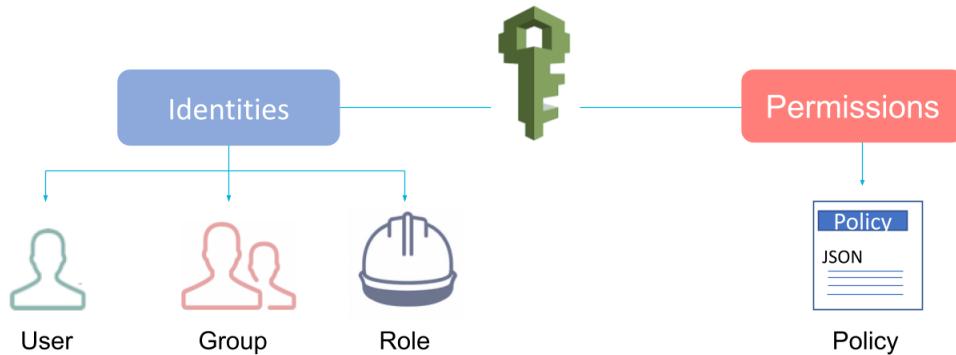


- IAM stands for **Identity & Access Management**,
- IAM is the primary service that **handles authentication and authorization** processes within AWS environments.

CLARUSWAY
WAY TO REINVENT YOURSELF

Introduction to IAM

Categorizing IAM Components



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

CLARUSWAY
WAY TO REINVENT YOURSELF

5

IAM Users

What is IAM User?

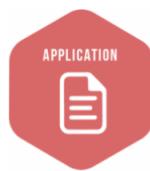
- An IAM user represents the person or service who uses AWS
- Who can be an IAM User? There are 4 types of user:



Real person



Software



Web Application



Services Account

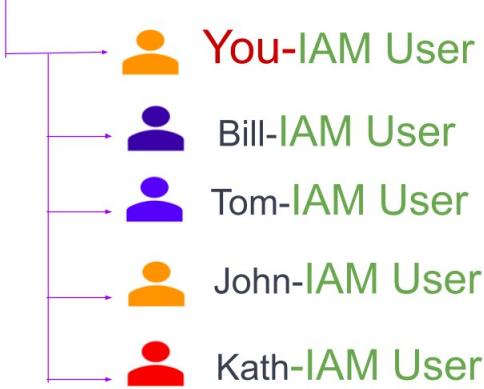
CLARUSWAY
WAY TO REINVENT YOURSELF

7

IAM Users

What is Root User and IAM User.

AWS Account Owner - **Root User (you)**

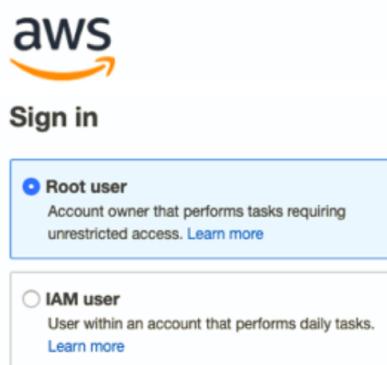


CLARUSWAY
WAY TO REINVENT YOURSELF

IAM Users

Sign in Options as User

- If you want to sign in to AWS, you have two options: **Root User** or **IAM User**.
- When you create an AWS account, you also create a root user identity account called **Root User**.
- After entering with Root User, you can create new user identities for both **for you and the other team members**. These are called **IAM users**.



IAM Users

Root User

- The AWS account owner is also a Root User.
- Root Users have complete access to all AWS services.
- Using your root account user for daily work is not recommended.
- Using the root user only to create new IAM users is considered best practice.



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

IAM Users

IAM User

- A root user can create new IAM users and give them authorization for using AWS services within the account.
- The limit of creating new IAM users is restricted to 5000 users per account.
- Even if you are an account owner, it's recommended to create an individual IAM user for yourself.



Sign in

Root user

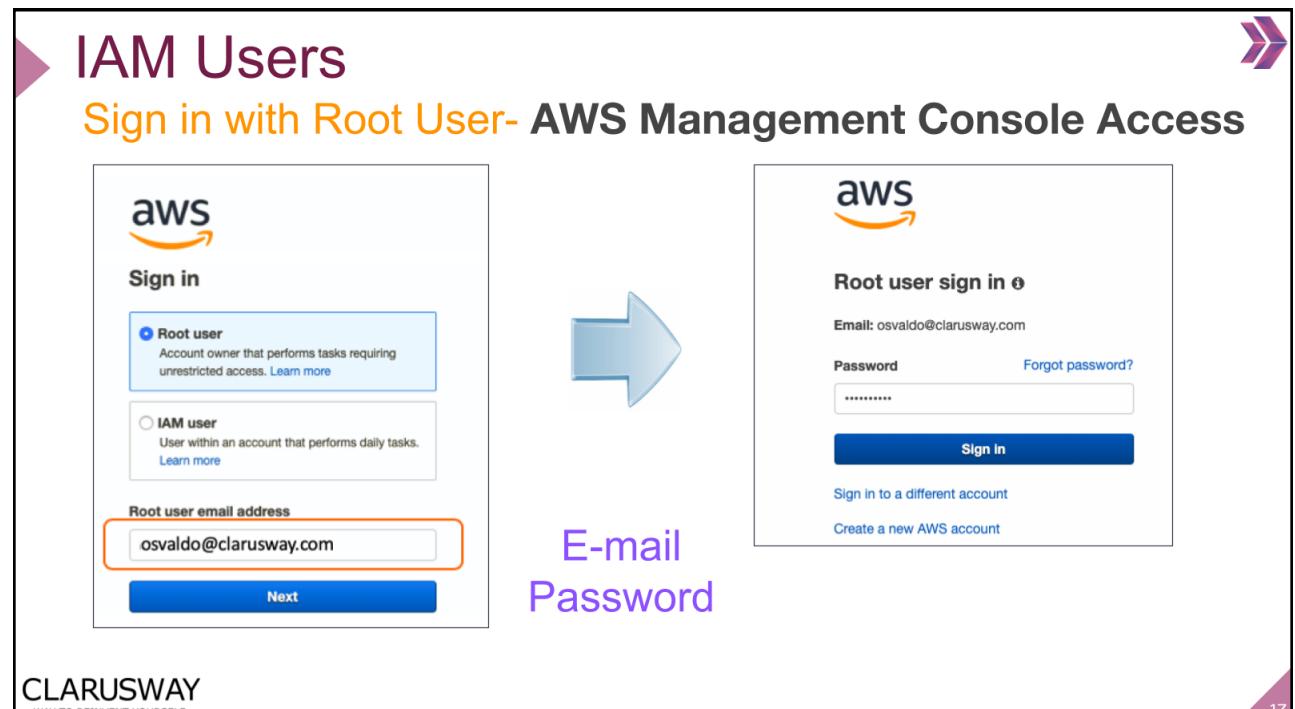
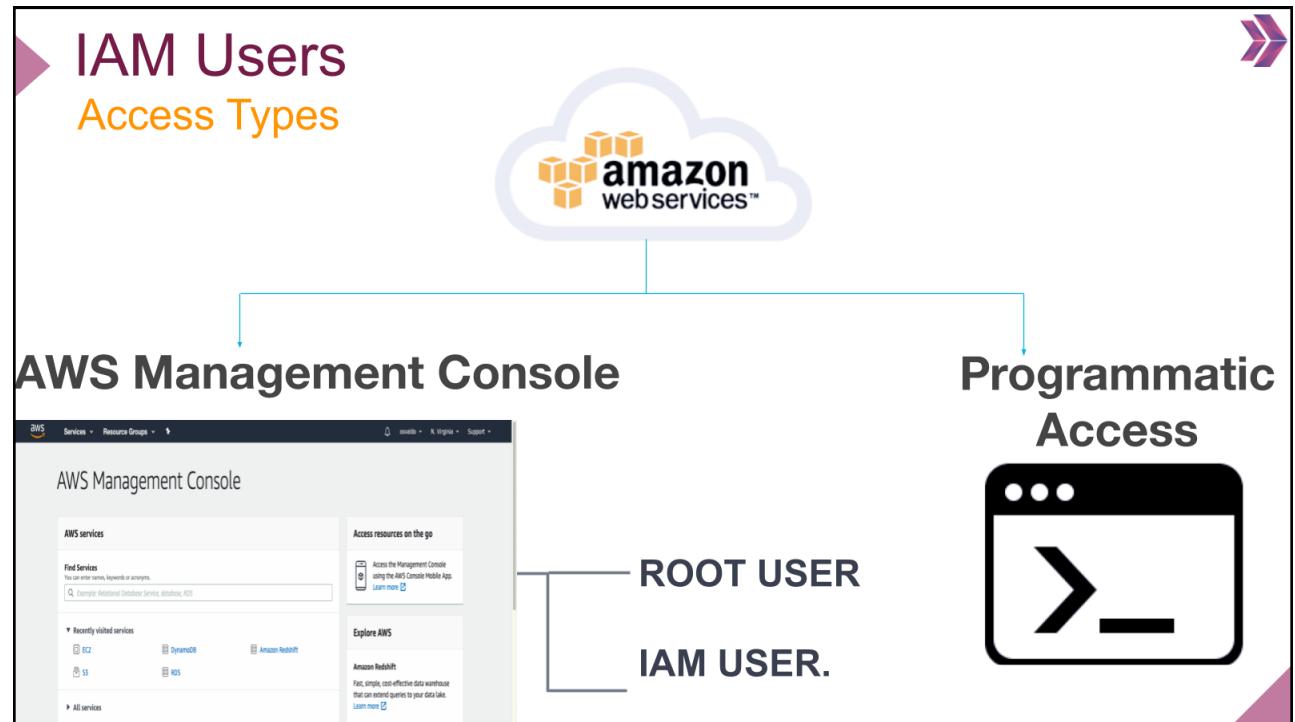
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user

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

Account ID (12 digits) or account alias

Next



IAM Users

Sign in with IAM 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](#)

Account ID (12 digits) or account alias
awsdevopsteam

Next



aws
Sign in as IAM user

Account ID (12 digits) or account alias
awsdevopsteam

IAM user name
user-1

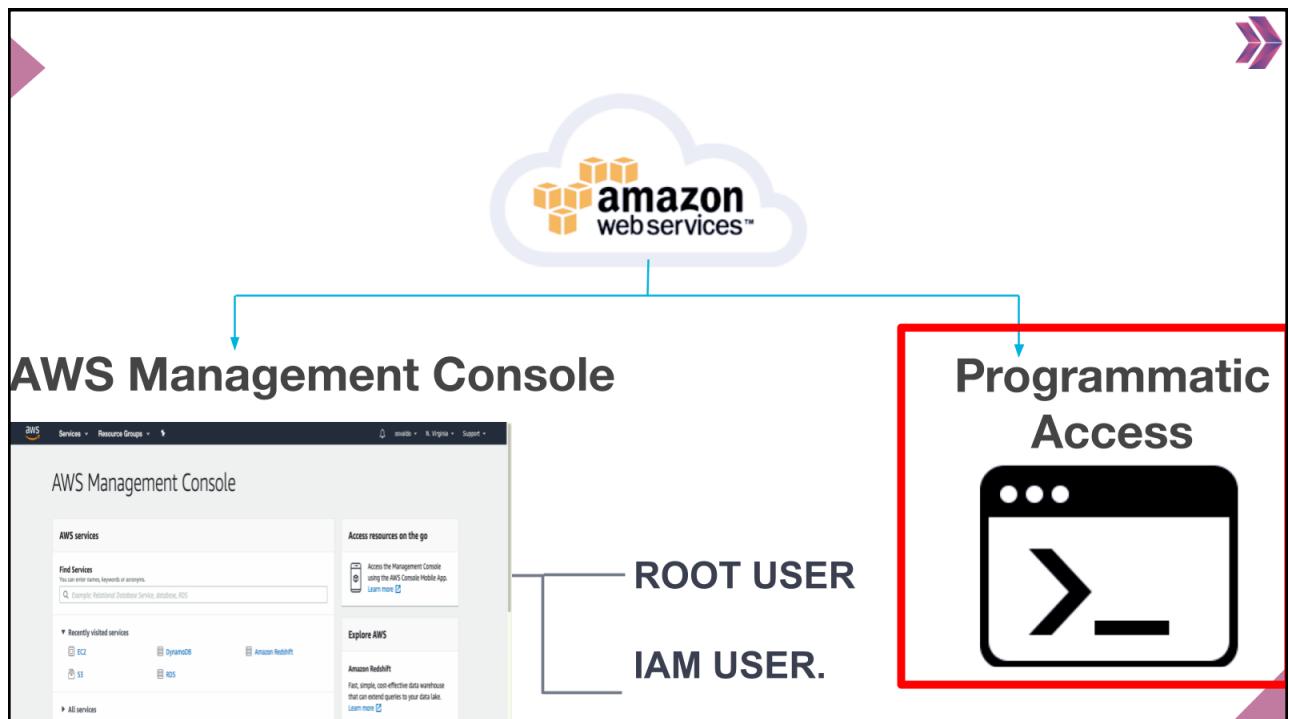
Password
.....

Sign In

[Sign in using root user email](#)
[Forgot password?](#)

CLARUSWAY
WAY TO REINVENT YOURSELF

Account ID/Alias
User name
Password



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 EclipseAWS Toolkit
for Visual StudioAWS 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$
```

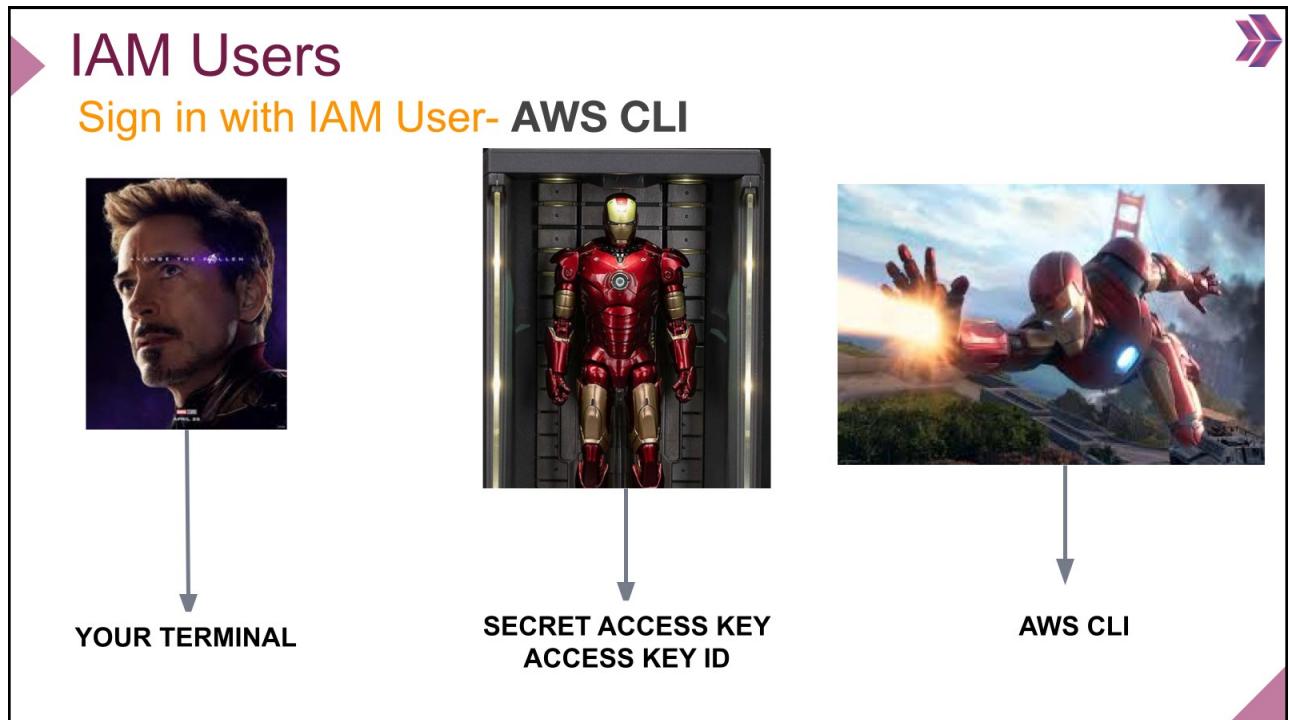
Access Key ID !!!!!

Secret Access Key !!!!!



**ROOT USER

IAM USER.



The screenshot shows the AWS IAM Dashboard with the following steps highlighted:

- 1**: The "Welcome to Identity and Access Management" section displays the "IAM users sign-in link" URL: <http://awsdevopsteam.signin.aws.amazon.com/console>.
- 2**: A modal window titled "Create Account Alias" shows the "Account Alias" field containing "awsdevopsteam".
- 3**: The "Yes, Create" button in the modal is highlighted, and a red arrow points down to the "IAM users sign-in link" URL in the modal, which is: <http://2234565487644.signin.aws.amazon.com/console>.

CLARUSWAY
WAY TO REINVENT YOURSELF

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.

CLARUSWAY
WAY TO REINVENT YOURSELF

21

IAM Policies

Policies - JSON Identifiers

```

1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": "*",
7              "Resource": "*"
8          }
9      ]
10 }
```

Version: Specifies the version of the policy document.

Statement: The basic part of a policy where you define permissions

Effect: It determines what the statement actually does. Can contain only the **Allow** or **Deny** values.

Actions: Determines which actions the identity can perform.

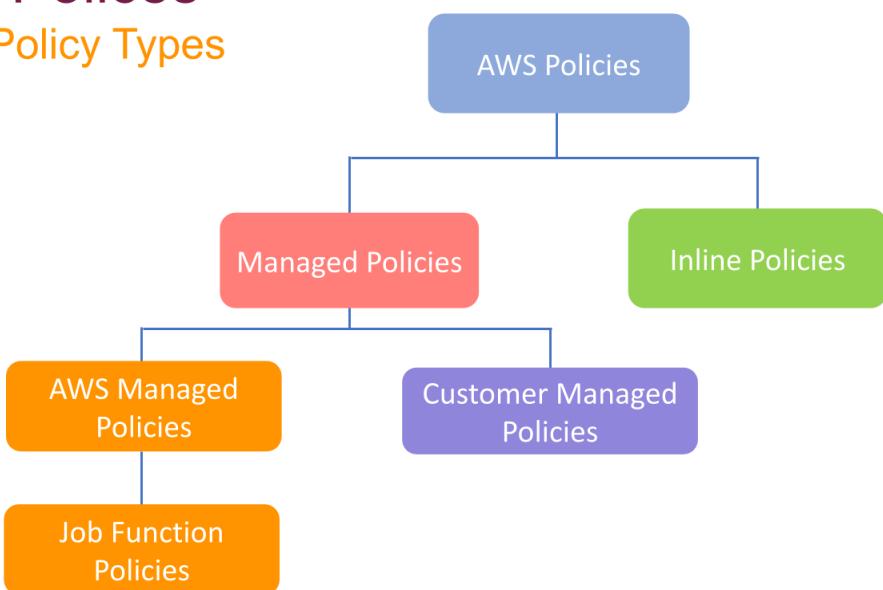
Resource: Explains in which AWS resources the statement will perform the operations.

CLARUSWAY
WAY TO REINVENT YOURSELF

22

IAM Policies

IAM Policy Types



CLARUSWAY
WAY TO REINVENT YOURSELF

IAM Policies

Managed Policy

Policy name	Type	Used as	Description
AdministratorAccess	Job function	Permissions policy (2)	Provides full access to AWS services and resources.
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to r...

You can reach managed Policies from the left-hand menu on IAM Dashboard

CLARUSWAY
WAY TO REINVENT YOURSELF

IAM Policies

Inline Policies

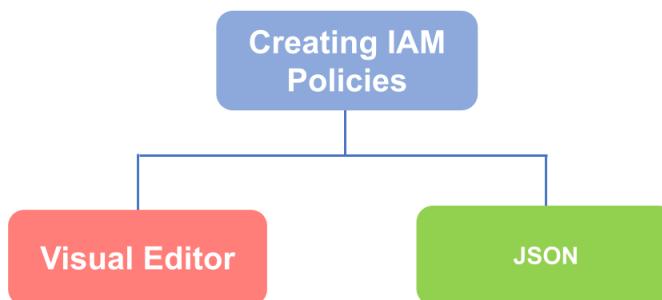
The screenshot shows the AWS IAM User Summary page for a user named 'test_user'. The left sidebar has 'Users' selected (marked with a green circle labeled 1). The main summary section shows the User ARN as 'arn:aws:iam::387408214354:user/test_user', Path as '/', and Creation time as '2019-12-04 14:28 UTC+0300'. Below this, there are tabs for 'Permissions', 'Groups (1)', 'Tags (1)', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is selected, showing 'Permissions policies (3 policies applied)'. A blue button labeled 'Add permissions' is visible. On the right side, there is a 'Policy type' dropdown and a 'Policy name' dropdown. A green circle labeled 2 points to the 'Permissions' tab. A green circle labeled 3 points to the 'Add inline policy' button.

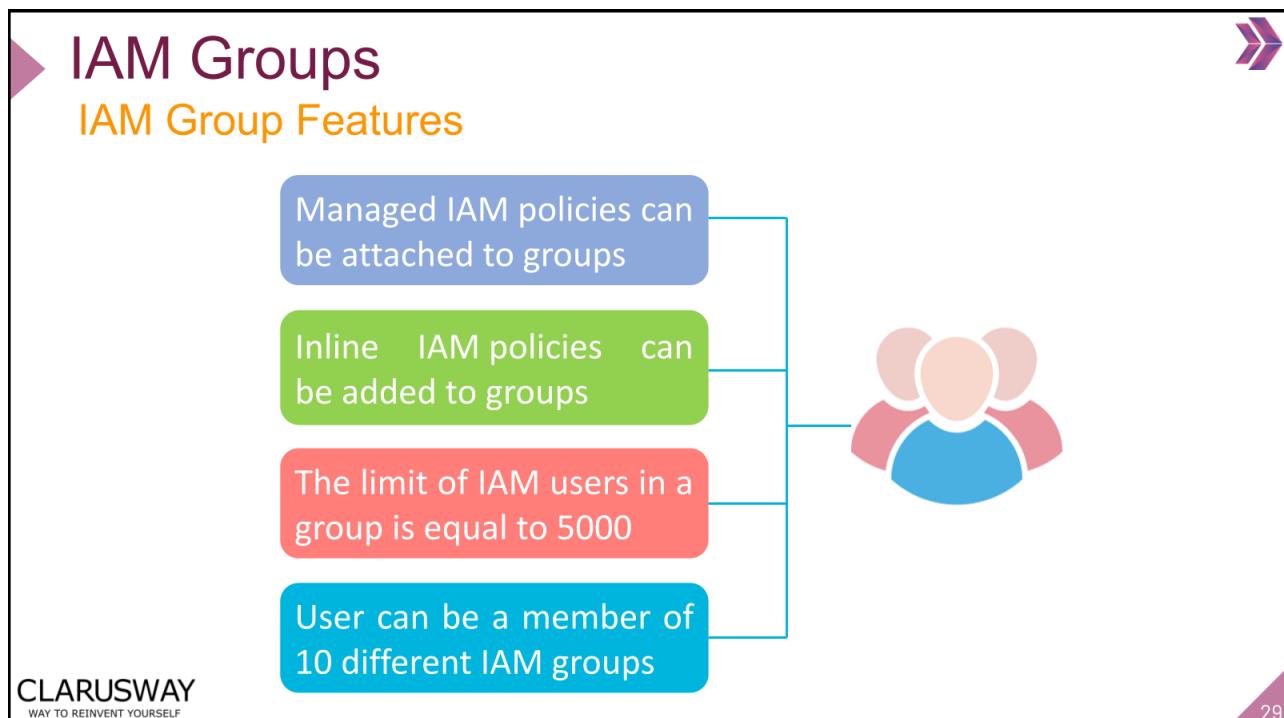
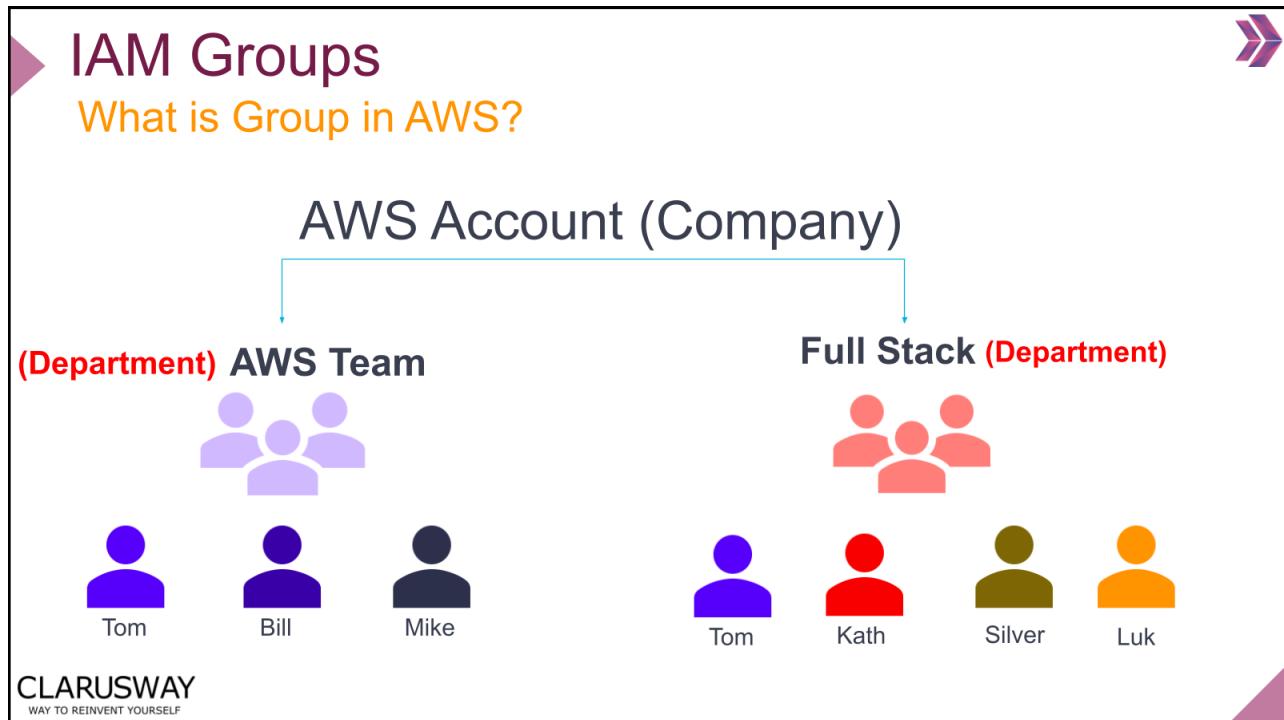
AWS IAM inline policies are created and managed by users and **embedded** directly into a single entity.

To reach inline policies; Click **User** from the left-hand menu on IAM Dashboard
 Select **any user** you created
 Click **Add inline policy** tab on right-hand

IAM Policies

Creating IAM Policies





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?



Another AWS account
Belonging to you or 3rd party



AWS service
EC2, Lambda and others



Web identity
Cognito or any OpenID provider



SAML 2.0 federation
Your corporate directory



okta

IAM Roles

What does IAM ROLE do ?

www.e-commerce...

What if you sold something?

EC2

aws

Policy
JSON

RDS

Record:
-Customer info

CLARUSWAY WAY TO REINVENT YOURSELF

33

IAM Roles Anatomy of a Role

Trusted Entity

AWS service
EC2, Lambda and others

Target

AWS service
EC2, Lambda and others

Permission Policy

Policy
JSON

EC2

RDS

CLARUSWAY WAY TO REINVENT YOURSELF

34