AWS IAM

CLARUSWAY
WAY TO REINVENT YOURSELF

Table of Contents

1 Introduction to IAM

CLARUSWAY
WAY TO REINVENT YOURSELF

What Is IAM?

IAM = **I**dentity & **A**ccess **M**anagement

Authentication
Prove your identity

- Username + Password + {MFA}
  or
- Access Key + Secret Key
  or
- Access Key + Secret Key + Session Token

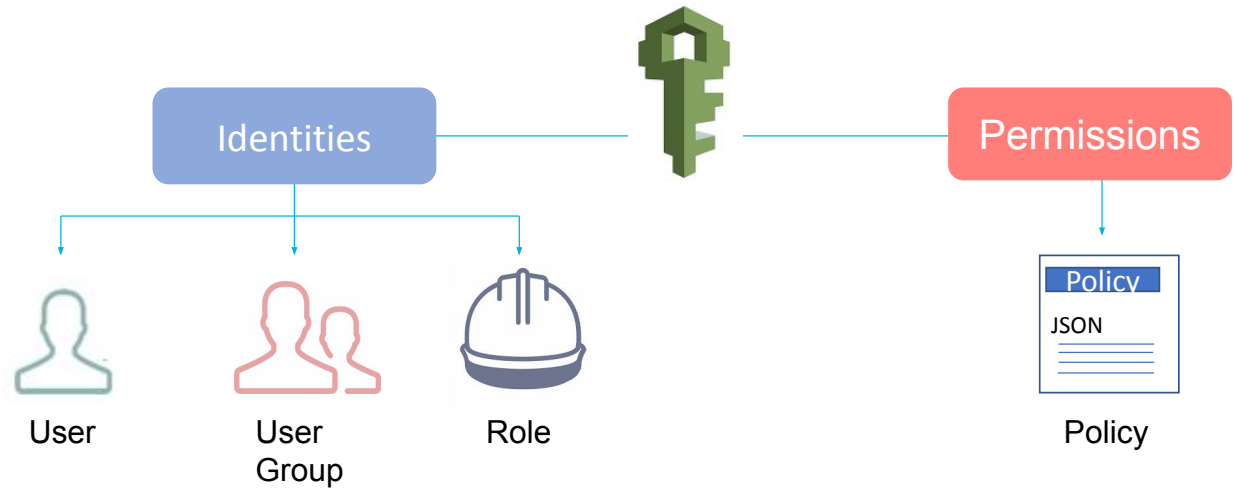
Authorization
Permission to access resources

- IAM Policies
  and/or
- Resource Policies

CLARUSWAY
WAY TO REINVENT YOURSELF

Introduction to IAM

Categorizing IAM Components



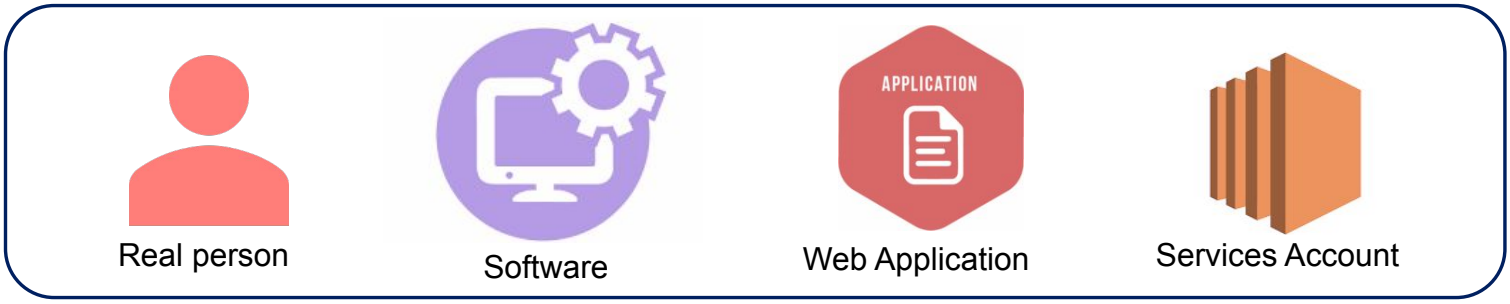
- IAM components can be mainly categorized under two terms; Identities and Permissions.

2 IAM Users

IAM Users

What is IAM User?

(IAM) user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS



IAM Users

What is Root User and IAM User.

AWS Account Owner - Root User (You)

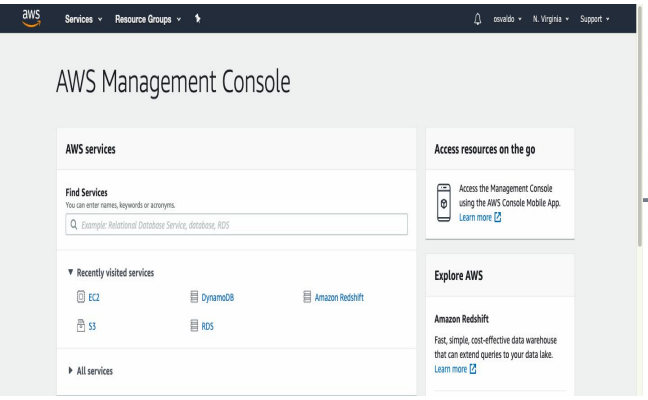
- You-IAM User
- Bill-IAM User
- Tom-IAM User
- John-IAM User
- Kath-IAM User

- 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 user Root User for day-to-day work
  - Keep password in a secure location

IAM Users

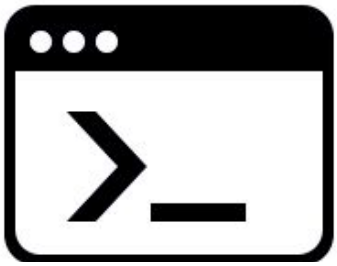
Access Types

AWS Management Console



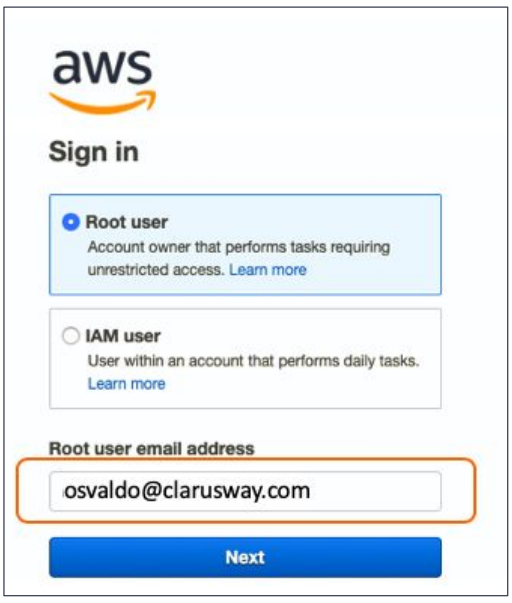
- **ROOT USER**
- **IAM USER.**

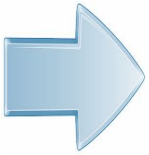
Programmatic Access



IAM Users

Sign in with Root User- AWS Management Console Access

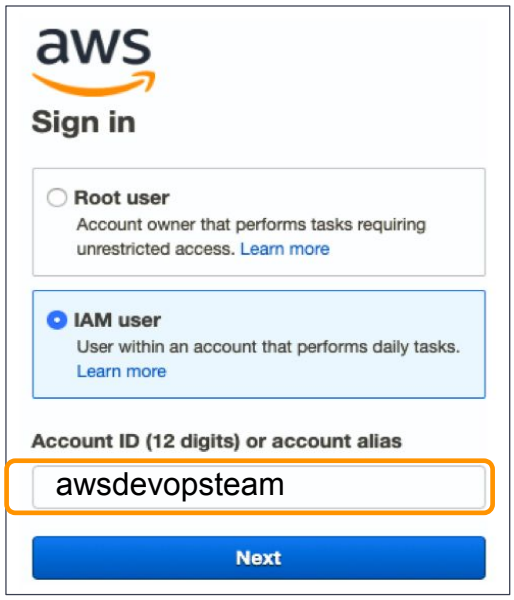




E-mail
Password

IAM Users

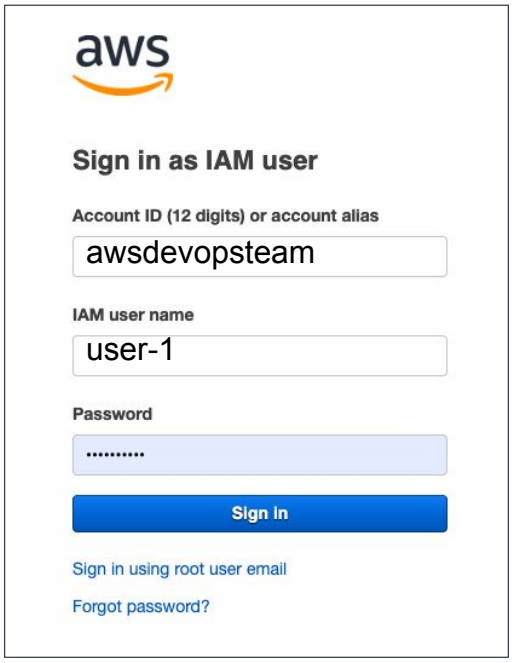
Sign in with IAM User- AWS Management Console Access



Account ID/Alias

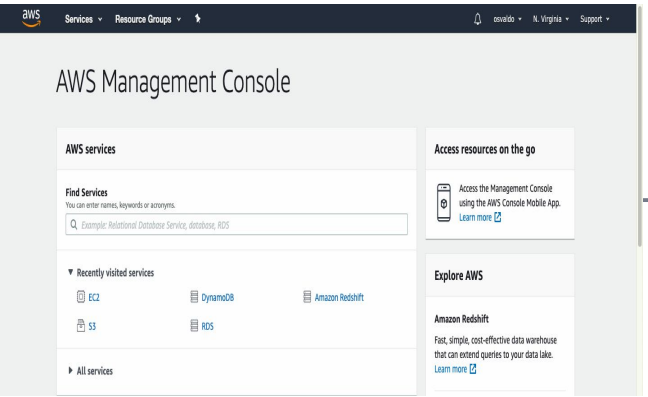
User name

Password



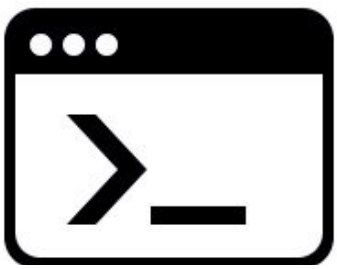
CLARUSWAY
WAY TO REINVENT YOURSELF

AWS Management Console



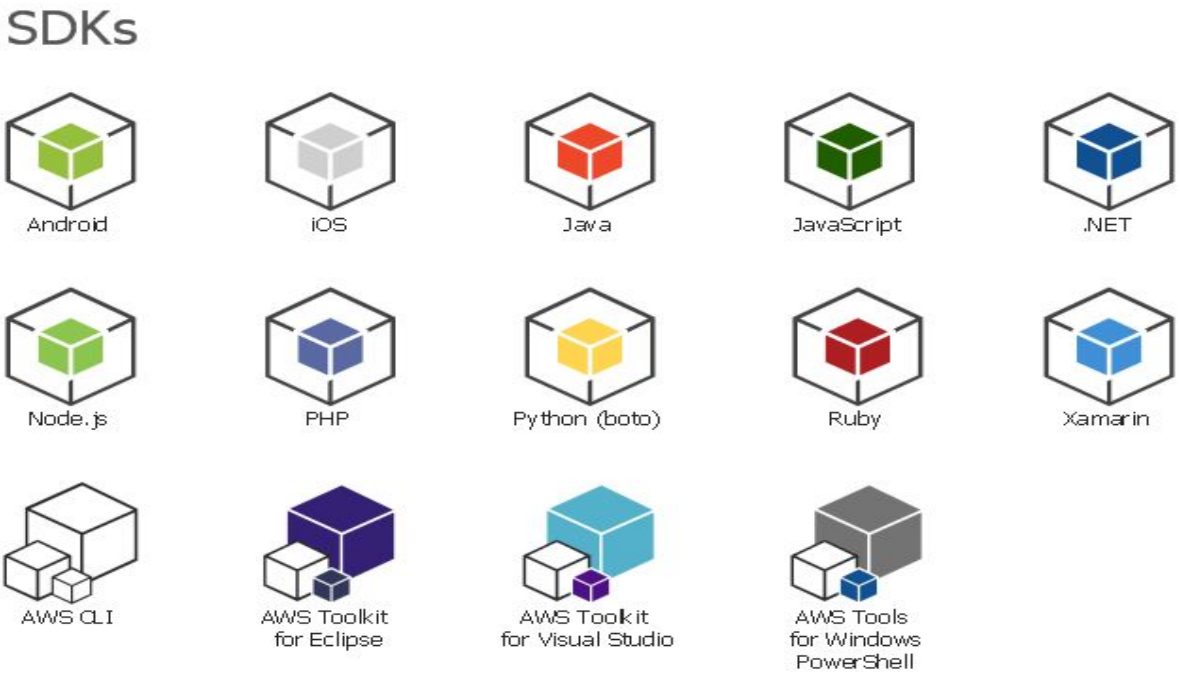
- ROOT USER
- IAM USER.

Programmatic Access



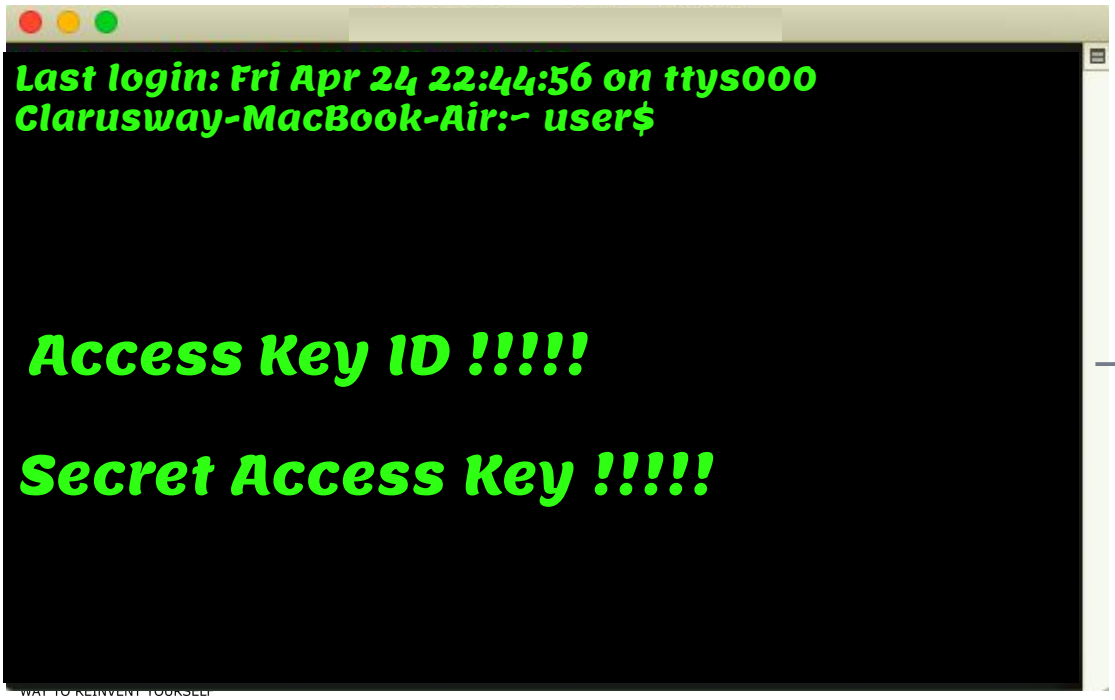
IAM Users

Sign in with IAM User- **Programmatic Access**



IAM Users

Sign in with IAM User- **Programmatic Access**



AWS CLI

**ROOT USER

IAM USER.

IAM Users

Sign in with IAM User- **AWS CLI**

YOUR TERMINAL

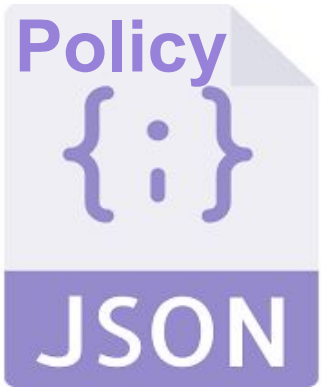
SECRET ACCESS KEY
ACCESS KEY ID

AWS CLI

3 IAM Polices

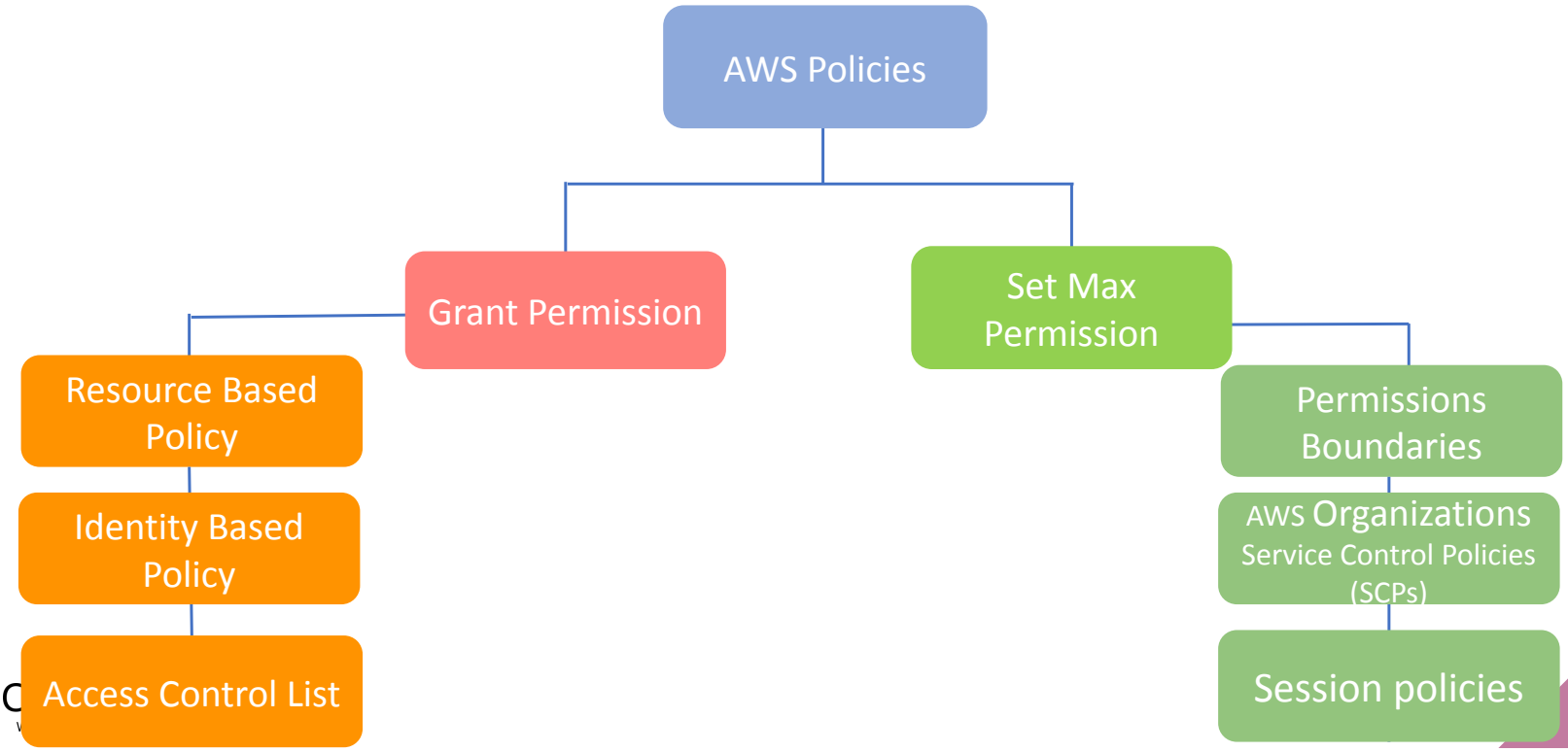
IAM Polices

What is a Policy?

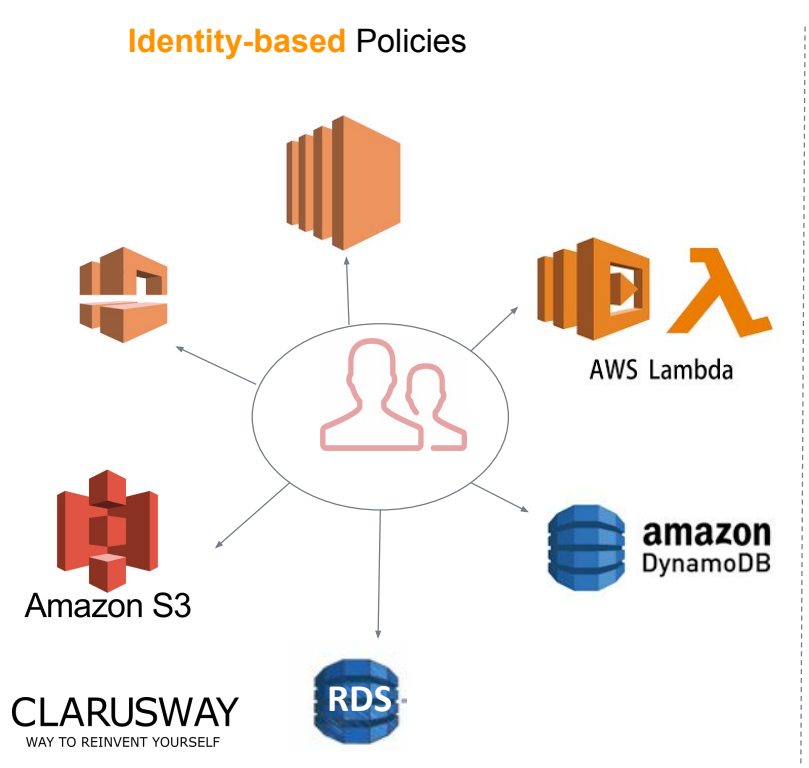


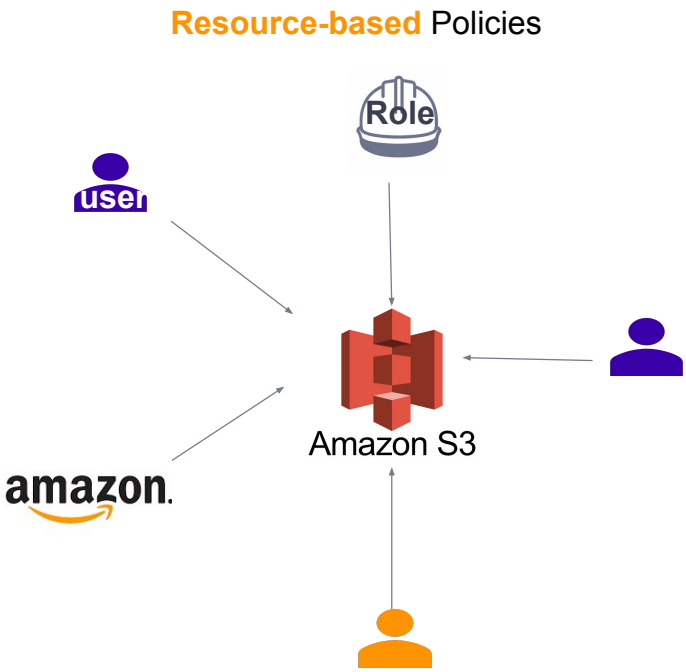
- A policy is an object used to define the **permissions** of an identity or resource in AWS
- Permissions in the policies determine whether the request is **allowed** or **denied.**
- Policies are stored in AWS as **JSON** documents.

Policy Types



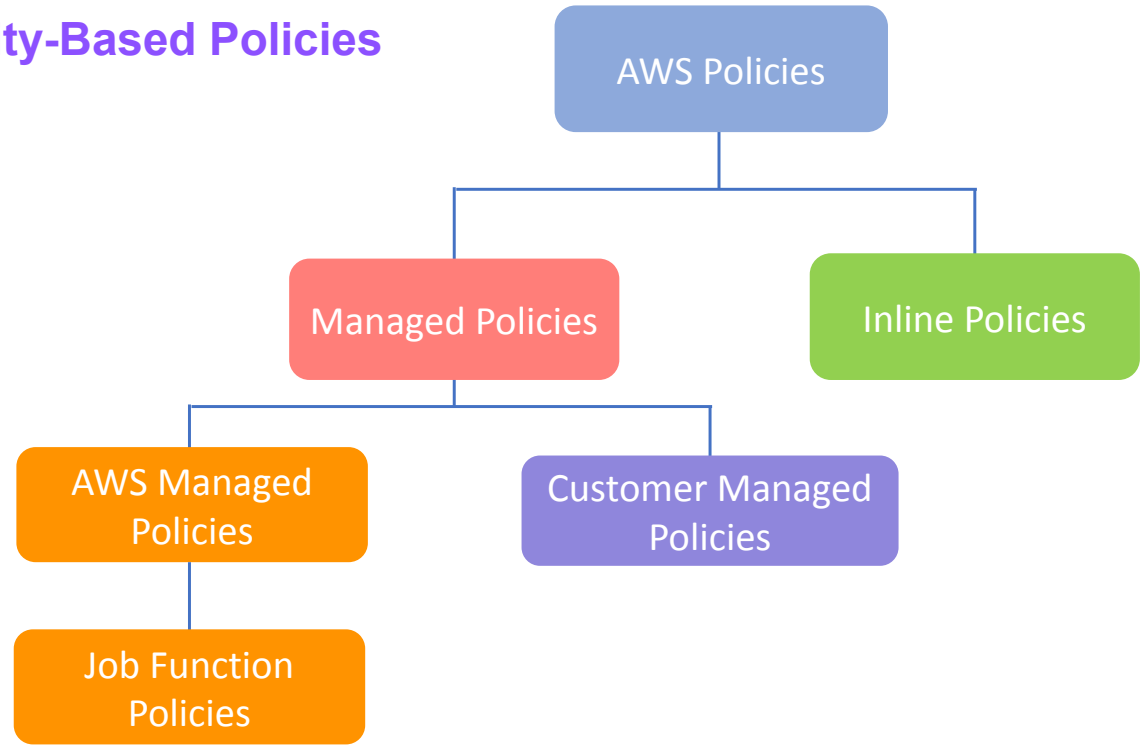
Identity-based vs. Resource-based Policies





IAM Polices

Identity-Based Policies



IAM Polices

Policies - JSON Identifiers

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": "*",
         "Resource": "*"
      }
   ]
}
```

Version: Specifies the version of the policy document.

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

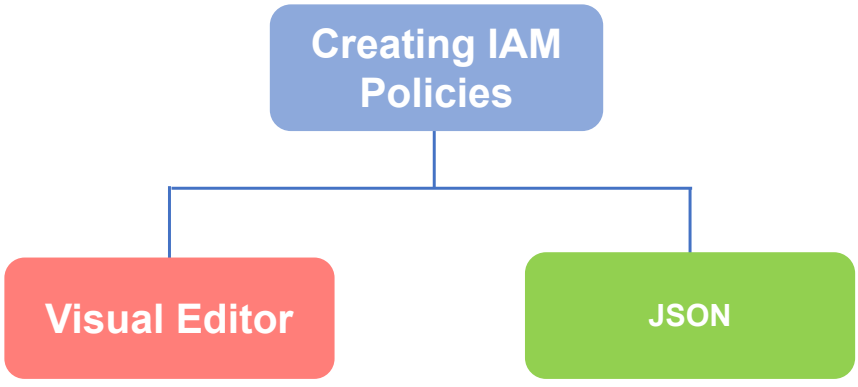
Effect: It determines what the statement actually does. Can contain only the **Allow** or **Deny** values.

Actions: Determines which actions the identity can perform.

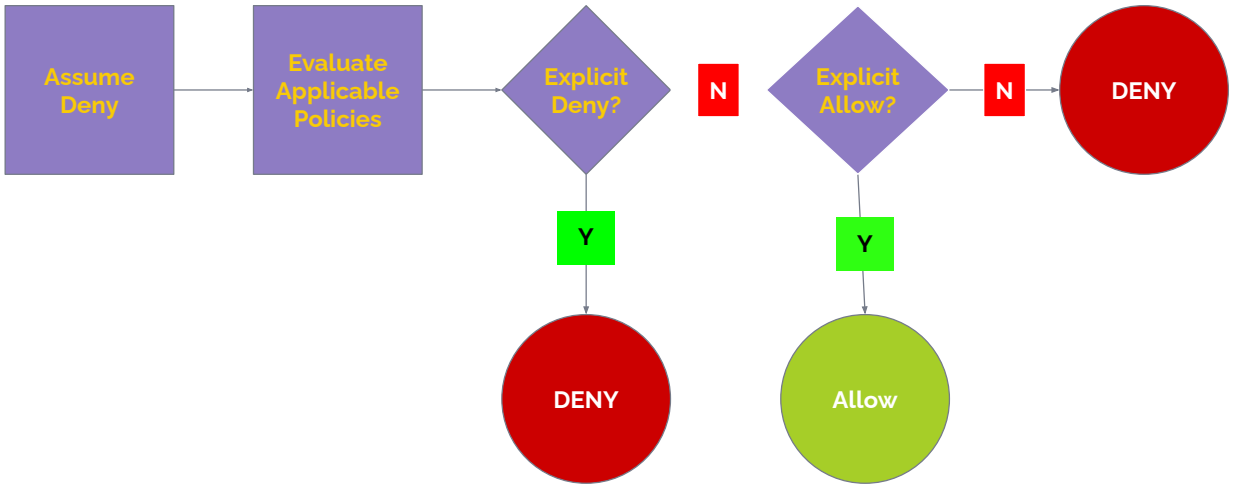
Resource: Explains **in which AWS resources** the statement will perform the operations.

IAM Polices

Creating IAM Policies



Policy Evaluation

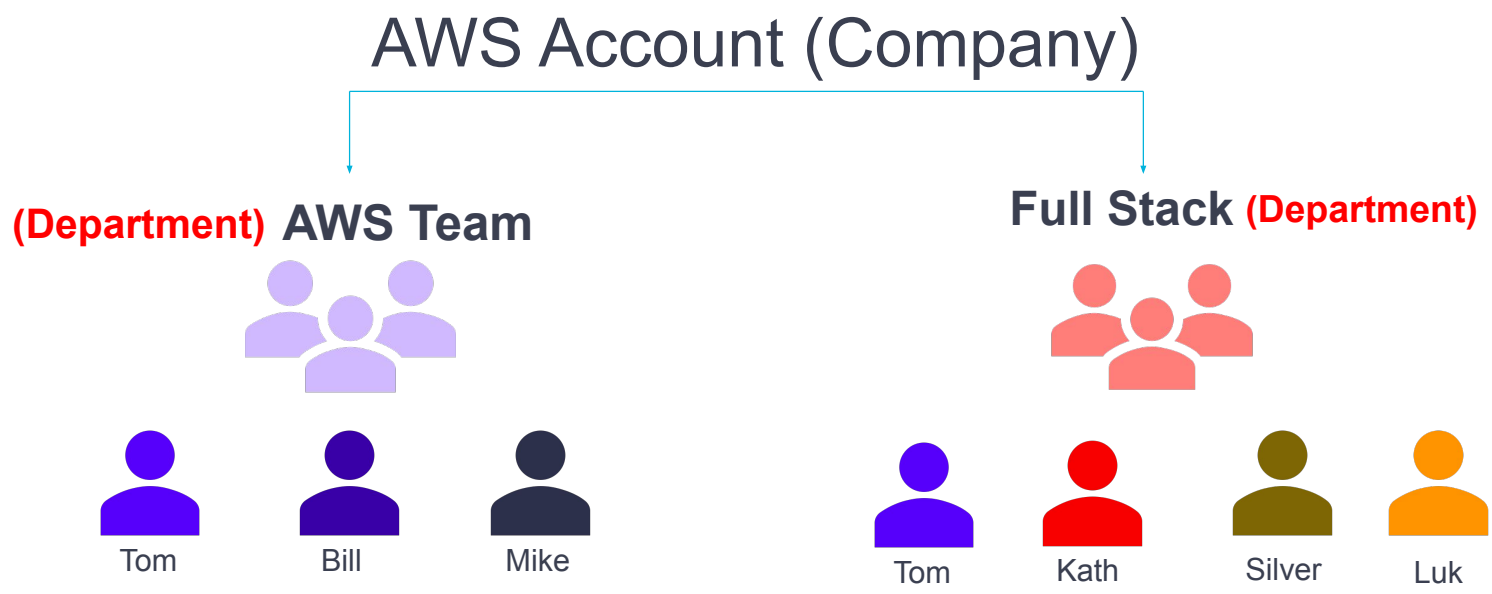


- Deny by **default**
- Deny takes **precedence** over allow

4 IAM User Groups

IAM User Groups

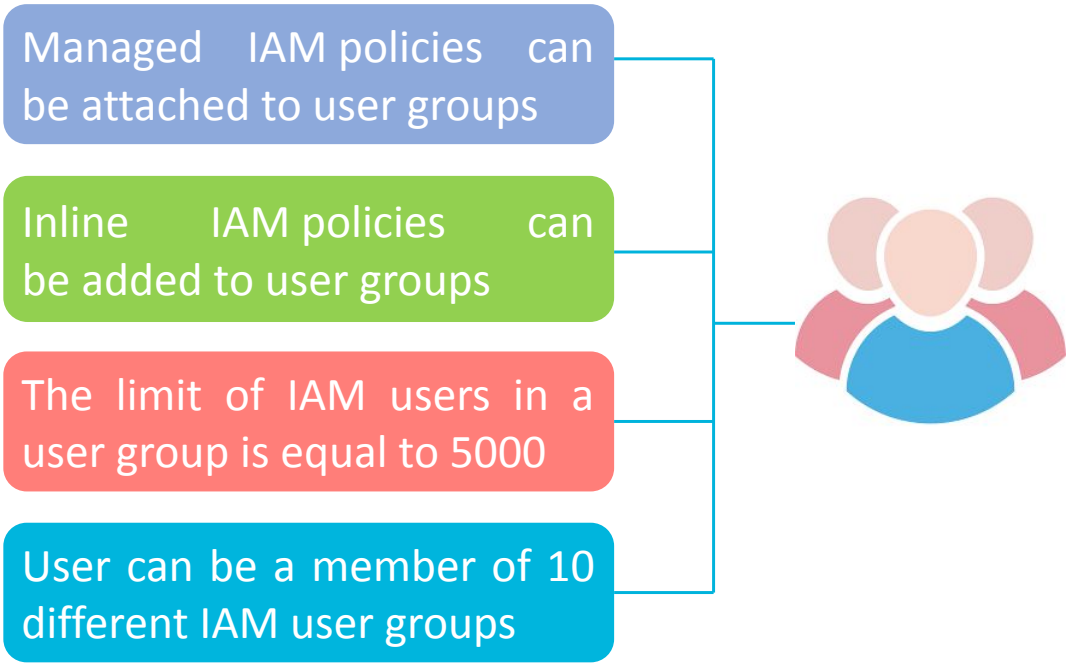
What is User Group in AWS?



CLARUSWAY
WAY TO REINVENT YOURSELF

IAM User Groups

IAM User Group Features



CLARUSWAY
WAY TO REINVENT YOURSELF

5 IAM Roles

CLARUSWAY
WAY TO REINVENT YOURSELF

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

Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

IAM Roles

What does IAM ROLE do ?

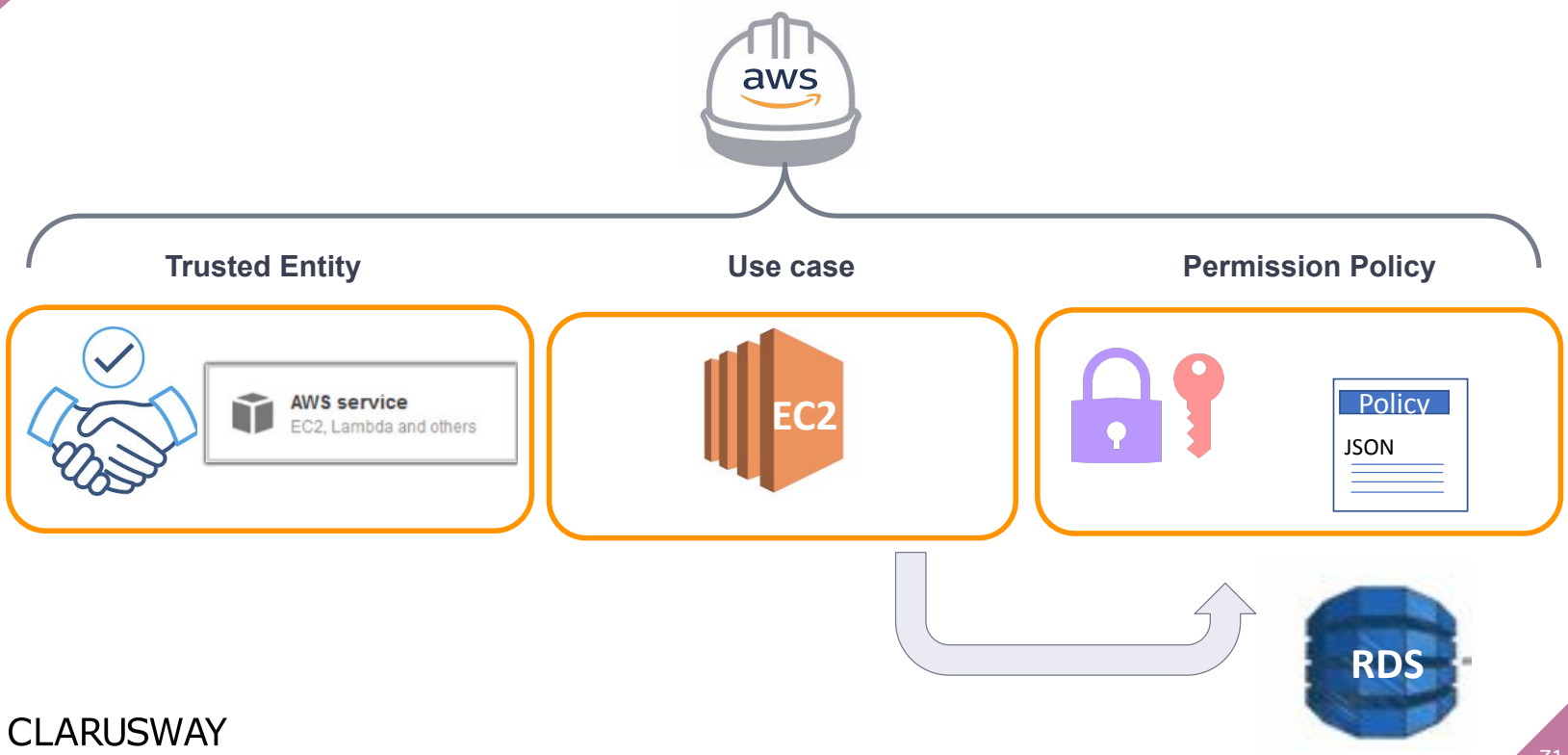
www.e-commerce...

What if you sold something?

Record:
-Customer info

IAM Roles

Anatomy of a Role



Role Credentials

```
aws_access_key_id=ASIA5RBXKVCZWCMV4AFJ

aws_secret_access_key=23uUyY07I0PKG1URM6iQPV+A8wSsvLEbmHEA37wF

aws_session_token=IQoJb3JpZ2luX2VjEK//////////wEaCXVzLWVhc3QtMSJHMEUCIGrn7HEV38ejafaba56pEv1UxDIPjFdYLjgLSv0UvpmiA
iEA4b9Z2Noc0Ah3ru6bogoW+iBRtUrdg05zk7LkM4HQaNsqkgMIFxACGgw5Mjk5NzY0NjE0OTEiDAwgg62YKfWxIzb1TSrvArdvoRgYW4EvWtPAkM9R
IPk6EpWeHVMbDgVtyk7TGXCRTF6uZpyWSX33QS3Pwvb6d0pwiqomeOFDgG28U82eXrXGoKZnbTmnC+7X0QWgqAUI0Ku2kU/KLLwbLhjpv1Ai/oFpAvG
0FmZMtVZH+w6/uuyHgzFmPjwgrLTOj0AlnRfA1rjYJm6b2QD6ou5ZMK1JrV/jdW2z0Os7sPVkSA4lH6VPZ2D6vjAnRWDC+0uBV6QUfKlLLeJ1F51bTI
F3tI2Yu9VnXEV6usAblStCt3NnTpZRnGQTIyUcICLzAiGhJUdZpGQofdLrLEL/Matyg1wVA45RpT2MhgH+HPuoIGGT0uISBSt6YQV4/1wf9w2KSIT4U
dZgaQt8L+TDXIz1/ywn4f11dU0K9vwIINIwp+8s9le7hn1vQPm7HAetLi5mRE30vzXJ6Eoai9RbfgFW7HpxffZLImdOgealQ51w+0Zu7Rx4jGWhWLMd
WyrJQQw+ZXhgwY6pgESvD6LuI39m2hhJMC378lE8Q4OL+Jnl7CysdjNpBH9AjNwGuI9Ad3y3q1u8z1849KzCZCx9GbG/n9YYy3fGnBrrvNY3nrwiA4d
XKP4KfZU8OIQ3GlLJkK1d24lhhe9UBL3I1ySfMbvDbRoMOXESF6tCpMVLNMa4QaoVY7aThxDvAA6p51pftyPhCK3MJe4qBL4zTC3pXFJe+LPc6uwZ1F
sL/OTBH
```

Once an entity assumes a role, it receives **temporary credentials** in the form of an **access key**, **secret key** and **session token**.

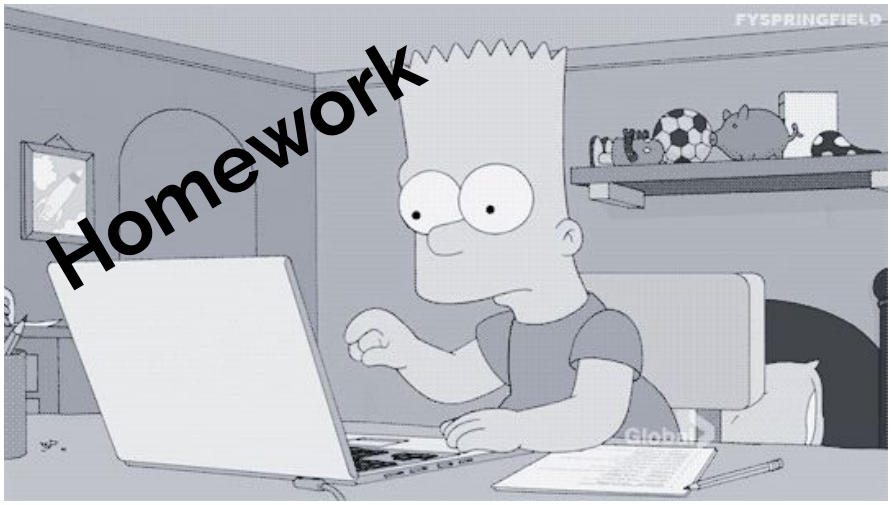
Note that with an **IAM user**, there is **no session token**, since the credentials are **permanent**

6 Implication of AWS SSO

CLARUSWAY
WAY TO REINVENT YOURSELF

Implication of AWS SSO- IAM Identity Center

- Today, most organizations use **AWS SSO to authenticate** users into AWS
- Users are given permanent credentials to log in to SSO
- Those permanent credentials (e.g. email & password) enable the **SSO user to assume an IAM** role by way of short term AWS credentials
- Bottom line:
  - Most organizations today **discourage the use of IAM users**
  - Instead, **roles are used** which map to SSO users
- **AWS IAM Identity Center** is the updated console for the features of AWS Single Sign-On (AWS SSO)



Video on Multi-Factor Authentication (MFA)

https://lms.clarusway.com/mod/lesson/view.php?id=7626&pageid=7570

Let's get our hands dirty!

AWS Account owner - Root User (you)

Administrator (you)-**Newly Created IAM user**

(Department-1)

Database
(RDS FullAccess)

Bill

Tom

(Department-2)

AWS & DevOps
(Power User)

Kath

Tom*

CLARUSWAY
WAY TO REINVENT YOURSELF

THANKS!

Any questions?

You can find me at:

- @osvaldo
- osvaldo@clarusway.com