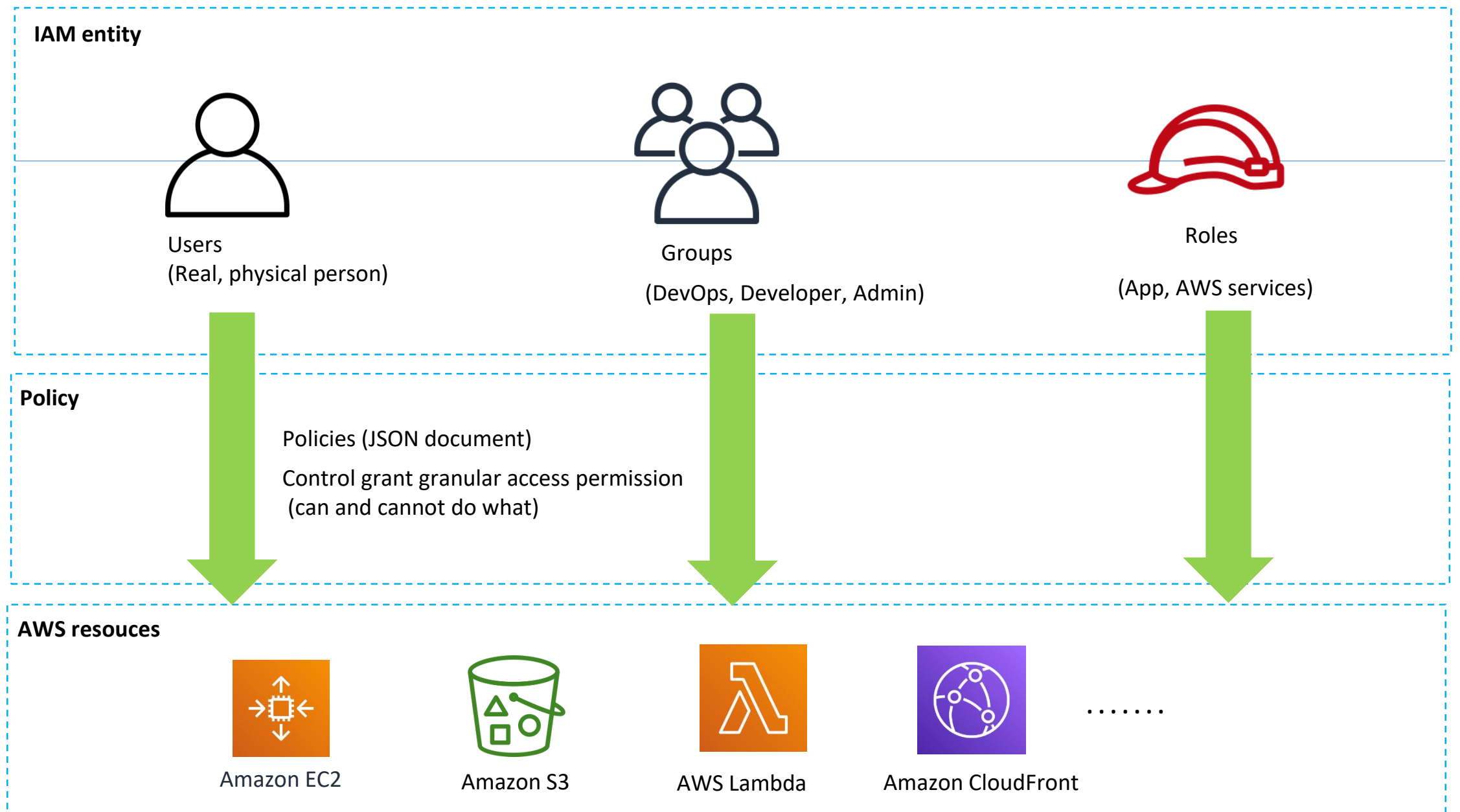


IAM Introduction

What is IAM?

- IAM stands for Intity Access Management
- IAM is core service of AWS
- IAM entity: Users, Groups, Roles
- Whole AWS security is related to control the level of access of IAM entity
- IAM entities are attached policies to define the level of access, permission
- Policy is written in JSON (JavaScript Object Notation) format





IAM key features

- Centralized control of AWS account
- Shared access permission to other AWS accounts
- Granular Permissions
- Identity Federation (Active Directory, Facebook, LinkedIn...)
- Multifactor Authentication
- Setup your own password policy
- Intergrated with many AWS services



IAM best practice

- One **Real User** – One **IAM User** and One **Application** – One **Role**
- Do not use **Root User** for normal operation
- Never embedding **IAM credentials** into code or commit to public SVC
- Never using ROOT user credentials
- Always enable Multifactor Authentication
- Always compliance with “Least Privilege Principle”

