Identity and Access Management (IAM)

Member: Phan Ba Van
Phung Sy Linh
Ngo Quang Vinh
Do Duc Thuong

Introduce

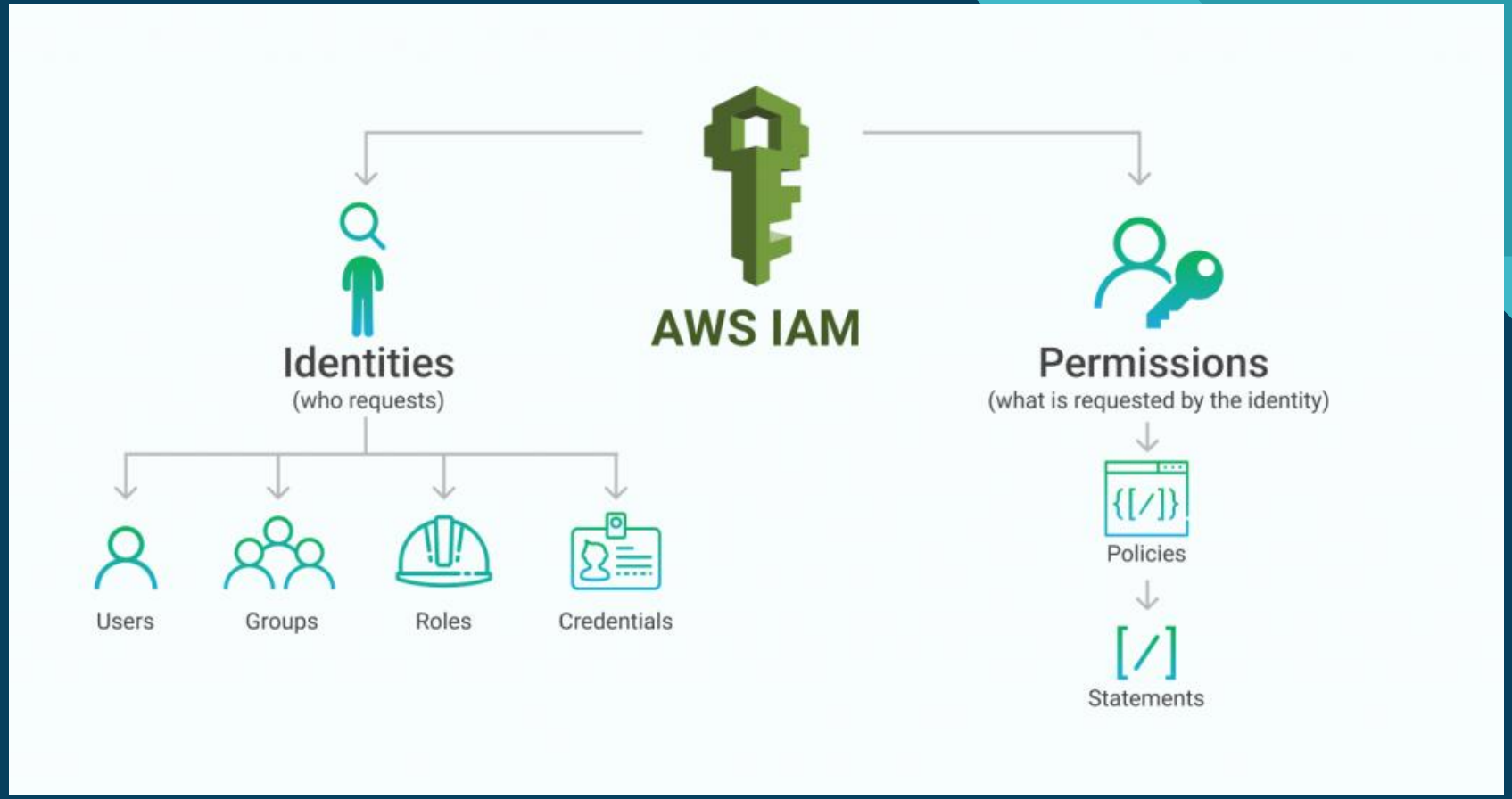
- AWS Identity and Access Management (IAM) enables to manage access to AWS services and resourves securely.
- Create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

Use case:

- Fine-grained access control to AWS resources
- Multi-factor authentication for highly privileged users
- Analyze access

IAM allows to:

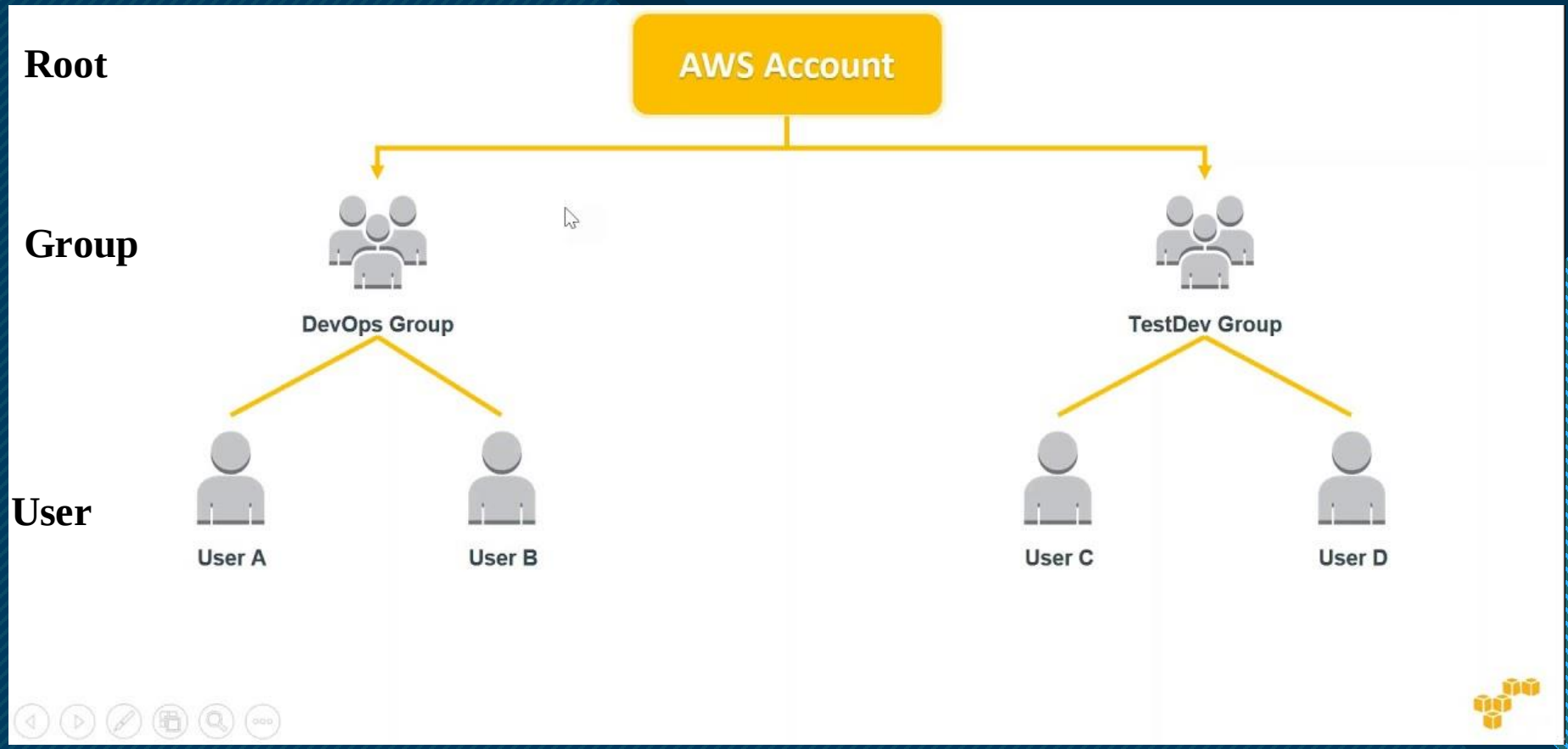
- Manage IAM users and their access
- Manage IAM roles and their permissions
- Manage federated users and their permissions

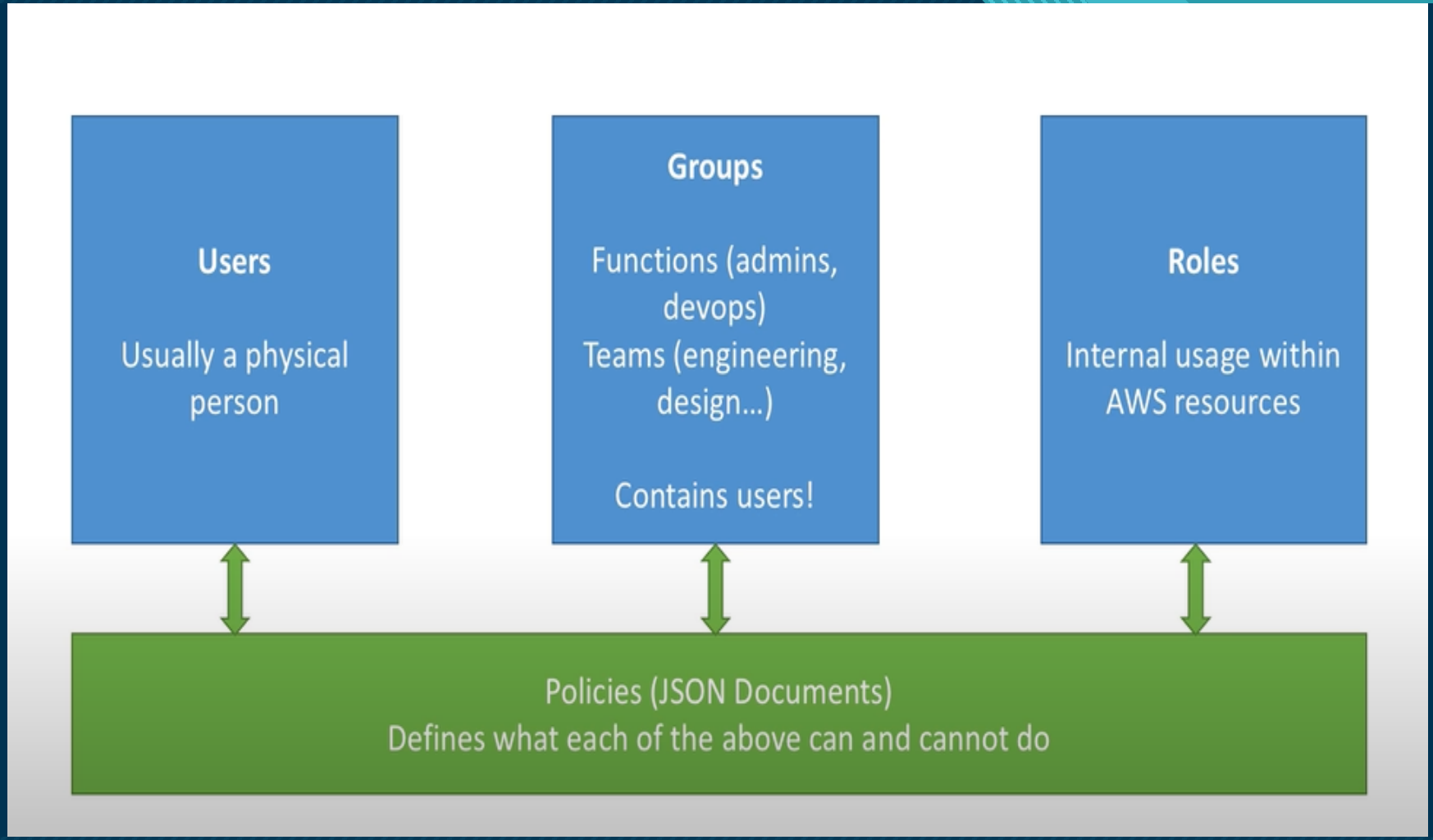

AWS IAM
Identities
(who requests)
Users
Groups
Roles
Credentials
Permissions
(what is requested by the identity)
Policies
Statements

Root

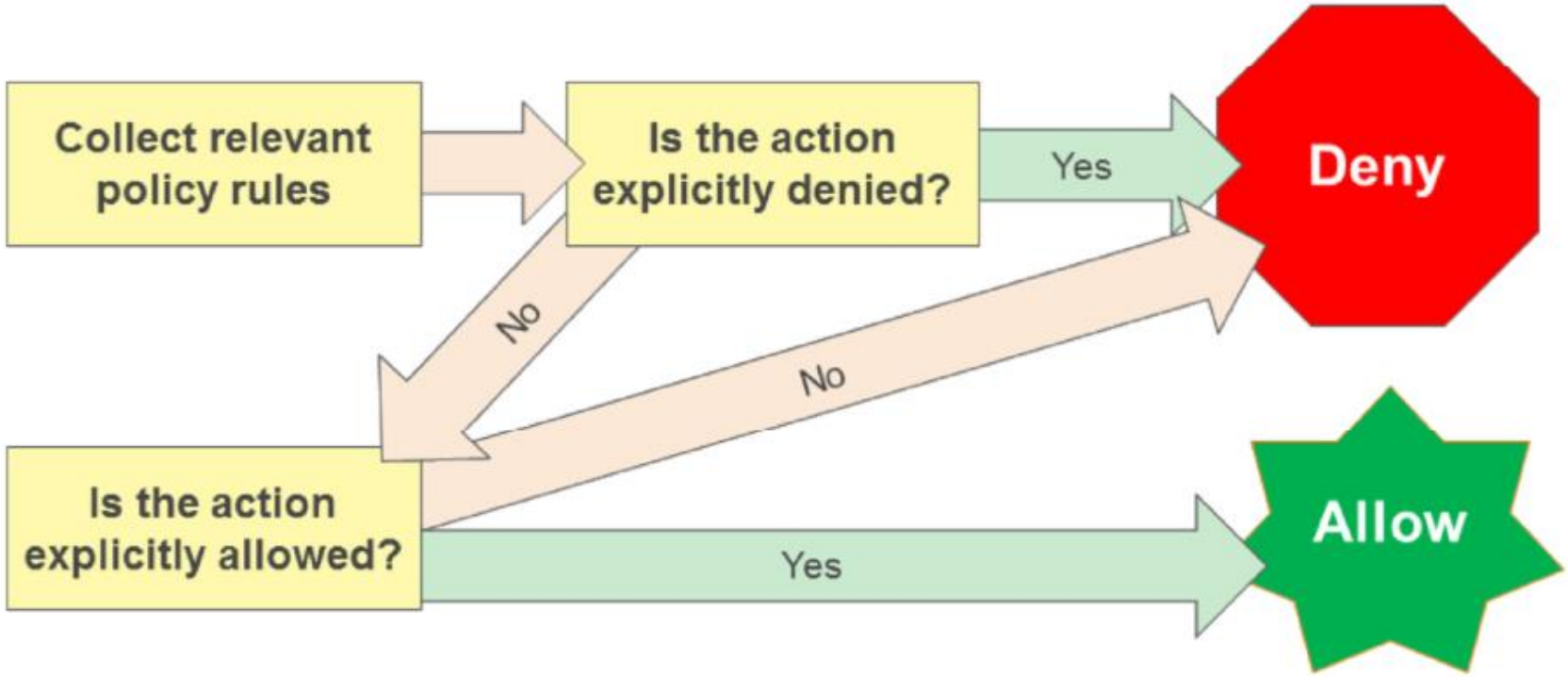
Group

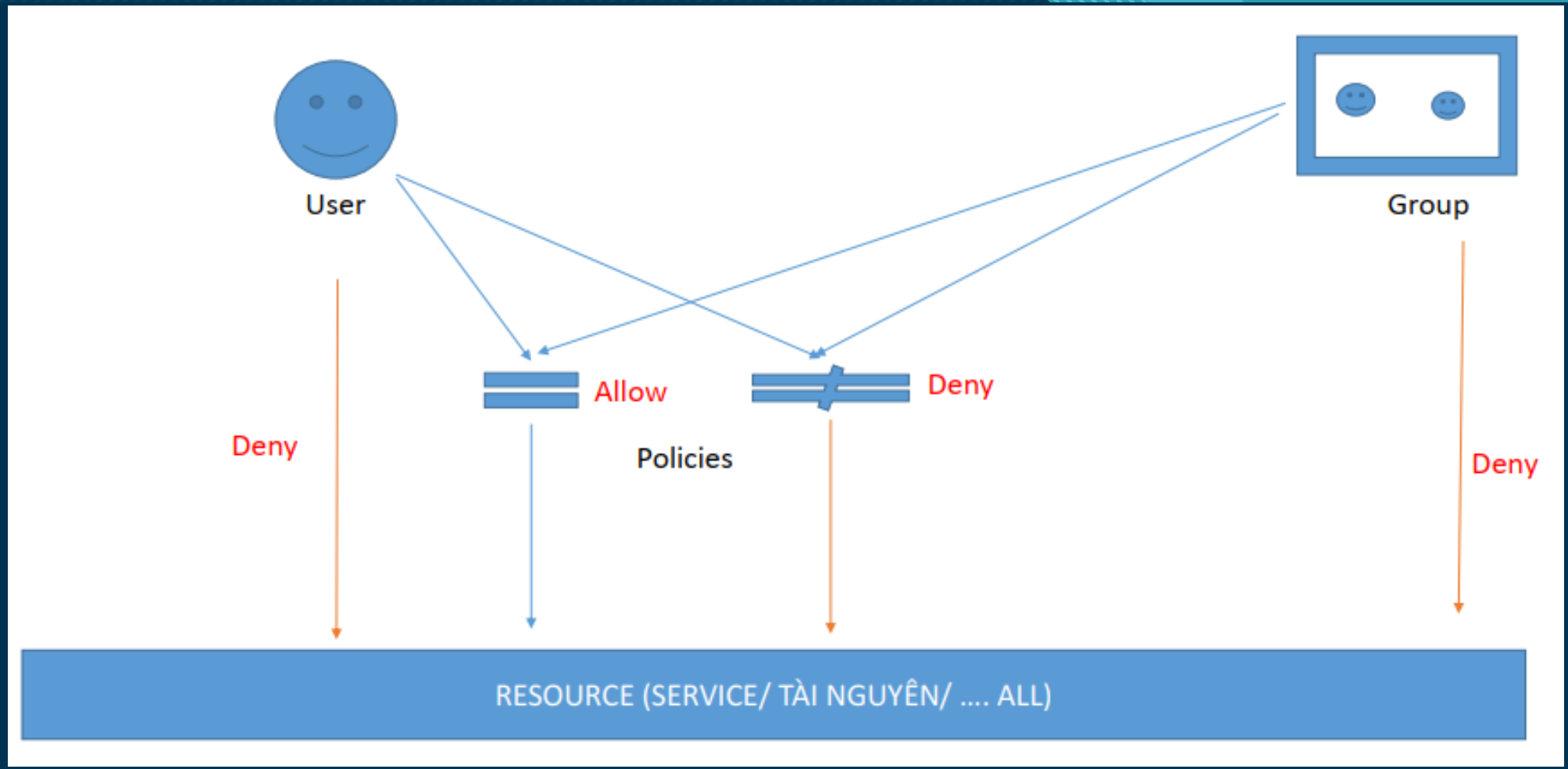
User



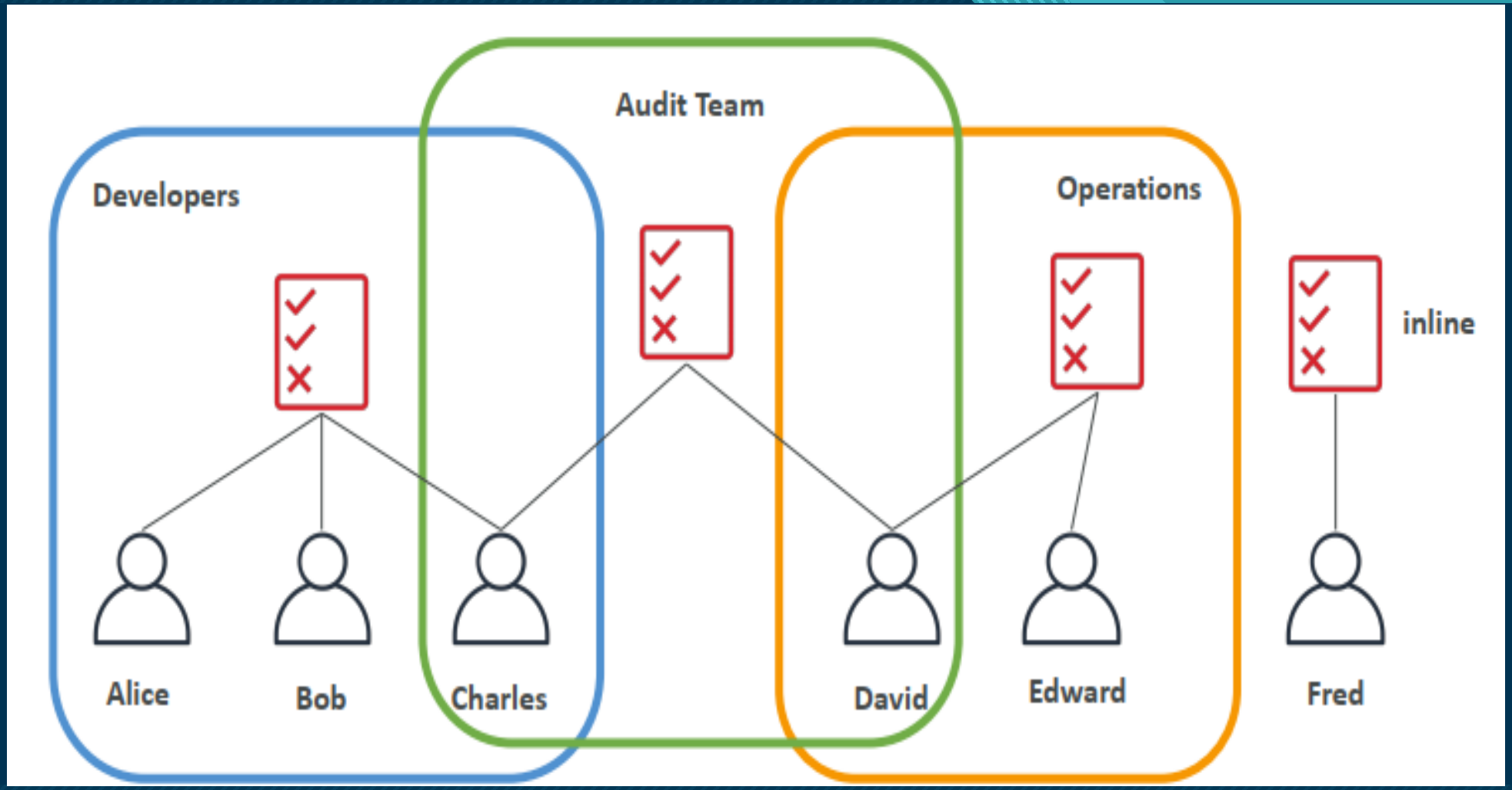

Users
Usually a physical person
Groups
Functions (admins, devops)
Teams (engineering, design...)
Contains users!
Roles
Internal usage within AWS resources
Policies (JSON Documents)
Defines what each of the above can and cannot do

IAM Policy Rule Precedence




User
Group
Allow
Deny
Deny
Policies
Deny
RESOURCE (SERVICE/ TÀI NGUYÊN/ …. ALL)

IAM Policies inheritance



IAM Policies Structure

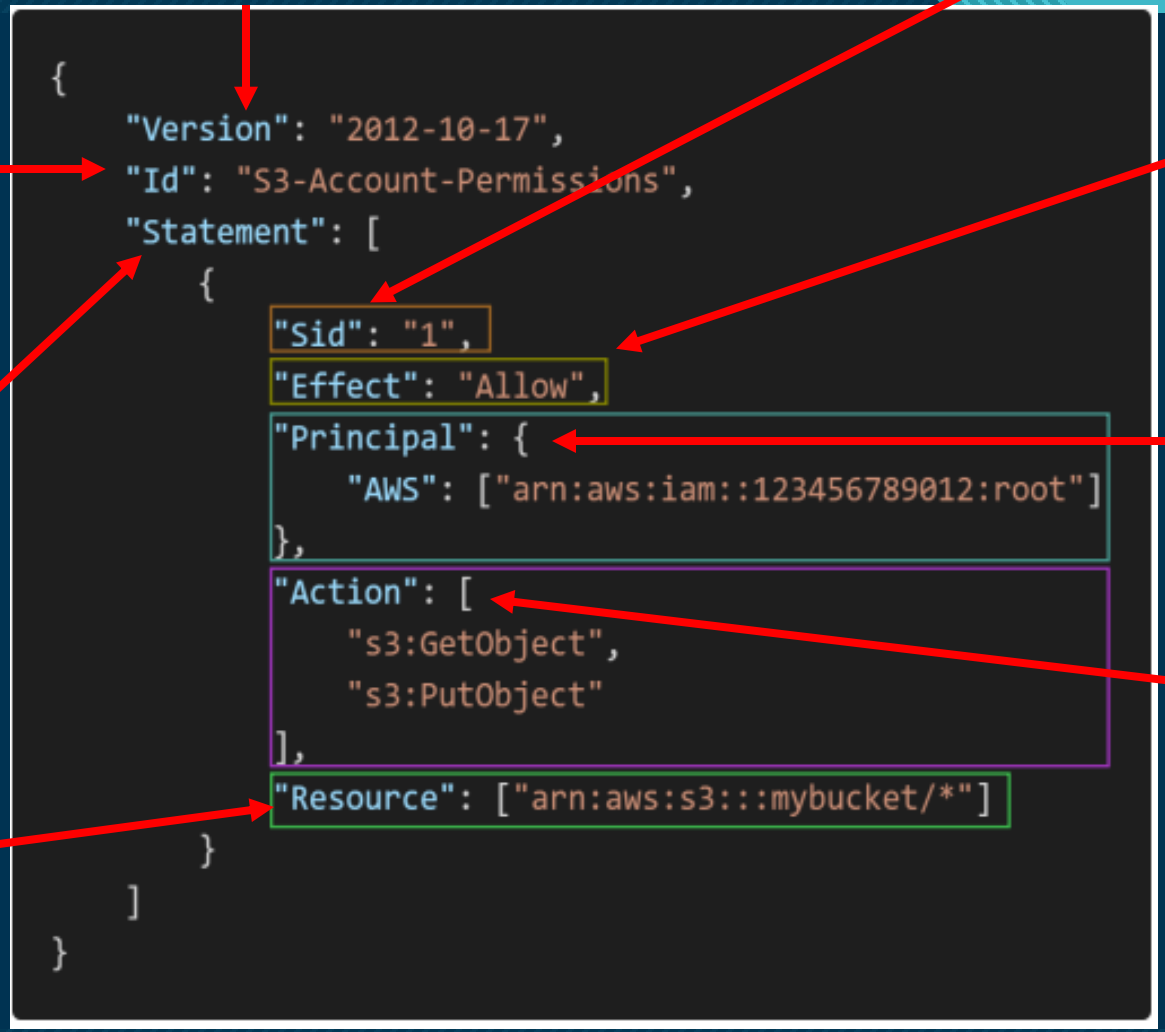
Version: policy language version, always include "2012-10-17"

Sid: an indentifer for the statement (optional)

Id: an indentifer for the policy (optional)

Statement: one or more individual statements (required)

Resource: list of resources to which the actions applied to



Effect: whether the statement allows or denies access (allow, deny)

Principal: account/user/role which this policy applied to

Action: list of actions this policy allows or denies

Condition: conditions for when this policy is in effect (optional)

- Password Policy
- Multi Factor Authentication (MFA)
- IAM security tool
- IAM Guidelines

Thank You!!!