



Become a Solutions Architect



## Week 4 - Agenda

### 1. Technical Track (45 Min)

- AWS IAM

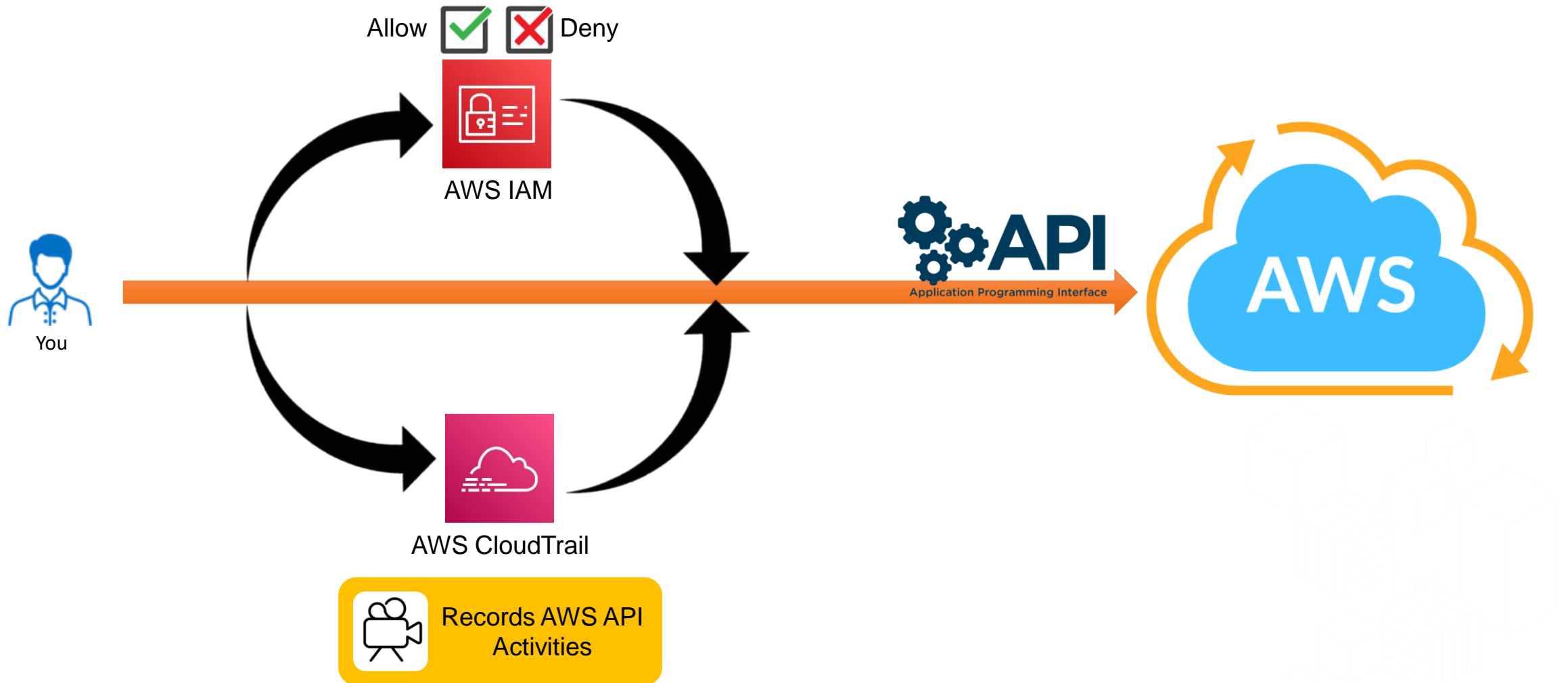
### 2. Networking Track (40 Min)

- Cloud and beyond - VPN and Direct Connect

### 3. Hands On (30 Min)

- Working with Identity & Access Management (IAM)

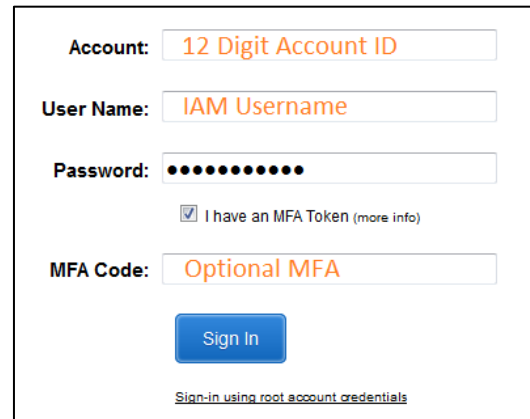
# Flow of a request to AWS





# Accessing AWS Services

IAM Username  
and Password



Account: 12 Digit Account ID

User Name: IAM Username

Password: ••••••••

☒ I have an MFA Token (more info)

MFA Code: Optional MFA

Sign In

[Sign-in using root account credentials](#)

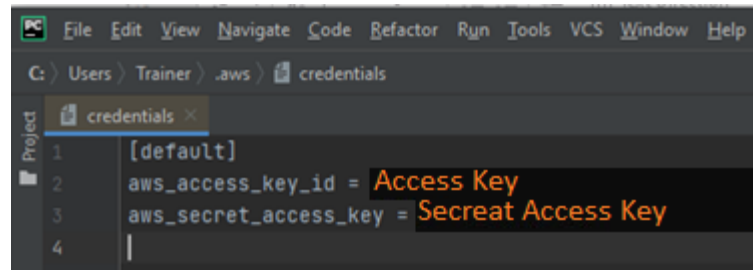


AWS  
Management  
Console

```
C:\Users>aws configure
AWS Access Key ID [None]: Access Key
AWS Secret Access Key [None]: Secret Access Key
Default region name [None]: Region
Default output format [None]: JSON / Text / Table
```



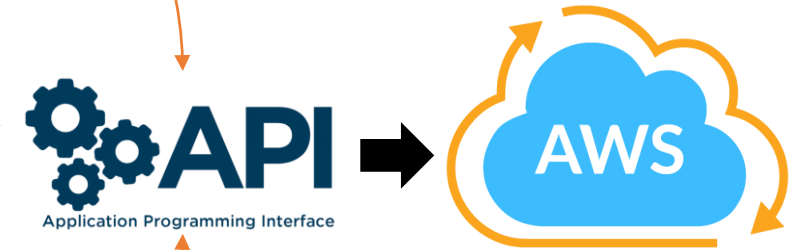
AWS  
Command  
Line Interface



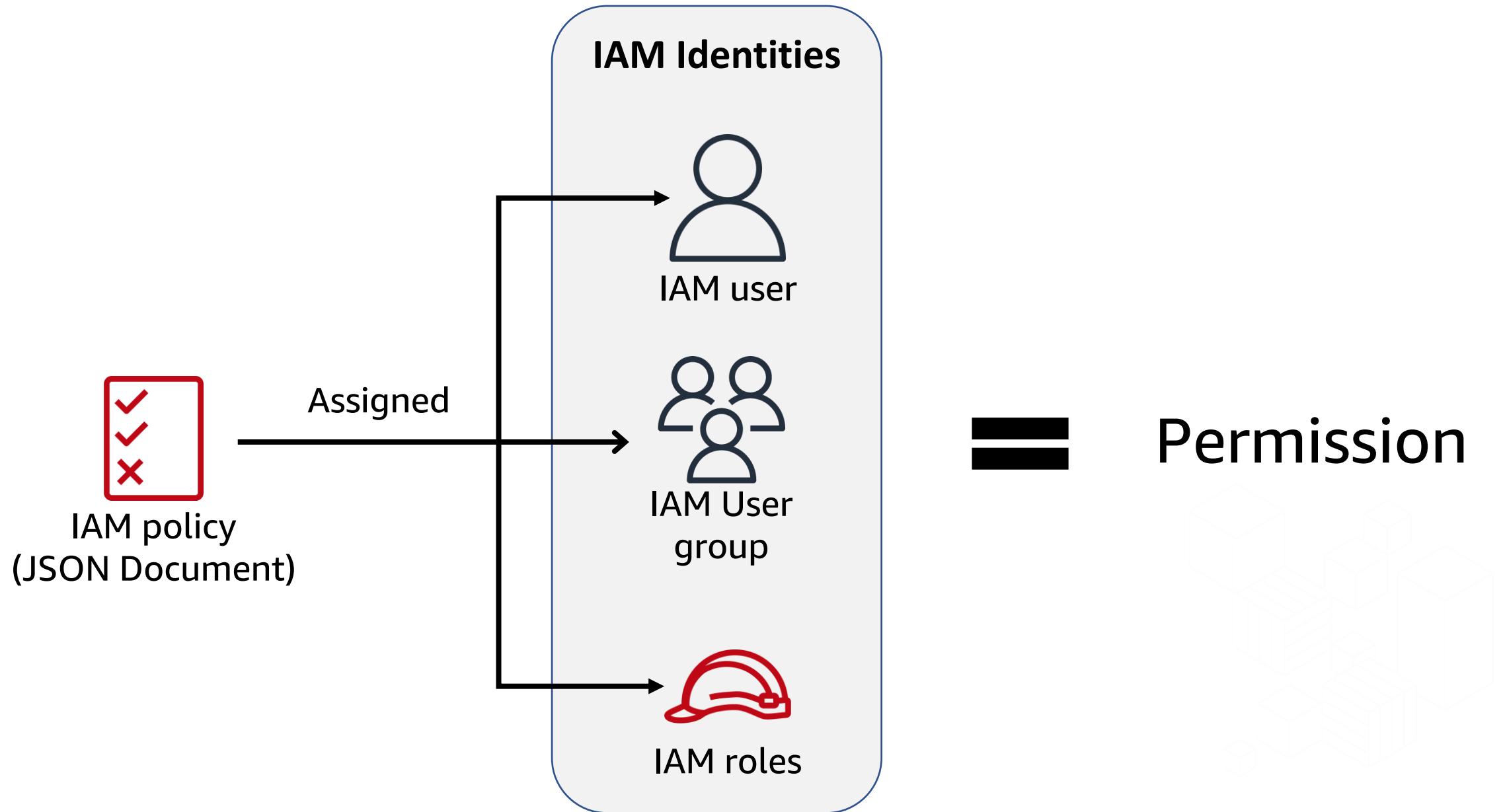
```
1 [default]
2 aws_access_key_id = Access Key
3 aws_secret_access_key = Secret Access Key
4 |
```

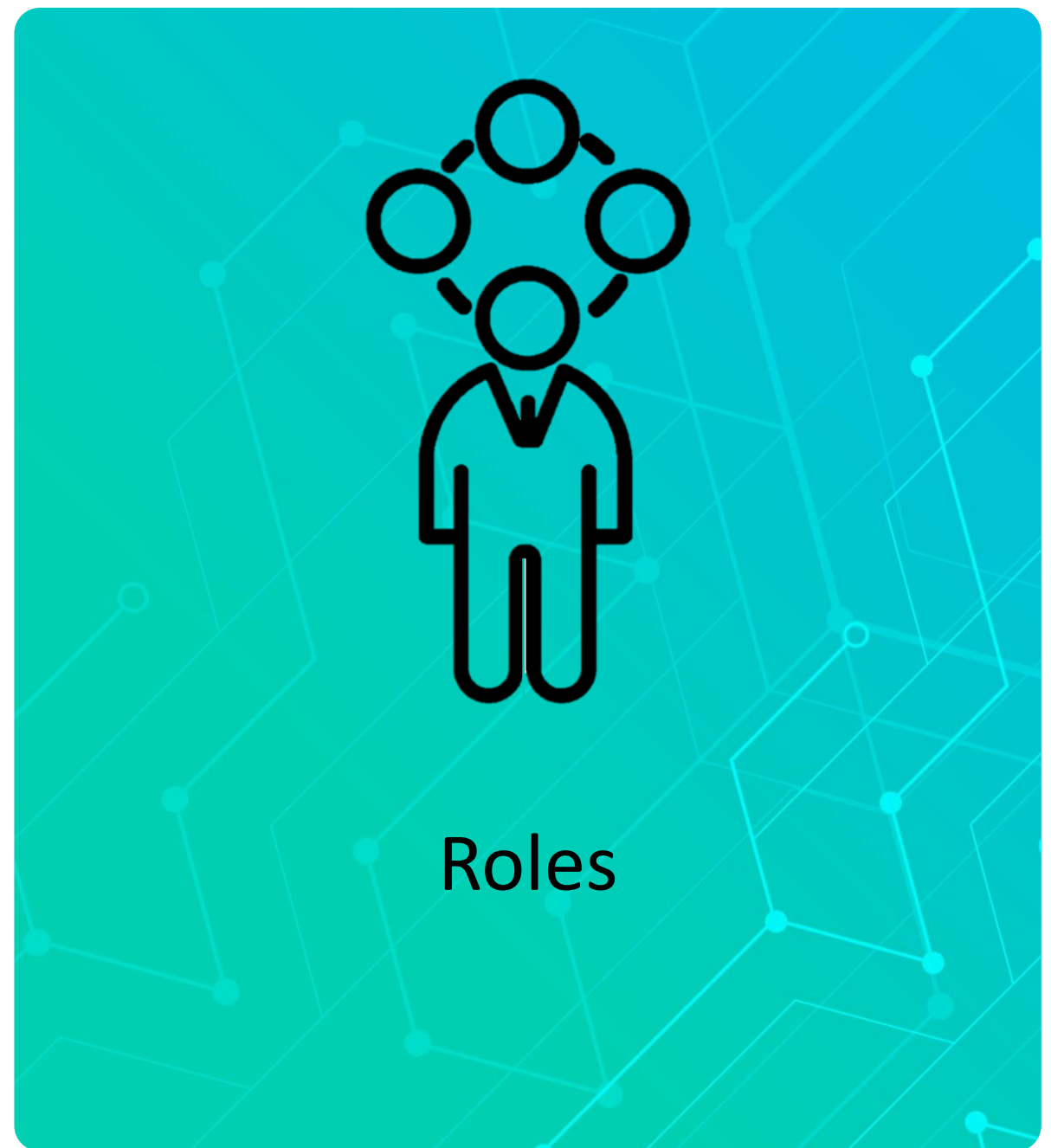


AWS Tools  
and SDKs



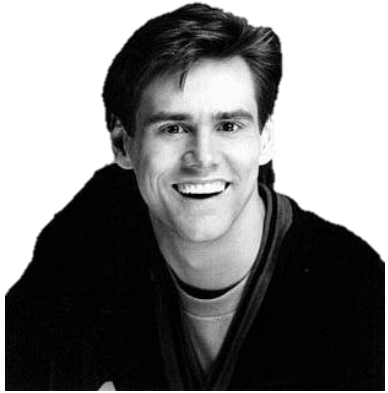
# Permission







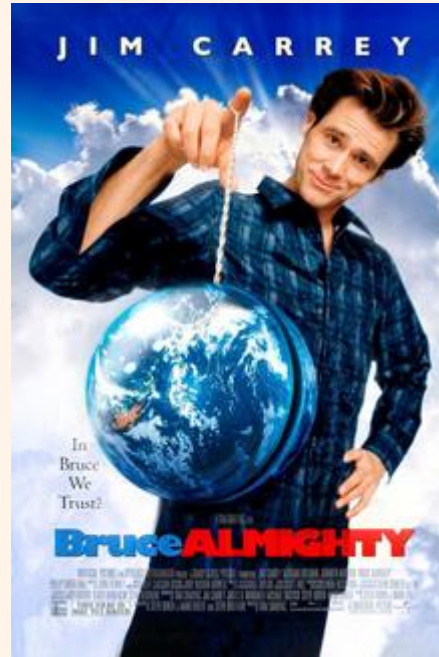
# Understanding Role



Jim Carrey

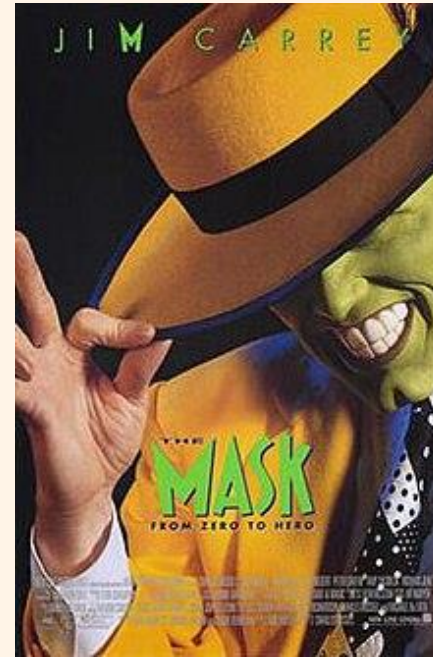
Canadian-American  
Actor

Bruce Almighty



Role  
God

The Mask



Role  
The Green Thing

Ace Ventura



Role  
Pet Detective

## Assuming a role



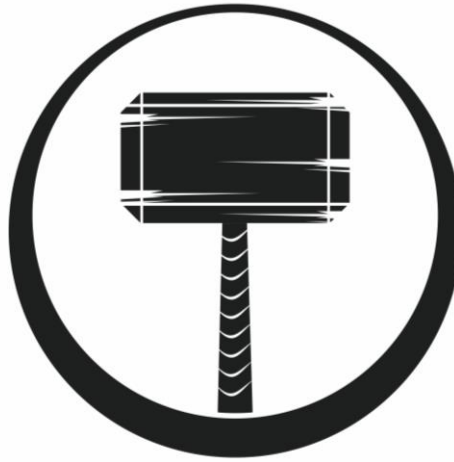
<https://cinespia.org/event/the-mask/>

<https://www.youtube.com/watch?v=GEVfiRbYA8o>



# Trust Policy

- Mjölner - can only be lifted by Thor. It trusts Thor to lift it.

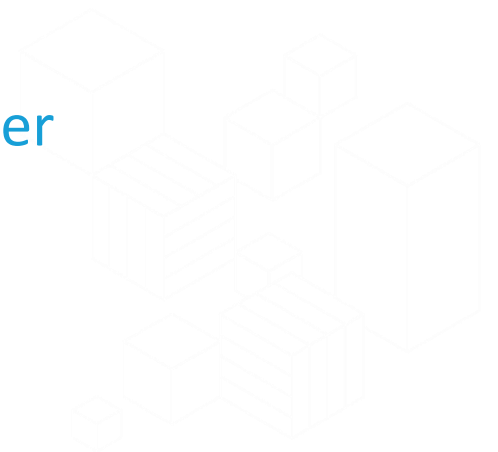


Mjölner trusts Thor

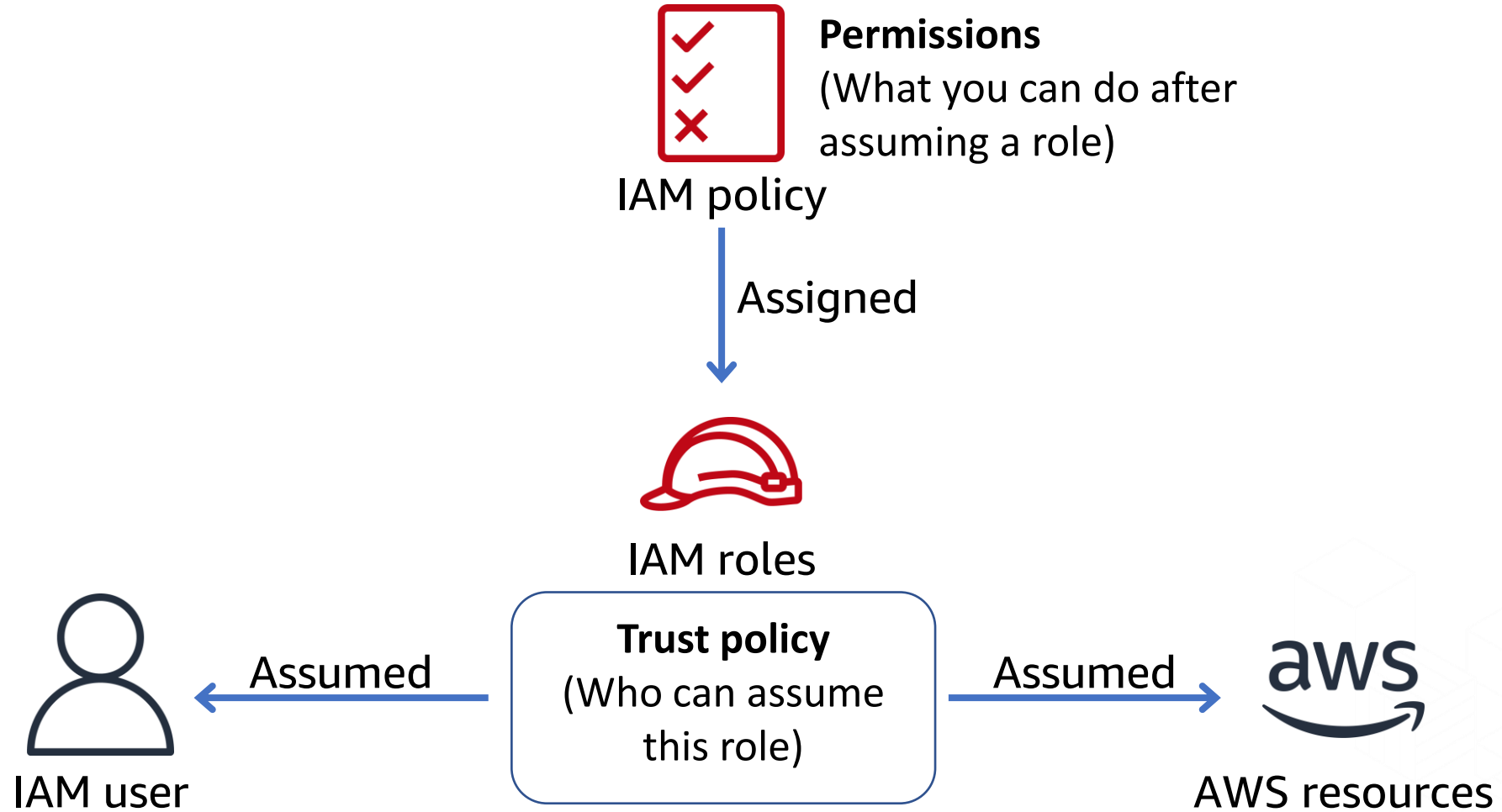


## Business Requirement

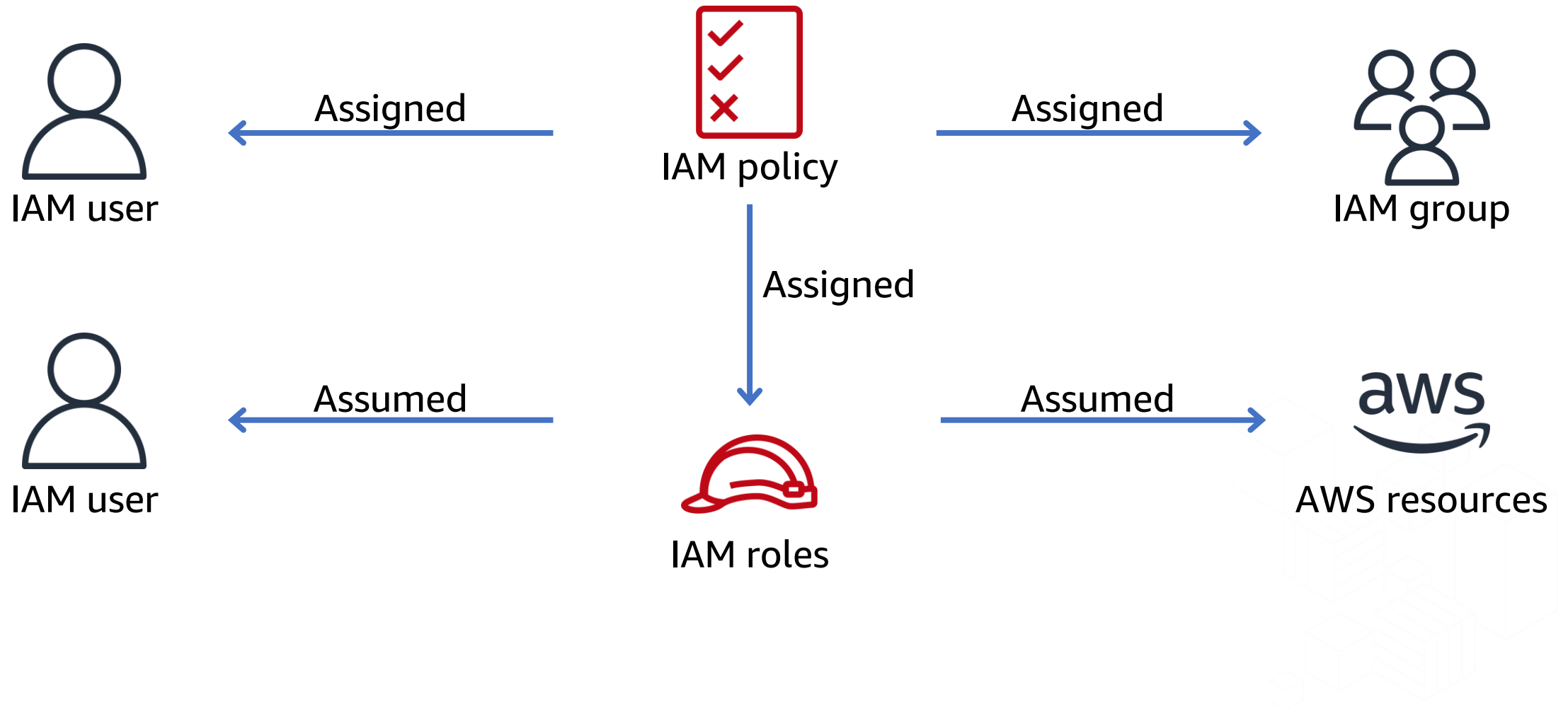
- Allow Q1 user to assume a role, giving him/her permission equivalent to a developer user
- Three Step Process:
  1. Create a Role
  2. Add Q1 as a trusted principal to assume the role
  3. Add permissions to Role which are equivalent to a developer user



# IAM Role – Trust Policy



# IAM Role





## Facts to remember

- Roles can be assumed within AWS account or across AWS accounts.
- At a time only one role can be assumed.
- Trusted Entities to assume a role can be external (SAML / Web Identity).
- Behind the scene AWS Security Token Service (STS) generates a set of temporary security credentials that you can use to access AWS resources.

[Try Web Identity Federation Playground](#) - 

