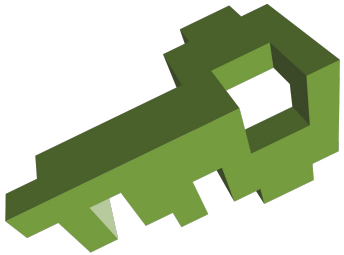


IAM

Identity and Access Management

Part 2

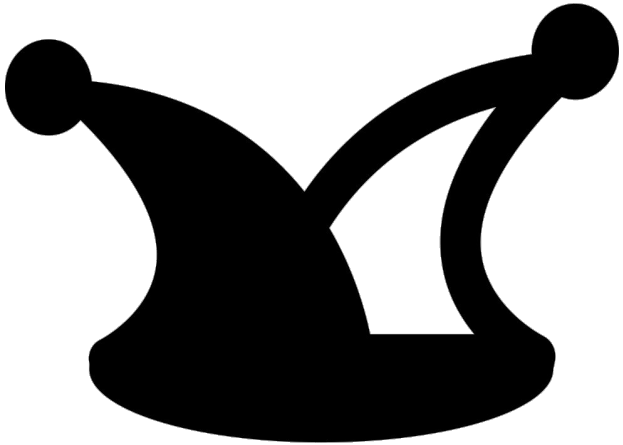
IAM Identities

user

role

Provides authentication for people and processes

IAM Roles



Roles are identity wild cards. They are assumed by whoever/whatever needs it

IAM Roles

Roles can be assigned policies like a user

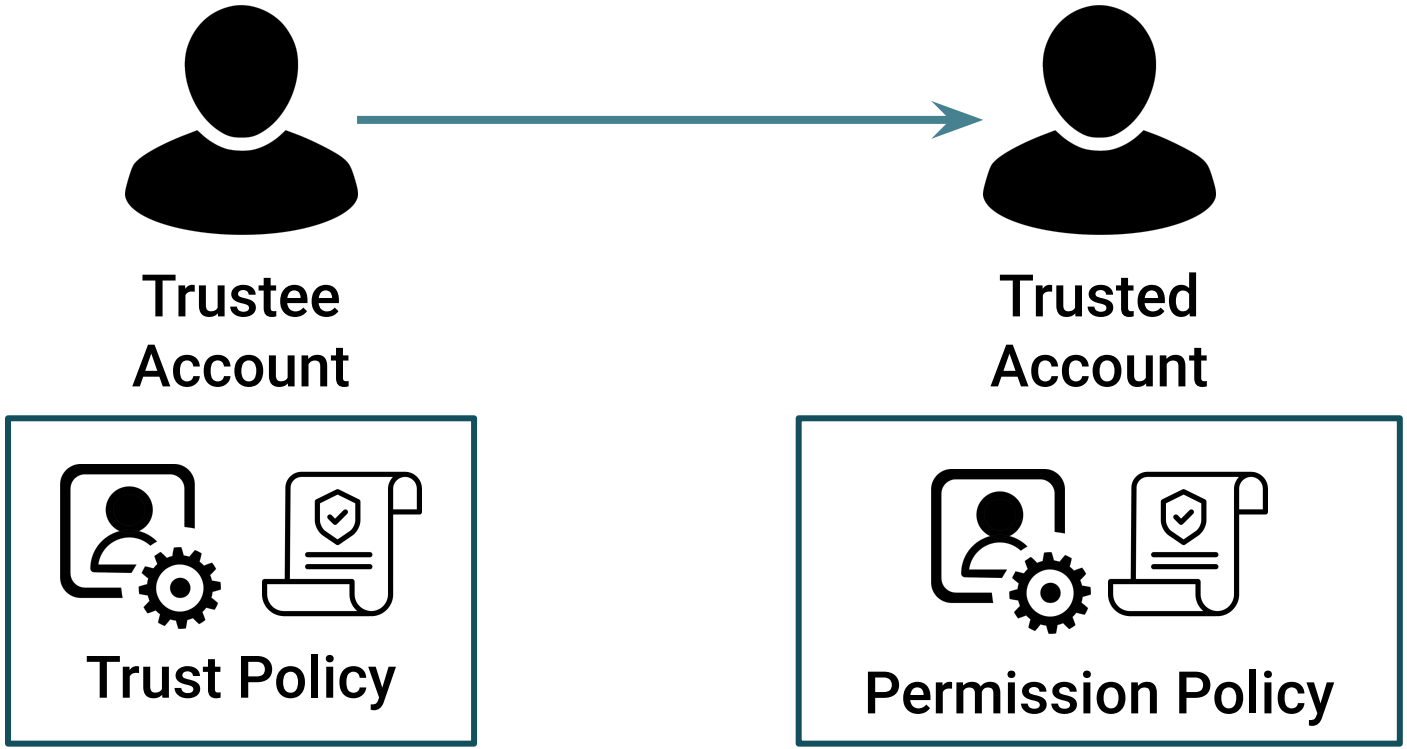
AWS Service Role

A lambda function might need permissions to access an S3 bucket or dynamoDB table

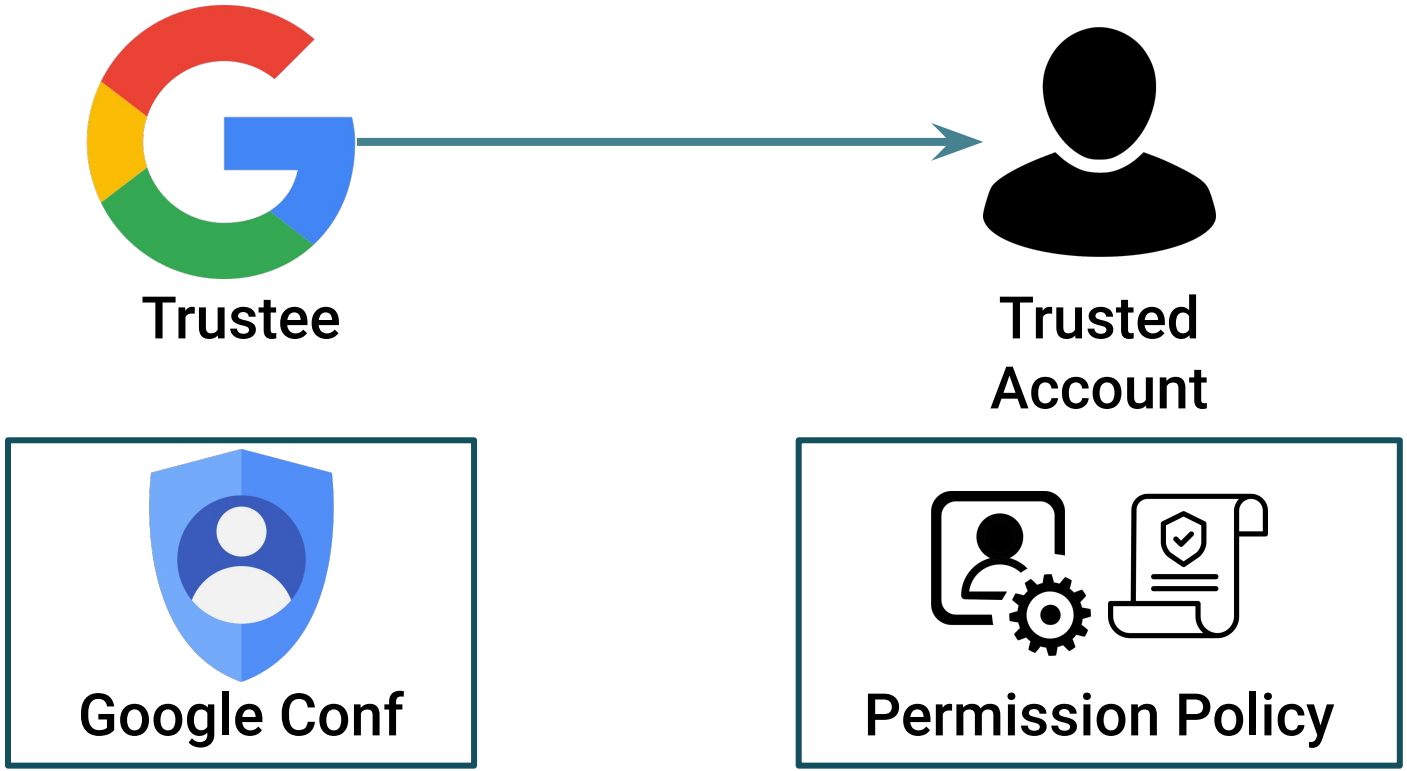
Delegation

A user from another account might want to access resources in your AWS account

Delegation


Trustee
Account
Trusted
Account
Trust Policy
Permission Policy

Federation



IAM best practices

9. Use Roles to Delegate Permissions
10. Do Not Share Access Keys

IAM Characteristics

1. Centralized
2. Fine-grained
3. Secure by default

STS

Security Token Service

Requests credentials for IAM identities

IAM Limits

link