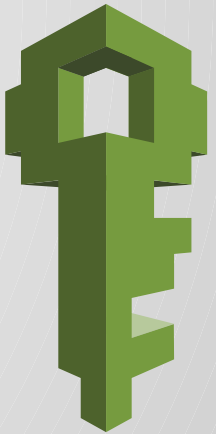
REA AWS Training

Identity and Access Management (IAM)

Basic IAM

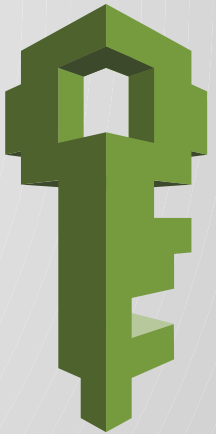
- Identity and Access Management
- “It gives people or things access to other things”
- Global service
- Concepts
  - Users (Long live credentials)
  - Roles (Short live credentials)
  - Policies
    - Resource-Based (SQS, S3, SNS, Lambda)
    - User-Based (IAM Role, User, Group)



What does this have to do with me?

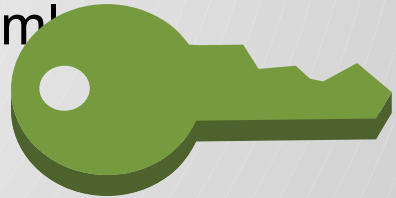
- Root user has access to **everything**
- We could create IAM Users with the right scope
- But long lived and shared credentials are a bad idea
- So we use IDP and temporarily assume IAM Roles
  - Like the IAM Role “REA-Training-User”

- IAM Roles are defined by their IAM Policies...



IAM policies

- Access controls to users, groups, roles
- Default DENY
- Apply controls based on principal, API call, resource plus conditions
- Managed policies
- Policy generator
  - https://awspolicygen.s3.amazonaws.com/policygen.html



Example IAM policy

```
Statement:
- Sid: PermitStartAndStop
  Action:
  - ec2:StartInstances
  - ec2:StopInstances
  Effect: Allow
  Resource: "*"
  Condition:
    IpAddress:
      aws:SourceIp: 203.17.253.249/32
```

IAM and EC2 Instances

- EC2 Instances invoking services
- Instance has an Instance Profile
- The Instance Profile assumes an IAM Role
- IAM Role has associated IAM Policies
- IAM Policies give access to other services

IAM: Hands on

./iam-user/hands-on.md

- Create an IAM user
- Test access
- Attach and detach policies
- Delete user