Cloud-based Data Management

AWS Storage

Ira A. Fulton Schools of Engineering
Arizona State University

Objective

Objective

Explain AWS services

Security

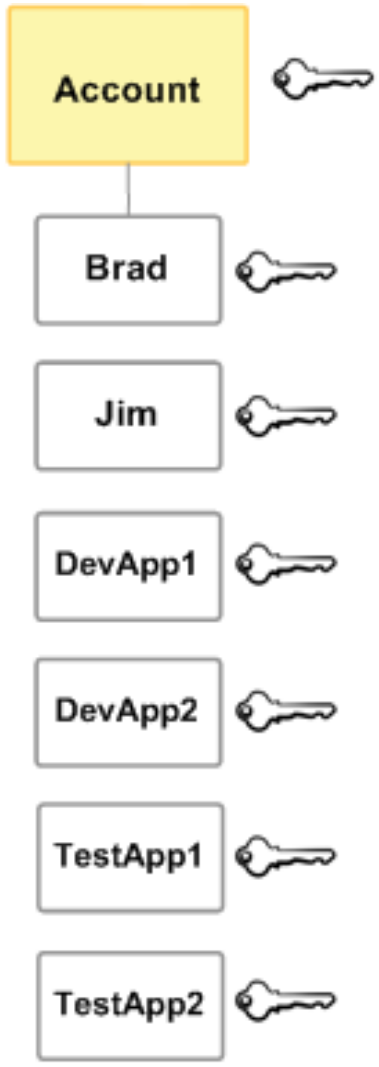
Security credentials are required to access EC2 using command line tools and API

EC2 Key Pairs

- Public key used to encrypt a piece of data (e.g., password)
- Private key used to decrypt the data—keep your private key private and safe!
- Create a key pair using EC2, or upload your own key pair
- Lose your private key, involved process to connect to your instance—check user guide

AWS Identity & Access Management (IAM)

- Use IAM to allow other users, services, and applications to use your EC2 resources
- Do not use your AWS root account for day-to-day interaction with AWS
  - Root account provides unrestricted access to your AWS resources



AWS Identity & Access Management (IAM)

Use IAM to allow other users, services, and applications to use your EC2 resources without sharing your root security credentials

- Create users and groups under your AWS account
- Assign unique security credentials to each user under your AWS account
- Control each user's permissions to perform tasks using AWS resources
- Allow users in another AWS account to share your AWS resources
- Create roles for your AWS account and define users or services that can assume them

Security Group

- A virtual firewall that controls the traffic for instances
- You can add rules to a security group to allow/block traffic to/from its associated instances
- When deciding whether to allow traffic to an instance, EC2 evaluates all rules from all security groups associated with an instance

Security Group