IAM ESSENTIALS

Amazon Web Services

What is IAM?

- **IAM** (**I**dentity & **A**ccess **M**anagement) is where you manage your AWS users and their access to AWS accounts and services.

- The common use of **IAM** is to manage:
  - ***Users***
  - ***Groups***
  - ***IAM Access Policies***
  - ***Roles***

NOTE: The user created when you created the AWS account is called the "root" user.

- By default, the root user has ***FULL*** administrative rights and access to every part of the account.

- By default, any new users you create in the AWS account are created with ***NO*** access to any AWS services (except the ability to log in).

- For all users (besides the root user), permissions must be given that grant access to AWS services.

IAM initial setup & Configuraration

IAM Initial Configuration:

- ***AWS Best Practices:*** Guidelines that recommend settings, configurations and architecture for the purpose of having a high level of security, accessibility and efficiency.

- When a new AWS root account is created, it is "***best practice***" to complete the tasks listed in IAM under "***Security Status***".

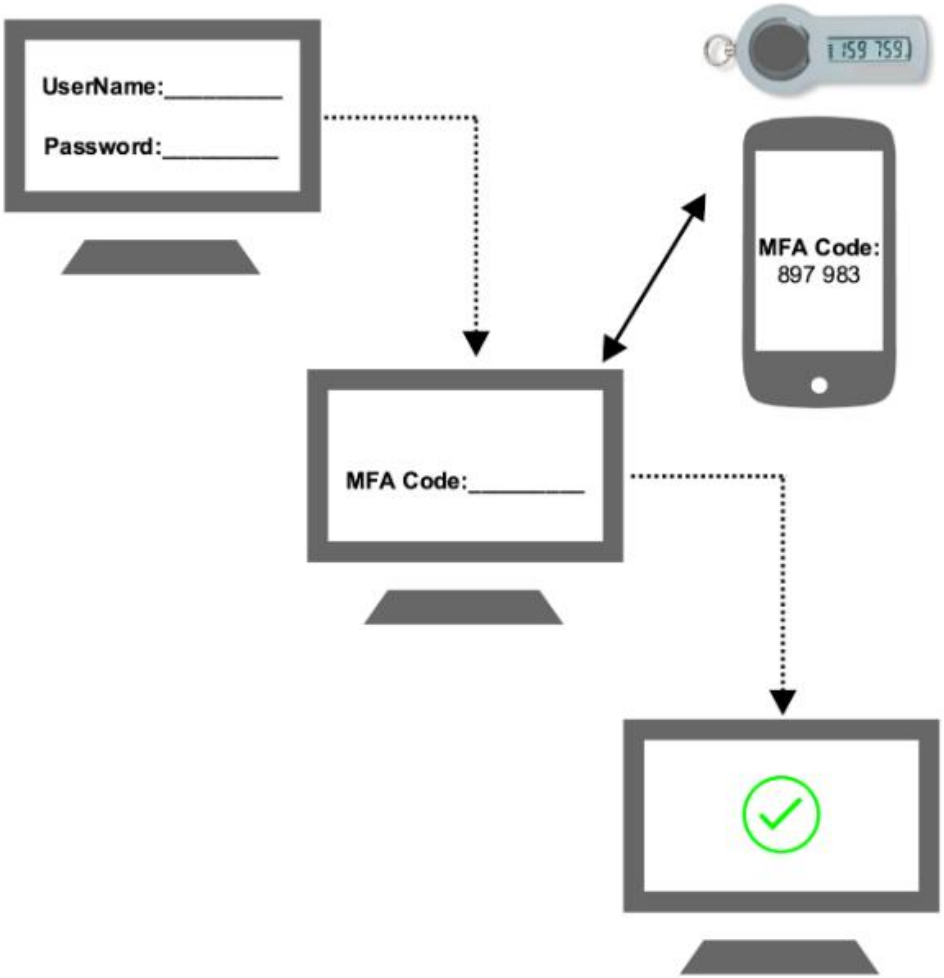
- Those tasks include:
  - **Delete your root access keys**
  - **Activate MFA on your root account**
  - **Create individual IAM users**
  - **User groups to assign permissions**
  - **Apply an IAM password policy**

Activate MFA on your Root Account:

- What is **MFA**?
  - **MFA** is an abbreviation for **M**ulti-**F**actor **A**uthentication.
  - It is an additional layer of security on your root account that is provided by a 3rd party.
  - And it takes the form of a continually-changing, random six digit code that you will need to input (in addition to your password) when logging into your root account.

- How do I get the **MFA** code?
  - **Virtual MFA Device:**
    - Smartphone or tablet.
    - Commonly used app (iOS & Android): Google Authenticator.

  - **Hardware Key Fob:**
    - Small physical device with a display that you can attached to your keychain.
    - Order it directly from AWS.



QUALITY THOUGHT
INFO SYSTEMS (INDIA) PVT. LTD

Create Individual IAM Users:

- AWS ***best practice*** is to **NEVER** use your root account for day-to-day use.
- If you want full admin access for yourself, create an IAM user and attach the "**AdministratorAccess**" policy to it.
- Then use that account as your daily driver.

Use Groups to Assign Permissions:

- It can often be more convenient and efficient to set up groups and assign permissions to the group rather than manage each user individually.

Apply an IAM Password Policy:

- A password policy dictates the format and expiration rules that must be followed when a user creates or modifies their password.

- These rules include password:
  - Length
  - Case requirements
  - Number requirements
  - Non-alphanumeric requirements
  - Password expiration
  - Password reuse
  - User rights to change their own password
  - Administrator reset requirements

IAM Users and policies

What is IAM?

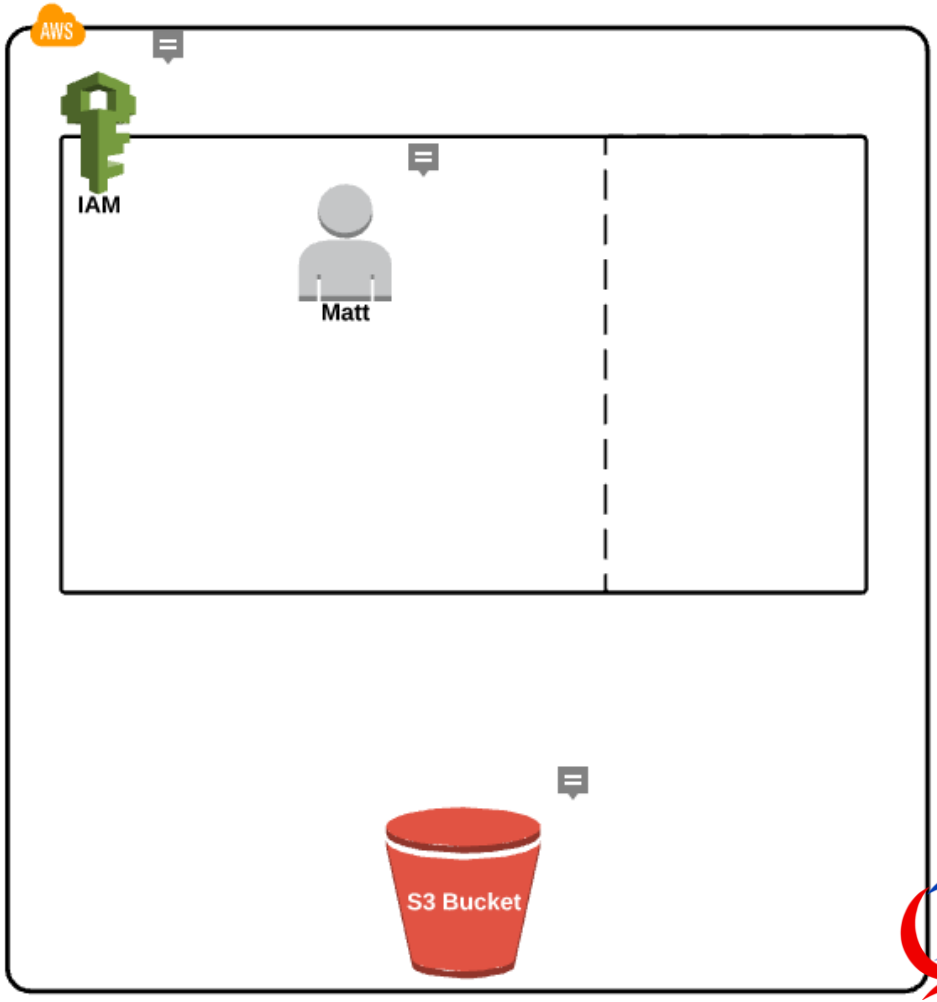
- **IAM** (**I**dentity & **A**ccess **M**anagement) is where you manage your AWS users, and their access to AWS accounts and services.

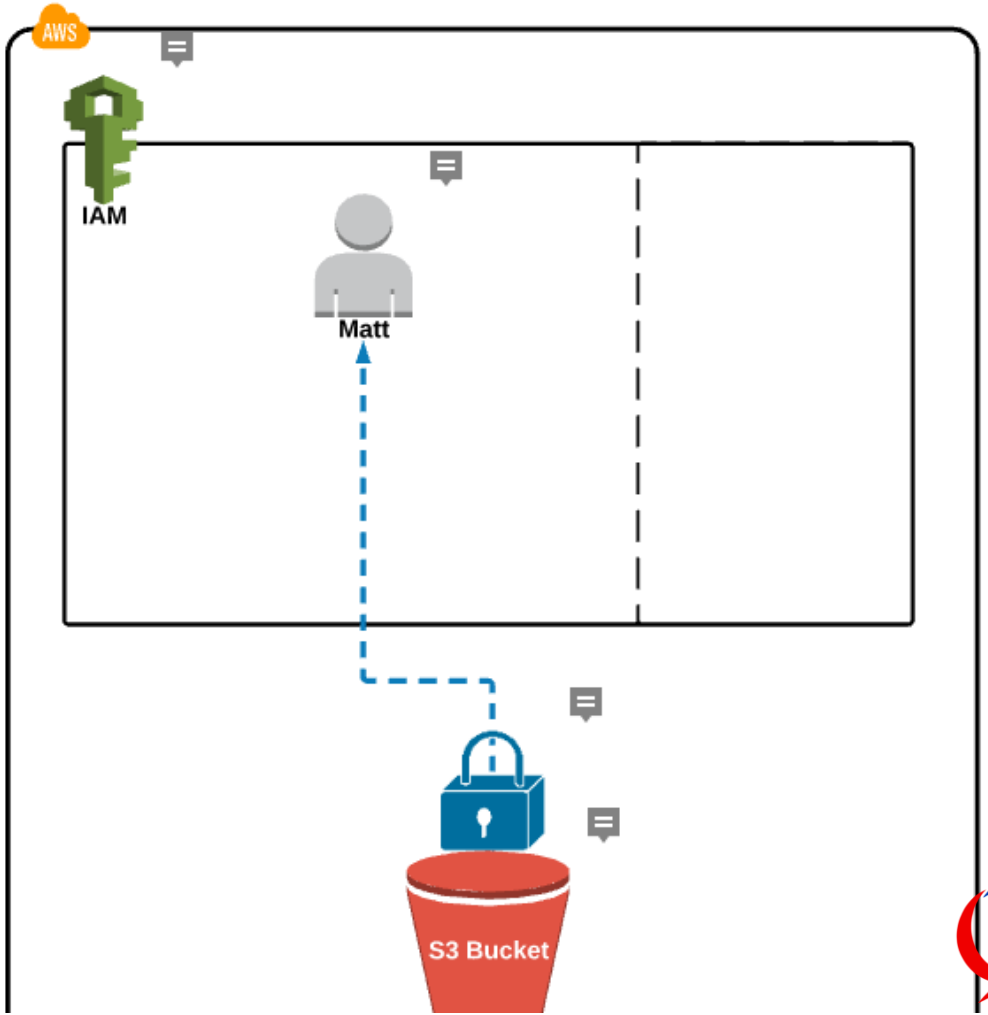
- The common use of **IAM** is to manage:
  - ***Users***
  - ***Groups***
  - ***IAM Access Policies***
  - ***Roles***

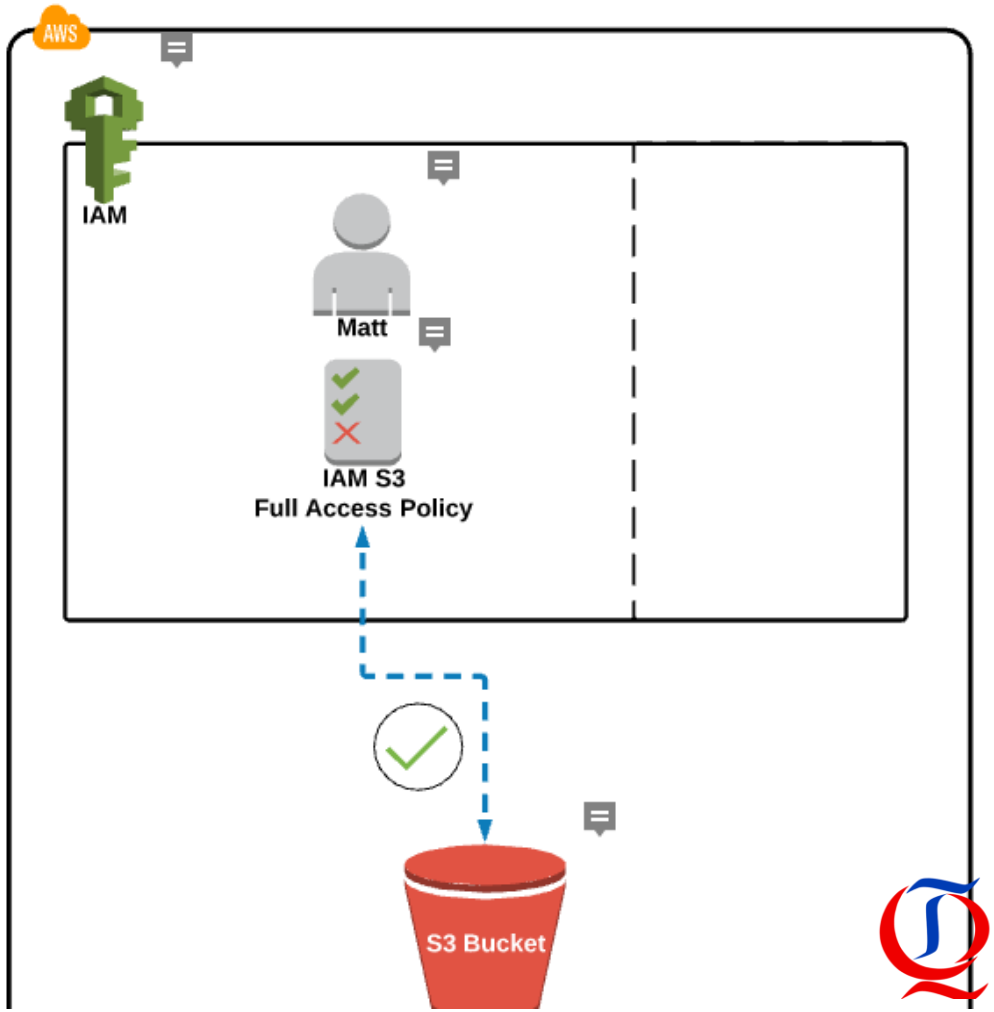
NOTE: The user created when you created the AWS account is called the "root" user.

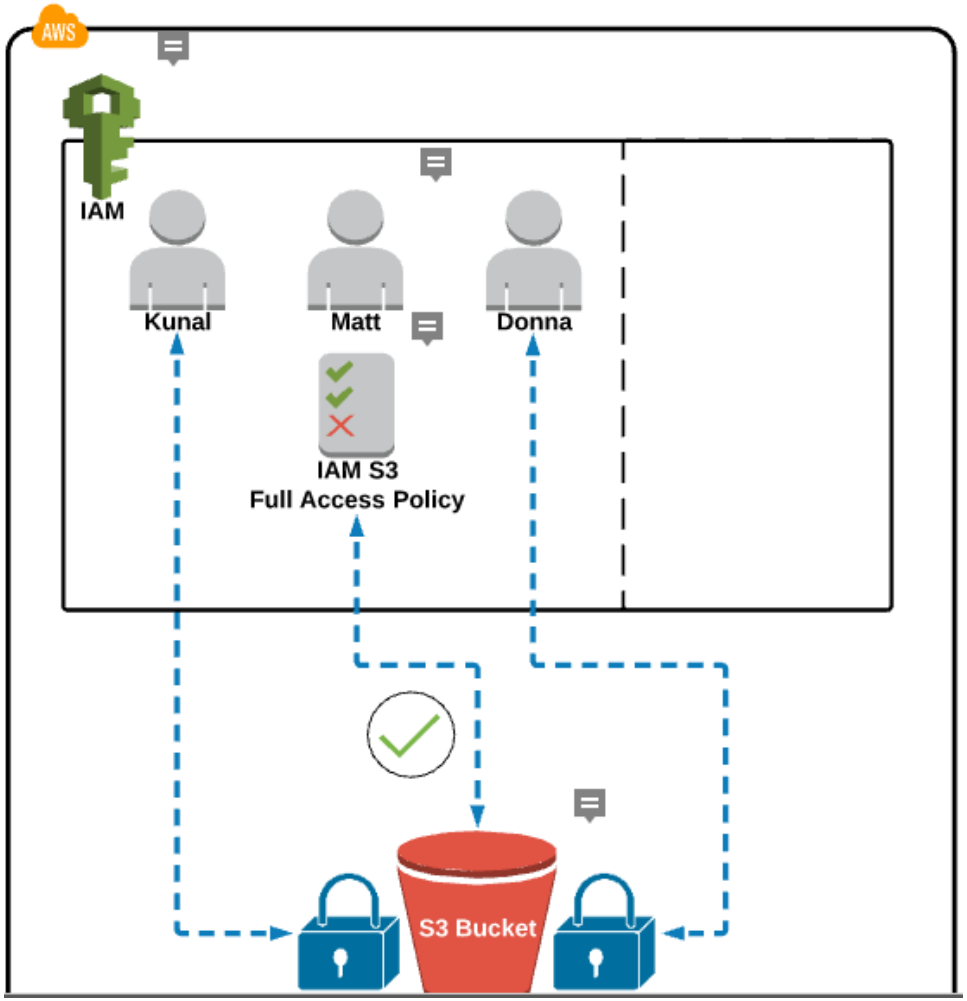
- By default, the root user has ***FULL*** administrative rights and access to every part of the account.

- Any new or additional users you create in the AWS account are created with ***NO*** access to anything by default (except the ability to log in).

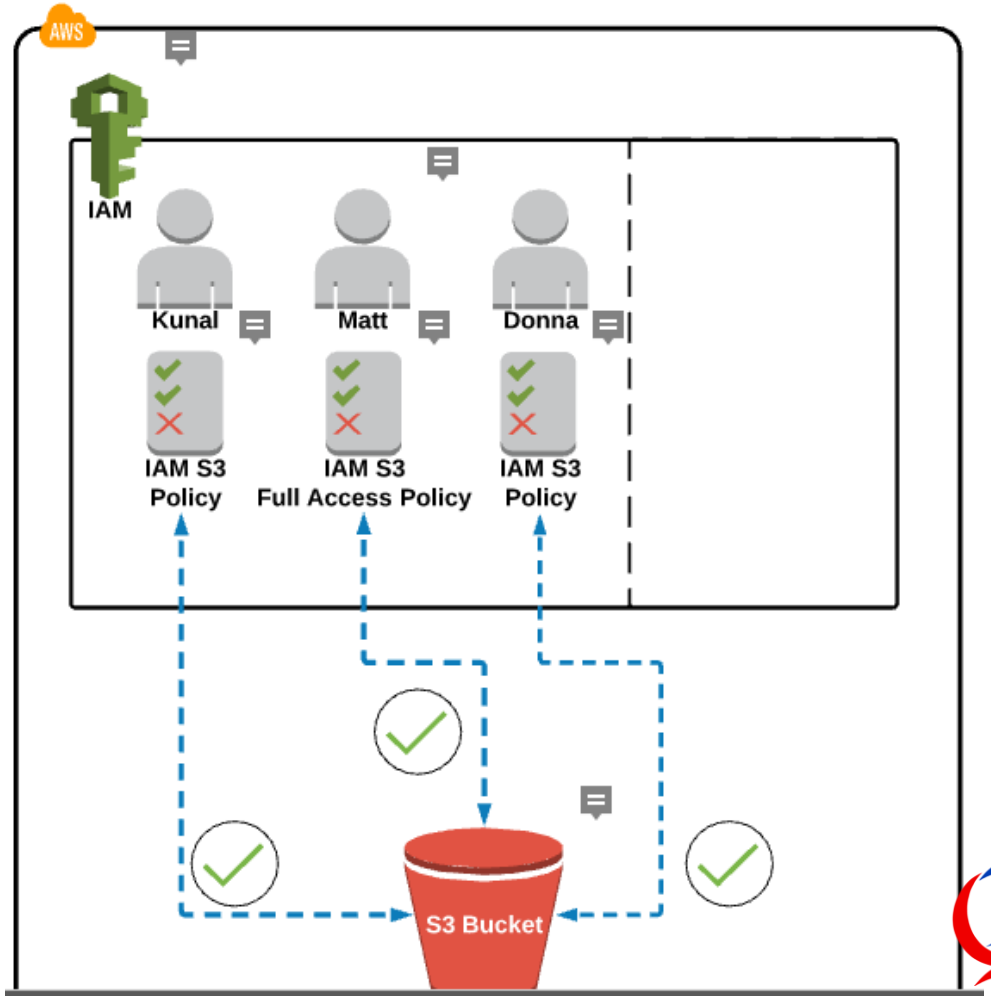




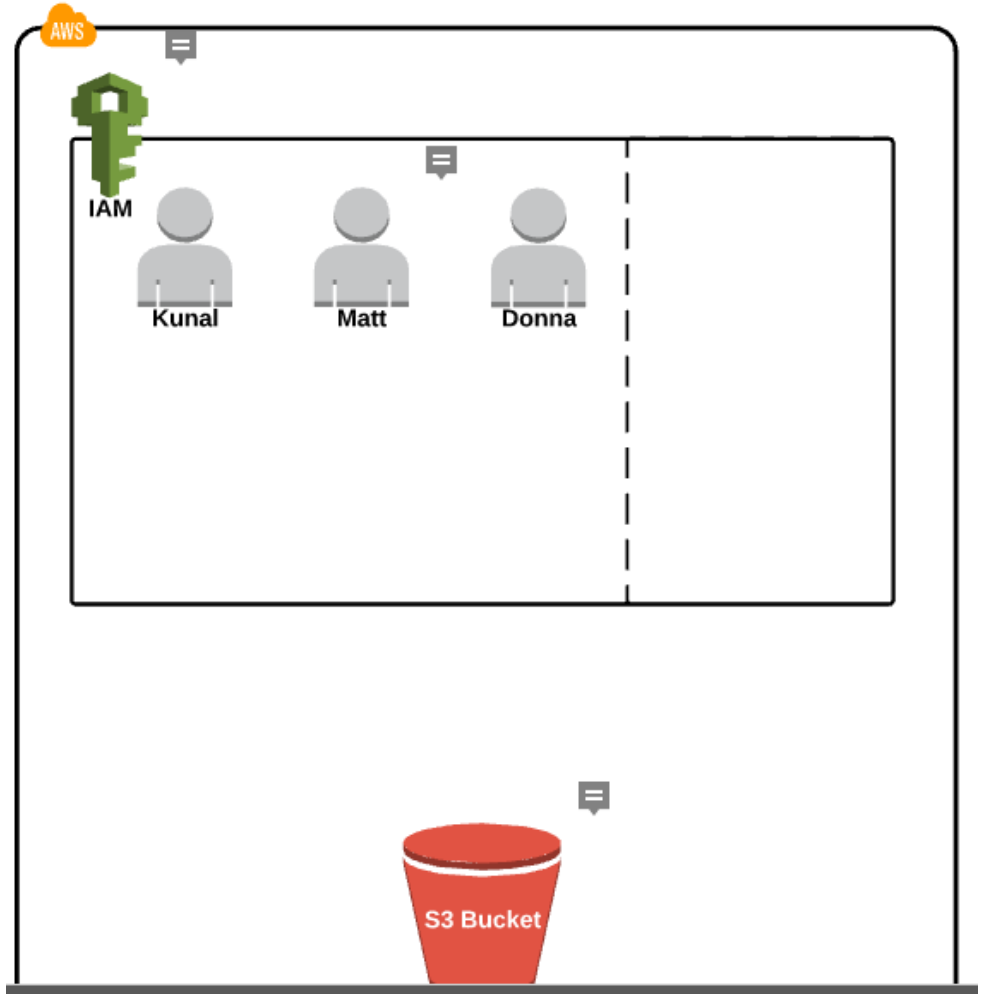


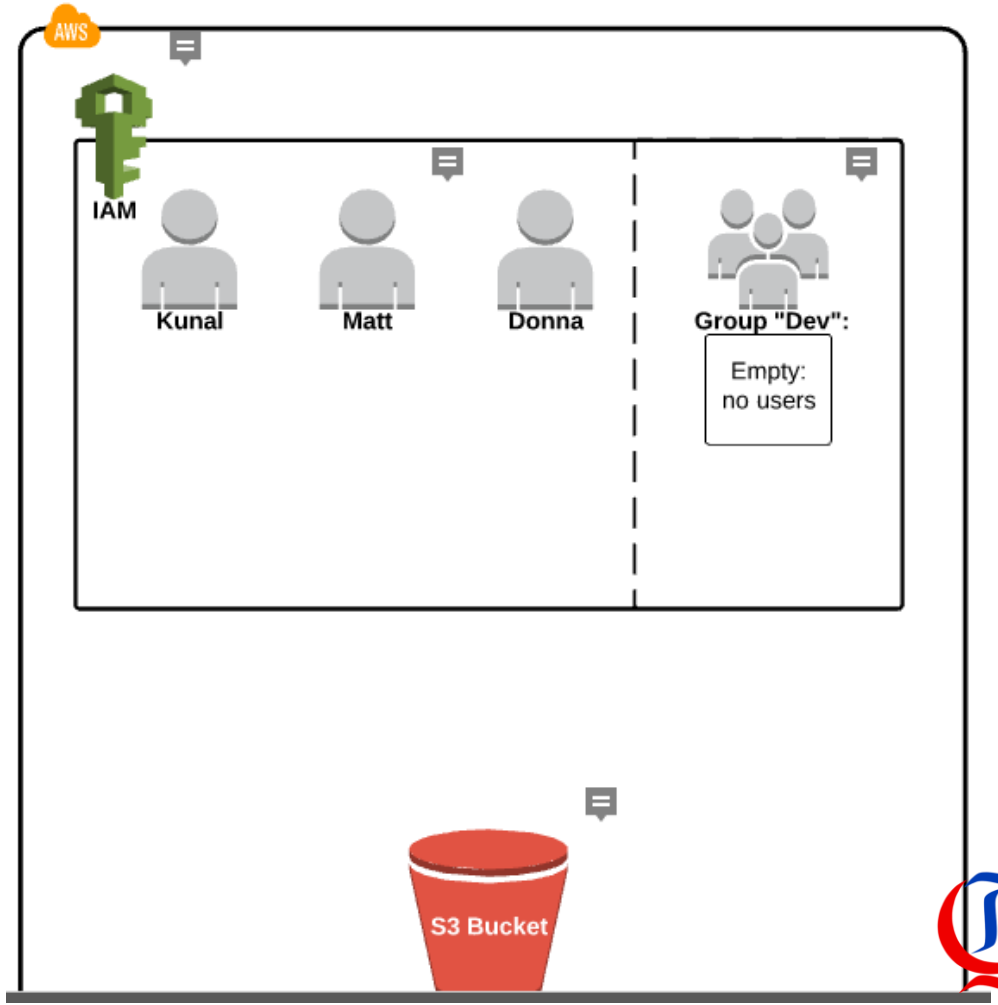


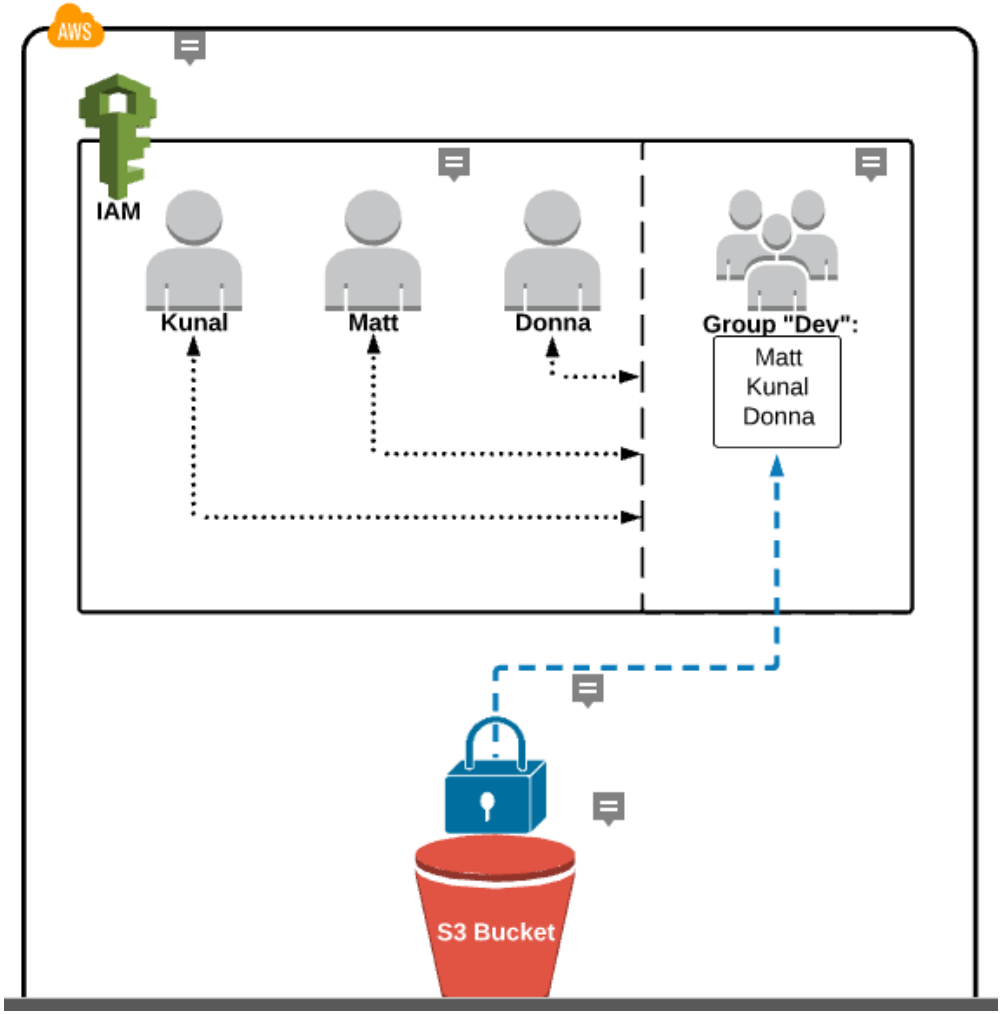
QUALITY THOUGHT
INFO SYSTEMS (INDIA) PVT. LTD

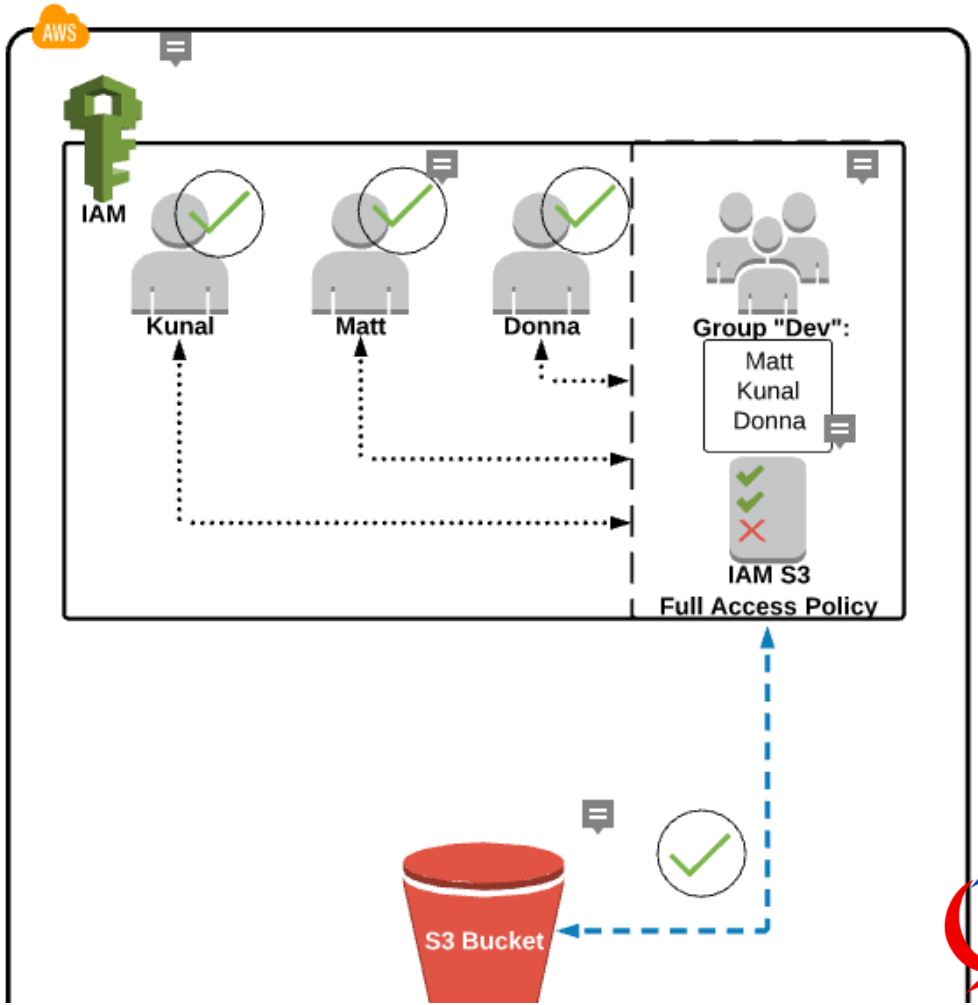


IAM Groups and Policies









IAM ROLES