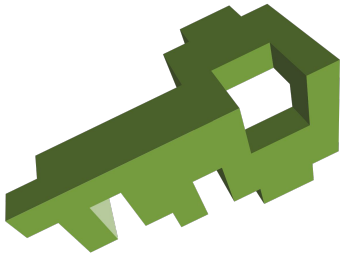
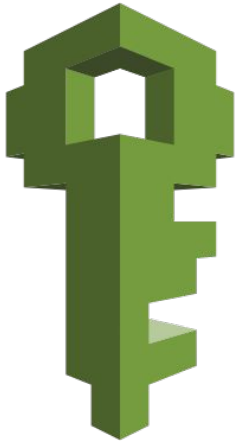


IAM

Identity and Access Management



IAM controls access to AWS resources

Two access points

Root account

1. Has no restrictions
2. It cannot be disabled or discontinued

Admin Account

1. Has restrictions imposed by the Root Account
2. It can be disabled or discontinued

Development environment

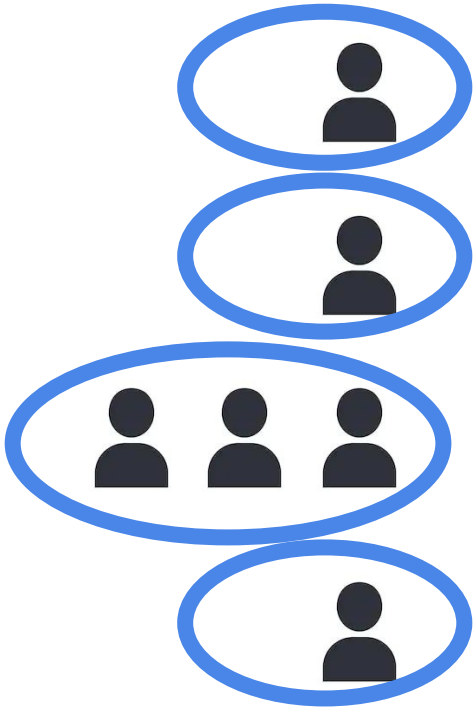
Three steps:

1. Identify who will access the environment
2. Create the users and group them
3. Give users permission

#1. Identify who will access the environment

1. Client
2. Accounting people
3. Team
    a. Developers
    b. Testers
    c. PM, Scrum master, etc...

#2. Create the users and group them



1 user for the client

1 user for an auditor

3 users for developers

1 user for Administration

You make sure each user is part of at least one group

#3. Give groups permissions

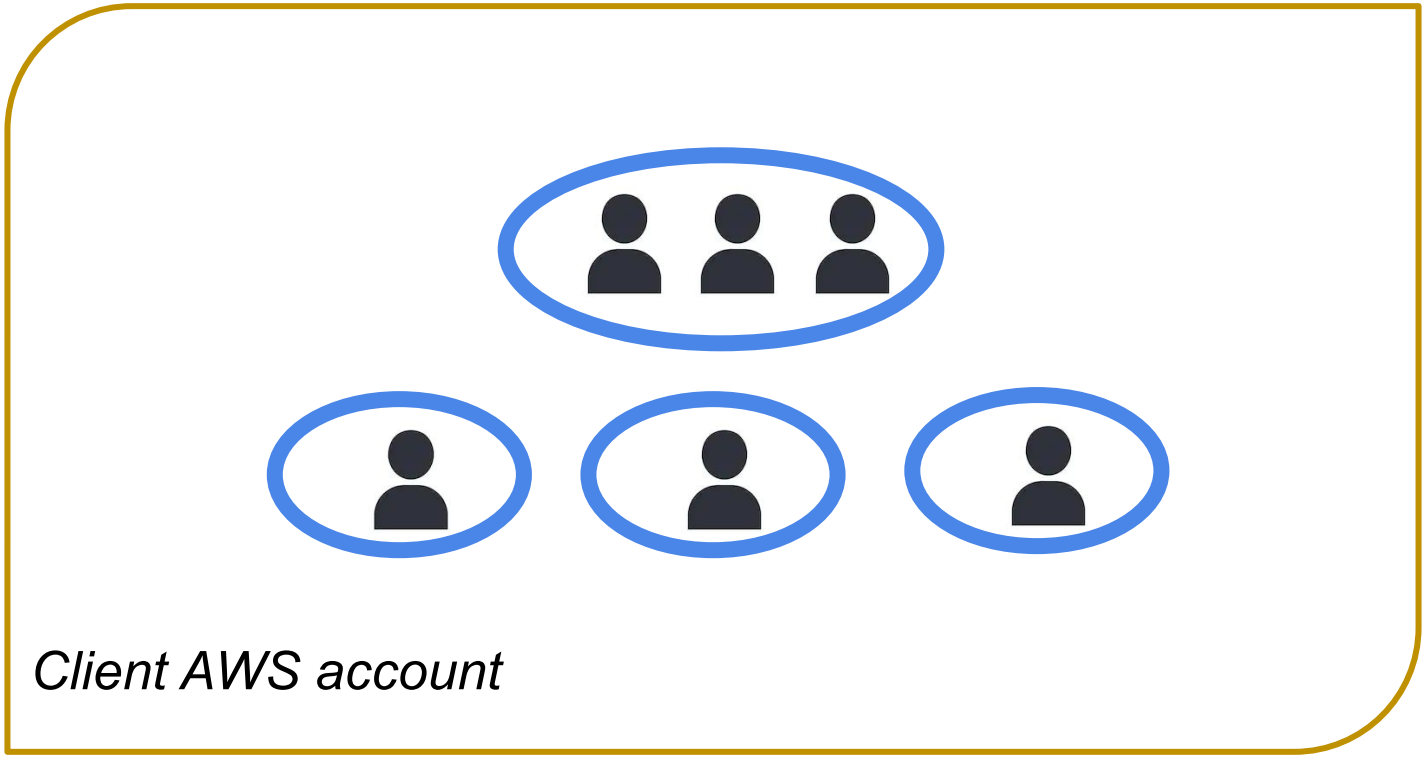
Developer Group: Full Access to AWS Services

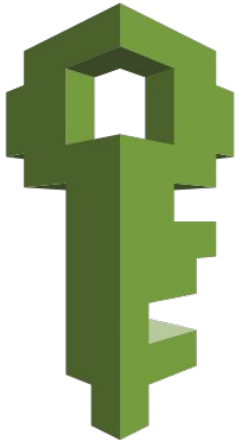
Accounting Group: Access to the billing board

Client Group: Read Only Access to AWS Services and Access to billing board

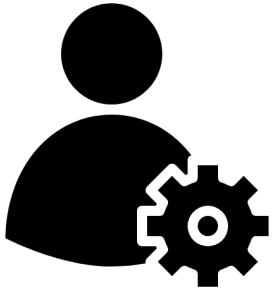
Admin Group: Read Only Access to AWS Services and Access to billing board

All users reside inside one AWS account





IAM controls access to AWS resources



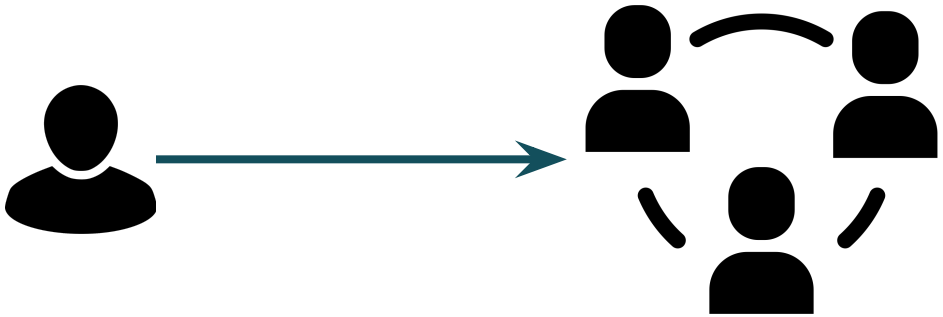
IAM Lab #1

Setup users and groups for aws account

IAM best practices

1. Lock Away Your AWS Account Root User Access Keys
2. Enable MFA (read more here)

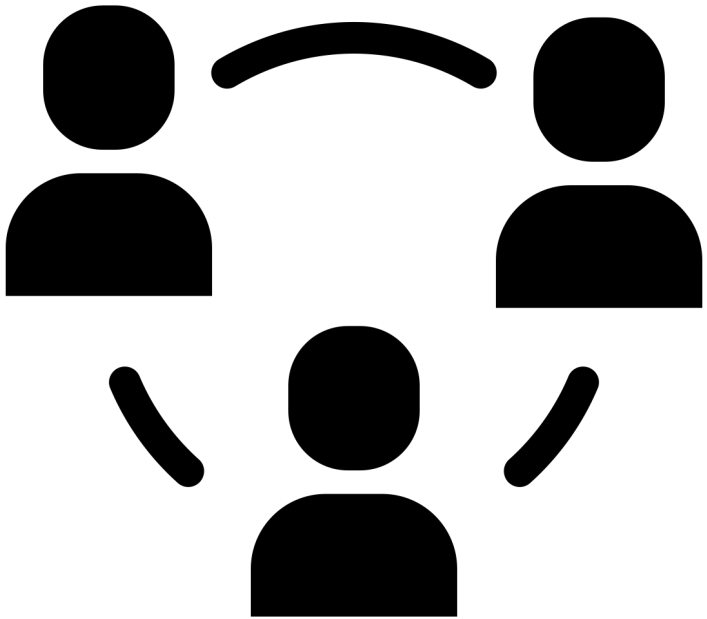
IAM users and groups



1. When a user gets added to a group, it acquires the permissions of the group
2. A user can belong to any amount of groups

IAM best practices

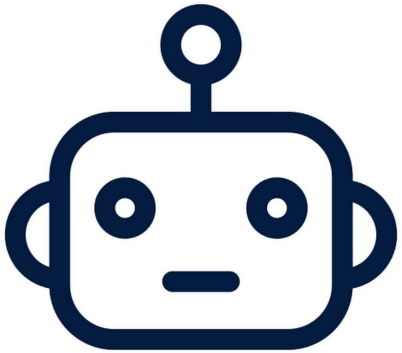
3. Create Individual IAM Users
4. Use Groups to Assign Permissions to IAM Users



IAM users

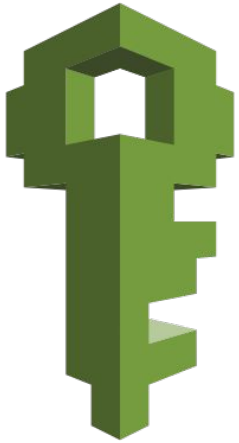
IAM users can represent

1. An actual user
2. An application or program



IAM best practices

5. Grant Least Privilege
6. Configure a Strong Password Policy for Your Users (read more here)



What does IAM do?

Controls access to AWS resources

IAM evaluation

1. Principal (identity)
2. Action
3. Resource
4. Data

1. Verify identity
2. Evaluate policies
3. Allow or deny

IAM Policy evaluation

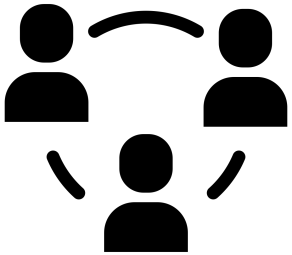
1. An entity has no permissions by default
2. An explicit allow overwrites the default
3. An explicit deny overwrites any allow

Policy types

1. Identity based policies
    a. AWS managed policies
    b. Customer managed policies
2. Resource based policies
3. Inline policies

IAM elements

user



group

policy

role

IAM best practices

7. Prefer using AWS Managed Policies
8. Use Customer Managed Policies Instead of Inline Policies