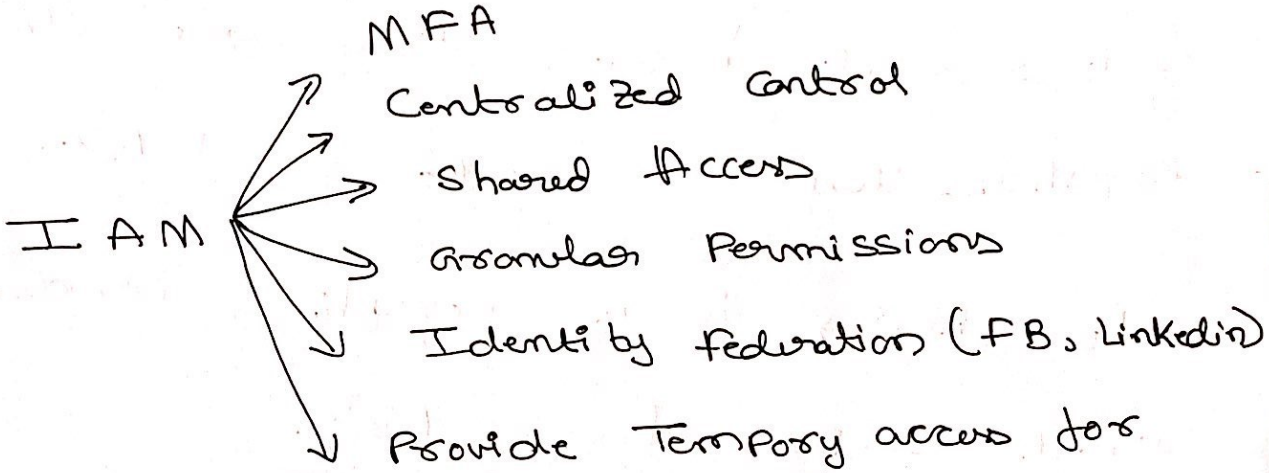
Identity Access Management

→ IAM allows you to manage users and thier level of access to the AWS Console.

→



Users
↓
End users such as Peoples employee etc

Groups
↓
Collection of users.
users inherit group Policies

Policies
↓
Made up of documents.
These are in JSON. which give Permissions what a user/group can do.

Roles
↓
Create a role & assign to AWS Resource

→ IAM is "global"

→ User → Programmatic access
→ Console Sign-in

→ Policy.

```
{
  Version :
  Statement :
      {
      Effect :
      Action :
      Resource :
      }
}
```

→ IAM is universal
→ "root account" is having Complete admin access
→ New users have no Permission when created
→ New users are assigned Access Key ID and Secret Access Keys when first created
→ These are not Same as Password & Can see only once but Can regenerate them.
These are useful to login by Command line

→ Cloudwatch is used to set billing alerts in aws cloud.

→ Power users cannot manage groups and users within IAM.