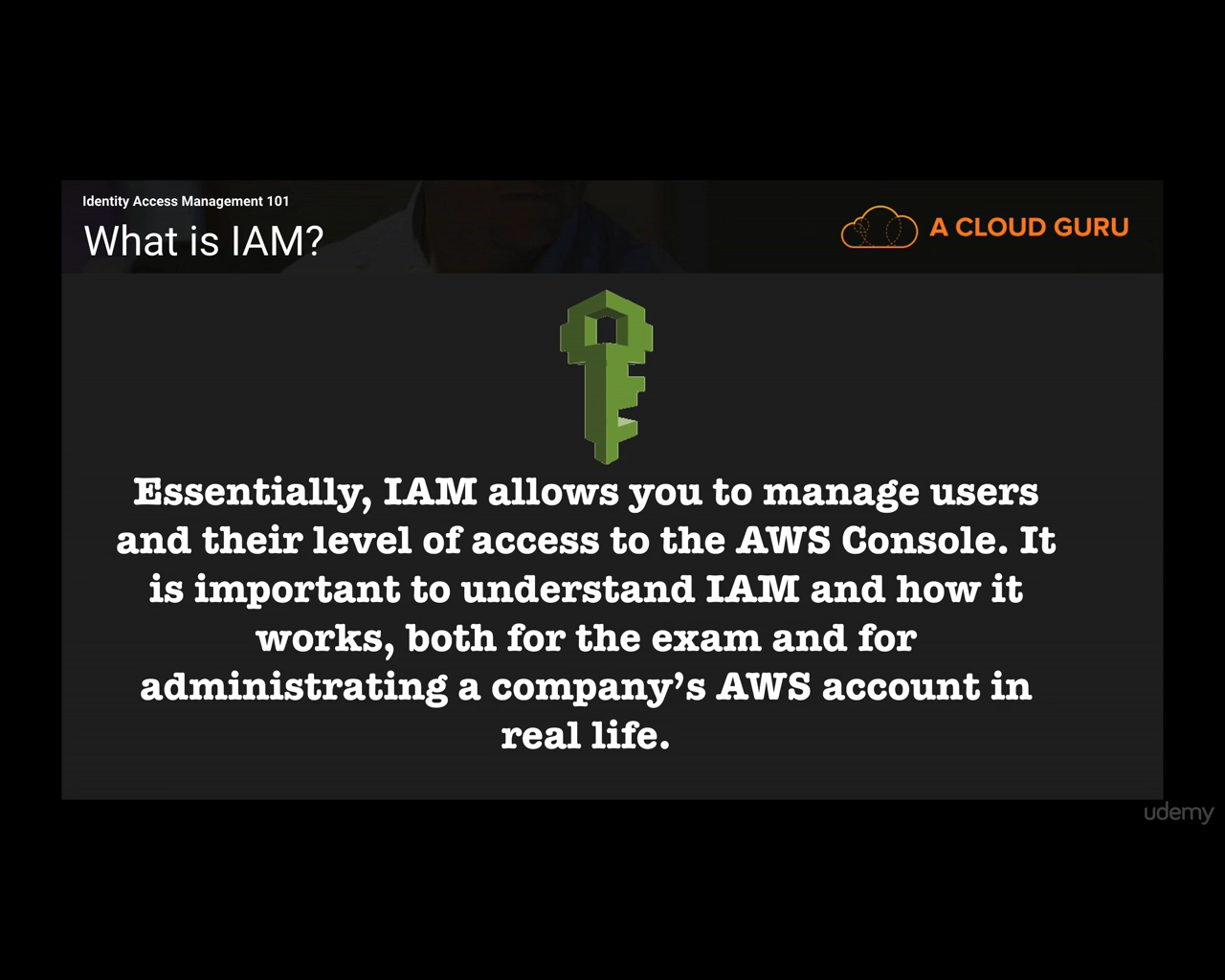
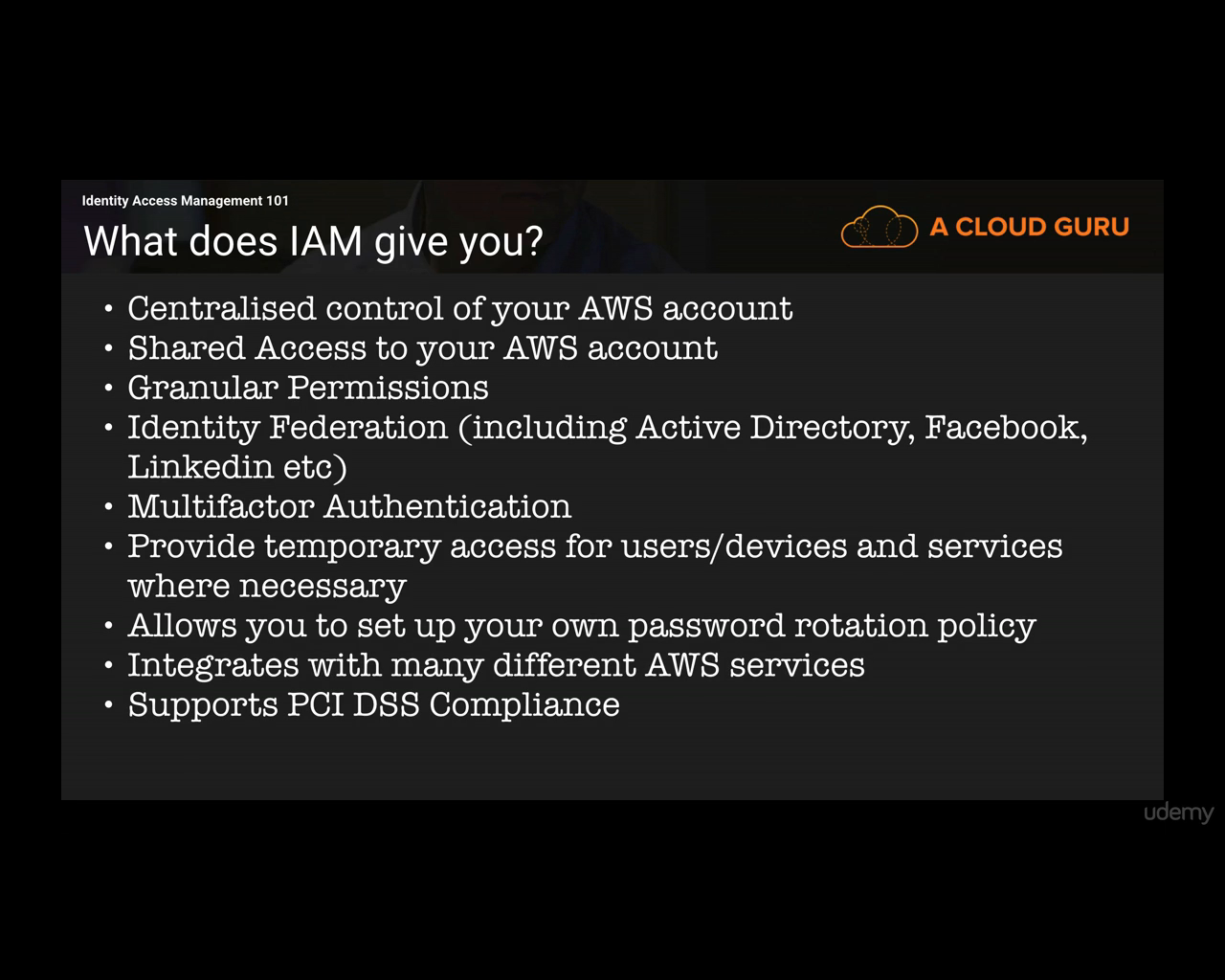
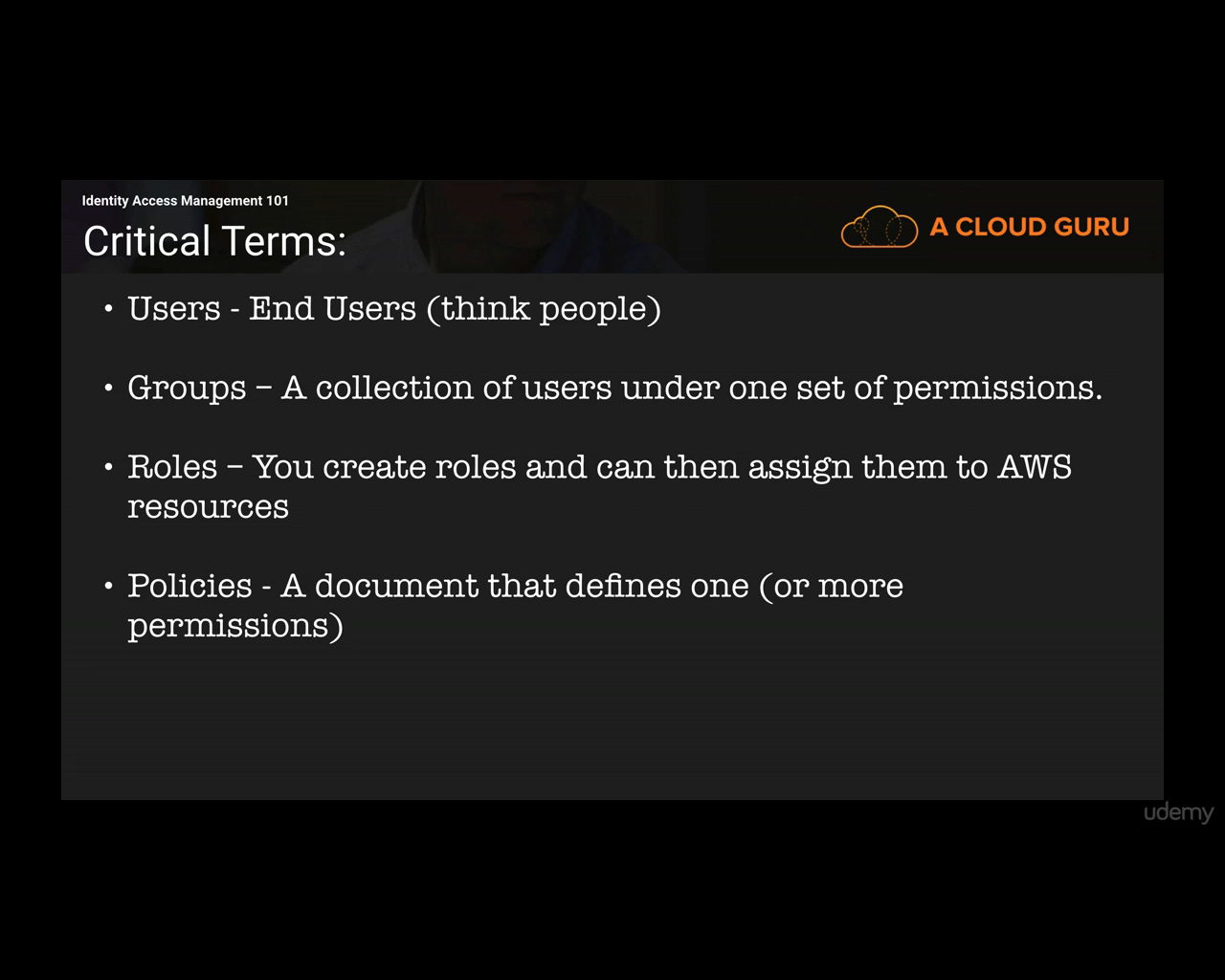
**IAM**







Policies can be attached to users, groups or roles. Each can have 1 policy.

After login first time, in IAM there are 5 points to make it checked.

* Activate MFA on your root account:

Manage MFA-> A virtual MFA device. -> for iPhone Install google authenticator.

For Android install Authenticator. -> scan authentication code1 and 2.

* Create individual users

User name: aish

Select AWS access type:

programmatic access: access key ID, secret access key ID

AWS management Console access: username and password

Console Password: Autogenerated password. -> next -> create group -> system-admins:select policy type- SystemAdministrator(check once the policy document)-> create.

Now each user got access key and secret access key and password.

**ROLE:**

Allow EC2 to store files in S3

Create Role-> Select Role Type -> AWS Service- EC2 -> Select use Case- EC2 -> Policy Type- AmazonS3FullAccess -> Role Name- S3-AdminAccessto-EC2

