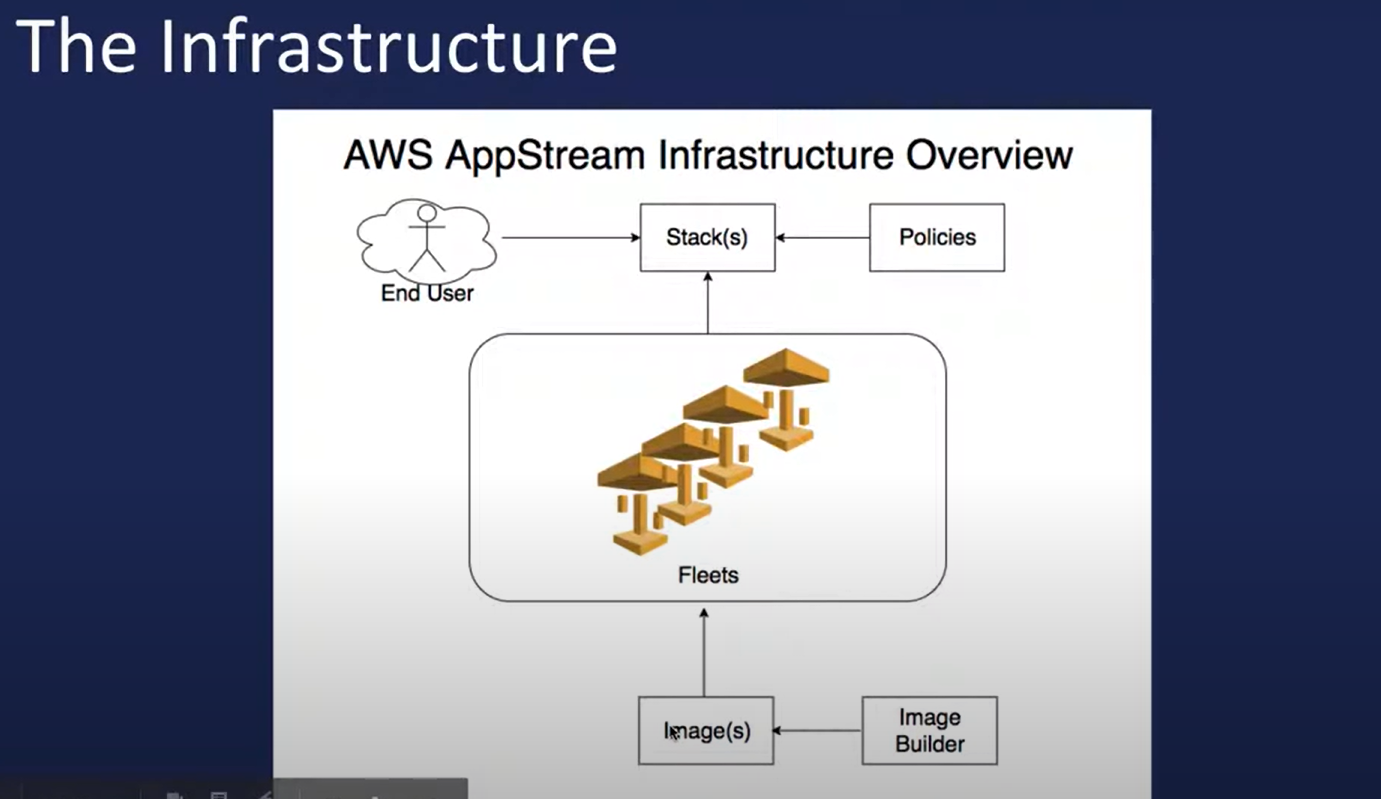
Appstream



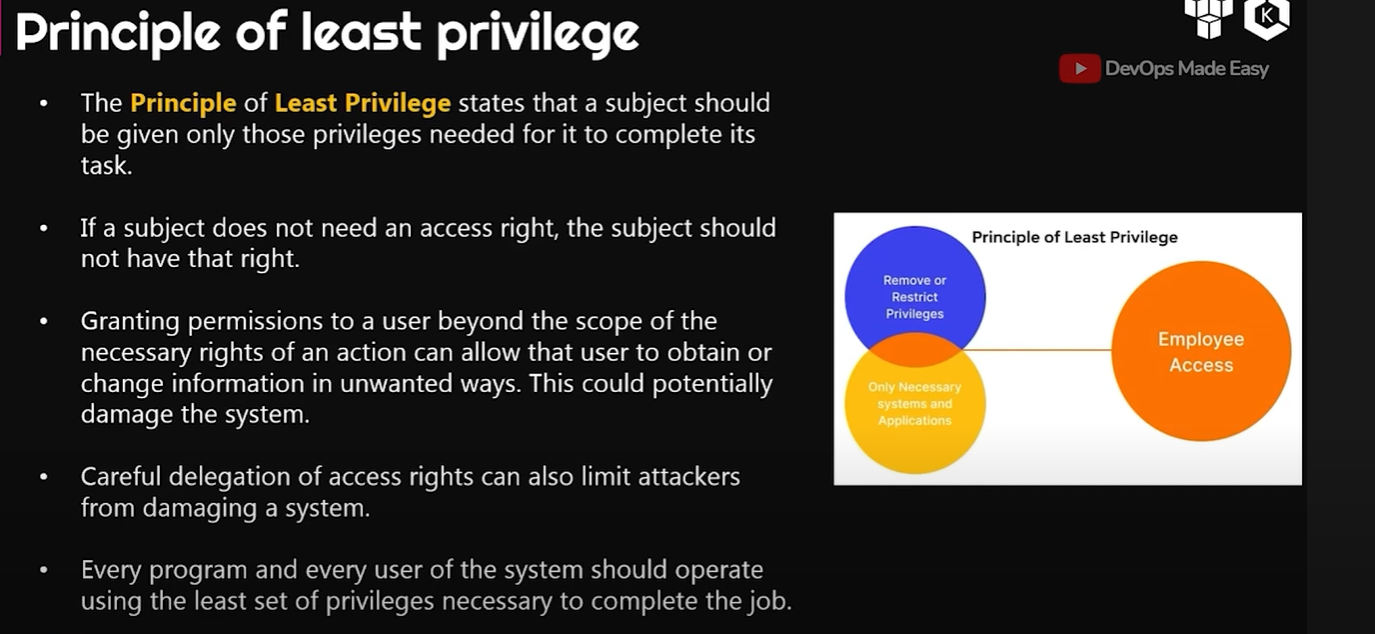


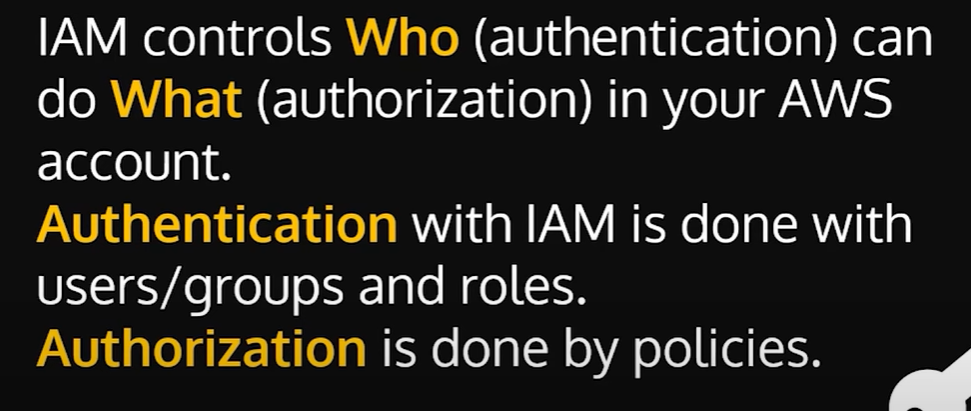


APPSTREAM\_FLLET\_IAM\_ROLE\_ARN=arn:aws:iam::883660979569:role/image\_builder\_viewer\_role

<https://us-east-1.console.aws.amazon.com/iam/home?region=eu-west-1#/roles/details/image_builder_viewer_role?section=permissions>

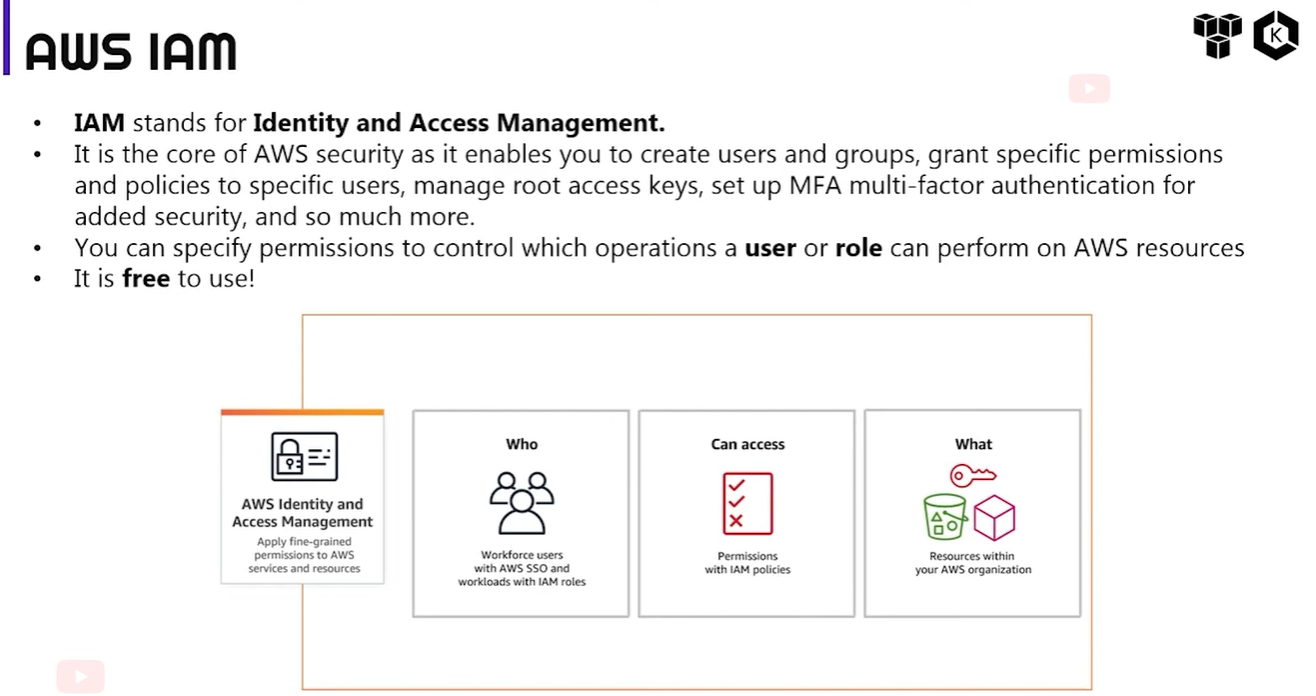
* **Principle of least privilege**
* **Aws IAM Service**
* **IAM Users, Groups & Roles**
* **IAM Policies**
* **AWS Access Modes**
* **Creating IAM User with Programmatic Access**
* **Install and Configure AWS CLI**



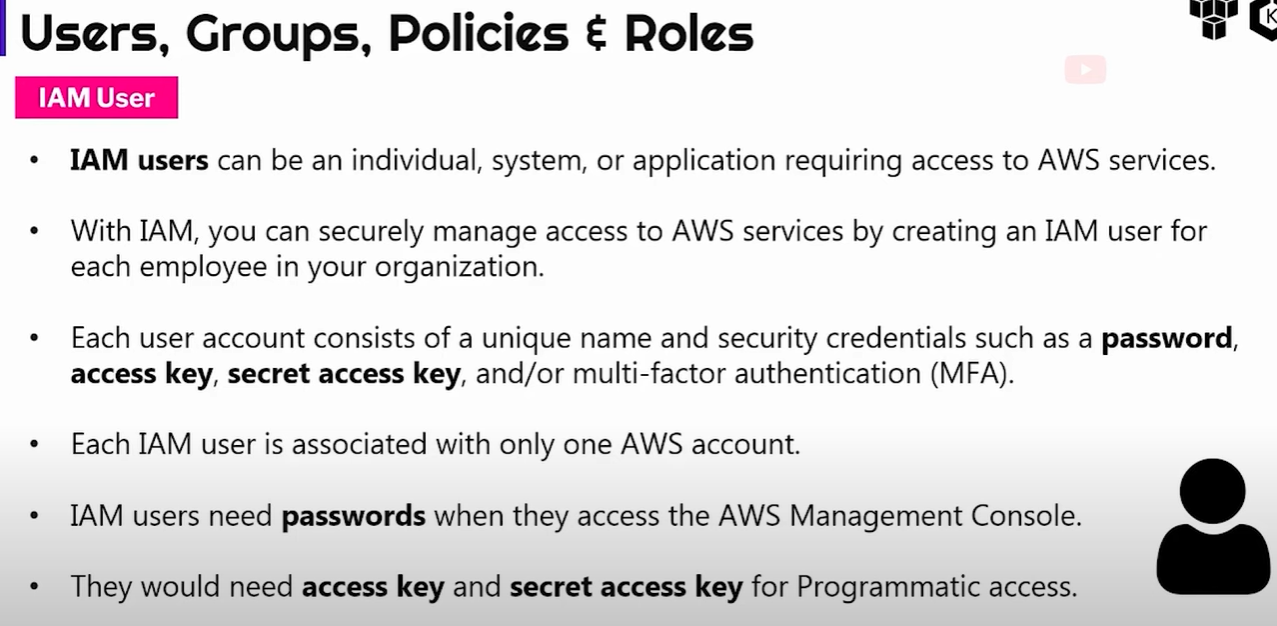


WHO : Authentication : users/groups and roles

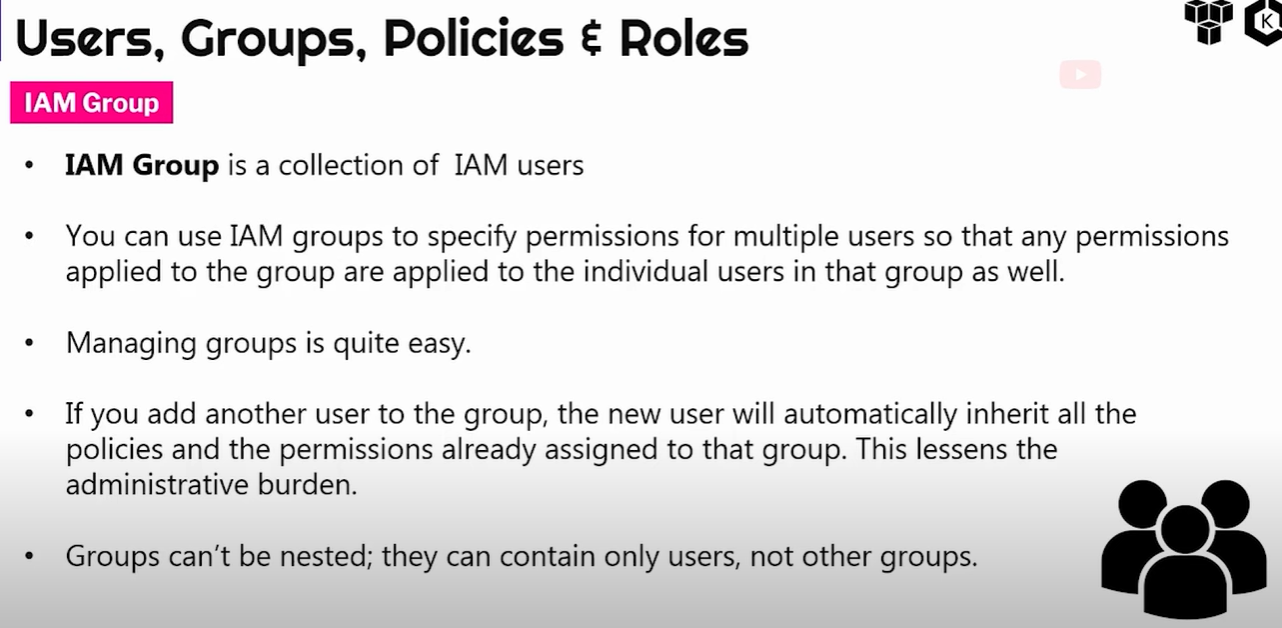
WHAT : Authorization : policies







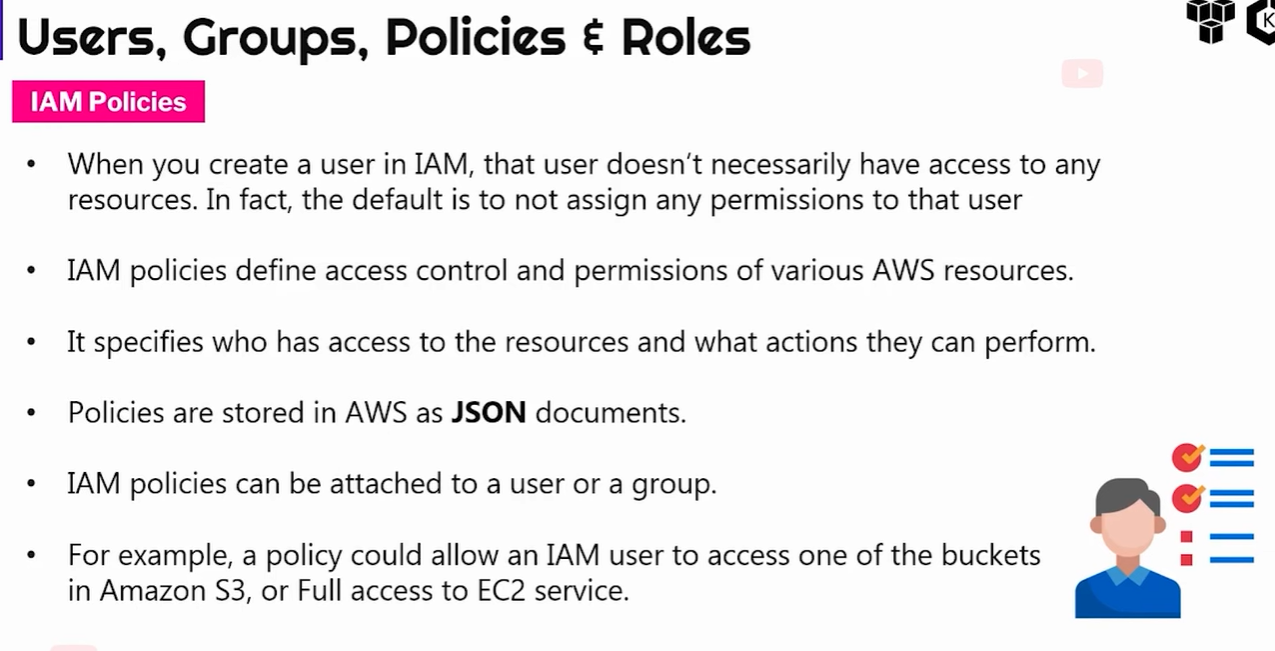
Users : can be an individual, system, or application requiring access to AWS services.



IAM Groups is a collection of IAM users.

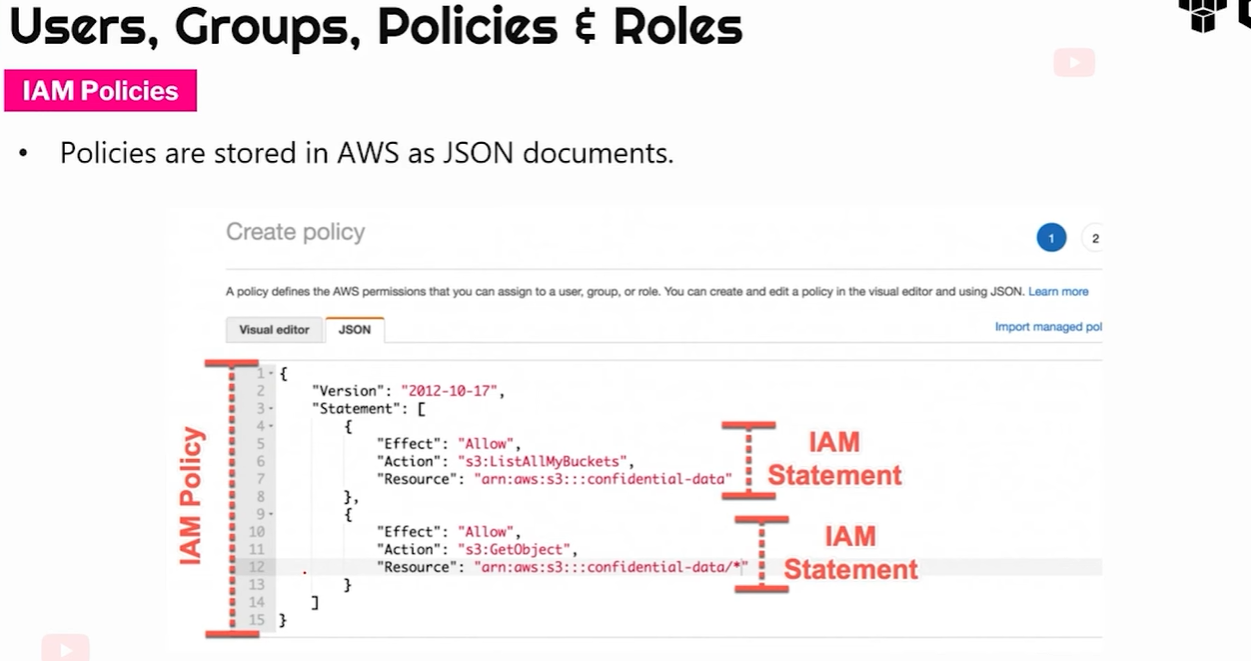
A user that is a part of a group inherits automatically all permissions attached to the group.

Groups can’t be nested !!!



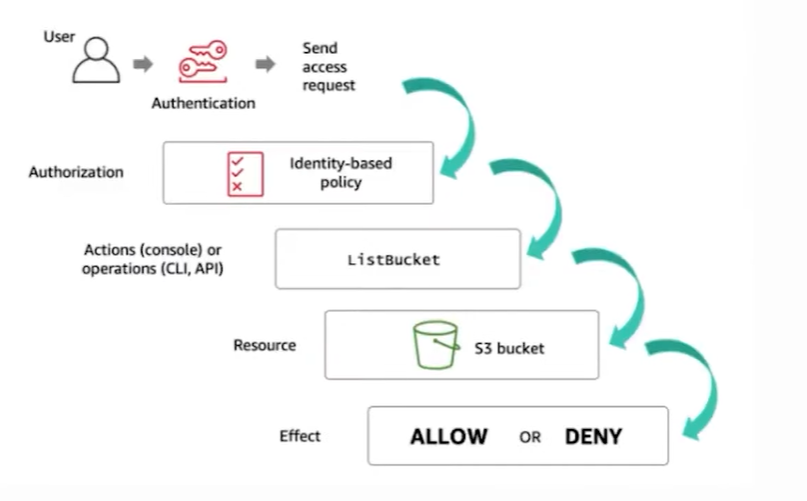
Policies are simply the permission attached to an IAM user/group or role !

IAM Policies define access control and permissions of various AWS resources !

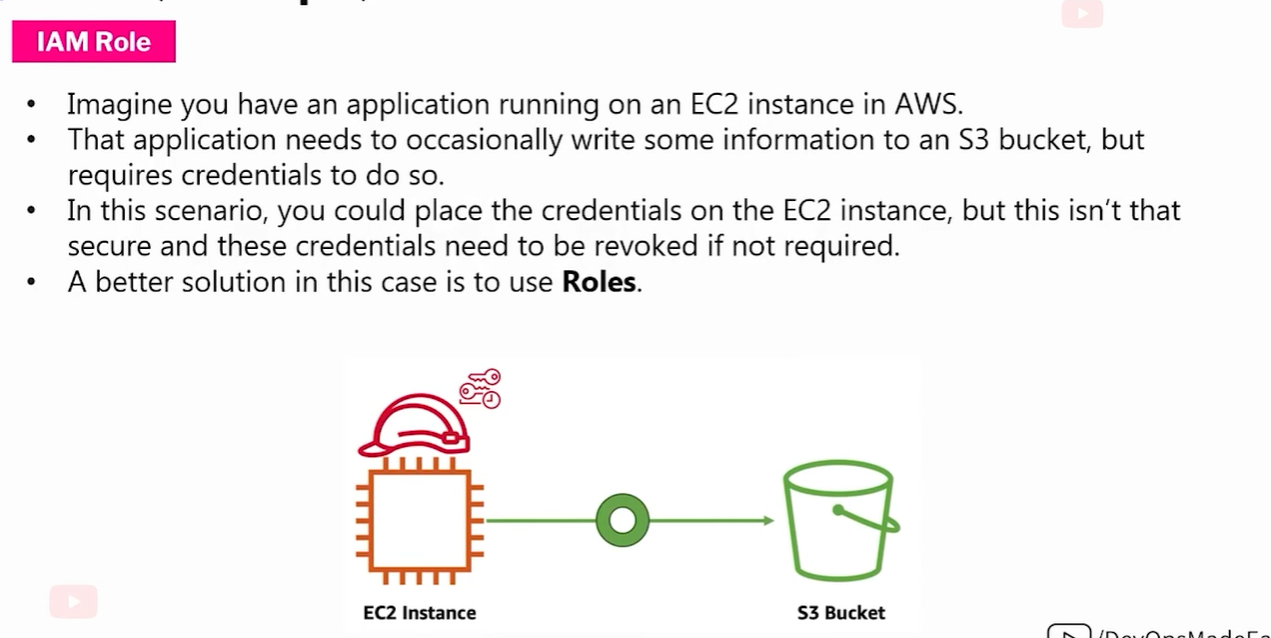




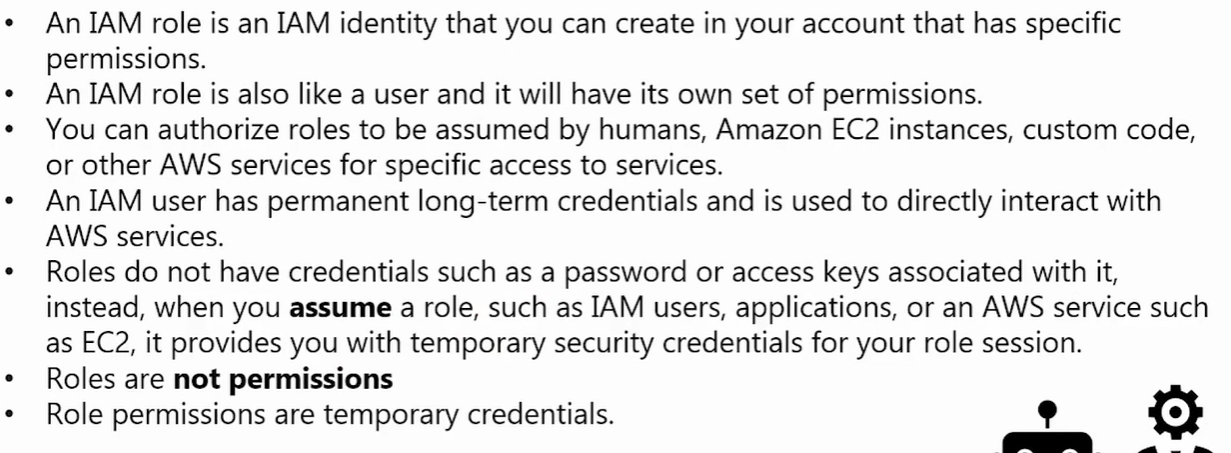
Policies can be attached to roles (AdministratorAccess role in the example above)

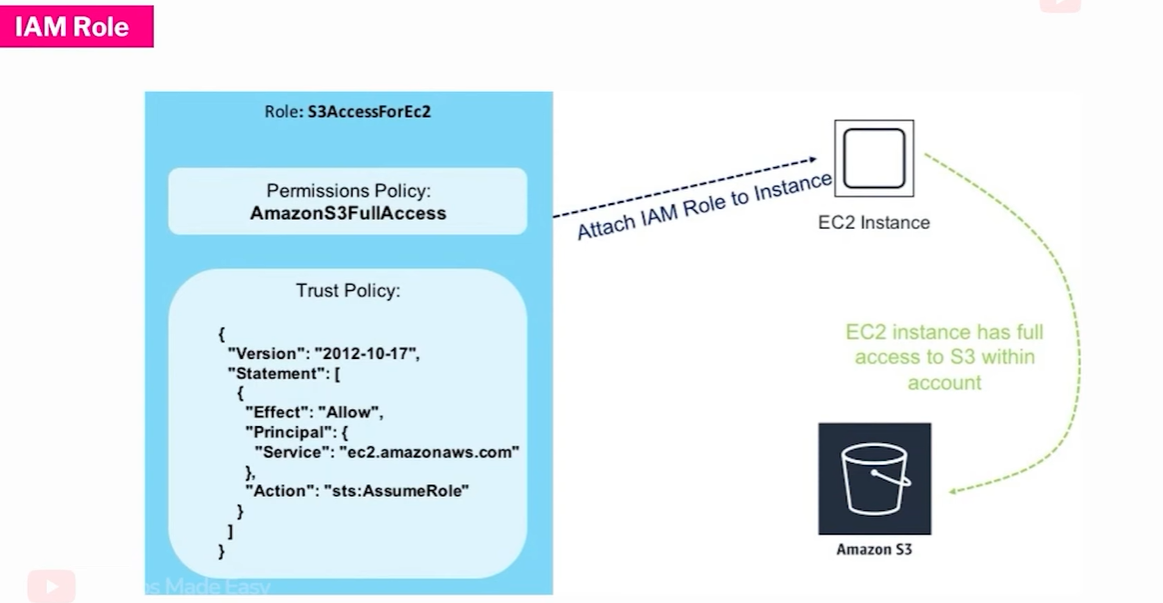


IAM ROLES



Difference between IAM user AND IAM role





AWS ACCESS TYPES /

