Azure Role based Access Control (RBAC)

Roles

ACTIONS

DISK
VM
SQL
WEB

CREATE DISK
UPDATE DISK

START VM
STOP VM
ATTACH DISK

SCALE DB
UPDATE DB

DEPLOY APP
DELETE WEB
CHANGE SETTING

ROLES

VM OPERATOR
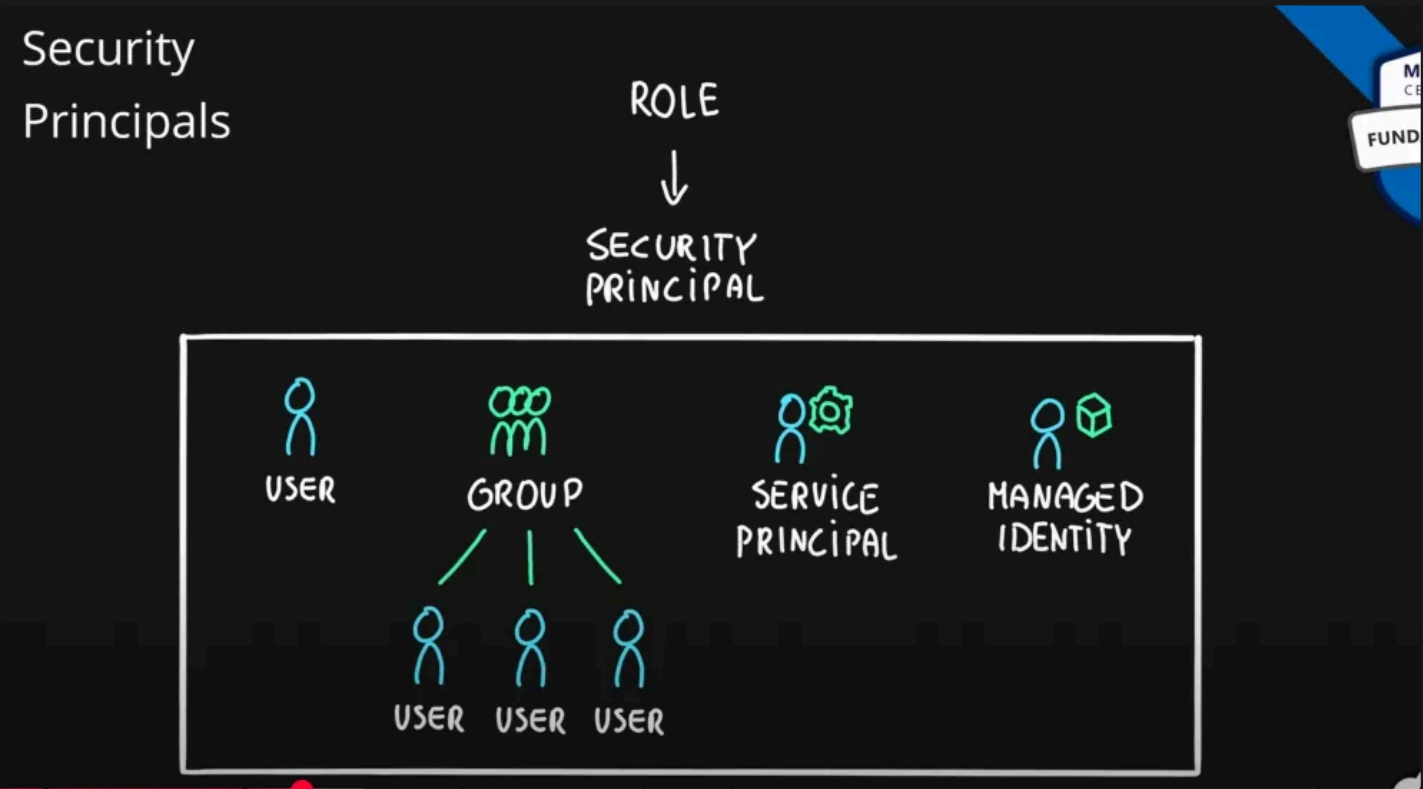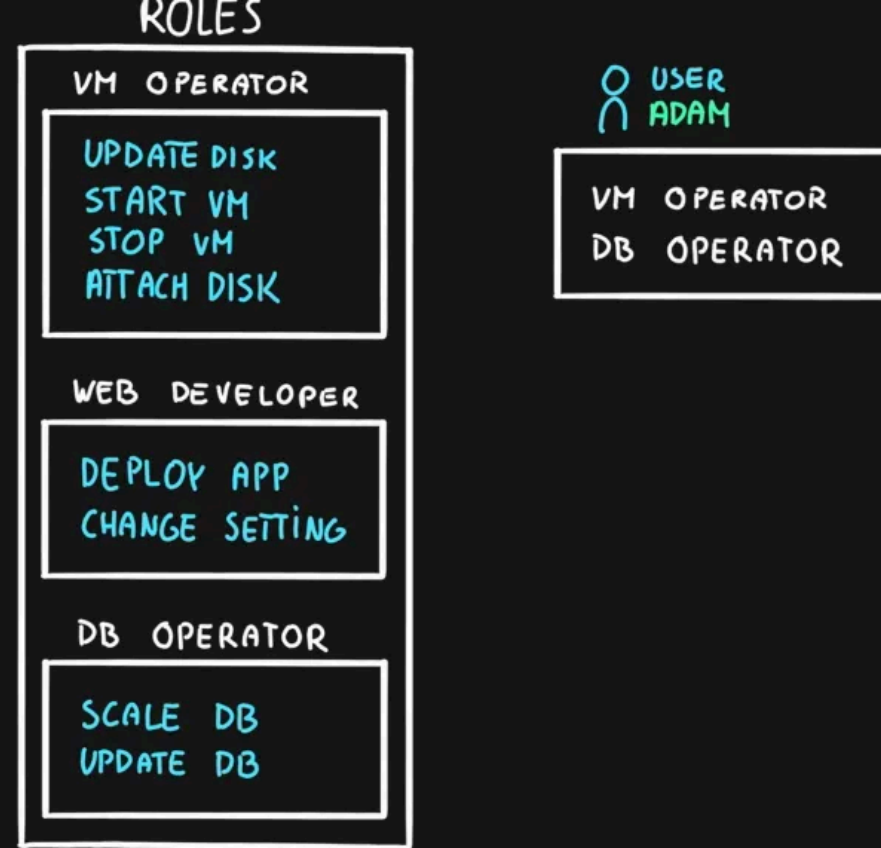UPDATE DISK
START VM
STOP VM
ATTACH DISK

WEB DEVELOPER
DEPLOY APP
CHANGE SETTING

DB OPERATOR
SCALE DB
UPDATE DB
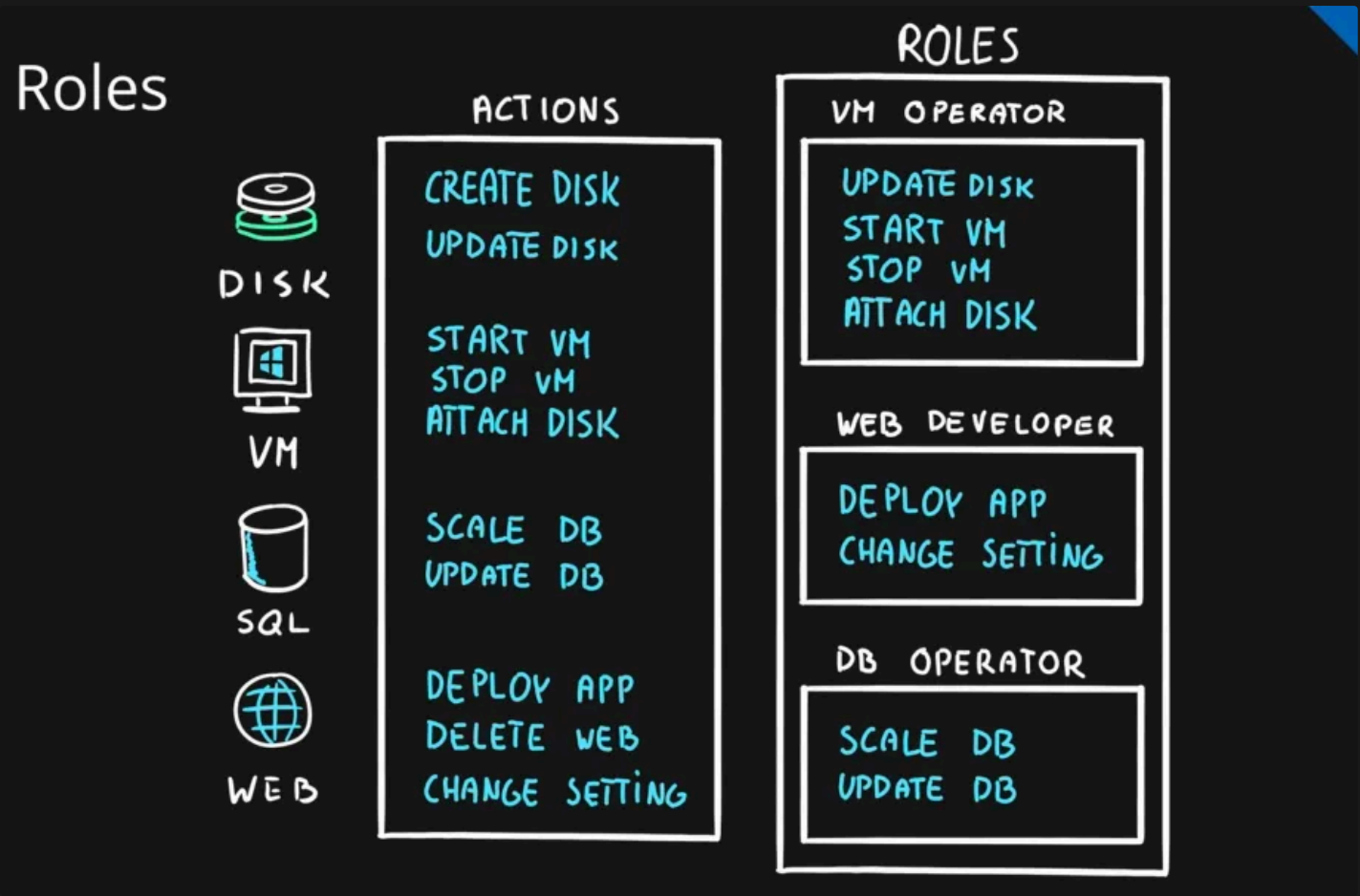
Role

Role (role definition) *is a* collection of actions *that the assigned identity will be able to perform.*

Role definition is an answer to a question "What can be done?"

Security Principals

ROLE
↓
SECURITY PRINCIPAL

USER
GROUP
SERVICE PRINCIPAL
MANAGED IDENTITY

USER   USER   USER

Security Principals

ROLES

VM OPERATOR
- UPDATE DISK
- START VM
- STOP VM
- ATTACH DISK

WEB DEVELOPER
- DEPLOY APP
- CHANGE SETTING

DB OPERATOR
- SCALE DB
- UPDATE DB

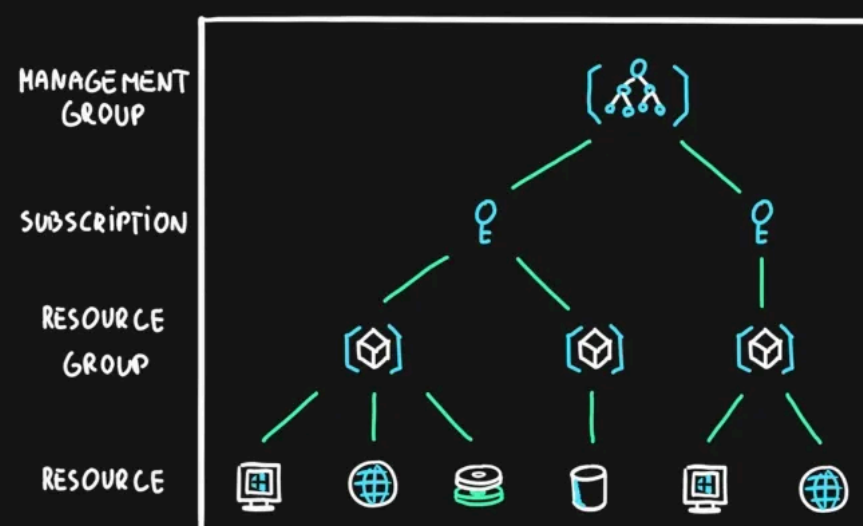USER ADAM
- VM OPERATOR
- DB OPERATOR

Security Principal

Security Principal is an Azure object (identity) that can be assigned to a role (ex. users, groups or applications).

Security Principal assignment is an answer to a question "Who can do it?"

Scopes

ROLE
↓
SCOPE

- MANAGEMENT GROUP
- SUBSCRIPTION
- RESOURCE GROUP
- RESOURCE

Key Characteristics

- Authorization system built on Azure Resource Manager (ARM)

- Designed for fine-grained access management of Azure Resources

- Role assignment is combination of
  - Role definition – list of permissions like create VM, delete SQL, assign permissions, etc.
  - Security principal – user, group, service principal and managed identity and
  - Scope – resource, resource groups, subscription, management group

- Scopes are hierarchical
  - Management Groups > Subscriptions > Resource Groups > Resources

- Built-in and Custom roles are supported