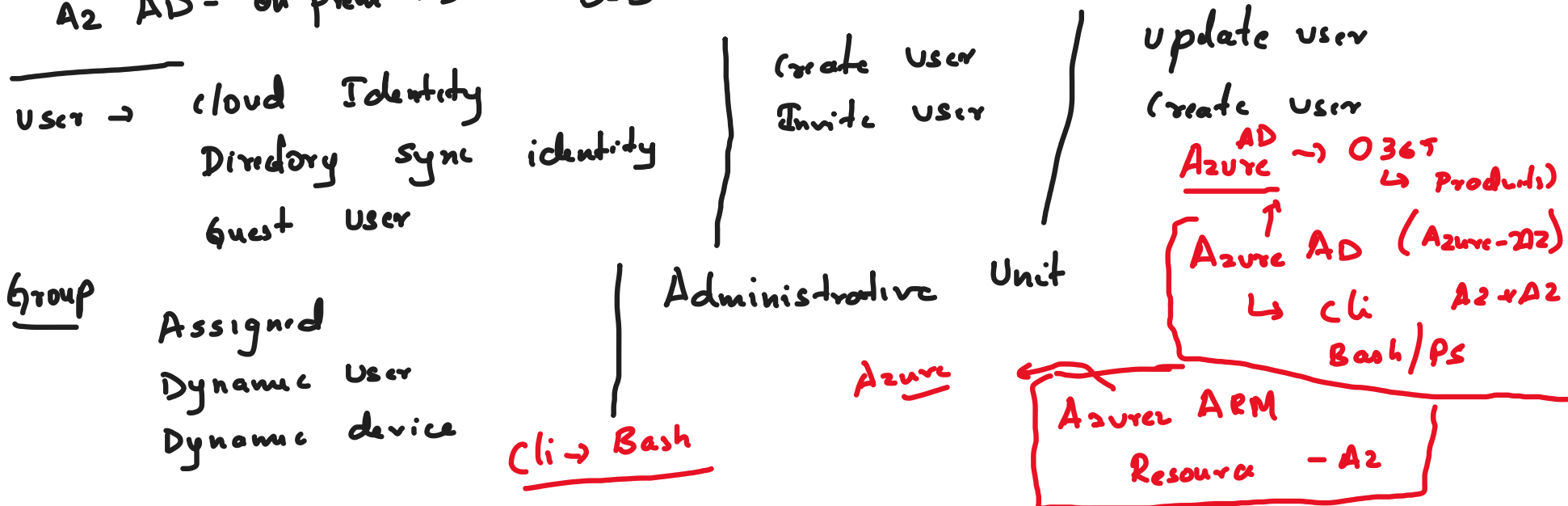


Azure AD

Identity, Account, A2 Account, tenant, Subscription

A2 AD - On prem AD - B2B B2C



Play let authenticate [Active Directory] → (Portal)

Administrative Unit ⇔ Organization Unit

↳ Help group, manage, control AD Directory

↳ Role Grouping Global → Least Required → [VM → Read VM] ⇒ Administration

RBAC → Control (can do) → Audit → Managing → Security

Owner → Full, grant

Contributor → Full

Reader → Read

User Access Administrator → Control

RBAC vs. A2 AD

- Resource

- Scope

- AD Resource

- Tenant level

Assign

Scope

User Group

1) Management Group

2) Subscription

3) Resource Group

4) Resource (VM, storage, ...)

Everything

All

Rg []

Mgmt → Subscrip → Rg → R (Billing)

Group (Tenant)

Control

User → AD

↳ map RBAC

RBAC

Scope

MG ↓

Sub (subscrip)

Rg

(R) ↓

Control

Read

Delete

Start/stop

Assign -

- Monitoring

- Local Admin

- Production

→ stop

start

- Develop

- Release

↳ change deployment

Device

Iphone

Android

2nd

Azure AD

On prem AD

B2B

B2C