Microsoft, IBM → IAM

- Segítségével azonosítják, hitelesítik és engedélyezik a felhasználók hozzáférését az adatokhoz, alkalmazásokhoz és szolgáltatásokhoz.
- Négy A-ból tevődik össze

1. Administration → Felhasználó/Identitás kezelés
2. Authentication → Bejelentkezés
3. Authorization → Jogosultságkezelés

} Hozzáférés kezelés

4. Audit → Jól állították-e be az előző három pontot.

- **Megfelelő hozzáférés a megfelelő személyek számára**
  - Probléma → Felesleges engedélyek
  - Megoldás → Csak a szükséges jogokat állítsuk be
- **Adatbiztosítás**
  - Probléma → Adatok nincsenek titkosítva
  - Megoldás → AES, 3DES, DES titkosítási módszerek alkalmazása az adatátvitelhez, hitelesítő adatokhoz
- **Felhasználói élmény → UX**
  - Probléma → Például minden alkalommal a felhasználónak be kell jelentkeznie
  - Megoldás → Használjunk Single-Sign-on (SSO) technológiát, amivel elég egyszer belépni
- **Kevesebb manuális munka az informatikai részlegen**
  - Probléma → Például a jelszó-visszaállítás
  - Megoldás → Funkciók automatizálása
- **Adatbiztonsági incidensek elleni védelem**
  - Probléma → Feltörések
  - Megoldás → Plusz réteg a bejelentkezéshez (2FA)

- **Identity**
  - Öntudat, identitás
  - Hitelesítési információ olyan csoportja, amik a rendszer egy adott egyedét egyértelműen meghatározzák.
    - A egyedet (entitást) leggyakrabban a felhasználóval azonosítják, de lehet szolgáltatás vagy alrendszer is.
- **User Provisioning**
  - Felhasználás, szolgáltatás
  - Felhasználói fiókok létrehozása és jogosultságaik beállítása cél- erőforrásokon.
- **IBM Tivoli Identity Manager**
  - **Identity Manager működési modellje "Role Based Provisioning"**

    Felhasználó → Szerep → Provisioning Policy → Szolgáltatás (erőforrás)

    1. A felhasználó feladatkörének megfelelő szerepkörhöz rendelés.
    2. A szerepkör tagjainak erőforráshoz rendelése.
       - Provisioning Policy attribútumokat is meghatározhat.
         - Felhasználó lemezkerület évfolyam
         - Csoport-tagság
  - **A "reconciliation" összeveti az elvárt és a valós állapotot**

    Felhasználó → Szerep → Provisioning Policy → Szolgáltatás (erőforrás)

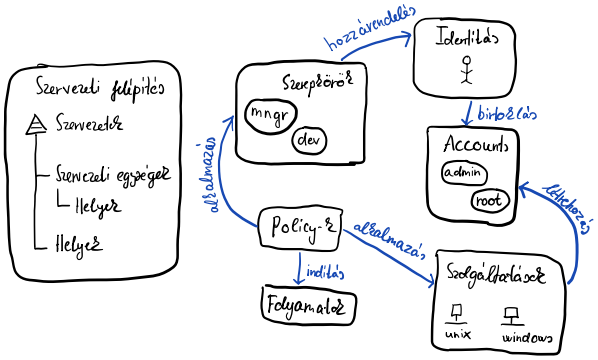
    - A szabályok betartása történik a reconciliation során:
      - Például egy erőforrás elérési jogosultságai
      - A TIM visszaállítja a jogosulatlan módosítások előtti állapotot
        - Lokális Admin tevékenység
    - Felfedi az "árva" fiókokat, amik adoptálhatóak, felfüggeszthetőek, törölhetőek.

• "Önkiszolgálás" - jelszó menedzsment

- Jelszó szabályzat ellenőrzése
- Challenge - Response, vagyis kérdés-válasz megoldás az elfelejtett jelszavak kezelésére
- Jelszó eljuttatás biztonságos módon

• Audit és riportok

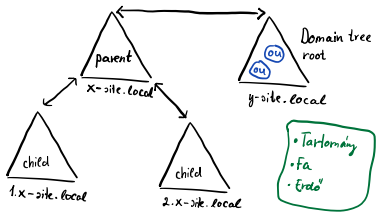
- Kérelmek, jóváhagyások és változtatások kerülnek időbélyeggel a TIM adatbázisában tárolásra.
- Standard jelentések PDF formátumban:
  - Működtetés - Operation
  - Szolgáltatások - Services
  - Felhasználók - Users
  - Eltávolított - Levételek
  - Egyeztetés - Reconciliation
- CSV formátumú jelentések a továbbfeldolgozáshoz



• Lehetséges problémák

- Nincs aktuális szervezeti ábra, nyilvántartás
- Folyamatoknál nincs döntéshozó és a bevonandó folyamatok túl sok szálon vannak.

- **Active Directory**
  - Microsoft címtár implementációja
  - Infrastruktúra alapja -> Hitelesítés, menedzsment
  - Felhasználók központi menedzselése
    - Jelszó jogosultságok
    - Csoportok
    - Szervezetek
  - A csoportházirenddel az AD csoportjaihoz rendelhetünk jogosultság-gyűjteményeket, amik az adott csoport tagjaira lesznek érvényesek. -> Adott felhasználónál egy adott jogosultság felülbírálható.
- **Hierarchia eleme**
  - Szervezeti egység (Organization Unit - OU)
- **Struktúra kialakításának alapja**
  - Delegálás
    - Adott részfa menedzselését át tudjuk adni másoknak.
    - Nagy szervezet esetén hasznos.
    - A címtár szerkezetét úgy kell kialakítani, hogy egybe tartozó elemek felügyeletét lehessen együtt delegálni
  - Házirend
    - Működést szabályozó beállítások összessége.
    - Házirendet OU-ra is lehet definiálni.
- **AD szerkezet**
  - Tartomány (domain)
    - AD egysége a tartomány (domain), az ebben lévő elemeket kezeljük közösen
    - Tartományoknak lehetnek gyerek tartományai (child domain)



  - Fa (tree)
    - Szülő felhasználói is elérhetőek a gyerek tartományban
      - Így alakul ki a fa (tree)
  - Erdő (forest) -> AD legnagyobb egysége
    - Egy erdőbe tartozó tartományoknak közös a sémája.
    - Közös katalógus a keresésnek.
    - Tartományok között kétirányú bizalmi kapcsolat van.

- Tartományvezérlő
  - Ezek a gépek tárolják a címtárat
  - Mindegyik tárol egy-egy példányt és a változtatásokat egymás között szinkronizálják.
  - Fontos, hogy mindig válasszuk szét AD esetén a belső" AD tartomány nevét a külső" DNS névtől, erre jó konvenció a .local végződés a belső" tartomány DNS nevére.
    - Nem szeretnénk a tartományvezérlőt publikusan elérhetővé tenni.