7.b Vesse össze a Microsoft és az IBM által nyújtott eszközöket felhasználó- és hozzáférés menedzsment szemszögből!

Felhasználó és hozzáférés kezelés

- Identity and Access Management (IAM)
- Segítségével azonosítják, hitelesítik és engedélyezik a felhasználók hozzáférését az adatokhoz, alkalmazásokhoz és szolgáltatásokhoz.
- **Négy A-ből tevődik össze:**
    - Adminisztráció
        - **Felhasználó/Identitás kezelés**
    - Autentikáció – Ki vagy?
        - **Hozzáférés kezelés**
    - Autorizáció – Mit akarsz csinálni?
        - **Hozzáférés kezelés**
    - Audit
        - Azt a célt szolgálja, hogy megbizonyosodjunk arról, hogy biztosan jól csináltuk az **Adminisztráció**-t, **Autentikáció**-t, **Autorizáció**-t.

IAM rendszer problémák, megoldások

Megfelelő hozzáférés a megfelelő személyek számára

- **Probléma**
    - A felhasználók rendelkeznek nem szükséges jogokkal.
- **Megoldás**
    - Biztosítja, hogy a felhasználók a számukra nem szükséges bizalmas információk elérésének lehetővé tétele nélkül hozzáférjenek azokhoz az erőforrásokhoz, amikre szükségük van.

Akadálytalan munkavégzés

- Fontos a felhaszálói élmény.
- **Problémák**
    - Többszöri bejelentkezések és jelszavak bekérése.
- **Megoldás**
    - Single-Sign-On (SSO) bevezetése, amivel csak egyszer kell bejelentkezni a felhasználóknak.

Adatbiztonsági incidensek elleni védelem

- **Probléma**
    - Adatbiztonsági incidensek kockázata
    - Feltörések
- **Megoldás**
    - További biztonsági réteget ad hozzá a bejelentkezési folyamathoz.

Adattitkosítás

- **Probléma**
    - Bizalmas adatok nincsenek védve.
- **Megoldás**
    - Titkosítás használata, például AES, RSA vagy SHA megoldásokkal.
    - Használhatunk titkosítást az adatok tárolására, adatátvitelkor vagy a hitelesítő adatokhoz.

Identity

- **Öntudat, identitás**
- Hitelesítési információk olyan csoportja, amik a rendszer egy adott egyedét egyértelműen meghatározzák.
    - Az egyedet (entitást) legtöbbször a felhasználóval azonosítják, de lehet szolgáltatás vagy alrendszer is.

User provisioning

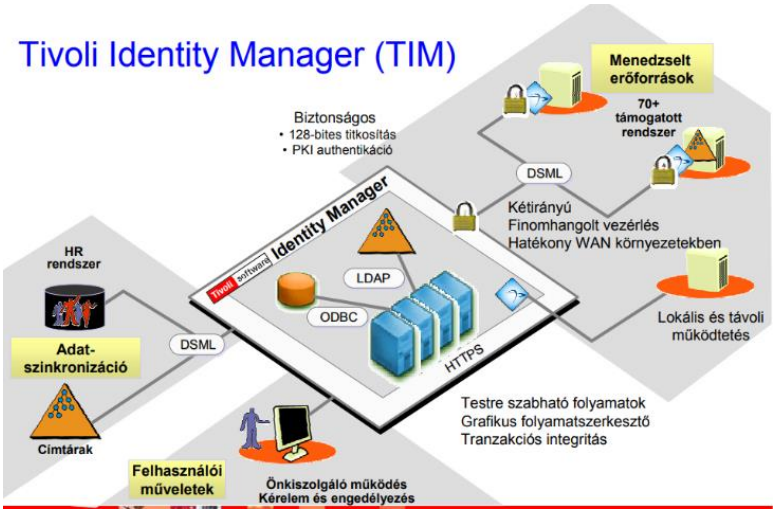
- **Felkészülés, szolgáltatás**
- Felhasználói fiókok létrehozása és jogosultságaik beállítása cél-erőforrásokon.

IBM Tivoli Identity Manager

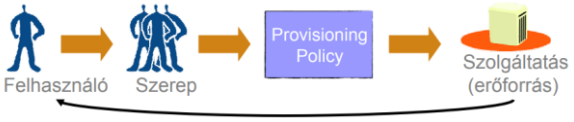
Identity Manager működési modellje „Role Based Provisioning”

1. A felhasználó felelősségi körnek megfelelő szerepkörhöz rendelés.
2. A szerepkör tagjainak erőforráshoz rendelése.

- Provisioning Policy attribútumokat is meghatározhat.
    a. Felhasználó lemezterület kvóta
    b. Csoport-tagság



A “reconciliation” összeveti az elvárt és a valós állapotot



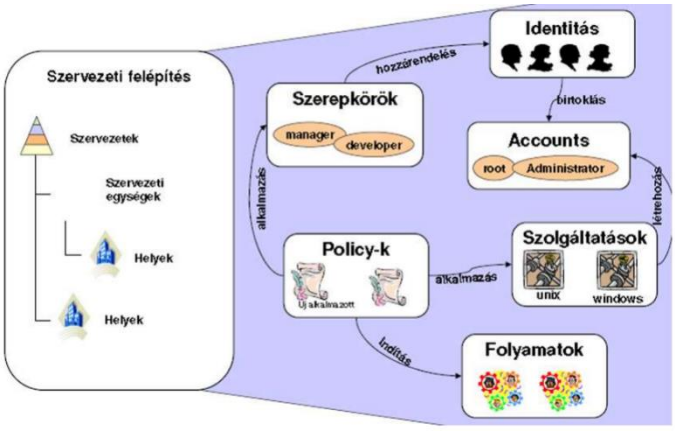
- A szabályok betartása történik a reconciliation során
    - Például egy erőforrás elérési jogosultságai
    - A TIM visszaállítja a jogosulatlan módosítások előtti állapotot (**lokális admin tevékenység**)
- Felfedi az „árva” fiókokat, amik adoptálhatóak, felfüggeszthetőek vagy törölhetőek.

“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 adatbázisban tárolásra.
- **Standard jelentések PDF formátumban**
    - Működtetés – Operation
    - Szolgáltatások – Service
    - Felhasználók – User
    - Elutasított tevékenységek – Rejected
    - Egyeztetés – Reconciliation
- **CSV formátumú jelentések a továbbfeldolgozáshoz**



Lehetséges problémák

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

Microsoft Active Directory

- **Microsoft címtár implementációja**
- **Infrastruktúra alapja**
    - Hitelesítés, menedzsment
- **Felhasználók központi menedzselése**
    c. Jelszó jogosultságok
    d. Csoportok
    e. Szervezetek
- A csoportházirendekkel az AD csoportjaihoz rendelhetünk jogosultság-gyűjteményeket, amik az adott csoport tagjaira lesznek érvényesek.
    f. Adott felhasználónál egy adott jogosultság felüldefiniálható.

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.
- **Házirendek**
    - Működést szabályozó beállítások összessége.
    - Házirendeket OU-ra is lehet definiálni.

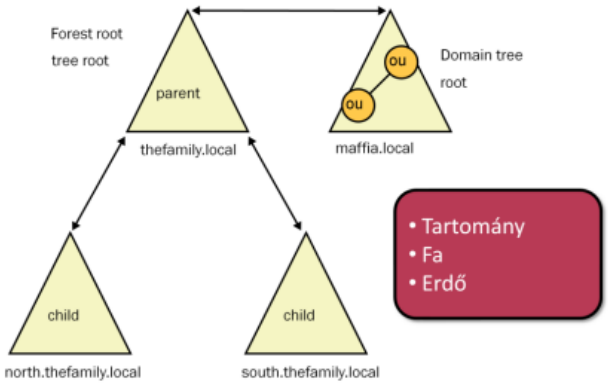
AD szerkezet

Tartomány (domain)

- AD egysége a tartomány (**domain**), az ebben lévő elemeket kezeljük közösen.
- A tartományoknak lehetnek gyerek tartományaik (**child domain**).

Fa (tree)

- A szülő felhasználói is elérhetőek a gyerek tartományokban.
    - Így alakul ki a fa (**tree**).



Erdő (forest)

- AD legnagyobb egysége az erdő (**forest**).
- Egy erdőbe tartozó tartományoknak közös a sémája.
- Van egy közös katalógusuk a kereséshez
- A tartományok között kétirányú bizalmi kapcsolat (**trust**) van.

Tartományvezérlő (Domain Controller, DC)

- 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.