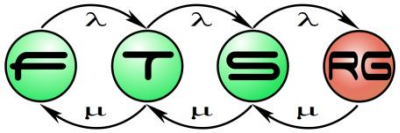
Felhasználói Identitás Menedzsment

Szombath István

szombath@mit.bme.hu



A mérési környezet

- itim5.tivdemo.hu
  - Win 2003 szerver
    - Felh.: Administrator
    - Jelszó: LaborImage
    - Domain: TIVDEMO
  - DB2 adatbázis szerver
  - IBM WebSphere alkalmazás szerver
  - Tivoli AD Agent (ld. Később)
- ad.tivdemo.hu
  - Win 2000 szerver
    - Felh.: Administrator
    - Jelszó: LaborImage
    - Domain: TIVDEMO
  - Active Directory szerver
  - DNS szerver

A mérés célja

- CSV-ből felolvassuk kik vannak a rendszerünkben
- Nekik csinálunk ITIM hozzáférést (Usereknek csinálunk ITIM accountot)
- ITIM összelövése AD-val
  - Összerendeljük az AD accountokat az ITIM Userekkel (figyelem, nem az ITIM accountokkal!)
    - Összerendelés Adoptation Policy alapján
  - Ha valakinek nincs AD accountja létrehozunk egyet, és beállítjuk az account attribútumait az ITIM User attribútumai alapján
    - Ezt Provisioning Policy-val érhetjük el
  - Ha valakinek van AD accountja de nincs az ITIM-ben, azt felfüggesztjük (miért is?)

0. Feladat

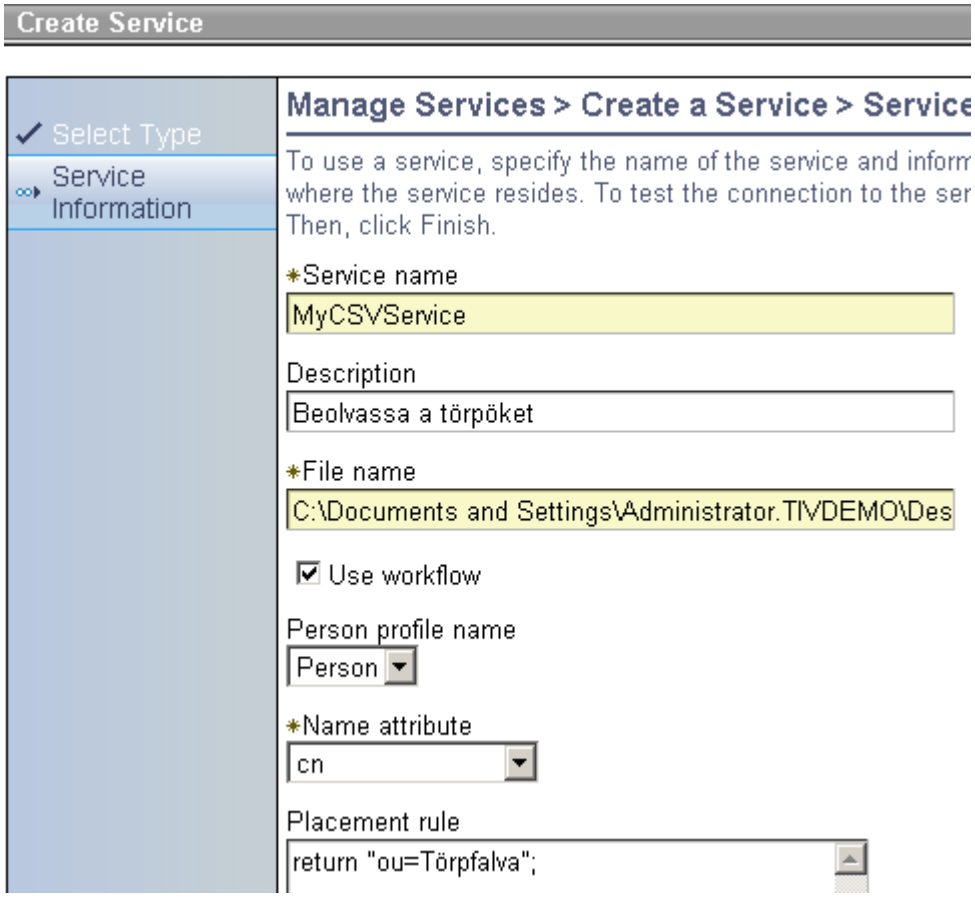
- Indítsuk el mindkét gépet, lépjünk be (ld. előző slide)
  - „ad” gépen nézzük meg a tartomány felhasználóit
    - Start menü / programok / admin eszközök / AD Users…
  - „itim5” gépen indítsuk el az asztalon lévő start-all.bat-ot
    - ez indítja a szolgáltatásokat, a megfelelő sorrendben)
    - ha felálltak a szolgáltatások, start menü / programok / IBM Tivoli Identity Manager 5.0 / IBM Tivoli Identity Manager
    - a web böngészőben megjelenik az ITIM bejelentkező felülete
      - Felh.: itim manager
      - Jelszó: LaborImage

0. melléklet – A GUI

- Függőleges sávban a menü
- Vízszintes sávban az ún. tabok
- Manage xyz kezeli a:
  - Szerepeket
  - Szervezeti egységeket
  - Felhasználókat
  - Szolgáltatásokat
    - Itt definiáljuk a vezérlendő erőforrásokat, pl. AD, LDAP
- Manage xyz policy:
  - Policy-k kilistázása, hogy mi mire jó ld. jegyzet.
- View All Request
  - Kiadott utasítások végrehajtását követhetjük nyomon

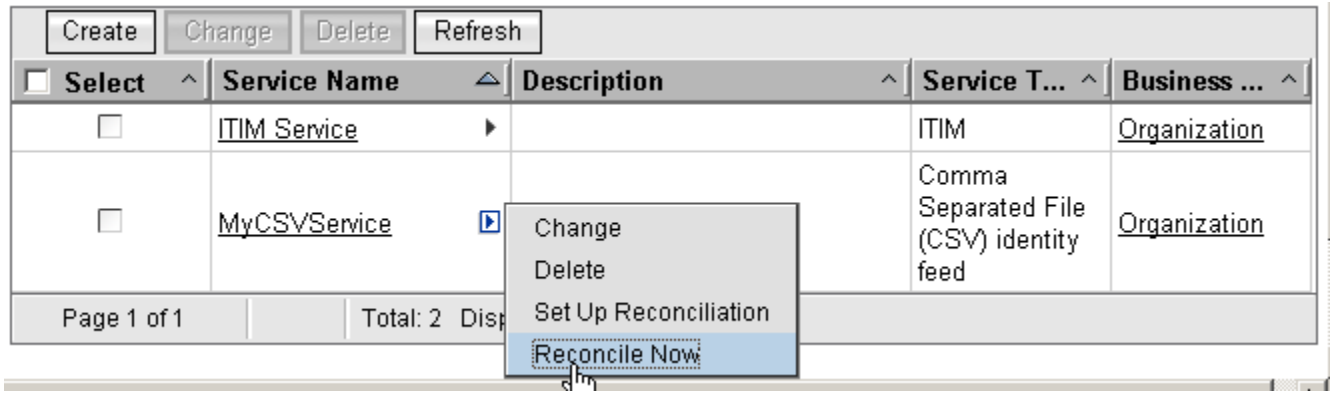
CSV-ből Userek felolvasása

- Új Ordanization Unit létrehozása (1-es melléklet)
  - Manage Organization Structure
    - Create Organization Unit: Törpfalva
- Manage Services
  - (refresh) create /
    CSV identity feed / next
    - File name az asztalon lévő csv fájl FQN-je (Fully Qualified Name)
    - A beolvasott felhasználókat Törpfalvába teszi
  - Finish / close

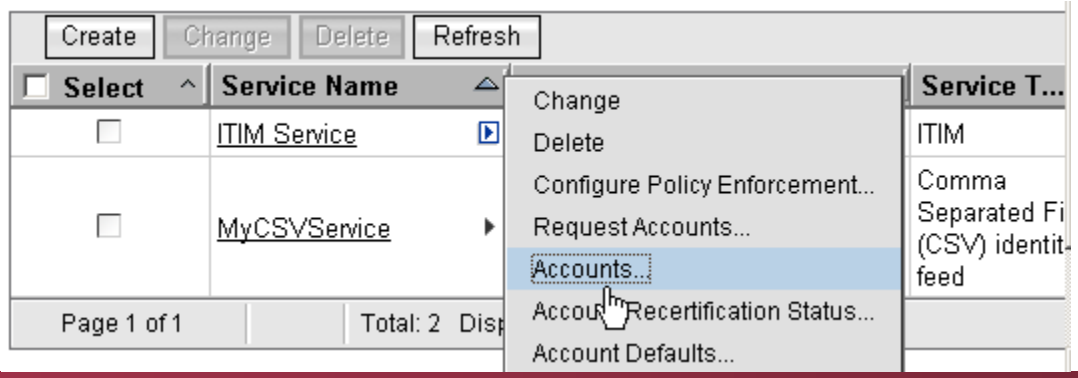


CSV-ből Userek felolvasása

- Manage Services tab alatt kiválasztjuk a CSV feedet, majd „összeegyeztetünk”



- Ellenőrizzük, hogy az új felhasználók létrejöttek-e
- Nézzük meg, hogy létrejöttek-e a felhasználókhoz ITIM fiókok



CSV-ből Userek felolvasása

- Miért jöttek létre automatikusan ITIM fiókok a felhasználókhoz?
  - Identity Policy-ket nézzük meg (különösen a MyIdentityPolicyt), értelmezzük, itt nem kell egyebet csinálni

- Egyéb megjegyzés: minden művelet végrehajtását nyomon tudjuk követni
  - View Requests / View All Requests

2 requests were submitted between **October 30, 2009** and **October 30, 2009**.

Cancel request | Refresh

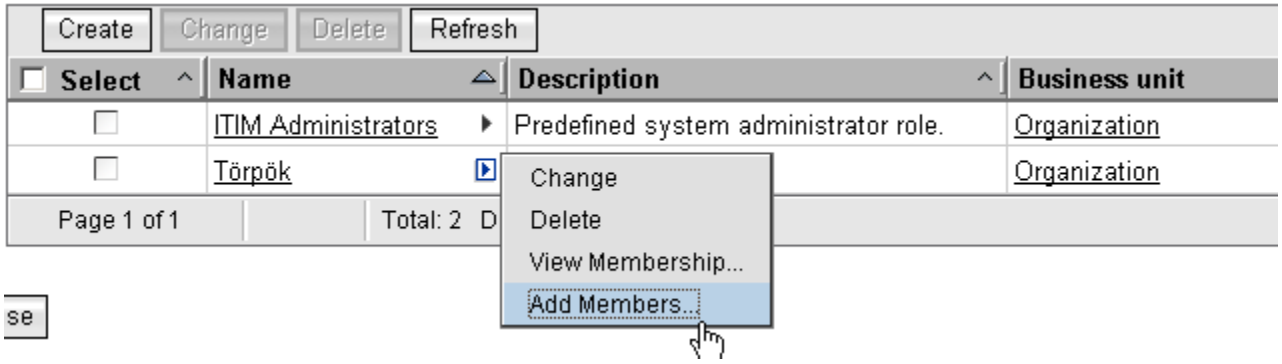
Sel...	Status	Request type	Date submitted	Requestor
	Success	Reconciliation	October 30, 2009 2:45:59 PM	System Administrator
	Success	Add Provisioning Policy	October 30, 2009 2:44:33 PM	System Administrator

Page 1 of 1 | Total: 2 Displayed: 2 Selected: 0

Role definiálása

- Manage Roles / refresh, create
  - Role name: Törpök
  - Többit nem kell változtatni, Finish

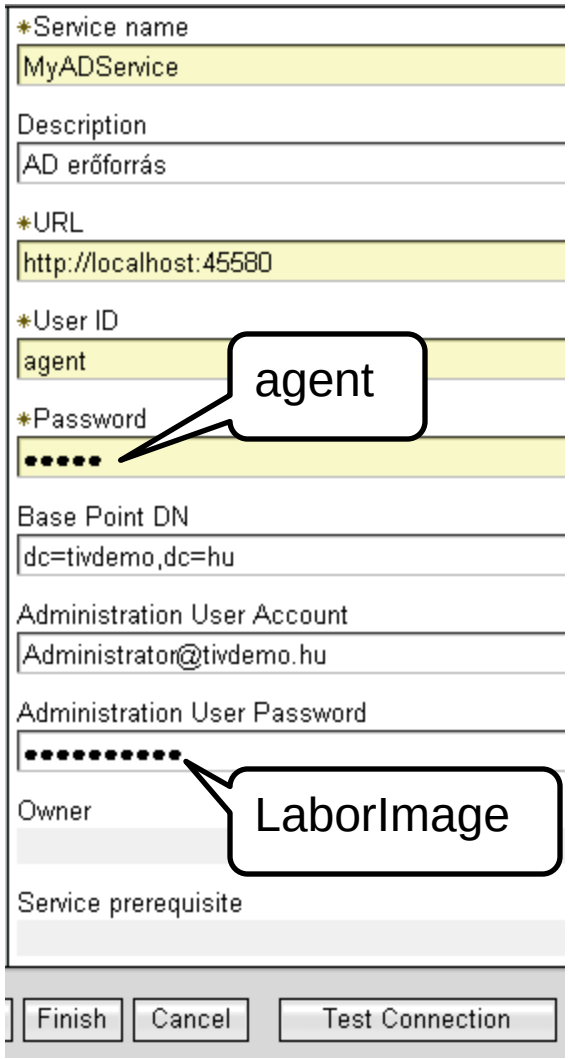
- Ez után adjunk törpöket a Törpök szerephez



(a System Admin kivételével mindenkit)

ITIM - AD „összelövés”

- Új AD Profile service (lásd: 2-es melléklet)
  - Test connenction
  - Finish
- Hozzunk létre egy új Adoptation policy-t
  - Services-nél válasszuk ki az AD service-t
  - Rule-nál sima egyezést keresünk
    - Add a match field
    - Eruid = uid
- AD Service / Reconcile now
- Majd Accounts… (ld. 2-es melléklet)
  - Mit látunk?



2. Kérdés

- A User ID oszlop az AD accountra vagy az ITIM Userra vonatkozik?
- Az Owner field helyén miért van néha None?

- Az ITIM-ben jötték létre új accountok / userek?

- Beugratós kérdés:
  - A csak AD-ban szereplő Accountok miért nem jöttek létre az ITIM-ben?

ITIM Userek lenyomása AD-be

- ITIM → AD lenyomás Provisioning Policyvel történik
- AD service megalkotásakor létrejött egy default provisioning policy, ezt módosítsuk
  - Entitlements alatt MyADService kijelöl, módosít
    - Provisioning options Automaticra állít
  - Entitlements alatt MyADService kijelöl, parameters
    - Create
    - Kiválaszt valamit, pl Lastname
    - JavaScript kijelöl
    - Mandatory kijelöl
    - Value: subject.getProperty(”Y”)[0]; ahol Y lehet cn, sn, givenname, uid, stb
    - Continue

    - Még pár paramétert állítsunk be pl display name, first name, stb

ITIM Userek lenyomása AD-be

- Preview-ben megnézhetjük mi fog változni (ez eltart egy darabig)
- Ha megfelel, Submit-ot nyomhatunk

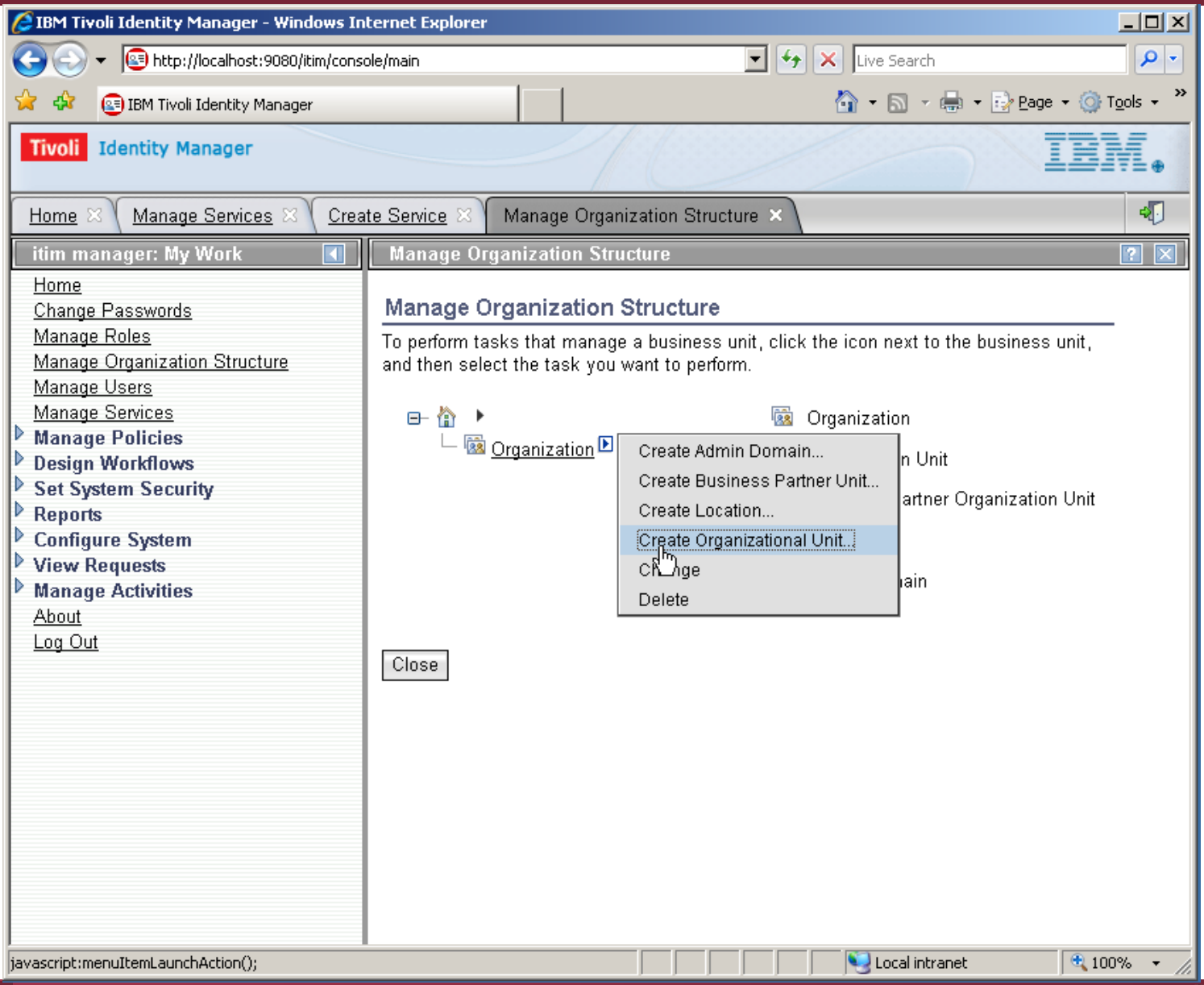
- Ez után AD service reconciliation

- Nézzük meg az AD-ben, hogy létrejöttek-e az ITIM-ben létező felhasználókhoz, az új AD fiókok (akiknek eddig nem volt)

Árva Accountok kezelése

- Mik azok az árva accountok?
- Vannak ilyenek a rendszerben? Kik azok (és hogyan állapítjuk meg)?
- Suspendeljük az árva accountok AD hozzáférését
  - Ellenőrizzük az AD-ben, hogy valóban fel lettek-e függesztve az accountok

1-es melléklet



2-es melléklet