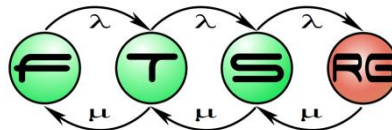


Felhasználói Identitás Menedzsment

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 Adoption 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, lépünk 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 Organization 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

Create Service

Manage Services > Create a Service > Service

To use a service, specify the name of the service and inform where the service resides. To test the connection to the server, click Test. Then, click Finish.

*Service name
MyCSVService

Description
Beolvassa a törpöket

*File name
C:\Documents and Settings\Administrator.TIVDEMO\Des

Use workflow

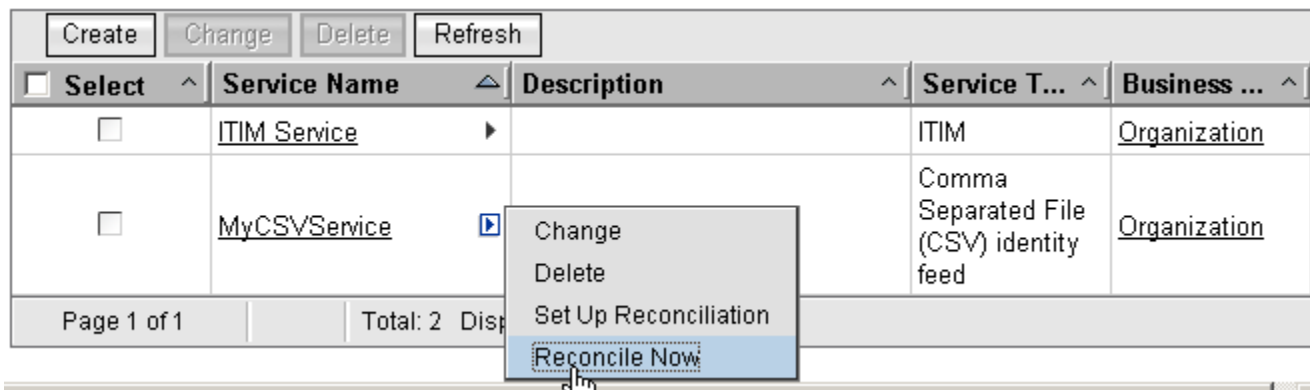
Person profile name
Person

*Name attribute
cn

Placement rule
return "ou=Törpfalva";

CSV-ből Userek felolvasása

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

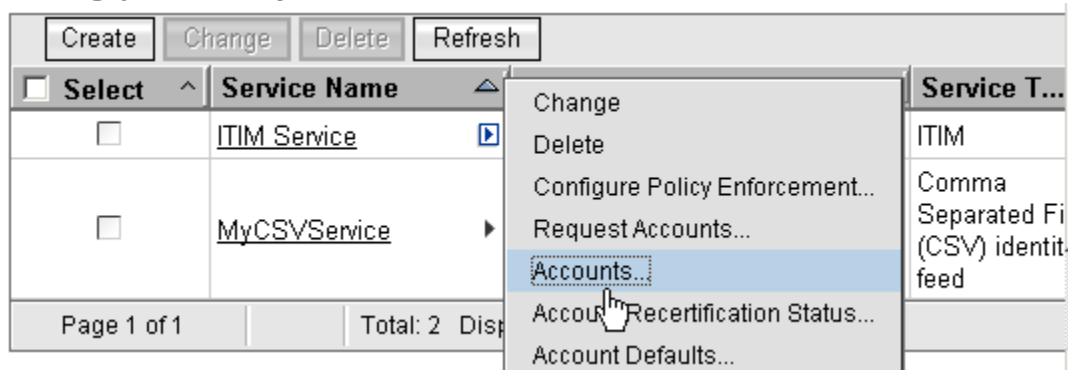


<input type="checkbox"/> Select	Service Name	Description	Service T...	Business ...
<input type="checkbox"/>	ITIM Service		ITIM	Organization
<input type="checkbox"/>	MyCSVService		Comma Separated File (CSV) identity feed	Organization

Page 1 of 1 Total: 2 Dis

Change
Delete
Set Up Reconciliation
Reconcile Now

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



<input type="checkbox"/> Select	Service Name	Service T...
<input type="checkbox"/>	ITIM Service	ITIM
<input type="checkbox"/>	MyCSVService	Comma Separated Fi (CSV) identit-feed

Page 1 of 1 Total: 2 Dis

Change
Delete
Configure Policy Enforcement...
Request Accounts...
Accounts...
Account Recertification Status...
Account Defaults...

CSV-ből Userek felolvasása

- Miért jöttek létre automatikusan ITIM fiókok a felhasználókhhoz?
 - Identity Policy-ket nézzük meg (különösen a MyIdentityPolicyt), értelmezzük, itt nem kell egyébbet 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**.

<input type="checkbox"/> 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

The screenshot shows a web-based interface for managing roles. At the top, there are buttons for 'Create', 'Change', 'Delete', and 'Refresh'. Below these is a table with the following columns: 'Select', 'Name', 'Description', and 'Business unit'. The table contains two rows: 'ITIM Administrators' and 'Törpök'. The 'Törpök' row is selected, and a context menu is open over it, showing options: 'Change', 'Delete', 'View Membership...', and 'Add Members...'. The 'Add Members...' option is highlighted. Below the table, there is a search box containing 'se' and a status bar showing 'Page 1 of 1' and 'Total: 2 D'.

Select	Name	Description	Business unit
<input type="checkbox"/>	ITIM Administrators	Predefined system administrator role.	Organization
<input checked="" type="checkbox"/>	Törpök		Organization

(a System Admin kivételével mindenkit)

ITIM - AD „összelövés”

- Új AD Profile service (lásd: 2-es melléklet)
 - Test connection
 - Finish
- Hozzuk létre egy új Adoption 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?

*Service name	MyADService
Description	AD erőforrás
*URL	http://localhost:45580
*User ID	agent
*Password	*****
Base Point DN	dc=tivdemo,dc=hu
Administration User Account	Administrator@tivdemo.hu
Administration User Password	*****
Owner	LaborImage
Service prerequisite	

Buttons: Finish, Cancel, Test Connection

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 jöttek létre új accountok / usererek?
- 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

The screenshot shows the IBM Tivoli Identity Manager console in a Windows Internet Explorer browser. The address bar shows the URL `http://localhost:9080/itim/console/main`. The page title is "IBM Tivoli Identity Manager". The navigation tabs include "Home", "Manage Services", "Create Service", and "Manage Organization Structure". The left sidebar contains a "My Work" section with various links like "Home", "Change Passwords", "Manage Roles", "Manage Organization Structure", "Manage Users", "Manage Services", "Manage Policies", "Design Workflows", "Set System Security", "Reports", "Configure System", "View Requests", "Manage Activities", "About", and "Log Out". The main content area is titled "Manage Organization Structure" and contains the instruction: "To perform tasks that manage a business unit, click the icon next to the business unit, and then select the task you want to perform." Below this is a tree view showing a folder named "Organization" with a sub-item "Organization". A context menu is open over the "Organization" sub-item, listing the following actions: "Create Admin Domain...", "Create Business Partner Unit...", "Create Location...", "Create Organizational Unit..." (which is highlighted), "Change", and "Delete". A "Close" button is visible below the tree view. The status bar at the bottom shows "Local intranet" and "100%".

2-es melléklet

Tivoli Identity Manager

Home > Manage Users > Manage Passwr > Manage Identity > Manage Access > Manage Accour > Change Account > Manage Service

itim manager: My Work

Manage Services

Services

To perform a particular task on a service, click the icon next to the service name, and then select the task you want to perform.

3 results found for: *

Create Change Delete Refresh

<input type="checkbox"/> Select	Service Name	Description	Service T...	Business ...
<input type="checkbox"/>	ITIM Service	Change	ITIM	Organization
<input type="checkbox"/>	MyADService	Delete	Active Directory Profile	Organization
<input type="checkbox"/>	MyCSVService	Set Up Reconciliation Configure Policy Enforcement... Manage Groups and Access... Request Accounts... Accounts... Account Recertification Status... Account Defaults... Reconcile Now	Comma Separated File (CSV) identity feed	Organization

Page 1 of 1 Total: 3 Dis

Close