Informatikai technológiák laboratórium 2

Felhasználói identitás menedzsment

Mérési segédlet

Készítette: Paljak Gergely és Szombath István

Bősze Tibor és Gönczy László anyagának felhasználásával

2009. október 20.

Verzió: 1.3

Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

1 Bevezető

A mérés során a központosított felhasználói azonosító kezelés (identitás menedzsment) feladataival ismerkedünk meg, IBM Tivoli Identity Manager 5.0 eszközt, valamint Windows Active Directory szolgáltatást használva.

A felkészülést a mérésvezető minden alkalommal ellenőrzi. A mérést megelőző otthoni felkészülésként végezze el az alábbiakat önállóan.

- Olvassa el a jelen segédletben szereplő áttekintőt!
- Válaszolja meg a (mérési leírás végén található) Ellenőrző kérdéseket!

2 Alapfogalmak

Ez a fejezet röviden ismerteti a központosított felhasználókezelés fogalmait, előnyeit, tipikus megvalósítási lehetőségeit, valamint a mérés során használt eszközöket, elsődlegesen az IBM Tivoli Identity Manager 5.0 (ITIM) és a Microsoft Windows Active Directory (AD) funkcióinak és felépítésének leírásával.

2.1 Felhasználói azonosítók kezelése

2.1.1 A központosított felhasználókezelés előnyei

A központosított (federált) felhasználó azonosítókezelésnek számtalan előnye van:

- Felhasználók életciklusának központosított kezelése
  - Azonosító kérése
  - Erőforrásokhoz (pl. szerverekhez) történő hozzáférés szabályozása
  - Azonosítók automatikus felfüggesztése/törlése/meghosszabbítása
- Központosított kockázatkezelés (pl. elbocsátott dolgozónak nem marad hozzáférése)
- Egyszerű interfész a felhasználók adatainak és azonosítóinak kezeléshez
- Központi policy (házirend) definiálás (pl. gyenge jelszavak elutasítása)
- Központosított jelszókezelés (nem azonos a Single Sign-On-al!)
- Felhasználók csoporttagságainak központosított kezelése
- Help desk terhelésének csökkentése (felhasználói panaszok kezelésére egyszerű folyamatok)
- Felhasználótárak (pl. LDAP, HR rendszer, alkalmazások) és IT erőforrások (pl. operációs rendszerek, hálózati eszközök, hozzáférésvédelmi –Access management– eszközök) egységes kezelése

A központi felhasználói azonosítókezelés lehetővé teszi emellett az egységes audit és jelentéskészítés (reporting) megvalósítását, melyet bizonyos területeken szabványok, törvényi szabályozás ír elő. Ilyenek pl. a Sarbanes-Oxley az amerikai tőzsdén jelenlévő vállalatokra, a Basel II az európai pénzügyi rendszerekre, ill. PSZÁF szabályozása és ajánlásai magyar pénzügyi intézetekre (bankok, biztosítók, magánnyugdíjpénztárak, befektetési alapok, stb.).

2.1.2 Hozzáférésszabályozási modellek

A hozzáférés szabályozási modellek alapvetően azt írják le, hogy a rendszer különböző szereplői a rendszer erőforrásain milyen műveletek elvégzésére jogosultak.

A legismertebb hozzáférés szabályozási modellek a következők:

Role-Based Access Control (RBAC). A felhasználókat ill. felhasználói csoportokat szerepekhez rendeljük, és ezekhez a szerepekhez rendelünk központilag hozzáférési jogokat (pl. „Minden menedzser használhatja az X modult.” „Minden projektvezetőnek írási joga van az Y adatbázistáblához”).

Az ITIM alapvetően ennek a modellnek a megvalósítását támogatja.

Discretionary Access Control (DAC). Ebben a modellben az erőforrás tulajdonosa dönti el, hogy kinek milyen jogot ad. Tipikusan olyan elosztott környezetekben használható, amik fokozatosan „épültek össze" egy rendszerré. Veszélye, hogy nehezen ellenőrizhető, karbantartható, és nagyon sok múlik az egyes erőforrások tulajdonosain, előnye ugyanakkor, hogy könnyen megvalósítható.

Mandatory Access Control (MAC). Ebben a modellben az erőforrásokat „érzékenységüknek" megfelelően csoportosítjuk (pl. dokumentumoknál Unclassified/Restricted/Confidential/Secret) és a felhasználókat jogosultsági szintjük alapján engedjük műveleteket végezni. Ez használatos pl. katonai rendszerekben (ahol olyan plusz követelmények is lehetnek, mint pl. ne lehessen egyszerre olvasni titkos dokumentumokat, és írni nyilvánosakat). Előnye, hogy nagyon biztonságos, ugyanakkor nehéz megvalósítani (főképp heterogén rendszerekben).

2.1.3 Felhasználómenedzsment megvalósítások

Az alábbiakban azt tekintjük át, hogyan tárolhatóak (logikailag) a felhasználói adatok ill. jogosultságok.

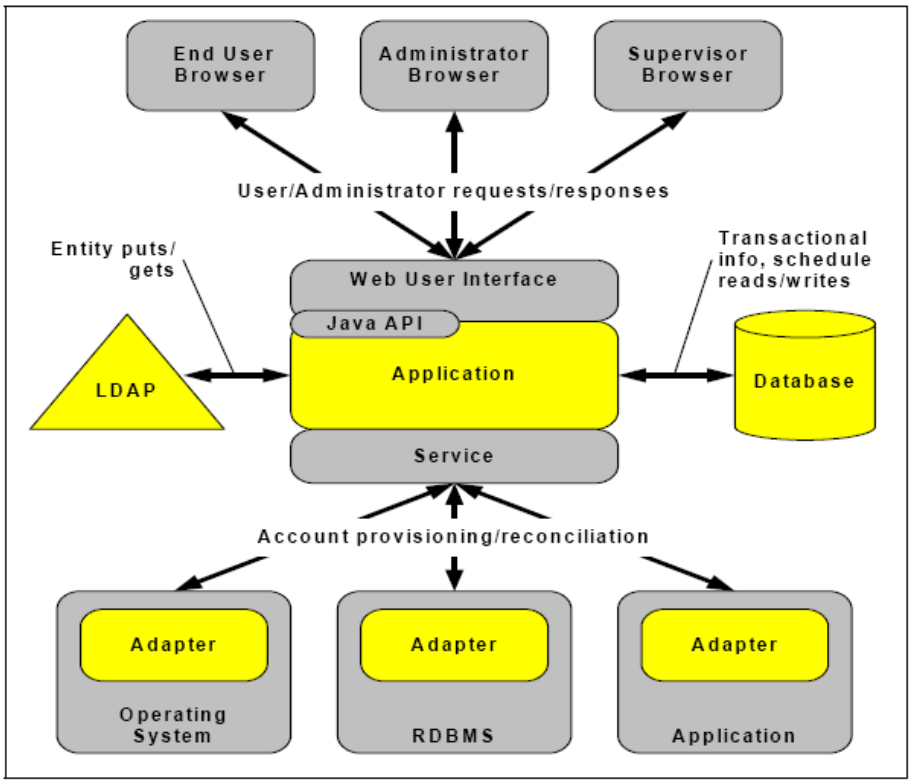
- *Egy címtár (Single Directory).* Egy központi címtárban tároljuk a felhasználókat (pl. MS Active Directory). Ennek megvan az az előnye, hogy minden felhasználót, szerepet, házirendet egy helyen kell karbantartani, hátránya viszont, hogy az egyes rendszereket, alkalmazásokat mind egy rendszerhez kell integrálni.
- *Több címtár (Mupltiple directories).* A legtöbbször ez alakul ki, mivel flexibilis, kevés tervezést igényel. Hátránya, hogy nehezen karbantartható, ill, nehéz házirendeket definiálni, valamint könnyen jönnek létre „árva" felhasználók (melyek igazából már nincsenek a rendszerben, de egy címtárban mégis megtalálhatóak). Tipikus példája lehet egy szervezeten belül egy LDAP és egy Active Directory használata.
- *Metakönyvtár (Meta directory).* Egy olyan címtár/könyvtár, mely a szervezeten belüli összes felhasználói adat másolatát tartalmazza. Itt problémát jelenthet a teljesítmény ill. a többszöri adminisztrációs belépési pontok (a metakönyvtárban ill. a tényleges könyvtárakban), valamint a komplex szabályrendszerek definiálása, melyek pl. a több címtárban egyszerre kezelik egy felhasználó változását. Ismert ennek virtuális változata is, ahol a felhasználói címtárakról nem jön létre tényleges másolat.
- *Saját felhasználói adminisztrációs eszközök.* Tipikusan régebben definiált, nehezen bővíthető eszközök, melyek egy-egy célalkalmazás igényeit szolgálják (de akár példa lehet az LDAP valamilyen speciális sémával).
- *Felhasználói azonosító menedzsment eszközök (identity management).* Leginkább a virtuális metacímtárakhoz hasonlítanak, tipikusan valamilyen saját házirend ill. munkafolyamat definíciós lehetőséggel, egyszerű webes felülettel. A megoldás hátránya, hogy adott esetben valamilyen adapter létrehozását igényli az egyes címtárak központi rendszerbe kapcsolásához (mint ahogy ez igaz az ITIM esetében), ugyanakkor rugalmas, bővíthető, könnyen ellenőrizhető. Sok esetben identity management megoldásnak neveznek pl. több, web alapú rendszer összekapcsolásával előálló, elosztott felhasználó nyilvántartást megvalósító technológiát (pl. Liberty project), azonban jelen labor alatt egy központosított eszközt használunk.

Az ITIM az eddigiek alapján egy szerep alapú hozzáférést támogató felhasználói identitás menedzsment eszköz.

2.2 IBM Tivoli Identity Manager

Ez a fejezet bemutatja a mérésen használt ITIM felépítését és főbb feladatait. A szintén használt ***IBM Tivoli Directory Integrator*** eszközről a mérés elején rövid ismertető hangzik el, ill. bővebb információ található a források közt. Ennek funkciója esetünkben lényegében adatkonverzió egy „kívülről kapott" leíró (jelen esetben CSV állomány) és az ITIM által használt LDAP közt.

2.2.1 Az ITIM komponensei



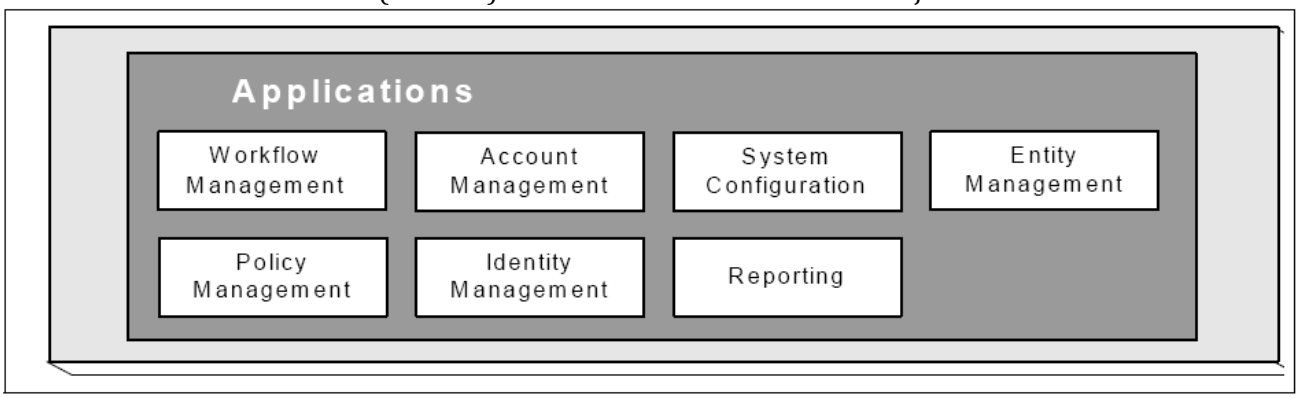
Az ITIM logikai architektúrája

Az ITIM főbb komponensei a következők (az ábra középső része):

Webes felület: ezen keresztül érik el a felhasználók ill. adminisztrátorok. Feladata űrlapok megjelenítése, munkakörnyezet megjelenítése, szervezeti struktúra (organization) ill. folyamatok (workflow) megjelenítése, interfész biztosítása az alkalmazás mag felé.

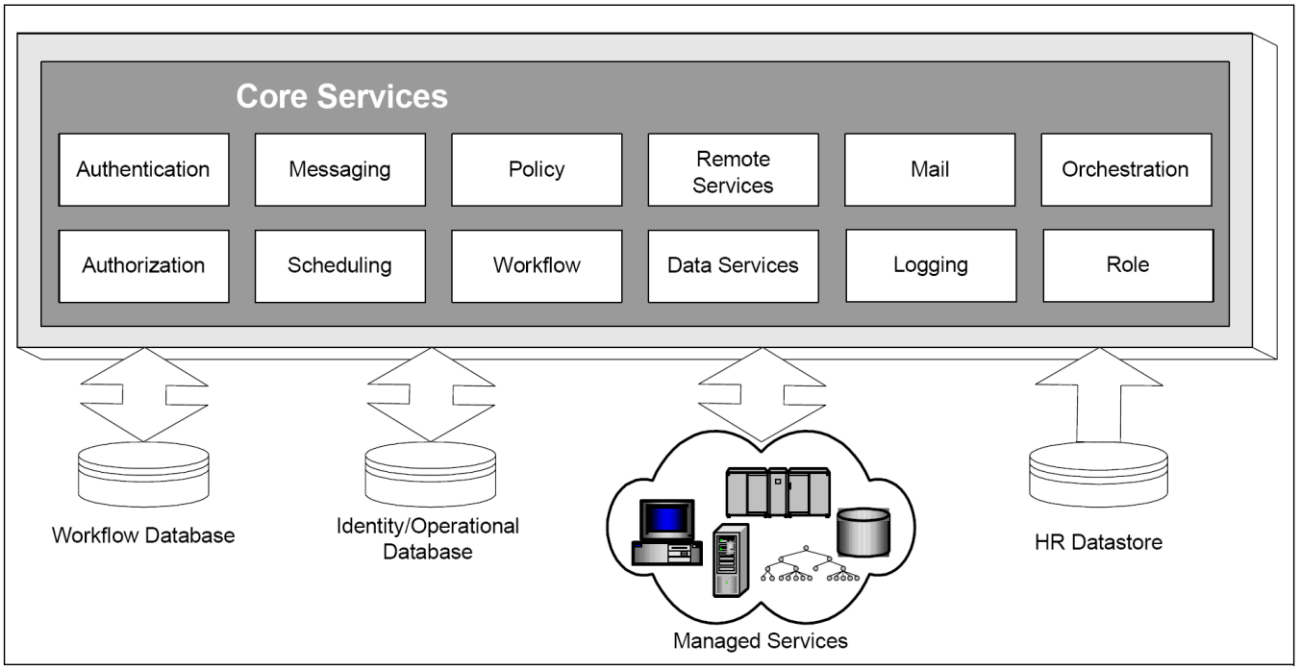
Java API: a webes felület részben ezen keresztül éri el az alkalmazást. Elvileg hívható saját alkalmazásból is, illetve pl. a definiált folyamatok is ezt használják.

Az alkalmazási réteg (***Application layer***) valósítja meg a „provisioning" feladatokat, vagyis az egyes felhasználókhoz történő fiók (account) hozzárendelést. Ennek almoduljai az alábbi ábrán láthatóak.



ITIM alkalmazás réteg

A szolgáltatási réteg (***Service Layer***) feladata részben magának az ITIM-nek a hozzáférésvédelme (autentikáció és autorizáció), részben a különböző adatforrások elérése. Ilyen adatforrások maguk a menedzselt erőforrások (Active Directory, LDAP, adatbázis, stb., lásd részletesen az adapterek ismertetésénél) és az ITIM-en belül definiált azonosítók, folyamatok, stb.



Az ITIM szolgáltatásai

(Érdemes megjegyezni, hogy maga az ITIM tulajdonképpen egy IBM WebSphere Application Server felett futó Java alapú webalkalmazás.)

Ahhoz, hogy az ITIM működjön, értelemszerűen szükség van további, perzisztenciát biztosító komponensekre.

LDAP (*Lightweight Directory Access Protocol*): Egy olyan alkalmazás, mely a szabványos LDAP protokollt megvalósítva tárolja a szervezeti egység állapotát. Az ITIM is LDAP séma használatával végzi saját, központi felhasználókezelését (a DB2 LDAP szolgáltatását használva), valamint itt tárolja a szervezeti egység(ek) teljes állapotát (felhasználók, szervezeti csoportok, házirendek, folyamatok stb.). A mérés során ebbe az LDAP címtárba fogunk közvetlenül felhasználókat importálni Tivoli Directory Integrator segítségével.

Adatbáziskezelő *(Database)*: Az épp végrehajtott tranzakciók állapotát, ütemezési, statisztikai, riportolási információkat tároló adatbázis.

A menedzselt erőforrásokat ***adaptereken*** keresztül éri el az ITIM. Ezeket az adaptereket egyrészt telepíteni kell az adott erőforrásra, másrészt be kell állítani a központi alkalmazásban az elérés paramétereit (pl. protokoll, hálózati cím). Az adapter elérése jelszóhoz kötött, ill. az adapternek ismernie kell egy adminisztrátori joggal rendelkező felhasználó adatait az erőforrás menedzsmenthez (pl. felhasználó létrehozása LDAP-ban). Ezeket az adatokat szintén eltárolhatjuk a központi rendszerben.

Adapter típusok. A mérésen használt (5.0 verziójú) ITIM-hez elérhető fontosabb adapterek a következők:

Operációs rendszerhez illesztett adapterek:

- AIX (IBM UNIX)
- Linux
- HP-UX
- OS/400
- Solaris

Címtár rendszerekhez illesztett adapterek:

- Windows Active Directory
- LDAP
- Novell Netware

Adatbáziskezelőkhöz illesztett adapterek:

- DB2 adapter
- Oracle adapter
- Sybase

Alkalmazásokhoz illesztett adapterek:

- Lotus Notes (ez kezelhet egyfajta címtárat is, a Domino Directory-t)
- Tivoli Access Manager for Single Sign-On (integrált IBM security megoldás)

Saját adapter is definiálható, ehhez két komponenst kell megírni. Egyrészt magát a menedzselt szerverre feltelepíthető adaptert, másrészt az adapterrel kommunikáló ill. ahhoz felületet biztosító alkalmazást, amit az ITIM-et futtató alkalmazásszerverre kell feltelepíteni (.jar formájában). Az adapterek képessége értelemszerűen eltérő lehet, viszont vagy az IBM által használt DAML (Directory Access Markup Language) vagy az ipari szabványnak számító DSML (Directory Service Markup Language) XML sémának megfelelő adatcsomagokkal kommunikálnak, HTTPS (SSL) felett.

Emellett Tivoli Directory Integrator használatával számos egyéb adatforrás integrálható egyszerű szkriptekkel (a labor során is ezt csináljuk, CSV állományt felhasználva).

2.2.2 Az ITIM funkciói

- Felhasználók számára felület biztosítása az egységes account kezeléshez (pl. személyes adatok – akár telefonszám - megváltoztatása, jelszó megadása) szabványos böngészőn keresztül. Emellett teendőket is lehet kezelni (pl. adminisztrátori joggal rendelkező felhasználók láthatják a jóváhagyásra váró kéréseket).
- Jelszókezelés. A központi rendszerben érvényes jelszavakat automatikusan érvényesíti a menedzselt erőforrásokra (password synchronization), ill. ha ez engedélyezett, képes az egy erőforráson megváltoztatott jelszót a többi erőforrásra is érvényesíteni (reverse password synchronization). A műveletek során érvényesíti a jelszavakra vonatkozó házirendeket (password policy) pl. gyenge jelszavak elutasítására. Emellett definiálhatóak biztonsági kérdések az elfejtett jelszavak kezeléséhez.
- Személyek (Person) és fiókok (Account) kezelése, keresése, beállítása, szerepek és csoportok kezelése, stb. A felhasználókat az LDAP-ra emlékeztető fa struktúrában jeleníti meg az eszköz, ami alapvetően a szervezeti felépítést követi. Minden szerep, házirend és szabály definiálható ennek a fának tetszőleges részeire. Emellett ITIM-en belül definiált szerepekhez köthető az is, hogy milyen funkciók legyenek elérhetőek a felületen (pl. ITIM adminisztrátorok láthassák az összes felhasználó adatait, a felhasználók csak saját adataikat, stb.), ill. bizonyos felhasználók számára akár le is tiltható a központi felület elérése (pl. külső partnereknek). Az ITIM következő (5.) verziójában tovább finomíthatóak ezek a nézetek.
- Házirendek betartatása. Az ITIM-ben definiálhatóak házirendek (ld. alább), melyek egy részét folyamatosan, más részét az erőforrásokkal történő szinkronizáció során kiértékel a rendszer. Ha valamelyik házirend nem teljesül, akkor vagy megpróbálja végrehajtani (pl. hiányzó accountot létrehoz), vagy jelzi ezt az ITIM adminisztrátoroknak. A házirend érvényesítésének beállításai erőforrás szinten adhatóak meg.
- Felhasználói fiókok szinkronizálása az erőforrásokkal (reconciliation). Ütemezett módon lekérdezi az erőforrásokon érvényes felhasználói fiókokat az adapterektől, ill. végrehajtja a házirendben definiált változtatásokat. Fontos, hogy nem mindegyik változtatással várja meg a szinkronizációt, pl. a jelszóváltás hatása azonnali, a felhasználó törlése is kikényszeríthető azonnal, ezzel szemben pl. csoporttagság változást a szinkronizáció alkalmával hajt végre.

- Egyszerűbb folyamatok (workflow) definiálása és végrehajtása. Ilyenekkel kezelhető pl. ha egy személy belépve az ITIM felületére, hozzáférést igényel egy erőforráshoz, ha egy személynek megváltozik a szervezetben betöltött szerepe (és ezért pl. le kell tiltani egy erőforráshoz való hozzáférését, vagy másik csoportba kell rakni). A folyamatokban definiálhatóak automatikus ill. ember által végrehajtandó lépések (pl. jóváhagyás). Fontos, hogy a házirendekben definiált szabályok ilyen esetekben sem sérülhetnek.
- Jelentések generálása (pl. milyen változások voltak a felhasználói fiókokban, hány új fiók jött létre, hány nem megfelelő fiók van a rendszerben, hány kérés vár jóváhagyásra, hány elutasított kérés volt, stb.)
- E-mail értesítés (pl. adminisztrátoroknak új tennivalóról, felhasználóknak jelszó lejáratról, stb.).
- Tennivalók (todo) kezelése, delegálási lehetőség (pl. szervezetileg illetékes egység adminisztrátorának).
- Import/export funkció az ITIM-en belül definiált entitásokhoz (szerepek, házirendek, csoportok, folyamatok). Fontos, hogy maguknak a felhasználóknak az importját az ITIM „alatti" LDAP migrálásával kell elvégezni (pl. Tivoli Directory Integrator használatával).

2.2.3 Házirend (policy) típusok

- *Provisioning policy*. Ennek használatával adhatjuk meg, hogy egy menedzselt erőforráson milyen fiókokkal (account) rendelkezzenek a felhasználók, ill. ezeknek milyen paraméterei legyenek (ideértve pl. a csoporttagságot, jelszó megváltoztatásának lehetőségét, stb.). Fontos, hogy az ITIM önmagában nem alkalmas arra, hogy a menedzselt erőforráson pl. csoportoknak hozzáférési jogot adjon, ezt vagy az erőforrás adminisztrátorának kell megoldania, vagy valamilyen más központosított eszközzel (pl. Tivoli Access Manager) oldható meg. Egy provisioning policy valós rendszerekben tipikusan csoporthoz/szerephez rendelt, de definiálható az egész szervezeti egységre is.
- *Service selection policy.* A service selection policy segítségével kiválaszthatjuk, hogy pontosan melyik erőforrás példányra akarunk fiókot létrehozni egy felhasználónak. Pl. földrajzilag elosztott szervezetnél definiálható egy központi policy az Active Directory fiókok létrehozására, és egy service selection policy a szervezeti egység (pl. ország) tagjainak konkrét Active Directory példányhoz rendelésére.
- *Identity policy.* Az identity policy szabja meg, hogyan jön létre a felhasználói azonosító (pl vezetéknév+keresztnév első betűje). Alkalmazható globálisan, erőforrás típusra (pl. LDAP) és erőforrás példányra (pl. BME MIT LDAP) is.
- *Password policy.* Ennek segítségével állíthatóak be a jelszavak paraméterei, pl. hosszúság, megkövetelt karakterosztályok, stb. Alkalmazható globálisan, erőforrás típusra vagy példányra.

2.3 Windows Active Directory

Az Active Directory (AD) főbb jellemzői:

- Az AD-ben tárolható fontosabb objektumok: felhasználók, csoportok, számítógépek, nyomtatók, házirendek, de akár felhasználó által definiált típusok is.
- Minden objektumtípushoz egy előre megadott attribútum halmaz tartozik (pl. a felhasználónak neve, email címe, telefonszáma, stb. van), melyet a séma definiál.
- Az Active Directory hierarchikus felépítésű. Az adminisztráció egysége a tartomány (domain). A tartományt a DNS nevével adjuk meg (melyet általában célszerű elkülöníteni a publikus internetes DNS névtől, pl. clusterdemo.hu és clusterdemo.local). Egy tartomány képez egy biztonsági egységet, pl. a felhasználók a tartományi login-ükkel be tudnak jelentkezni bármelyik, a tartományba beléptetett gépre. A tartományon belül a hierarchiát szervezeti egységeknek (organizational unit) nevezett konténerek létrehozásával adhatjuk meg.

3 A mérés menete

A mérés két fő részre osztható. Először egy előre elkészített állományból beolvasunk felhasználókat az ITIM-be, majd ezeknek a felhasználóknak elkészítjük az AD fiókjait, illetve összerendeljük őket a meglévő AD fiókokkal, kezeljük az árva fiókok problémáját.

A mérés pontos leírását a mérés alkalmával kapják meg.

4 Ellenőrző kérdések

1) Milyen előnyei vannak a központosított felhasználókezelésnek?
2) Milyen központosított felhasználókezelési megoldásokat ismer?
3) Mik a szerep alapú hozzáférés szabályozás (RBAC) főbb feladatai?
4) Mik a Windows Active Directory szolgáltatás főbb feladatai?
5) Milyen logikai komponensei vannak az ITIM-nek?
6) Milyen komponensekből áll az ITIM alkalmazás ill. szolgáltatási réteg?
7) Mi a feladata az LDAP-nak, ill. mi a szerepe az ITIM háttér adatbázisának?
8) Milyen főbb funkciói vannak az ITIM-nek?
9) Milyen erőforrásokat képes menedzselni az ITIM?
10) Hogyan illeszthető hozzá egyéb erőforrás a rendszerhez?
11) Milyen házirendek definiálhatóak az ITIM-ben?
12) Mit értünk árva felhasználó alatt?

Források

Tivoli Identity Manager rövid magyar leírás

http://www-142.ibm.com/software/dre/ecatalog/detail.wss?locale=hu_HU&synkey=H106131Z52161X73

Online help

http://www-01.ibm.com/software/tivoli/products/directory-integrator/

Identity Management Design Guide with IBM Tivoli Identity Manager (mérés közben is hasznos)

http://www.redbooks.ibm.com/abstracts/SG246996.html?Open

Tivoli Software Information Center

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itim.doc/welcome.htm

Active Directory, LDAP bemutatása az Intelligens rendszerfelügyelet tárgyban

(Címtár szolgáltatások:LDAP, Active Directory) http://sauron.inf.mit.bme.hu/Edu/IIM/iim08.nsf

A Liberty Alliance project

http://www.projectliberty.org

Identity management wikipedia oldal (némileg más megközelítés)

http://en.wikipedia.org/wiki/Identity_management