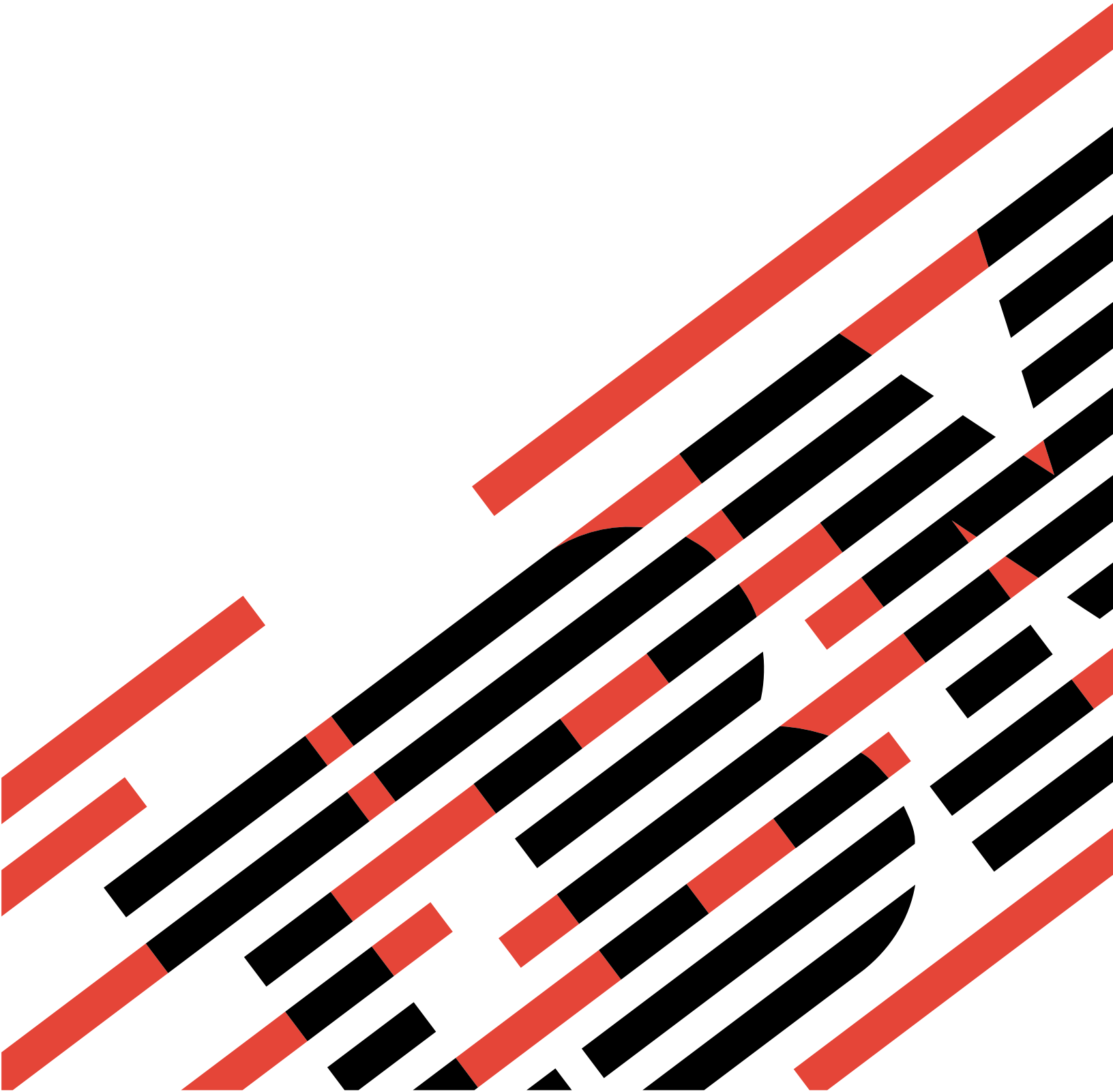
IBM

eserver

iSeries

Vállalati azonosság leképezés



IBM

@server

iSeries

Vállalati azonosság leképezés

Tartalom

Vállalati azonosság leképezés (EIM)

A legtöbb hálózatot alkalmazó vállalat szembekerül a több felhasználói nyilvántartás használatából adódó problémákkal, amelyek megkövetelik, hogy a vállalat minden egyes személye vagy entitása minden nyilvántartásban rendelkezzen egy felhasználói azonossággal. A több felhasználói nyilvántartás szükségessége hamar olyan adminisztrációs problémává növi ki magát, amely a felhasználókra, adminisztrátorokra és alkalmazásfejlesztőkre is hatással lesz. A Vállalati azonosság leképezés (EIM) költséghatékony megoldást biztosít a vállalati felhasználói nyilvántartások és felhasználói azonosságok kezelésének leegyszerűsítésére.

Az EIM mechanizmusa lehetővé teszi egy személy vagy entitás leképezését (társítását) a vállalatban alkalmazott különféle nyilvántartások megfelelő felhasználói azonosságaira. Az EIP által biztosított API-k az említett leképezési viszonyok létrehozására és kezelésére, illetve lekérdezésére is alkalmasak. Emellett az OS/400(R) az EIM és Kerberos képességeivel biztosít egyszeri bejelentkezést alkalmazó környezetet.

Az iSeries navigátor, az iSeries grafikus felhasználói felülete több varázslót is kínál az EIM beállítására és kezelésére. Emellett az adminisztrátorok az iSeries navigátorból kezelhetik a felhasználói profilok EIM viszonyait is.

Az iSeries(TM) server az EIM segítségével biztosítja, hogy az OS/400 illesztői a hálózati hitelesítési szolgáltatás segítségével hitelesítsék a felhasználókat. Az alkalmazások az OS/400 operációs rendszerrel együtt elfogadnak Kerberos jegyeket is, és az EIM segítségével keresik ki a Kerberos jegyet képviselő személynek megfelelő felhasználói profilt.

Az EIM támogatásról a következő témakörök nyújtanak részletes információkat:

A témakör kinyomtatása
Az EIM témakör és más kapcsolódó témakörök kinyomtatása.

Vállalati azonosság leképezés (EIM) áttekintése
Itt ismerheti meg az EIM segítségével megoldható problémákat, a problémáknak az iparágban alkalmazott jelenlegi megközelítéseit, és ezek összehasonlítását az EIM megközelítésével.

EIM alapelvek
Itt szerezheti meg az EIM sikeres megvalósításához szükséges EIM alapismereteket.

EIM LDAP alapelvek
Itt szerezheti meg az EIM sikeres megvalósításához szükséges Egyszerűsített címtárhozzáférési protokoll (LDAP) alapismereteket.

Egyszeri bejelentkezés kialakítása
Itt ismerheti meg azokat az előnyöket, amelyeket az EIM a felhasználói bejelentkezés leegyszerűsítésével nyújt.

EIM tervezése
Ezen szakasz segítségével győződhet meg arról, hogy minden szükséges szolgáltatás és alkalmazás beállításra került az EIM konfigurálásának megkezdése előtt.

EIM beállítása
Ez a szakasz írja le a Vállalati azonosság leképezés (EIM) konfigurációs varázslót (a továbbiakban EIM konfigurációs varázsló), amely végigvezeti az EIM támogatással kapcsolatos kezdeti lépéseken.

EIM kezelése
Az EIM tulajdonságok, tartományok, felhasználói nyilvántartások, EIM felhasználói jogosultságok és további elemek kezelése.

EIM API-k
Ez a szakasz írja le az EIM API-k használatát az alkalmazásokban és a hálózaton.

EIM hibaelhárítás
Itt találja az EIM használata során felmerülő általános problémák megoldásait.

EIM kapcsolódó információk
Az EIM funkcióval kapcsolatos további információk.

A témakör kinyomtatása

A PDF változat megjelenítéséhez vagy kinyomtatásához kattintson a Vállalati azonosság leképezés (EIM)  hivatkozásra (megközelítőleg 390 KB vagy 50 oldal).

További információk

A következő kapcsolódó témakörök megtekintésére és letöltésére is lehetőség van:

- Hálózati hitelesítési szolgáltatások (megközelítőleg 200 KB vagy 60 oldal) - Ez a kiadvány írja le az egyszeri bejelentkezést biztosító környezetek kialakítását a Hálózati hitelesítési szolgáltatás és az EIM együttes felhasználásával.
- Címtár szolgáltatások (LDAP) (megközelítőleg 323 KB vagy 66 oldal) - Ez a kiadvány tárgyalja az EIM tartományvezérlőként használható LDAP szerverek beállítását, illetve körüljár néhány speciális konfigurációs kérdést is.

PDF fájlok mentése

A PDF fájlok mentése a munkaállomásra megjelenítés vagy nyomtatás céljából:

1. Nyissa meg a fájlt a böngészőben (kattintson a fenti hivatkozásra).
2. Válassza a böngésző **Fájl** menüjét.
3. Kattintson a **Mentés másként...** menüpontra.
4. Válassza ki a könyvtárat, amelybe a PDF fájlt menteni kívánja.
5. Kattintson a **Mentés** gombra.

Az Adobe Acrobat Reader letöltése

A PDF fájlok megjelenítéséhez és nyomtatáshoz szükség van az Adobe Acrobat Reader programra, amely letölthető az Adobe webhelyéről (www.adobe.com/prodindex/acrobat/readstep.html) .

Vállalati azonosság leképezés (EIM) áttekintése

Napjaink hálózati környezetei rendszerek és alkalmazások összetett csoportjai, amelyek egy idő után szükségszerűen vezetnek több felhasználói nyilvántartás fenntartásához. A több felhasználói nyilvántartás kezelése hamar olyan adminisztrációs problémává növi ki magát, amely a felhasználókra, adminisztrátorokra és alkalmazásfejlesztőkre egyaránt hatással lesz. Ennek következtében több vállalat is sziszifuszi küzdelmet folytat rendszereik és alkalmazásaik hitelesítési és jogosultsági kérdéseinek biztonságos kezelésével. A Vállalati azonosság leképezés (EIM) az IBM @server infrastruktúrájának technológiája, amely lehetővé teszi az adminisztrátoroknak és alkalmazásfejlesztőknek, hogy a problémát a korábbiaknál egyszerűbb és költséghatékonyabb megközelítéssel kezeljék.

A következő szakaszok vázolják fel részletesebben a problémákat, körvonalazzák az iparágban jelenleg alkalmazott megközelítéseket, és írják le, hogy az EIM megközelítése mennyiben jobb ezeknél.

A sok felhasználói nyilvántartás kezelésének problémája

Sok adminisztrátor felügyel olyan hálózatokat, amelyben különböző rendszerek és szerverek találhatók, amelyek mindegyikének megvan a maga egyedi módja a felhasználók kezelésére a saját felhasználói nyilvántartásában. Az összetett hálózatokban az adminisztrátoroknak több rendszeren kell kezelniük minden egyes felhasználó azonosságait és jelszavait. Emellett az adminisztrátoroknak gyakran össze kell hangolniuk ezen azonosságokat és jelszavakat, a felhasználókra pedig szintén nagy terheket ró egy sor azonosság és jelszó fejben tartása. Az ilyen környezetekben az adminisztrátori és felhasználói teher túllép minden ésszerű korlátot. Ennek következtében az adminisztrátoroknak egyre gyakrabban kell értékes idejüket meghiúsult bejelentkezések hibaelhárítására és elfelejtett jelszavak alaphelyzetbe állítására fecsérelniük.

A sokféle felhasználói nyilvántartás problémájával az alkalmazásfejlesztők is szembekerülnek, akiknek többrétegű vagy heterogén alkalmazásokat kellene írniuk. A fejlesztők megértik, hogy az ügyfelek fontos üzleti adatai többféle rendszeren találhatók, és ezek mindegyike saját felhasználói nyilvántartással rendelkezik. Ennek következtében általában saját felhasználói nyilvántartást kell létrehozniuk, és meg kell teremteniük a szükséges biztonsági környezeteket. Bár ez megoldja az alkalmazásfejlesztők problémáját, a felhasználók és adminisztrátorok terhei ezzel tovább nőnek.

Jelenlegi megközelítések

A sok felhasználói nyilvántartás fenntartásából adódó problémák megoldására több megközelítés és létezik, azonban ezek egyike sem biztosít teljes körű megoldást. Az Egyszerűsített címtárhozzáférési protokoll (LDAP) például osztott felhasználói nyilvántartási megoldást nyújt. Az LDAP (vagy más népszerű megoldások, például a Microsoft Passport) használata azt jelenti, hogy az adminisztrátoroknak egy újabb felhasználói nyilvántartást és biztonsági szemantikát kell kezelniük, vagy le kell cserélniük a jelenlegi nyilvántartásokra épülő meglévő alkalmazásokat.

Az ilyen jellegű megoldásokkal az adminisztrátoroknak a különféle erőforrásoknak megfelelően többféle biztonsági mechanizmust kell kezelniük, ez azonban az adminisztrátori terhek növelése mellett növelheti a biztonsági kockázatok valószínűségét is. Amikor egy erőforrásra többféle mechanizmus is vonatkozik, akkor jelentősen megnő annak az esélye, hogy a jogosultságoknak egy adott mechanizmusban való módosítása után elfelejtik módosítani azokat a többi mechanizmus szerint is. Komoly biztonsági kockázat lehet például, amikor egy felhasználó egy adott felületen nem érhet el egy erőforrást, legalább egy másikon viszont igen.

A munka befejezése után az adminisztrátorok joggal fogják azt gondolni, hogy a probléma nem lett teljes mértékben megoldva. A vállalatoknak általában igen sokat kell költeniük a jelenlegi felhasználói nyilvántartásokra és biztonsági technikákra, amíg ez a fajta megoldás praktikussá válik. Egy újabb felhasználói nyilvántartás és a hozzá tartozó biztonsági ellenőrzések létrehozása megoldja ugyan az alkalmazás szállítójának problémáját, a felhasználók és adminisztrátorok életét azonban cseppet sem könnyíti meg.

Egy másik lehetséges megoldást nyújthat az egyszeri bejelentkezéses megközelítés. Több olyan termék is rendelkezésre áll, amely lehetővé teszi az adminisztrátoroknak olyan fájlok fenntartását, amely az összes felhasználói azonosságot és jelszót tartalmazza. Ennek a megközelítésnek azonban számos gyenge pontja van:

- A felhasználók által tapasztalt problémáknak csak az egyikét oldja meg. Bár lehetővé teszi a felhasználóknak, hogy egyetlen azonossággal és jelszóval több rendszerre jelentkezzenek be, nem küszöböli ki annak szükségességét, hogy a felhasználók külön azonosítóval és jelszóval rendelkezzenek, emellett továbbra is szükség van ezen jelszavak kezelésére.
- Bevezet egy új biztonsági problémát a nyílt szöveges vagy visszafejthető jelszavak tárolásával. A jelszavakat sohasem szabad nyílt szöveges vagy bárki számára (adminisztrátorokat is ideértve) egyszerűen hozzáférhető formában tárolni.
- Nem oldja meg a többrétegű heterogén alkalmazásokat biztosító külső alkalmazásfejlesztők problémáit. Nekik ugyanis továbbra is biztosítaniuk kell alkalmazásaik egyéni felhasználói nyilvántartásait.

Gyengeségeik ellenére több vállalat is ezen megközelítések valamelyike mellett döntött, mivel így is biztosítanak némi megkönnyebbülést a vázolt problémák kezelésében.

Az EIM megközelítése

Az EIM új megközelítése költséghatékony megoldást nyújt a több felhasználói nyilvántartással és felhasználói azonossággal rendelkező vállalatok számára. Az EIM egy olyan architektúra, amellyel leírhatók a vállalat egyéneinek vagy entitásainak (például fájlszerverek vagy nyomtatószerverek) illetve az ezek képviseletére használt számos azonosság közötti viszonyok. Emellett az EIM különféle alkalmazásprogram illesztőket is biztosít ezen viszonyok lekérdezéséhez.

Egy adott személynek az egyik felhasználói nyilvántartásban vett felhasználói azonossága alapján például meghatározhatja, hogy egy másik felhasználói nyilvántartás melyik felhasználói azonossága utal ugyanazon személyre. Ha a felhasználó hitelesítésre került az egyik felhasználói azonosság szerint, és le tudja képezni ezen felhasználói azonosságot egy másik felhasználói nyilvántartás megfelelő felhasználói azonosságára, akkor a felhasználónak a másik nyilvántartáshoz nem kell ismét hitelesítési információkat megadnia. A felhasználó már ismert, tehát csak azt kell tudni, hogy a különféle felhasználói nyilvántartások melyik felhasználói azonossága képviseli ezt a felhasználót. Ennek megfelelően az EIP általánosított azonosság leképezési funkciókat biztosít a vállalatok számára.

A felhasználói azonosságok különféle felhasználói nyilvántartások közötti leképezésének képessége számos előnnyel jár. Elsősorban azt jelenti, hogy az alkalmazások kihasználhatják annak rugalmasságát, hogy egy felhasználói nyilvántartást használnak hitelesítésre, és egy teljesen másikat a jogosultságok kezelésére. Egy adminisztrátor leképezhet egy SAP azonosságot (illetve az SAP magától is képes a leképezésre) SAP erőforrások elérése céljából.

Az azonosság leképezés használata a következőket követeli meg az adminisztrátoroktól:

1. A vállalat személyeit és entitásait képviselő EIP azonosítók létrehozása.
2. EIP nyilvántartási meghatározások létrehozása a vállalat meglévő felhasználói nyilvántartásainak leírásához.
3. Viszonyok meghatározása a nyilvántartások azonosságai és a létrehozott EIM azonosítók között.

A meglévő felhasználói nyilvántartásokon nem szükséges módosítani. Az adminisztrátornak nem kell a nyilvántartások valamennyi azonosságához leképezéseket megadnia. Az EIM lehetővé teszi 1-N (más szavakkal amikor egy felhasználó egy felhasználói nyilvántartásban egynél több azonossággal rendelkezik) leképezések megadását. Az EIM ezen kívül biztosítja N-1 leképezések megadását is (más szavakkal amikor több felhasználó osztja meg egy felhasználói nyilvántartás valamely azonosságát; ez bár támogatott, adminisztrációs okok miatt nem ajánlott). Az adminisztrátorok tetszőleges típusú tetszőleges felhasználói nyilvántartást ábrázolhatnak az EIM-ben.

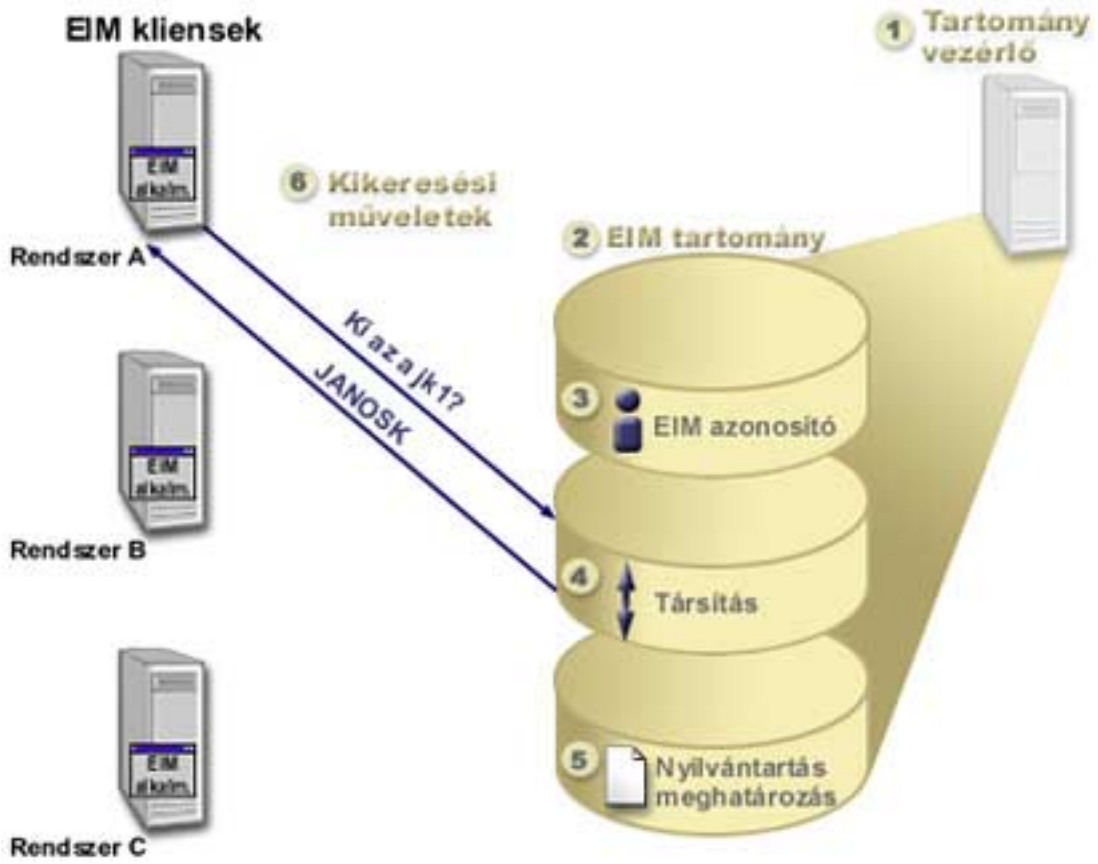
Az EIM nyílt architektúra, amellyel tetszőleges nyilvántartáshoz készíthető azonosság leképezés. Nem igényli a meglévő adatok új lerakatba másolását, hanem megpróbálja szinkronban tartani ezeket. Az EIM által bevezetett egyetlen új információ a viszony. Az adminisztrátorok ezt LDAP címtárban kezelhetik, amelynek rugalmassága lehetővé teszi az adatok egy helyben kezelését, és többszörözését a megfelelő helyekre. Végül az EIM megadja a vállalatok és alkalmazásfejlesztők számára azt a rugalmasságot, amellyel mindenki könnyedén dolgozhat tetszőleges összetételű környezetben.

EIM alapelvek

Az EIM vállalaton belüli felhasználhatóságának megértéséhez meg kell ismerni az EIM alapelveit. Bár az EIM API-k konfigurációja és megvalósítása eltérő lehet a különféle szerver platformokon, az EIM alapelvei minden IBM @server platformon megegyeznek.

Az 1. Ábra bemutat egy EIM megvalósítási példát. Három szerver működik EIM kliensként, és ezeken EIM támogatással rendelkező alkalmazások futnak, amelyek az EIM adatokhoz EIM kikeresési műveletekkel 6 jutnak. A tartományvezérlő 1 tárolja az EIM tartományra 2 vonatkozó információkat; ez egy EIM azonosítóból 3 , az EIM azonosítók és felhasználói azonosságok társításaiból 4 , illetve az EIM nyilvántartás meghatározásaiból 5 áll.

1. ábra: EIM megvalósítási példa



Az EIM alapelvekről további információkat az alábbi témakörökből szerezhet:

- EIM tartományvezérlő
- EIM tartomány
- EIM azonosító
- EIM nyilvántartás meghatározások
- EIM társítások
- EIM kikeresési műveletek
- EIM jogosultságok

EIM tartományvezérlő

Az *EIM tartományvezérlő* egy Egyszerűsített címtárhozzáférési protokoll (LDAP) szerver, amely be van állítva legalább egy EIM tartomány kezelésére. Az *EIM tartomány* egy LDAP címtár, amely a tartományban meghatározott EIM azonosítókból, EIM társításokból és felhasználói nyilvántartásokból áll. A rendszerek (vagyis EIM kliensek) úgy vesznek részt a tartományban, hogy EIM kikeresési műveletekkel a tartomány adatait használják fel. A vállalatban lennie kell legalább egy EIM tartományvezérlőnek.

Jelenleg az IBM @server platformok csak egy része képes EIM tartományvezérlőként működni. Kliensként az EIM alkalmazásprogram illesztőket támogató tetszőleges rendszer része lehet a tartománynak. Ezek a kliens rendszerek az EIM API-k segítségével lépnek kapcsolatba a tartományvezérlővel EIM kikeresési műveletek végrehajtása érdekében.

Az EIM kliens helye határozza meg, hogy az EIM tartományvezérlő helyi vagy távoli rendszer-e. A tartományvezérlő akkor *helyi*, ha az EIM kliens a tartományvezérlővel megegyező rendszeren fut. Ha az EIM kliens a tartományvezérlőtől eltérő rendszeren fut, akkor a tartományvezérlő *távoli*.

EIM tartomány

Az *EIM tartomány* egy olyan LDAP címtár, amely a vállalat EIM adatait tartalmazza. Az EIM tartomány a tartományban meghatározott EIM azonosítókból, EIM társításokból és felhasználói nyilvántartásokból áll. A rendszerek (vagyis EIM kliensek) úgy vesznek részt a tartományban, hogy EIM kikeresési műveletekkel a tartomány adatait használják fel.

Az EIM tartományok nem felhasználói nyilvántartások. A felhasználói nyilvántartások felhasználói azonosságok olyan halmazát határozzák meg, amelyeket egy operációs rendszer egy adott példánya ismer, és amelyekben megbízik. A felhasználói nyilvántartás tartalmazza ezenkívül az azonosság felhasználójának hitelesítéséhez szükséges információkat is. Emellett a felhasználói nyilvántartások számos további jellemzőt is tartalmazhatnak, például felhasználói beállításokat, rendszer privilégiumokat vagy egyéb személyes információkat.

Ezzel ellentétben az EIM tartományok csak *hivatkoznak* a felhasználói nyilvántartásokban tárolt felhasználói azonosságokra. Az EIM tartományok a különféle felhasználói nyilvántartások azonosságai és az azonosságok által képviselt tényleges személyek vagy entitások közötti *viszonyokról* tartalmaznak információkat. Mivel az EIM csak viszonyinformációkkal foglalkozik, semmilyen szinkronizálás nem szükséges a felhasználói nyilvántartások és az EIM között.

A 2. ábra mutatja be az EIM tartományban tárolt adatokat. Ezek közé az EIM azonosítók, EIM nyilvántartás meghatározások és EIM társítások tartoznak. Az EIM adatok határozzák meg a felhasználói azonosságok és az azonosságok által a vállalatban képviselt személyek vagy entitások közötti viszonyokat.

2. ábra: Az EIM tartomány és a tartományban tárolt adatok

Az EIM adatok a következőket foglalják magukban:

- **EIM azonosítók.** Minden egyes EIM azonosító egy vállalaton belüli személyt vagy entitást (például nyomtatószervert vagy fájlszervert) képvisel. További információkat az EIM azonosító című témakörben talál.
- **EIM nyilvántartás meghatározások.** Minden EIM nyilvántartás meghatározás valamelyik vállalati rendszer tényleges felhasználói nyilvántartását képviseli (az itt tárolt felhasználó azonosság információkkal együtt). Az adott felhasználói nyilvántartás meghatározása után a felhasználói nyilvántartás részt vehet az EIM tartományban. További információkat az EIM nyilvántartás meghatározások című témakörben talál.
- **EIM társítások.** Minden egyes EIM társítás egy EIM azonosító és a hozzá tartozó személy vagy entitás közötti viszony. A társításokat az EIM tartományban részt vevő felhasználói nyilvántartások azonosságai számára kell létrehozni. A társítások biztosítják azokat az információkat, amelyek az EIM azonosítókat egy adott felhasználói nyilvántartás egy adott felhasználói azonosságához társítják. Ennek következtében a társításokat oly módon kell meghatározni, hogy az EIM kliensek az EIM API-k segítségével sikeres EIM kikeresési műveleteket hajthatnak végre. Ezek az EIM kikeresési műveletek keresik meg az EIM tartományokban az EIM azonosítók és az ismert felhasználói nyilvántartásokban szereplő azonosságok és az EIM azonosítók közötti társításokat. További információkat az EIM kikeresési műveletek című témakörben talál.

Az EIM azonosítók, nyilvántartás meghatározások és társítások létrehozása után az EIM segítségével könnyebben tarthatja kézben és kezelheti a vállalat felhasználói azonosságait.

EIM azonosító

EIM azonosítók képviselik a vállalat személyeit és entitásait. Egy tipikus hálózat különféle hardverplatformokból és alkalmazásokból, illetve ezek felhasználói nyilvántartásaiból áll. A legtöbb platform, és az alkalmazások jelentős része platformra jellemző vagy alkalmazásra jellemző felhasználói nyilvántartást használ. Ezek a felhasználói nyilvántartások tartalmazzák a szervereket vagy alkalmazásokat használó személyek összes azonosítási információját.

Az EIM azonosítók létrehozásával, illetve ennek különféle felhasználói azonosságokhoz rendelésével egyszerűbbé válik a heterogén, többrétegű alkalmazások, például egy egyszeri bejelentkezéses környezet összeállítása. EIM azonosítók és társítások létrehozásakor egyszerűbbé válik a vállalat személyeihez vagy entitásaihoz kötődő felhasználói azonosságok kezelésével járó adminisztráció.

Személyt képviselő EIM azonosító

A 3. ábra példaként bemutatja egy *Kovács János* nevű személy EIM azonosítóját, és a vállalaton belüli többféle felhasználói azonosságát. A példában *Kovács János* négy különböző felhasználói nyilvántartásban négy felhasználói azonossággal rendelkezik: kovacsjanos, jk1, JANOSK és JKovacs.

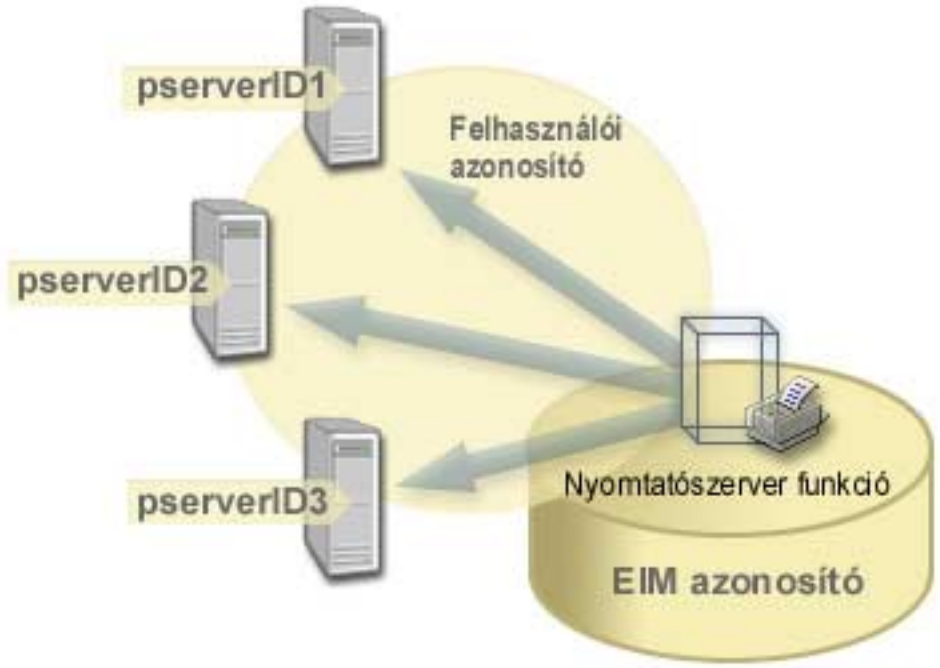
3. ábra: *Kovács János* EIM azonosítója és különféle felhasználói azonosságai közötti viszony.

Az EIM segítségével létrehozhat olyan társításokat, amelyek meghatározzák a Kovács János azonosító, és *Kovács János* valamennyi felhasználói azonossága közötti viszonyokat. A viszonyokat meghatározó társítások létrehozásával lehetőség van olyan alkalmazások írására, amelyek az EIM API-k felhasználásával keresnek ki szükséges, ámde ismeretlen felhasználói azonosságokat egy ismert felhasználói azonosság alapján.

Entitást képviselő EIM azonosító

Felhasználók mellett az EIM azonosítók entitásokat is képviselhetnek a vállalaton belül, amint az a 4. ábrán látható is. A vállalati nyomtatószerver funkció például gyakran több rendszeren fut. A 4. ábrán látható módon a vállalati nyomtatószerver funkció három különböző rendszeren fut három különböző felhasználói azonosság (pserverID1, pserverID2 és pserverID3) alatt.

4. ábra: A nyomtatószerver funkciót képviselő EIM azonosság és a funkció különféle felhasználói azonosságai közötti viszony.



Az EIM segítségével létrehozhat olyan egyedülálló azonosítót, amely a teljes vállalaton belül képviseli a nyomtatószerver funkciót. A példában a nyomtatószerver funkció EIM azonosító a tényleges vállalati nyomtatószerver funkciót képviseli. Az EIM azonosító (nyomtatószerver funkció) és a funkció különféle felhasználói azonosságai (pserverID1, pserverID2 és pserverID3) közötti viszonyok meghatározására társításokat kell létrehozni. Ezek a társítások lehetővé teszik az alkalmazásfejlesztőknek, hogy egy adott nyomtatószerver funkciót EIM kikeresési művelettel keressenek meg. Az alkalmazás szolgáltatók olyan osztott alkalmazásokat írhatnak, amelyek egyszerűbben kezelik a nyomtatószerver funkciót a teljes vállalaton belül.

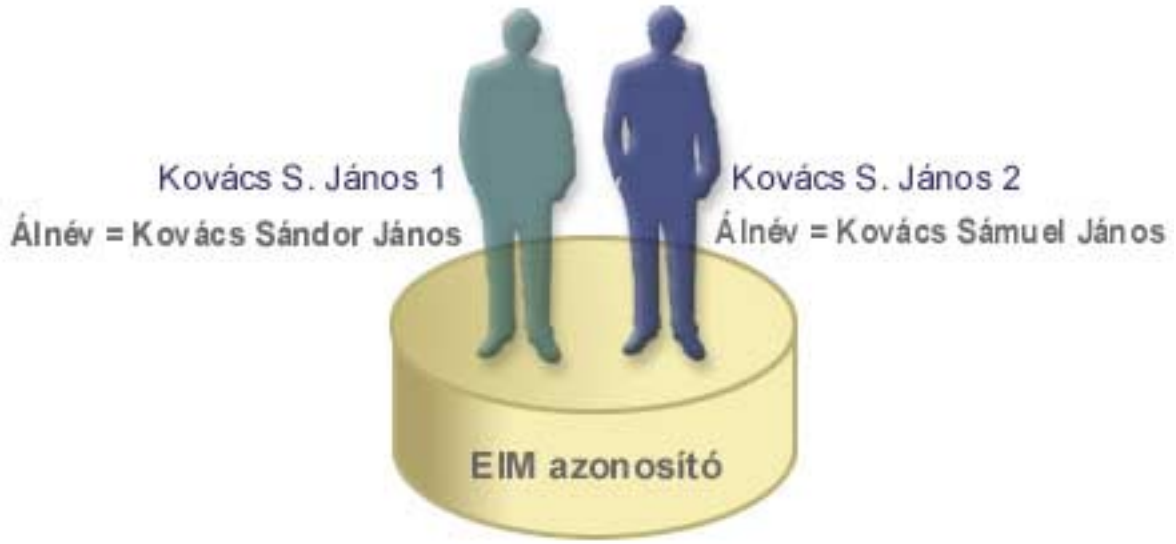
EIM azonosítók és álnevek

Az EIM azonosítókhoz álnevek is létrehozhatók. Az álnevek segítséget nyújthatnak egy adott EIM azonosítók keresésekor az EIM kikeresés műveletek során. Az álnevek például hasznosak lehetnek az olyan helyzetekben, amikor valakinek a hivatalos neve eltér attól a névtől, amelyen a személyt ismerik.

Az EIM azonosítók neveinek egyedinek kell lenniük az EIM tartományban. Az álnevek segítségével megoldhatók az olyan helyzetek is, amikor egyedi azonosítónevek használata nehéz lehet. Elképzelhető például, hogy a vállalatnál több azonos nevű személy dolgozik, amely zavaró lehet, ha hivatalos neveket használ EIM azonosítóként.

Az 5. ábra bemutat egy példát, amelyben a vállalatnál két *Kovács S. János* van. Az EIM adminisztrátor két különböző EIM azonosítót hoz létre, hogy különbséget lehessen tenni közöttük: Kovács S. János1 és Kovács S János2. Az viszont, hogy melyik azonosító melyik *Kovács S. Jánost* ábrázolja, nem feltétlenül nyilvánvaló.

5. ábra: Álnevek két EIM azonosítóhoz a közös *Kovács S. János* név alapján.



Álnevek használatával az EIM adminisztrátor további információkat biztosíthat az EIM azonosítóhoz tartozó egyénekről. Ezek az információk felhasználhatók EIM kikeresés során is az azonosító által képviselt felhasználók megkülönböztetéséhez. Kovács S. János1 álneve lehet például Kovács Sándor János, Kovács S. János2 álneve pedig Kovács Sámuel János.

Minden egyes EIM azonosító rendelkezhet több álnévvel is, amelyek azonosíthatják, hogy az EIM azonosító melyik *Kovács S. Jánost* képviseli. Az EIM adminisztrátor hozzáadhat egy másik álnevet mindkét személy EIM azonosítójához, amely még inkább megkülönböztetheti őket. A további álnevek tartalmazhatják például a felhasználók dolgozói kódját, osztályát, munkakörét vagy bármely más megkülönböztető jellemzőt.

EIM nyilvántartás meghatározások

Az *EIM nyilvántartás meghatározások* a vállalat valamely rendszerének tényleges felhasználói nyilvántartását képviselik. A felhasználói nyilvántartás egy címtárhoz hasonlóan működik, és egy adott rendszer vagy alkalmazás érvényes felhasználói azonosságainak listáját tartalmazza. Egy alapszintű felhasználói nyilvántartás felhasználói azonosságokat és jelszavakat tartalmaz. Felhasználói nyilvántartás például a z/OS biztonság szerver Resource Access Control Facility (RACF$^{(R)}$) nyilvántartása. A felhasználói nyilvántartások emellett más információkat is tartalmazhatnak. Egy Egyszerűsített címtárhozzáférési protokoll (LDAP) címtár például megkülönböztetett neveket, jelszavakat és hozzáférés felügyeleti adatokat tartalmaz. Általános felhasználói nyilvántartás ezen kívül például a Kerberos kulcselosztó központ (KDC) és az OS/400 felhasználói profil nyilvántartása.

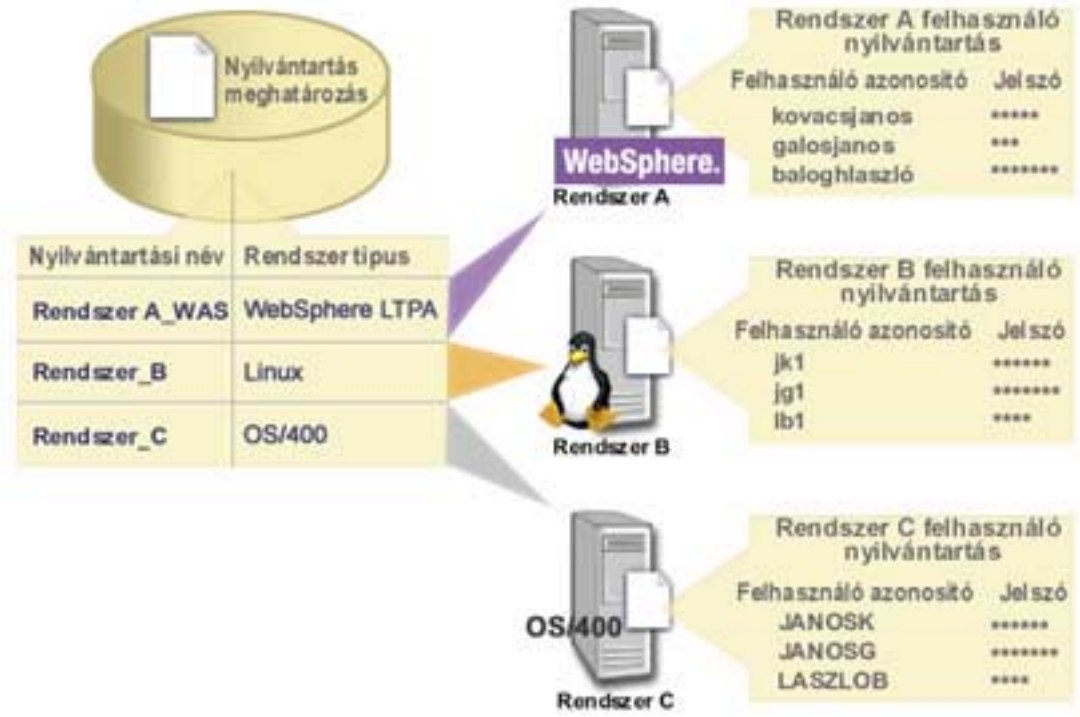
Az EIM nyilvántartás meghatározások biztosítják a vállalati felhasználói nyilvántartásokra vonatkozó információkat. Az adminisztrátor ezeket a nyilvántartásokat a következő információk megadásával határozza meg:

- Az EIM nyilvántartás tetszőleges, de egyedi neve
- A felhasználói nyilvántartás típusa

Minden egyes nyilvántartás meghatározás egy felhasználói nyilvántartás egy adott példányát képviseli. Ennek megfelelően az EIM nyilvántartás meghatározásnak olyan nevet kell választani, amely alapján azonosítani tudja az adott felhasználói nyilvántartást. Rendszer felhasználói nyilvántartás esetén jó választás például a rendszer TCP/IP hosztneve, vagy egy alkalmazás esetén a hosztnév és az alkalmazásnév kombinációja. Az EIM nyilvántartás meghatározások neveiben kis- és nagybetűs alfanumerikus karakterek illetve szóközök használhatók.

A 6. ábrán az adminisztrátor létrehozott egy EIM nyilvántartás meghatározást az A, B és C rendszerhez. Az A rendszer tartalmazza például a WebSphere Egyszerűsített külső hitelesítés (LTPA) felhasználói nyilvántartást. Az adminisztrátor által használt nyilvántartás meghatározás név segít azonosítani egy felhasználói nyilvántartás típus adott előfordulását. A felhasználói nyilvántartások nagy részénél egy IP cím vagy hosztnév például általában elegendő. Ebben a példában az adminisztrátor az adott felhasználói nyilvántartás példányt a Rendszer_A_WAS névvel azonosítja. A név mellett az adminisztrátor megadja a nyilvántartás típusát is, ami WebSphere LTPA.

6. ábra: EIM nyilvántartás meghatározások három felhasználói nyilvántartáshoz



Meghatározhatók már felhasználói nyilvántartásokon belül található felhasználói nyilvántartások is. Ilyen például a z/OS biztonság szerver (RACF) nyilvántartás, amely tartalmazhat olyan felhasználói nyilvántartásokat, amelyek a teljes RACF nyilvántartás részét képezik. Ennek működéséről a Rendszer és alkalmazás nyilvántartás meghatározások című témakörben találhat egy részletesebb példát.

EIM nyilvántartás meghatározások és álnevek

Az EIM nyilvántartás meghatározások számára is létrehozhat álneveket. Ezek lehetnek előre meghatározott álnévtípusok, de meghatározhatók saját álnévtípusok is. Előre meghatározott álnévtípusok például a következők:

- Tartománynév rendszer (DNS) hosztnév
- Kerberos tartomány
- Kibocsátó megkülönböztetett név (DN)
- Gyökér megkülönböztetett név (DN)
- TCP/IP cím
- LDAP DNS hosztnév

Az álnév támogatás segítségével a programozók úgy is megírhatnak alkalmazásokat, hogy előzőleg ne kelljen ismerniük az alkalmazást bevezető adminisztrátor által alkalmazott EIM nyilvántartásneveket. Az alkalmazás dokumentációja megadhatja az adminisztrátornak az alkalmazás által használt álnevet. Ez

alapján az EIM adminisztrátor hozzárendelheti a tényleges felhasználói nyilvántartást képviselő EIM nyilvántartás meghatározáshoz az alkalmazás által használt álnevet.

Amikor az adminisztrátor hozzáad egy álnevet az EIM nyilvántartás meghatározáshoz, akkor az alkalmazás egy álnév kikereséssel határozhatja meg az EIM nyilvántartás nevét. Az alkalmazás az álnév kikeresés segítségével határozhatja meg az EIM kikeresési műveletekben alkalmazandó EIM nyilvántartásnevet vagy neveket.

Rendszer és alkalmazás nyilvántartás meghatározások

Bizonyos alkalmazások egy felhasználói nyilvántartás részhalmazát képező felhasználói nyilvántartásokat használnak. Az EIM kétféle EIM nyilvántartás meghatározási típust biztosít ennek megvalósításához, az egyik a rendszer, a másik az alkalmazás.

A **rendszer nyilvántartás meghatározás** egy munkaállomás vagy szerver különálló nyilvántartását jelképezi. Rendszer nyilvántartás meghatározás abban az esetben hozható létre, ha a vállalati nyilvántartásra teljesül a következő feltételek valamelyike:

- A nyilvántartást egy operációs rendszer, például AIX(R) vagy OS/400(R), vagy egy biztonság felügyeleti termék, például egy z/OS biztonsági szerver Resource Access Control Facility (RACF(R)) biztosítja.
- A nyilvántartás egy adott alkalmazásra vonatkozóan (például Lotus Notes(R)) egyedi felhasználói azonosságokat tartalmaz.
- A nyilvántartás osztott felhasználói azonosságokat, például Kerberos azonosítókat vagy Egyszerűsített címtárhozzáférési protokoll (LDAP) megkülönböztetett neveket tartalmaz.

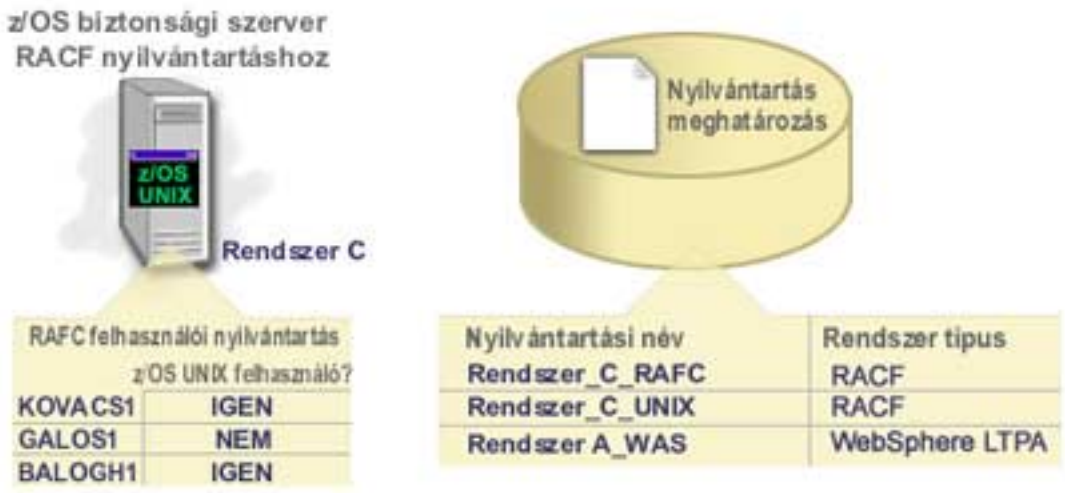
Az **alkalmazás nyilvántartás meghatározás** egy rendszer nyilvántartásban meghatározott felhasználói azonosságok egy részhalmazát képviseli. Ezek a felhasználói azonosságok közös attribútumokkal vagy jellemzőkkel rendelkeznek, amelyek lehetővé teszik számukra egy adott alkalmazás vagy alkalmazáscsoport használatát. Alkalmazás nyilvántartás meghatározás abban az esetben hozható létre, ha a felhasználói azonosságokra teljesülnek a következők:

- Az alkalmazás vagy alkalmazáscsoport felhasználói azonosságai nem az alkalmazásra vagy alkalmazáscsoportra jellemző felhasználói nyilvántartásban vannak.
- Az alkalmazás vagy alkalmazáscsoport felhasználói azonosságai olyan rendszer nyilvántartásban találhatók, amely más alkalmazások felhasználói azonosságait is tárolja.

Az EIM kikeresési műveletek a nyilvántartás típusától függetlenül helyesen le fognak futni. Ettől függetlenül az önálló nyilvántartás meghatározások lehetővé teszik az adatok alkalmazásonkénti leképezését. Az alkalmazásra jellemző leképezések kezelésének felelőssége rábízható az adott nyilvántartás adminisztrátorára.

A 7. ábra bemutatja, hogyan hozott létre egy EIM adminisztrátor egy rendszer nyilvántartás meghatározást egy z/OS biztonsági szerver RACF nyilvántartáshoz. Az adminisztrátor emellett létrehozott egy alkalmazás nyilvántartás meghatározást is, amely a RACF nyilvántartásnak a z/OS UNIX rendszerszolgáltatásokat (z/OS UNIX) használó felhasználói azonosságokat képviseli. A C rendszeren egy olyan RACF felhasználói nyilvántartás található, amely három felhasználói azonosságról (KOVACS1, GALOS1 és BALOGH1) tartalmaz információkat. A felhasználói azonosságok közül kettő (KOVACS1 és BALOGH1) használja a z/OS UNIX szolgáltatást a C rendszeren. Ezek valójában RACF felhasználók, csak egyedi attribútumaik azonosítják őket z/OS UNIX felhasználóként. Az EIM nyilvántartás meghatározásokon belül az EIM adminisztrátor beállított egy Rendszer_C_RACF meghatározást, amely a teljes RACF felhasználói nyilvántartást képviseli. Emellett beállított egy Rendszer_C_UNIX meghatározást is a z/OS UNIX attribútumokkal rendelkező felhasználói azonosságok számára.

7. ábra: EIM nyilvántartás meghatározások a RACF felhasználói nyilvántartás és a z/OS UNIX számára



EIM társítások

Az *EIM társítások* egy adott személyt képviselő EIM azonosító és egy felhasználói nyilvántartás ugyanazon személyére utaló felhasználói azonossága között meghatározott viszonyok. Amikor létrehozza egy EIM azonosító, és az adott személy vagy entitás összes felhasználói azonossága közötti társításokat, akkor összefoglaló és teljes áttekintést biztosít arról, hogyan használja a kérdéses személy vagy entitás a vállalat erőforrásait. Az EIM által biztosított API-k lehetővé teszik az alkalmazásoknak, hogy egy (forrás) felhasználói nyilvántartás egy ismert felhasználói azonosságának megadásával megtalálják a felhasználót egy adott (cél) felhasználói nyilvántartásban. Ezt a folyamatot *azonosságleképezésnek* hívjuk.

Mielőtt lehetőség lenne társítások létrehozására, létre kell hoznia a megfelelő EIM azonosítót és a társított felhasználói azonosságot tartalmazó felhasználói nyilvántartás EIM nyilvántartás meghatározását. A társítások az EIM azonosítók és a felhasználói azonosságok között fennálló viszonyokat határozzák meg az alábbi információkkal:

- EIM azonosító neve
- Felhasználói azonosság neve
- EIM nyilvántartás meghatározás neve
- Társítás típusa

Az adminisztrátorok a felhasználói azonosság felhasználásától függően többféle társítást is létrehozhatnak egy EIM azonosító és a kapcsolódó felhasználói azonosságok között. A felhasználói azonosságok használhatók hitelesítéshez, felhatalmazáshoz vagy mindkettőhöz.

A *hitelesítés* az a folyamat, amelynek során a rendszer ellenőrzi, hogy a felhasználói azonosságot megadó entitás vagy személy felveheti-e az adott azonosságot. Az ellenőrzés általában úgy történik, hogy a felhasználói azonosságot megadó személynek meg kell adnia a felhasználói azonosságra vonatkozóan egy titkos vagy privát információt, például egy jelszót.

A *felhatalmazás* az a folyamat, amellyel a rendszer biztosítja, hogy egy megfelelően hitelesített felhasználói azonosság csak olyan funkciókat hajthat végre, illetve csak olyan erőforrásokhoz férhet hozzá, amelyre az azonosság jogosult. Korábban szinte minden alkalmazás egyetlen felhasználói nyilvántartást használt a felhasználói azonosságok hitelesítéséhez és felhatalmazásához. EIM kikeresési műveletek használatával az alkalmazásoknak lehetőségük van arra, hogy az egyik felhasználói nyilvántartás felhasználói azonosságai alapján végezzék a hitelesítést, míg a felhatalmazást egy másik nyilvántartás felhasználásával.

Az EIM háromféle társítást tesz lehetővé az EIM azonosítók és felhasználói azonosságok között. Ezek a forrás, cél és adminisztrációs társítások.

Forrás társítás

Egy felhasználói azonosság *hitelesítési* célú felhasználásához a felhasználói azonosságnak forrás társítással kell rendelkeznie egy EIM azonosítóhoz. A forrás társítás segítségével a felhasználói azonosság felhasználható EIM kikeresési művelet forrásaként, vagyis alapján azonos EIM azonosítóhoz tartozó másik felhasználói azonosság kereshető ki. Ha egy EIM kikeresési műveletben egy kizárólag forrás társítással rendelkező felhasználói azonosság kerül felhasználásra cél azonosságként, akkor a kikeresés nem jár eredménnyel.

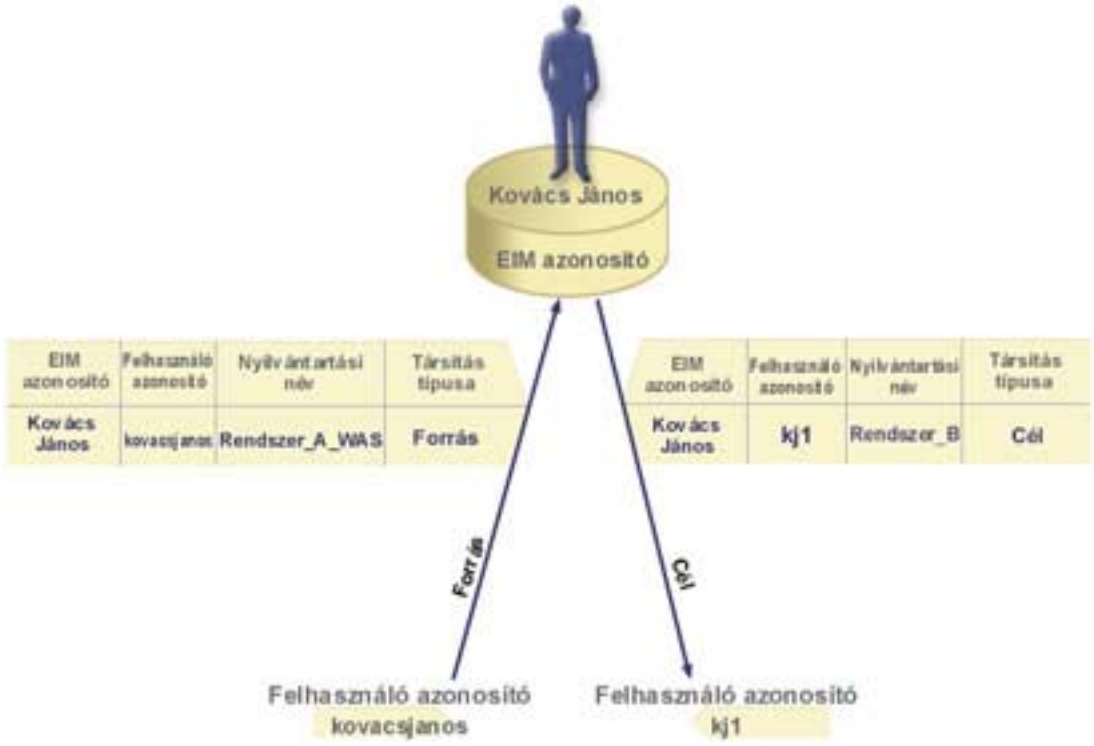
Cél társítás

Amikor egy felhasználói azonosság hitelesítés helyett *felhatalmazáshoz* kerül felhasználásra, akkor a felhasználói azonosságnak cél társítással kell rendelkeznie egy EIM azonosítóhoz. A cél társítás teszi lehetővé a felhasználói azonosság visszaadását egy EIM kikeresési művelet eredményeként. Ha egy EIM kikeresési műveletben egy kizárólag cél társítással rendelkező felhasználói azonosság kerül felhasználásra forrás azonosságként, akkor a kikeresés nem jár eredménnyel.

Elképzelhető, hogy egyetlen felhasználói azonosság esetén is szükség van mind cél mind forrás társítás létrehozására. Erre adminisztrátorként tevékenykedő személyek esetén, illetve még akkor van szükség, amikor valaki egy rendszert kliensként és szerverként is használ. Tegyük fel például, hogy egy felhasználó hitelesítése általában Windows platformon történik, és AIX szervert használó alkalmazásokat futtat. Munkaköri tevékenységek miatt a felhasználónak időnként közvetlenül is be kell jelentkeznie az AIX szerverre. Ebben az esetben a személy EIM azonosítója és az AIX felhasználói azonosság között forrás és cél társítást is létre kell hozni. A végfelhasználókat képviselő felhasználói azonosságoknak általában elegendő, ha csak cél társítással rendelkeznek.

A forrás és cél társításra a 6. ábra mutat be egy példát. A példában az adminisztrátor két társítást hozott létre a Kovács János EIM azonosítóhoz, így meghatározva az azonosító és két hozzá tartozó felhasználói azonosság közötti viszonyt. Az adminisztrátor forrás társítást hozott létre a kovacsjanos WebSphere LTPA felhasználói azonosság számára a Rendszer_A_WAS felhasználói nyilvántartásban. Az adminisztrátor létrehozott egy cél társítást is a kj1 OS/400 felhasználói profil számára a B rendszer felhasználói nyilvántartásában. Ezek a társítások lehetőséget adnak az alkalmazásoknak, hogy egy EIM kikeresési művelettel meghatározzanak egy ismeretlen felhasználói azonosságot (a kj1 cél) egy ismert felhasználói azonosság (a kovacsjanos cél) alapján.

6. ábra: A Kovács János EIM azonosítóhoz tartozó EIM cél és forrás társítások



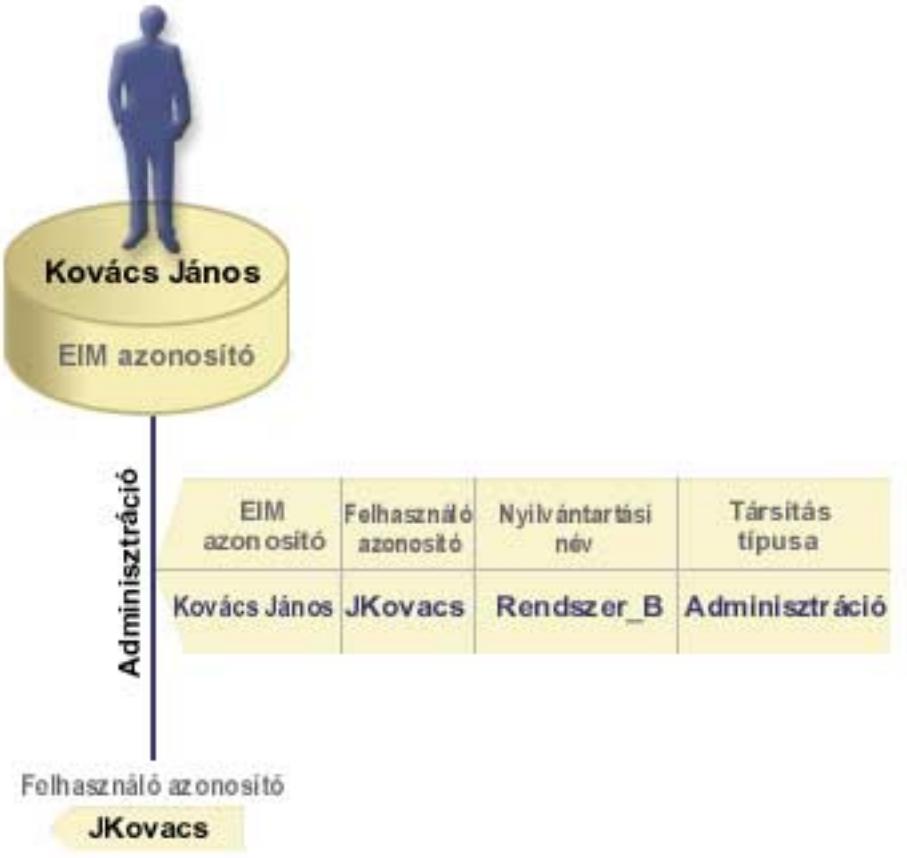
Adminisztrációs társítás

Az EIM azonosítók adminisztrációs társítása általában azt hivatott jelölni, hogy az EIM azonosító által képviselt személy vagy entitás a megadott rendszeren speciális szempontokat igénylő felhasználói azonosságot birtokol. Ez a fajta társítás használható például a rendkívül bizalmas felhasználói nyilvántartásokhoz.

Az adminisztrációs társítások természete miatt az adminisztrációs társítással rendelkező felhasználói azonosságok forrásként való meghatározása az EIM kikeresési műveletekben nem jár eredménnyel. Hasonlóan, adminisztrációs társítással rendelkező felhasználó azonosság sohasem kerül visszaadásra EIM kikeresés eredményeként.

Az adminisztrációs társításra a 7. ábra mutat be egy példát. A példában Kovács János rendelkezik egy azonossággal az A és B rendszeren is, amelyek közül ez utóbbi egy rendkívül biztonságos rendszer. A rendszeradminisztrátor biztosítani szeretné, hogy a B rendszer felé végzett hitelesítés csak a rendszer helyi felhasználói nyilvántartása alapján történjen. Az adminisztrátor nem szeretné, hogy egy alkalmazás idegen hitelesítési mechanizmus alapján hitelesítse Kovács Jánost a rendszeren. Ha a B rendszer JKovacs felhasználói azonosságához adminisztrációs társítást hoz létre, akkor az EIM adminisztrátor látja, hogy Kovács János rendelkezik fiókkal a B rendszeren, de az EIM a kikeresési műveletek során nem ad vissza információkat a JKovacs azonossággal kapcsolatban. Még ha a rendszeren EIM kikeresést használó alkalmazások is vannak, az adminisztrációs társításokkal rendelkező felhasználói azonosságokat nem találnák meg.

7. ábra: EIM adminisztrációs társítás a Kovács János EIM azonosítóhoz.



EIM kikeresési műveletek

Az *EIM kikeresési művelet* olyan folyamat, amellyel egy alkalmazás vagy operációs rendszer megkeres egy ismeretlen felhasználói azonosságot egy felhasználói nyilvántartásban valamely ismert és megbízható információ megadásával. Az alkalmazások csak akkor tudják az EIM API-k segítségével végrehajtani ezen kikeresést, ha az információk megtalálhatók az EIM tartományban. Az alkalmazások a kikeresési művelet forrásaként megadott információk (felhasználói azonosság vagy EIM azonosító) alapján kétféle EIM kikeresési műveletet hajthatnak végre.

Amikor egy alkalmazás *felhasználói azonosságot ad meg forrásként*, akkor az alkalmazásnak meg kell adnia a forrás felhasználói azonosság EIM nyilvántartás meghatározásának nevét, illetve az EIM kikeresési művelet célját jelentő EIM nyilvántartás meghatározás nevét. Ahhoz, hogy EIM kikeresés művelet forrásában szerepelhessen, a felhasználói azonosságnak rendelkeznie kell legalább egy forrás társítással.

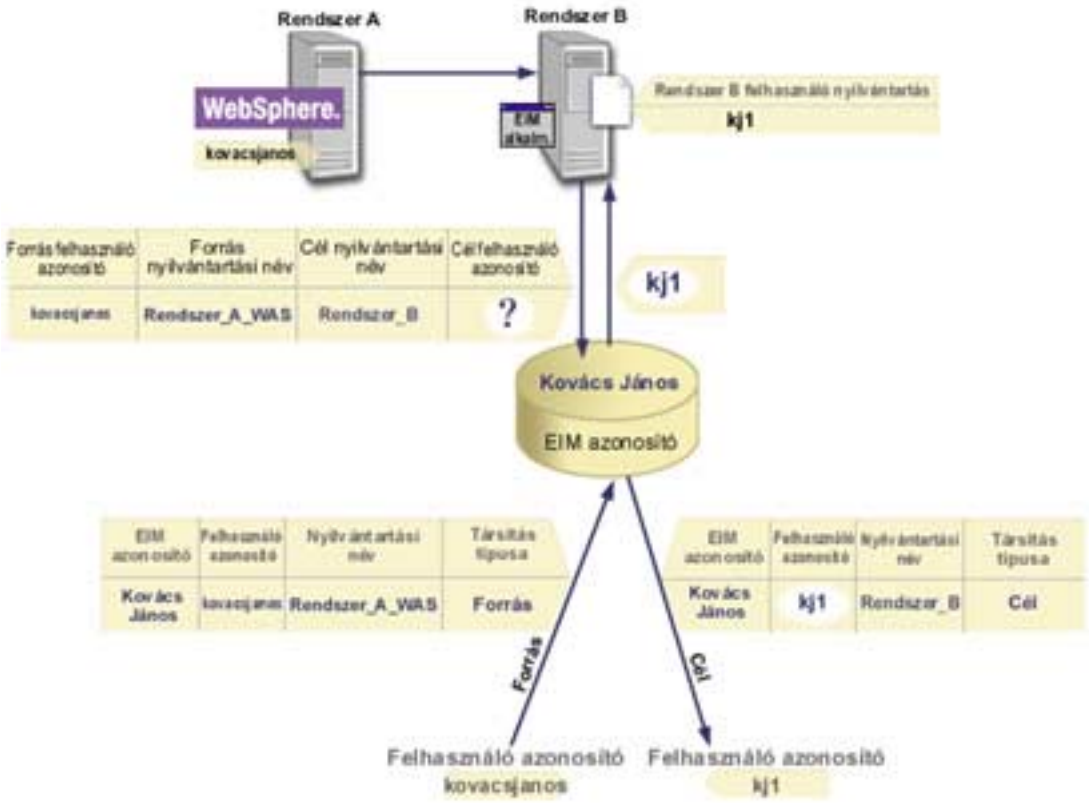
Amikor egy alkalmazás *EIM azonosítót ad meg forrásként*, akkor az alkalmazásnak meg kell adnia az EIM kikeresési művelet célját jelentő EIM nyilvántartás meghatározást. Ahhoz, hogy egy felhasználói azonosság visszaadható legyen bármelyik típusú kikeresés művelet eredményeként, az azonosságnak rendelkeznie kell cél társítással.

A megadott információk az EIM tartományvezérlőhöz kerülnek, ahol minden EIM információ megtalálható, és az EIM kikeresés megkeresi a megadott információknak megfelelő forrás társítást. Az (alkalmazásprogram illesztőnek átadott vagy a forrás társítás információkból meghatározott) EIM azonosító alapján az EIM kikeresés ezután megkeresi a cél EIM nyilvántartás meghatározás nevének megfelelő cél társítást.

A 10. ábrán a kovacsjanos felhasználói azonosság Egyszerűsített külső hitelesítés (LTPA) alapján kerül hitelesítésre az A rendszeren futó WebSphere alkalmazásszerveren. Az A rendszer WebSphere alkalmazásszervere meghív egy saját programot a B rendszeren a B rendszeren tárolt adatok eléréséhez. A

program az EIM API segítségével végrehajt egy EIM kikeresést az A rendszeren alkalmazott felhasználói azonosság alapján. Az alkalmazás a művelet végrehajtásához a következő információkat adja meg: a kovacsjanos forrás felhasználói azonosságot, a Rendszer_A_WAS forrás és a Rendszer_B cél EIM nyilvántartás meghatározás nevet. A forrásinformációk az EIM tartományvezérlőhöz kerülnek, az EIM kikeresési művelet pedig keres egy forrás társítást az információk alapján. Az EIM azonosító alapján az EIM kikeresés megkeresi a Kovács János azonosító cél társítását, amely megfelel a Rendszer_B cél EIM nyilvántartás meghatározás névnek. A megfelelő cél társítás megtalálásakor az EIM kikeresés a jk1 felhasználói azonosságot adja vissza az alkalmazásnak.

10. ábra: EIM kikeresési művelet az ismert kovacsjanos felhasználói azonosság alapján.



EIM jogosultságok

Az *EIM jogosultságok* engedélyezik a felhasználóknak a különféle adminisztrációs feladatok és EIM kikeresési műveletek végrehajtását. Csak az EIM adminisztrátori jogosultsággal rendelkező felhasználók adományozhatják és vonhatják vissza más felhasználók jogosultságait. EIM jogosultságok csak olyan felhasználói azonosságok számára adományozhatók, amelyek ismertek az EIM tartományvezérlőn.

Az egyes EIM jogosultsági csoportok által végrehajtható funkciók leírása a következő:

- **Egyszerűsített címtárhozzáférési protokoll (LDAP) adminisztrátor** Ezzel a jogosultsággal a felhasználó új EIM tartományt állíthat be. A jogosultsággal rendelkező felhasználók a következő műveleteket végezhetik el:
  - Tartomány létrehozása
  - Tartomány törlése
  - EIM azonosítók létrehozása és eltávolítása
  - EIM nyilvántartás meghatározások létrehozása és eltávolítása
  - Forrás, cél és adminisztrációs társítások létrehozása és eltávolítása

  - EIM kikeresési műveletek végrehajtása
  - Társítások, EIM azonosítók és EIM nyilvántartás meghatározások visszakeresése
  - EIM jogosultsági információk hozzáadása, eltávolítása és megjelenítése
- **EIM adminisztrátor** Ezzel a jogosultsággal a felhasználó az EIM tartomány összes EIM adatát kezelheti. A jogosultsággal rendelkező felhasználók a következő műveleteket végezhetik el:
  - Tartomány törlése
  - EIM azonosítók létrehozása és eltávolítása
  - EIM nyilvántartás meghatározások létrehozása és eltávolítása
  - Forrás, cél és adminisztrációs társítások létrehozása és eltávolítása
  - EIM kikeresési műveletek végrehajtása
  - Társítások, EIM azonosítók és EIM nyilvántartás meghatározások visszakeresése
  - EIM jogosultsági információk hozzáadása, eltávolítása és megjelenítése
- **EIM azonosító adminisztrátor** Ezzel a jogosultsággal a felhasználó hozzáadhat és módosíthat EIM azonosítókat, és kezelheti a forrás és adminisztrációs társításokat. A jogosultsággal rendelkező felhasználók a következő műveleteket végezhetik el:
  - EIM azonosító létrehozása
  - Forrás társítások hozzáadása és eltávolítása
  - Adminisztrációs társítások hozzáadása és eltávolítása
  - EIM kikeresési műveletek végrehajtása
  - Társítások, EIM azonosítók és EIM nyilvántartás meghatározások visszakeresése
- **EIM leképezés kikeresés** Ezzel a jogosultsággal a felhasználó EIM kikeresési műveleteket hajthat végre. A jogosultsággal rendelkező felhasználók a következő műveleteket végezhetik el:
  - EIM kikeresési műveletek végrehajtása
  - Társítások, EIM azonosítók és EIM nyilvántartás meghatározások visszakeresése
- **EIM nyilvántartás adminisztrátor** Ezzel a jogosultsággal a felhasználó az EIM összes nyilvántartás meghatározását kezelheti. A jogosultsággal rendelkező felhasználók a következő műveleteket végezhetik el:
  - Cél társítások hozzáadása és eltávolítása
  - EIM kikeresési műveletek végrehajtása
  - Társítások, EIM azonosítók és EIM nyilvántartás meghatározások visszakeresése
- **EIM X nyilvántartás adminisztrátor** Ezzel a jogosultsággal a felhasználó egy adott EIM nyilvántartás meghatározást kezelhet. A jogosultsággal rendelkező felhasználók a következő műveleteket végezhetik el:
  - Cél társítások hozzáadása és eltávolítása az EIM nyilvántartás meghatározásban
  - EIM kikeresési műveletek végrehajtása
  - Társítások, EIM azonosítók és EIM nyilvántartás meghatározások visszakeresése

Az alábbi táblázatok az API által végzett EIM feladat szerint vannak rendezve. Minden táblázatban megjelenik minden egyes EIM API, a különféle EIM jogosultságok, illetve ezen jogosultságoknak bizonyos EIM funkciók elérésére vonatkozó hozzáférése.

1. táblázat: Tartományok kezelése

EIM API	LDAP adminisztr.	EIM adminisztr.	EIM azonosító adminisztr.	EIM leképezés kikeresés	EIM nyilvántartás adminisztr.	EIM X nyilvántartás adminisztr.
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-

EIM API	LDAP adminisztr.	EIM adminisztr.	EIM azonosító adminisztr.	EIM leképezés kikeresés	EIM nyilvántartás adminisztr.	EIM X nyilvántartás adminisztr.
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

2. táblázat: Azonosítók kezelése

EIM API	LDAP adminisztr.	EIM adminisztr.	EIM azonosító adminisztr.	EIM leképezés kikeresés	EIM nyilvántartás adminisztr.	EIM X nyilvántartás adminisztr.
eimAddIdentifier	X	X	X	-	-	-
eimChangeIdentifier	X	X	X	-	-	-
eimListIdentifiers	X	X	X	X	X	X
eimRemoveIdentifier	X	X	-	-	-	-

3. táblázat: Nyilvántartások kezelése

EIM API	LDAP adminisztr.	EIM adminisztr.	EIM azonosító adminisztr.	EIM leképezés kikeresés	EIM nyilvántartás adminisztr.	EIM X nyilvántartás adminisztr.
eimAddApplicationRegistry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChangeRegistryUser	X	X	-	-	X	X
eimChgRegistryAlias	X	X	-	-	X	X
eimGetRegistryFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistryUsers	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

4. táblázat: Társítások kezelése

Az eimAddAssociation() és eimRemoveAssociation() API-k esetén négy paraméter határozza meg a hozzáadott vagy eltávolított társítás típusát. Az API-k használatára vonatkozó jogosultság a paraméterekben meghatározott társítástípustól függ. Az alábbi táblázatban ezen API-k esetén a társítás típusa is megjelenik.

EIM API	LDAP adminisztr.	EIM adminisztr.	EIM azonosító adminisztr.	EIM leképezés kikeresés	EIM nyilvántartás adminisztr.	EIM X nyilvántartás adminisztr.
eimAddAssociation (adminisztrációs)	X	X	X	-	-	-
eimAddAssociation (forrás)	X	X	X	-	-	-
eimAddAssociation (forrás és cél)	X	X	X	-	X	X
eimAddAssociation (cél)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (adminisztrációs)	X	X	X	-	-	-
eimRemoveAssociation (forrás)	X	X	X	-	-	-
eimRemoveAssociation (forrás és cél)	X	X	X	-	X	X
eimRemoveAssociation (cél)	X	X	-	-	X	X

5. táblázat: Leképezések kezelése

EIM API	LDAP adminisztr.	EIM adminisztr.	EIM azonosító adminisztr.	EIM leképezés kikeresés	EIM nyilvántartás adminisztr.	EIM X nyilvántartás adminisztr.
eimGetAssociatedIdentifier	X	X	X	X	X	X
eimGetTargetFromIdentifier	X	X	X	X	X	X
eimGetTargetFromSource	X	X	X	X	X	X

6. táblázat: Hozzáférés kezelése

EIM API	LDAP adminisztr.	EIM adminisztr.	EIM azonosító adminisztr.	EIM leképezés kikeresés	EIM nyilvántartás adminisztr.	EIM X nyilvántartás adminisztr.
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

EIM LDAP alapelvek

A Vállalati azonosság leképezés (EIM) egy Egyszerűsített címtárhozzáférési protokoll (LDAP) szervert használ EIM tartományvezérlőként az EIM adatok tárolására. Amikor az EIM szolgáltatást beállítja az iSeries szerveren, akkor ehhez, illetve az EIM tartományvezérlő hitelesítéséhez használhat LDAP megkülönböztetett neveket is.

Ha LDAP megkülönböztetett neveket kíván használni az EIM beállításakor és adminisztrálásakor, akkor tisztában kell lennie a következő témakörökben felvázolt LDAP alapfogalmakkal:

- LDAP megkülönböztetett nevek
- LDAP szülő megkülönböztetett nevek

LDAP megkülönböztetett név

Az LDAP megkülönböztetett nevek Egyszerűsített címtárhozzáférési protokoll (LDAP) bejegyzések egy LDAP szerver hitelesített felhasználóinak azonosítására és leírására. Az EIM tartomány információkat tároló LDAP szerver beállításához az EIM konfigurációs varázsló nyújt segítséget. Az LDAP megkülönböztetett nevek segítségével érhetők el és kereshetők ezek az EIM adatok, így az iSeries szerver is részt vehet egyszeri bejelentkezéses környezetben.

A megkülönböztetett nevek a bejegyzés nevéből, illetve az LDAP címtárban az objektum felett található bejegyzések nevéből állnak. Egy teljes LDAP megkülönböztetett név például a cn=Kovács János, o=IBM, c=US. Minden egyes bejegyzés rendelkezik legalább egy attribútummal a bejegyzés nevéhez. Ez az elnevezési attribútum a bejegyzés relatív megkülönböztetett neve (RDN). Egy adott RDN feletti bejegyzést nevezzük LDAP szülő megkülönböztetett névnek. A példában a bejegyzést a cn=Kovács János nevezi meg, így ez az RDN. A cn=Kovács János szülő megkülönböztetett neve az o=IBM, c=US. Az EIM általi felhasználásról további részleteket az LDAP szülő megkülönböztetett név című témakörből tudhat meg.

Mivel az EIM LDAP szerveren tárolja az EIM adatokat, az EIM tartományvezérlő hitelesítés alapjául LDAP megkülönböztetett neveket is használhat. LDAP megkülönböztetett nevek az iSeries szerver EIM funkciójának beállításakor is használhatók. LDAP megkülönböztetett nevek például a következő esetekben használhatók:

- LDAP szerver beállítása EIM tartományvezérlőként. Ehhez létre kell hoznia az LDAP adminisztrátort azonosító LDAP megkülönböztetett nevet az LDAP szerveren. Ha az LDAP szerver még nem került beállításra, akkor az LDAP szerver az EIM konfigurációs varázsló végrehajtása során is beállítható egy új tartomány létrehozásakor.
- Az EIM konfigurációs varázsló használata a varázsló által az EIM tartományvezérlőre csatlakozáshoz használt felhasználói azonosság típusának kiválasztásához. A megkülönböztetett név az egyik kiválasztható felhasználótípus. Az LDAP megkülönböztetett névnek azt a felhasználót kell képviselnie, aki jogosult az LDAP szerver helyi névterében objektumok létrehozására.
- Az EIM konfigurációs varázsló használata az operációs rendszer funkciók által végrehajtott EIM műveletekhez használt felhasználó típusának meghatározásához. Ilyen művelet például a leképezések kikeresése és a társítások törlése egy helyi OS/400 felhasználói profil törlésekor. A megkülönböztetett név az egyik kiválasztható felhasználótípus.
- Csatlakozás egy tartományvezérlőhöz EIM adminisztrációs feladatok elvégzése, például nyilvántartások és azonosítók kezelése vagy kikeresési műveletek végrehajtása céljából.

A megkülönböztetett nevekről és ezek felhasználásáról az LDAP alapok című témakörben olvashat.

LDAP szülő megkülönböztetett név

Az LDAP megkülönböztetett név egy Egyszerűsített címtárhozzáférési protokoll (LDAP) címtár szerver névterének egy bejegyzése. Az LDAP szerver bejegyzései hierarchikus szervezésűek, amely hierarchia ábrázolhat politikai, földrajzi, szervezeti vagy tartomány határokat. Egy megkülönböztetett név akkor minősül szülő megkülönböztetett névnek, ha az az LDAP szerver névterének legfelső szintjén van.

Egy teljes LDAP megkülönböztetett név például a cn=Kovács János, o=IBM, c=US. Minden egyes bejegyzés rendelkezik legalább egy attribútummal a bejegyzés nevéhez. Ez az elnevezési attribútum a bejegyzés relatív megkülönböztetett neve (RDN). Egy adott RDN feletti bejegyzést nevezzük szülő megkülönböztetett névnek. A példában a bejegyzést a cn=Kovács János nevezi meg, így ez az RDN. A cn=Kovács János szülő megkülönböztetett neve az o=IBM, c=US.

Mivel az EIM LDAP szerveren tárolja az EIM adatokat, az EIM tartományvezérlő hitelesítés alapjául LDAP megkülönböztetett neveket is használhat. LDAP megkülönböztetett neveket és szülő megkülönböztetett neveket az iSeries szerver EIM funkciójának beállításakor is használhat. Amikor például az EIM konfigurációs varázslóban létrehoz egy új tartományt és csatlakozik hozzá, akkor kiválaszthatja a létrehozni kívánt tartomány szülő megkülönböztetett nevét. A szülő megkülönböztetett név használatával megadhatja, hogy az EIM tartományra vonatkozó adatok a helyi LDAP névtér mely részébe kerüljenek. Ha nem ad nem szülő megkülönböztetett nevet, akkor az EIM adatok saját utótagjuknak megfelelő helyre kerülnek a névtérben.

A megkülönböztetett nevekről az LDAP alapok című témakörben olvashat.

Egyszeri bejelentkezés kialakítása

Az EIM költséghatékony mechanizmust biztosít a vállalati egyszeri bejelentkezési környezet megvalósításához. Az EIM és Kerberos OS/400 megvalósítása valódi többrétegű, heterogén egyszeri bejelentkezési környezetet biztosít. Az egyszeri bejelentkezést alkalmazó környezetek a következő előnyökkel járnak a felhasználók, adminisztrátorok és alkalmazásfejlesztők számára:

Felhasználói előnyök
Egyszeri bejelentkezést alkalmazó környezetben a hitelesítés minden új rendszer elérésére tett kísérlet során bekövetkezik, a felhasználóknak azonban ehhez nem kell jelszót beírniuk. Az EIM segítségével a felhasználóknak nem kell külön figyelmet szentelniük számos felhasználói név és jelszó követéséhez a hálózat más rendszereinek használatához. Miután egy felhasználó hitelesítette magát a hálózaton, a teljes vállalat szolgáltatásait és alkalmazásait használhatja anélkül, hogy a különböző rendszereken újabb és újabb jelszavakat kelljen megadnia.

Adminisztrátori előnyök
Az adminisztrátorok esetén az egyszeri bejelentkezés leegyszerűsíti a vállalat átfogó biztonsági felügyeletét. Egyszeri bejelentkezés hiányában a felhasználók és alkalmazások tárolhatják különféle rendszerek jelszavait, amely a teljes hálózat biztonságát veszélyeztetheti. Az adminisztrátoroknak ilyenkor jóval több időt kell szánniuk a biztonsági kockázatok megszüntetésére. Az egyszeri bejelentkezés csökkenti az adminisztrátorok terheit, és a hálózati biztonságot is javítja. Emellett az egyszeri bejelentkezés csökkenti az elfelejtett jelszavak alaphelyzetbe állításával kapcsolatos kérések számát.

Alkalmazásfejlesztői előnyök
A heterogén hálózatban futó alkalmazások fejlesztői számára az EIM olyan infrastruktúrát biztosít, amelyre alapozva tetszőleges platformon futó alkalmazások fejleszthetők. Az EIM API-k felhasználásával a programozók olyan alkalmazásokat írhatnak, amelyek a legmegfelelőbb felhasználói nyilvántartást használják a hitelesítésre, és egy másikat a felhatalmazásra. Az alkalmazásfejlesztőknek nem kell támogatniuk a platformfüggő felhasználói nyilvántartásokat az alkalmazásban, mivel az EIM infrastruktúrája lehetővé teszi az ilyen felhasználói nyilvántartásokban lévő felhasználói azonosságok egyetlen EIM azonosítóra képezését. Emellett az EIM lehetővé teszi a programozóknak, hogy az alkalmazásokat a biztonsági környezet módosítása nélkül tartsák karban, így az alkalmazásszintű biztonság jelentősen csökkenti a többrétegű keresztplatformos alkalmazások fejlesztési költségeit.

Az iSeries egyszeri bejelentkezés támogatása
Az egyszeri bejelentkezés megvalósításához az IBM két együttműködő technológiát biztosít, az egyik az EIM, a másik a Hálózati hitelesítési szolgáltatás, amely a Kerberos és GSS API-k IBM megvalósítása. Az adminisztrátorok ezen két technológia beállításával hozhatnak létre egyszeri bejelentkezést alkalmazó környezetet. A Windows 2000/XP, AIX és zSeries rendszerek a Kerberos protokollal hitelesítik a hálózati felhasználókat. A Kerberos egy hálózaton működő biztonságos kulcselosztó központ használatán alapul, amely hitelesíti az azonosítókat (Kerberos felhasználók) a hálózat felé. A felhasználó egy Kerberos jegyet kap a kulcselosztó központtól. Ez a jegy jogosítja fel a felhasználót a vállalat más szolgáltatásainak használatára. A jegyet a felhasználó átadhatja egy olyan szolgáltatásnak, amely elfogad jegyeket. A jegyet

elfogadó szolgáltatás a jegy alapján határozza meg, hogy ki a felhasználó (a Kerberos felhasználói nyilvántartásban és tartományban), és valóban az-e, akinek vallja magát.

Míg a Hálózati hitelesítési szolgáltatás lehetővé teszi az iSeries szervereknek, hogy Kerberos tartomány tagjai legyenek, az EIM mechanizmusa biztosítja a Kerberos azonosítóknak a vállalati felhasználókat képviselő EIM azonosítókra való leképezését. Ezzel az EIM azonosítóval más azonosságok, például OS/400 felhasználói profilok is társíthatók. Ezen társításokra épülve az EIM lehetővé teszi az OS/400 és az alkalmazások számára, hogy megállapítsák a Kerberos azonosító által képviselt személyhez tartozó OS/400 felhasználói profil nevét. Az EIM információkat leginkább egy olyan faként lehet elképzelni, amelynek gyökere egy EIM azonosító, az ezzel társított felhasználói azonosságok pedig az ágak.

Az alábbi ábrát tekintve tegyük fel, hogy egy Kiss István nevű felhasználó bejelentkezik a hálózatra windowsos számítógépén, és egy OS/400 rendszeren Kerberos támogatással rendelkező alkalmazásokat használ. Istvánnak ehhez nem kell megadnia OS/400 felhasználói nevét. Az alkalmazások ki tudják keresni István EIM azonosítóját az OS/400 felhasználónév megkereséséhez. Az OS/400 felhasználói profilhoz a továbbiakban nincs is szükség jelszóra, hiszen nem hitelesítési, hanem csak felhatalmazási célokat szolgál.

1. ábra: Egyszeri bejelentkezést biztosító környezet

A Példahelyzet: Egyszeri bejelentkezés engedélyezése című témakörben talál egy példát arról, hogyan állíthatja be az adminisztrátor a Hálózati hitelesítési szolgáltatást és az EIM támogatást egyszeri bejelentkezést biztosító környezet megvalósításához.

Egyszeri bejelentkezéssel az alábbi alkalmazások érhetők el:

- iSeries navigátor
- PC5250 emulátor
- Distributed Relational Database Architecture (TM)(DRDA)(R)
- Hálózati szerver
- QFileSvr.400

EIM tervezése

Az EIM számos technológiát és szolgáltatást magában foglal az iSeries szerveren. Mielőtt beállítná az EIM támogatást a szerveren, el kell döntenie, hogy milyen funkcionalitást kíván megvalósítani az EIM és az egyszeri bejelentkezés segítségével.

Az EIM beállításának megkezdése előtt döntésre kell jutnia a hálózat alapszintű biztonsági követelményeit illetően, és meg kell valósítani ezen biztonsági intézkedéseket. Az EIM egyszerűbb azonosságkezelést tesz lehetővé az adminisztrátorok és felhasználók számára is a teljes vállalatra vonatkozóan. A Hálózati hitelesítési szolgáltatással használva az EIM egyszeri bejelentkezést tesz lehetővé a vállalaton belül.

Az EIM beállítása előtt telepítendő szolgáltatásokat a következő tervezési munkalap foglalja össze.

Tervezési munkalap	Válaszok
Az OS/400 (5722-SS1) kiadása V5R2 vagy újabb?	
A Cryptographic Access Provider (5722-AC3) termék telepítve van az iSeries szervereken?	
Telepítve van az iSeries Access for Windows (5722-XE1) a hálózat megfelelő számítógépein és iSeries szerverein?	
Telepítve van az iSeries navigátor Hálózat részösszetevője a hálózatban található számítógépeken és iSeries rendszereken?	
Ha van beállított LDAP szerver, amelyet EIM tartományvezérlőként szeretne felhasználni, akkor ismeri az LDAP adminisztrátor megkülönböztetett nevét és jelszavát?	
Ha van beállított LDAP szerver, akkor van lehetőség annak ideiglenes leállítására? (Erre az EIM konfigurációs folyamatának befejezéséhez van szükség.)	
Rendelkezik *SECADM, *ALLOBJ és *IOSYSCFG speciális jogosultságokkal?	
Alkalmazta a legfrissebb ideiglenes program javításokat (PTF)?	

Ha a felhasználók hitelesítését Kerberos alapon tervezi megoldani, akkor be kell állítania a Hálózati hitelesítési szolgáltatást is. A Hálózati hitelesítési szolgáltatás megtervezéséhez a Hálózati hitelesítési szolgáltatás tervezése című témakörben talál egy teljes munkalapot.

Ha a Hálózati hitelesítési szolgáltatás és az EIM együttes felhasználásával egyszeri bejelentkezést kíván megvalósítani, akkor a Példahelyzet: egyszeri bejelentkezés engedélyezése című témakörben tekintse át az említett termékek beállítását erre a célra.

Szükséges iSeries navigátor összetevők telepítése

Ahhoz, hogy az EIM és a Hálózati hitelesítési szolgáltatás egyszeri bejelentkezést biztosító környezet nyújtson, telepítenie kell az iSeries navigátor Hálózat és Biztonság összetevőjét is. Az EIM a Hálózat kategóriában, az Hálózati hitelesítési szolgáltatás pedig a Biztonság kategóriában található. Ha nem tervezi a Hálózati hitelesítési szolgáltatás használatát a hálózaton, akkor az iSeries navigátor Biztonság összetevőjének telepítése nem szükséges.

Az iSeries navigátor Hálózat összetevőjének telepítéséhez, illetve az összetevő sikeres telepítésének ellenőrzéséhez győződjön meg, hogy az iSeries szerver kezelésére használt számítógépen telepítve van-e az iSeries Access for Windows.

A Hálózat összetevő telepítése:

1. Kattintson a **Start —> Programok —> IBM iSeries Access for Windows —> Szelektív telepítő** menüpontra.
2. Kövesse a megjelenő útmutatásokat. Az **Összetevők kiválasztása** képernyőn bontsa ki az **iSeries navigátor** kategóriát, majd válassza ki a **Hálózat** lehetőséget.
   Ha tervezi a Hálózati hitelesítési szolgáltatás használatát is, akkor a **Biztonság** lehetőséget is ki kell választania.
3. Fejezze be a Szelektív telepítő hátralévő részét.

Hálózati hitelesítési szolgáltatás beállítása

A Hálózati hitelesítési szolgáltatás teszi lehetővé Kerberos hitelesítés alkalmazását az iSeries szerveren. A szolgáltatás nem előfeltétele az EIM használatának, ettől függetlenül a Kerberos számos előnyt biztosít a hálózat biztonsága szempontjából.

A Hálózati hitelesítési szolgáltatás és az EIM együttes felhasználása teremti meg az egyszeri bejelentkezést biztosító környezetek alapjait. Az egyszeri bejelentkezést biztosító környezetek a felhasználók és adminisztrátorok számára is számos előnyt hordoznak. A felhasználóknak kevesebb felhasználónevet és jelszót kell megjegyezniük, az adminisztrátoroknak pedig kevesebb felhasználói információt kell figyelemmel kísérniük. Mivel az egyszeri bejelentkezés segítségével hidat verhet számos különböző platform és rendszer között ezáltal az alkalmazásfejlesztési és általános adminisztrációs költségek is csökkennek.

Ha a Hálózati hitelesítési szolgáltatás jelenleg nincs beállítva a hálózat összes iSeries szerverén, akkor a kezdeti lépéseket a Hálózati hitelesítési szolgáltatás tervezése című témakörből tudhatja meg. Ha már ismeri a Hálózati hitelesítési szolgáltatást, akkor a konfigurációs folyamatról a Hálózati hitelesítési szolgáltatás beállítása című témakörből tájékozódhat.

EIM beállítása

Ha az alapként szolgáló biztonsági stratégiák módosítása nélkül kíván egyszeri bejelentkezést biztosító környezetet létrehozni, akkor az EIM mellett a Hálózati hitelesítési szolgáltatást is be kell állítani. Ettől függetlenül a Hálózati hitelesítési szolgáltatás nem előfeltétele vagy követelménye az EIM működésének.

Az egyszeri bejelentkezést biztosító környezet alapjául szolgáló EIM beállítását az iSeries szerveren az EIM konfigurációs varázslóval kezdheti meg. Konfigurációs igényeitől függően a varázslóval csatlakozhat egy meglévő tartományhoz, vagy létrehozhat egy új tartományt, és csatlakozhat ahhoz.

Az EIM konfigurációs varázsló segítségével könnyedén összeállíthat egy alapszintű EIM konfigurációt. Ha például még nem rendelkezik beállított LDAP szerverrel, vagy még nem állította be a Hálózati hitelesítési szolgáltatást, akkor az EIM konfigurációs varázsló segítséget nyújt ezen feladatok végrehajtásához is.

Miután a varázsló létrehozta az alapszintű EIM konfigurációt, néhány további konfigurációs lépést kell végrehajtani, mielőtt az egyszeri bejelentkezést biztosító környezetet használatba lehetne venni. A Példahelyzet: Egyszeri bejelentkezés engedélyezése című témakör bemutatja, hogyan állított be egy fiktív vállalat egyszeri bejelentkezést biztosító környezetet a Hálózati hitelesítési szolgáltatás és az EIM segítségével.

Az EIM konfigurációs varázsló használata előtt az EIM és a Hálózati hitelesítési szolgáltatás pontos felhasználási módjának meghatározása érdekében be kell fejezni az összes tervezési lépést. A tervezés befejezése után a varázsló segítségével kétféleképpen állíthatja be az EIM szolgáltatást az iSeries szerveren: létrehozhat új tartományokat, illetve csatlakozhat meglévőkhöz. Az EIM beállításával az alábbi témakörök foglalkoznak részletesen:

Új tartomány létrehozása és csatlakozás hozzá
Ezzel a feladattal hozhat létre vállalata számára egy EIM tartományt, és állíthatja be az iSeries szervert a benne való részvételre. A varázsló létrehozza az új tartományt, beállítja a helyi LDAP szervert az új tartomány EIM tartományvezérlőjeként. Emellett, ha a Kerberos még nincs beállítva az iSeries szerveren, akkor a varázsló lehetőséget nyújt a Hálózati hitelesítési szolgáltatás konfigurációs varázsló elindítására. A feladat befejezése után további iSeries szervereket is beállíthat a tartományban való részvételre. Ha más szerverekkel is csatlakozni kíván a tartományhoz, akkor lépjen be ezek mindegyikére, és az EIM konfigurációs varázslóval csatlakoztassa a rendszereket egy meglévő EIM tartományhoz.

Csatlakozás meglévő tartományhoz
Miután az EIM konfigurációs varázslóval beállított egy tartományvezérlőt és egy EIM tartományt, ezzel a feladattal illeszthet be további iSeries szervereket a tartományba. Ezt a feladatot az hálózat összes olyan iSeries szerverén el kell végeznie, amely használni fogja az EIM funkciókat. A varázsló befejezése után meg kell adnia a tartomány nevét, amelyhez csatlakozni kíván, beleértve az EIM tartományvezérlőre vonatkozó kapcsolati információkat (például portszám, és TLS/SSL használat). Ha a Kerberos még nincs beállítva az iSeries szerveren, akkor a varázsló lehetőséget nyújt a Hálózati hitelesítési szolgáltatás konfigurációs varázsló elindítására.

Az EIM konfigurációs varázsló elérése

Az EIM konfigurációs varázsló elindításához tegye a következőket:

1. Indítsa el az iSeries navigátort.
2. Jelentkezzen be az iSeries szerverre, amelyen be kívánja állítani az EIM szolgáltatást. Ha az EIM beállítását egynél több iSeries szerveren végzi, akkor azzal kezdje, amelyet EIM tartományvezérlőként kíván beállítani.
3. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM)** kategóriát.
4. Kattintson a jobb egérgombbal a **Konfiguráció** elemre, majd válassza az előugró menü **Beállítás...** menüpontját az EIM konfigurációs varázsló elindításához.
5. Válassza ki a **Csatlakozás meglévő tartományhoz** vagy az **Új tartomány létrehozása és csatlakozás** kiindulási helyzetet.

Miután az EIM konfigurációs varázslóval létrehozta az EIM tartományvezérlőt, és az iSeries szervereket beállította a tartományban való részvételre, az EIM konfiguráció véglegesítéséhez még végre kell hajtani az alábbi feladatokat:

1. Adja hozzá a tartományba bevonni kívánt nem iSeries szerverek és alkalmazások nyilvántartásait az EIM tartományhoz.
2. Hozza létre minden egyes egyedi felhasználó vagy entitás EIM azonosítóit a tartományban.
3. Hozza létre a különféle felhasználói azonosságok és a fenti EIM azonosítók közötti társításokat.

Új tartomány létrehozása és csatlakozás

Ez EIM konfigurációs varázsló segítségével állíthatja be az iSeries szerveren futó LDAP szervert az új tartomány EIM tartományvezérlőjeként. Ha szükséges, akkor az EIM konfigurációs varázsló meggyőződik arról, hogy rendelkezésre állnak az LDAP szerver alapvető konfigurációs információi.

Emellett, ha a Kerberos még nincs beállítva az iSeries szerveren, akkor a varázsló lehetőséget nyújt a Hálózati hitelesítési szolgáltatás konfigurációs varázsló elindítására. A varázsló befejezésekor beállításra kerül egy új EIM tartomány, az iSeries szerver csatlakozik ehhez, és a megadott felhasználói nyilvántartások bekerülnek a tartományba.

A feladat elvégzéséhez Biztonsági adminisztrátor (*SECADM), Minden objektum (*ALLOBJ) és Rendszerkonfiguráció (*IOSYSCFG) speciális jogosultságokkal kell rendelkeznie.

Ez EIM konfigurációs varázsló elindításához, illetve egy új EIM tartomány létrehozásához és a hozzá való csatlakozáshoz tegye a következőket az iSeries navigátorban:

Megjegyzés: A varázsló a helyi LDAP szervert állítja be az új EIM tartomány tartományvezérlőjeként.

1. Bontsa ki a **Hálózat** —> **Vállalati azonosság leképezés (EIM)** kategóriát.
2. Kattintson a jobb egérgombbal a **Konfiguráció** elemre, majd válassza az előugró menü **Beállítás...** menüpontját az EIM konfigurációs varázsló elindításához.
3. A varázsló **Üdvözlet** lapján válassza az **Új tartomány létrehozása és csatlakozás** lehetőséget, majd kattintson a **Tovább** gombra.
4. Ha a Hálózati hitelesítési szolgáltatás jelenleg nincs beállítva az iSeries szerveren, akkor megjelenik a **Hálózati hitelesítési szolgáltatás beállítása** párbeszédablak. A párbeszédablak felszólítja a Hálózati hitelesítési szolgáltatás beállítására. Ha az **Igen** lehetőséget választja, akkor elindul a Hálózati hitelesítési szolgáltatás konfigurációs varázsló. Az EIM konfigurációs varázsló a Hálózati hitelesítési szolgáltatás beállítása után folytatódik.
5. Ha a helyi LDAP szerver jelenleg nincs beállítva, akkor megjelenik a **Címtár szerver beállítása** párbeszédablak. A helyi LDAP szerver beállításához adja meg a következő információkat:
   - A **Port** mezőben fogadja el az alapértelmezett **389** portszámot, vagy írjon be egy másik portszámot a címtár szerverrel folytatott nem biztonságos EIM kommunikációhoz.
   - A **Megkülönböztetett név** mezőben adja meg az LDAP szerver LDAP adminisztrátorát azonosító LDAP megkülönböztetett nevet (DN). Az EIM konfigurációs varázsló létrehozza a megadott LDAP adminisztrátori megkülönböztetett nevet, és ezt használja fel a létrehozott tartomány tartományvezérlőjeként szolgáló LDAP szerver beállítására.
   - A **Jelszó** mezőben adja meg az LDAP adminisztrátor jelszavát.
   - A **Jelszó megerősítése** mezőben adja meg ismét a jelszót.
   - Kattintson a **Tovább** gombra.
6. A **Tartományvezérlő meghatározása** párbeszédablakban adja meg a következő információkat:
   - A **Tartomány** mezőben adja meg a létrehozni kívánt EIM tartomány nevét. Fogadja el az alapértelmezett **EIM** nevet, vagy írjon be tetszőleges más karaktersorozatot. Ne feledje azonban, hogy speciális karakterek, például az = + < > , # ; \ és * nem használhatók.
   - A **Leírás** mezőben írja be a tartomány szöveges leírását.
   - Kattintson a **Tovább** gombra.
7. A **Tartomány szülő DN meghatározása** párbeszédablakban jelezze, hogy kíván-e szülő megkülönböztetett nevet megadni a tartományhoz. A szülő megkülönböztetett név használatával megadhatja, hogy az EIM tartományra vonatkozó adatok a helyi LDAP névtér mely részébe kerüljenek. Ha nem ad nem szülő megkülönböztetett nevet, akkor az EIM adatok saját utótagjuknak megfelelő helyre kerülnek a névtérben. Ha az **Igen** választás mellett döntött, akkor a listában válassza ki a szülő megkülönböztetett névként használni kívánt helyi LDAP utótagot, vagy írjon be egy új szülő megkülönböztetett nevet. A tartomány szülő megkülönböztetett nevének meghatározása nem kötelező.
8. A **Kapcsolati felhasználó meghatározása** párbeszédablakban válassza ki a kapcsolat **Felhasználó típusát**. A következő felhasználói típusok közül választhat: Megkülönböztetett név és jelszó, Kerberos kulcscímke fájl és azonosító vagy Kerberos azonosító és jelszó. A két Kerberos felhasználói típus csak akkor választható, ha a helyi iSeries szerveren be van állítva a Hálózati hitelesítési szolgáltatás. A megadott felhasználótípus határozza meg a párbeszédablakban megadandó további információkat az alábbiak szerint:
   - A **Megkülönböztetett név és jelszó** választásakor adja meg a következőket:
     - A **Megkülönböztetett név** mezőben adja meg azt az LDAP megkülönböztetett nevet, amely jogosult objektumok létrehozására az LDAP szerver helyi címterében. Ha az LDAP szervert a varázslóval állította be egy korábbi lépésben, akkor a létrehozott LDAP adminisztrátor megkülönböztetett nevét kell megadni.
     - A **Jelszó** mezőben adja meg a felhasználó jelszavát.

- A **Jelszó megerősítése** mezőben adja meg ismét a jelszót.

- A **Kerberos kulcscímke fájl és azonosító** választásakor adja meg a következőket:
  - A **Kulcscímke fájl** mezőben adja meg az LDAP szerver helyi névterében objektumok létrehozására jogosult felhasználót azonosító kulcscímke fájl nevét az iSeries szerveren. Ha a kulcscímke fájlt ki kívánja választani, akkor kattintson a **Tallózás** gombra.
  - Az **Azonosító** mezőben adja meg a felhasználót azonosító Kerberos azonosító nevét.
  - A **Tartomány** mezőben adja meg az azonosító Kerberos tartományát. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcscímke fájlban szereplő Kerberos felhasználókat. A hoszt.vallalat.hu tartomány jkovacs felhasználóját például a kulcscímke fájlban a jsmith@ordept.myco.com képviseli.
- A **Kerberos azonosító és jelszó** választásakor adja meg a következőket:
  - Az **Azonosító** mezőben adja meg az LDAP szerver helyi névterében objektumok létrehozására jogosult felhasználót azonosító Kerberos azonosítót nevét.
  - A **Tartomány** mezőben adja meg az azonosító Kerberos tartományát.
  - A **Jelszó** mezőben adja meg a felhasználó jelszavát.
  - A **Jelszó megerősítése** mezőben adja meg ismét a jelszót. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcscímke fájlban szereplő Kerberos felhasználókat. A hoszt.vallalat.hu tartomány jkovacs felhasználóját például a kulcscímke fájlban a jsmith@ordept.myco.com képviseli.
- Kattintson a **Kapcsolat ellenőrzése** gombra a felhasználói beállítások ellenőrzéséhez a tartományvezérlőn.
- Kattintson a **Tovább** gombra.

9. A **Nyilvántartás információk** párbeszédablakban válassza ki az EIM tartományba felvenni kívánt felhasználói nyilvántartások típusát. A következő felhasználói nyilvántartási típusok közül választhat:
   - Válassza az **OS400** elemet a helyi nyilvántartást képviselő felhasználói nyilvántartás hozzáadásához. A mezőben adja meg a tartományban létrehozni kívánt nyilvántartásnevet. Az EIM nyilvántartás neve tetszőleges karaktersorozat lehet, amely azonosítja a nyilvántartás típusát és az adott példányt.
   - Válassza a **Kerberos** elemet, ha egy Kerberos felhasználói nyilvántartást kíván hozzáadni az EIM tartományhoz. A mezőben írja be a tartományban létrehozni kívánt nyilvántartásnevet, és szükség esetén válassza ki a **Kerberos felhasználói azonosságokban a kis- és nagybetűk eltérőnek számítanak** beállítást.
   - Kattintson a **Tovább** gombra.
10. Az **EIM rendszer felhasználó meghatározása** párbeszédablakban válassza ki, hogy milyen típusú felhasználót használjon a rendszer az operációs rendszer funkciók nevében végzett EIM műveleteknél. Ilyen művelet például a leképezések kikeresése és a társítások törlése egy helyi OS/400 felhasználói profil törlésekor. A következő felhasználói típusok közül választhat: Megkülönböztetett név és jelszó, Kerberos kulcscímke fájl és azonosító vagy Kerberos azonosító és jelszó. A megadott felhasználótípus határozza meg a párbeszédablakban megadandó további információkat az alábbiak szerint:

Megjegyzés: A megadott felhasználónak jogosultnak kell lennie leképezés kikeresési és nyilvántartás adminisztrációs funkciók elvégzésére legalább a helyi felhasználói nyilvántartáson. Ha a megadott felhasználó nem rendelkezik ezen jogosultságokkal, akkor az egyszeri bejelentkezéssel és a felhasználói profilok törlésével kapcsolatos operációs rendszer funkciók meghiúsulhatnak.

11. A **Megkülönböztetett név és jelszó** választásakor adja meg a következőket:
    - A **Megkülönböztetett név** mezőben adja meg az OS/400 által az EIM tartományvezérlő megkereséséhez használt felhasználót azonosító LDAP megkülönböztetett nevet.
    - A **Jelszó** mezőben adja meg a felhasználó jelszavát.
    - A **Jelszó megerősítése** mezőben adja meg ismét a jelszót.

12. A **Kerberos azonosító és jelszó** választásakor adja meg a következőket:
    - Az **Azonosító** mezőben adja meg az OS/400 által az EIM tartományvezérlő megkereséséhez használt felhasználót azonosító Kerberos azonosítót nevét.
    - A **Tartomány** mezőben adja meg az azonosító Kerberos tartományát.
    - A **Jelszó** mezőben adja meg a felhasználó jelszavát.
    - A **Jelszó megerősítése** mezőben adja meg ismét a jelszót. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcscímke fájlban szereplő Kerberos felhasználókat. A hoszt.vallalat.hu tartomány jkovacs felhasználóját például a kulcscímke fájlban a jsmith@ordept.myco.com képviseli.
13. A **Kerberos kulcscímke fájl és azonosító** választásakor adja meg a következőket:
    - A **Kulcscímke fájl** mezőben adja meg az OS/400 által az EIM tartományvezérlő megkereséséhez használt felhasználót azonosító kulcscímke fájl nevét az iSeries szerveren. Ha a kulcscímke fájlt ki kívánja választani, akkor kattintson a **Tallózás** gombra.
    - Az **Azonosító** mezőben adja meg a felhasználót azonosító Kerberos azonosító nevét.
    - A **Tartomány** mezőben adja meg az azonosító Kerberos tartományát. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcscímke fájlban szereplő Kerberos felhasználókat. A hoszt.vallalat.hu tartomány jkovacs felhasználóját például a kulcscímke fájlban a jsmith@ordept.myco.com képviseli.
14. Kattintson a **Kapcsolat ellenőrzése** gombra a tartományvezérlő kapcsolatának ellenőrzéséhez a megadott rendszer felhasználóval.
15. Kattintson a **Tovább** gombra.
16. Az **Összegzés** párbeszédablakban tekintse át a megadott konfigurációs információkat. Ha a megjelenő információk helyesek, akkor kattintson a **Befejezés** gombra.

A varázsló befejezése után készen áll az alapszintű EIM konfiguráció. A szerver EIM konfigurációjának véglegesítéséhez azonban még el kell végeznie a következő feladatokat is:

1. Adja hozzá a létrehozott tartományt az EIM tartománykezelés mappához.
2. Adja hozzá a tartományba bevonni kívánt egyéb szerverek és alkalmazások nyilvántartásait az EIM tartományhoz.
3. Hozza létre minden egyes egyedi felhasználó vagy entitás EIM azonosítóit a tartományban.
4. Hozza létre a különféle felhasználói azonosságok és a fenti EIM azonosítók közötti társításokat.

Emellett szükség esetén beállíthatja a tartományvezérlő biztonságos kapcsolatát a Védett socket réteg (SSL) vagy Szállítási réteg biztonság (TLS) protokollokkal.

Biztonságos kapcsolat kialakítása az EIM tartományvezérlővel

Miután a varázsló segítségével létrehozott egy új tartományt és csatlakozott hozzá, a Védett socket réteg (SSL) vagy a Szállítási réteg biztonság (TLS) protokoll segítségével biztonságos kapcsolatokat alakíthat ki az EIM tartományvezérlővel. Az EIM SSL/TLS támogatásának beállításához tegye a következőket:

1. Engedélyezze az SSL-t a tartományvezérlő LDAP szerverén.
2. A Digitális igazolás kezelő segítségével hozza létre az LDAP szerver SSL igazolását.
3. A Digitális igazolás kezelő segítségével rendelje hozzá az igazolást az LDAP szerverhez.
4. Frissítse az EIM konfiguráció tulajdonságait, és adja meg, hogy az iSeries szerver SSL kapcsolatot használ.
5. Frissítse az EIM tartomány tulajdonságait minden EIM tartománynál, és adja meg, hogy az EIM SSL kapcsolatot használ a tartománynak az iSeries navigátorból végzett kezeléséhez.

Csatlakozás meglévő tartományhoz

Az EIM konfigurációs varázsló segítségével csatlakozhat egy meglévő EIM tartományhoz. Az EIM konfigurációs varázsló ezen lehetőségét abban az esetben használja, ha a hálózaton már van beállított EIM tartomány és tartományvezérlő. A varázsló végrehajtása során meg kell adnia a tartományra vonatkozó

információkat, ideértve az EIM tartományvezérlő kapcsolati információit is. A varázsló a megadott értékeket az iSeries szerveren tárolja, és ezek segítségével csatlakozik az EIM tartományvezérlőhöz. A varázsló emellett létrehoz egy EIM felhasználói nyilvántartást is az iSeries szerver OS/400 felhasználói profil nyilvántartásához.

A feladat elvégzéséhez Biztonsági adminisztrátor (*SECADM) és Minden objektum (*ALLOBJ) speciális jogosultságokkal kell rendelkeznie.

Az EIM konfigurációs varázsló indításához, és egy meglévő EIM tartományhoz való csatlakozáshoz tegye a következőket az iSeries navigátorban:

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM)** kategóriát.
2. Kattintson a jobb egérgombbal a **Konfiguráció** elemre, majd válassza az előugró menü **Beállítás...** menüpontját az EIM konfigurációs varázsló elindításához. Miután a varázsló elindult, a megjelenő párbeszédablakokban adja meg az következő információkat.
3. A varázsló **Üdvözlet** párbeszédablakában válassza a **Csatlakozás meglévő tartományhoz** lehetőséget, majd kattintson a **Tovább** gombra.
4. Ha a Hálózati hitelesítési szolgáltatás jelenleg nincs beállítva az iSeries szerveren, akkor megjelenik a **Hálózati hitelesítési szolgáltatás beállítása** párbeszédablak. A párbeszédablak felszólítja a Hálózati hitelesítési szolgáltatás beállítására. Ha az **Igen** lehetőséget választja, akkor elindul a Hálózati hitelesítési szolgáltatás konfigurációs varázsló. Az EIM konfigurációs varázsló a Hálózati hitelesítési szolgáltatás beállítása után folytatódik.
5. A **Tartományvezérlő meghatározása** párbeszédablakban adja meg a következő információkat:
   - A **Tartományvezérlő neve** mezőben adja meg az használni kívánt EIM tartomány tartományvezérlőjeként szolgáló szerver nevét.
   - Ha az EIM adatok átvitelét titkosítani kívánja, akkor válassza ki a **Védett socket réteg (SSL) használata** beállítást.
   - Kattintson a **Kapcsolat ellenőrzése** gombra a tartományvezérlő konfigurációs információinak ellenőrzéséhez.

Megjegyzés: Ha megadta az SSL használatát, de hibaüzenetet kap, akkor a hibaüzenet utalhat rá, hogy az LDAP szerver nincs beállítva az SSL használatára.

   - Kattintson a **Tovább** gombra.
6. A **Kapcsolati felhasználó meghatározása** párbeszédablakban válassza ki a kapcsolat **Felhasználó típusát**. A következő felhasználói típusok közül választhat: Megkülönböztetett név és jelszó, Kerberos kulcscímke fájl és azonosító vagy Kerberos azonosító és jelszó. A két Kerberos felhasználói típus csak akkor választható, ha a helyi iSeries szerveren be van állítva a Hálózati hitelesítési szolgáltatás. A megadott felhasználótípus határozza meg a párbeszédablakban megadandó további információkat az alábbiak szerint:
   - A **Megkülönböztetett név és jelszó** választásakor adja meg a következőket:
     - A **Megkülönböztetett név** mezőben adja meg azt az LDAP megkülönböztetett nevet, amely jogosult objektumok létrehozására az LDAP szerver helyi címterében.
     - A **Jelszó** mezőben adja meg a felhasználó jelszavát.
     - A **Jelszó megerősítése** mezőben adja meg ismét a jelszót.
   - A **Kerberos kulcscímke fájl és azonosító** választásakor adja meg a következőket:
     - A **Kulcscímke fájl** mezőben adja meg az LDAP szerver helyi névterében objektumok létrehozására jogosult felhasználót azonosító kulcscímke fájl nevét az iSeries szerveren. Ha a kulcscímke fájlt ki kívánja választani, akkor kattintson a **Tallózás** gombra.
     - Az **Azonosító** mezőben adja meg a felhasználót azonosító Kerberos azonosító nevét.

- A **Tartomány** mezőben adja meg az azonosító Kerberos tartományát. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcscímke fájlban szereplő Kerberos felhasználókat. A hoszt.vallalat.hu tartomány jkovacs felhasználóját például a kulcscímke fájlban a jsmith@ordept.myco.com képviseli.

• A **Kerberos azonosító és jelszó** választásakor adja meg a következőket:
  - Az **Azonosító** mezőben adja meg az LDAP szerver helyi névterében objektumok létrehozására jogosult felhasználót azonosító Kerberos azonosítót nevét.
  - A **Tartomány** mezőben adja meg az azonosító Kerberos tartományát.
  - A **Jelszó** mezőben adja meg a felhasználó jelszavát.
  - A **Jelszó megerősítése** mezőben adja meg ismét a jelszót. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcscímke fájlban szereplő Kerberos felhasználókat. A hoszt.vallalat.hu tartomány jkovacs felhasználóját például a kulcscímke fájlban a jsmith@ordept.myco.com képviseli.
• Kattintson a **Kapcsolat ellenőrzése** gombra a felhasználói beállítások ellenőrzéséhez a tartományvezérlőn.
• Kattintson a **Tovább** gombra.

7. A **Tartomány meghatározása** lapon válassza ki a tartományt, amelyhez csatlakozni kíván, majd kattintson a **Tovább** gombra.
8. A **Nyilvántartás információk** lapon válassza ki az EIM tartományba felvenni kívánt felhasználói nyilvántartások típusát. A következő felhasználói nyilvántartási típusok közül választhat:
   • Válassza az **OS400** elemet a helyi nyilvántartást képviselő felhasználói nyilvántartás hozzáadásához. A mezőben adja meg a tartományban létrehozni kívánt nyilvántartásnevet. Az EIM nyilvántartás neve tetszőleges karaktersorozat lehet, amely azonosítja a nyilvántartás típusát és az adott példányt.
   • Válassza a **Kerberos** elemet, ha egy Kerberos felhasználói nyilvántartást kíván hozzáadni az EIM tartományhoz. A mezőben írja be a tartományban létrehozni kívánt nyilvántartásnevet, és szükség esetén válassza ki a **Kerberos felhasználói azonosságokban a kis- és nagybetűk eltérőnek számítanak** beállítást. Elfogadhatja az alapértelmezett értéket is; a Kerberos nyilvántartás neve megegyezik a tartomány nevével. Ha a Kerberos nyilvántartás nevét használja tartománynévként, akkor ezzel javíthatja a nyilvántartásban tárolt információk visszakeresésének teljesítményét. A felhasználói nyilvántartások meghatározásával kapcsolatban nézze meg az EIM nyilvántartás meghatározások című témakört.
   • Kattintson a **Tovább** gombra.
9. Az **EIM rendszer felhasználó meghatározása** párbeszédablakban válassza ki, hogy milyen típusú felhasználót használjon a rendszer az operációs rendszer funkciók nevében végzett EIM műveleteknél. Ilyen művelet például a leképezések kikeresése és a társítások törlése egy helyi OS/400 felhasználói profil törlésekor. A következő felhasználói típusok közül választhat: Megkülönböztetett név és jelszó, Kerberos kulcscímke fájl és azonosító vagy Kerberos azonosító és jelszó. A megadott felhasználótípus határozza meg a párbeszédablakban megadandó további információkat az alábbiak szerint:
   • A **Megkülönböztetett név és jelszó** választásakor adja meg a következőket:
     - A **Megkülönböztetett név** mezőben adja meg az OS/400 által az EIM tartományvezérlő megkereséséhez használt felhasználót azonosító LDAP megkülönböztetett nevet.
     - A **Jelszó** mezőben adja meg a felhasználó jelszavát.
     - A **Jelszó megerősítése** mezőben adja meg ismét a jelszót.
   • A **Kerberos azonosító és jelszó** választásakor adja meg a következőket:
     - Az **Azonosító** mezőben adja meg az OS/400 által az EIM tartományvezérlő megkereséséhez használt felhasználót azonosító Kerberos azonosítót nevét.
     - A **Tartomány** mezőben adja meg az azonosító Kerberos tartományát.
     - A **Jelszó** mezőben adja meg a felhasználó jelszavát.

- A **Jelszó megerősítése** mezőben adja meg ismét a jelszót. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcscímke fájlban szereplő Kerberos felhasználókat. A hoszt.vallalat.hu tartomány jkovacs felhasználóját például a kulcscímke fájlban a jsmith@ordept.myco.com képviseli.

- A **Kerberos kulcscímke fájl és azonosító** választásakor adja meg a következőket:
  - A **Kulcscímke fájl** mezőben adja meg az OS/400 által az EIM tartományvezérlő megkereséséhez használt felhasználót azonosító kulcscímke fájl nevét az iSeries szerveren. Ha a kulcscímke fájlt ki kívánja választani, akkor kattintson a **Tallózás** gombra.
  - Az **Azonosító** mezőben adja meg a felhasználót azonosító Kerberos azonosító nevét.
  - A **Tartomány** mezőben adja meg az azonosító Kerberos tartományát.
- Kattintson a **Kapcsolat ellenőrzése** gombra a kapcsolat ellenőrzéséhez a megadott rendszer felhasználóval.
- Kattintson a **Tovább** gombra.

10. Az **Összegzés** párbeszédablakban tekintse át a megadott konfigurációs információkat. Ha a megjelenő információk helyesek, akkor kattintson a **Befejezés** gombra.

A varázsló befejezése után készen áll az alapszintű EIM konfiguráció. A szerver EIM konfigurációjának véglegesítéséhez azonban még el kell végeznie a következő feladatokat is:

1. Adja hozzá az EIM tartománykezelés mappájához a tartományt, amelyhez az imént csatlakozott.
2. Adja hozzá a tartományba bevonni kívánt nem iSeries szerverek és alkalmazások nyilvántartásait az EIM tartományhoz.
3. Hozza létre minden egyes egyedi felhasználó vagy entitás EIM azonosítóit a tartományban.
4. Hozza létre a különféle felhasználói azonosságok és a fenti EIM azonosítók közötti társításokat.

Egyszeri bejelentkezést biztosító környezet kialakításához be kell állítani a Hálózati hitelesítési szolgáltatást is az iSeries szerveren.

EIM kezelése

Miután beállította az EIM funkciót az iSeries szerveren, számos feladat végrehajtása szükséges az EIM tartomány és az információk kezeléséhez. Az iSeries szerveren illetve a vállalatnál alkalmazott EIM szolgáltatás kezeléséhez szükséges feladatokat az alábbi témakörök tárgyalják:

EIM tartományok kezelése
Az EIM tartományban található EIM információk és az EIM tartomány tulajdonságainak kezelése.

Társítások kezelése
A felhasználói azonosságok és EIM azonosítók közötti társítások karbantartása.

EIM azonosítók kezelése
A vállalati felhasználókhoz társított EIM azonosítók karbantartása.

EIM felhasználói jogosultságok kezelése
Az EIM információk biztonságának fenntartása a felhasználók által használható funkciók és műveletek jogosultságainak felügyeletével.

Felhasználói nyilvántartások kezelése
Az EIM tartományba felvett felhasználói nyilvántartások kezelése.

EIM tartományok kezelése

Az EIM tartományok kezelése az iSeries navigátorból történik. Ahhoz, hogy egy tartomány kezelhető legyen, szerepelnie kell az iSeries navigátor Hálózat kategóriájában található Tartománykezelés mappában. Miután létrehozott és beállított egy új EIM tartományt, hozzá kell adnia azt a Tartománykezelés mappához a benne tárolt információk kezeléséhez.

Az azonos hálózatban található EIM tartományok kezelésére tetszőleges iSeries kapcsolat használható. Az iSeries navigátorhoz csatlakozó iSeries szervernek nem kell részt vennie a tartományban ahhoz, hogy a tartományt kezelni lehessen róla.

Az EIM tartományok kezelése a következő feladatokból áll:

- Tartomány hozzáadása a Tartománykezelés mappához
- Csatlakozás egy tartományhoz
- Tartomány törlése
- Tartomány eltávolítása a Tartománykezelés mappából

Tartomány hozzáadása a Tartománykezelés mappához

Tartomány hozzáadásához *SECADM speciális jogosultsággal kell rendelkeznie. Ha egy meglévő EIM tartományt fel kíván venni a Tartománykezelés mappába, akkor tegye a következőket.

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM)** kategóriát.
2. Kattintson a jobb egérgombbal a **Tartománykezelés** elemre, majd válassza az előugró menü **Tartomány hozzáadása...** menüpontját.
3. Adja meg a szükséges tartományt és a kapcsolatra vonatkozó információkat.
4. A tartomány felvételéhez kattintson az **OK** gombra.

Csatlakozás tartományhoz

Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor először csatlakoznia kell hozzá. EIM tartományhoz akkor is csatlakozhat, ha az iSeries szerver jelenleg nincs beállítva a tartomány tagjaként.

Ha csatlakozni kíván egy EIM tartományhoz, akkor tegye a következőket:

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Válassza ki a tartományt, amelyhez csatlakozni kíván. Ha a kezelni kívánt tartomány nem szerepel a felsorolásban, akkor hozzá kell adnia az EIM tartományt a Tartománykezelés mappához.
3. Kattintson a jobb egérgombbal az EIM tartományra, amelyhez csatlakozni kíván, majd válassza az előugró menü **Csatlakozás...** menüpontját.
4. Az EIM tartományvezérlőre csatlakozáshoz adja meg a felhasználó típusát, és a szükséges felhasználói információkat.
5. Kattintson az **OK** gombra.

Tartomány törlése

A feladat elvégzéséhez LDAP adminisztrátor vagy EIM adminisztrátor jogosultsággal kell rendelkeznie. EIM tartományok törlése előtt a tartományból el kell távolítania az összes nyilvántartást és EIM azonosító információt.

EIM tartomány törléséhez tegye a következőket.

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Távolítsa el az EIM tartomány összes felhasználói nyilvántartását.
3. Távolítsa el az EIM tartomány összes EIM azonosítóját.
4. Kattintson a jobb egérgombbal a törölni kívánt tartományra, majd válassza az előugró menü **Törlés...** menüpontját.
5. A **Törlés megerősítése** párbeszédablakban kattintson az **Igen** gombra.

Tartomány eltávolítása a Tartománykezelés mappából
Bár erre általában nincs szükség, az EIM tartományok eltávolíthatók a Tartománykezelés mappából, miután befejezte módosításokat.

Tartomány eltávolításához tegye a következőket:

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM)** kategóriát.
2. Kattintson a jobb egérgombbal a **Tartománykezelés** mappára, majd válassza az előugró menü **Tartomány eltávolítása...** menüpontját.
3. Válassza ki a Tartománykezelés mappából eltávolítani kívánt EIM mappát.
4. A tartomány eltávolításához kattintson az **OK** gombra.

Társítások kezelése
A társítások az EIM azonosítók és a nyilvántartáson belüli felhasználói azonosságok közötti viszonyt írják le. Létrehozható például társítás egy OS/400 felhasználói profil vagy Kerberos azonosító és egy EIM azonosító között. Ez a társítás használható fel annak meghatározására, hogy melyik EIM azonosító felel meg egy helyi iSeries felhasználói profilnak vagy Kerberos azonosítónak.

A felhasználói azonosságok és a megfelelő EIM azonosítók közötti társítások karbantartása kulcsfontosságú kérdés a hálózat különféle rendszerein fiókokkal rendelkező felhasználók nyomon követéséhez szükséges adminisztrációs feladatok leegyszerűsítésében.

A társítások kezelése teszi lehetővé továbbá az egyszeri bejelentkezés megvalósítását a hálózatban. Biztonságos egyszeri bejelentkezést biztosító környezet kialakításakor a társításoknak folyamatosan naprakészeknek kell lenniük.

Háromféle társítás létrehozására van lehetőség: forrás, cél és adminisztrációs. A felhasználói azonosságok és a megfelelő EIM azonosítók közötti társítások létrehozásához vagy karbantartásához válasszon az alábbi feladatok közül:

- Társítás létrehozása
- Társítás törlése

Társítás létrehozása
egyszeri bejelentkezést biztosító környezet kialakításához létre kell hoznia a személyek különféle felhasználói azonosságai és az adott személy EIM azonosítója közötti megfelelő társításokat. Háromféle társítás hozható létre: cél, forrás és adminisztrációs.

Adminisztrációs vagy forrás társítás létrehozásához azonosító adminisztrátori vagy EIM adminisztrátori jogosultsággal kell rendelkeznie. Cél társítás létrehozásához minden nyilvántartáshoz nyilvántartás adminisztrátori, vagy EIM adminisztrátori jogosultság szükséges.

Ha társítást szeretne létrehozni egy EIM azonosító számára, akkor tegye a következőket:

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Csatlakoznia kell a kezelni kívánt EIM tartományhoz.
   - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg az EIM tartomány hozzáadása a Tartománykezelés mappához című témakört.
   - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson az **Azonosítók** elemre az EIM azonosítók listájának megjelenítéséhez.
5. Kattintson a jobb egérgombbal a megfelelő EIM azonosítóra, majd válassza az előugró menü **Tulajdonságok...** menüpontját.
6. Kattintson a **Társítások** lapra.

7. A **Hozzáadás...** gombra kattintva nyissa meg a **Társítás hozzáadása** párbeszédablakot.
8. Ha a mezők kitöltéséhez további információkra van szüksége, akkor kattintson a **Súgó** gombra.
9. A szükséges információk megadása után kattintson az **OK** gombra.

Társítás törlése
Adminisztrációs vagy forrás társítás törléséhez azonosító adminisztrátori vagy EIM adminisztrátori jogosultsággal kell rendelkeznie. Cél társítás törléséhez rendelkeznie kell adminisztrátori jogosultsággal a kijelölt nyilvántartásokhoz (beleértve azt is, amelyet kezelni kíván), esetleg nyilvántartás adminisztrátornak vagy EIM adminisztrátornak kell lennie.

Társítás törléséhez tegye a következőket.
1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Csatlakoznia kell a kezelni kívánt EIM tartományhoz:
   - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg az EIM tartomány hozzáadása a Tartománykezelés mappához című témakört.
   - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás EIM tartományhoz című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson az **Azonosítók** elemre.
5. Kattintson a jobb egérgombbal a kívánt EIM azonosítóra, majd válassza az előugró menü **Tulajdonságok...** menüpontját.
6. Kattintson a **Társítások** lapra az EIM azonosító aktuális társításainak megjelenítéséhez.
7. Válassza ki az eltávolítani kívánt társítást.
8. A társítások eltávolításához kattintson az **Eltávolítás** gombra.
9. Kattintson az **OK** gombra.

EIM azonosítók kezelése
A hálózati felhasználókat képviselő EIM azonosítók kezelése biztonság szempontból kritikus fontosságú. A vállalati felhasználók folyamatosan mozgásban vannak: újak jönnek, néhányan elmennek vagy munkakört váltanak. A változásokkal együtt jár a felhasználói fiókok jogosultságaik nyomon követésének szükségessége. Ezt a nyomon követést teszi egyszerűvé az EIM azonosítók létrehozása és felhasználói azonosságokhoz társítása.

Az egyszeri bejelentkezés kialakítása lényegesen leegyszerűsíti a felhasználók életét, és ez arra is igaz, amikor a felhasználó munkakört vált a vállalaton belül. Ilyenkor módosítani kell biztonsági jogosultságaikat és a rendszerek elérhetőségét. Egyszeri bejelentkezés kialakítása esetén a felhasználóknak az új rendszerekhez nem kell új felhasználói neveket és jelszavakat megjegyezniük.

A vállalaton belüli felhasználók EIM azonosítóinak kezelése számos rutinfeladatot jelent. A hálózat és tartományok EIM azonosítóinak kezeléséhez válasszon a következő feladatok közül:
- EIM azonosító létrehozása
- Álnév hozzáadása EIM azonosítóhoz
- EIM azonosító törlése

A társítások kezelésére vonatkozó tudnivalókat a Társítások kezelése című témakörben találja.

EIM azonosító létrehozása
EIM azonosító létrehozásához azonosító adminisztrátori vagy EIM adminisztrátori jogosultság szükséges.

Ha egy személy vagy entitás számára EIM azonosítót szeretne létrehozni, akkor tegye a következőket:
1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.

2. Csatlakoznia kell a kezelni kívánt EIM tartományhoz:
   - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg az EIM tartomány hozzáadása a Tartománykezelés mappához című témakört.
   - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás EIM tartományhoz című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson a jobb egérgombbal az **Azonosítók** elemre, majd válassza az előugró menü **Új azonosító...** menüpontját.
5. Ha a mezőkkel kapcsolatban további információkra van szüksége, akkor kattintson a **Súgó** gombra.
6. Ha megadta a szükséges információkat, akkor kattintson az **OK** gombra.

Álnév hozzáadása EIM azonosítóhoz

Elképzelhető, hogy egy EIM azonosító további megkülönböztetéséhez szükség van egy álnév létrehozására. Az álnév segítségével különíthetők el egymástól az EIM azonosítók. Ha a vállalatnál két Kovács S. János nevű személy dolgozik, akkor érdemes létrehozni például egy Kovács Sándor János és egy Kovács Sámuel János álnevet a felhasználók azonosságainak egyszerűbb megkülönböztetése érdekében.

Álnév hozzáadásához azonosító adminisztrátori vagy EIM adminisztrátori jogosultság szükséges.

Ha egy EIM azonosítóhoz álnevet kíván hozzáadni, akkor tegye a következőket.

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Csatlakoznia kell a kezelni kívánt EIM tartományhoz:
   - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg az EIM tartomány hozzáadása a Tartománykezelés mappához című témakört.
   - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson a jobb egérgombbal a kívánt EIM azonosítóra, majd válassza az előugró menü **Tulajdonságok** menüpontját. Ha nincsenek EIM azonosítók, akkor nézze meg az EIM azonosítók létrehozása című témakört.
5. Adja meg az EIM azonosítóhoz hozzáadni kívánt álnevet, majd kattintson a **Hozzáadás** gombra.
6. A módosítások mentéséhez kattintson az **OK** gombra.

EIM azonosító törlése

EIM azonosító törléséhez EIM adminisztrátori jogosultság szükséges.

EIM azonosító törléséhez tegye a következőket:

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Csatlakoznia kell a kezelni kívánt EIM tartományhoz:
   - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg az EIM tartomány hozzáadása a Tartománykezelés mappához című témakört.
   - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson az **Azonosítók** elemre.
5. Válassza ki a törölni kívánt EIM azonosítókat.
6. Kattintson a jobb egérgombbal a kijelölt EIM azonosítókon, majd válassza az előugró menü **Törlés** menüpontját.
7. A kijelölt EIM azonosítók eltávolításához kattintson a **Törlés megerősítése** párbeszédablak **Igen** gombjára.

EIM felhasználói jogosultságok kezelése

Az EIM számos jogosultságot határoz meg a tartományban végrehajtandó műveletekhez. Ilyen tartománykezelési funkció például az azonosítók létrehozása, a nyilvántartások listázása és a leképezés kikeresési műveletek végrehajtása. Csak az EIM adminisztrátori jogosultsággal rendelkező felhasználók adományozhatják és vonhatják vissza más felhasználók jogosultságait.

Az egyes jogosultsági csoportok leírását, illetve az EIM funkciók végrehajtásához szükséges hozzáférési szintek listáját az EIM jogosultságok című témakörben találja.

Egy felhasználó EIM jogosultságainak módosításához tegye a következőket:

1. Az iSeries navigátorban bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Bontsa ki a kezelni kívánt EIM tartományt. Ha nem csatlakozik a tartományhoz, akkor a rendszer felszólítja a csatlakozásra. Győződjön meg róla, hogy a tartományhoz EIM adminisztrátori jogosultsággal rendelkező felhasználóval csatlakozik.
3. Kattintson a jobb egérgombbal az EIM tartományon, majd válassza az előugró menü **Jogosultság...** menüpontját.
4. Az **EIM jogosultság szerkesztése** párbeszédablakban jelölje ki a felhasználót, amelynek módosítani kívánja jogosultságait.
5. Kattintson az **OK** gombra.
6. Az **EIM jogosultság szerkesztése** párbeszédablakban végezze el a felhasználó jogosultságainak módosítását.
7. Ha végzett, akkor a jogosultságok változásainak mentéséhez kattintson az **OK** gombra.

Felhasználói nyilvántartások kezelése

Mielőtt társításokat hozhatna létre a felhasználói nyilvántartásokban található azonosságok és a megfelelő EIM azonosítók között, először meg kell határoznia a felhasználói nyilvántartást az EIM tartományban:

Az EIM tartományok felhasználói nyilvántartásainak kezelése a következő feladatok végrehajtását jelenti.

- Felhasználói nyilvántartás hozzáadása
- Álnév hozzáadása felhasználói nyilvántartáshoz
- Saját felhasználói nyilvántartás meghatározása
- Felhasználói nyilvántartás eltávolítása
- Felhasználói nyilvántartás álnevének eltávolítása

Felhasználói nyilvántartás hozzáadása

Felhasználói nyilvántartás hozzáadásához EIM adminisztrátor jogosultság szükséges. A jogosultságra vonatkozó részleteket, illetve a jogosultság birtokában végrehajtható tevékenységeket az EIM jogosultságok című témakör tárgyalja.

Ha felhasználói nyilvántartást szeretne egy EIM tartományhoz hozzáadni, akkor tegye a következőket.

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Csatlakozzon az EIM tartományhoz egy EIM adminisztrátor jogosultságú felhasználóval.
   - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg az EIM tartomány hozzáadása a Tartománykezelés mappához című témakört.
   - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson a jobb egérgombbal a **Felhasználói nyilvántartások** lehetőségre, majd válassza az előugró menü **Nyilvántartás hozzáadása...** menüpontját.

5. Adja meg a szükséges felhasználói nyilvántartás információkat. A felhasználói nyilvántartás számára álnév információkat is megadhat.
6. Kattintson az **OK** gombra az információk mentéséhez és a felhasználói nyilvántartás felvételéhez az EIM tartományba.

Álnév hozzáadása felhasználói nyilvántartáshoz

Elképzelhető, hogy egy alkalmazásfejlesztő létre szeretne hozni egy álnevet, hogy további megkülönböztető információval rendelkezzen egy felhasználói nyilvántartásról. Az álnév segítségével különíthetők el egymástól a felhasználói nyilvántartások. Az alkalmazásfejlesztők és adminisztrátorok például egy álnév segítségével határozhatják meg az alkalmazások által használandó EIM nyilvántartásokat. A felhasználói nyilvántartások álnévvel ellátásáról további információkat az EIM nyilvántartás meghatározások című témakörben talál.

Ha egy felhasználói nyilvántartáshoz álnevet kíván rendelni, akkor EIM adminisztrátor vagy nyilvántartás adminisztrátor jogosultsággal kell rendelkeznie a kérdéses nyilvántartásra vonatkozóan.

EIM tartományban lévő felhasználói nyilvántartás álnév hozzáadásához tegye a következőket:

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Csatlakoznia kell a kezelni kívánt EIM tartományhoz:
   - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg az EIM tartomány hozzáadása a Tartománykezelés mappához című témakört.
   - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson a **Felhasználói nyilvántartások** elemre a tartományban lévő nyilvántartások listájának megjelenítéséhez.
5. Kattintson a jobb egérgombbal a felhasználói nyilvántartásra, amelynek álnevet kíván adni, majd válassza az előugró menü **Tulajdonságok...** menüpontját.
6. Kattintson a **Tulajdonságok** párbeszédablak **Álnév** lapjára.
7. Határozza meg a hozzáadni kívánt álnév nevét és típusát. Olyan álnév típust is meghatározhat, amely nem szerepel a típusok listáján.
8. Kattintson a **Hozzáadás** gombra.
9. A módosítások mentéséhez kattintson az **OK** gombra.

Saját felhasználói nyilvántartás meghatározása

Ha olyan felhasználói nyilvántartást kíván meghatározni, amelyet az EIM alapértelmezésben nem ismer, akkor a nyilvántartás típusát **Objektumazonosító-normalizálás** formában kell megadni, ahol az **Objektumazonosító** egy pontozott decimális objektumazonosító, a **normalizálás** pedig a **caseExact** vagy **caseIgnore** értékek valamelyike. Az OS/400 objektumazonosítója (OID) például 1.3.18.0.2.33.2-caseIgnore.

Egyedi OID értékek létrehozása és használata érdekében a szükséges OID értékeket jogosult OID bejegyzési hatóságoktól kell beszerezni. Az egyedi OID értékek segítenek elkerülni a más szervezetek által létrehozott OID értékekkel bekövetkező ütközések lehetőségét.

Az objektumazonosítók kétféleképpen szerezhetők be:

- **Objektumok bejegyeztetése egy hatósággal**.
  Ez a megoldás akkor célravezető, ha kis számú rögzített objektumazonosítót használ az információk ábrázolására. Ezek az objektumazonosítók például a vállalati felhasználók igazolás házirendjeit képviselhetik.
- **Szerezzen jogosítványt egy hatóságtól, és szükségleteinek megfelelően határozzon meg saját objektumazonosítókat**.
  Ez a módszer, amely egy pontozott decimális objektumazonosító-tartomány használatára jogosítja fel, abban az esetben jó választás, ha nagy számú objektumazonosítót használ, vagy az OID

hozzárendelések változhatnak. A jogosítvány tartalmaz egy kezdő pontozott decimális számot, ezt kell felhasználnia saját **objektumazonosítóinak** kiindulási alapjaként. Ez lehet például 1.2.3.4.5.. Ebben az esetben OID értékek létrehozásához ehhez kell hozzáadni. A létrehozható objektumazonosítók formátuma például 1.2.3.4.5.x.x.x lehet.

Objektumazonosítók hatósági bejegyeztetéséről további információkat a következő webhelyeken talál:

- A Nemzetközi Szabványosítási Szervezet (ISO) és a Nemzetközi Telekommunikációs Unió (ITU) által megállapított globális bejegyzési folyamat hatálya alá tartozó szervezeti nevek amerikai bejegyzési hatósága az Amerikai Nemzeti Szabványügyi Hivatal (ANSI). A jelentkezési lapra mutató hivatkozásokat is tartalmazó összefoglalót az ANSI webhelyén találja a http://web.ansi.org/public/services/reg_org.html címen. A szervezetek számára kiadható objektumazonosítók kezdőértéke 2.16.840.1. Az ANSI díjat számol fel az OID jogosítványok kiadása után. Az ANSI megközelítőleg két hét elteltével adja ki az OID jogosítványokat. Az ANSI az új OID jogosítvány létrehozása során egy számot (ÚJSZÁM) rendel a jogosítványhoz: 2.16.840.1.ÚJSZÁM.
- A legtöbb országban a nemzeti szabványügyi hivatal saját OID nyilvántartással rendelkezik. Az ANSI jogosítványhoz hasonlóan általában ezeket a jogosítványokat a 2.16 számú OID alatt bocsátják ki. Előfordulhat, hogy az adott országban hosszas utánajárás szükséges az OID hatóság megtalálásához.

  Az ISO nemzeti tagszervezeteinek címei a http://www.iso.ch/addresse/membodies.html helyen találhatók. Az információk között a postacím és az elektronikus levélcím is megtalálható. Több esetben az adott szervezethez tartozó webhely címe is megjelenik.
- A keresés másik kiindulópontja az ISO DCC NSAP sémák nemzetközi regisztere lehet. Az NSAP rövidítés a Hálózati szolgáltatáshozzáférési pontra utal, amely több nemzetközi szabványnak részét képezi. A sémák nyilvántartása a http://www.fei.org.uk címen kérhető az ISO DCC NSAP kategóriában. A webhely jelenleg 13 névkibocsátó hatóság elérhetőségi információit tartalmazza, és ezek közül néhányan objektumazonosítók kibocsátásával is foglalkoznak.
- Az Interneten kibocsátott számok hatósága (IANA) magánvállalati számokat bocsát ki az 1.3.6.1.4.1. tartományban. Az IANA eddig több mint 7500 cég számára bocsátott ki jogosítványokat. A jelentkezési lap a http://www.iana.org/cgi-bin/enterprise.pl címen, a Magánvállalati számok kategóriában található. Az IANA általában egy hét elteltével válaszol. Az IANA által kibocsátott OID ingyenes. Az IANA egy számot is kibocsát (ÚJSZÁM), így az új OID jogosítvány száma 1.3.6.1.4.1.ÚJSZÁM lesz.
- Az Egyesült Államok Szövetségi Kormánya tartja fenn a Számítógépes biztonsági objektumok nyilvántartását (CSOR). A CSOR a 2.16.840.1.101.3 tartomány elnevezési hatósága, és jelenleg biztonsági címkék, kriptográfiai algoritmusok és igazolás irányelvek számára regisztrál objektumokat. Az igazolás irányelv objektumazonosítókat a 2.16.840.1.101.3.2.1 számú OID határozza meg. A CSOR az Egyesült Államok Szövetségi Kormányához tartozó ügynökségek számára biztosít irányelv objektumazonosítókat. A CSOR működésével kapcsolatban további információkat a http://csrc.nist.gov/csor/ címen talál.

Az igazolás irányelvek objektumazonosítóiról további információkért keresse fel a http://csrc.nist.gov/csor/pkireg.htm webhelyet.

Felhasználói nyilvántartás eltávolítása

Ha eltávolít egy felhasználói nyilvántartást az EIM tartományból, akkor ezzel a felhasználói nyilvántartásban található felhasználói azonosságok és az EIM azonosítók között létrejött összes társítás elvész. Ha az eltávolítás után ismét hozzáadja a felhasználói nyilvántartást az EIM tartományhoz, akkor nem állnak vissza a társítási viszonyok.

Felhasználói nyilvántartás eltávolításához EIM adminisztrátor jogosultság szükséges.

Felhasználói nyilvántartás eltávolításához tegye a következőket:

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Csatlakoznia kell a kezelni kívánt EIM tartományhoz.

- Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg az EIM tartomány hozzáadása a Tartománykezelés mappához című témakört.
- Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.

3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson a **Felhasználói nyilvántartások** menüpontra a tartomány felhasználói nyilvántartásainak megjelenítéséhez.
5. Kattintson a jobb egérgombbal az eltávolítani kívánt felhasználói nyilvántartásra, majd válassza az előugró menü **Törlés...** menüpontját.
6. A felhasználói nyilvántartás törléséhez kattintson a **Megerősítés** párbeszédablak **Igen** gombjára.

Felhasználói nyilvántartás álnevének eltávolítása

Felhasználói nyilvántartás álnevének eltávolításához a kijelölt nyilvántartások nyilvántartás adminisztrátorának kell lennie, vagy EIM adminisztrátori jogosultsággal kell rendelkeznie.

EIM tartomány felhasználói nyilvántartásához tartozó álnév eltávolításához tegye a következőket:

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Csatlakoznia kell a kezelni kívánt EIM tartományhoz:
   - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg az EIM tartomány hozzáadása a Tartománykezelés mappához című témakört.
   - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson a **Felhasználói nyilvántartások** elemre a tartományban lévő nyilvántartások listájának megjelenítéséhez.
5. Kattintson a jobb egérgombbal arra a felhasználói nyilvántartásra, amelyből álnevet kíván eltávolítani, majd válassza az előugró menü **Tulajdonságok** menüpontját.
6. Kattintson a **Tulajdonságok** párbeszédablak **Álnév** lapjára.
7. Válassza ki az eltávolítani kívánt álnevet, majd kattintson az **Eltávolítás** gombra.
8. A módosítások mentéséhez kattintson az **OK** gombra.

EIM alkalmazásprogram illesztők

Az EIM számos alkalmazásprogram illesztővel (API) rendelkezik, amelyekkel az alkalmazások EIM műveleteket hajthatnak végre az alkalmazás vagy az alkalmazás felhasználójának nevében. Az API-k segítségével azonosság kikeresési műveletekre, különféle EIM kezelési és konfigurációs funkciókra, illetve módosítási és lekérdezési tevékenységekre van lehetőség.

Az EIM API-k az alábbi kategóriákhoz tartozhatnak:

- EIM kapcsolatazonosító és kapcsolat műveletek
- EIM tartomány adminisztráció
- Nyilvántartás műveletek
- EIM azonosító műveletek
- EIM társítások kezelése
- EIM leképezés kikeresési műveletek
- EIM jogosultságkezelés

Azok az alkalmazások, amelyek ezen API-k segítségével kezelik és használják az EIM tartományokban található EIM információkat, általában a következő programozási modell alapján működnek:

1. EIM kapcsolatazonosító szerzése

2. Csatlakozás egy EIM tartományhoz
3. Az alkalmazás szokásos tevékenysége
4. EIM adminisztrációs vagy azonosság leképezés kikeresési művelet API használata
5. Az alkalmazás szokásos tevékenysége
6. A befejezés előtt az EIM kapcsolatazonosító megsemmisítése

A rendelkezésre álló EIM alkalmazásprogram illesztőre vonatkozó részletes információkat, illetve ezek részletes listáját a Vállalati azonosság leképezés (EIM) API-k című témakörben találja.

EIM hibaelhárítás

Az EIM számos technológiát, alkalmazást és funkciót ötvöz. Ennek megfelelően a problémák hibaelhárítása is szerteágazó lehet, ezért válasszon az alábbi témakörök közül a kapcsolódó általános hibák megtekintésére és kijavítására vonatkozó részletes információk megtekintéséhez.

- Nem lehet csatlakozni a tartományvezérlőhöz
- Az EIM azonosítók listázása hosszú ideig tart
- Az EIM konfigurációs varázsló lefagy a befejezés során
- Az EIM kapcsolatazonosító már nem érvényes
- Kerberos hitelesítési és diagnosztikai üzenetek

Nem lehet csatlakozni a tartományvezérlőhöz

A tartományvezérlő kapcsolatának sikertelensége számos okra vezethető vissza. A probléma okának meghatározásához ellenőrizze a következőket:

- Ellenőrizze az alábbiak megfelelő beállítását:
  - Tartományvezérlő neve
  - Portszám
  - Felhasználói azonosító és jelszó
- Ellenőrizze, hogy a tartományvezérlő aktív-e. Ha a tartományvezérlő egy iSeries szerver, akkor az iSeries navigátorban tegye a következőket:
  1. Bontsa ki a **Hálózat —> Szerverek —> TCP/IP** kategóriát.
  2. Győződjön meg róla, hogy a Címtár szerver állapota **Elindult**. Ha a szerver áll, akkor kattintson a jobb egérgombbal a **Címtár szerver** bejegyzésre, majd válassza az előugró menü **Indítás...** menüpontját.

A tartományvezérlő aktiválása után próbálkozzon újra a csatlakozással.

1. Bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Válassza ki a tartományt, amelyhez csatlakozni kíván. Ha a listában nincsenek EIM tartományok, vagy a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg az EIM tartomány hozzáadása a Tartománykezelés mappához című témakört.
3. Kattintson a jobb egérgombbal az EIM tartományra, amelyhez csatlakozni kíván, majd válassza az előugró menü **Csatlakozás...** menüpontját.
4. Az EIM tartományvezérlőre csatlakozáshoz adja meg a felhasználó típusát, és a szükséges felhasználói információkat.
5. Kattintson az **OK** gombra.

Az EIM azonosítók listázása hosszú ideig tart

Az iSeries navigátor Azonosítók mappájának megnyitásakor az azonosítók listájának összeállítása hosszú ideig tart. Ha a tartományban nagy számú EIM azonosító található, akkor érdemes szűkíteni a megjelenítendő EIM azonosítók listáját.

Az EIM azonosítók megjelenésének testreszabásához tegye a következőket:

1. Az iSeries navigátorban bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Bontsa ki a tartományt, amelynek EIM azonosítóit meg kívánja jeleníteni.
3. Kattintson a jobb egérgombbal az **Azonosítók** elemre, majd válassza az előugró menü **Nézet testreszabása —> Tartalmazás...** menüpontját.
4. Válassza ki a kívánt megjelenítési feltételeket. Helyettesítő karakterként a csillag (*) használható.
5. Kattintson az **OK** gombra.

Az **Azonosítók** következő kiválasztásakor a megjelenő EIM azonosítók a fentiekben megadott feltételeknek megfelelő elemekre korlátozódnak. Az összes EIM azonosító megtekintéséhez a fenti lépések ismételt végrehajtásával válassza ki az egyéni nézetben a **Minden azonosító** beállítást.

Az EIM konfigurációs varázsló lefagy a befejezés során

Ha a varázsló a befejezés során úgy tűnik, mintha lefagyott volna, akkor elképzelhető, hogy a varázsló a tartományvezérlő indítására vár. Ellenőrizze, hogy az LDAP szerver indítása során történtek-e hibák. iSeries szerverek esetén ellenőrizze a QSYSWRK alrendszer QDIRSRV munkanaplóját.

A munkanapló ellenőrzéséhez tegye a következőket:

1. Az iSeries navigátorban bontsa ki a **Jobkezelés —> Alrendszerek —> Qsyswrk** elemet.
2. Kattintson a jobb egérgombbal a **Qdirsrv** bejegyzésen, majd válassza az előugró menü **Munkanapló** menüpontját.

Az EIM kapcsolatazonosító már nem érvényes

Az EIM iSeries navigátorban végzett kezelése során elképzelhető, hogy hibaüzenet érkezik, amely szerint az EIM kapcsolatazonosító a továbbiakban már nem érvényes, és a tartományvezérlő kapcsolata megszakadt.

Az újracsatlakozáshoz tegye a következőket:

1. Az iSeries navigátorban bontsa ki a **Hálózat —> Vállalati azonosság leképezés (EIM) —> Tartománykezelés** mappát.
2. Kattintson a jobb egérgombbal a kezelni kívánt tartományra, majd válassza az előugró menü **Újracsatlakozás...** menüpontját.
3. Adja meg a kapcsolati információkat.
4. Kattintson az **OK** gombra.

Kerberos hitelesítési és diagnosztikai üzenetek

Ha Kerberos protokollt használt az EIM hitelesítéshez, akkor a munkanaplóba CPD3E3F diagnosztikai üzenet kerül minden egyes alkalommal, amikor egy hitelesítési vagy azonosság leképezési művelet meghiúsul. A diagnosztikai üzenetben egy fő és egy al állapotkód jelzi a hiba bekövetkezésének helyét. A legáltalánosabb hibákat és ezek helyreállítását az üzenet is megadja.

A probléma helyreállításához hívja segítségül a diagnosztikai üzenet súgóját.

EIM kapcsolódó információk

Ez a szakasz sorolja fel a Vállalati azonosság leképezéshez (EIM) kapcsolódó egyéb technológiák információforrásait. A kapcsolódó technológiák megértésében az Információs központ alábbi témakörei nyújthatnak segítséget:

- **Hálózati hitelesítési szolgáltatás**
  Ez a témakör írja le az iSeries Hálózati hitelesítési szolgáltatás beállítását. A Hálózati hitelesítési

szolgáltatás teszi lehetővé az iSeries szervereknek a Kerberos hálózatokban való részvételt. A Vállalati azonosság leképezéssel (EIM) együtt használva a Hálózati hitelesítési szolgáltatás alkalmas egyszeri bejelentkezést biztosító környezet kialakítására.

- **Címtár szolgáltatások (LDAP)**
  Ez a témakör ismerteti a Címtár szolgáltatások (LDAP) konfigurációjának alapelveit. Az EIM LDAP szerveren tárolja az EIM adatokat és leképezési társításokat.

Nyomtatva Dániában