

IBM

@server

iSeries

Vállalati azonosság leképezés (EIM)

V5R3







@server

iSeries

Vállalati azonosság leképezés (EIM)

*V5R3*

**Megjegyzés**

A kiadvány és a tárgyalt termék használatba vétele előtt olvassa el a “Megjegyzések” oldalszám: 119 szakasz általános információit.

**Negyedik kiadás (2005. augusztus)**

| Ez a kiadás az IBM Operating System/400 (termékszám: 5722–SS1) V5R3M0 kiadására, illetve minden ezt követő változatra és  
| módosításra vonatkozik mindaddig, amíg az újabb kiadások ezt másképp nem jelzik. Ez a változat nem fut minden csökkentett  
| utasításkészletű (RISC) rendszeren, illetve a CISC modelleken.

© Szerzői jog IBM Corporation 2002, 2005. Minden jog fenntartva

---


# Tartalom

<b>Vállalati azonosság leképezés (EIM)</b> . . . . .	<b>1</b>	Vállalati azonosság leképezés (EIM) kezelése . . . . .	79
A V5R3 újdonságai . . . . .	2	Vállalati azonosság leképezés (EIM) tartományok kezelése . . . . .	80
A témakör nyomtatása . . . . .	2	Vállalati azonosság leképezés nyilvántartás meghatározások kezelése . . . . .	84
Vállalati azonosság leképezés (EIM) áttekintés . . . . .	3	Vállalati azonosság leképezés (EIM) azonosítók kezelése . . . . .	90
Vállalati azonosság leképezés (EIM) példahelyzetek . . . . .	5	Társítások kezelése . . . . .	93
Vállalati azonosság leképezés (EIM) alapelvek . . . . .	6	EIM hozzáférés felügyelet kezelése . . . . .	108
EIM tartományvezérlő . . . . .	7	EIM konfigurációs tulajdonságok kezelése . . . . .	109
EIM tartomány . . . . .	7	Vállalati azonosság leképezés (EIM) alkalmazásprogram illesztők . . . . .	110
EIM azonosító . . . . .	9	Vállalati azonosság leképezés (EIM) hibaelhárítása . . . . .	110
EIM nyilvántartás meghatározások . . . . .	12	Tartományvezérlő kapcsolat problémák hibaelhárítása . . . . .	110
EIM társítások . . . . .	16	Általános EIM konfigurációs- és tartományproblémák hibaelhárítása . . . . .	113
Vállalati azonosság leképezés (EIM) kikeresési műveletek . . . . .	25	Vállalati azonosság leképezés (EIM) hibaelhárítás: leképezési hibák . . . . .	114
Vállalati azonosság leképezés: leképezés irányelv támogatás és engedélyezése . . . . .	33	Vállalati azonosság leképezés (EIM) kapcsolódó információk . . . . .	117
EIM hozzáférés felügyelet . . . . .	34	Az információk letöltésére és kinyomtatására vonatkozó feltételek . . . . .	117
EIM LDAP alapelvek . . . . .	40	<b>Megjegyzések . . . . .</b>	<b>119</b>
iSeries Vállalati azonosság leképezés (EIM) alapelvek . . . . .	43	Védjegyek . . . . .	121
Vállalati azonosság leképezés (EIM) megtervezése . . . . .	44	Az információk letöltésére és kinyomtatására vonatkozó feltételek . . . . .	122
Vállalati azonosság leképezés (EIM) megtervezése . . . . .	44		
eServer rendszeren . . . . .	45		
Vállalati azonosság leképezés (EIM) megtervezése . . . . .	45		
OS/400 rendszeren . . . . .	59		
Vállalati azonosság leképezés (EIM) beállítása . . . . .	62		
Új helyi tartomány létrehozása és csatlakozás . . . . .	63		
Új távoli tartomány létrehozása és csatlakozás . . . . .	68		
Csatlakozás meglévő tartományhoz . . . . .	73		
Biztonságos kapcsolat kialakítása az EIM tartományvezérlővel . . . . .	79		



---

## Vállalati azonosság leképezés (EIM)

| Az Enterprise Identity Mapping (EIM) for iSeries az OS/400 megvalósítása az IBM  infrastruktúrájának, melynek lehetővé teszi az adminisztrátorok és alkalmazásfejlesztők számára a vállalaton belüli több felhasználói azonosság problémájának kezelését. 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 segítségével azonosság leképezések, másnéven társítások rendszerét hozhatja létre egy személy különböző felhasználói nyilvántartásokban található felhasználói azonosságai között. Az EIM egy általános API készletet is biztosít, amelyet a különböző platformok között használhatnak az azonosság leképezést támogató alkalmazások a felhasználói azonosságok közötti kapcsolatok feltárására. Továbbá az EIM képes együttműködni a Hálózati hitelesítési szolgáltatással, a Kerberos OS/400 megvalósításával, és ezáltal kialakítható egy egyszerű bejelentkezési környezet.

Az EIM konfigurálható és kezelhető az iSeries navigátorból, az iSeries grafikus felhasználói felületéből. Az iSeries szerver 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 elfogadják Kerberos jegyeket is, és az EIM segítségével keresik ki a Kerberos jegyet képviselő személynek megfelelő felhasználói profilt.

Az EIM működésével, az alapfogalmakkal és az EIM vállalati felhasználásával kapcsolatban tekintse át az alábbi témaköröket:

A témakör nyomtatása

A témakör és más kapcsolódó témakörök PDF változatának kinyomtatása.

| A V5R3 újdonságai

| Ismerje meg az EIM új funkcióit.

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 ismerheti meg az EIM sikeres megvalósításához szükséges fontos legfontosabb EIM alapelveket.

EIM tervezése

Ismerje meg, hogyan kell megtervezni az EIM megvalósítását a sikeres iSeries vagy kevert környezetbe bevezetés érdekében.

EIM beállítása

Ismerje meg, hogyan kell a Vállalati azonosság leképezés (EIM) konfigurációs varázsló segítségével elvégezni az EIM beállítását az iSeries szervereken.

EIM kezelése

Ismerkedjen meg az EIM tartomány és tartományadatok kezelésével, ideértve az EIM tartományok, az azonosítók, a nyilvántartás meghatározások, az EIM hozzáférés felügyelet kezelését, és így tovább.

EIM API hívások

Ismerje meg az EIM API hívásokat, és tanulja meg a használatukat az alkalmazásokban és a hálózaton.

EIM hibaelhárítás

Ismerkedjen meg az EIM használata során gyakran felbukkanó problémákkal és hibákkal, valamint a lehetséges megoldásukkal.

EIM kapcsolódó információk

Ismerje meg az EIM használatához kapcsolódó egyéb forrásokat és információkat.

---


## A V5R3 újdonságai

Az iSeries V5R3 Vállalati azonosság leképezés (EIM) továbbfejlesztései és a kapcsolódó OS/400 továbbfejlesztések:

### Új vagy bővített EIM funkció

- **Funkciók összehangolása varázsló.** Az iSeries navigátor **Funkciók összehangolása** varázslójának segítségével egy csoport V5R3 rendszerre terjesztheti a Hálózati hitelesítési szolgáltatást és az EIM konfigurációt. A varázsló a modell rendszer konfigurációját és a csoportban szereplő többi rendszerre másolja. Ha egyszer végzi el a beállítást, majd a konfigurációt átmásolja a többi gépre, akkor időt takarít meg ahhoz képest, mintha minden rendszert egyedileg konfigurálna. A technikai és konfigurációs részleteket a Hálózati hitelesítési szolgáltatás és EIM terjesztése több rendszerre példahelyzetben találja.
- **leképezés irányelv támogatás.** Az EIM leképezés irányelv támogatásának segítségével az adminisztrátorok az irányelv társításokat az egyedi azonosító társításokhoz hasonló módon használhatják az EIM tartományban. Az irányelv társítások segítségével közvetlen viszonyt határozhat meg különböző felhasználói nyilvántartásokban szereplő felhasználói azonosságok között. Egy irányelv társítás egy különböző felhasználói nyilvántartásokban található azonosságokból álló halmaz és egy adott cél felhasználói nyilvántartásban található felhasználói azonosság közötti viszony leírására ad módot. Az irányelv társítások használhatók az azonosító társítások helyett, vagy azokkal párhuzamosan, az azonosító társításokat kiegészítve.
- **felhasználói azonosság parancs bővítés.** A Felhasználói profil létrehozása (CRTUSRPRF) és a felhasználói profil módosítása (CHGUSRPRF) parancsok az EIMASSOC paraméterrel bővültek. A paraméter segítségével EIM azonosító társításokat határozhat meg a megadott felhasználói profilhoz a helyi nyilvántartásban. A paraméter használatához adja meg az EIM azonosítót, egy művelet paramétert a társításhoz, az azonosító társítás típusát, és azt, hogy létre kell-e hozni a megadott EIM azonosítót abban az esetben, ha még nem létezik. Az új paraméterről bővebb információkat az "OS/400 felhasználói profilokkal kapcsolatos Vállalati azonosság leképezés megfontolások" oldalszám: 43 résznél talál.



### EIM információk bővítése

Ez a kiadás egy nagymértékben kibővített tervezési részt tartalmaz, amely tetszőleges  platformokon általánosságban, az OS/400 rendszeren konkrétan tárgyalja az EIM tervezésére és megvalósítására vonatkozó információkat.

Az Egyszeri bejelentkezés új Információs központ témakör részletes információkat tartalmaz az EIM megvalósításáról egyszeri bejelentkezési környezet részeként a jelszókezeléssel kapcsolatos teendők csökkentése érdekében. A témakör számos példahelyzetet tartalmaz, amelyek gyakori egyszeri bejelentkezés helyzeteket modelleznek részletekbe menően, és tartalmazzák a megvalósításhoz szükséges konfigurációs lépéseket is.

### Hogyan tudom meg, hogy valami újdonság vagy megváltozott?


A technikai változásokat segítenek figyelemmel kísérni az alábbi jelölések:

- A  kép jelöli a megváltozott vagy új információk kezdetét.
- A  kép jelöli a megváltozott vagy új információk végét.

Ha többet szeretne tudni arról, mi az újdonság és mi változott meg ebben a kiadásban, akkor olvassa el a Felhasználói feljegyzések részt.

---

## A témakör nyomtatása

A PDF változat megjelenítéséhez vagy letöltéséhez válassza ki a Vállalati azonosság leképezést (EIM)  (kb. 1389 KB).

### További információk

A következő kapcsolódó témakörök megtekintésére és letöltésére is lehetőség van:




- Hálózati hitelesítési szolgáltatások (megközelítőleg 1398 KB) - Ez a kiadvány írja le az egyszeri bejelentkezést biztosító környezetek kialakítását a Hálózati hitelesítési szolgáltatás és az EIM együttes felhasználásával.
- Címtárszerver (LDAP) (megközelítőleg 1700 KB) - Ez a kiadvány tárgyalja az EIM tartományvezérlőként használható LDAP szerverek beállítását, illetve körüljár néhány speciális konfigurációs kérdést is.

### PDF fájlok mentése

A PDF fájl mentése a munkaállomáson 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.

### Adobe Acrobat Reader letöltése

A PDF fájlok megjelenítéséhez és nyomtatáshoz szükség van az Adobe Acrobat Reader programra, amely az Adobe honlapjáról ([www.adobe.com/prodindex/acrobat/readstep.html](http://www.adobe.com/prodindex/acrobat/readstep.html))  tölthető le.

---

## Vállalati azonosság leképezés (EIM) áttekintés

Napjaink hálózati környezeteti rendszerek és alkalmazások összetett csoportjai, amelyek egy idő után szükségszerűen vezetnek több felhasználói nyilvántartás fenntartásához. A több felhasználói nyilvántartás kezelése hamar olyan adminisztrációs problémává női 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 meghíúsult bejelentkezések hibaelhárítására és elfelejtett jelszavak alaphelyzetbe állítására fecsérelniük.

A sokféle felhasználói nyilvántartás problémájával az alkalmazásfejlesztők is szembekerülnek, akiknek többretegű 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 kockázatokat 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 bejelentkezéssel 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 többretegű 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 megközelítésének segítségével a vállalatok költséghatékony és egyszerű megoldást építhetnek többszintű, heterogén alkalmazáskörnyezetben több felhasználói nyilvántartás és felhasználói azonosság kezelésére. Az EIM egy olyan architektúra, amellyel leírhatók a vállalat egyéneinek vagy entitásainak (például fájlszerverek vagy nyomtatáserverek) illetve az ezek képviselőit használt számos azonosság közötti viszonyok. Emellett az EIM különféle alkalmazásprogram illesztőket is biztosít ezen viszonyok visszakereséséhez.

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.

Az EIM lehetővé teszi 1-N (más szavakkal amikor egy felhasználó egy felhasználói nyilvántartásban egynél több azonossággal rendelkezik) leképezések megadását. Azonban az adminisztrátornak nem kell a nyilvántartások összes

felhasználói azonosságához egyedi leképezéseket megadnia. EIM ezenkívül lehetővé teszi N-1 leképezések megadását (más szavakkal több felhasználót képez le egyetlen felhasználói azonosságra egy felhasználói nyilvántartásban).

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 használják hitelesítésre, és egy teljesen másikat a jogosultságok kezelésére. Ha például az adminisztrátor bizonyos OS/400 erőforrásokhoz hozzáférést kíván biztosítani egy Windows felhasználónak, akkor leképezheti a Kerberos nyilvántartásban található Windows felhasználói azonosságot egy másik felhasználó nyilvántartásban lévő megfelelő OS/400 felhasználói profilra.

Az EIM nyílt architektúra, amellyel tetszőleges nyilvántartáshoz készíthető azonosság leképezés. Nem igényli a meglévő adatok új lerakatra másolását, hanem megpróbálja szinkronban tartani ezeket. Az EIM által bevezetett egyetlen új információ a viszony. Az EIM ezeket az adatokat LDAP címtárban tárolja, 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.

- | Az EIM valamilyen hálózati hitelesítési szolgáltatással, például a Kerberos OS/400 megvalósításával együtt alkalmazva
- | egyszeri bejelentkezési megoldást biztosít. A GSS API és az EIM segítségével olyan alkalmazások készíthetők,
- | amelyek Kerberos jegyeket fogadnak, és ezeket leképezik egy másik felhasználói nyilvántartásban található társított
- | felhasználói azonosságra. Az azonosság leképezés alapját képező felhasználói azonosságok közötti társítást meg lehet
- | valósítani olyan azonosító társítások segítségével, amelyek közvetlenül képezik le az egyik felhasználói azonosságot a
- | másikkra egy EIM azonosító közbeiktatásával, vagy olyan irányelv társítások segítségével, amelyek közvetlenül
- | hozzárendelnek egy felhasználói azonossághoz egy másikat.

Az azonosság leképezés használatához az adminisztrátoroknak az alábbi teendőket kell elvégezniük:

1. EIN tartomány beállítása a hálózatban. Az iSeries EIM konfigurációs varázsló segítségével hozzon létre egy tartományvezérlőt a tartomány számára és konfigurálja a tartomány elérését. A varázslóval létrehozhat egy új EIM tartományt és egy tartományvezérlőt a helyi vagy egy távoli rendszeren. Ha már létezik egy tartomány, akkor dönthet annak használata mellett is.
2. Állapítsa meg, hogy az EIM tartományvezérlőt kiszolgáló címtárszerveren megadott felhasználók közül melyek jogosultak az EIM tartomány információinak elérésére és kezelésére, és rendelje ezeket a felhasználókat a megfelelő EIM hozzáférés felügyeleti csoportokhoz.
3. Hozza létre az EIM nyilvántartás meghatározásokat az EIM tartományban részvevő felhasználói nyilvántartásokhoz. Az EIM tartományban bármely felhasználói nyilvántartást meghatározhat, de az EIM támogatással rendelkező alkalmazások és operációs rendszerek meghatározása kötelező.
4. Az EIM megvalósítással szemben támasztott követelményektől függően válassza ki az EIM beállításának véglegesítéséhez szükséges feladatokat az alábbiak közül:
  - EIM azonosítók és azonosító társítások létrehozása szükséges minden egyes egyedi felhasználó vagy entitás számára a tartományban.
  - Irányelv társítások létrehozása
  - A fentiek valamely kombinációjának létrehozása

Ha a lehető legkisebbre szeretné csökkenteni a jelszókezeléshez kapcsolódó adminisztrációt, akkor érdemes megfontolni egy egyszeri bejelentkezés környezet létrehozását; az ehhez szükséges EIM információkat az Egyszeri bejelentkezés témakörnél találja az iSeries Információs központban.

---

## | **Vállalati azonosság leképezés (EIM) példahelyzetek**

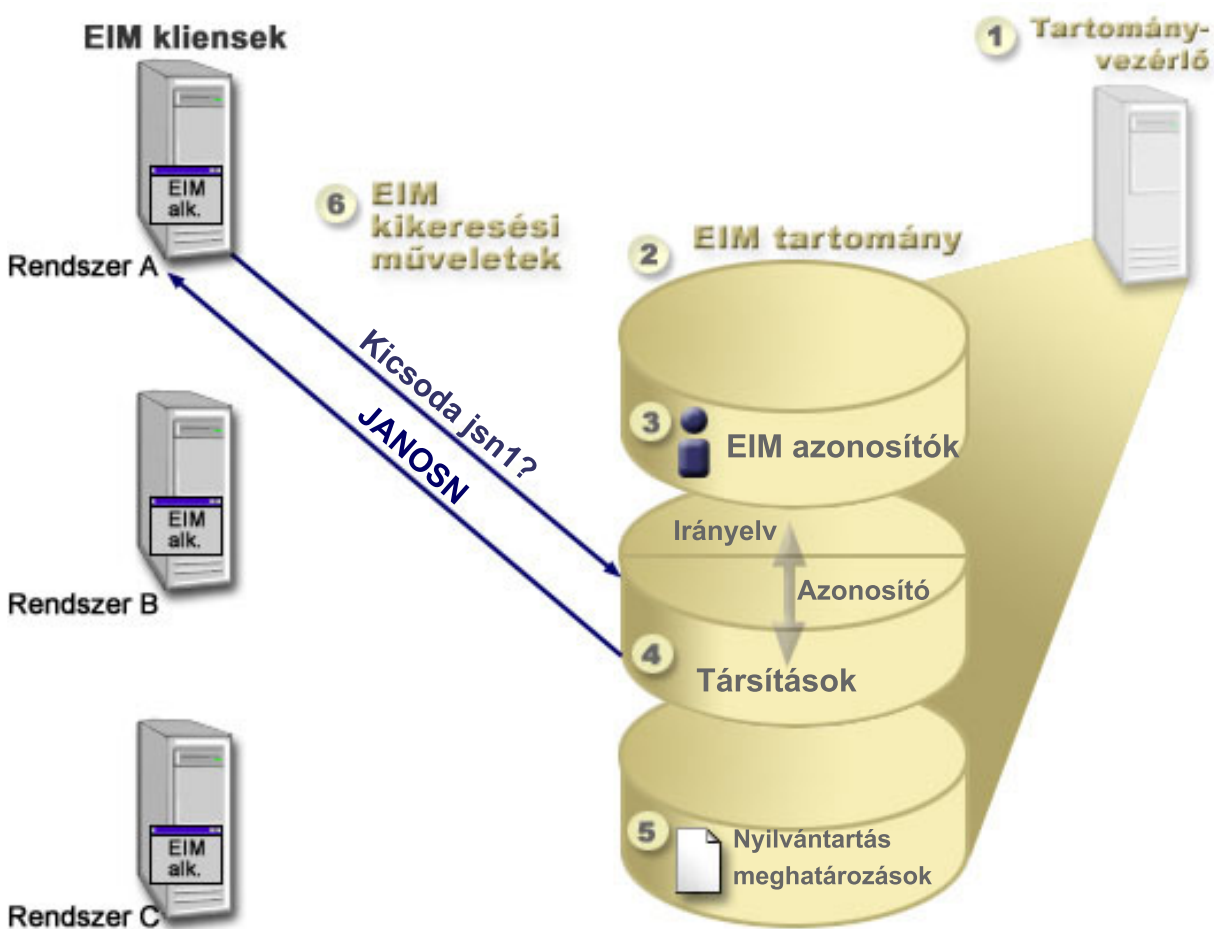
- | A Vállalati azonosság leképezés (EIM) egy IBM infrastruktúra technológia, amely lehetővé teszi a felhasználói
- | azonosság nyomonkövetését és kezelését a teljes vállalati hálózaton. Általában az EIM valamilyen hitelesítési
- | technológiával, például a Hálózati hitelesítési szolgáltatással együtt alkot egyszeri bejelentkezési környezetet.

- | Következésképpen ha érdeklődik az EIM szélesebb körű felhasználása iránt, akkor tekintse át a Példahelyzetek részt az
- | Egyszeri bejelentkezés Információs központ témakörben.

## Vállalati azonosság leképezés (EIM) alapelvek

Az EIM vállalaton belüli felhasználhatóságának megértéséhez meg kell ismerni az EIM alapelveit. Bár az EIM API hívások 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: Egy EIM megvalósítási példa

Az EIM **@server** alapelvekről további információkat az alábbi témakörökből szerezhet:

- “EIM tartományvezérlő” oldalszám: 7
- “EIM tartomány” oldalszám: 7
- “EIM azonosító” oldalszám: 9
- “EIM nyilvántartás meghatározások” oldalszám: 12
- “EIM társítások” oldalszám: 16


- “Vállalati azonosság leképezés (EIM) kikeresési műveletek” oldalszám: 25
- “Vállalati azonosság leképezés: leképezés irányelv támogatás és engedélyezése” oldalszám: 33
- “EIM hozzáférés felügyelet” oldalszám: 34

Tekintse át az alábbi, az EIM használatával kapcsolatos további fontos alapelveket bemutató információkat:

- “EIM LDAP alapelvek” oldalszám: 40
- “iSeries Vállalati azonosság leképezés (EIM) alapelvek” oldalszám: 43

## 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 azonosítók, 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.

Jelenleg az IBM Directory Server képes bizonyos  platformokon EIM tartományvezérlőként működni. Kliensként az EIM alkalmazásprogram illesztőket támogató tetszőleges rendszer része lehet a tartománynak. Ezek a kliens rendszerek az EIM API hívások segítségével lépnek kapcsolatba a tartományvezérlővel “Vállalati azonosság leképezés (EIM) kikeresési műveletek” oldalszám: 25 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*.

**Megjegyzés:** Ha a címtár szervert egy távoli rendszeren tervezi beállítani, akkor győződjön meg róla, hogy a címtár szerver tartalmaz EIM támogatást. Az EIM megköveteli, hogy a tartományvezérlőt 3-as verziójú Egyszerűsített címtárhozzáférési protokollt (LDAP) támogató címtár szerver szolgáltatassa, továbbá hogy a címtár szerver terméknek fogadnia kell az EIM sémát. Az IBM Directory Server for iSeries és az IBM Directory Server V5.1 tartalmazza ezt a támogatást.

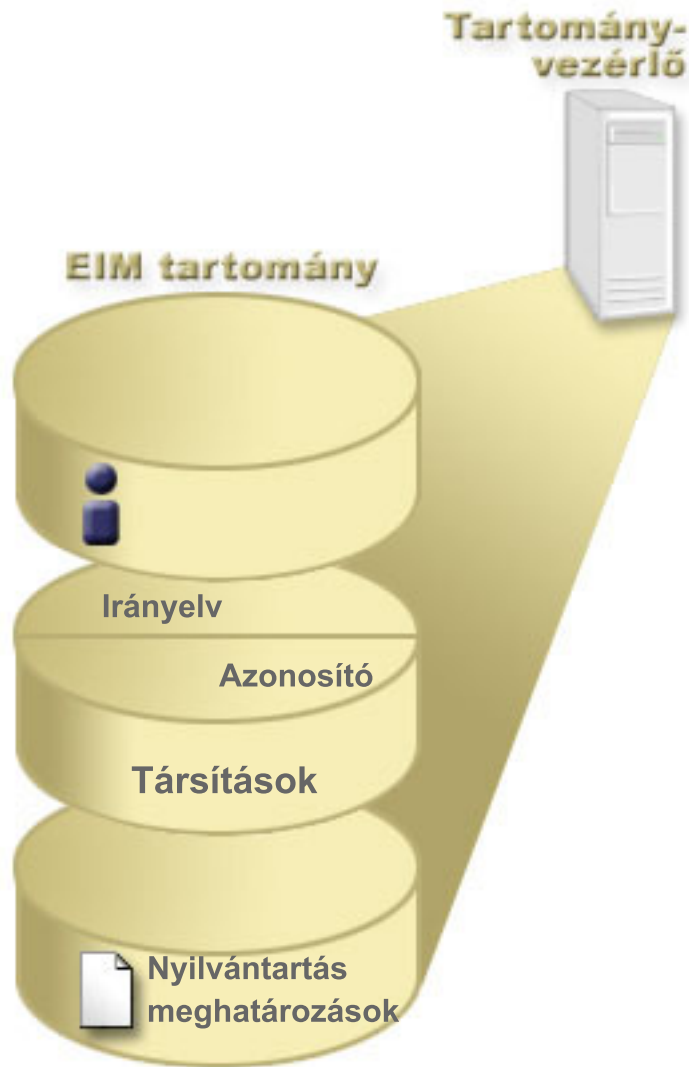
## EIM tartomány

Az *EIM tartomány* egy olyan LDAP címtár, amely a vállalat EIM adatait tartalmazza. Az EIM tartomány EIM azonosítókból, EIM társításokból és felhasználói nyilvántartásokból és az adatok elérését vezérlő hozzáférés felügyeletéből 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.

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 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. Kétfajta
- | nyilvántartás meghatározást hozhat létre: az egyik rendszer felhasználói nyilvántartásokra, a másik alkalmazás
- | felhasználói nyilvántartásokra vonatkozik. Bővebb információkat az “EIM nyilvántartás meghatározások”
- | oldalszám: 12 című témakörben talál.
- | • **EIM azonosítók.** Minden egyes EIM azonosító egy vállalaton belüli személyt vagy entitást (például
- | nyomtatószervert vagy fájlservert) egyedileg képvisel. Akkor van szükség EIM azonosítóra, ha 1-1 leképezéseket
- | kíván létrehozni egyes személyeket vagy entitásokat képviselő felhasználói azonosságok között. Bővebb
- | információkat az “EIM azonosító” oldalszám: 9 című témakörben talál.
- | • **EIM társítások.** Az EIM társítások felhasználói azonosságok közötti viszonyt képviselnek. A társításokat oly
- | módon kell meghatározni, hogy az EIM kliensek az EIM API hívások segítségével sikeres EIM kikeresési
- | műveleteket hajthassanak végre. Ezek az EIM kikeresési műveletek egy EIM tartományban keresnek meghatározott
- | társításokat. További információkat a “Vállalati azonosság leképezés (EIM) kikeresési műveletek” oldalszám: 25
- | című témakörben talál. Két különböző típusú társítást hozhat létre:

- **Azonosító társítások.** Az azonosító társítások felhasználói azonosságok közötti 1-1 leképezések megadását teszik lehetővé egyedi EIM azonosítók segítségével. Az EIM társítások egyetlen egyedi viszonyt képviselnek a vállalaton belüli felhasználói azonosság és a hozzá tartozó EIM azonosító között. Az azonosító társítások által biztosított információk kötik össze az EIM azonosítót egy adott felhasználói nyilvántartásban található felhasználói azonossággal, és segítségével 1-1 azonosság leképezések hozhatók létre a felhasználókhöz. Az azonosság társítások különösen akkor hasznosak, ha egyes különleges jogosultságokkal rendelkező felhasználói azonosságokat kiemelten szeretne kezelni és 1-1 leképezések segítségével biztosítani tulajdonosaiknak.
- **Írányelv társítások.** Az irányelv társítások segítségével közvetlenül képezhet le több, akár különböző felhasználói nyilvántartásokban szereplő felhasználói azonosságot egy másik felhasználói nyilvántartásban található egyetlen cél felhasználói azonosságra. Minden EIM irányelv társítás eredménye egy N-1 leképezés az egyik felhasználói nyilvántartásban található felhasználói azonosságok egy csoportja mint forrás, és egyetlen felhasználói azonosság, mint cél között. Az irányelv társítások általános felhasználási módja, amikor egy csoport hasonló jogosultságokat igénylő felhasználót képez le az adminisztrátor a kívánt jogosultságokkal rendelkező egyetlen felhasználói azonosságra.

Az EIM azonosítók, a nyilvántartás meghatározások és a különböző 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 használata során minden egyes személy vagy entitás egyedi EIM azonosítót kaphat. Ezután létre lehet hozni azonosító társításokat, vagyis 1-1 azonosság leképezéseket egy EIM azonosító és az általa jelképezett személy vagy entitás különböző felhasználói azonosságai között. Ez a folyamat egyszerűbbé teszi heterogén többszintű alkalmazás összeállítását. Egyszerűbbé válik a vállalat személyeihez vagy entitásaihoz kötődő felhasználói azonosságok kezelésével járó adminisztráció.

### Személyt képviselő EIM azonosító

A 3. ábra példaként bemutatja egy *Nap János* nevű személy EIM azonosítóját, és a vállalaton belüli többféle felhasználói azonosságát. A példában *Nap János* öt különböző felhasználói nyilvántartásban négy felhasználói azonossággal rendelkezik: *janosnap*, *jsn1*, *JANOSN*, *jsnap* és *JNap*.

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



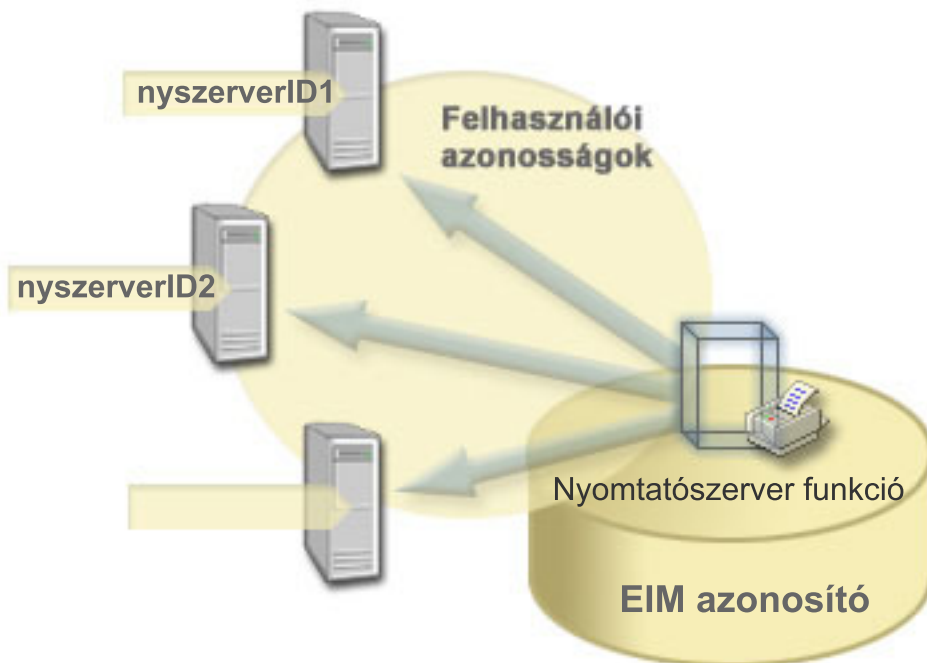
Az EIM segítségével létrehozhat olyan társításokat, amelyek meghatározzák a **Nap János** azonosító, és *Nap János* valamennyi felhasználói azonossága közötti viszonyokat. A viszonyokat meghatározó társítások létrehozásával lehetőség van olyan alkalmazások írására, amelyek az EIM API hívások felhasználásával 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 (*nyszerverID1*, *nyszerverID2* és *nyszerverID3*) alatt.

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





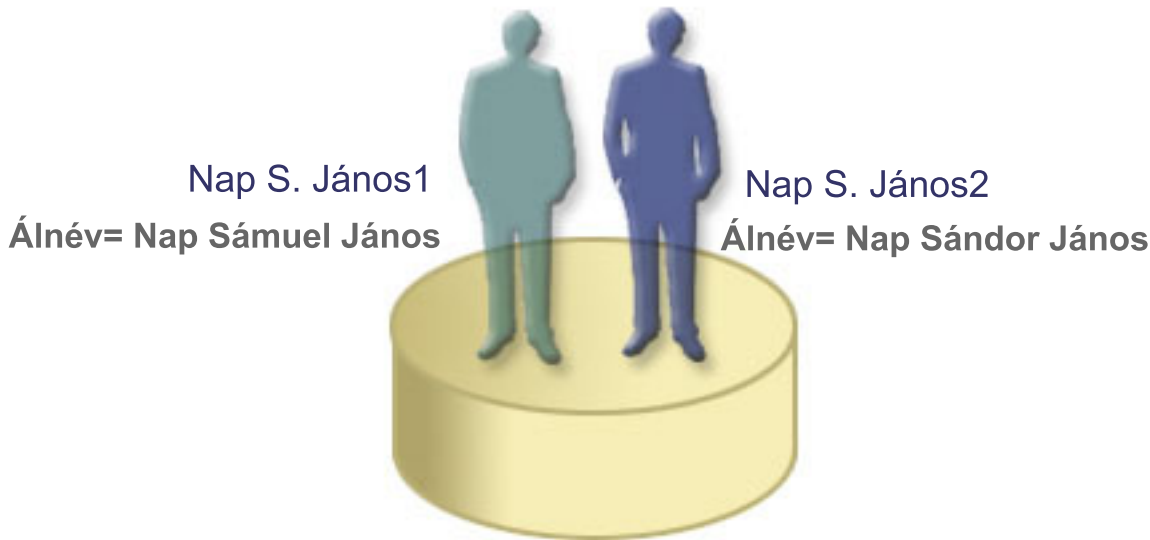
Az EIM segítségével létrehozhat olyan egyedülálló azonosítót, amely a teljes vállalaton belül képviseli a nyomtatószerver funkciót. Ahogy a példában is látszik, a Nyomtatószerver funkció EIM azonosító a tényleges vállalati nyomtatószerver funkciót képviseli. Az EIM azonosító (Nyomtatószerver funkció) és a funkció különféle felhasználói azonosságai (nyszerverID1, nyszerverID2 és nyszerverID3) 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 azonosítók neveinek egyedinek kell lenniük az EIM tartományban. Az álnevek segítségével megoldhatók az
- | olyan helyzetek is, amikor egyedi azonosítónevek használata nehéz lehet. Az EIM azonosító álnevek például az olyan
- | helyzetekben lehetnek hasznosak, amikor valakinek a hivatalos neve eltér attól a névtől, amelyen a személyt ismerik.
- | 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 *Nap S. János* van. Az EIM adminisztrátor két különböző EIM azonosítót hoz létre, hogy különbséget lehessen tenni közöttük: *Nap S. János1* és *Nap S János2*. Az viszont, hogy melyik azonosító melyik *Nap S. Jánost* ábrázolja, nem feltétlenül nyilvánvaló.

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



Álnevek használatával az EIM adminisztrátor további információkat biztosíthat az EIM azonosítóhoz tartozó egyénekről. Minden egyes EIM azonosító rendelkezhet több álnévvel is, amelyek azonosíthatják, hogy az EIM azonosító melyik *Nap S. Jánost* képviseli. A további álnevek tartalmazhatják például a felhasználók dolgozói kódját, osztályát, munkakörét vagy bármely más megkülönböztető jellemzőt. Ebben a példában Nap S. János1 álneve lehet Nap Sándor János, Nap S. János2 álneve pedig Nap Sámuel János.

- | Az álnév információk felhasználhatók egy adott EIM azonosító keresése során. Tegyük fel, hogy egy EIM alkalmazás
- | megad egy álnevet, amelyet egy adott EIM azonosító megtalálásához fog felhasználni. Az adminisztrátor
- | hozzárendelheti ezt az álnevet a megfelelő EIM azonosítóhoz, így az alkalmazásba nem kell beégetni egy egyedi
- | azonosító nevet, hanem az álnéven keresztül fogja végrehajtani az EIM műveleteket. Az alkalmazás a Cél EIM
- | azonosítók visszakeresése azonosság alapján (`eimGetTargetFromIdentifier()`) API segítségével végrehajthat egy EIM
- | kikeresési műveletet a szükséges felhasználói azonosság visszakereséséhez.

## EIM nyilvántartás meghatározások

Az *EIM nyilvántartás meghatározások* olyan EIM bejegyzések, amelyek 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) nyilvántartása. A felhasználói nyilvántartások emellett más információkat is tartalmazhatnak. Egy Egyszerűsített címtárhozzáférési protokoll (LDAP) címtár például megkülönböztetett neveket, jelszavakat és hozzáférés felügyeleti adatokat tartalmaz. Szintén elterjedt felhasználói nyilvántartások például az azonosítók a Kerberos tartományban, a felhasználói azonosságok a Windows Active Directory tartományban és az OS/400 felhasználói profilok nyilvántartása.

- | Meghatározhatók már felhasználói nyilvántartásokon belül található felhasználói nyilvántartások is. Bizonyos
- | alkalmazások egy felhasználói nyilvántartás részalalmazat képező felhasználói nyilvántartásokat használnak. Ilyen
- | például a z/OS biztonság szerver (RACF) nyilvántartás, amely tartalmazhat olyan felhasználói nyilvántartásokat,
- | amelyek a teljes RACF nyilvántartás részét képezik. Ennek a viselkedésnek a modellezésére az EIM az alábbi két
- | típusú EIM nyilvántartás meghatározás létrehozását teszi lehetővé az adminisztrátor számára:
- | • Rendszer nyilvántartás meghatározás
- | • Alkalmazás nyilvántartás meghatározás

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. 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 hosztnéve, vagy egy alkalmazás esetén a hosztnév és az alkalmazásnév kombinációja. Az EIM nyilvántartás meghatározások neveiben kis- és nagybetűs alfanumerikus karakterek illetve szóközők használhatók.

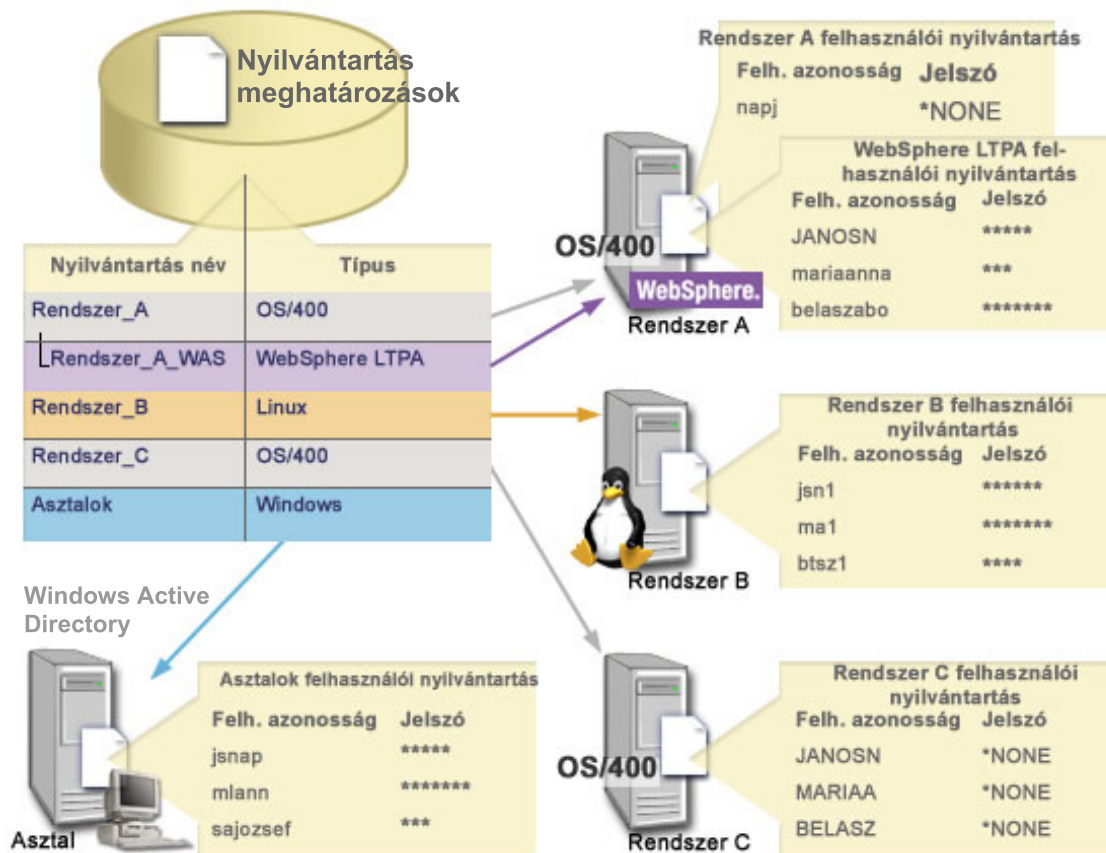
- A felhasználói nyilvántartás típusa. Az EIM számos előre meghatározott felhasználói nyilvántartás típust tartalmaz, amelyek lefedik a legtöbb operációs rendszer felhasználói nyilvántartását. Ezek az alábbiak:

- AIX
- Domino - hosszú név
- Domino - rövid név
- Kerberos
- Kerberos - kis- és nagybetű érzékeny
- LDAP
- Linux
- Novell
- Címtár szerver
- OS/400
- Tivoli Access Manager
- RACF
- Windows - helyi
- Windows tartomány (Kerberos) (Ez a típus érzékeny a kis- és nagybetűkre.)
- X.509

**Megjegyzés:** Noha az előre meghatározott nyilvántartás meghatározás típusok a legtöbb operációs rendszer felhasználói nyilvántartását lefedik, elképzelhető, hogy olyan nyilvántartás meghatározást kell létrehozni, amelyhez az EIM nem tartalmaz előre meghatározott nyilvántartás típust. Ebben az esetben két választási lehetőség áll rendelkezésre. Használhat egy a kívánt felhasználói nyilvántartás jellemzőinek megfelelő létező nyilvántartás meghatározást vagy létrehozhat saját felhasználói nyilvántartás típust. A 6. ábrán például az adminisztrátor végrehajtotta a szükséges lépéseket és a **Rendszer\_A\_WAS** alkalmazás nyilvántartás meghatározáshoz beállította a **WebSphere LTPA** nyilvántartás típust.

A 6. ábrán az adminisztrátor EIM rendszer nyilvántartás meghatározásokat hozott létre az A, B, és C rendszerek képviselő felhasználói nyilvántartásokhoz, illetve a felhasználók által az asztali munkaállomásokra bejelentkezéshez használt Kerberos azonosítókat tartalmazó Windows Active Directory nyilvántartáshoz. ezen kívül létrehozott egy alkalmazás nyilvántartás meghatározást az A rendszeren futó WebSphere Egyszerűsített külső hitelesítés (LTPA) számára. A használt nyilvántartás meghatározás nevek segítik azonosítani a felhasználói nyilvántartás típusok egyes előfordulásait. A felhasználói nyilvántartások nagy részénél egy IP cím vagy hosztnév például általában elegendő. Ebben a példában az adminisztrátor a **Rendszer\_A\_WAS** alkalmazás nyilvántartás meghatározás névvel azonosítja a WebSphere LTPA adott példányát. Azt is meghatározza, hogy az alkalmazás nyilvántartás meghatározáshoz a **Rendszer\_A** szülő rendszer nyilvántartás tartozik.

**6. ábra:** EIM nyilvántartás meghatározások öt felhasználói nyilvántartáshoz



**Megjegyzés:** A felhasználói jelszavak kezelésére vonatkozó igényeket további csökkentése érdekében az adminisztrátor a 6. ábrán az A és C rendszereken \*NONE jelszót állít be az OS/400 felhasználói profilokhoz. Ebben az esetben egyszeri bejelentkezési környezet létrehozásáról van szó, és a felhasználók csak az iSeries navigátorhoz hasonló EIM támogatással rendelkező alkalmazásokat használnak. Következésképpen az adminisztrátor eltávolítja az OS/400 felhasználói profilok jelszavát, így a felhasználóknak és a rendszergazdáknak is kevesebb jelszót kell kezelniük.

### EIM nyilvántartás meghatározások és álnévek

Az EIM nyilvántartás meghatározások számára is létrehozhat álnéveket. Egy nyilvántartás meghatározáshoz több álnévet is meg lehet adni. 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 álnévet. Ez alapján az EIM adminisztrátor hozzárendelheti a tényleges felhasználói nyilvántartást képviselő EIM nyilvántartás meghatározáshoz az alkalmazás által használt álnévet.

Amikor az adminisztrátor hozzáad egy álnévet az EIM nyilvántartás meghatározáshoz, akkor az alkalmazás egy `eimGetRegistryFromAlias()` EIM API hívással végrehajtott álnév kikeresés segítségével határozhatja meg az EIM nyilvántartás nevét. Az alkalmazás az álnév kikeresés segítségével határozhatja meg az EIM kikeresési műveletekben alkalmazandó EIM nyilvántartásnevet vagy neveket.

- | Például egy EIM használatára felkészített alkalmazás egy forrás vagy egy cél nyilvántartás álnévet használ, esetleg
- | mindkettőt. Ha hozzárendeli ezeket az álnéveket a megfelelő nyilvántartás meghatározásokhoz, akkor az alkalmazás
- | végrehajthat egy álnév keresést, és az álnévek alapján képes megtalálni a szükséges EIM nyilvántartás
- | meghatározásokat. Ez az álnév kikeresés biztosítja, hogy az alkalmazás azokat a felhasználói nyilvántartásokat
- | használja, amelyeket az adminisztrátor tervezett. Az alkalmazás igényeinek megfelelően az adminisztrátor több álnévet
- | is rendelhet egyetlen nyilvántartás meghatározáshoz.

| Amikor álnevet ad meg a nyilvántartás meghatározáshoz, akkor meg kell adnia egy nevet és az álnév típusát. 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
- Egyéb

| Az álnévnek nincs kötelező formátuma. Tetszőleges típust megadhat.

| Egy alkalmazás előírhatja például, hogy a rendszergazda vegyen fel egy alkalm típusú és forrás nyilvántartás nevű álnevet. Ezután az `eimGetRegistryNameFromAlias()` API segítségével az álnév típusának és nevének megadásával megkeresheti a szükséges felhasználói nyilvántartást.

## Rendszer nyilvántartás meghatározások

A rendszer nyilvántartás meghatározás egy munkaállomáson vagy szerveren található különálló felhasználói nyilvántartást képviselő EIM bejegyzés. EIM rendszer nyilvántartás meghatározás abban az esetben hozható létre egy felhasználói nyilvántartáshoz, ha a vállalati nyilvántartásra teljesül a következő feltételek valamelyike:

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

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.

## Alkalmazás nyilvántartás meghatározások

| Az alkalmazás nyilvántartás meghatározások olyan EIM bejegyzések, amelyek egy rendszer nyilvántartásban található felhasználói azonosságok adott részhalmozát képviselik és írják le. Ezek a felhasználói azonosságok közös attribútumokkal vagy jellemzőkkel rendelkeznek, amelyek lehetővé teszik számukra egy adott alkalmazás vagy alkalmazáscsoport használatát. Az alkalmazás nyilvántartás meghatározások más felhasználói nyilvántartásokon belül létező felhasználói nyilvántartásokat képviselnek. Ilyen például a z/OS biztonság szerver (RACF) nyilvántartás, amely tartalmazhat a teljes RACF nyilvántartás részét képező felhasználói nyilvántartásokat. E viszony miatt minden alkalmazás nyilvántartás meghatározáshoz meg kell adni a szülő rendszer nyilvántartás nevét.

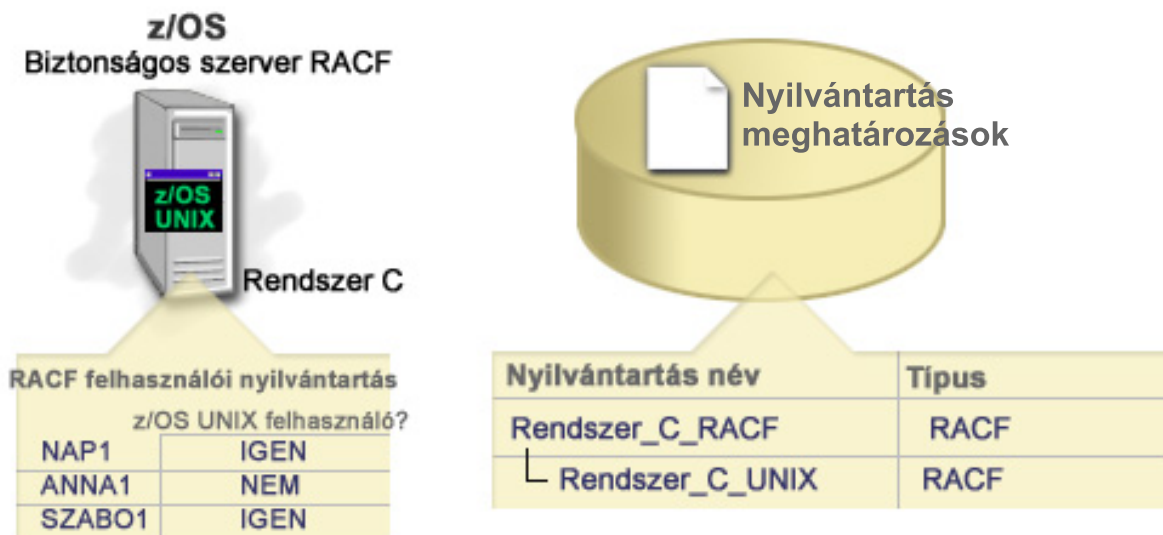
EIM alkalmazás nyilvántartás meghatározás abban az esetben hozható létre egy felhasználói nyilvántartáshoz, ha a nyilvántartásban található felhasználói azonosságok teljesítik az feltételeket:

- Az alkalmazás felhasználói azonosságai nem egy kizárólag az alkalmazásra jellemző felhasználói nyilvántartásban vannak.
- Az alkalmazás felhasználói azonosságai olyan rendszer nyilvántartásban található, amely más alkalmazások felhasználói azonosságait is tárolja.

Az EIM kikeresési műveletek sikere nem függ attól, hogy az EIM adminisztrátor létrehoz-e a felhasználói nyilvántartások számára alkalmazás- illetve rendszer nyilvántartás meghatározásokat. 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 nyilvántartásban található z/OS<sup>(TM)</sup> UNIX rendszerszolgáltatásokat (z/OS UNIX) felhasználói azonosságokat képviseli. A C rendszeren egy olyan RACF felhasználói nyilvántartás található, amely három felhasználói azonosságról (NAP1, ANNA1 és SZABO1) tartalmaz információkat. A felhasználói azonosságok közül kettő (NAP1 és SZABO1) használja a z/OS UNIX szolgáltatást a C rendszeren. Ezek valójában RACF felhasználók, de egyedi attribútumaik z/OS UNIX felhasználóként azonosítják őket. 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 az EIM tartományban létrehozott bejegyzések, amelyek különböző felhasználói nyilvántartásban található felhasználói azonosságok között létesítenek hozzárendelést. A létrehozott társítás típusa határozza meg, hogy a megadott viszony közvetlen vagy közvetett. Az EIM megvalósítása során kétféle társítást hozhat létre: azonosító társításokat és irányelv társításokat. Az irányelv társítások használhatók az azonosító társítások helyett, vagy azokkal párhuzamosan, az azonosító társításokat kiegészítve. A társítások használata függ az átfogó EIM megvalósítási tervtől.

A társítások kezelésével kapcsolatban tekintse át az alábbi információkat:

- | **Azonosító társítások**
- | Tanulja meg az azonosító társítások segítségével leírni az EIM azonosítók és a felhasználói nyilvántartásokban található, egyes személyeket képviselő felhasználói azonosságok közötti kapcsolatokat. Egy azonosító társítás egy közvetlen, 1-1 relációt hoz létre egy EIM azonosító és egy adott felhasználói azonosság között. Az azonosító társítások indirekt segítségével indirekt viszony hozható létre felhasználó azonosságok között egy EIM azonosítón keresztül.
- | **Irányelv társítások**
- | Tanulja meg több felhasználói azonosság és egy adott felhasználói nyilvántartásban található egyetlen felhasználói azonosság közötti viszony leírását irányelv társítások segítségével. Az irányelv társítások az EIM leképezés irányelv támogatását felhasználva N-1 relációkat hoznak létre felhasználói azonosságok között EIM azonosító közbeiktatása nélkül.

- | Kikeresési információk
- | Ismerje meg, hogy az EIM API hívások hogyan használják a kikeresési műveletek során ezeket a felhasználói azonosság
- | azonosságok további azonosításához tetszés szerint megadható információkat a cél felhasználói azonosság
- | keresésnek finomításához.

## Azonosító társítások

- | EIM azonosítók képviselik a személyeket és entitásokat a vállalaton belül. Az EIM azonosító társítások egy EIM
- | azonosító és egy felhasználói nyilvántartás ugyanazon személyre 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.

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 azonosságai alapján végezzék a hitelesítést, míg a felhatalmazást egy másik nyilvántartás felhasználásával.

- | Az EIM azonosítók közvetett hozzárendelést biztosítanak ezek között a felhasználói azonosságok között, ezáltal
- | lehetővé teszik az alkalmazások számára, hogy egy ismert felhasználói azonosság alapján megtaláljanak egy másik
- | felhasználói azonosságot. Az EIM által biztosított API hívások 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.

- | Az EIM háromféle társítás létrehozását teszi lehetővé az EIM azonosítók és felhasználói azonosságok között. Az
- | azonosító társítások lehetnek forrás, cél vagy adminisztrációs típusúak. A létrehozandó társítás típusa a felhasználói
- | azonosság felhasználásának módjától függ. Tegyük fel például, hogy a leképezés kikeresési műveletekben szereplő
- | felhasználói azonosságokhoz szeretne forrás és cél társításokat létrehozni. Általában a hitelesítésben részvevő
- | felhasználói azonossághoz forrás társítást kell létrehozni. Ezután kell a felhatalmazásban szereplő felhasználói
- | azonosságokhoz cél társításokat létrehozni.

Mielőtt lehetőség lenne azonosító 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 név
- Felhasználói azonosság név
- EIM nyilvántartás meghatározás név
- Társítás típus
- | • Választható: a cél felhasználói azonosságot a cél társításban pontosabban leíró kikeresési információk.

## Forrás társítás

A forrás társítás segítségével a felhasználói azonosság felhasználható EIM kikeresési művelet forrásaként, vagyis alapján azonos EIM azonosítóhoz tartozó másik felhasználói azonosság kereshető ki.

- | Egy felhasználói azonosság *hitelesítési* célú felhasználásához a felhasználói azonosságnak forrás társítással kell
- | rendelkeznie egy EIM azonosítóhoz. Egy Kerberos azonosítóhoz például forrás társítást kell létrehozni, mert a
- | felhasználói azonosság ezen formáját hitelesítésre használjuk. Az EIM azonosítókhoz kapcsolódó leképezés kikeresési
- | műveletek sikerének biztosításához a forrás és cél társításokat együttesen kell felhasználni.

## Cél társítás

A cél társítás teszi lehetővé a felhasználói azonosság visszaadását egy EIM kikeresési művelet eredményeként. A végfelhasználókat képviselő felhasználói azonosságoknak általában elegendő, ha csak cél társítással rendelkeznek.

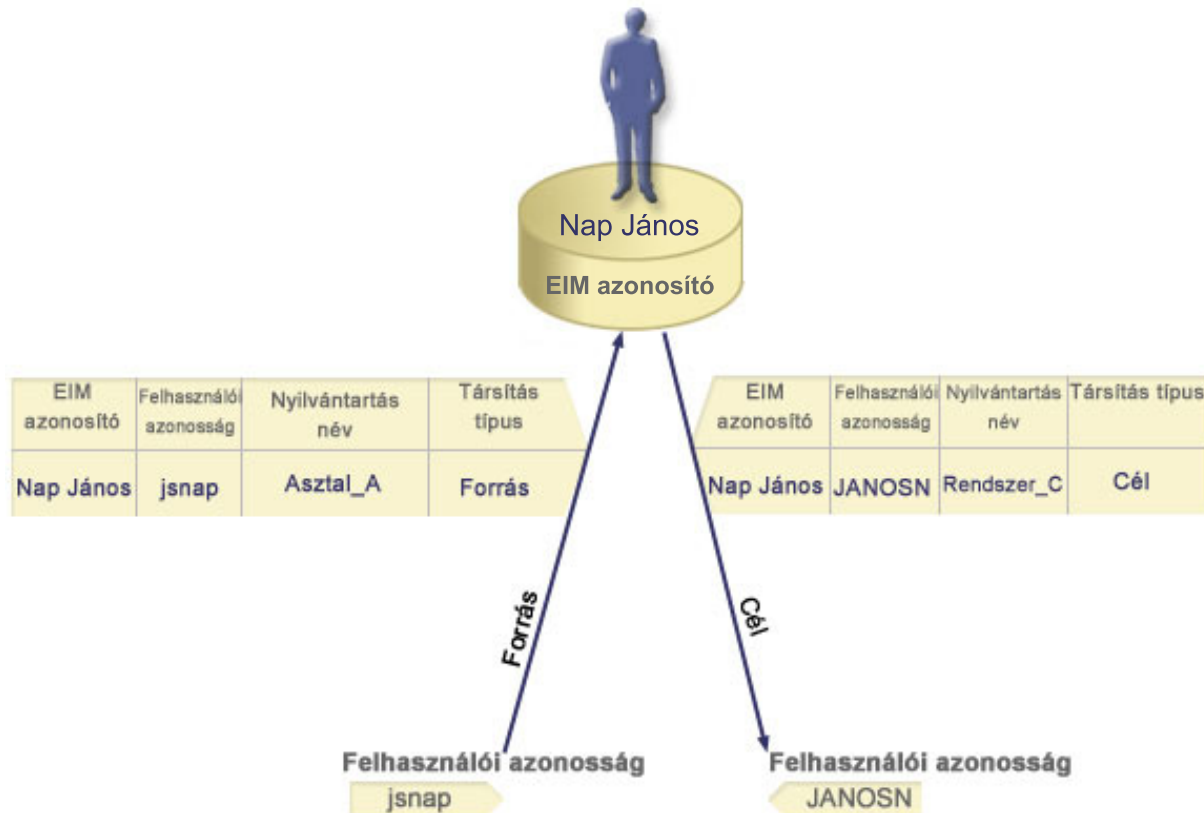
Amikor egy felhasználói azonosság hitelesítés helyett *felhatalmazáshoz* kerül felhasználásra, akkor a felhasználói azonosságnak cél társítással kell rendelkeznie egy EIM azonosítóhoz. Egy OS/400 felhasználói profilhoz például cél társítás létrehozására van szükség, mert a felhasználói azonosságnak ezen formája azt határozza meg, hogy a felhasználónak milyen erőforrások és jogosultságok állnak rendelkezésére egy adott iSeries rendszeren. Az EIM azonosítókhoz kapcsolódó leképezés kikeresési műveletek sikerének biztosításához a forrás és cél társításokat együttesen kell felhasználni.

### A forrás és cél társítások viszonya

- | A sikeres leképezés kikeresési műveletek érdekében legalább egy forrás- és egy vagy több cél társítást kell létrehozni az EIM azonosítóhoz. Általában a felhasználói nyilvántartásokban található összes olyan felhasználói azonossághoz létre kell hozni cél társítást, amelyet a tulajdonosa felhasználhat hitelesítésre az adott felhasználói nyilvántartáshoz tartozó alkalmazás vagy rendszer felé.
- | Tegyük fel például, hogy a vállalat felhasználói általában az asztali Windows<sup>(R)</sup> rendszerükbe jelentkeznek be, a hitelesítést is itt végzik el, majd egy iSeries rendszerhez csatlakoznak, és végrehajtanak bizonyos feladatokat. A felhasználók az asztali rendszerükbe egy Kerberos azonosító felhasználásával jelentkeznek be, az iSeries szervert pedig egy OS/400 felhasználói profil segítségével érik el. Létre szeretne hozni egy egyszeri bejelentkezés környezetet, amelyben a felhasználók elvégzik a hitelesítést az asztali rendszeren a Kerberos azonosítójuk segítségével, és a továbbiakban nincs szükség kézi hitelesítésre az iSeries szerver felé.
- | A cél eléréséhez minden egyes felhasználó Kerberos azonosítóját és EIM azonosítóját össze kell kapcsolni egy forrás társítás segítségével. Ezután minden egyes felhasználó OS/400 felhasználói profilját és EIM azonosítóját össze kell kapcsolni egy cél társítás segítségével. Ez a beállítás biztosítja, hogy miután a felhasználó elvégezte a hitelesítést az asztali rendszerén, az iSeries szerverhez kapcsolódás során az OS/400 egy leképezés kikeresési művelettel meg tudja találni a megfelelő felhasználói profilt a számára. Az OS/400 ezután a megfelelő felhasználói profil alapján biztosítja a hozzáférést az erőforrásokhoz, és a felhasználónak nem kell kézzel elvégeznie a hitelesítést a szerver felé.
- | A 6. ábrán egy másik példa látható, amelyben az EIM adminisztrátor egy forrás és egy cél társítás segítségével meghatároz egy viszonyt a Nap János EIM azonosító és két másik felhasználói azonosság között. Az adminisztrátor a forrás társítást az Asztalok felhasználói nyilvántartásban található jsnap Kerberos azonosítóhoz hozza létre, a cél társítást pedig a Rendszer\_C felhasználói nyilvántartásban található JANOSN OS/400<sup>(R)</sup> felhasználói profilhoz. Ezek a társítások biztosítják az alkalmazások számára azt a lehetőséget, hogy egy EIM kikeresési művelettel meghatározzanak egy ismeretlen felhasználói azonosságot (ez a cél, JANOSN) egy ismert felhasználói azonosság (a forrás, jsnap) alapján.

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





Bizonyos felhasználók esetén akkor is szükség lehet, mind a forrás, mind a cél társítás létrehozására, ha a két felhasználói azonosság megegyezik. Erre adminisztrátorként tevékenykedő személyek esetén, illetve még akkor van szükség, amikor valaki egy rendszert kliensként és szerverként is használ.

**Megjegyzés:** Az átlagos felhasználókat képviselő felhasználói azonosságoknak általában elegendő, ha csak cél társítással rendelkeznek.

Tegyük fel, hogy az adminisztrátor az iSeries navigátor Kezelőközpont funkciójával kezeli a központi rendszert és számos végpont rendszert. Az adminisztrátor különféle funkciókat hajt végre, amelyek kiindulási pontja lehet a központi rendszer vagy akármelyik végpont rendszer. Ebben a helyzetben célszerű minden egyes rendszeren az adminisztrátorhoz tartozó összes felhasználói azonosság számára forrás és cél társítást létrehozni. Ez biztosítja, hogy bármelyik rendszerrel is érje el az adminisztrátor a többi rendszert, a kapcsolathoz felhasznált felhasználói azonosság leképezhető annak a rendszernek egy megfelelő felhasználói azonosságára, amelyikhez az adminisztrátor kapcsolódik.

### Adminisztrációs társítás

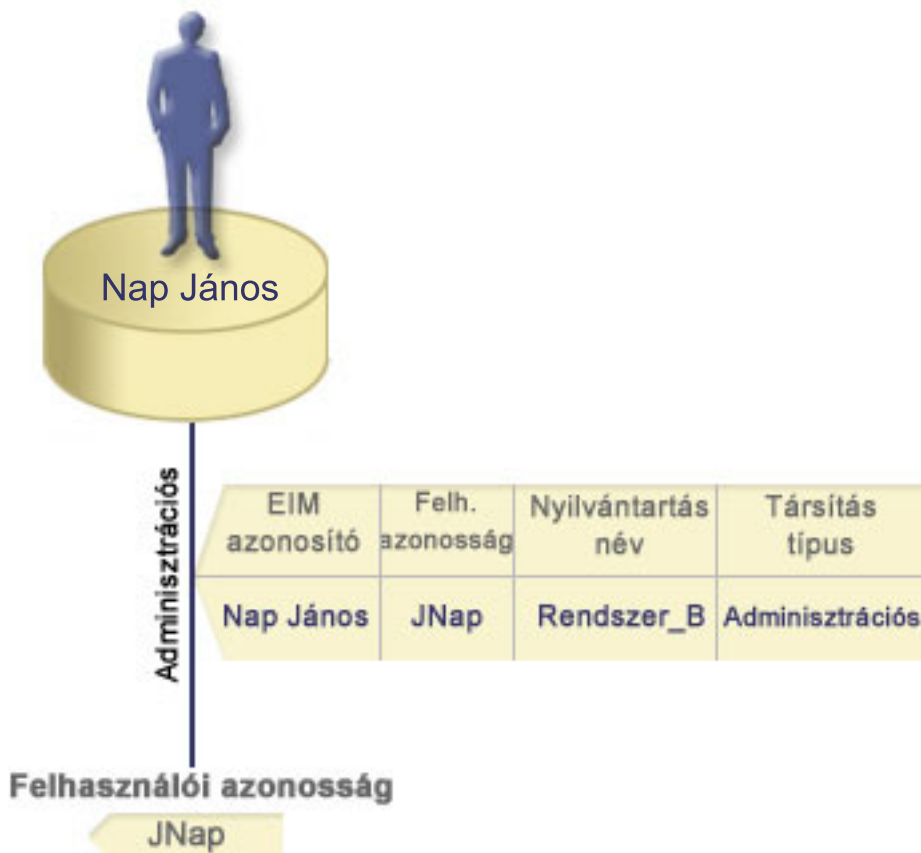
Az EIM azonosítók adminisztrációs társítása általában azt hivatott jelölni, hogy az EIM azonosító által képviselt személy vagy entitás a megadott rendszeren speciális szempontokat igénylő felhasználói azonosságot birtokol. Ez a fajta társítás használható például a rendkívül bizalmas felhasználói nyilvántartásokhoz.

Az adminisztrációs társítások különleges természete miatt ez a típus nem vehet részt EIM leképezés kikeresés műveletekben. Következésképpen 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 a Nap János nevű alkalmazott az A rendszeren a Nap\_Janos, míg a rendkívül biztonságos B rendszeren a JNap felhasználói azonossággal rendelkezik. 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 másik hitelesítési mechanizmus alapján hitelesítse Nap Jánost a rendszeren. Ha a B rendszer JNap felhasználói azonosságához adminisztrációs társítást hoz létre, akkor az EIM adminisztrátor látja, hogy Nap János rendelkezik fiókkal a B rendszeren, de az EIM a kikeresési műveletek során nem ad vissza információkat a JNap azonossággal kapcsolatban. Még ha a rendszeren EIM kikeresést használó alkalmazások is vannak, az adminisztrációs társításokkal rendelkező felhasználói azonosságokat nem találják meg.

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



## Irányelv társítások

A V5R3 kiadástól kezdődően a Vállalati azonosság leképezés (EIM) leképezés támogatás segítségével az EIM adminisztrátor irányelv társításokat hozhat létre több, akár különböző nyilvántartásokban található felhasználói azonosság és egy másik felhasználói nyilvántartásban található egyetlen felhasználói azonosság közötti viszony megadására. Az irányelv társítások az EIM leképezés irányelv támogatását felhasználva N-1 relációkat hoznak létre felhasználói azonosságok között EIM azonosító közbeiktatása nélkül. Az irányelv társítások használhatók az EIM azonosítók és egy felhasználói azonosság között 1-1 leképezéseket biztosító azonosító társítások helyett, vagy azokkal párhuzamosan, az azonosító társításokat kiegészítve.

Az irányelv társítások csak azokat a felhasználói azonosság érintik, amelyekhez nem létezik egyedi EIM társítás. Ha egy EIM azonosító és egy felhasználói azonosság között egyedi azonosító van megadva, akkor egy kikeresési művelet akkor is az azonosító társítás által meghatározott cél felhasználói azonosságot adja vissza, ha létezik irányelv társítás, és az irányelv társítások használata engedélyezett. A “Vállalati azonosság leképezés (EIM) kikeresési műveletek” oldalszám: 25 részben bővebb információkat talál arról, hogy a kikeresési műveletek hogyan kezelik a társításokat.

Háromféle irányelv társítást hozhat létre:

- Alapértelmezett tartomány irányelv társításokat, amelyek segítségével a tartományban található összes felhasználói azonosságot érintő leképezéseket hozhat létre.
- Alapértelmezett nyilvántartás irányelv társításokat, amelyek segítségével a nyilvántartásban található összes felhasználói azonosságot érintő leképezéseket hozhat létre.
- Igazolásszűrő irányelv társításokat, amelyek segítségével egy X.509 nyilvántartásban található, digitális igazolások formájában létező felhasználói azonosságokat érintő leképezéseket hozhat létre.

**Alapértelmezett tartomány irányelv társítások:** Az alapértelmezett tartomány irányelv társítás segítségével N-1 leképezéseket hozhat létre felhasználói azonosságok között. Az alapértelmezett tartomány irányelv társítás több felhasználói azonosságot (ebben az esetben a tartomány összes felhasználóját) rendeli egyetlen felhasználói azonossághoz egy megadott felhasználói nyilvántartásban. Az alapértelmezett tartomány irányelv társításban a tartományban található összes felhasználó forrása az irányelv társításnak, és leképeződik egyetlen cél nyilvántartásra és cél felhasználói azonosságra.

Az alapértelmezett tartomány irányelv társítások használatához engedélyeznie kell az irányelv társítások használatát és a leképezés kereséseket a tartományban. Az irányelv társításhoz tartozó cél felhasználói nyilvántartáshoz is engedélyezni kell a leképezés kikereséseket. Ha kiadja ezeket az engedélyeket, akkor az irányelv társítás felhasználói nyilvántartásai részt vehetnek a leképezés kikeresési műveletekben.

Az alapértelmezett tartomány irányelv társítás akkor lép életbe, ha a leképezés kikeresési művelet feltételeinek nem felel meg egyetlen azonosító társítás, igazolásszűrő irányelv társítás vagy alapértelmezett nyilvántartás irányelv társítás sem a cél nyilvántartáshoz. Az eredmény az, hogy a tartományban található összes felhasználói azonosság az alapértelmezett tartomány irányelv társítás által megadott egyetlen cél felhasználói azonosságra képeződik le.

Tegyük fel például, hogy az adminisztrátor létrehoz egy alapértelmezett tartomány irányelv társítást, amelynek cél felhasználói azonossága a Nyilvántartás\_xyz nyilvántartásban található Nap\_Janos, és nincs olyan azonosító társítás vagy más irányelv társítás, ami erre a felhasználói azonosságra végezne leképezést. Ebben az esetben ha a kikeresési művelet cél nyilvántartásaként a Nyilvántartás\_xyz van megadva, akkor az alapértelmezett tartomány irányelv társítás biztosítja, hogy a tartományban található, más társítással nem rendelkező összes felhasználói azonosság esetében a visszaadott cél felhasználói azonosság a Nap\_Janos legyen.

Az alapértelmezett tartomány irányelv társítás meghatározásához az alábbi információk megadása szükséges:

- **Cél nyilvántartás.** A megadott cél nyilvántartás egy Vállalati azonosság leképezés (EIM) nyilvántartás meghatározás név tartalmazza azt a felhasználói azonosságot, amelyre a tartományban található összes felhasználói azonosságot le kell képezni.
- **Cél felhasználó.** A cél felhasználó annak a felhasználói azonosságnak a neve, amelyet a meghatározandó irányelv társításon alapuló EIM leképezés kikeresési műveletek adnak vissza.

A tartományban található összes nyilvántartáshoz megadhat alapértelmezett tartomány irányelv társítást. Ha egy cél nyilvántartásra kettő vagy több tartomány irányelv társítás hivatkozik, akkor egyedi kikeresési információk megadásával biztosítani kell, hogy a leképezés kikeresési műveletek különbséget tudjanak tenni közöttük. Ellenkező esetben a leképezés kikeresési műveletek több felhasználói azonosságot fognak visszaadni. Ezeknek miatt a kétértelmű eredmények miatt előfordulhat, hogy az EIM használatára támaszkodó alkalmazások nem tudják pontosan megállapítani a használandó cél felhasználói azonosságot.

Mivel az irányelv társítások használatára számos, sokszor egymást átfedő mód létezik, nagyon fontos megérteni az EIM leképezés irányelv támogatást és a kikeresési műveletek működését az irányelv társítások létrehozása előtt.

**Alapértelmezett nyilvántartás irányelv társítások:** Az alapértelmezett nyilvántartás irányelv társítás segítségével N-1 leképezéseket hozhat létre felhasználói azonosságok között. Az alapértelmezett nyilvántartás irányelv társítás több felhasználói azonosságot (ebben az esetben egy nyilvántartás felhasználóit) rendeli egyetlen felhasználói azonossághoz egy megadott felhasználói nyilvántartásban. Az alapértelmezett nyilvántartás irányelv társításban a nyilvántartásban található összes felhasználó forrása az irányelv társításnak, és leképeződik egyetlen cél nyilvántartásra és cél felhasználóra.

l Az alapértelmezett nyilvántartás irányelv társítások használatához engedélyeznie kell az irányelv társítások használatát és a leképezés kereséseket a tartományban. Engedélyeznie kell továbbá a leképezés kereséseket a forrás és a cél felhasználói nyilvántartásban, illetve irányelv társítások használatát az utóbbiban. Ha kiadja ezeket az engedélyeket, akkor az irányelv társítás felhasználói nyilvántartásai részt vehetnek a leképezés kikeresési műveletekben.

l Az alapértelmezett nyilvántartás irányelv társítás akkor lép életbe, ha a leképezés kikeresési művelet feltételeinek nem felel meg egyetlen azonosító társítás, igazolásszűrő irányelv társítás vagy más alapértelmezett nyilvántartás irányelv társítás sem a cél nyilvántartáshoz. Az eredmény az, hogy a forrás nyilvántartásban található összes felhasználói azonosság az alapértelmezett nyilvántartás irányelv társítás által megadott egyetlen cél felhasználói azonosságra képeződik le.

l Tegyük fel, hogy az adminisztrátor létrehoz egy alapértelmezett nyilvántartás irányelv társítást, amelynek forrás nyilvántartása egy adott Kerberos tartománybeli azonosítókat tartalmazó **sajat\_tartomany.com**. Az adminisztrátor létrehoz ehhez az irányelv társításhoz egy **altalanos\_felhasznalo1** cél felhasználói azonosságot az **os/400\_rendszer\_nyilv** cél nyilvántartásban, ami tulajdonképpen egy konkrét felhasználói profil egy OS/400 felhasználói nyilvántartásban. Ebben az esetben nem létezik olyan azonosító társítás vagy irányelv társítás, amely a forrás nyilvántartásban bármelyik felhasználói azonosságra érvényes lenne. Ezért ha cél nyilvántartásként az **os/400\_rendszer\_nyilv**, forrás nyilvántartásként pedig az **sajat\_tartomany.com** szerepel egy kikeresési műveletben, akkor az alapértelmezett nyilvántartás irányelv társítás biztosítja, hogy az **sajat\_tartomany.com** nyilvántartásban szereplő összes olyan felhasználói azonosság esetén az **altalanos\_felhasznalo1** legyen az eredmény, amelyhez nincs meghatározva azonosító társítás.

l Az alapértelmezett nyilvántartás irányelv társítás meghatározásához az alábbi információk megadása szükséges:

- l • **Forrás nyilvántartás.** Ezt a nyilvántartás meghatározást jelöli ki forrásként az irányelv társítás számára. A forrás felhasználói nyilvántartásban található összes felhasználói azonosság le lesz képezve az irányelv társításhoz tartozó megadott cél felhasználói azonosságra.
- l • **Cél nyilvántartás.** Egy Vállalati azonosság leképezés (EIM) nyilvántartás meghatározás neve. A cél nyilvántartásnak tartalmaznia kell azt a felhasználói azonosságot, amelyre a forrás nyilvántartás összes felhasználói azonosságát le kell képezni.
- l • **Cél felhasználó.** A cél felhasználó annak a felhasználói azonosságnak a neve, amelyet a meghatározandó irányelv társításon alapuló EIM leképezés kikeresési műveletek adnak vissza.

l Egynél több alapértelmezett nyilvántartás irányelv társítást is meghatározhat. Ha egy cél nyilvántartásra kettő vagy több megegyező forrás nyilvántartással rendelkező irányelv társítás hivatkozik, akkor egyedi kikeresési információk megadásával biztosítani kell, hogy a leképezés kikeresési műveletek különbséget tudjanak tenni közöttük. Ellenkező esetben a leképezés kikeresési műveletek több felhasználói azonosságot fognak visszaadni. Ezeknek miatt a kétértelmű eredmények miatt előfordulhat, hogy az EIM használatára támaszkodó alkalmazások nem tudják pontosan megállapítani a használandó cél azonosságot.

l Mivel az irányelv társítások használatára számos, sokszor egymást átfedő mód létezik, nagyon fontos megérteni az EIM leképezés irányelv támogatást és a kikeresési műveletek működését az irányelv társítások létrehozása előtt.

l **Igazolásszűrő irányelv társítások:** Az igazolásszűrő irányelv társítás segítségével N-1 leképezéseket hozhat létre felhasználói azonosságok között. Az igazolásszűrő irányelv társítás egy igazoláshalmazt rendel egyetlen felhasználói azonossághoz egy megadott felhasználói nyilvántartásban.

l Az igazolásszűrő irányelv társítások kijelölik egy startégi társítás forrásául szolgáló X.509 nyilvántartásban található igazoláskészletet. Ezeket az igazolásokat a megadott cél nyilvántartásra és felhasználóra képezi le. Az alapértelmezett nyilvántartás irányelv társításhoz képest, amikor egy irányelv társítás forrása a nyilvántartásban található összes felhasználó, az igazolásszűrő irányelv társítás hatóköre jóval rugalmasabb. Forrásként a nyilvántartásban található igazolás egy részalmazát is megadhatja. Az irányelv társításhoz megadott igazolásszűrő határozza meg a hatókört.

l **Megjegyzés:** Amennyiben az X.509 felhasználói nyilvántartásban található összes igazolást meg kívánja feleltetni egyetlen felhasználói azonosságnak, akkor alapértelmezett nyilvántartás irányelv társítást kell létrehoznia.

| Az igazolásszűrő irányelv társítások használatához engedélyeznie kell az irányelv társítások használatát és a leképezés  
| kereséseket a tartományban. Engedélyeznie kell továbbá a leképezés kereséseket a forrás és a cél felhasználói  
| nyilvántartásban, illetve irányelv társítások használatát az utóbbiban. Ha kiadja ezeket az engedélyeket, akkor az  
| irányelv társítás felhasználói nyilvántartásai részt vehetnek a leképezés kikeresési műveletekben.

| Ha egy leképezés kikeresési műveletben a forrás felhasználói azonosság egy digitális igazolás, akkor (miután a  
| lekérdező alkalmazás használta az `eimFormatUserIdentity()` EIM API hívást a felhasználó azonosság név  
| formázásához) az EIM először ellenőrzi, hogy létezik-e azonosító társítás az EIM azonosító és a megadott felhasználói  
| azonosság között. Ha ilyen nem létezik, akkor az EIM összehasonlítja az igazolás DN információit az irányelv  
| társításhoz tartozó szűrőben megadott DN információkkal. Ha az igazolás DN információi kielégítik a szűrő feltételeit,  
| akkor az EIM visszaadja az irányelv társítás által megadott cél felhasználói azonosságot. Végeredményben az X.509  
| nyilvántartásban található, az igazolásszűrő feltételeket kielégítő igazolások az igazolásszűrő irányelv társítás által  
| megadott egyetlen felhasználói azonosságra képeződnek le.

| Tegyük fel például, hogy az adminisztrátor létrehoz egy olyan igazolásszűrő irányelv társítást, amelynek a  
| forrásnyilvántartása a `certificates.x509`. Ez a nyilvántartás tartalmazza a társaság összes alkalmazottjának igazolását,  
| beleértve a HR részlegen dolgozó vezetőket is, akik az igazolásaik segítségével bizonyos titkos belső weboldalakat és  
| egyéb erőforrásokat érnek el az iSeries szerveren. Az adminisztrátor létrehoz ehhez az irányelv társításhoz egy  
| `hr_vezetok` cél felhasználói azonosságot a `rendszer_abc` cél nyilvántartásban, ami tulajdonképpen egy konkrét  
| felhasználói profil egy OS/400 felhasználói nyilvántartásban. Annak biztosítására, hogy ez az irányelv társítás csak a  
| HR vezetők által használt igazolásokra legyen érvényes, adjon meg egy igazolásszűrőt a  
| `ou=hrvez,o=tarsasag.com,c=us` tárgy megkülönböztetett névvel (SDN).

| Ebben az esetben nem létezik olyan azonosító társítás vagy másik igazolásszűrő irányelv társítás, amely a forrás  
| nyilvántartásban bármelyik felhasználói azonosságra érvényes lenne. Ezért ha cél nyilvántartásként a `rendszer_abc`,  
| forrás nyilvántartásként pedig az `igazolasok.x509` szerepel egy kikeresési műveletben, akkor az igazolásszűrő irányelv  
| társítás biztosítja, hogy az `igazolasok.x509` nyilvántartásban szereplő összes olyan igazolás esetén `hr_vezetok` legyen  
| az eredmény, amelyiknek az igazolásszűrő megfelel, és nincs hozzá meghatározva azonosító társítás.

| Az igazolásszűrő irányelv társítások meghatározásához az alábbi információkat kell megadnia:

- | • **Forrás nyilvántartás.** A megadott forrás nyilvántartásnak kötelezően X.509 típusú felhasználói nyilvántartásnak  
| kell lennie. Az igazolásszűrő irányelv az X.509 felhasználói nyilvántartásban található felhasználói azonosságok és  
| egy megadott cél felhasználói azonosság között hoz létre társítást. A társítás csak azokra a felhasználói  
| azonosságokra vonatkozik, amelyekre teljesül az irányelvhez megadott igazolásszűrő feltétele.
- | • **Igazolásszűrő.** Az igazolásszűrő bizonyos szempontból hasonló felhasználói igazolás jellemzők egy halmazát  
| határozza meg. Az igazolásszűrő irányelv társítás az X.509 felhasználói nyilvántartásban található összes olyan  
| igazolást leképezi egy cél felhasználó azonosságra, ami rendelkezik ezekkel a megadott jellemzőkkel. A szűrőt a  
| leképezés forrásául használni kívánt igazolásoknak megfelelő Tárgy megkülönböztetett név (SDN) és a Kibocsátó  
| megkülönböztetett név (IDN) értékek kombinációja alapján kell megadni. Az irányelvhez megadott  
| igazolásszűrőnek már léteznie kell az EIM tartományban.
- | • **Cél nyilvántartás.** A cél nyilvántartás meghatározás által megadott felhasználói nyilvántartás tartalmazza azt a  
| felhasználói azonosságot, amelyre le kívánja képezni az igazolásszűrőnek megfelelő igazolásokat.
- | • **Cél felhasználó.** A cél felhasználó annak a felhasználói azonosságnak a neve, amelyet a meghatározandó irányelv  
| társításon alapuló EIM leképezés kikeresési műveletek adnak vissza.

| Mivel az igazolás irányelv társítások és más társítások használatára számos, sokszor egymást átfedő mód létezik,  
| nagyon fontos megérteni az EIM leképezés irányelv támogatást és a keresés műveletek működését az igazolás irányelv  
| társítások létrehozása előtt.

| *Igazolásszűrők:* Az igazolásszűrők megkülönböztetett név igazolás-attribútumok segítségével határozzák meg egy  
| X.509 felhasználói nyilvántartásban a bizonyos szempontból összetartozó felhasználói igazolásokat. Az igazolásszűrők  
| szolgálnak az igazolásszűrő irányelv társítások alapjául. Az igazolásszűrő egy irányelv társításban azt határozza meg,  
| hogy a forrásul szolgáló X.509 nyilvántartásban található igazolások közül melyeket kell leképezni az adott cél

felhasználói azonosságra. A szűrő feltételeit kielégítő Tárgy megkülönböztetett név és Kibocsátó megkülönböztetett név információkkal rendelkező igazolás leképezése a megadott cél felhasználóra az EIM kikeresési műveletek során történik meg.

Tegyük fel, hogy létezik egy igazolásszűrő `o=ibm,c=us` Tárgy megkülönböztetett névvel (SDN). Az összes olyan igazolás teljesíti a szűrő feltételeit, amiben megtalálhatók ezek a megkülönböztetett nevek az SDN információk részeként (például: `cn=NapJanos,ou=JogiReszleg,o=ibm,c=us`). Ha az igazolás egynél több szűrő feltételeinek is megfelel, akkor a legpontosabb és az igazolásnak leginkább megfelelő szűrő kap elsőbbséget. Tegyük fel, hogy létezik két igazolásszűrő az alábbi SDN információkkal: `o=ibm,c=us` és `ou=JogiReszleg,o=ibm,c=us`. Ebben az esetben a forrás X.509 nyilvántartásban található `cn=NapJanos,ou=JogiReszleg,o=ibm,c=us` SDN információkkal rendelkező igazolás a második, pontosabb igazolásszűrő feltételeit fogja teljesíteni, míg a `cn=SharonJones,o=ibm,c=us` SDN információkkal rendelkező igazolás esetében az első, kevésbé pontos igazolásszűrő lép életbe, mert ennek feltételei illeszkednek leginkább az igazolás SDN információira.

Igazolásszűrőt az alábbiak megadásával határozhat meg:

- Tárgy megkülönböztetett név (SDN). Az itt megadott részleges vagy teljes megkülönböztetett névnek meg kell felelnie a digitális igazolás részét képező Tárgy megkülönböztetett névnek, ami az igazolás tulajdonosát jelöli ki. Megadhatja a teljes megkülönböztetett nevet, illetve egy vagy több DN részletet is.
- Kibocsátó megkülönböztetett név (IDN). Az itt megadott részleges vagy teljes megkülönböztetett névnek meg kell felelnie a digitális igazolás részét képező Kibocsátó megkülönböztetett névnek, ami az igazolást kibocsátó hitelesítő szervezetet azonosítja. Megadhatja a teljes megkülönböztetett nevet, illetve egy vagy több DN részletet is.

Igazolásszűrők létrehozására számos módszer létezik, beleértve az EIM irányelv szűrő formázás (`eimFormatPolicyFilter()`) API hívást, amely egy sablon igazolás segítségével hozza létre a megfelelő formátumú és sorrendű SDN és IDN megkülönböztetett nevekkal rendelkező igazolásszűrőt.

## Kikeresési információk

A V5R3 kiadástól kezdődően kikeresési információknak nevezett *nem kötelező* adatok segítségével pontosabban azonosíthatja a cél felhasználói azonosságot. Ez a cél felhasználói azonosság meg lehet adva azonosító társítással vagy irányelv társítással. A kikeresési információk egyedi karaktersorozat, amelyet az `eimGetTargetFromSource` vagy az `eimGetTargetFromIdentifier` EIM API használ a leképezés kikeresési műveletek során a keresett cél felhasználói azonosság pontosításához. A fenti API hívások a kikeresési információkat a nyilvántartás felhasználók kiegészítő információk paraméterrel felel meg a kikeresési információknak.

A kikeresési információkra akkor van szükség, ha egy leképezés kikeresési művelet egynél több cél felhasználói azonosságot adhat vissza. Egy leképezés kikeresési művelet akkor talál egynél több cél felhasználói azonosságot, ha az alábbi körülmények közül legalább egy fennáll:

- Egy EIM azonosítóhoz több külön cél társítás tartozik ugyanabban a cél nyilvántartásban.
- Egynél több EIM azonosítónál szerepel forrás társításként ugyanaz a felhasználói azonosság, és noha a cél társításként megadott felhasználói azonosság különbözhet, a cél nyilvántartás szintén megegyezik.
- Egynél több alapértelmezett tartomány irányelv társítás határozza meg ugyanazt a cél nyilvántartást.
- Egynél több alapértelmezett nyilvántartás irányelv társítás határozza meg ugyanazt a forrás nyilvántartást és cél nyilvántartást.
- Egynél több igazolásszűrő irányelv társítás határozza meg ugyanazt az X.509 nyilvántartást, igazolásszűrőt és cél nyilvántartást.

**Megjegyzés:** Az egynél több cél felhasználói azonosságot eredményező leképezés kikeresési műveletek problémákat okozhatnak az EIM támogatással rendelkező alkalmazások működésében, beleértve az olyan OS/400 alkalmazásokat és termékeket is, amelyek nincsenek felkészítve a kétértelmű eredmények kezelésére. Azonban az alap OS/400 alkalmazások, mint például az iSeries Access for Windows nem használhatják a keresési információkat arra, hogy különbséget tegyenek egy kikeresési művelet több eredménye között. Ebből következően érdemes megfontolni a tartomány társításainak átdefiniálását annak érdekében, hogy

a leképezés kikeresési műveletek egyetlen eredménnyel térjenek vissza, és így az alap OS/400 alkalmazások is képesek legyenek kikeresési műveletek végrehajtására és azonosságok leképezésére.

A kikeresési információk használatával elkerülheti azt, hogy a leképezés kikeresési művelet egynél több cél felhasználói azonosságot adjanak vissza. Annak megakadályozására, hogy a leképezés kikeresési műveletek több cél felhasználói azonosságot adjanak vissza, minden társításban minden egyes felhasználói azonossághoz egyedi kikeresési információkat kell megadni. Ezeket az információkat elérhetővé kell tenni a felhasználó kikeresés művelet számára annak érdekében, hogy a művelet képes legyen egyedi cél felhasználói azonosságok visszaadására. Ellenkező esetben előfordulhat, hogy az EIM használatára támaszkodó alkalmazások nem tudják pontosan megállapítani a használandó cél azonosságot.

Tegyük fel, hogy a Nap János nevű EIM azonosító két felhasználói profillal rendelkezik az A rendszeren, az egyik a JNFELH, a másik a biztonság adminisztrátor különleges jogosultságokkal rendelkező JNBIZTADM. Két cél társítás létezik a Nap János azonosítóhoz. Az egyik ilyen cél társítás a JNFELH felhasználói azonossághoz van megadva a Rendszer\_A cél nyilvántartásban, és a JNFELH felhasználói azonossághoz megadott kikeresési információk: felhasználói jogosultság. A másik társítás a JNBIZTADM felhasználói azonossághoz van felvéve a Rendszer\_A cél nyilvántartásban, és a JNBIZTADM felhasználói azonossághoz megadott kikeresési információk: biztonsági tiszt.

Ha egy leképezés kikeresési művelet nem ad meg kikeresési információkat, akkor a művelet a JNFELH és a JNBIZTADM felhasználói azonosságokat is vissza fogja adni. Ha a leképezés kikeresési művelet a felhasználói jogosultság kikeresési információkat adja meg, akkor a művelet csak a JNFELH felhasználói azonossággal tér vissza. Ha a leképezés kikeresési művelet a biztonsági tiszt kikeresési információkat adja meg, akkor a művelet csak a JNBIZTADM felhasználói azonossággal tér vissza.

**Megjegyzés:** Ha kitörli a felhasználói azonossághoz tartozó utolsó cél (azonosító vagy irányelv) társítást is, akkor a cél felhasználói azonosság és a hozzá tartozó összes kikeresési információk is törlődnek a tartományból.

Mivel az igazolás irányelv társítások és más társítások használatára számos, sokszor egymást átfedő mód létezik, nagyon fontos megérteni az EIM leképezés irányelv támogatást és a keresés műveletek működését az igazolás irányelv társítások létrehozása előtt.

## Vállalati azonosság leképezés (EIM) kikeresési műveletek

Egy alkalmazás vagy operációs rendszer egy EIM API hívást használ a *kikeresési műveletek* végrehajtásához, amelynek során egy adott nyilvántartásban található felhasználói azonosságot leképez egy másik nyilvántartás felhasználói azonosságára. 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 hívások 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 az alkalmazás vagy operációs rendszer az `eimGetTargetFromSource()` API hívással hajtja végre a leképezést a cél nyilvántartásban található felhasználói azonosságra, akkor meg kell adnia egy *forrásként szolgáló felhasználói azonosságot* a kikeresési művelethez. Ahhoz, hogy EIM kikeresés művelet forrásában szerepelhessen, a felhasználói azonosságnak rendelkeznie kell legalább egy forrás társítással, vagy szerepelnie kell egy irányelv társításban. Az API végrehajtásához az alkalmazásnak vagy operációs rendszernek az alábbi információkat kell megadnia:

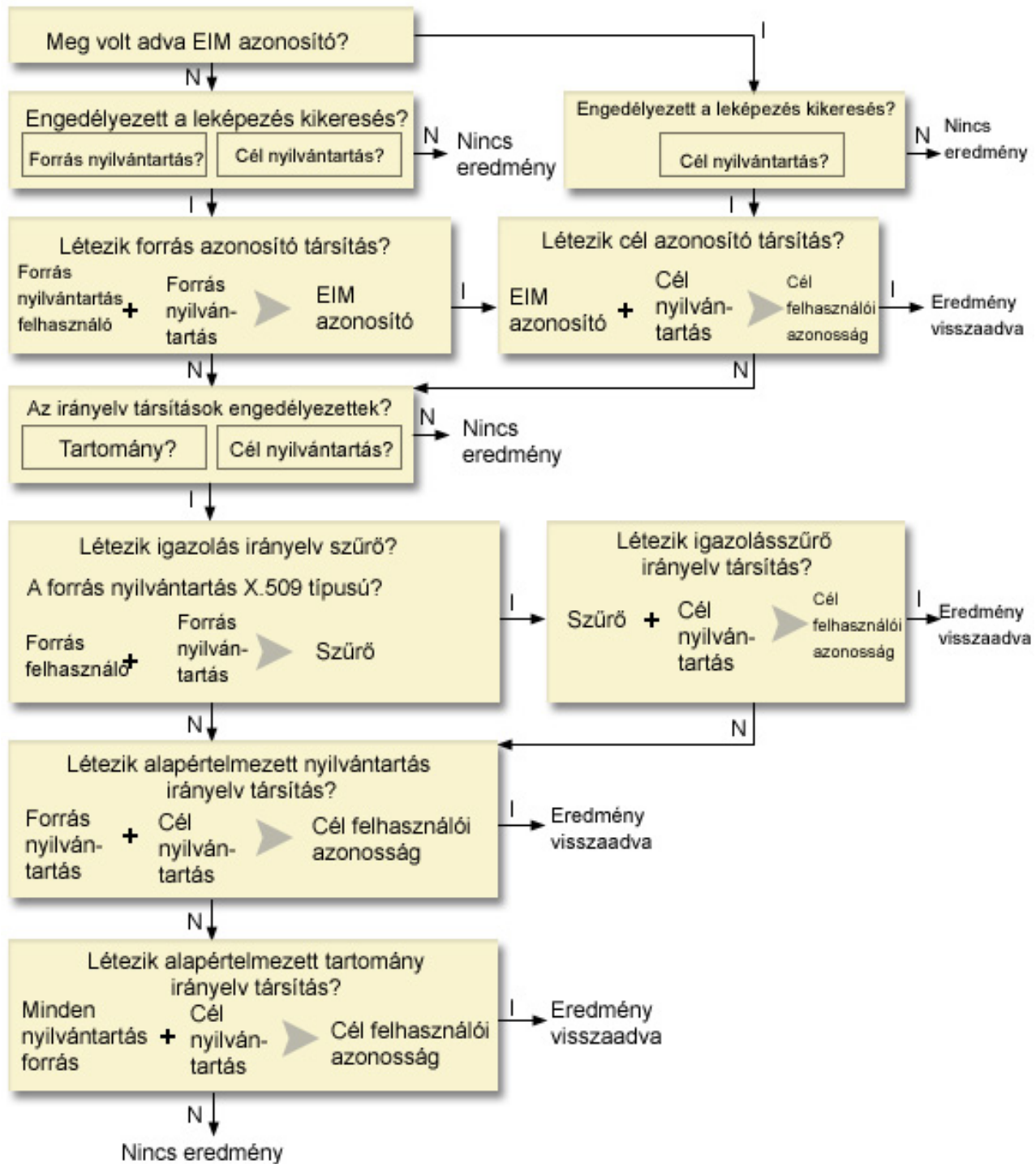
- A művelet forrásaként, vagyis kiinduló pontjaként szolgáló felhasználói azonosság.
- A forrás felhasználói azonossághoz tartozó EIM nyilvántartás meghatározás neve.
- Az EIM kikeresési művelet cél nyilvántartás meghatározás neve. Ez a nyilvántartás meghatározás írja le azt a felhasználói nyilvántartást, amelyben az alkalmazás által keresett felhasználói azonosság található.

Amikor az alkalmazás vagy operációs rendszer az `eimGetTargetFromIdentifier()` API hívással hajtja végre a leképezést a cél nyilvántartásban található felhasználói azonosságra, akkor meg kell adnia egy *forrásként szolgáló EIM azonosítót* a kikeresési művelethez. Az API végrehajtásához az alkalmazásnak az alábbi információkat kell megadnia:

- A művelet forrásaként, vagyis kiinduló pontjaként szolgáló EIM azonosító.

- | • Az EIM kikeresési művelet cél nyilvántartás meghatározás neve. Ez a nyilvántartás meghatározás írja le azt a felhasználói nyilvántartást, amelyben az alkalmazás által keresett felhasználói azonosság található.
- | Ahhoz, hogy egy felhasználói azonosság visszaadható legyen bármelyik típusú kikeresés művelet eredményeként, az azonosságnak rendelkeznie kell cél társítással. Ez a cél társítás lehet azonosító társítás vagy irányelv társítás.
- | A megadott információk alapján az EIM kikeresési művelet megkeresi és visszaadja a cél felhasználói azonosságokat a 10. ábrán is látható módon az alábbi sorrend szerint:
  - | 1. EIM azonosítóhoz tartozó azonosító cél társítás. Az EIM azonosító felismerése kétféle módon történhet: vagy az `eimGetTargetFromIdentifier()` API adja vissza, vagy az `eimGetTargetFromSource()` API által visszaadott információk határozzák meg.
  - | 2. Igazolásszűrő irányelv társítás.
  - | 3. Alapértelmezett nyilvántartás irányelv társítás.
  - | 4. Alapértelmezett tartomány irányelv társítás.
- | **10. ábra:** EIM kikeresési művelet - feldolgozás általános folyamatábrája





I A kikeresés művelet az alábbiak szerint végzi a keresést:

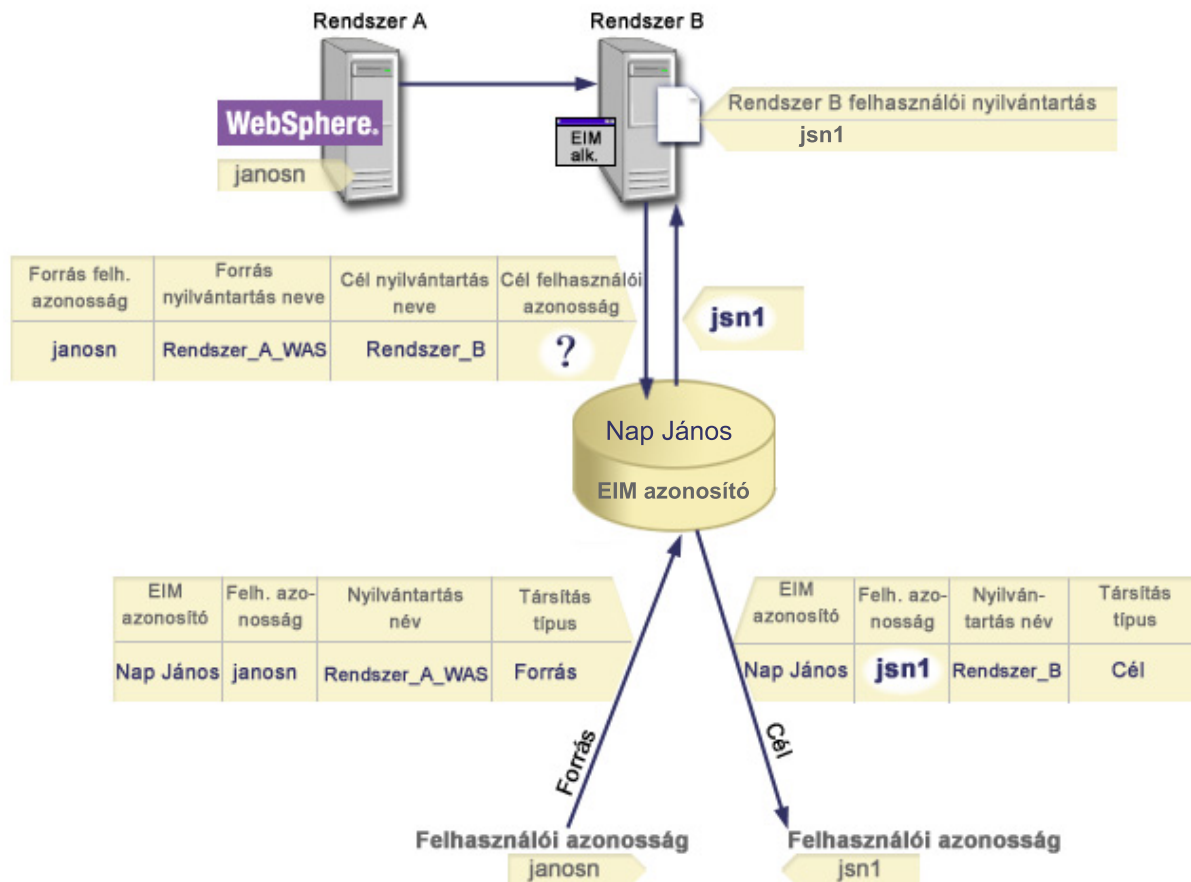
1. A kikeresési művelet ellenőrzi, hogy leképezés kikeresés engedélyezett-e. A kikeresési művelet megállapítja, hogy a leképezés kikeresés engedélyezett-e a megadott forrás nyilvántartásban, a cél nyilvántartásban, vagy mindkettőben. Ha a leképezés kikeresés engedélyezett, akkor valamelyik nyilvántartásban, akkor a kikeresés művelet azonnal véget ér, és nem adja vissza a cél felhasználói azonosságot.
2. A kikeresési művelet megvizsgálja, hogy vannak-e olyan azonosító társítások, amelyek teljesítik a kikeresés feltételeit. Ha egy EIM azonosító van megadva, akkor a kikeresési művelet az EIM azonosító nevet használja. Ha nem létezik ilyen, akkor azt vizsgálja, hogy létezik-e megadott forrás felhasználói azonosságnak és forrás

- nyilvántartásnak megfelelő azonosító forrás társítás. Amennyiben igen, akkor a kikeresési művelet azt használja a megfelelő EIM azonosító név meghatározásához. Ezután a kikeresési művelet az EIM azonosító név segítségével keresi meg az EIM azonosítóhoz tartozó cél azonosító társítások közül azt, amelyik megfelel a megadott cél EIM nyilvántartás meghatározás névnek. Amennyiben létezik megfelelő azonosító cél társítás, akkor a kikeresési művelet visszaadja az általa meghatározott felhasználói azonosságot.
3. A kikeresési művelet ellenőrzi, hogy engedélyezve van-e az irányelv társítások használata. A kikeresési művelet megvizsgálja, hogy a tartomány és a cél társítás engedélyezi-e az irányelv társítások használatát a leképezés kikeresések során. Ha a tartomány vagy a nyilvántartás ezt nem teszi lehetővé, akkor a kikeresési művelet véget ér, de nem ad vissza felhasználói azonosságot.
  4. A kikeresési művelet megvizsgálja az igazolásszűrő irányelv társításokat. A kikeresési művelet megvizsgálja a forrás nyilvántartás típusát. Ha X.509 típusú, akkor a kikeresési művelet ellenőrzi, hogy létezik-e olyan igazolásszűrő irányelv társítás, amely megfelel a forrás és cél nyilvántartás meghatározás neveknek. A művelet ellenőrzi, hogy a forrás X.509 nyilvántartásban található-e olyan igazolások, amelyek kielégítik az igazolásszűrő irányelv társítás feltételeit. Ha léteznek az igazolásszűrő feltételeit kielégítő igazolások és a megfelelő irányelv társítás, akkor a kikeresési művelet visszaadja az irányelv társítás által meghatározott cél felhasználói azonosságot.
  5. A kikeresési művelet alapértelmezett nyilvántartás irányelv társításokat keres. A kikeresési művelet ellenőrzi, hogy létezik-e a forrás és cél nyilvántartás meghatározás neveknek megfelelő alapértelmezett nyilvántartás irányelv társítás. Ha létezik a megfelelő irányelv társítás, akkor a kikeresési művelet visszaadja az irányelv társítás által meghatározott cél felhasználói azonosságot.
  6. A kikeresési művelet alapértelmezett tartomány irányelv társításokat keres. A kikeresési művelet ellenőrzi, hogy a cél nyilvántartás meghatározáshoz van-e meghatározva alapértelmezett tartomány irányelv társítás. Ha létezik a megfelelő irányelv társítás, akkor a kikeresési művelet visszaadja az irányelv társításhoz rendelt cél felhasználói azonosságot.
  7. A kikeresési művelet eredmény nélkül véget ér.

#### **Kikeresési művelet példák: 1. példa**

A 10. ábrán a **janosnap** felhasználói azonosság Egyszerűsített külső hitelesítés (LTPA) alapján kerül hitelesítésre az A rendszeren futó WebSphere alkalmazáserveren. Az A rendszer WebSphere alkalmazáservere 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 **janosnap** forrás felhasználói azonosságot, a **Rendszer\_A\_WAS** forrás és a **Rendszer\_B** cél EIM nyilvántartás meghatározás nevet. A forrásinformációk az EIM szolgáltatáshoz kerülnek, az EIM kikeresési művelet pedig keres egy azonosító forrás társítást az információk alapján. A **Nap János** EIM azonosító név felhasználásával az EIM kikeresési művelet megkeres egy azonosító cél társítást, amely megfelel a **Rendszer\_B** cél EIM nyilvántartás meghatározás névnek. Ha megtalálta a megfelelő cél társítást, akkor az EIM kikeresési művelet visszaadja a **jsn1** felhasználói azonosságot az alkalmazásnak.

**11. ábra:** Az EIM kikeresési művelet a **JANOSN** felhasználói azonossághoz azonosító társítások alapján megkeresi a cél felhasználói azonosságot



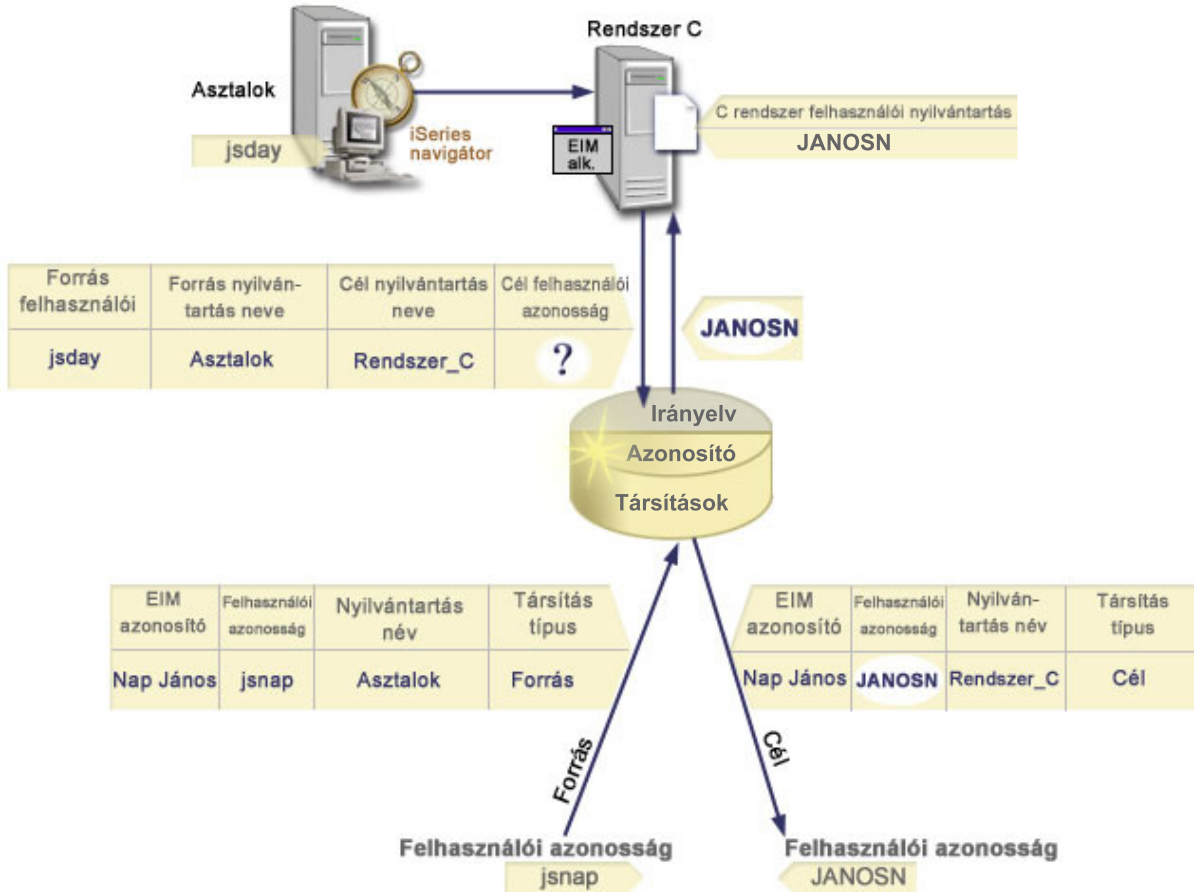
## Kikeresési művelet példák: 2. példa

A 12. ábrán egy adminisztrátor egy Windows Active Directory nyilvántartásban található Windows felhasználót képez le egy OS/400 felhasználói profilra. A Windows Kerberos hitelesítési módszert használ, és az adminisztrátor a Windows Active Directory nyilvántartást az EIM számára Asztalok néven határozta meg. Az adminisztrátor a jsnap Kerberos azonosítót kívánja leképezni. Az OS/400 nyilvántartáshoz tartozó EIM nyilvántartás meghatározás neve Rendszer\_C, és az adminisztrátor a JANOSN felhasználói profilra kívánja elvégezni a leképezést.

A rendszergazda létrehoz egy Nap János nevű EIM azonosítót. Ezután két társítást vesz fel az azonosítóhoz:

- Egy forrás társítást a jsnap Kerberos azonosítóhoz az Asztalok nyilvántartásban.
- Egy cél társítást a JANOSN OS/400 felhasználói profilhoz a Rendszer\_C nyilvántartásban.

**12. ábra:** Az EIM kikeresési művelet azonosító társítások alapján a jsnap Kerberos azonosítóhoz megkeresi a cél felhasználói azonosságot



Ez a konfiguráció lehetővé teszi egy Kerberos azonosító leképezését egy OS/400 felhasználói profilra az alábbiak szerint:

Forrás felhasználói azonosság és nyilvántartás	---	EIM azonosító	---	Cél felhasználói azonosság
jsnap az Asztalok nyilvántartásban	---	Nap János	---	JANOSN (a Rendszer_C nyilvántartásban)

A kikeresés művelet az alábbiak szerint végzi a keresést:

1. A jsnap felhasználó bejelentkezik, és hitelesít a Windows felé az Asztalok Windows Active Directory nyilvántartásban található Kerberos azonosítója segítségével.
2. A felhasználó elindítja az iSeries navigátort a Rendszer\_C rendszeren található adatok eléréséhez.
3. Az OS/400 az EIM API segítségével végrehajt egy kikeresési műveletet, amelyben a forrás felhasználói azonosság a jsnap, a forrás nyilvántartás az Asztalok, a cél nyilvántartás pedig a Rendszer\_C.
4. Az EIM kikeresési művelet megállapítja, hogy a leképezés kikeresés engedélyezett-e az Asztalok forrás nyilvántartásban és a Rendszer\_C cél nyilvántartásban. Az eredmény pozitív.
5. A kikeresési művelet megvizsgálja, hogy vannak-e olyan azonosító társítások, amelyek megfelelnek a megadott Asztalok forrás nyilvántartásban található jsnap forrás felhasználói azonosságnak.
6. A kikeresési művelet a megfelelő azonosító forrás társítás felhasználásával meghatározza a megfelelő EIM azonosító nevet, ami a Nap János.

- | 7. Ezután a kikeresési művelet ennek az EIM azonosító névnek a segítségével keresi meg az EIM azonosítóhoz tartozó cél azonosító társítások közül azt, amelyik megfelel a megadott **Rendszer\_C** cél EIM nyilvántartás meghatározás névnek.
- | 8. Létezik ilyen azonosító cél társítás, és a kikeresési művelet visszaadja a **JANOSN** cél felhasználói azonosságot a cél társításnak megfelelően.
- | 9. A kikeresési művelet véget ér, és az iSeries navigátor a **JANOSN** felhasználói profil alatt kezdi meg a működését. A felhasználó jogosultságait az erőforrások eléréséhez és a tevékenységek végrehajtásához az iSeries navigátoron belül a **JANOSN** felhasználói profil jogosultságai határozzák meg, és nem a **jsnap** felhasználói azonossághoz megadott jogosultságok.

| A következő példa azt az esetet mutatja be, amikor nincs megadva azonosító társítás a felhasználói azonossághoz, és a keresés az irányelv társítások alapján folyik le.

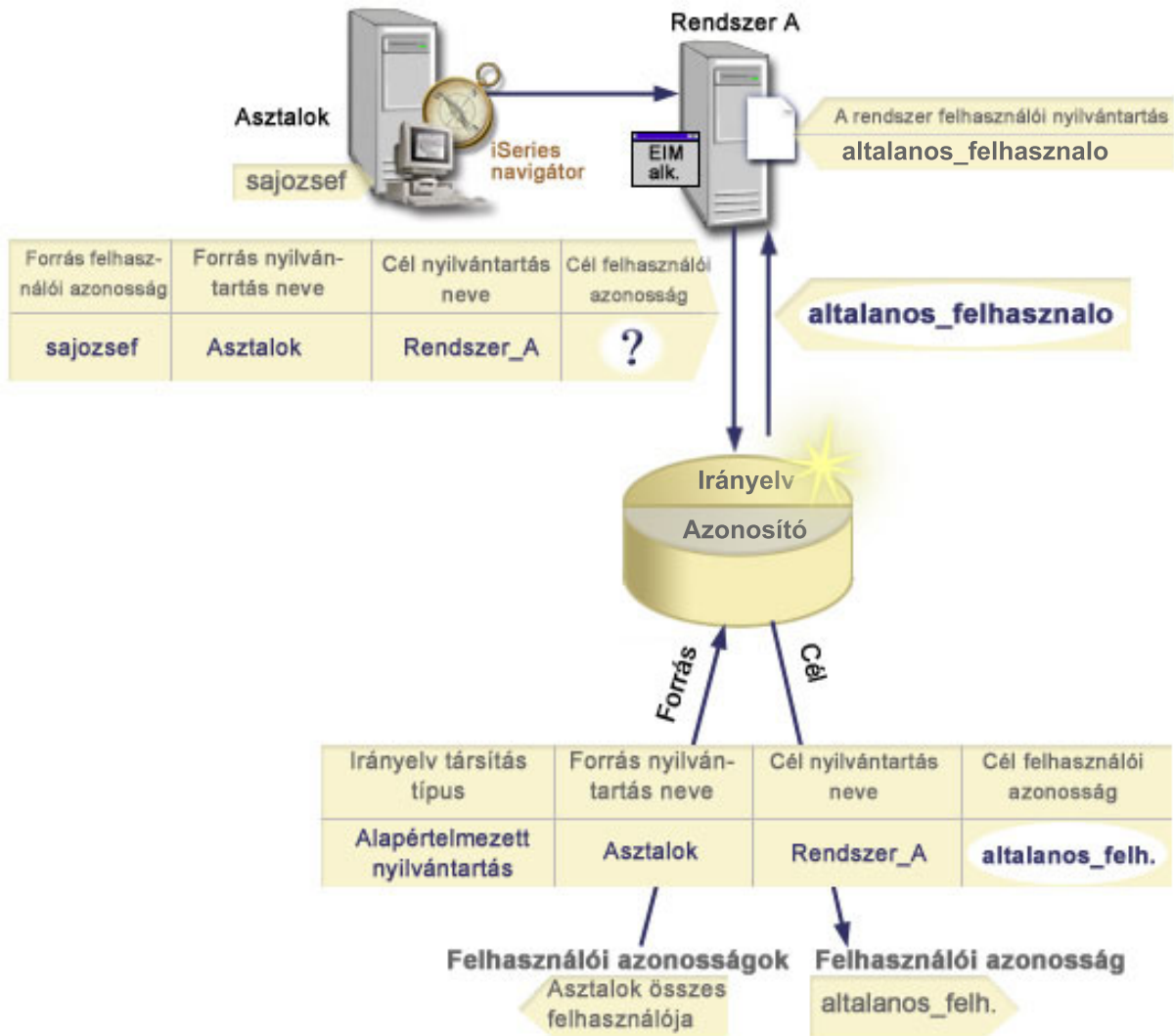
### | **Kikeresési művelet példák: 3. példa**

| A 13. ábrán a rendszergazda a Windows Active Directory nyilvántartásban található összes munkaállomás felhasználót le kívánja képezni a **Rendszer\_A** EIM nevű OS/400 nyilvántartásban található **altalanos\_felhasznalo** nevű OS/400 felhasználói profilra. A Windows Kerberos hitelesítési módszert használ, és az adminisztrátor a Windows Active Directory nyilvántartást az EIM számára **Asztalok** néven határozta meg. Az adminisztrátor többek között a **sajozsef** Kerberos azonosítót kívánja leképezni.

| Az adminisztrátor létrehoz egy alapértelmezett nyilvántartás irányelv társítást az alábbi információkkal:

- | • A forrás nyilvántartás az **Asztalok**.
- | • A cél nyilvántartás a **Rendszer\_A**.
- | • A cél felhasználói azonosság az **altalanos\_felhasznalo**.

| **13. ábra:** A kikeresési művelet visszaad egy cél felhasználói azonosságot egy alapértelmezett nyilvántartás irányelv társítás alapján.



Ez a konfiguráció lehetővé teszi, hogy a kikeresési művelet a sajozsef azonosítóval együtt az Asztalok nyilvántartásban található összes Kerberos azonosítót leképezze az altalanos\_felhasznalo nevű OS/400 felhasználói profilra az alábbiak szerint:

Forrás felhasználói azonosság és nyilvántartás	---	Alapértelmezett nyilvántartás irányelv társítás.	---	Cél felhasználói azonosság
sajozsef az Asztalok nyilvántartásban	---	Alapértelmezett nyilvántartás irányelv társítás.	---	altalanos_felhasznalo (a Rendszer_C nyilvántartásban)

A kikeresés művelet az alábbiak szerint végzi a keresést:

1. A sajozsef felhasználó bejelentkezik, és elvégzi a hitelesítést a Windows felé az Asztalok nyilvántartásban neki megfelelő Kerberos azonosító segítségével.
2. A felhasználó elindítja az iSeries navigátort a Rendszer\_A rendszeren található adatok eléréséhez.
3. Az OS/400 az EIM API segítségével végrehajt egy kikeresési műveletet, amelyben a forrás felhasználói azonosság a sajozsef, a forrás nyilvántartás az Asztalok, a cél nyilvántartás pedig a Rendszer\_C.
4. Az EIM kikeresési művelet megállapítja, hogy a leképezés kikeresés engedélyezett-e az Asztalok forrás nyilvántartásban és a Rendszer\_A cél nyilvántartásban. Az eredmény pozitív.

5. A kikeresési művelet megvizsgálja, hogy vannak-e olyan azonosító társítások, amelyek megfelelnek a megadott **Asztalok** forrás nyilvántartásban található **sajozsef** forrás felhasználói azonosságnak. Nem talál megfelelő azonosító társítást.
6. A kikeresési művelet ellenőrzi, hogy a tartomány engedélyezi-e az irányelv társítások használatát. Az eredmény pozitív.
7. A kikeresési művelet ellenőrzi, hogy a **Rendszer\_A** cél nyilvántartás engedélyezi-e az irányelv társítások használatát. Az eredmény pozitív.
8. A kikeresési művelet megvizsgálja, hogy a forrás nyilvántartás (**Asztalok**) X.509 típusú-e. Nem az.
9. A kikeresési művelet ellenőrzi, hogy létezik-e a forrás (**Asztalok**) és cél (**Rendszer\_A**) nyilvántartás meghatározás névnek megfelelő alapértelmezett nyilvántartás irányelv társítás.
10. A kikeresési művelet megállapítja, hogy létezik ilyen, és visszaadja a **altalanos\_felhasznalo** cél felhasználói azonosságot.

Néha az EIM kikeresési művelet kétértelmű eredménnyel ér véget. Ez előfordulhat például olyan esetekben, amikor egynél több cél felhasználó azonosság teljesíti a megadott keresési feltételeket. Bizonyos EIM támogatással rendelkező alkalmazások, beleértve az olyan OS/400 alkalmazásokat és termékeket is, nincsenek felkészítve ezeknek a kétértelmű eredményeknek a kezelésére, és ilyen esetekben hibás vagy nemvárt működés léphet fel. Ilyenkor a probléma feloldása a felhasználón múlik. Elkerülheti a többszörös feloldást, ha például megváltoztatja az EIM konfigurációt, vagy az összes problémás felhasználói azonossághoz keresési információkat ad meg. A változtatások elvégzése után hajtson végre leképezés tesztet annak ellenőrzésére, hogy a módosítások az elvártan megfelelően működnek.

## Vállalati azonosság leképezés: leképezés irányelv támogatás és engedélyezése

A Vállalati azonosság leképezés (EIM) leképezés irányelv támogatásának segítségével az adminisztrátorok az irányelv társításokat az egyedi azonosító társításokhoz hasonló módon használhatják az EIM tartományban. Az irányelv társítások használhatók az azonosító társítások helyett, vagy azokkal párhuzamosan, az azonosító társításokat kiegészítve.

Az EIM leképezés irányelv támogatás módot kínál az irányelv társítások engedélyezésére és letiltására az egész tartományban, vagy akár egy adott cél felhasználói nyilvántartásban. Az adminisztrátor azt is beállíthatja, hogy egy adott nyilvántartás általánosságban részt vehet-e a leképezés kikeresési műveletekben. Következésképpen az adminisztrátor a felügyel irányelv támogatás segítségével pontosabban vezérelheti a leképezés kikeresési műveleteket.

Az EIM tartomány alapértelmezett beállítása szerint az irányelv társítást használó leképezés kikeresések nem engedélyezettek. Ha az irányelv társítások használata nem engedélyezett a tartományban, akkor a leképezés kikeresési műveletek csak felhasználói azonosságok és EIM azonosítók közötti egyedi azonosító társításokat használhatják.

A nyilvántartások számára az alapértelmezett beállítás szerint engedélyezett a részvétel a leképezés kikeresési műveletben, az irányelv társítások használata azonban tiltott. Ha az adminisztrátor engedélyezi az irányelv társítások használatát egy egyedi nyilvántartás számára, akkor biztosítania kell azt is, hogy egy a lehetőség a tartomány számára is engedélyezett legyen.

Minden egyes nyilvántartáshoz háromféleképpen állíthatja be a leképezés kikeresések és az irányelv társítások használatát:

- Az adott nyilvántartáshoz egyáltalán nem lehet leképezés kikereséseket használni. Más szavakkal ha egy alkalmazás az adott nyilvántartás bevonásával hajt végre leképezés kikeresési műveletet, akkor a művelet meghiúsul és nem ad vissza eredményt.
- A leképezés kikeresési műveletek csak felhasználói azonosságok és EIM azonosítók közötti egyedi azonosító társításokat használhatnak. A leképezés kikeresések engedélyezettek a nyilvántartás számára, de az irányelv társítások használata tiltott.
- A leképezés kikeresési műveletek használhatják az egyedi azonosító társításokat, és amennyiben ilyenek nem léteznek, akkor az irányelv társításokat is (minden beállítás engedélyezett).

- | A leképezés irányelv támogatás és a leképezés kikeresés engedélyezésével kapcsolatban bővebb információkat az alábbi részeknél talál:
- | • Irányelv társítások engedélyezése a tartományban
- | • Leképezés kikeresések és irányelv társítások használatának engedélyezése egy cél nyilvántartásban

## EIM hozzáférés felügyelet

- | Az EIM felhasználók olyan felhasználók, akik egy előre meghatározott Egyszerűsített címtárhozzáférési protokoll (LDAP) felhasználói csoportbeli tagságuk alapján EIM hozzáférés felügyelettel rendelkeznek egy adott tartományban.
- | Ha EIM *hozzáférés felügyeletet* határoz meg egy felhasználóhoz, akkor a felhasználó belekerül a tartományhoz tartozó egyik LDAP felhasználói csoportba. Minden LDAP csoport rendelkezik jogosultsággal bizonyos EIM adminisztrátori feladatok elvégzésére az adott tartományban. Az EIM felhasználó által végrehajtható adminisztratív feladatokat (beleértve a kikeresési műveleteket is) az a hozzáférés felügyeleti csoport határozza meg, amelyikbe az adott felhasználó tartozik.

**Megjegyzés:** Az EIM konfigurálásához nem csak egy adott rendszeren, hanem a teljes hálózaton megbízhatónak kell lenni. Az EIM konfigurálásához szükséges jogosultság alapja nem az OS/400 felhasználói profil, hanem az EIM hozzáférés felügyelet jogosultsága. Az EIM hálózati erőforrás, nem pedig egy bizonyos rendszer hatáskörébe tartozó erőforrás, ezért nem ismeri fel az OS/400 rendszerhez kötődő különleges jogosultságokat, mint például az \*ALLOBJ vagy a \*SECADM. Az EIM beállítása után azonban az egyes feladatok végrehajtásához számos felhasználótípus alapján lehetséges a hitelesítés, beleértve az olyan OS/400 felhasználói profilokat is. Például az IBM Directory Server for iSeries (LDAP) termék az \*ALLOBJ és \*IOSYSCFG különleges jogosultsággal rendelkező OS/400 profilokat címtár adminisztrátorként kezeli.

- | Csak EIM adminisztrátori hozzáférés felügyelettel rendelkező felhasználók vehetnek fel más felhasználókat egy EIM hozzáférés felügyeleti csoportba vagy változtathatják meg más felhasználók hozzáférés felügyeleti beállításait. Ahhoz, hogy egy felhasználó tagja lehessen egy EIM hozzáférés felügyeleti csoportnak, rendelkeznie kell egy bejegyzéssel az EIM tartományvezérlőként működő címtár szerveren. Továbbá csak bizonyos típusú felhasználók lehetnek tagjai egy EIM hozzáférés felügyeleti csoportnak. A felhasználói azonosság lehet egy Kerberos azonosító, egy LDAP megkülönböztetett név vagy egy OS/400 felhasználói profil, ha meg van határozva a címtár szerveren.

- | **Megjegyzés:** Ahhoz, hogy a Kerberos azonosító típusú felhasználó az rendelkezésre álljon az EIM számára, be kell állítani a hálózati hitelesítési szolgáltatást a rendszeren. Ahhoz, hogy az OS/400 felhasználói profil típus az EIM rendelkezésére álljon, be kell állítani egy rendszerobjektum utótagot a címtár szerveren. Ez lehetővé teszi a címtár szervernek, hogy OS/400 rendszerobjektumokra, például OS/400 felhasználói profilokra hivatkozzon.

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

- | • **Egyszerűsített címtárhozzáférési protokoll (LDAP) adminisztrátor** Az LDAP adminisztrátor egy különleges megkülönböztetett név (DN) a címtárban: a teljes címtár adminisztrátora. Ezért az LDAP adminisztrátornak hozzáférése van az összes EIM adminisztrációs funkcióhoz, és a teljes címtárhoz is. Az ilyen hozzáférés felügyelettel rendelkező felhasználók az alábbi 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.
  - | – Irányelv társítások létrehozása és eltávolítása.
  - | – Igazolásszűrők létrehozása és eltávolítása.
  - | – Irányelv társítások használatának engedélyezése és letiltása a tartományban.
  - | – Leképezés kikeresések engedélyezése és letiltása egy nyilvántartásban.
  - | – Irányelv társítások használatának engedélyezése és letiltása egy nyilvántartásban.
  - | – EIM kikeresési műveletek végrehajtása.



- | – Azonosító társítások, irányelv társítások, igazolásszűrők, EIM azonosítók és EIM nyilvántartás meghatározások visszakeresése.
- | – EIM hozzáférés felügyeleti információk hozzáadása, eltávolítása és megjelenítése.
- | • **EIM adminisztrátor.** Ebben a hozzáférés felügyeleti csoportban található felhasználók az EIM tartomány összes EIM adatát kezelhetik. Az ilyen hozzáférés felügyelettel rendelkező felhasználók az alábbi műveleteket végezhetik el:
  - | – Tartomány törlése.
  - | – EIM azonosítók létrehozása és eltávolítása.
  - | – EIM nyilvántartás meghatározások létrehozása és eltávolítása.
  - | – Forrás, cél és adminisztrációs társítások létrehozása és eltávolítása.
  - | – Irányelv társítások létrehozása és eltávolítása.
  - | – Igazolásszűrők létrehozása és eltávolítása.
  - | – Irányelv társítások használatának engedélyezése és letiltása a tartományban.
  - | – Leképezés kikeresések engedélyezése és letiltása egy nyilvántartásban.
  - | – Irányelv társítások használatának engedélyezése és letiltása egy nyilvántartásban.
  - | – EIM kikeresési műveletek végrehajtása.
  - | – Azonosító társítások, irányelv társítások, igazolásszűrők, EIM azonosítók és EIM nyilvántartás meghatározások visszakeresése.
  - | – EIM hozzáférés felügyeleti információk hozzáadása, eltávolítása és megjelenítése.
- | • **Azonosító adminisztrátor.** Ebben a hozzáférés felügyeleti csoportban található felhasználók hozzáadhatnak és módosíthatnak EIM azonosítókat, és kezelhetik a forrás és adminisztrációs társításokat. Az ilyen hozzáférés felügyelettel rendelkező felhasználók az alábbi műveleteket végezhetik el:
  - | – EIM azonosítók létrehozása.
  - | – Forrás társítások hozzáadása és eltávolítása.
  - | – Adminisztrációs társítások hozzáadása és eltávolítása.
  - | – EIM kikeresési műveletek végrehajtása.
  - | – Azonosító társítások, irányelv társítások, igazolásszűrők, EIM azonosítók és EIM nyilvántartás meghatározások visszakeresése.
- | • **EIM leképezési műveletek.** Ebben a hozzáférés felügyeleti csoportban található felhasználók végrehajthatnak EIM leképezés kikeresési műveleteket. Az ilyen hozzáférés felügyelettel rendelkező felhasználók az alábbi műveleteket végezhetik el:
  - | – EIM kikeresési műveletek végrehajtása.
  - | – Azonosító társítások, irányelv társítások, igazolásszűrők, EIM azonosítók és EIM nyilvántartás meghatározások visszakeresése.
- | • **Nyilvántartás adminisztrátor.** Ebben a hozzáférés felügyeleti csoportban található felhasználók az összes EIM nyilvántartás meghatározás kezelésére jogosultak. Az ilyen hozzáférés felügyelettel rendelkező felhasználók az alábbi műveleteket végezhetik el:
  - | – Cél társítások hozzáadása és eltávolítása.
  - | – Irányelv társítások létrehozása és eltávolítása.
  - | – Igazolásszűrők létrehozása és eltávolítása.
  - | – Leképezés kikeresések engedélyezése és letiltása egy nyilvántartásban.
  - | – Irányelv társítások használatának engedélyezése és letiltása egy nyilvántartásban.
  - | – EIM kikeresési műveletek végrehajtása.
  - | – Azonosító társítások, irányelv társítások, igazolásszűrők, EIM azonosítók és EIM nyilvántartás meghatározások visszakeresése.
- | • **Kijelölt nyilvántartások adminisztrátora.** Ebben a hozzáférés felügyeleti csoportban található felhasználók csak egy adott felhasználói nyilvántartás meghatározásban (például Nyilvántartas\_X) kezelhetik az EIM információkat, és csak a megadott felhasználói nyilvántartás meghatározásban vehetik fel vagy törölhetik a cél társításokat. A

leképezés kikeresések és az irányelv társítások előnyeinek minél jobb kihasználása érdekében célszerű az ilyen hozzáférés felügyelettel rendelkező felhasználók számára az **EIM leképezés műveletek** hozzáférés felügyeletet is biztosítani. Az ilyen hozzáférés felügyelettel rendelkező felhasználók az alábbi műveleteket végezhetik el:

- Cél társítások létrehozása, eltávolítása és listázása az adott EIM nyilvántartás meghatározásában.
- Alapértelmezett tartomány irányelv társítások felvétele és eltávolítása.
- Irányelv társítások felvétele és eltávolítása az adott nyilvántartás meghatározásában.
- Igazolásszűrők felvétele az adott nyilvántartás meghatározásában.
- Leképezés kikeresések engedélyezése és letiltása az adott nyilvántartás meghatározáshoz.
- Irányelv társítások használatának engedélyezése és letiltása az adott nyilvántartásban meghatározásban.
- EIM azonosítók visszakeresése.
- Azonosító társítások és igazolásszűrő visszakeresése az adott nyilvántartás meghatározásában.
- EIM nyilvántartás meghatározás információk visszakeresése az adott nyilvántartás meghatározásában.

**Megjegyzés:** A **Kijelölt nyilvántartások adminisztrátora** és az **EIM leképezés kikeresési műveletek** hozzáférés felügyelettel egyaránt rendelkező felhasználók ezen kívül az alábbi műveletek végrehajtására is képesek:

- Irányelv társítások felvétele és eltávolítása az adott nyilvántartás meghatározásában.
- EIM kikeresési műveletek végrehajtása.
- Azonosító társítások, irányelv társítások, igazolásszűrők, EIM azonosítók és EIM nyilvántartás meghatározások visszakeresése.

Az alábbi fejezetek segítséget nyújtanak annak megállapításában, hogy egy adott EIM hozzáférés felügyelet biztosít-e jogosultságot bizonyos műveletek végrehajtására:

- EIM hozzáférés felügyeleti csoport: API jogosultság
- EIM hozzáférés felügyeleti csoport: EIM feladat jogosultság

## EIM hozzáférés felügyeleti csoport: API jogosultság

Az alábbi táblázatok az API által végzett EIM művelet szerint vannak rendezve. Minden táblázatban megjelenik az összes EIM API, a különböző EIM hozzáférés felügyeleti csoportok, illetve az egyes csoportok által végrehajtható EIM funkciók.

1. táblázat: Tartományok kezelése

EIM API	LDAP adminisztrátor	EIM adminisztrátor	Azonosítók adminisztrátor	EIM leképezés kikeresés	Nyilvántartás adminisztrátor	Kiválasztott nyilvántartás adminisztr.
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

2. táblázat: Azonosítók kezelése

EIM API	LDAP adminisztrátor	EIM adminisztrátor	EIM azonosító adminisztrátor	EIM leképezés kikeresés	EIM nyilvántartás adminisztrátor	Adott EIM nyilvántartás adminisztrátora
eimAddIdentifier	X	X	X	-	-	-
eimChangeIdentifier	X	X	X	-	-	-
eimListIdentifiers	X	X	X	X	X	X
eimRemoveIdentifier	X	X	-	-	-	-
eimGetAssociated Identifiers	X	X	X	X	X	X

3. táblázat: Nyilvántartások kezelése

EIM API	LDAP adminisztrátor	EIM adminisztrátor	EIM azonosító adminisztrátor	EIM leképezés kikeresés	EIM nyilvántartás adminisztrátor	Adott EIM nyilvántartás adminisztr.
eimAddApplicationRegistry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChangeRegistryUser	X	X	-	-	X	X
eimChangeRegistryAlias	X	X	-	-	X	X
eimGetRegistryNameFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistryAssociations	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: Azonosító társítások kezelése. Az `eimAddAssociation()` és `eimRemoveAssociation()` API hívások esetén négy paraméter határozza meg a hozzáadott vagy eltávolított társítás típusát. Az API hívások használatára vonatkozó jogosultság a paraméterekben meghatározott társítástípustól függ. Az alábbi táblázatban ezen API hívások esetén a társítás típusa is megjelenik.

EIM API	LDAP adminisztrátor	EIM adminisztrátor	EIM azonosító adminisztrátor	EIM leképezés kikeresés	EIM nyilvántartás adminisztrátor	Adott EIM nyilvántartás adminisztrátora
eimAddAssociation (adminisztrátori)	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 (adminisztrátori)	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: Irányelv társítások kezelése

EIM API	LDAP adminisztrátor	EIM adminisztrátor	EIM azonosító adminisztrátor	EIM leképezés kikeresés	EIM nyilvántartás adminisztrátor	Adott EIM nyilvántartás adminisztrátora
eimAddPolicyAssociation	X	X	-	-	X	X
eimAddPolicyFilter	X	X	-	-	X	X
eimListPolicyFilters	X	X	X	X	X	X
eimRemovePolicyAssociation	X	X	-	-	X	X
eimRemovePolicyFilter	-	-	-	-	-	-

6. táblázat: Leképezések kezelése

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

7. táblázat: Hozzáférés kezelése

EIM API	LDAP adminisztrátor	EIM adminisztrátor	EIM azonosító adminisztrátor	EIM leképezés kikeresés	EIM nyilvántartás adminisztrátor	Adott EIM nyilvántartás adminisztrátora
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

## Vállalati azonosság leképezés (EIM) hozzáférés felügyeleti csoport: EIM feladat jogosultság

Az alábbi táblázat a különböző Vállalati azonosság leképezés (EIM) hozzáférés felügyeleti csoportok közötti kapcsolatokat és a csoportok által végrehajtható feladatokat sorolja fel.

Noha az LDAP adminisztrátor nincs felsorolva a táblázatban, a hozzáférés felügyelet ezen szintje új EIM tartomány létrehozásához szükséges. Az LDAP adminisztrátor ugyanolyan hozzáféréssel rendelkezik, mint az EIM adminisztrátor, de az EIM adminisztrátor nem rendelkezik automatikusan LDAP adminisztrátori szinttel.

8. táblázat: 1. Táblázat: EIM hozzáférés felügyeleti csoportok

EIM feladatok	EIM adminisztrátor	Azonosító adminisztrátor	EIM leképezés kikeresési műveletek	Nyilvántartás adminisztrátor	Kiválasztott nyilvántartás adminisztrátora
Tartomány létrehozása	-	-	-	-	-
Tartomány törlése	X	-	-	-	-
Tartomány Módosítása	X	-	-	-	-
Írányelv társítások engedélyezése vagy letiltása a tartományhoz	X	-	-	-	-
Tartomány keresése	X	-	-	-	-
Rendszer-nyilvántartás felvétele	X	-	-	-	-
Alkalmazás-nyilvántartás felvétele	X	-	-	-	-
Nyilvántartás eltávolítása	X	-	-	-	-

8. táblázat: 1. Táblázat: EIM hozzáférés felügyeleti csoportok (Folytatás)

EIM feladatok	EIM adminisztrátor	Azonosító adminisztrátor	EIM leképezés kikeresési műveletek	Nyilvántartás adminisztrátor	Kiválasztott nyilvántartás adminisztrátora
Nyilvántartás módosítása	X	-	-	X	X
Nyilvántartás leképezés keresés engedélyezése vagy letiltása	X	-	-	X	X
Írányelv társítások engedélyezése vagy letiltása a nyilvántartáshoz	X	-	-	X	X
Nyilvántartások keresése	X	X	X	X	X
Azonosító felvétele	X	X	-	-	-
Azonosító eltávolítása	X	-	-	-	-
Azonosító módosítása	X	X	-	-	-
Azonosítók keresése	X	X	X	X	X
Társított azonosítók visszakeresése	X	X	X	X	X
Adminisztrátori társítás felvétele/eltávolítása	X	X	-	-	-
Forrás társítás felvétele/eltávolítása	X	X	-	-	-
Cél társítás felvétele/eltávolítása	X	-	-	X	X
Írányelv társítás felvétele/eltávolítása	X	-	-	X	X
Igazolásszűrő felvétele/eltávolítása	X	-	-	X	X
Igazolásszűrő keresése	X	X	X	X	X
Társítások keresése	X	X	X	X	X
Írányelv társítások keresése	X	X	X	X	X
Cél társítás visszakeresése forrás társítás alapján	X	X	X	X	-
Cél társítás visszakeresése az azonosító alapján	X	X	X	X	X

8. táblázat: 1. Táblázat: EIM hozzáférés felügyeleti csoportok (Folytatás)

EIM feladatok	EIM adminisztrátor	Azonosító adminisztrátor	EIM leképezés kikeresési műveletek	Nyilvántartás adminisztrátor	Kiválasztott nyilvántartás adminisztrátora
Nyilvántartás felhasználók módosítása	X	-	-	X	X
Nyilvántartás felhasználók keresése	X	X	X	X	X
Nyilvántartás álnév módosítása	X	-	-	X	X
Nyilvántartás álnévek keresése	X	X	X	X	X
Nyilvántartás visszakeresése álnév alapján	X	X	X	X	X
EIM hozzáférés felügyelet	X	-	-	-	-
Hozzáférés felügyeleti csoporttagok megjelenítése	X	-	-	-	-
EIM hozzáférés felügyelet megjelenítése megadott felhasználóhoz	X	-	-	-	-
EIM hozzáférés felügyelet visszakeresése	X	-	-	-	-

## EIM LDAP alapelvek

A Vállalati azonosság leképezés (EIM) egy Egyszerűsített címtárhozzáférési protokoll (LDAP) szervert használ tartományvezérlőként az EIM adatok tárolására. Következésképpen az adminisztrátoroknak meg kell érteniük az EIM beállításával és használatával kapcsolatos LDAP fogalmakat. Használhat például felhasználói azonossággént egy LDAP megkülönböztetett nevet az EIM beállításához és a hitelesítéshez az EIM tartományvezérlő felé.

Az EIM konfigurálásának és használatának érdekében az alábbi LDAP fogalmakkal kell tisztában lennie:

- Megkülönböztetett név
- Szülő megkülönböztetett név
- LDAP séma és más EIM megfontolások

### Megkülönböztetett név

A megkülönböztetett nevek Egyszerűsített címtárhozzáférési protokoll (LDAP) bejegyzések egy LDAP szerver bejegyzéseinek egyedi azonosítására és leírására. Az EIM tartomány információkat tároló címtár szerver beállításához az EIM konfigurációs varázsló nyújt segítséget. Mivel az EIM címtár szerveren tárolja az EIM adatokat, az EIM tartományvezérlő hitelesítés alapjául megkülönböztetett neveket is használhat.

A megkülönböztetett nevek a bejegyzés nevéből, illetve az LDAP címtárban az objektum felett található bejegyzések nevéből állnak. Egy teljes megkülönböztetett név például a `cn=NapJanos, 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=NapJanos` nevezi meg, így ez az RDN. A `cn=NapJanos` szülő megkülönböztetett neve az `o=IBM, c=US`. Az EIM általi felhasználásról további részleteket a következő témakörből tudhat meg: “Szülő megkülönböztetett név”.

Mivel az EIM címtár szerveren tárolja az EIM adatokat, a felhasználói azonosság megkülönböztetett név segítségével is végezheti a hitelesítést a tartományvezérlő felé. Az iSeries szerver EIM konfigurációját végző felhasználói azonosság is használhat megkülönböztetett nevet. Például az alábbi műveletek során használhat megkülönböztetett nevet:

- Címtár szerver beállítása EIM tartományvezérlőként. Ehhez létre kell hoznia az LDAP adminisztrátort azonosító megkülönböztetett nevet a címtár szerveren. Ha a címtár szerver még nem került beállításra, akkor a címtár 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. A megkülönböztetett névnek azt a felhasználót kell képviselnie, aki jogosult a címtárszerver 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 leképezés kikeresésének művelete 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.
- Igazolásszűrők létrehozásával határozza az igazolásszűrő irányelv társítás hatókörét. Igazolásszűrő létrehozásakor a Tárgy megkülönböztetett név (SDN), a Kibocsátó megkülönböztetett név (IDN), vagy egy igazolás segítségével meg kell határozni a szűrő az irányelv társítás által érintett igazolások meghatározására szolgáló feltételét.

A megkülönböztetett nevekről és ezek felhasználásáról a Címtár szerver alapelvek témakörben olvashat.

## Szülő megkülönböztetett név

A 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 névre akkor hivatkozunk szülő megkülönböztetett névként, ha az közvetlenül megy másik DN fölötti bejegyzés a címtárban.

Egy teljes megkülönböztetett név például a `cn=NapJanos, 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=NapJanos` nevezi meg, így ez az RDN. A `cn=NapJanos` szülő megkülönböztetett neve az `o=IBM, c=US`.

- Az EIM a címtárszerveret tartományvezérlőként használja az EIM adatok tárolására. A szülő DN az EIM tartománynévvel kombinálva egyértelműen meghatározza az EIM tartományadatokat helyét a címtárszerver névterében.
- Amikor 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 az LDAP névtér mely részébe kerüljenek. Ha nem adja meg a szülő megkülönböztetett nevet, akkor az EIM adatok a saját utótagjukban kapnak helyet a névtérben, és az EIM tartományadatokat alapértelmezett helye **`ibm-cimDomainName=EIM`**.

A megkülönböztetett nevekről és ezek felhasználásáról a Címtár szerver alapelvek témakörben olvashat.

## LDAP séma és egyéb Vállalati azonosság leképezéssel (EIM) kapcsolatos szempontok

- A V5R3 kiadásban a Vállalati azonosság leképezés (EIM) megköveteli, hogy a tartományvezérlőt 3-as verziójú Egyszerűsített címtárhozzáférési protokollt (LDAP) támogató címtár szerver szolgáltatassa. Továbbá az is követelmény, hogy a címtár szerver terméknek képesnek kell lennie az EIM séma elfogadására, és fel kell ismernie az alábbi attribútumokat és objektumosztályokat:

- | • Az `ibm-entryUUID` attribútum.
- | • Az `ibm` attribútum típusok:
  - | – `acIEntry`
  - | – `acIPropagate`
  - | – `acISource`
  - | – `entryOwner`
  - | – `ownerPropagate`
  - | – `ownerSource`
- | • Az EIM attribútumok, beleértve az irányelv társítások támogatását szolgáló három új attribútumot:
  - | – `ibm-eimAdditionalInformation`
  - | – `ibm-eimAdminUserAssoc`
  - | – `ibm-eimDomainName`, `ibm-eimDomainVersion`,
  - | – `ibm-eimRegistryAliases`
  - | – `ibm-eimRegistryEntryName`
  - | – `ibm-eimRegistryName`
  - | – `ibm-eimRegistryType`
  - | – `ibm-eimSourceUserAssoc`
  - | – `ibm-eimTargetIdAssoc`
  - | – `ibm-eimTargetUserName`
  - | – `ibm-eimUserAssoc`
  - | – `ibm-eimFilterType`
  - | – `ibm-eimFilterValue`
  - | – `ibm-eimPolicyStatus`
- | • Az EIM objektumosztályok, beleértve az irányelv társítások támogatását szolgáló három új objektumosztályt:
  - | – `ibm-eimApplicationRegistry`
  - | – `ibm-eimDomain`
  - | – `ibm-eimIdentifier`
  - | – `ibm-eimRegistry`
  - | – `ibm-eimRegistryUser`
  - | – `ibm-eimSourceRelationship`
  - | – `ibm-eimSystemRegistry`
  - | – `ibm-eimTargetRelationship`
  - | – `ibm-eimFilterPolicy`
  - | – `ibm-eimDefaultPolicy`
  - | – `ibm-eimPolicyListAux`


| Az IBM Directory Server for iSeries V5R3 kiadása tartalmazza ezt a támogatást. Az EIM tartományvezérlő megtervezése részben bővebb információkat talál arról, hogy mely IBM cím tár server termékek tartalmazzák az EIM által megkövetelt szolgáltatásokat, továbbá az EIM tartományvezérlőkkel kapcsolatos egyéb szempontokról is olvashat.

| Amennyiben jelenleg egy V5R2 kiadású iSeries rendszer cím tár serverét használja EIM tartományvezérlőként, akkor a V5R3 kiadású EIM tartományadatok kezeléséhez frissítenie kell a server LDAP sémáját és EIM támogatását. Erről

| bővebben az iSeries LDAP  lapon olvashat az IBM webhelyén.



## iSeries Vállalati azonosság leképezés (EIM) alapelvek

A Vállalati azonosság leképezést (EIM) bármely IBM  platformon megvalósíthatja. Azonban ha az EIM megvalósítása iSeries rendszeren történik, akkor figyelembe kell venni néhány, az iSeries megvalósításokra vonatkozó különleges körülményt. Tanulmányozza az alábbi információkat az EIM támogatással rendelkező OS/400 alkalmazásokkal, illetve a felhasználói profilokkal és a hatékony iSeries EIM megvalósításokra vonatkozó egyéb témakörökkel kapcsolatban.

- OS/400 felhasználói profilokkal kapcsolatos Vállalati azonosság leképezés megfontolások
- OS/400 megfigyelése a Vállalati azonosság leképezés (EIM) számára
- EIM támogatással rendelkező OS/400 alkalmazások

## OS/400 felhasználói profilokkal kapcsolatos Vállalati azonosság leképezés megfontolások

A Vállalati azonosság leképezés (EIM) műveletek végrehajtása nem az OS/400 felhasználói profil jogosultságán, hanem az "EIM hozzáférés felügyelet" oldalszám: 34 jogosultságán alapszik. Néhány további feladatot azonban el kell végezni ahhoz, hogy az OS/400 képes legyen az EIM használatára. Ezekhez a feladatokhoz szükség van egy megfelelő különleges jogosultságokkal rendelkező OS/400 felhasználói profilra.

Ha az OS/400 rendszert az iSeries navigátorból segítségével be kívánja állítani az EIM használatához, akkor az alábbi különleges jogosultságokra lesz szüksége:

- Biztonsági adminisztrátor (\*SECADM).
- Minden objektum (\*ALLOBJ).
- Rendszerkonfiguráció (\*IOSYSCFG).

## OS/400 felhasználói profil parancs továbbfejlesztés az EIM azonosítókhoz

Az EIM beállítása után a rendszeren kihasználhatja a Felhasználói profil létrehozása (CRTUSRPRF) és a Felhasználói profil módosítása (CHGUSRPRF) parancsok új paramétereinek előnyeit. A paraméter segítségével EIM azonosító társításokat határozhat meg a megadott felhasználói profilhoz a helyi nyilvántartásban.

A paraméter használatakor az alábbi információkat adhatja meg:

- EIM azonosító név, ami lehet egy új vagy egy létező azonosító név.
- A művelet paraméter, ami lehet hozzáadás (\*ADD), csere (\*REPLACE) vagy eltávolítás (\*REMOVE).

**Megjegyzés:** Új társítások esetén használja a \*ADD értéket. A \*REPLACE érték például akkor lehet hasznos, ha korábban rossz azonosítóhoz adott meg társításokat. A \*REPLACE paraméter eltávolít egy adott azonosítóhoz tartozó adott típusú társítást a helyi nyilvántartásból, majd hozzáadja helyette a paraméter által meghatározott társítást. A \*REMOVE művelet eltávolítja az adott társításokat az adott azonosítóról.

- Az azonosító társítás típusa, ami lehet cél, forrás, mindkettő vagy adminisztrációs társítás.
- Szükséges-e létrehozni a megadott EIM azonosítót, ha nem létezik.

Egy OS/400 profilhoz jellemzően cél társítást kell létrehozni, különösen egyszeri bejelentkezés környezetben. Miután a parancs segítségével létrehozta a szükséges cél társítást (és szükség esetén az EIM azonosítót) a felhasználói profilhoz, létre kell hoznia megfelelő forrás társítást. Az iSeries navigátorban hozzon létre egy forrás társítást egy másik felhasználói azonossághoz, például ahhoz a Kerberos azonosítóhoz, amellyel a felhasználó bejelentkezik a hálózatra.

Az EIM konfigurálása során meg kellett adni egy felhasználó azonosságát és jelszót, amelyet az operációs rendszer nevében végrehajtott EIM műveletekhez használ a rendszer. Ennek a felhasználói azonosságnak rendelkeznie kell az azonosító létrehozásához és társítások felvételéhez szükséges EIM hozzáférés felügyelet jogosultsággal.

## OS/400 felhasználói profil jelszavak és az EIM

Amikor az adminisztrátor az EIM beállítását egyszeri bejelentkezési környezet részeként végzi el, akkor az elsődleges célja a tipikus vállalati végfelhasználókkal kapcsolatos felhasználói jelszókezeléssel kapcsolatos feladatok csökkentése. Az EIM által biztosított azonosság leképezés és a Kerberos hitelesítés együttes használatával a felhasználóknak kevesebb bejelentkezést kell végrehajtaniuk és kevesebb jelszót kell megjegyezniük és kezelniük. Az adminisztrátornak sok ideje felszabadul azáltal, hogy kevesebbet kell foglalkoznia a leképezett felhasználói azonosságok karbantartásával, például az elfelejtett jelszavak visszaállításával. Azonban a szervezet jelszóbiztonsági házirendje továbbra is életben van, és az adminisztrátornak időt kell fordítania a lejárt jelszavú felhasználói profilok kezelésére.

Az egyszeri bejelentkezési környezet egyik további előnye közé tartozik, hogy meg lehet változtatni az azonosság leképezések céljaként szereplő felhasználói profilok jelszóbeállításait. Mivel a felhasználói profil egy azonosság leképezés célja, ezért a felhasználónak nem kell megadnia a jelszót amikor egy iSeries rendszeren található vagy EIM támogatással rendelkező OS/400 erőforrást ér el. Az átlagos felhasználó esetében megfelelő a \*NONE jelszóbeállítás, ami azt jelenti, hogy nem lehet jelszót használni az adott felhasználói profillal. A felhasználói profil tulajdonosának nincs többé jelszóra szüksége az azonosság leképezés és az egyszeri bejelentkezés miatt. A \*NONE jelszónak további előnyei vannak, mert a felhasználóknak és az adminisztrátornak nem kell a jelszó lejáráásával törődniük, továbbá a profil felhasználásával senki nem jelentkezhet be közvetlenül egy iSeries rendszerre, és nem érhet el EIM támogatással rendelkező OS/400 erőforrásokat. Érdemes azonban megfontolni, hogy az adminisztrátorok továbbra is rendelkezzenek jelszóval, mert előfordulhat, hogy közvetlenül be kell jelentkezniük az iSeries rendszerre. Ha például az EIM tartományvezérlő kiesik és az azonosság leképezések nem tudnak lefutni, akkor az adminisztrátoroknak addig is be kell tudniuk jelentkezni az iSeries rendszerre, amíg a probléma a tartományvezérlővel meg nem oldódik.

## OS/400 megfigyelése a Vállalati azonosság leképezés (EIM) számára

Az általános biztonsági terv fontos része annak eldöntése, hogy mit szükséges megfigyelni. Amennyiben a Vállalati azonosság leképezés (EIM) használata mellett dönt, úgy be kell állítania a címtárkiszolgálón a megfigyelés támogatását, hogy rendelkezésre álljon a biztonsági stratégiának megfelelő szintű felelősségre vonhatóság. A megfigyelés támogatása hasznos lehet például annak megállapításában, hogy az irányelv társítás által leképezett felhasználók közül melyik hajtott végre műveletet vagy változtatott meg egy objektumot a rendszeren.

Az IBM Directory Server for iSeries (LDAP) megfigyelés támogatásával kapcsolatban olvassa el a Megfigyelés részt az IBM Directory Server for iSeries (LDAP) témakörben az Információs központban. A dokumentum az OS/400 megfigyeléssel kapcsolatos szempontjaira és beállításaira vonatkozó hivatkozásokat is tartalmaz, amelyek elengedhetetlenül szükségesek a címtárszerver megfigyelésének helyes beállításához.

## Vállalati azonosság leképezés (EIM) támogatással rendelkező OS/400 alkalmazások

Az alábbi OS/400 alkalmazásokat lehet beállítani a Vállalati azonosság leképezés (EIM) használatára:

- OS/400 hoszt szerverek (jelenleg az iSeries Access for Windows és az iSeries navigátor használja.)
- Telnet Server (jelenleg a PC5250 és az IBM Websphere Host On-Demand) használja)
- QFileSrv.400 ODBC (egyszeri bejelentkezést tesz lehetővé SQL-en keresztül)
- JDBC (lehetővé teszi az EIM használatát SQL-en keresztül)
- Osztott relációs adatbázis felépítés (DRDA) (lehetővé teszi az EIM használatát SQL-en keresztül)
- IBM WebSphere Host On-Demand Version 8, (Web Express bejelentkezési szolgáltatás)
- Hálózati szerver
- QFileSvr.400

---

## Vállalati azonosság leképezés (EIM) megtervezése

A megvalósítási terv alapvető fontosságú a Vállalati azonosság leképezés (EIM) sikeres beállításához és használatához a vállalatban. A terv elkészítéséhez adatokat kell gyűjteni a rendszerekről, az alkalmazásokról és a felhasználókról. Az összegyűjtött információk felhasználásával meg lehet hozni azokat a döntéseket, amelyek az EIM a vállalat igényeinek leginkább megfelelő beállítását eredményezik.

Mivel az EIM egy IBM **@server** infrastruktúra technológia, amely az összes IBM platformon elérhető, a megvalósítás nagyban függ a vállalat rendelkezésre álló platformoktól. Noha minden egyes platformhoz léteznek csak az adott környezetben jellemző egyedi tervezési lépések, az EIM tervezésével kapcsolatos legtöbb teendő az összes IBM platformon közös. Hajtsa végre az általános EIM tervezési lépéseket az átfogó EIM megvalósítási terv elkészítéséhez. Az EIM megvalósítással az alábbi oldalakon ismerkedhet meg:

- **@server** EIM megvalósítás tervezése Ez az anyag az átfogó EIM megvalósítás megtervezésével foglalkozik.
- OS/400 EIM megtervezése Ez az anyag az EIM OS/400 megvalósításának tervezésével foglalkozik.

## Vállalati azonosság leképezés (EIM) megtervezése eServer rendszeren

A megvalósítási terv alapvető fontosságú a Vállalati azonosság leképezés (EIM) sikeres beállításához és használatához egy heterogén vállalati környezetben. A megvalósítási terv elkészítéséhez adatokat kell gyűjteni a rendszerekről, az alkalmazásokról és a felhasználókról. Az összegyűjtött információk felhasználásával meg lehet hozni azokat a döntéseket, amelyek az EIM a heterogén vállalati környezet igényeinek leginkább megfelelő beállítását eredményezik.

Az alábbi lista azokat a tervezési feladatokat tartalmazza, amelyeket az EIM beállítása és használata előtt kell elvégezni egy többféle platformot tartalmazó környezetben. Az alábbi fejezetek tartalmazzák az EIM konfigurációjának sikeres megtervezéséhez szükséges információkat, beleértve a megvalósításért felelős csoport tagjai számára szükséges jártasságok, az összegyűjtendő információk és a fontosabb meghozandó döntések felsorolását. Hasznos lehet kinyomtatni és a tervezési folyamat során kitölteni az EIM tervezési munkalapokat (az alábbi lista 8-as pontja).

1. EIM telepítési követelmények
2. Szükséges jártasságok, szerepkörök és jogosultságok azonosítása
3. EIM tartomány megtervezése
4. EIM tartományvezérlő megtervezése
5. EIM nyilvántartás meghatározások elnevezési megállapodásának kialakítása
6. EIM azonosítók elnevezési megállapodásának kialakítása
7. Alkalmazás fejlesztéssel kapcsolatos megfontolások
8. EIM megvalósítás tervezési munkalapok

## Vállalati azonosság leképezés (EIM) telepítési követelményei eServer rendszeren

Az EIM sikeres bevezetéséhez szükséges követelmények három fő csoportra oszthatók:

1. Vállalati vagy hálózati szintű követelmények
2. Rendszerkövetelmények
3. Alkalmazáskövetelmények

### Vállalati vagy hálózati szintű követelmények

Be kell állítania egy rendszert EIM tartományvezérlőnek, ami általában az EIM adatokat tároló és szolgáltató különlegesen beállított Egyszerűsített címtárhozzáférési protokoll (LDAP) szerver. Számos szempontot kell figyelembe venni annak eldöntésekor, hogy milyen címtár szolgáltatást megvalósító terméket használ tartományvezérlőként, többek között azt is, hogy nem minden LDAP szerver tartalmaz EIM tartományvezérlő támogatást.

Egy másik szempont lehet az adminisztrációs eszközök hozzáférhetősége. Egy lehetőség az, hogy az EIM API segítségével megvalósítja az adminisztrációs funkciókat az alkalmazásaiban. Amennyiben a Directory Server for iSeries (LDAP) terméket tervezi használni EIM tartományvezérlőként, akkor rendelkezésére áll az iSeries navigátor az EIM kezeléséhez. Ha az IBM Directory termék mellett dönt, akkor használhatja az eimadmin segédprogramot, amely a V1R4 LDAP SPE része.

Az alábbiakban alapvető információkat olvashat arról, hogy mely IBM platformok tartalmazzák EIM támogatással rendelkező címtárszerver terméket. A tartományvezérlő támogatást biztosító címtárszerver kiválasztásáról bővebb információkat talál az EIM tartományvezérlő tervezése témakörnél.

### Rendszer- és alkalmazás követelmények

l Az EIM tartományban található összes rendszernek teljesíteni kell az alábbi követelményeket:

- l • LDAP kliens szoftvernek telepítve kell lennie.
- l • Rendelkeznie kell egy EIM API megvalósítással.

l Az EIM tartomány összes rendszerének képesnek kell lennie az EIM API használatára a leképezés keresés és egyéb műveletek végrehajtásához.


l **Megjegyzés:** Osztott alkalmazás esetén nem feltétlenül szükséges, hogy a szerver és a kliens egyaránt képes legyen az EIM API kezelésére. Általánosságban elegendő, ha az alkalmazás szerveroldali része képes az EIM API használatára.

l Az alábbi táblázat az **eServer** platformok által biztosított EIM támogatásról tartalmaz információkat. Az információk platform szerint vannak rendszerezve, az oszlopok az alábbiakat jelölik:

- l • Az adott környezetben az EIM API támogatásához szükséges kliens.
- l • A platformon rendelkezésre álló EIM konfigurációs és adminisztrációs eszközök.
- l • A platformon telepíthető EIM tartományvezérlőként szolgáló címtárszerver termék.

l A platformnak feltétlenül kell feltétlenül képesnek lennie EIM tartományvezérlőként működni ahhoz, hogy tagja lehessen egy EIM tartománynak.

l **9. táblázat: eServer EIM támogatás**

Platform	EIM kliens (API támogatás)	Tartományvezérlő	EIM adminisztrációs eszközök
AIX pSeries rendszeren	AIX R5.2	IBM Directory V5.1	Nem áll rendelkezésre
LINUX <ul style="list-style-type: none"><li>• SLES8 PPC64 rendszeren</li><li>• Red Hat 7.3 i386 rendszeren</li><li>• SLES7 zSeries rendszeren</li></ul>	Töltse le az alábbiak egyikét: <ul style="list-style-type: none"><li>• IBM Directory V4.1 kliens</li><li>• IBM Directory V5.1 kliens</li><li>• Open LDAP v2.0.23 kliens</li></ul> 	IBM Directory V5.1	Nem áll rendelkezésre
OS/400 iSeries rendszeren	OS/400 V5R2 és OS/400 V5R3	OS/400 V5R2 és V5R3 Directory Server	iSeries navigátor V5R2 és V5R3
Windows 2000 xSeries rendszeren	Töltse le az alábbiak egyikét: <ul style="list-style-type: none"><li>• IBM Directory V4.1 kliens</li><li>• IBM Directory V5.1 kliens</li></ul>	IBM Directory V5.1 kliens	Nem áll rendelkezésre
z/OS zSeries rendszeren	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP	V1R4 LDAP SPE OW57137

l **Megjegyzés:** Az IBM Directory Server termékről bővebb információkat az IBM webhelyén a <http://www-3.ibm.com/software/network/help-directory/> címen.

l Amennyiben egy platform tartalmaz EIM kliens (API) támogatást, akkor része lehet EIM tartománynak. Elegendő csak annak a platformnak EIM tartományvezérlő támogatást biztosítania, amelyik környezetben ezt a szolgáltatást meg kívánja valósítani.

l Miután meggyőződött róla, hogy az EIM összes követelménye teljesül, akkor folytathatja tovább a szükséges képességek, szerepek és jogosultságok azonosítása témakörrel az EIM konfigurálását.

## l **Szükséges képességek és szerepkörök azonosítása**

l Az Vállalati azonosság leképezést úgy tervezték, hogy egy kis szervezet konfigurációs és adminisztrációs feladatait egyetlen személy is könnyen el tudja látni. Egy nagyobb szervezet esetében azonban indokolt lehet, hogy több személy

l lássa el ezeket a feladatokat. A szükséges csapattagok száma függ attól, hogy az egyes személyek a kívánt jártasságok  
 l közül melyekkel rendelkeznek, továbbá az EIM megvalósításba bevont platformok típusától és a szervezet biztonság  
 l szerepkörökre és felelőségekre vonatkozó politikájától.

l Egy sikeres EIM megvalósításhoz számos szoftvertermék beállítására és együttműködésére van szükség. Mivel ezen  
 l termékek mindegyike különleges jártasságok meglétét és szerepkörök kialakítását követeli meg, az EIM  
 l megvalósításért felelős csapatot különböző területekről származó szakemberekből kell összeállítani. Különösen igaz ez  
 l egy nagy szervezet esetében.

l Az alábbi információk az EIM sikeres megvalósításához szükséges jártasságokat és “EIM hozzáférés felügyelet”  
 l oldalszám: 34 jogosultságokat tartalmazzák. A jártasságok az adott ismeretre szakosodott személyekhez tartozó  
 l munkakörök szerint vannak megadva. Például egy Egyszerűsített címtárhozzáférési protokoll (LDAP) jártasságot  
 l igénylő feladatra címtár szerver adminisztrátori feladatként történik a hivatkozás.

### l **Csapattagok és szerepkörök**

l Az alábbi információk az EIM kezeléséhez szükséges felelőségeket és az egyes szerepekhez szükséges  
 l jogosultságokat írják le. A szerepek listájának segítségével meghatározhatja az EIM megvalósításához nélkülözhetetlen  
 l termékek telepítéséhez és az EIM illetve a tartományok beállításához szükséges csapattagokat.

l Az elsők között kell meghatározni azt, hogy hány EIM tartomány adminisztrátor legyen a csapatban, és ezek milyen  
 l típusúak legyenek. A megvalósítási csapat tagjaként minden olyan személyt be kell vonni az EIM tervezés  
 l folyamatába, akinek adminisztratív feladata és jogosultsága lesz.

l **Megjegyzés:** Az EIM adminisztrátorok fontos szerepet játszanak a szervezetben és egyénileg olyan szakmai erőt  
 l képviselnek, hogy jogosultak felhasználói azonosságok létrehozására a rendszerben. Amikor EIM  
 l társításokat hoznak létre a felhasználói azonosságok számára, akkor azt meghatározzák meg, hogy ki és  
 l milyen jogosultsággal érheti el a szervezet számítógéprendszereit. Az IBM ajánlása szerint ezzel a joggal  
 l olyan személyeket kell felruházni, akik a társaság biztonsági politikája szerint nagyfokú bizalmat  
 l élveznek.

l Az alábbi táblázat a lehetséges csapattagok szerepköreit, illetve az EIM konfigurálásához és kezeléséhez szükséges  
 l jártasságokat, valamint a feladatokat tartalmazza. Az egyes szerepkörök által végrehajtható EIM adminisztrációs  
 l feladatokról részletesebb információkat az “EIM hozzáférés felügyelet” oldalszám: 34 részben talál.

l **Megjegyzés:** Ha a szervezetben az összes EIM adminisztrációs és konfigurációs feladat egyetlen személy felelőssége,  
 l akkor ennek a személynek EIM adminisztrátori szerepkörrel és jogosultságokkal kell rendelkeznie.

l *10. táblázat: EIM konfigurációhoz kapcsolódó szerepkörök, feladatok és jártassághoz*

Szerepkör	Jogosult feladatok	Szükséges jártasságok
EIM adminisztrátor	<ul style="list-style-type: none"> <li>Tartomány műveletek összehangolása</li> <li>Nyilvántartás meghatározások, EIM azonosítók illetve felhasználói azonosságokhoz tartozó társítások felvétele, eltávolítása és módosítása</li> <li>Vezérlő jogosultság az EIM tartományban található adatokhoz</li> </ul>	Az EIM adminisztrációs eszközök ismerete
EIM azonosító adminisztrátor	<ul style="list-style-type: none"> <li>EIM azonosítók létrehozása és módosítása</li> <li>Adminisztrációs és forrás társítások hozzáadása és eltávolítása (nem vonatkozik a cél társításokra)</li> </ul>	Az EIM adminisztrációs eszközök ismerete

10. táblázat: EIM konfigurációhoz kapcsolódó szerepkörök, feladatok és jártassághoz (Folytatás)

Szerepkör	Jogosult feladatok	Szükséges jártasságok
EIM nyilvántartás adminisztrátor	Minden EIM nyilvántartás meghatározás kezelése: <ul style="list-style-type: none"> <li>Cél társítások hozzáadása és eltávolítása (nem vonatkozik a forrás és adminisztrációs társításokra)</li> <li>EIM nyilvántartás meghatározások frissítése</li> </ul>	Az alábbiak ismerete: <ul style="list-style-type: none"> <li>Az EIM tartományban megadott összes felhasználói nyilvántartás (beleértve az összes felhasználói azonosságra vonatkozó információkat)</li> <li>Az EIM adminisztrációs eszközök</li> </ul>
Adott EIM nyilvántartás adminisztrátora	Egy adott EIM nyilvántartás meghatározás kezelése: <ul style="list-style-type: none"> <li>Cél társítások hozzáadása és eltávolítása egy adott felhasználói nyilvántartásban</li> <li>Egy adott EIM nyilvántartás meghatározás frissítése</li> </ul>	Az alábbiak ismerete: <ul style="list-style-type: none"> <li>Az EIM tartományban megadott egyik felhasználói nyilvántartás (beleértve az felhasználói azonosságokra vonatkozó információkat)</li> <li>Az EIM adminisztrációs eszközök</li> </ul>
Címtár kiszolgáló (LDAP) adminisztrátor	<ul style="list-style-type: none"> <li>Címtár szerver telepítése és konfigurálása (ha szükséges)</li> <li>Címtár szerver konfigurációjának beállítása az EIM igényei szerint</li> <li>EIM tartomány létrehozása (lásd a megjegyzést)</li> <li>Az EIM tartományvezérlő elérésére jogosult felhasználó meghatározása</li> <li>Választható: Az első EIM adminisztrátor megadása</li> </ul> <p><b>Megjegyzés:</b> A címtár szerver adminisztrátor mindent megtehet, amire az EIM adminisztrátornak joga van.</p>	Az alábbiak ismerete: <ul style="list-style-type: none"> <li>Címtár szerver telepítése, összeállítása és testreszabása</li> <li>EIM adminisztrációs eszközök</li> </ul>
Felhasználói nyilvántartás adminisztrátor	<ul style="list-style-type: none"> <li>Felhasználói profilok vagy felhasználói azonosságok beállítása az adott felhasználói nyilvántartásban.</li> <li>Választható: az adott felhasználói nyilvántartás EIM adminisztrátoraként is szolgálhat</li> </ul>	Az alábbiak ismerete: <ul style="list-style-type: none"> <li>A felhasználói nyilvántartás felügyeletéhez szükséges eszközök</li> <li>EIM adminisztrációs eszközök</li> </ul>
Rendszerprogramozó vagy rendszeradminisztrátor	Szükséges szoftvertermékek telepítése (tartalmazhatja az EIM telepítését is)	Az alábbiak ismerete: <ul style="list-style-type: none"> <li>Rendszerprogramozási vagy -adminisztrációs jártasságok</li> <li>A platform telepítési eljárásai</li> </ul>
Alkalmazásprogramozó	EIM API hívásokat használó alkalmazások készítése	Az alábbiak ismerete: <ul style="list-style-type: none"> <li>A platform</li> <li>Jártasság a programozásban</li> <li>Programok fordítása</li> </ul>

Miután megállapította, hogy milyen szerepkörökre lesz szükség az EIM beállításához és kezeléséhez a vállalatban, készítse el az EIM tartomány tervét.

### Vállalati azonosság leképezés (EIM) tartomány megtervezése

A Vállalati azonosság leképezés (EIM) megvalósítás tervezési folyamatának részeként meg kell tervezni az EIM tartományt. Ahhoz, hogy a leképezési információk központosított tárolásának előnyeit a lehető legjobban ki lehessen használni, úgy kell megtervezni a tartományt, hogy minél több alkalmazás és rendszer osztozzon rajta.

| Az EIM tervezési folyamattal foglalkozó témakörök feldolgozása során a tartomány megadásához szükséges  
 | összegyűjtött információk rögzítésre kerülnek a tervezési munkalapokon. A mintaként közölt munkalaprészek  
 | útmutatóul szolgálnak az információk összegyűjtéséhez és rögzítéséhez a témakörben tárgyalt összes tervezési fázisban.

| Az alábbi táblázat tartalmazza a tartomány tervezésekor összegyűjtendő információkat, és javaslatokat tesz arra, hogy  
 | az EIM megvalósító csapat mely szerepköreinek felelőssége legyen az adott információs elem.

| **Megjegyzés:** A táblázat az adott szerepkör az információk összegyűjtésére vonatkozó felelősségét csak javaslatként  
 | tartalmazza, a szerepek végleges kiosztását mindig a szervezet igényei és biztonsági politikájának  
 | megfelelően kell kialakítani. Például egy kisebb szervezetben célszerű lehet egyetlen személyt EIM  
 | adminisztrátorrá kinevezni, és az EIM tervezésének, beállításának és kezelésének minden aspektusáért  
 | egy személyben felelőssé tenni.

| 11. táblázat: Az EIM tartomány tervezéséhez szükséges információk

Szükséges információk	Szerepkör
1. Létezik-e az igényeknek megfelelő tartomány, vagy létre kell hozni egyet.	EIM adminisztrátor
2. Melyik cím tár szerver fog tartományvezérlőként szolgálni? (Lásd az EIM tartományvezérlő megtervezése részt a tartományvezérlő kiválasztásával kapcsolatos információkkal kapcsolatban.)	Cím tár szerver (LDAP) adminisztrátor vagy EIM adminisztrátor
3. A tartomány neve. (Megadhat egy nem kötelező leírást is.)	EIM adminisztrátor
4. Az EIM adatok tárolásának helye a cím tárban. <b>Megjegyzés:</b> Az EIM adatok tárolását végző cím tár szerver futtatásához kiválasztott rendszertől és magától a cím tártól függően a tartomány létrehozása előtt bizonyos cím tár szolgáltatások beállítási feladatokat végre kell hajtani.	A cím tár szerver (LDAP) adminisztrátor vagy EIM adminisztrátor
5. A tartományban részvevő alkalmazások és operációs rendszerek. Ha ez az első beállított tartomány, akkor elképzelhető, hogy csak egyetlen rendszert tartalmaz. (Bővebb információkért lásd az EIM nyilvántartás meghatározások elnevezési terve részt.)	EIM csapat
5. A tartományban részvevő személyek és entitások. <b>Megjegyzés:</b> A kezdeti tesztelés egyszerűsítése érdekében érdemes a részvevők számát egyre vagy kettőre korlátozni.	EIM csapat

| Most, miután megismerte, hogy mire lesz szükség az EIM tartomány meghatározásához, hozzáfoghat az EIM  
 | tartomány adatok tárolásáért felelős EIM tartományvezérlő megtervezéséhez.

## Vállalati azonosság leképezés (EIM) tartományvezérlő megtervezése

| A Vállalati azonosság leképezés (EIM) megtervezése során fontos lépés annak eldöntése, hogy milyen cím tár szerver  
 | termék fogja kiszolgálni az EIM tartományvezérlőt. A V5R3 kiadásban a Vállalati azonosság leképezés (EIM)  
 | megköveteli, hogy a tartományvezérlőt 3-as verziójú Egyszerűsített cím tárhozzáférési protokollt (LDAP) támogató  
 | cím tár szerver szolgáltassa. Továbbá az is követelmény, hogy a cím tár szerver terméknek képesnek kell lennie az  
 | LDAP séma és az EIM egyéb alapfogalmainak kezelésére, és fel kell ismernie bizonyos attribútumokat és  
 | objektumosztályokat.

| Ha a vállalat egynél több, az EIM tartományvezérlő kiszolgálására alkalmas cím tár szerverrel rendelkezik, akkor  
 | érdemes megfontolni a másodlagos többszörözött tartományvezérlők használatának lehetőségét. Nagy mennyiségű  
 | EIM leképezés kikeresési művelet esetén a másolat szerverek megnövelhetik a rendszer teljesítményét.

| Azt is érdemes átgondolni, hogy a tartományvezérlő *helyi* vagy *távoli* legyen ahhoz a rendszerhez képest, amelyen a  
 | leképezés kikeresési művelet a legnagyobb számban várható. Azzal is lehet növelni A teljesítményt, hogy a

l tartományvezérlő a legnagyobb terhelésnek kitett rendszerre kerül. Rögzítse ezeket, illetve a tartománnyal és más  
l címtár információkkal kapcsolatos egyéb tervezési döntéseket a tervezési munkalapon.

l Miután meghatározta, hogy a vállalat mely címtár szervere fogja kiszolgálni a tartományvezérlőt, meg kell hozni  
l néhány fontos döntést a tartományvezérlő elérésével kapcsolatban.

### l **Tartományvezérlő elérésének megtervezése**

l Meg kell terveznie, hogy az EIM támogatással rendelkező alkalmazások és operációs rendszerek hogyan fogják elérni  
l az EIM tartományvezérlőt kiszolgáló címtár szervert. Az EIM tartomány eléréséhez az alábbiakra van szükség:

- l 1. Képesnek kell lenni kötetést létrehozni az EIM tartományvezérlőhöz
- l 2. győződjön meg róla, hogy a kötés tárgya tagja egy EIM hozzáférés felügyeleti csoportnak, vagy pedig LDAP  
l adminisztrátori jogosultsággal rendelkezik. Ezzel kapcsolatban bővebb információkat az EIM hozzáférés felügyelet  
l kezelése részben talál.

l Az EIM API hívások számos különböző mechanizmust támogatnak a kapcsolódáshoz (másképpen kötéshez) az EIM  
l tartományvezérlőhöz. Minden egyes kötési mechanizmus más szintű hitelesítést és kapcsolat biztonságot nyújt. A  
l választási lehetőségek az alábbiak:

- l • **Egyszerű kötés** Az egyszerű kötés egy LDAP kapcsolat, ahol az LDAP kliens biztosítja az LDAP kiszolgálónak a  
l hitelesítéshez a kötési megkülönböztetett nevet és jelszót. A kötési megkülönböztetett nevet és jelszót az LDAP  
l adminisztrátor határozza meg az LDAP címtárban. Ez a hitelesítés leggyengébb és legkevesebb biztonságos formája,  
l mivel a kötési megkülönböztetett név és jelszó kódolatlanul továbbítódik, ezért könnyen lehallgatható. A  
l CRAM-MD5 (kérdés-válasz hitelesítési mechanizmus) nagyobb védelmet biztosít a kötési jelszó számára. A  
l CRAM-MD5 protokoll esetében a kliens a kódolatlan karaktersorozat helyett a jelszóból készült kivonatot küldi el a  
l szervernek hitelesítésre.
- l • **Szerver hitelesítés Védett socket rétegen (SSL) keresztül - szerveroldali hitelesítés** Az LDAP szervert be lehet  
l állítani az SSL vagy Szállítási réteg biztonság (TLS) kapcsolatok fogadására. Ebben az esetben az LDAP szerver  
l digitális igazolás segítségével hitelesíti magát a kliens felé, majd egy kódolt kommunikációs csatornát nyit meg.  
l Csak az LDAP kiszolgáló hitelesítése történik igazolással. A végfelhasználó kötési megkülönböztetett nevet és  
l jelszót használ a hitelesítéshez. A hitelesítés ereje megegyezik az egyszerű kötésével, azonban minden adat  
l (beleértve a kötési megkülönböztetett nevet és jelszót is) kódolva van a biztonság érdekében.
- l • **Kliens hitelesítés SSL segítségével** Az LDAP kiszolgálót be lehet állítani úgy, hogy megkövetelje a  
l végfelhasználótól, hogy az SSL vagy TSL biztonságos szerverkapcsolatokon keresztül kötési megkülönböztetett név  
l és jelszó helyett digitális igazolással végezze a hitelesítést. A kliens és a szerver egyaránt elvégzi a hitelesítést, és a  
l munkamenet titkosított. Ez a lehetőség egy erősebb szintű felhasználói hitelesítést biztosít, és megóvja a továbbított  
l adatok titkosságát.
- l • **Kerberos hitelesítés** Az LDAP kliens hitelesítése a szerver felé kötési megkülönböztetett név és jelszó helyett  
l történhet Kerberos jegy felhasználásával is. A Kerberos egy harmadik féltől származó megbízható hálózati  
l hitelesítési rendszer, melynek segítségével egy entitás (felhasználó vagy szolgáltatás) igazolhatja a kiletét egy másik  
l szolgáltatás számára egy nem biztonságos hálózaton. Az entitások hitelesítése egy kulcselosztó központnak (KDC)  
l nevezett kiszolgálón keresztül történik. A KDC a felhasználókat Kerberos jegyek segítségével hitelesíti. Ezek a  
l jegyek bizonyítják az entitás azonosságát a hálózaton található többi szolgáltatás felé. Miután az entitás hitelesítése a  
l jegyek segítségével megtörtént, az entitás és a szolgáltatás megkezdheti a titkosított adatforgalmazást a cél  
l szolgáltatással. Ez a lehetőség egy erősebb szintű felhasználói hitelesítést biztosít, és titkosítja a hitelesítési  
l információkat.

l Az alkalmazandó kötési mechanizmus függ az EIM támogatással rendelkező alkalmazások számára szükséges  
l biztonsági szinttől, és az EIM tartományt kiszolgáló LDAP szerver által támogatott hitelesítési mechanizmusoktól.

l Ezen kívül szükség lehet a kiválasztott hitelesítés mechanizmus beállítására az LDAP kiszolgálón. Tanulmányozza a  
l tartományvezérlőt kiszolgáló LDAP szerver dokumentációját a szükséges további konfigurációs lépésekkel  
l kapcsolatban.

### l **Példa tervezési munkalap: tartományvezérlő információk**



Miután az EIM tartományvezérlőre vonatkozó alapvető kérdéseket eldöntötte, a tervezési munkalap segítségével rögzítse az operációs rendszer és az alkalmazások számára szükséges információkat. A folyamat során összegyűjtött információkat az LDAP adminisztrátor felhasználhatja annak az azonosságnak a meghatározásához, amelyet az alkalmazás vagy az operációs rendszer használ a csatlakozáshoz az EIM tartományvezérlőt kiszolgáló LDAP szerverhez.

Az alábbi tervezési munkalap példa részletek az összegyűjtendő információk típusait szemléltetik. Az EIM tartományvezérlő beállításához felhasználható példaértékeket is tartalmaznak.

12. táblázat: Tartomány és tartományvezérlő munkalap az EIM tervezési munkalaphoz

Az EIM tartomány és tartományvezérlő beállításához szükséges információk	Példa válaszok
A tartomány beszédes neve. Ez lehet a tartományt használó cég, részleg vagy alkalmazás neve.	SajatTartomany
választható: ha már létező LDAP címtárban állítja be az EIM tartományt, akkor adjon meg egy szülő megkülönböztetett nevet a tartományhoz. Ez a megkülönböztetett név képviseli a címtár információk fa hierarchiájában közvetlenül a tartománynév bejegyzés fölött elhelyezkedő bejegyzést. Például: o=ibm,c=us.	o=ibm,c=us
Az eredményül kapott teljes képzésű EIM tartomány megkülönböztetett név. Ez az EIM tartomány teljesen megadott neve, amely meghatározza az EIM tartományadatok címtárbeli helyét. A teljes képzésű tartomány megkülönböztetett név minimálisan tartalmazza a tartomány DN-t (ibm-eimDomainName=), plusz a megadott tartománynevet. Ha úgy dönt, hogy szülő megkülönböztetett nevet ad meg a tartományhoz, akkor a teljes képzésű tartomány DN tartalmazza a relatív tartomány DN-t (ibm-eimDomainName=), a tartománynevet (SajatTartomany), és a szülő DN-t (o=ibm,c=us). <b>Megjegyzés:</b>	Az alábbiak egyike attól függően, hogy választott-e szülő megkülönböztetett nevet: <ul style="list-style-type: none"> <li>ibm-eimDomainName=SajatTartomany</li> <li>ibm-eimDomainName=SajatTartomany,o=ibm,c=us</li> </ul>
A tartományvezérlő kapcsolati címe. Ez tartalmazza a kapcsolat típusát (például alap ldap vagy biztonságos ldap esetén ldap:// vagy ldaps://) plusz az alábbi információkat:	ldap://
<ul style="list-style-type: none"> <li>Választható: a hosztnév vagy IP cím</li> <li>Választható: a portszám</li> </ul>	<ul style="list-style-type: none"> <li>egy.ldap.gazdagep</li> <li>389</li> </ul>
A tartományvezérlő eredményül kapott teljes kapcsolati címe.	ldap://egy.ldap.gazdagep:389
Az alkalmazásoknak vagy rendszereknek kötési mechanizmusra van szükségük. A választási lehetőségek:	Kerberos
<ul style="list-style-type: none"> <li>Egyszerű kötés</li> <li>CRAM MD5</li> <li>Szerver hitelesítés</li> <li>Kliens hitelesítés</li> <li>Kerberos</li> </ul>	

Ha az EIM konfigurációját és adminisztrációját végző csapat több főből áll, akkor a kötési azonosságot és mechanizmust úgy kell megválasztani, hogy a csapat összes tagja a szerepének megfelelően hozzáférhessen az EIM tartományhoz. Ki kell választani a kötési azonosságot és mechanizmust az EIM alkalmazás végfelhasználók számára is. Az ehhez szükséges információk összegyűjtéséhez hasznos példával szolgál az alábbi munkalap.

13. táblázat: Kötési azonosság tervező példa munkalap

EIM jogosultság vagy szerep	Kötési azonosság	Kötési mechanizmus	Mihez szükséges
EIM adminisztrátor	eimadmin@krbtartomany1.com	Kerberos	EIM beállítás és kezelés

### 13. táblázat: Kötési azonosság tervező példa munkalap (Folytatás)

EIM jogosultság vagy szerep	Kötési azonosság	Kötési mechanizmus	Mihez szükséges
LDAP adminisztrátor	cn=admin	egyszerű kötés	EIM tartományvezérlő beállítása
Adott EIM nyilvántartás adminisztrátora	cn=admin2	CRAM MD5	adott nyilvántartás meghatározás kezelése
EIM leképezés kikeresés	cn=SajatAlkalmazas,c=HU	egyszerű kötés	alkalmazás leképezés kikeresési műveletek végrehajtása

Miután összegyűjtötte a tartományvezérlő beállításához szükséges információkat, elkezdheti az azonosság leképezési terv elkészítését.

### Vállalati azonosság leképezés (EIM) nyilvántartás meghatározás elnevezési megállapodás elkészítése

Amennyiben egy adott felhasználói nyilvántartásban szereplő felhasználó azonosságot meg kíván feleltetni az EIM segítségével egy másik felhasználói nyilvántartás felhasználói azonosságának, akkor mindkét nyilvántartás meghatározását létre kell hozni az EIM számára. Az EIM tartományban szereplő összes alkalmazás és operációs rendszer számára létre kell hozni egy nyilvántartás meghatározást. A felhasználói nyilvántartások képviselhetnek operációs rendszer nyilvántartásokat, mint például a Resource Access Control Facility (RACF) vagy az OS/400, osztott nyilvántartásokat, mint például a Kerberos, vagy rendszer nyilvántartások kizárólag egyetlen alkalmazás által használt részhalmozait.

Az EIM tartomány tetszőleges platformon létező nyilvántartásokról tartalmazhat nyilvántartás meghatározásokat. Például egy OS/400 rendszeren futó tartományvezérlő által kezelt tartomány tartalmazhat olyan nyilvántartás meghatározásokat, amelyek nem OS/400 környezetből (például AIX operációs rendszerből) származó nyilvántartásokat képviselnek. Az EIM tartományban bármely felhasználói nyilvántartást meghatározhat, de az EIM támogatással rendelkező alkalmazások és operációs rendszerek definíciója kötelező.

Az EIM nyilvántartás meghatározások neveivel kapcsolatban egyetlen megkötés létezik: minden névnek egyedinek kell lennie az adott EIM tartományra nézve. Például el lehet nevezni az EIM nyilvántartás meghatározásokat az adott felhasználói nyilvántartást tartalmazó rendszer alapján. Ha ez nem elegendő a nyilvántartás meghatározás megkülönböztetésére, akkor a pont (.) vagy aláhúzás ( \_ ) karakterekkel hozzáfűzheti a nyilvántartás típusát a névhez. Tekintet nélkül a használni kívánt feltételekre célszerű egy elnevezési megállapodást készíteni az EIM nyilvántartás meghatározásokhoz. Így biztosítható, hogy a definíciók nevei konzisztensek maradnak a tartományban, és elegendő információt biztosítanak a definíció típusát, példányát és a használatának módját illetően. Dönthet úgy például, hogy minden nyilvántartás meghatározás nevének a nyilvántartást használó operációs rendszer vagy alkalmazás nevének és a nyilvántartás vállalaton belüli fizikai helyének kombinációjából kell állnia.

Egy EIM használatára felkészített alkalmazás egy forrás vagy egy cél nyilvántartás álnevet használ, esetleg mindkettőt. EIM nyilvántartás meghatározások létrehozásakor ellenőrizze az alkalmazások dokumentációit, hogy létre kell-e hoznia álneveket a nyilvántartás meghatározásokhoz. Ha hozzárendeli ezeket az álneveket a megfelelő nyilvántartás meghatározásokhoz, akkor az alkalmazás végrehajthat egy álnév keresést, és az álnevek alapján képes megtalálni a szükséges EIM nyilvántartás meghatározásokat.

Az alábbi minta tervezési munkalap részlet hasznosnak bizonyulhat a tartományban részvevő felhasználói nyilvántartásokra vonatkozó információk nyilvántartása során. A tényleges munkalapon rögzítheti a felhasználói nyilvántartásokhoz tartozó nyilvántartás meghatározás nevet, az esetleges álneveket, illetve a nyilvántartás helyét és használatának módját. Az alkalmazások telepítési és konfigurációs dokumentációja tartalmazza a munkalap kitöltéséhez szükséges információk egy részét.

14. táblázat: Minta EIM nyilvántartás meghatározás információs tervezési munkalap

Nyilvántartás meghatározás név	Felhasználói nyilvántartás típusa	nyilvántartás meghatározás álnév	Nyilvántartás leírása
Rendszer_C	OS/400 rendszer felhasználói nyilvántartás	Lásd az alkalmazás dokumentációját	A C rendszer fő OS/400 rendszer felhasználói nyilvántartása
Rendszer_A_WAS	WebSphere LTPA	alkalmazas_23_alnev_forras	WebSphere LTPA felhasználói nyilvántartás az A rendszeren
Rendszer_B	Linux	Lásd az alkalmazás dokumentációját	Linux felhasználói nyilvántartás a B rendszeren
Rendszer_A	OS/400 rendszer felhasználói nyilvántartás	alkalmazas_23_alnev_cel alkalmazas_xx_alnev_cel	Az A rendszer fő OS/400 rendszer felhasználói nyilvántartása
Rendszer_D	Kerberos felhasználói nyilvántartás	alkalmazas_xx_alnev_forras	ervenyes.tartomany.com Kerberos tartomány
Rendszer_4	Windows 2000 felhasználói nyilvántartás	Lásd az alkalmazás dokumentációját	Emberierőforrás-kezelő alkalmazás felhasználói nyilvántartása a 4 rendszeren

**Megjegyzés:** A nyilvántartások társítás típusa a tervezési folyamat későbbi szakaszában kerül meghatározásra.

A tervezési munkalap ezen részének kitöltése után készítse el az azonosság leképezési tervet annak eldöntéséhez, hogy azonosság társítások, irányelv társítások vagy mindkét típus felhasználásával hozza létre a meghatározott felhasználói nyilvántartásokban található felhasználói azonosságokhoz szükséges leképezéseket.

## Azonosságleképezés megtervezése

Az EIM megvalósítás tervezésének korai szakaszában kritikus pont annak eldöntése, hogy milyen módon kívánja használni az azonosság leképezést a vállalatban. Az EIM használatával két módon lehet leképezni az azonosságokat:

- **Azonosító társítások** - az EIM azonosítók és a felhasználói nyilvántartásokban található, egyes személyeket képviselő felhasználói azonosságok közötti kapcsolatokat írják le. Egy azonosító társítás egy közvetlen, 1-1 relációt hoz létre egy EIM azonosító és egy adott felhasználói azonosság között. Az azonosító társítások indirekt segítségével indirekt viszony hozható létre felhasználó azonosságok között egy EIM azonosítón keresztül.

Amennyiben a biztonsági házirend nagy részletességű felelősségre vonhatóságot követel meg, akkor a leképezést szinte kizárólag azonosító társítások segítségével kell megvalósítani. Ugyanis mivel a felhasznált azonosság társítások a felhasználók birtokában lévő azonosságok között 1-1 relációkat hoznak létre, mindig megállapítható, hogy pontosan ki hajtott végre egy adott műveletet egy objektumon vagy rendszeren.

- **Irányelv társítások** - több felhasználói azonosság és egy adott felhasználói nyilvántartásban található egyetlen felhasználói azonosság közötti viszonyt írják le. Az irányelv társítások az EIM leképezés irányelv támogatását felhasználva N-1 relációkat hoznak létre felhasználói azonosságok között EIM azonosító közbeiktatása nélkül.

Az irányelv társítások olyan esetben bizonyulhatnak hasznosnak, ha egy rendszerhez vagy alkalmazáshoz felhasználók nagy csoportjainak kíván hozzáférést biztosítani, azonban ehhez nem kíván külön felhasználói azonosságokat kiosztani. Ha például egy belső alkalmazást felhasználó webalkalmazás karbantartásáról van szó, akkor szükségtelen lehet felhasználói azonosságok százainak vagy ezreinek létrehozása a hitelesítéshez a belső alkalmazás felé. Ehelyett elég beállítani úgy az azonosság leképezést, hogy a webes alkalmazás összes felhasználója leképeződjön egy az alkalmazás futtatásához minimálisan szükséges jogosultsággal rendelkező felhasználó azonosságra. Az ilyen típusú azonosság leképezést az irányelv társítások segítségével végezheti el.

Dönthet úgy, hogy az azonosító társításokat használja, és a legmodernebb jelszókezelési technológiák előnyei mellett a lehető legnagyobb mértékben kézben tartja a felhasználói azonosságokat a vállalatban belül. Vagy választhatja azt az utat is, hogy az irányelv társítások és azonosító társítások keverékét használja; ebben az esetben kihasználhatja az egyszerű bejelentkezés előnyeit, ahol erre lehetőség van, miközben az adminisztrátorok megtartják az ellenőrzést

| bizonyos felhasználói azonosságok fölött. Függetlenül attól, hogy az üzleti igényeinek és a biztonsági stratégiájának melyik leképezési típus felel meg leginkább, el kell készítenie az azonosság leképezési tervet.

| Az azonosság leképezési terv elkészítéséhez az alábbiakat kell tennie:

- | • “EIM azonosítók elnevezési megállapodásának kialakítása” oldalszám: 56
- | • “Vállalati azonosság leképezés (EIM) társítások megtervezése”

| **Vállalati azonosság leképezés (EIM) társítások megtervezése:** A Társítások az EIM tartományban létrehozott bejegyzések, amelyek különböző felhasználói nyilvántartásban található felhasználói azonosságok között létesítenek hozzárendelést. Az EIM megvalósítása során kétféle társítást hozhat létre: az azonosító társítások 1-1 leképezéseket, míg az irányelv társítások N-1 leképezéseket határoznak meg. Az irányelv társítások használhatók az azonosító társítások helyett, vagy azokkal párhuzamosan, az azonosító társításokat kiegészítve.

| Az alkalmazott társítások pontos típusa függ attól, hogy a felhasználó pontosan hogyan használja az adott felhasználói azonosságot, és természetesen az átfogó azonosság leképezési tervtől is.

| Az alábbi típusú azonosító társításokat hozhatja létre:

- | • **Cél társítások**

| Az adott rendszert egy másik kliens rendszerről általában csak szerverként elérő felhasználókhöz adjon meg cél társítást. Az alkalmazás által végrehajtott leképezés kikeresési műveletek használják ezt a társítás típust.

- | • **Forrás társítások**

| A felhasználó által a rendszerbe vagy hálózatra bejelentkezéshez először megadott felhasználói azonossághoz forrás társításokat határozzon meg. Az alkalmazás által végrehajtott leképezés kikeresési műveletek használják ezt a társítás típust.

- | • **Adminisztrációs társítások**

| Ha nyomon szeretné követni azt a tényt, hogy egy felhasználó azonosság egy adott felhasználóhoz tartozik, de el szeretné kerülni, hogy a felhasználó azonosság leképezés kikeresési műveleteket hajthasson végre, akkor adminisztrációs társítást határozzon meg. Ezt a társítás típust használhatja egy személy összes felhasználói azonosságának nyomon követésére a vállalaton belül.

| Az **irányelv társítások** mindig meghatároznak egy cél társítást.

| Elképzelhető, hogy egy nyilvántartás meghatározás több különböző típusú társítással rendelkezik a hozzá tartozó felhasználói nyilvántartás használatának módjától függően. Noha nincs felső korlát a társítások és a típusok számát illetően, az EIM tartomány adminisztrációjának egyszerűsítése érdekében célszerű a számot a minimumon tartani.

| Az alkalmazások általában csak a forrás és cél nyilvántartásokhoz elvárt nyilvántartás meghatározásokkal kapcsolatban adnak útmutatást, a társítás típusokhoz nem. Az alkalmazás minden végfelhasználóját legalább társításnak le kell képeznie. Ez a társítás lehet az egyedi EIM azonosító és a kívánt cél nyilvántartásbeli felhasználó azonosság közötti 1-1 leképezés, vagy a felhasználó azonosságot tartalmazó forrás nyilvántartás és a cél nyilvántartás közötti N-1 leképezés. A használt társítás típusa függ az azonosság leképezéssel kapcsolatos egyedi igényektől és az alkalmazás által támasztott követelményektől.

| A tervezési folyamat során korábban a szervezeten belüli felhasználói azonosságokhoz elkészült két, az EIM azonosítókra és az EIM nyilvántartás meghatározásokra vonatkozó információkat tartalmazó munkalap. Most a vállalat felhasználói azonosságainak leképezéséhez használni kívánt társítás típusok megadásával össze kell kapcsolni ezeket az információkat. El kell dönteni, hogy irányelv társításra van szükség egy adott alkalmazás és a hozzá tartozó felhasználói nyilvántartás számára, vagy a rendszer illetve alkalmazás nyilvántartásában található összes felhasználóhoz egyedi (forrás, cél vagy adminisztrációs) azonosító társítást kell megadni. Ehhez rögzítse a szükséges társítás típusokra vonatkozó információkat a nyilvántartás meghatározás tervezési munkalapon és a társítások munkalapjainak megfelelő soraiban.

| Az azonosság leképezés megvalósítási tervének véglegesítéséhez szükség van a társításokkal kapcsolatos információk rögzítésére. Ehhez használhatja az alábbi példa munkalapokat.

15. táblázat: Példa EIM nyilvántartás meghatározás információs tervezési munkalap

Nyilvántartás meghatározás név	Felhasználói nyilvántartás típusa	nyilvántartás meghatározás álnév	Nyilvántartás leírása	Társítás típusok
Rendszer_C	OS/400 rendszer felhasználói nyilvántartás	Lásd az alkalmazás dokumentációját	A C rendszer fő OS/400 rendszer felhasználói nyilvántartása	Cél
Rendszer_A_WAS	WebSphere LTPA	alkalmazas_23_alnev_forras	WebSphere LTPA felhasználói nyilvántartás az A rendszeren	Elsősorban forrás
Rendszer_B	Linux	Lásd az alkalmazás dokumentációját	Linux felhasználói nyilvántartás a B rendszeren	Forrás és cél
Rendszer_A	OS/400 rendszer felhasználói nyilvántartás	alkalmazas_23_alnev_cel alkalmazas_xx_alnev_cel	Az A rendszer fő OS/400 rendszer felhasználói nyilvántartása	Cél
Rendszer_D	Kerberos felhasználói nyilvántartás	alkalmazas_xx_alnev_forras	ervenyes.tartomany.com Kerberos tartomány	Forrás
Rendszer_4	Windows 2000 felhasználói nyilvántartás	Lásd az alkalmazás dokumentációját	Emberierőforrás-kezelő alkalmazás felhasználói nyilvántartása a 4 rendszeren	Adminisztrációs
beszerzes.tartomany.com	Windows 2000 felhasználói nyilvántartás		A beszerzési részlegben dolgozó alkalmazottak elsődleges bejelentkezési nyilvántartása	Alapértelmezett nyilvántartás irányelv (forrás nyilvántartás)
Rendszer_A_beszerzes_alk	A beszerzési részleg által használt alkalmazás		Beszerzések frissítésére szolgáló alkalmazásra jellemző nyilvántartás	Alapértelmezett nyilvántartás irányelv (cél nyilvántartás)
rendszer_C_beszerzes_alk	A beszerzési részleg által használt alkalmazás		Beszerzések frissítésére szolgáló alkalmazásra jellemző nyilvántartás	Alapértelmezett nyilvántartás irányelv (cél nyilvántartás)

16. táblázat: Példa EIM azonosító tervezési munkalap

Egyedi azonosító név	Az azonosító vagy azonosság leírása	Azonosító álnév
Nap S János	Emberi erőforrás kezelő	alk_23_admin
Nap J János	Jogi részleg	alk_xx_admin
József A. Sára	Beszerzési részleg adminisztrátor	

17. táblázat: Példa azonosító társítás tervezési munkalap

Identifier unique name: _____Nap S János_____		
Felhasználói nyilvántartás	Felhasználó azonosság	Társítás típusok
Rendszer A WAS a Rendszer A rendszeren	JANOSN	Forrás
Linux a Rendszer B rendszeren	jsn1	Forrás és cél
OS/400 a Rendszer C rendszeren	JANOSN	Cél
Nyilvántartás 4 a Windows 2000 emberi erőforrás rendszeren	JNAP	Adminisztrációs

18. táblázat: Példa tervezési munkalap irányelv társításokhoz

Irányelv társítás típus	Forrás felhasználói nyilvántartás	Cél felhasználói nyilvántartás	Felhasználó azonosság	Leírás
Alapértelmezett nyilvántartás	beszerzes.tartomany.com	Rendszer_A_beszerzes_alk	RENDSZERFELHA	A beszerzési részleghez tartozó hitelesített Windows felhasználót képezi le az megfelelő alkalmazás felhasználói azonosságra
Alapértelmezett nyilvántartás	beszerzes.tartomany.com	rendszer_C_beszerzes_alk	RENDSZERFELHB	A beszerzési részleghez tartozó hitelesített Windows felhasználót képezi le az megfelelő alkalmazás felhasználói azonosságra

**EIM azonosítók elnevezési megállapodásának kialakítása:** Az EIM azonosság leképezéshez kapcsolódó igények megtervezése során ha 1-1 leképezéseket szeretne létrehozni egy felhasználó birtokában lévő felhasználói azonosságok között, akkor egyedi EIM azonosítókat hozhat létre az EIM támogatással rendelkező alkalmazások és operációs rendszerek felhasználói számára. Az azonosító társítások segítségével létrehozott 1-1 leképezések használatával maximálisan kihasználhatja az EIM jelszókezelés terén nyújtott előnyeit.

Az elkészített elnevezési megállapodás az üzleti igényeit és egyedi preferenciáit tükrözi, az EIM azonosítókkal szemben támasztott egyetlen elvárás az, hogy egyediek legyenek. Bizonyos társaságok előnyben részesítik az egyes személyek teljes, valódi nevének használatát, mások egyéb típusú adatokat használnak, például minden alkalmazottnak kiosztanak egy számot. Ha az EIM azonosítókat a személyek teljes neve alapján hozza létre, akkor előre meg kell tervezni az esetleges névegyezések kikerülésének módját. A többszörös azonosító nevek kezelése teljes mértékben az adminisztrátor egyedi belátására van bízva. Elképzelhető, hogy minden esetet egyedileg kezelve egy előre meghatározott karaktersorozat hozzáfűzésével teszi egyedivé az azonosító nevet, például minden azonosítóhoz hozzáadja annak a részlegnek a számát, ahol az adott személy dolgozik.

Az EIM azonosítók elnevezési megállapodásának megtervezése során meg kell határozni az átfogó azonosság leképezési tervet. Ez a terv segítségével lehet annak eldöntésében, hogy mikor kell azonosítókat és azonosító társításokat használni, és mely esetekben célravezetőbbek az irányelv társítások a vállalat azonosságainak leképezése során. Az EIM azonosítók elnevezési megállapodásának kialakításához használhatja az alábbi munkalapot a szervezetben található azonosságra vonatkozó információk összegyűjtéséhez, és az EIM azonosítók létrehozásához a felhasználói azonosságok számára. A munkalap tartalmazza mindazokat az információkat, amelyekre az EIM adminisztrátornak szüksége van az EIM azonosítók és irányelv társítások létrehozása során.

19. táblázat: Példa EIM azonosító tervezési munkalap

Egyedi azonosító név	Az azonosító vagy azonosság leírása	Azonosító álnév
Nap S János	Emberi erőforrás kezelő	app_23_admin
Nap J János	Jogi részleg	alk_xx_admin
József A. Sára	Beszerzési részleg adminisztrátor	

Egy EIM használatára felkészített alkalmazás megadhat egy álnevet, amelynek segítségével kikeresi a megfelelő EIM azonosítót, azt pedig egy adott felhasználói azonosság meghatározására használja fel. Ellenőrizze az alkalmazások dokumentációit, hogy létre kell-e hoznia álneveket az azonosítóhoz. Az EIM azonosítókhöz és a felhasználói azonosságokhoz tartozó leírás mezők szabványos formátumúak, és az adott felhasználót leíró információk megadására szolgál.

Nem kell azonnal a vállalat összes felhasználója számára EIM azonosítót létrehozni. Miután létrehozott egy kezdeti azonosítót, és ezzel elvégezte az EIM konfiguráció tesztelését, elkezdheti a további EIM azonosítók létrehozását a szervezet EIM használatával kapcsolatos céljai alapján. Az EIM azonosítók felvételét végezheti területi alapon vagy részlegek szerint. Vagy folytathatja az EIM azonosítók létrehozását az új EIM alkalmazások bevezetésével párhuzamosan.

Miután összegyűjtötte az EIM azonosítók elnevezési megállapodásának kialakításához szükséges információkat, elkezdheti a társítások megtervezését a felhasználói azonosságok számára.

### Vállalati azonosság leképezés (EIM) megvalósítás tervezési munkalap

Az Vállalati azonosság leképezés (EIM) megtervezésének folyamata során igen hasznosnak fognak bizonyulni ezek a munkalapok az EIM konfigurációjához szükséges információk összegyűjtéséhez. A megfelelő helyeken illusztrációként kitöltött munkalaprészeket talál.

Ezek a munkalapok az EIM megvalósítási terv elkészítéséhez szükséges munkalaptípusok szemléltetésére szolgálnak. A bejegyzések száma például a tényleges összegyűjtött EIM információknál jóval kevesebb lesz. Indokolt esetben nyugodtan változtassa meg a munkalapokat, hogy jobban igazodjanak a tényleges körülményekhez.

#### 20. táblázat: Tartomány és tartományvezérlő információs munkalap

Az EIM tartomány és tartományvezérlő beállításához szükséges információk	Válaszok
A tartomány beszédes neve. Ez lehet a tartományt használó cég, részleg vagy alkalmazás neve.	
Választható: A tartomány szülő megkülönböztetett neve. Ez a megkülönböztetett név képviseli a címtár információk fa hierarchiájában közvetlenül a tartománynev bejegyzés fölött elhelyezkedő bejegyzést. Például: o=ibm,c=us.	
Az eredményül kapott teljes képzésű EIM tartomány megkülönböztetett név. Ez az EIM tartomány teljesen megadott neve, amely meghatározza az EIM tartományadatok címtárbeli helyét. A teljes képzésű tartomány megkülönböztetett név minimálisan tartalmazza a tartomány DN-t (ibm-eimDomainName=), plusz a megadott tartománynevet. Ha úgy dönt, hogy szülő megkülönböztetett nevet ad meg a tartományhoz, akkor a teljes képzésű tartomány DN tartalmazza a relatív tartomány DN-t (ibm-eimDomainName=), a tartománynevet (SajatTartomány), és a szülő DN-t (o=ibm,c=us).	
A tartományvezérlő kapcsolati címe. Ez tartalmazza a kapcsolat típusát (például alap ldap vagy biztonságos ldap esetén ldap:// vagy ldaps://) plusz az alábbi információkat:	
<ul style="list-style-type: none"> <li>Választható: a hosztnév vagy IP cím</li> <li>Választható: a portszám</li> </ul>	
A tartományvezérlő eredményül kapott teljes kapcsolati címe.	
Az alkalmazásoknak vagy rendszereknek kötési mechanizmusra van szükségük. A választási lehetőségek:	
<ul style="list-style-type: none"> <li>Egyszerű kötés</li> <li>CRAM MD5</li> <li>Szerver hitelesítés</li> <li>Kliens hitelesítés</li> <li>Kerberos</li> </ul>	

A munkalap használatára az EIM tartományvezérlő megtervezése részben talál egy példát.

21. táblázat: Azonosság kötés tervezési munkalap

EIM jogosultság vagy szerep	Kötési azonosság	Kötési mechanizmus	Mihez szükséges

A munkalap használatára az EIM tartományvezérlő megtervezése részben talál egy példát.

22. táblázat: EIM nyilvántartás meghatározás információs tervezési munkalap

Nyilvántartás meghatározás név	Felhasználói nyilvántartás típusa	nyilvántartás meghatározás álnév	Nyilvántartás leírása	Társítás típusok

A munkalap használatára az EIM nyilvántartás meghatározások elnevezési megállapodásának megtervezése részben talál egy példát.

23. táblázat: EIM azonosító tervezési munkalap

Egyedi azonosító név	Az azonosító vagy azonosság leírása	Azonosító álnév



23. táblázat: EIM azonosító tervezési munkalap (Folytatás)

Egyedi azonosító név	Az azonosító vagy azonosság leírása	Azonosító álnév

A munkalap használatára az EIM azonosítók elnevezési megállapodásának megtervezése részben talál egy példát.

24. táblázat: Azonosító társítás tervezési munkalap

Azonosító egyedi név: _____ Nap S János _____		
Felhasználói nyilvántartás	Felhasználó azonosság	Társítás típusok

A munkalap használatára az EIM társítások megtervezése részben talál egy példát.

25. táblázat: Irányelv társítás tervezési munkalap

Irányelv társítás típus	Forrás felhasználói nyilvántartás	Cél felhasználói nyilvántartás	Felhasználó azonosság	Leírás

A munkalap használatára az EIM társítások megtervezése részben talál egy példát.

## Vállalati azonosság leképezést (EIM) támogató alkalmazások fejlesztésének megtervezése

Ahhoz, hogy egy alkalmazás képes legyen a Vállalati azonosság leképezés (EIM) kezelésére és részt tudjon venni egy tartományban, képesnek kell lennie az EIM API hívások használatára. Olvassa el az EIM API dokumentációt és az adott környezetre vonatkozó EIM dokumentációt annak eldöntésére, hogy figyelembe kell-e venni különleges tervezési szempontokat az EIM API hívásokat felhasználó alkalmazások írása vagy átültetése során. A C vagy C++ nyelven íródott EIM API hívásokat használó alkalmazások esetében például lehetnek bizonyos fordítással kapcsolatos és egyéb megfontolások. Az alkalmazás platformjától függően szerkesztési és egyéb szempontok is szóba jöhetnek.

## Vállalati azonosság leképezés (EIM) megtervezése OS/400 rendszeren

A Vállalati azonosság leképezés (EIM) számos technológiát és szolgáltatást magában foglal az iSeries szerveren. Mielőtt beállítaná 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 iSeries konfigurációjának az alábbi oldalakon ismerkedhet meg:
- | • “EIM telepítési előfeltételek iSeries rendszeren”
- | • “Szükséges iSeries navigátor összetevők telepítése”
- | • “Vállalati azonosság leképezés (EIM) biztonsági mentéssel és helyreállítással kapcsolatos szempontok” oldalszám: 61

| Ha a felhasználók hitelesítését Kerberos alapon tervezi megoldani, akkor be kell állítania a Hálózati hitelesítési szolgáltatást is. A Hálózati hitelesítési szolgáltatás tervezésével kapcsolatban lásd a Hálózati hitelesítési szolgáltatás tervezése részt, az egyszeri bejelentkezési környezet tervezésével kapcsolatban pedig az Egyszeri bejelentkezési környezet tervezése részt.

## | EIM telepítési előfeltételek iSeries rendszeren

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

| 26. táblázat: EIM telepítési tervezési munkalap

EIM előfeltételek tervezési munkalap	Válaszok
Az OS/400 (5722-SS1) kiadása V5R2 vagy újabb?	
Az alábbi termékopciók és licenc hatálya alá eső termékek telepítve vannak az iSeries™ rendszeren? <ul style="list-style-type: none"> <li>• OS/400 Host Szerverek (5722-SS1 Opció 12)</li> <li>• iSeries Access for Windows® (5722-XE1)</li> <li>• Cryptographic Access Provider (5722-AC3)</li> <li>• Qshell Interpreter (5722-SS1 Opció 30) Akkor szükséges, ha az EIM konfigurálása mellett a Hálózati hitelesítési szolgáltatás beállítását is el szeretné végezni.</li> </ul>	
Az iSeries navigátor telepítve van az adminisztrátor számítógépén az alábbi részösszetevőkkel együtt? <ul style="list-style-type: none"> <li>• Biztonság Akkor szükséges, ha az EIM konfigurálása mellett a Hálózati hitelesítési szolgáltatás beállítását is el szeretné végezni.</li> <li>• Hálózat</li> </ul>	
Telepítve van a legújabb iSeries Access for Windows javítócsomag? A legújabb javítócsomagot az iSeries Access  webhelyen találja.	
Ha van beállított címtár szerver, például egy IBM Directory Server for iSeries (LDAP), amelyet EIM tartományvezérlőként szeretne felhasználni, akkor ismeri az LDAP adminisztrátor megkülönböztetett nevét és jelszavát?	
Ha van beállított címtár 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)?	

## | 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 felügyeletére használt számítógépen telepítve van-e az iSeries Access for Windows.

| A **Hálózat** összetevő telepítése:

1. Kattintson **Start > Programok > IBM iSeries Access for Windows > Szelektív telepítés** 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.

## Vállalati azonosság leképezés (EIM) biztonsági mentéssel és helyreállítással kapcsolatos szempontok

Nagyon fontos elkészíteni a Vállalati azonosság leképezés (EIM) adatainak mentési és helyreállítási tervét, hogy az EIM adatokat az EIM tartományvezérlőnek otthont adó címtár szerver esetleges meghibásodása esetén vissza lehessen állítani. Nagyon fontos megérteni az EIM konfigurációs információk helyreállításának módját is.

### EIM tartományadatok biztonsági mentése és helyreállítása

Az EIM adatok elmentésének módja attól függ, hogy milyen mentési stratégiát választ az EIM adatok számára tartományvezérlőként működő címtár szerveren.

A biztonsági mentés egyik módja az, amikor elsősorban az összeomlások utáni helyreállításhoz készül mentés az adatbázis könyvtárba. Alapértelmezésben ez a QUSRDIRDB. Ha a módosítási napló engedélyezve van, akkor akkor a QUSRDIRCL könyvtárat is menteni kell. A visszaállításra kijelölt címtár szervernek az eredeti szerverrel megegyező LDAP sémával és konfigurációval kell rendelkeznie. Ezeket az információkat a /QIBM/UserData/OS400/DirSrv fájlok tárolják. További konfigurációs adatok tárolódnak a QUSRSYS/QGLDCFG (\*USRSPC objektum) és a QUSRSYS/QGLDVLDD (\*VLDL objektum) könyvtárakban. Ha a szerver teljes állapotát le kívánja menteni, akkor mentse el mindkét könyvtárat, az integrált fájlrendszereket és a QUSRSYS objektumokat.

Az alapvető fontosságú címtár szerver adatok mentéséről és visszatöltéséről hasznos lehet áttanulmányozni a Címtár szerver információk mentése és visszatöltése részt az IBM Directory Server for iSeries (LDAP) témakörben az Információs központban.

Használhat például egy LDIF fájlt a címtár szerver tartalmának elmentéséhez. Egy IBM Directory Server for iSeries tartományvezérlő tartományadatainak biztonsági mentéséhez tegye a következőket:

- Az iSeries navigátorban bontsa ki a **Hálózat > Szerverek > TCP/IP** csomópontot.
- Kattintson a jobb egérgombbal az **IBM Directory Server** lehetőségre, majd válassza az előugró menü **Eszközök**, majd **Fájl exportálása** menüpontját. A megjelenő párbeszédablakon állítsa be, hogy a címtár szerver mely részeit kívánja fájlba exportálni.
- Vigye át az exportált fájlt a tartalék címtár kiszolgálóként használni kívánt iSeries szerverre.
- Az iSeries navigátorban bontsa ki a **Hálózat > Szerverek > TCP/IP** csomópontot.
- Kattintson a jobb egérgombbal az **IBM Directory Server** lehetőségre, majd válassza az előugró menü **Eszközök -> Importálás** menüpontját. Ezzel betölti a fájl tartalmát az új címtár szerverre.

A biztonsági mentés másik megfontolásra érdemes módja egy másolat címtár szerver beállítása. A másolat szerver az EIM adatok összes változását automatikusan megkapja, így ha a tartományvezérlőnek otthont adó címtár szerver kiesik vagy adatvesztés történik, akkor az adatok tovább szolgáltatathatók a másolat szerverről.

A másolat címtárszerver beállítása és használata nagyban függ a választott többszörözési modelltől. A többszörözésről és a címtár szerver beállításáról a Többszörözés és a Többszörözés kezelése részeknél olvashat az Információs központ IBM Directory Server for iSeries (LDAP) témakörében.

### EIM konfigurációs információk biztonsági mentése és helyreállítása

Egy rendszerösszeomlás esetén szükségessé válhat a rendszer konfigurációjának visszaállítása. Ezeket az információkat azonban nem egyszerű egyik rendszerről a másikra lementeni.

Az EIM konfiguráció lementésére és visszaállítására az alábbi lehetőségek állnak rendelkezésére:

- A Biztonsági adatok mentése (SAVSECDTA) paranccsal mindegyik rendszeren mentse el az EIM konfigurációt és más fontos konfigurációs információkat. Ezután állítsa vissza a QSYS felhasználói profilt mindegyik rendszeren.

**Megjegyzés:** A QSYS felhasználói profilt az EIM konfigurációval rendelkező összes rendszeren el kell mentenie a SAVSECDTA paranccsal, majd vissza kell töltenie. Amennyiben egy másik rendszeren lementett QSYS felhasználói profilt próbál meg helyreállítani, akkor problémákba ütközhet.

- Futtassa újra az EIM konfigurációs varázslót, vagy kézzel frissítse az EIM konfiguráció mappa tulajdonságait. A folyamat megkönnyítése érdekében mentse el az EIM megvalósítás tervezési munkalapokat, vagy rögzítse minden egyes rendszer konfigurációs információit.

Amennyiben a hálózati hitelesítési szolgáltatást egyszeri bejelentkezés környezet megvalósításának részeként állította be, akkor mindezekon felül végig kell gondolnia és meg kell terveznie a hálózati hitelesítési szolgáltatás adatainak biztonsági mentését és helyreállítását.

---

## Vállalati azonosság leképezés (EIM) beállítása

Az EIM konfigurációs varázsló segítségével gyorsan és könnyen elkészíthet egy alapszintű Vállalati azonosság leképezés (EIM) konfigurációt az iSeries rendszeren. A varázsló három EIM rendszerkonfigurációs beállítási lehetőséget biztosít. A varázsló használatának módja a konkrét rendszeren függ az általános EIM megvalósítási tervtől és a rendszerrel szemben támasztott igényektől. Hasznos lehet például az EIM szolgáltatást a hálózati hitelesítési szolgáltatással együtt használva egyszeri bejelentkezés környezetet kialakítani a különböző rendszerek és platformok között, és ehhez még a biztonsági stratégián sem kell változtatni. Ezért az EIM konfigurációs varázsló lehetővé teszi a hálózati hitelesítési szolgáltatás beállítását az EIM konfiguráció részeként. Ettől függetlenül a Hálózati hitelesítési szolgáltatás nem előfeltétele vagy követelménye az EIM működésének.

Az EIM konfigurálásának megkezdése előtt tervezze meg az EIM megvalósítást és gyűjtse össze a rendelkezésre álló információkat. El kell döntenie például az alábbiakat:

- Mely iSeries szervereket kívánja tartományvezérlőként beállítani az EIM tartományban? Ezen a rendszeren először létre kell hoznia egy tartományt az EIM konfigurációs varázsló segítségével, majd ugyancsak a varázslóval csatlakoztassa az összes többi iSeries szerveret a tartományhoz.
- Az EIM tartományhoz csatlakoztatott összes rendszeren be kívánja állítani a hálózati hitelesítési szolgáltatást? Ha igen, akkor az EIM konfigurációs varázsló segítségével az összes iSeries szerveren létrehozhat egy alapszintű hálózati hitelesítési szolgáltatás konfigurációt, azonban a végleges beállításhoz további lépések végrehajtására lesz szükség.

Miután az EIM konfigurációs varázsló segítségével elvégezte az alapszintű beállításokat az összes iSeries szerveren, további feladatokat kell végrehajtania a végleges EIM konfiguráció létrehozásához. 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 beállításához az alábbi különleges jogosultságokra van szükség:

- Biztonsági adminisztrátor (\*SECADM).
- Minden objektum (\*ALLOBJ).
- Rendszerkonfiguráció (\*IOSYSCFG).

Az EIM konfigurációs varázsló használata előtt végre kell hajtania a “Vállalati azonosság leképezés (EIM) megtervezése” oldalszám: 44 lépéseket, és meg kell állapítania, hogy pontosan mire kívánja használni az EIM szolgáltatást. Amennyiben az EIM szolgáltatást egyszeri bejelentkezés környezet megvalósításának részeként konfigurálja, akkor az egyszeri bejelentkezés környezet megtervezését is el kell végeznie.

Ha a tervek elkészültek, akkor megkezdheti a három alapvető EIM konfiguráció egyikének létrehozását az EIM konfigurációs varázslóval. A varázslóval csatlakozhat egy meglévő tartományhoz, de létrehozhat egy új tartományt, és

csatlakozhat ahhoz is. Ha egy új tartomány használata mellett dönt, akkor megadhatja, hogy az EIM tartományvezérlő a helyi vagy egy távoli rendszeren legyen. Az alábbi információk a kiválasztott alapszintű konfiguráció típusától függően tartalmazznak további utasításokat az EIM konfigurációhoz:

**“Új helyi tartomány létrehozása és csatlakozás”** Válassza ezt a feladatot, ha egy új EIM tartományt kíván létrehozni a vállalat számára, és a helyi címtár szerveret jelölte ki 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 csatlakoztathat a tartományhoz. 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.

**“Új távoli tartomány létrehozása és csatlakozás” oldalszám: 68** Válassza ezt a feladatot, ha egy új EIM tartományt kíván létrehozni a vállalat számára, és egy távoli címtár szerveret jelölt ki 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 csatlakoztathat a tartományhoz. 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” oldalszám: 73** Miután az EIM konfigurációs varázslóval beállított egy tartományvezérlőt és egy EIM tartományt egy iSeries szerverem, ezzel a varázsló feladattal csatlakoztathat további iSeries szervereket a tartományhoz. Ezt a varázsló feladatot az hálózat összes olyan iSeries szerverén el kell végeznie, amely használni fogja az EIM funkciókat. Meg kell adnia a tartomány nevét, amelyhez csatlakozni kíván, beleértve az EIM tartományvezérlőre vonatkozó kapcsolati információkat (például portszám, illetve Szállítási réteg biztonság (TLS) vagy Védett socket réteg (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)** elemet.
4. Kattintson a jobb egérgombbal a **Konfiguráció** elemre, majd válassza az előugró menü **Beállítás...** menüpontját az EIM konfigurációs varázsló elindításához.
5. Válasszon ki egy EIM konfigurációs lehetőséget, majd kövesse a varázsló útmutatásait.
6. Amennyiben segítségére szorul a varázsló által kért információkkal kapcsolatban, kattintson a **Súgó** gombra.

## Új helyi tartomány létrehozása és csatlakozás

Ha egy új tartomány létrehozását és használatát választja, akkor az EIM konfiguráció részeként beállíthatja az EIM tartományvezérlőt a helyi rendszeren. Ha szükséges, akkor az EIM konfigurációs varázsló meggyőződik arról, hogy rendelkezésre állnak a címtár 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.

Az EIM konfigurációs varázsló segítségével az alábbi feladatokat hajthatja végre:

- Új EIM tartomány létrehozása.
- Helyi címtár szerver beállítása EIM tartományvezérlőként.
- Hálózati hitelesítési szolgáltatás beállítása a rendszeren.
- EIM nyilvántartás meghatározások létrehozása a helyi OS/400 nyilvántartás és a Kerberos nyilvántartás számára.

- A rendszer csatlakoztatása az új tartományhoz.

Új tartomány létrehozásához és a rendszer csatlakoztatásához az alábbi különleges jogosultságokkal kell rendelkeznie:

- Biztonsági adminisztrátor (\*SECADM).
- Minden objektum (\*ALLOBJ).
- Rendszerkonfiguráció (\*IOSYSCFG).

Ha egy új helyi EIM tartományt kíván létrehozni, és rögtön kapcsolódni is szeretne hozzá, akkor az EIM konfigurációs varázsló segítségével tegye a következőket:

1. Az iSeries navigátorban válassza ki azt a rendszert, amelyen az EIM szolgáltatást be kívánja állítani, és bontsa ki a **Hálózat > Vállalati azonosság leképezés** elemet.
2. Kattintson a jobb egérgombbal a **Konfiguráció** elemre, majd válassza az előugró menü **Beállítás...** menüpontját az EIM konfigurációs varázsló elindításához.

**Megjegyzés:** Ha az EIM korábban már be volt állítva a rendszeren, akkor ennek a lehetőségnek a neve **Újrakonfigurálás...**

3. A varázsló **Üdvözet** lapján válassza az **Új tartomány létrehozása és csatlakozás** lehetőséget, majd kattintson a **Tovább** gombra.
4. Az **EIM tartomány helyének megadása** lapon válassza a **Helyi címtár szerveren** lehetőséget, majd kattintson a **Tovább** gombra.

**Megjegyzés:** Ez a beállítás a helyi címtár szervert konfigurálja EIM tartományvezérlőként. Mivel a tartomány összes EIM adatát ez a címtár szerver tárolja, aktívnek kell lennie és annak is kell maradnia az EIM leképezés keresések és más műveletek támogatásához.

**Megjegyzés:** Ha a hálózati hitelesítési szolgáltatás jelenleg nincs beállítva az iSeries szerveren, vagy az egyszerű bejelentkezés környezet beállításához további hálózati hitelesítési szolgáltatással kapcsolatos konfigurációs információk megadása szükséges, akkor megjelenik a **Hálózati hitelesítési szolgáltatás konfiguráció** lap. Ezen a lapon indíthatja el a Hálózati hitelesítési szolgáltatás konfigurációs varázslót, amely beállítja a hálózati hitelesítési szolgáltatást. Úgy is dönthet, hogy későbbre halasztja a hálózati hitelesítési szolgáltatás konfigurációját, ebben az esetben a varázslót az iSeries navigátorból indíthatja el. Az EIM konfigurációs varázsló a Hálózati hitelesítési szolgáltatás beállítása után folytatódik.

5. A hálózati hitelesítési szolgáltatás beállításának befejezéséhez tegye a következőket:
  - a. A **Hálózati hitelesítési szolgáltatás** lapon válassza ki az **Igen** lehetőséget a Hálózati hitelesítési szolgáltatás konfigurációs varázsló elindításához. Ezzel a varázslóval számos OS/400 illesztőt és szolgáltatást beállíthat a Kerberos tartományban való részvétellel, továbbá létrehozhat egy EIM szolgáltatást és hálózati hitelesítési szolgáltatást egyaránt használó egyszerű bejelentkezés környezetet.
  - b. A **Tartomány információk megadása** lap **Alapértelmezett tartomány** mezőjében adja meg az alapértelmezett tartományt. Ha a Kerberos hitelesítéshez Microsoft Active Directory szolgáltatást használ, akkor válassza ki a **Microsoft Active Directory használata Kerberos hitelesítéshez** lehetőséget, majd kattintson a **Tovább** gombra.
  - c. A **KDC információk megadása** lapon adja meg a tartomány Kerberos kiszolgálójának teljes képzésű nevét a **KDC** mezőben, írjon 88-at a **Port** mezőbe, majd kattintson a **Tovább** gombra.
  - d. A **Jelszó szerver információk megadása** lapon válassza ki az **Igen** vagy a **Nem** lehetőséget a jelszó szerver megadásához. A jelszó szerver lehetővé teszi a jelszavak módosítását a Kerberos kiszolgálón. Amennyiben az **Igen** lehetőséget választotta, akkor adja meg a jelszó szerver nevét a **Jelszó szerver** mezőben. A **Port** mezőben hagyja változatlanul a 464 értéket, és kattintson a **Tovább** gombra.
  - e. A **Kulcs címke bejegyzések kiválasztása** lapon válassza ki az **OS/400 Kerberos hitelesítés** lehetőséget, majd kattintson a **Tovább** gombra.

**Megjegyzés:** Ha egy IBM Directory Server for iSeries (LDAP), egy iSeries NetServer, vagy egy iSeries HTTP szerver szolgáltatást be kíván vonni a Kerberos hitelesítésbe, akkor ezekhez a

szerverekhez is létrehozhat kulcs címke bejegyzéseket. Elképzelhető, hogy további konfigurációs lépések végrehajtására lesz szükség, mielőtt ezek szolgáltatások használhatnák a Kerberos hitelesítést.

- f. Az **OS/400 kulcs címke bejegyzés létrehozása** lapon adja meg kétszer a jelszót, majd kattintson a **Tovább** gombra. Ezt a jelszót kell majd használni, amikor az OS/400 azonosítókat hozzáadja a Kerberos szerverhez.
- g. A **Parancsfájl létrehozása** lapon válassza ki az **Igen** lehetőséget, adja meg az alábbi információkat, majd kattintson a **Tovább** gombra:
  - A **Parancsfájl** mezőben adja meg a helyes könyvtár elérési utat. Kattintson a **Tallózás** gombra a megfelelő könyvtár elérési út megkereséséhez, vagy egyszerűen gépelje be az utat a **Parancsfájl** mezőbe.
  - A **Jelszó tartalmazása** mezőben válassza ki az **Igen** lehetőséget. Ez biztosítja, hogy az OS/400 szolgáltatás azonosítóval kapcsolatos összes jelszó belekerüljön a parancsfájlba. Fontos megjegyezni, hogy a jelszavak egyszerű szöveges formában kerülnek a parancsfájlba, ezért mindenki számára olvashatóak, akinek olvasási joga van a parancsfájllhoz. Ezért alapvető fontosságú, hogy használat után azonnal törölni kell a parancsfájlt a Kerberos szerverről és a PC-ről egyaránt. Ha a jelszavak nem kerülnek a parancsfájlba, akkor a parancsfájl minden futtatásakor jelszót fog kérni.

**Megjegyzés:** A varázsló által létrehozott szolgáltatás azonosítókat kézzel is hozzáadhatja a Microsoft Active Directory szolgáltatáshoz. Ennek módjáról bővebben az OS/400 azonosítók felvétele a Kerberos kiszolgálóra részről olvashat.

- Az **Összegzés** oldalon áttekintheti a hálózati hitelesítési szolgáltatás beállításának részleteit, majd a **Befejezés** gombbal visszatérhet az EIM konfigurációs varázslóhoz.
6. Ha a helyi LDAP szerver jelenleg nincs beállítva, akkor az EIM konfigurációs varázsló visszatérésekor megjelenik a **Címtár szerver beállítása** párbeszédablak. Adja meg az alábbi információkat a helyi címtár szerver beállításához:

**Megjegyzés:** Ha a helyi címtár szervert már az EIM konfigurációs varázsló futtatása előtt konfigurálta, akkor ehelyett a **Felhasználó megadása a kapcsolathoz** lap jelenik meg. Ezen a lapon az LDAP adminisztrátor megkülönböztetett nevének és jelszavának megadásával biztosíthatja, hogy a varázsló elegendő jogosultsággal rendelkezzen az EIM tartomány és objektumainak adminisztrálásához, és folytatni tudja az eljárást a következő lépéssel. Amennyiben segítségre szorul a varázsló által kért információkkal kapcsolatban, kattintson a **Súgó** gombra.

- A **Port** mezőben fogadja el az alapértelmezett 389 portszámot, vagy adjon meg egy másikat a címtár szerverrel folytatott nem biztonságos EIM kommunikációhoz.
  - A **Megkülönböztetett név** mezőben adja meg a címtár szerver LDAP adminisztrátorát azonosító megkülönböztetett nevet (DN). Az EIM konfigurációs varázsló létrehozza a megadott LDAP adminisztrátor megkülönböztetett nevet, és ezt használja fel a létrehozott új tartományhoz tartozó tartományvezerlőként szolgáló címtár szerver beállítására.
  - A **Jelszó** mezőben adja meg az LDAP adminisztrátor jelszavát.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
  - Kattintson a **Tovább** gombra.
7. A **Tartomány meghatározása** lapon 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 = + < > , # ; \ és \* nem használhatók.
    - A **Leírás** mezőben írja be a tartomány szöveges leírását.
    - Kattintson a **Tovább** gombra.
  8. A **Tartomány szülő DN megadása** lapon válassza az **Igen** lehetőséget a létrehozandó tartomány szülő megkülönböztetett nevének megadásához, vagy a **Nem** lehetőséget, ha az EIM adatokat a tartomány nevéből származó utótaggal rendelkező címtár helyen kívánja tárolni.

**Megjegyzés:** Ha a tartományt a helyi címtár szerveren hozza létre, akkor a szülő DN elhagyható. 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. Ha további információkra van szüksége a szülő megkülönböztetett névvel kapcsolatban, akkor kattintson a **Súgó** gombra.

9. A **Nyilvántartás információk** lapon adja meg, hogy a helyi felhasználói nyilvántartásokat fel kell-e venni az EIM tartományba nyilvántartás meghatározásokként. A következő felhasználói nyilvántartási típusok közül választhat:

**Megjegyzés:** Nem szükséges most létrehozni a nyilvántartás meghatározásokat. Ha úgy dönt, hogy később hozza létre a nyilvántartás meghatározásokat, akkor fel kell vennie a rendszer nyilvántartás meghatározásokat és frissítenie kell az EIM konfigurációs tulajdonságait.

- Ha a helyi nyilvántartáshoz kíván nyilvántartás meghatározást létrehozni, akkor válassza ki a **Helyi OS/400** lehetőséget. Elfogadhatja a mezőben felkínált alapértelmezett nyilvántartás meghatározás nevet, vagy megadhat egy új értéket. Az EIM nyilvántartás neve tetszőleges karaktersorozat lehet, amely azonosítja a nyilvántartás típusát és az adott példányt.
- Ha Kerberos nyilvántartáshoz kíván nyilvántartás meghatározást létrehozni, akkor válassza ki a **Kerberos** lehetőséget. Elfogadhatja a mezőben felkínált alapértelmezett nyilvántartás meghatározás nevet, vagy megadhat egy új értéket. Az alapértelmezett definíció név megegyezik a Kerberos tartománynévvvel. Ha elfogadja az alapértéket, és a Kerberos nyilvántartás nevét használja tartománynévként, akkor javíthatja a nyilvántartásban tárolt információk visszakeresésének teljesítményét. Szükség szerint válassza ki a **Kerberos felhasználói azonosságok kis- és nagybetű érzékenyek** lehetőséget.
- Kattintson a **Tovább** gombra.

10. Az **EIM rendszer felhasználó meghatározása** lapon a **Felhasználó típus** mezőben válassza ki, hogy milyen típusú felhasználót használjon a rendszer az operációs rendszer funkciók nevében végzett EIM műveleteknél. Ilyen művelet például a leképezés kikeresésének művelete és a társítások törlése egy helyi OS/400 felhasználói profil törlésekor. A következő felhasználói típusok közül választhat: **Megkülönböztetett név és jelszó**, **Kerberos kulcs címke fájl és azonosító** vagy **Kerberos azonosító és jelszó**. A ténylegesen kiválasztható felhasználó típusok függenek az aktuális rendszerkonfigurációtól. Ha például a Hálózati hitelesítési szolgáltatás nincs beállítva a rendszeren, akkor a Kerberos felhasználói típusok nem állnak rendelkezésre. A megadott felhasználótípus határozza meg a lapon megadandó további információkat az alábbiak szerint:

**Megjegyzés:** Meg kell adnia egy az EIM tartományvezérlőt kiszolgáló címtár szerveren már létező felhasználót. 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 egyszerű bejelentkezéssel és a felhasználói profilok törlésével kapcsolatos operációs rendszer funkciók meghiúsulhatnak.

Ha a címtár szerver beállítása nem történt meg a varázsló futtatását megelőzően, akkor az egyetlen kiválasztható felhasználó típus a **Megkülönböztetett név és jelszó**, és az egyetlen megadható megkülönböztetett név az LDAP adminisztrátori DN.

- A **Megkülönböztetett név és jelszó** választásakor adja meg a következőket:
  - A **Megkülönböztetett név** mezőben adja meg a rendszer által az EIM műveletek végrehajtásához használt felhasználót azonosító LDAP megkülönböztetett nevet.
  - A **Jelszó** mezőben adja meg az LDAP adminisztrátor jelszavát.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
- A **Kerberos azonosító és jelszó** választásakor adja meg a következőket:
  - Az **Azonosító** mezőben adja meg rendszer által az EIM műveletek végrehajtásához használt Kerberos azonosítót.
  - A **Tartomány** mezőben adja meg annak a Kerberos tartománynak a teljes képzésű nevét, amelynek a fenti azonosító tagja. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcs címke fájlban szereplő Kerberos felhasználókat. A `hoszt.vallalat.hu` tartomány `jnap` felhasználóját például a kulcs címke fájlban a `jnap@beszreszl.sajatceg.com` képviseli.



- A **Jelszó** mezőben adja meg a felhasználó jelszavát.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
  - A **Kerberos kulcs címke fájl és azonosító** választásakor adja meg a következőket:
    - A **Kulcs címke fájl** mezőben adja meg a rendszer által az EIM műveletek végrehajtásához használt Kerberos azonosítót tartalmazó kulcs címke fájl teljes képzésű elérési útját és nevét. Vagy kattintson a **Tallózás...** gombra, és keresse meg a kulcs címke fájlt az iSeries rendszer integrált fájlrendszerén.
    - Az **Azonosító** mezőben adja meg rendszer által az EIM műveletek végrehajtásához használt Kerberos azonosítót.
    - A **Tartomány** mezőben adja meg annak a Kerberos tartománynak a teljes képzésű nevét, amelynek a fenti azonosító tagja. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcs címke fájlban szereplő Kerberos felhasználókat. A [hoszt.vallalat.hu](http://hoszt.vallalat.hu) tartomány `jnap` felhasználóját például a kulcs címke fájlban a `jnap@beszreszl.sajatceg.com` képviseli.
  - A **Kapcsolat ellenőrzése** gombbal győződjön meg róla, hogy a varázsló a megadott felhasználói információk felhasználásával valóban képes-e csatlakozni az EIM tartományvezérlőhöz.
  - Kattintson a **Tovább** gombra.
11. Az **Összegzés** párbeszédablakban tekintse át a megadott konfigurációs információkat. Ha a megjelenő információk helyesek, akkor kattintson a **Befejezés** gombra.

Amikor a varázsló befejeződik, hozzáadja az új tartományt a **Tartománykezelés** mappához, és a szerveren létrejött egy alapszintű EIM konfiguráció. A tartomány EIM konfigurációjának véglegesítéséhez azonban még el kell végeznie a következő feladatokat is:

1. Futtassa le az EIM konfigurációs varázslót az összes olyan szerveren, amelyet szándékában áll csatlakoztatni a tartományhoz.
2. Szükség szerint adja hozzá a tartományba bevonni kívánt nem iSeries szerverek és alkalmazások nyilvántartás meghatározásait az EIM tartományhoz. Ezek a nyilvántartás meghatározások a tartományban szereplő felhasználói nyilvántartásokra hivatkoznak. Az EIM megvalósítástól függően lehetséges rendszer nyilvántartás meghatározások felvétele vagy alkalmazás nyilvántartás meghatározások hozzáadása.
3. Az EIM megvalósítás függvényében döntsön arról, hogy:
  - EIM azonosítók létrehozása és azonosító társítások elkészítése szükséges minden egyes egyedi felhasználó vagy entitás számára a tartományban.
  - Irányelv társítások létrehozása szükséges a felhasználók csoportjainak leképezéséhez egyetlen cél felhasználói azonosságra.
  - A fentiek kombinációjára van szükség.
4. A leképezés tesztelése EIM funkció segítségével ellenőrizze az EIM konfiguráció azonosság leképezéseit.
5. Ha az egyetlen beállított EIM felhasználó az LDAP adminisztrátor megkülönböztetett neve, akkor az aktuális EIM felhasználó magas szintű hozzáféréssel rendelkezik a címtár szerver adataihoz. Ezért érdemes megfontolni még legalább egy DN létrehozását, amely megfelelő, korlátozott hozzáférés felügyelettel rendelkezik az EIM adatok fölött. A megkülönböztetett nevek létrehozásáról bővebb információkat a *Megkülönböztetett nevek* témakörben talál az IBM Directory Server for iSeries (LDAP) dokumentációjában. A meghatározandó további EIM felhasználók száma attól függ, hogy a rendszer biztonsági stratégiája mekkora hangsúlyt fektet a biztonsági feladatok és felelőségek elkülönítésére. Általában célszerű létrehozni legalább az alábbi két DN típust:
  - **EIM adminisztratori hozzáférés felügyelettel rendelkező felhasználó**  
Ez az EIM adminisztratori DN biztosítja a megfelelő szintű jogosultságot az EIM tartomány kezeléséért felelős adminisztrátorok számára. Ezt az EIM adminisztratori megkülönböztetett nevet olyan esetekben lehet használni, amikor az EIM tartomány összes jellemzőjének kezelésére szükség lehet, például amikor az iSeries navigátor kapcsolódik a tartományvezérlőhöz.
  - **Legalább egy felhasználó, aki rendelkezik az alábbi hozzáférés felügyelettel:**
    - Azonosító adminisztrátor
    - Nyilvántartás adminisztrátor
    - EIM leképezés műveletek

Ez a felhasználó biztosítja a megfelelő szintű hozzáférés felügyeletet az operációs rendszer nevében EIM műveleteket végrehajtó rendszerfelhasználó számára.

**Megjegyzés:** Ahhoz, hogy ezt az új megkülönböztetett nevet használja a rendszerfelhasználó az LDAP adminisztrátori DN helyett, változtassa meg az iSeries szerver EIM konfigurációs tulajdonságait. A rendszerfelhasználó által használt DN megváltoztatásával kapcsolatban lásd az EIM konfigurációs tulajdonságok kezelése témakört.

Emellett az EIM adatok átvitelének biztosítása érdekében szükség esetén beállíthatja a tartományvezérlő biztonságos kapcsolatát a Védett socket réteg (SSL) vagy Szállítási réteg biztonság (TLS) protokollokkal. Ha engedélyezi az SSL használatát a címtár szerver számára, akkor az EIM konfigurációs tulajdonságok frissítésével meg kell adnia, hogy az iSeries szerver biztonságos SSL kapcsolatot használ. Ezen kívül a tartomány konfigurációjában is meg kell adnia, hogy az EIM biztonságos SSL kapcsolatot használ a tartomány kezeléséhez az iSeries navigátoron keresztül.

**Megjegyzés:** Ha alapszintű hálózati hitelesítési szolgáltatás konfigurációt is létrehozott, akkor további feladatokat is el kell végeznie, különösen egyszeri bejelentkezés környezet megvalósítása esetén. Ezekről a további lépésekről bővebb információkat talál a teljes konfigurációs folyamatot példahelyzetten keresztül bemutató Az OS/400 felkészítése egyszeri bejelentkezésre dokumentumban.

## Új távoli tartomány létrehozása és csatlakozás

Ha egy új tartomány létrehozását és használatát választja, akkor az EIM konfiguráció részeként beállíthat EIM tartományvezérlőnek egy távoli rendszeren található címtár szervert. A sikeres EIM beállítás érdekében meg kell adnia a távoli címtár szerver csatlakozási információit. Ha a Kerberos még nincs beállítva az iSeries szerveren, akkor a varázsló lehetőséget nyújt a Hálózati hitelesítési szolgáltatás konfigurációs varázsló elindítására.

**Megjegyzés:** A címtár szervernek a távoli rendszeren biztosítania kell EIM támogatást. Az EIM megköveteli, hogy a tartományvezérlőt 3-as verziójú Egyszerűsített címtárhozzáférési protokollt (LDAP) támogató címtár szerver szolgáltatassa, továbbá hogy az EIM séma konfigurálva legyen a címtár szerver termékben. Az IBM Directory Server V5.1 például teljesíti ezeket a feltételeket. Az EIM tartományvezérlővel szemben támasztott követelményekről bővebb információkat az EIM tartományvezérlő megtervezése résznél talál.

Az EIM konfigurációs varázsló segítségével az alábbi feladatokat hajthatja végre:

- Új EIM tartomány létrehozása.
- Távoli címtár szerver beállítása EIM tartományvezérlőként.
- Hálózati hitelesítési szolgáltatás beállítása a rendszeren.
- EIM nyilvántartás meghatározások létrehozása a helyi OS/400 nyilvántartás és a Kerberos nyilvántartás számára.
- A rendszer csatlakoztatása az új tartományhoz.

Új tartomány létrehozásához és a rendszer csatlakoztatásához az alábbi különleges jogosultságokkal kell rendelkeznie:

- Biztonsági adminisztrátor (\*SECADM).
- Minden objektum (\*ALLOBJ).
- Rendszerkonfiguráció (\*IOSYSCFG).

Ha egy távoli rendszeren új EIM tartományt kíván létrehozni, és rögtön kapcsolódni is szeretne hozzá, akkor az EIM konfigurációs varázsló segítségével tegye a következőket:

1. Győződjön meg róla, hogy a címtár szerver a távoli rendszeren aktív. Ennek módjával kapcsolatban olvassa el a címtár szerver termék dokumentációját.
2. Az iSeries navigátorban válassza ki azt a rendszert, amelyen az EIM szolgáltatást be kívánja állítani, és bontsa ki a **Hálózat > Vállalati azonosság leképezés** elemet.
3. Kattintson a jobb egérgombbal a **Konfiguráció** elemre, majd válassza az előugró menü **Beállítás...** menüpontját az EIM konfigurációs varázsló elindításához.

**Megjegyzés:** Ha az EIM korábban már be volt állítva a rendszeren, akkor ennek a lehetőségnek a neve **Újrakonfigurálás...**

4. A varázsló **Üdvözet** lapján válassza az **Új tartomány létrehozása és csatlakozás** lehetőséget, majd kattintson a **Tovább** gombra.
5. Az **EIM tartomány helyének megadása** lapon válassza a **Távoli című társzerveren** lehetőséget, majd kattintson a **Tovább** gombra.

**Megjegyzés:** Ez a beállítás egy távoli című társzervert állít be EIM tartományvezérlőként. Ahhoz, hogy megadott távoli című társzerver EIM tartományvezérlőként működhessen, EIM támogatást kell biztosítani. Az EIM konfiguráció sikeres befejezéséhez aktívnak kell lennie, és a továbbiakban is aktívnak kell maradnia az EIM leképezés keresések és más műveletek támogatásához.

**Megjegyzés:** Ha a hálózati hitelesítési szolgáltatás jelenleg nincs beállítva az iSeries szerveren, vagy az egyszeri bejelentkezés környezet beállításához további hálózati hitelesítési szolgáltatással kapcsolatos konfigurációs információk megadása szükséges, akkor megjelenik a **Hálózati hitelesítési szolgáltatás konfiguráció** lap. Ezen a lapon indíthatja el a Hálózati hitelesítési szolgáltatás konfigurációs varázslót, amely beállítja a hálózati hitelesítési szolgáltatást. Úgy is dönthet, hogy későbbre halasztja a hálózati hitelesítési szolgáltatás konfigurációját, ebben az esetben a varázslót az iSeries navigátorból indíthatja el. Az EIM konfigurációs varázsló a Hálózati hitelesítési szolgáltatás beállítása után folytatódik.

6. A hálózati hitelesítési szolgáltatás beállításának befejezéséhez tegye a következőket:
  - a. A **Hálózati hitelesítési szolgáltatás** lapon válassza ki az **Igen** lehetőséget a Hálózati hitelesítési szolgáltatás konfigurációs varázsló elindításához. Ezzel a varázslóval számos OS/400 illesztőt és szolgáltatást beállíthat a Kerberos tartományban való részvételre, továbbá létrehozhat egy EIM szolgáltatást és hálózati hitelesítési szolgáltatást egyaránt használó egyszeri bejelentkezés környezetet.
  - b. A **Tartomány információk megadása** lap **Alapértelmezett tartomány** mezőjében adja meg az alapértelmezett tartományt. Ha a Kerberos hitelesítéshez Microsoft Active Directory szolgáltatást használ, akkor válassza ki a **Microsoft Active Directory használata Kerberos hitelesítéshez** lehetőséget, majd kattintson a **Tovább** gombra.
  - c. A **KDC információk megadása** lapon adja meg a tartomány Kerberos kiszolgálójának teljes képzésű nevét a **KDC** mezőben, írjon 88-at a **Port** mezőbe, majd kattintson a **Tovább** gombra.
  - d. A **Jelszó szerver információk megadása** lapon válassza ki az **Igen** vagy a **Nem** lehetőséget a jelszó szerver megadásához. A jelszó szerver lehetővé teszi a jelszavak módosítását a Kerberos kiszolgálón. Amennyiben az **Igen** lehetőséget választotta, akkor adja meg a jelszó szerver nevét a **Jelszó szerver** mezőben. A **Port** mezőben hagyja változatlanul a 464 értéket, és kattintson a **Tovább** gombra.
  - e. A **Kulcsnév bejegyzések kiválasztása** lapon válassza ki az **OS/400 Kerberos hitelesítés** lehetőséget, majd kattintson a **Tovább** gombra.

**Megjegyzés:** Ha egy IBM Directory Server for iSeries (LDAP), egy iSeries NetServer, vagy egy iSeries HTTP szerver szolgáltatást be kíván vonni a Kerberos hitelesítésbe, akkor ezekhez a szerverekhez is létrehozhat kulcsnév bejegyzéseket. Elképzelhető, hogy további konfigurációs lépések végrehajtására lesz szükség, mielőtt ezek szolgáltatások használhatnák a Kerberos hitelesítést.

- f. Az **OS/400 kulcsnév bejegyzés létrehozása** lapon adja meg kétszer a jelszót, majd kattintson a **Tovább** gombra. Ezt a jelszót kell majd használni, amikor az OS/400 azonosítókat hozzáadja a Kerberos szerverhez.
- g. A **Parancsfájl létrehozása** lapon válassza ki az **Igen** lehetőséget, adja meg az alábbi információkat, majd kattintson a **Tovább** gombra:
  - A **Parancsfájl** mezőben adja meg a helyes könyvtár elérési utat. Kattintson a **Tallózás** gombra a megfelelő könyvtár elérési út megkereséséhez, vagy egyszerűen gépelje be az utat a **Parancsfájl** mezőbe.
  - A **Jelszó tartalmazása** mezőben válassza ki az **Igen** lehetőséget. Ez biztosítja, hogy az OS/400 szolgáltatás azonosítóval kapcsolatos összes jelszó belekerüljön a parancsfájlba. Fontos megjegyezni, hogy a jelszavak egyszerű szöveges formában kerülnek a parancsfájlba, ezért mindenki számára olvashatóak, akinek olvasási

joga van a parancsfájllhoz. Ezért alapvető fontosságú, hogy használat után azonnal törölni kell a parancsfájlt a Kerberos szerverről és a PC-ről egyaránt. Ha a jelszavak nem kerülnek a parancsfájlba, akkor a parancsfájl minden futtatásakor jelszót fog kérni.

**Megjegyzés:** A varázsló által létrehozott szolgáltatás azonosítókat kézzel is hozzáadhatja a Microsoft Active Directory szolgáltatáshoz. Ennek módjáról bővebben az OS/400 azonosítók felvétele a Kerberos kiszolgálóra részről olvashat.

- Az **Összegzés** oldalon áttekintheti a hálózati hitelesítési szolgáltatás beállításának részleteit, majd a **Befejezés** gombbal visszatérhet az EIM konfigurációs varázslóhoz.

7. Az **EIM tartományvezérlő megadása** lapon az alábbi kapcsolat információkat adhatja meg a beállítani kívánt EIM tartományvezérlőhöz.

- A **Tartományvezérlő neve** mezőben adja meg a létrehozandó EIM tartomány tartományvezérlőjeként beállítani kívánt távoli címtár szerver nevét. Az EIM tartományvezérlő név lehet a címtár szerver TCP/IP hoszt- és tartományneve, vagy a címtár szerver címe.
- Adja meg a tartományvezérlő kapcsolatára vonatkozó információkat az alábbiak szerint:
  - Ha az EIM tartományvezérlő eléréséhez biztonságos kapcsolatot kíván használni, akkor engedélyezze a **Biztonságos kapcsolat használata (SSL vagy TLS)** lehetőséget. Ha ez a lehetőség engedélyezve van, akkor az Internethez hasonló megbízhatatlan hálózatokon keresztül létesített kapcsolatok esetén Védett socket réteg (SSL) vagy Szállítási réteg biztonság (TLS) biztosítja az EIM adatforgalmat.

**Megjegyzés:** Ellenőrizze, hogy az EIM tartományvezérlő fel van-e készítve biztonságos kapcsolat használatára. Ha nem, akkor a kapcsolódás nem fog sikerülni.

- A **Port** mezőben adja meg azt a TCP/IP portot, amelyiken a címtár szerver a kapcsolatokat fogadja. Ha a **Biztonságos kapcsolat használata** lehetőség be van kapcsolva, akkor az alapértelmezett portszám 636; egyébként 389.
- A **Kapcsolat ellenőrzése** gombbal ellenőrizze, hogy a varázsló a megadott információk felhasználásával valóban képes-e csatlakozni a távoli EIM tartományvezérlőhöz.
- Kattintson a **Tovább** gombra.

8. A **Kapcsolati felhasználó meghatározása** lapon válasszon ki egy **Felhasználó típus** értéket a kapcsolathoz. A következő felhasználói típusok közül választhat: **Megkülönböztetett név és jelszó**, **Kerberos kulcs címke fájl és azonosító**, **Kerberos azonosító és jelszó**, vagy **Felhasználói profil 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:

**Megjegyzés:** Válassza a **Megkülönböztetett név és jelszó** felhasználótípust és felhasználónak adja meg az LDAP adminisztrátor megkülönböztetett nevét és jelszavát annak érdekében, hogy a varázslónak meglegyen a megfelelő jogosultsága a szükséges EIM objektumok létrehozására a címtárban.

Használhat más felhasználót is a kapcsolathoz, de a megadott felhasználónak az LDAP adminisztrátorral egyenértékű jogosultsággal kell rendelkeznie a távoli címtár szerverhez.

- A **Megkülönböztetett név és jelszó** választásakor adja meg a következőket:
  - A **Megkülönböztetett név** mezőben adja meg az LDAP adminisztrátor megkülönböztetett nevét (DN) és jelszavát ahhoz, hogy a varázsló elegendő jogosultsággal rendelkezzen az EIM tartomány és a benne található objektumok adminisztrálására.
  - A **Jelszó** mezőben adja meg az LDAP adminisztrátor jelszavát.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
- A **Kerberos kulcs címke fájl és azonosító** választásakor adja meg a következőket:
  - A **Kulcs címke fájl** mezőben adja meg a varázsló által az EIM tartományhoz kapcsolódáshoz használt Kerberos azonosítót tartalmazó kulcs címke fájl teljes képzésű elérési útját és nevét. Vagy kattintson a **Tallózás...** gombra, és keresse meg a kulcs címke fájlt az iSeries rendszer integrált fájlrendszerén.
  - Az **Azonosító** mezőben adja meg a felhasználót azonosító Kerberos azonosító nevét.

- A **Tartomány** mezőben adja meg annak a Kerberos tartománynak a teljes képzésű nevét, amelynek a fenti azonosító tagja. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcs címke fájlban szereplő Kerberos felhasználókat. A `hoszt.vallalat.hu` tartomány `jnap` felhasználóját például a kulcs címke fájlban a `jnap@beszreszl.sajatceg.com` képviseli.
- A **Kerberos azonosító és jelszó** választásakor adja meg a következőket:
  - Az **Azonosító** mezőben adja meg varázsló által az EIM tartományhoz kapcsolódáshoz használt Kerberos azonosítót.
  - A **Tartomány** mezőben adja meg annak a Kerberos tartománynak a teljes képzésű nevét, amelynek a fenti azonosító tagja. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcs címke fájlban szereplő Kerberos felhasználókat. A `hoszt.vallalat.hu` tartomány `jnap` felhasználóját például a kulcs címke fájlban a `jnap@beszreszl.sajatceg.com` képviseli.
  - A **Jelszó** mezőben adja meg a Kerberos azonosítóhoz tartozó jelszót.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
- A **Felhasználói profil és jelszó** választásakor adja meg a következőket:
  - Az **Felhasználói profil** mezőben adja meg varázsló által az EIM tartományhoz kapcsolódáshoz használt felhasználói profilt.
  - A **Jelszó** mezőben adja meg a felhasználói profilhoz tartozó jelszót.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
- A **Kapcsolat ellenőrzése** gombbal győződjön meg róla, hogy a varázsló a megadott felhasználói információk felhasználásával valóban képes-e csatlakozni az EIM tartományvezérlőhöz.
- Kattintson a **Tovább** gombra.

9. A **Tartomány meghatározása** lapon 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 = + < > , # ; \ és \* nem használhatók.
- A **Leírás** mezőben írja be a tartomány szöveges leírását.
- Kattintson a **Tovább** gombra.

10. A **Szülő DN megadása a tartományhoz** párbeszédablakon válassza az **Igen** lehetőséget a varázsló által a létrehozandó tartomány helyéhez használt szülő megkülönböztetett név megadásához. Ez a DN jelképezi a címtár információkat tartalmazó fahierarchiában közvetlenül a tartománynév fölött elhelyezkedő bejegyzést. Ha az EIM adatokat a tartománynévből származtatott utótaggal rendelkező címtár helyen kívánja tárolni, akkor válassza a **Nem** lehetőséget.

**Megjegyzés:** Ha a varázslóval egy távoli tartományvezérlőn állít be egy tartományt, akkor meg kell adnia egy megfelelő szülő megkülönböztetett nevet a tartomány számára. Mivel az EIM sikeres beállításához az összes szükséges konfigurációs objektumnak léteznie kell a szülő megkülönböztetett névhez, javasolt a DN információk kézi megadása helyett inkább a tallózással megkeresni azokat. Ha további információkra van szüksége a szülő megkülönböztetett névvel kapcsolatban, akkor kattintson a **Súgó** gombra.

11. A **Nyilvántartás információk** lapon adja meg, hogy a helyi felhasználói nyilvántartásokat fel kell-e venni az EIM tartományba nyilvántartás meghatározásokként. A következő felhasználói nyilvántartási típusok közül választhat:

**Megjegyzés:** Nem szükséges most létrehozni a nyilvántartás meghatározásokat. Ha úgy dönt, hogy később hozza létre a nyilvántartás meghatározásokat, akkor fel kell vennie a rendszer nyilvántartás meghatározásokat és frissítenie kell az EIM konfigurációs tulajdonságait.

- Ha a helyi nyilvántartáshoz kíván nyilvántartás meghatározást létrehozni, akkor válassza ki a **Helyi OS/400** lehetőséget. Elfogadhatja a mezőben felkínált alapértelmezett nyilvántartás meghatározás nevet, vagy megadhat egy új értéket. Az EIM nyilvántartás neve tetszőleges karaktersorozat lehet, amely azonosítja a nyilvántartás típusát és az adott példányt.
- Ha Kerberos nyilvántartáshoz kíván nyilvántartás meghatározást létrehozni, akkor válassza ki a **Kerberos** lehetőséget. Elfogadhatja a mezőben felkínált alapértelmezett nyilvántartás meghatározás nevet, vagy megadhat

egy új értéket. Az alapértelmezett definíció név megegyezik a Kerberos tartománynévvel. Ha elfogadja az alapértékeket, és a Kerberos nyilvántartás nevét használja tartománynévként, akkor javíthatja a nyilvántartásban tárolt információk visszakeresésének teljesítményét. Szükség szerint válassza ki a **Kerberos felhasználói azonosságok kis- és nagybetű érzékenyek** lehetőséget.

- Kattintson a **Tovább** gombra.

12. Az **EIM rendszer felhasználó meghatározása** lapon a **Felhasználó típus** mezőben válassza ki, hogy milyen típusú felhasználót használjon a rendszer az operációs rendszer funkciók nevében végzett EIM műveleteknél. Ilyen művelet például a leképezés kikeresésének művelete és a társítások törlése egy helyi OS/400 felhasználói profil törlésekor. A következő felhasználói típusok közül választhat: **Megkülönböztetett név és jelszó**, **Kerberos kulcs címke fájl és azonosító** vagy **Kerberos azonosító és jelszó**. A ténylegesen kiválasztható felhasználó típusok függenek az aktuális rendszerkonfigurációtól. Ha például a Hálózati hitelesítési szolgáltatás nincs beállítva a rendszeren, akkor a Kerberos felhasználói típusok nem állnak rendelkezésre. A megadott felhasználótípus határozza meg a lapon megadandó további információkat az alábbiak szerint:

**Megjegyzés:** Meg kell adnia egy az EIM tartományvezérlőt kiszolgáló címtár szerveren már létező felhasználót. 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.

Ha a címtár szerver beállítása nem történt meg a varázsló futtatását megelőzően, akkor az egyetlen kiválasztható felhasználó típus a **Megkülönböztetett név és jelszó**, és az egyetlen megadható megkülönböztetett név az LDAP adminisztrátori DN.

- A **Megkülönböztetett név és jelszó** választásakor adja meg a következőket:
  - A **Megkülönböztetett név** mezőben adja meg a rendszer által az EIM műveletek végrehajtásához használt felhasználót azonosító LDAP megkülönböztetett nevet.
  - A **Jelszó** mezőben adja meg az LDAP adminisztrátor jelszavát.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
- A **Kerberos azonosító és jelszó** választásakor adja meg a következőket:
  - Az **Azonosító** mezőben adja meg rendszer által az EIM műveletek végrehajtásához használt Kerberos azonosítót.
  - A **Tartomány** mezőben adja meg annak a Kerberos tartománynak a teljes képzésű nevét, amelynek a fenti azonosító tagja. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcs címke fájlban szereplő Kerberos felhasználókat. A `hoszt.vallalat.hu` tartomány `jnap` felhasználóját például a kulcs címke fájlban a `jnap@beszreszl.sajatceg.com` képviseli.
  - A **Jelszó** mezőben adja meg a felhasználó jelszavát.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
- A **Kerberos kulcs címke fájl és azonosító** választásakor adja meg a következőket:
  - A **Kulcs címke fájl** mezőben adja meg a rendszer által az EIM műveletek végrehajtásához használt Kerberos azonosítót tartalmazó kulcs címke fájl teljes képzésű elérési útját és nevét. Vagy kattintson a **Tallózás...** gombra, és keresse meg a kulcs címke fájl az iSeries rendszer integrált fájlrendszerén.
  - Az **Azonosító** mezőben adja meg rendszer által az EIM műveletek végrehajtásához használt Kerberos azonosítót.
  - A **Tartomány** mezőben adja meg annak a Kerberos tartománynak a teljes képzésű nevét, amelynek a fenti azonosító tagja. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcs címke fájlban szereplő Kerberos felhasználókat. A `hoszt.vallalat.hu` tartomány `jnap` felhasználóját például a kulcs címke fájlban a `jnap@beszreszl.sajatceg.com` képviseli.
- A **Kapcsolat ellenőrzése** gombbal győződjön meg róla, hogy a varázsló a megadott felhasználói információk felhasználásával valóban képes-e csatlakozni az EIM tartományvezérlőhöz.
- Kattintson a **Tovább** gombra.

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

Amikor a varázsló befejeződik, hozzáadja az új tartományt a **Tartománykezelés** mappához, és a szerveren létrejött egy alapszintű EIM konfiguráció. A tartomány EIM konfigurációjának véglegesítéséhez azonban még el kell végeznie a következő feladatokat is:

1. Futtassa le az EIM konfigurációs varázslót az összes olyan szerveren, amelyet szándékában áll csatlakoztatni az új tartományhoz.

2. Szükség szerint adja hozzá a tartományba bevonni kívánt nem iSeries szerverek és alkalmazások nyilvántartás meghatározásait az EIM tartományhoz. Ezek a nyilvántartás meghatározások a tartományban szereplő felhasználói nyilvántartásokra hivatkoznak. Az EIM megvalósítástól függően lehetséges rendszer nyilvántartás meghatározások felvétele vagy alkalmazás nyilvántartás meghatározások hozzáadása.

3. Az EIM megvalósítás függvényében döntsön arról, hogy:

- EIM azonosítók létrehozása és azonosító társítások elkészítése szükséges minden egyes egyedi felhasználó vagy entitás számára a tartományban.
- Irányelv társítások létrehozása szükséges a felhasználók csoportjainak leképezéséhez egyetlen cél felhasználói azonosságra.
- A fentiek kombinációjára van szükség.

4. A leképezés tesztelése EIM funkció segítségével ellenőrizze az EIM konfiguráció azonosság leképezéseit.

5. Ha az egyetlen beállított EIM felhasználó az LDAP adminisztrátor megkülönböztetett neve, akkor az aktuális EIM felhasználó magas szintű hozzáféréssel rendelkezik a címtár szerver adataihoz. Ezért érdemes megfontolni még legalább egy DN létrehozását, amely megfelelő, korlátozott hozzáférés felügyelettel rendelkezik az EIM adatok fölött. A megkülönböztetett nevek létrehozásáról bővebb információkat a *Megkülönböztetett nevek témakörben* talál az IBM Directory Server for iSeries (LDAP) dokumentációjában. A meghatározandó további EIM felhasználók száma attól függ, hogy a rendszer biztonsági stratégiája mekkora hangsúlyt fektet a biztonsági feladatok és felelőségek elkülönítésére. Általában célszerű létrehozni legalább az alábbi két DN típust:

- **EIM adminisztratori hozzáférés felügyelettel rendelkező felhasználó**

Ez az EIM adminisztratori DN biztosítja a megfelelő szintű jogosultságot az EIM tartomány kezeléséért felelős adminisztrátorok számára. Ezt az EIM adminisztratori megkülönböztetett nevet olyan esetekben lehet használni, amikor az EIM tartomány összes jellemzőjének kezelésére szükség lehet, például amikor az iSeries navigátor kapcsolódik a tartományvezérlőhöz.

- **Legalább egy felhasználó, aki rendelkezik az alábbi hozzáférés felügyelettel:**

- Azonosító adminisztrátor
- Nyilvántartás adminisztrátor
- EIM leképezés műveletek

Ez a felhasználó biztosítja a megfelelő szintű hozzáférés felügyeletet az operációs rendszer nevében EIM műveleteket végrehajtó rendszerfelhasználó számára.

**Megjegyzés:** Ahhoz, hogy ezt az új megkülönböztetett nevet használja a rendszerfelhasználó az LDAP adminisztratori DN helyett, változtassa meg az iSeries szerver EIM konfigurációs tulajdonságait. A rendszerfelhasználó által használt DN megváltoztatásával kapcsolatban lásd az EIM konfigurációs tulajdonságok kezelése témakört.

**Megjegyzés:** Ha alapszintű hálózati hitelesítési szolgáltatás konfigurációt is létrehozott, akkor további feladatokat is el kell végeznie, különösen egyszeri bejelentkezés környezet megvalósítása esetén. Ezekről a további lépésekről bővebb információkat talál a teljes konfigurációs folyamatot példahelyzetben keresztül bemutató Az OS/400 felkészítése egyszeri bejelentkezésre dokumentumban.

## Csatlakozás meglévő tartományhoz

Miután létrehozta az EIM tartományt és egy rendszeren tartományvezérlőnek állította be a címtár szervert, csatlakoztathatja az összes többi (V5R2 vagy későbbi) iSeries szervert az EIM tartományhoz. A varázsló végrehajtása

során meg kell adnia a tartományra vonatkozó információkat, ideértve az EIM tartományvezérlő kapcsolati információit is. Ha a Kerberos beállítását az EIM konfiguráció részeként kívánja elvégezni a rendszeren, akkor az EIM konfigurációs varázsló akkor is biztosítja a Hálózati hitelesítési szolgáltatás konfigurációs varázsló elindításának lehetőségét, ha a varázslót egy létező tartományhoz történő csatlakozásra használja.

l Az EIM konfigurációs varázsló segítségével egy létező tartományhoz csatlakozik, akkor az alábbi feladatokat hajthatja végre:

- l • Hálózati hitelesítési szolgáltatás beállítása a rendszeren.
- l • EIM nyilvántartás meghatározások létrehozása a helyi OS/400 nyilvántartás és a Kerberos nyilvántartás számára.
- l • A rendszer csatlakoztatása az meglévő tartományhoz.

A rendszer csatlakoztatásához a meglévő tartományhoz az alábbi különleges jogosultságokkal kell rendelkeznie:

- Biztonsági adminisztrátor (\*SECADM).
- Minden objektum (\*ALLOBJ).

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

- l 1. Győződjön meg róla, hogy a címtár szerver a távoli rendszeren aktív. Ennek módjával kapcsolatban olvassa el a címtár szerver termék dokumentációját.
- l 2. Az iSeries navigátorban válassza ki azt a rendszert, amelyen az EIM szolgáltatást be kívánja állítani, és bontsa ki a **Hálózat > Vállalati azonosság leképezés** elemet.
- l 3. Kattintson a jobb egérgombbal a **Konfiguráció** elemre, majd válassza az előugró menü **Beállítás...** menüpontját az EIM konfigurációs varázsló elindításához.

**Megjegyzés:** Ha az EIM korábban már be volt állítva a rendszeren, akkor ennek a lehetőségnek a neve **Újrakonfigurálás...**

- l 4. A varázsló **Üdvözet** lapján válassza a **Csatlakozás meglévő tartományhoz** lehetőséget, majd kattintson a **Tovább** gombra.

**Megjegyzés:** Ha a hálózati hitelesítési szolgáltatás jelenleg nincs beállítva az iSeries szerveren, vagy az egyszerű bejelentkezés környezet beállításához további hálózati hitelesítési szolgáltatással kapcsolatos konfigurációs információk megadása szükséges, akkor megjelenik a **Hálózati hitelesítési szolgáltatás konfiguráció** lap. Ezen a lapon indíthatja el a Hálózati hitelesítési szolgáltatás konfigurációs varázslót, amely beállítja a hálózati hitelesítési szolgáltatást. Úgy is dönthet, hogy későbbre halasztja a hálózati hitelesítési szolgáltatás konfigurációját, ebben az esetben a varázslót az iSeries navigátorból indíthatja el. Az EIM konfigurációs varázsló a Hálózati hitelesítési szolgáltatás beállítása után folytatódik.

- l 5. A hálózati hitelesítési szolgáltatás beállításának befejezéséhez tegye a következőket:
  - l a. A **Hálózati hitelesítési szolgáltatás** lapon válassza ki az **Igen** lehetőséget a Hálózati hitelesítési szolgáltatás konfigurációs varázsló elindításához. Ezzel a varázslóval számos OS/400 illesztőt és szolgáltatást beállíthat a Kerberos tartományban való részvételre, továbbá létrehozhat egy EIM szolgáltatást és hálózati hitelesítési szolgáltatást egyaránt használó egyszerű bejelentkezés környezetet.
  - l b. A **Tartomány információk megadása** lap **Alapértelmezett tartomány** mezőjében adja meg az alapértelmezett tartományt. Ha a Kerberos hitelesítéshez Microsoft Active Directory szolgáltatást használ, akkor válassza ki a **Microsoft Active Directory használata Kerberos hitelesítéshez** lehetőséget, majd kattintson a **Tovább** gombra.
  - l c. A **KDC információk megadása** lapon adja meg a tartomány Kerberos kiszolgálójának teljes képzésű nevét a **KDC** mezőben, írjon **88**-at a **Port** mezőbe, majd kattintson a **Tovább** gombra.
  - l d. A **Jelszó szerver információk megadása** lapon válassza ki az **Igen** vagy a **Nem** lehetőséget a jelszó szerver megadásához. A jelszó szerver lehetővé teszi a jelszavak módosítását a Kerberos kiszolgálón. Amennyiben az **Igen** lehetőséget választotta, akkor adja meg a jelszó szerver nevét a **Jelszó szerver** mezőben. A **Port** mezőben hagyja változatlanul a **464** értéket, és kattintson a **Tovább** gombra.



- e. A **Kulcscímke bejegyzések kiválasztása** lapon válassza ki az **OS/400 Kerberos hitelesítés** lehetőséget, majd kattintson a **Tovább** gombra.

**Megjegyzés:** Ha egy IBM Directory Server for iSeries (LDAP), egy iSeries NetServer, vagy egy iSeries HTTP szerver szolgáltatást be kíván vonni a Kerberos hitelesítésbe, akkor ezekhez a szerverekhez is létrehozhat kulcscímke bejegyzéseket. Elképzelhető, hogy további konfigurációs lépések végrehajtására lesz szükség, mielőtt ezek szolgáltatások használhatnák a Kerberos hitelesítést.

- f. Az **OS/400 kulcscímke bejegyzés létrehozása** lapon adja meg kétszer a jelszót, majd kattintson a **Tovább** gombra. Ezt a jelszót kell majd használni, amikor az OS/400 azonosítókat hozzáadja a Kerberos szerverhez.

- g. A **Parancsfájl létrehozása** lapon válassza ki az **Igen** lehetőséget, adja meg az alábbi információkat, majd kattintson a **Tovább** gombra:

- A **Parancsfájl** mezőben adja meg a helyes könyvtár elérési utat. Kattintson a **Tallózás** gombra a megfelelő könyvtár elérési út megkereséséhez, vagy egyszerűen gépelje be az utat a **Parancsfájl** mezőbe.
- A **Jelszó tartalmazása** mezőben válassza ki az **Igen** lehetőséget. Ez biztosítja, hogy az OS/400 szolgáltatás azonosítóval kapcsolatos összes jelszó belekerüljön a parancsfájlba. Fontos megjegyezni, hogy a jelszavak egyszerű szöveges formában kerülnek a parancsfájlba, ezért mindenki számára olvashatóak, akinek olvasási joga van a parancsfájllhoz. Ezért alapvető fontosságú, hogy használat után azonnal törölni kell a parancsfájlt a Kerberos szerverről és a PC-ről egyaránt. Ha a jelszavak nem kerülnek a parancsfájlba, akkor a parancsfájl minden futtatásakor jelszót fog kérni.

**Megjegyzés:** A varázsló által létrehozott szolgáltatás azonosítókat kézzel is hozzáadhatja a Microsoft Active Directory szolgáltatáshoz. Ennek módjáról bővebben az OS/400 azonosítók felvétele a Kerberos kiszolgálóra részről olvashat.

- Az **Összegzés** oldalon áttekintheti a hálózati hitelesítési szolgáltatás beállításának részleteit, majd a **Befejezés** gombbal visszatérhet az EIM konfigurációs varázslóhoz.

6. A **Tartományvezérlő meghatározása** lapon adja meg a következő információkat:

**Megjegyzés:** Az EIM beállítás sikeres befejezéséhez a tartományvezérlőként működő címtár szervernek aktívnek kell lennie.

- A **Tartományvezérlő neve** mezőben adja meg az használni kívánt EIM tartományhoz tartozó tartományvezérlőként szolgáló iSeries szerver nevét.
- Ha az EIM tartományvezérlő eléréséhez biztonságos kapcsolatot kíván használni, akkor engedélyezze a **Biztonságos kapcsolat használata (SSL vagy TLS)** lehetőséget. Ha ez a lehetőség engedélyezve van, akkor az Internethez hasonló megbízhatatlan hálózatokon keresztül létesített kapcsolatok esetén Védett socket réteg (SSL) vagy Szállítási réteg biztonság (TLS) biztosítja az EIM adatforgalmat.

**Megjegyzés:** Ellenőrizze, hogy az EIM tartományvezérlő fel van-e készítve biztonságos kapcsolat használatára. Ha nem, akkor a kapcsolódás nem fog sikerülni.

- A **Port** mezőben adja meg azt a TCP/IP portot, amelyiken a címtár szerver a kapcsolatokat fogadja. Ha a **Biztonságos kapcsolat használata** lehetőség be van kapcsolva, akkor az alapértelmezett portszám **636**; egyébként **389**.
- A **Kapcsolat ellenőrzése** gombbal ellenőrizze, hogy a varázsló a megadott információk felhasználásával valóban képes-e csatlakozni az EIM tartományvezérlőhöz.
- Kattintson a **Tovább** gombra.

7. A **Kapcsolati felhasználó meghatározása** lapon válasszon ki egy **Felhasználó típus** értéket a kapcsolathoz. A következő felhasználói típusok közül választhat: **Megkülönböztetett név és jelszó**, **Kerberos kulcscímke fájl és azonosító**, **Kerberos azonosító és jelszó**, vagy **Felhasználói profil 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:

**Megjegyzés:** Válassza a **Megkülönböztetett név és jelszó** felhasználótípust és felhasználónak adja meg az LDAP adminisztrátor megkülönböztetett nevét és jelszavát annak érdekében, hogy a varázslónak meglegyen a megfelelő jogosultsága a szükséges EIM objektumok létrehozására a címtárban.

Használhat más felhasználót is a kapcsolathoz, de a megadott felhasználónak az LDAP adminisztrátorral egyenértékű jogosultsággal kell rendelkeznie a távoli címtár szerverhez.

- 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 címtérében. 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 az LDAP adminisztrátor jelszavát.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
- A **Kerberos kulcs címke fájl és azonosító** választásakor adja meg a következőket:
  - A **Kulcs címke fájl** mezőben adja meg a varázsló által az EIM tartományhoz kapcsolódáshoz használt Kerberos azonosítót tartalmazó kulcs címke fájl teljes képzésű elérési útját és nevét. Vagy kattintson a **Tallózás...** gombra, és keresse meg a kulcs címke fájlt az iSeries rendszer integrált fájlrendszerén.
  - Az **Azonosító** mezőben adja meg a felhasználót azonosító Kerberos azonosító nevét.
  - A **Tartomány** mezőben adja meg annak a Kerberos tartománynak a teljes képzésű nevét, amelynek a fenti azonosító tagja. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcs címke fájlban szereplő Kerberos felhasználókat. A **hoszt.vallalat.hu** tartomány **jnap** felhasználóját például a kulcs címke fájlban a **jnap@beszreszl.sajatceg.com** képviseli.
- A **Kerberos azonosító és jelszó** választásakor adja meg a következőket:
  - Az **Azonosító** mezőben adja meg varázsló által az EIM tartományhoz kapcsolódáshoz használt Kerberos azonosítót.
  - A **Tartomány** mezőben adja meg annak a Kerberos tartománynak a teljes képzésű nevét, amelynek a fenti azonosító tagja. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcs címke fájlban szereplő Kerberos felhasználókat. A **hoszt.vallalat.hu** tartomány **jnap** felhasználóját például a kulcs címke fájlban a **jnap@beszreszl.sajatceg.com** képviseli.
  - A **Jelszó** mezőben adja meg a Kerberos azonosítóhoz tartozó jelszót.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
- A **Felhasználói profil és jelszó** választásakor adja meg a következőket:
  - Az **Felhasználói profil** mezőben adja meg varázsló által az EIM tartományhoz kapcsolódáshoz használt felhasználói profilt.
  - A **Jelszó** mezőben adja meg a felhasználói profilhoz tartozó jelszót.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
- A **Kapcsolat ellenőrzése** gombbal győződjön meg róla, hogy a varázsló a megadott felhasználói információk felhasználásával valóban képes-e csatlakozni az EIM tartományvezérlőhöz.
- Kattintson a **Tovább** gombra.

8. A **Tartomány meghatározása** lapon válassza ki a tartományt, amelyhez csatlakozni kíván, majd kattintson a **Tovább** gombra.

9. A **Nyilvántartás információk** lapon adja meg, hogy a helyi felhasználói nyilvántartásokat fel kell-e venni az EIM tartományba nyilvántartás meghatározásokként. A következő felhasználói nyilvántartási típusok közül választhat:

- Ha a helyi nyilvántartáshoz kíván nyilvántartás meghatározást létrehozni, akkor válassza ki a **Helyi OS/400** lehetőséget. Elfogadhatja a mezőben felkínált alapértelmezett nyilvántartás meghatározás nevet, vagy megadhat egy új értéket. Az EIM nyilvántartás neve tetszőleges karaktersorozat lehet, amely azonosítja a nyilvántartás típusát és az adott példányt.

**Megjegyzés:** Nem szükséges most létrehozni a helyi OS/400 nyilvántartás meghatározást. Ha úgy dönt, hogy később hozza létre az OS/400 nyilvántartás meghatározást, akkor fel kell vennie a rendszer nyilvántartás meghatározást és frissítenie kell az EIM konfigurációs tulajdonságait.

- Ha Kerberos nyilvántartáshoz kíván nyilvántartás meghatározást létrehozni, akkor válassza ki a **Kerberos** lehetőséget. Elfogadhatja a mezőben felkínált alapértelmezett nyilvántartás meghatározás nevét, vagy megadhat egy új értéket. Az alapértelmezett definíció név megegyezik a Kerberos tartománynévvel. Ha elfogadja az alapértéket, és a Kerberos nyilvántartás nevét használja tartománynévként, akkor javíthatja a nyilvántartásban tárolt információk visszakeresésének teljesítményét. Szükség szerint válassza ki a **Kerberos felhasználói azonosságok kis- és nagybetű érzékenyek** lehetőséget.

**Megjegyzés:** Ha az EIM konfigurációs varázsló segítségével egy másik rendszeren már felvett egy nyilvántartás meghatározást ahhoz a Kerberos nyilvántartáshoz, amelyhez ennek az iSeries rendszernek van szerviz azonosítója, akkor nem szükséges Kerberos nyilvántartás meghatározást felvenni ennek a konfigurációnak a részeként. Azonban a rendszer konfigurációs tulajdonságai között meg kell adnia ennek a Kerberos nyilvántartásnak a nevét a varázsló befejezése után.

- Kattintson a **Tovább** gombra.

10. Az **EIM rendszer felhasználó meghatározása** lapon a **Felhasználó típus** mezőben válassza ki, hogy milyen típusú felhasználót használjon a rendszer az operációs rendszer funkciók nevében végzett EIM műveleteknél. Ilyen művelet például a leképezés kikeresésének művelete 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 ténylegesen kiválasztható felhasználó típusok függenek az aktuális rendszerkonfigurációtól. Ha például a Hálózati hitelesítési szolgáltatás nincs beállítva a rendszeren, akkor a Kerberos felhasználói típusok nem állnak rendelkezésre. A megadott felhasználótípus határozza meg a lapon megadandó további információkat az alábbiak szerint:

**Megjegyzés:** Meg kell adnia egy az EIM tartományvezérlőt kiszolgáló címtár szerveren már létező felhasználót. 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 egyszerű bejelentkezéssel és a felhasználói profilok törlésével kapcsolatos operációs rendszer funkciók meghiúsulhatnak.

- A **Megkülönböztetett név és jelszó** választásakor adja meg a következőket:
  - A **Megkülönböztetett név** mezőben adja meg a rendszer által az EIM műveletek végrehajtásához használt felhasználót azonosító LDAP megkülönböztetett nevet.
  - A **Jelszó** mezőben adja meg az LDAP adminisztrátor jelszavát.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
- A **Kerberos azonosító és jelszó** választásakor adja meg a következőket:
  - Az **Azonosító** mezőben adja meg rendszer által az EIM műveletek végrehajtásához használt Kerberos azonosítót.
  - A **Tartomány** mezőben adja meg annak a Kerberos tartománynak a teljes képzésű nevét, amelynek a fenti azonosító tagja. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcscímke fájlban szereplő Kerberos felhasználókat. A `hoszt.vallalat.hu` tartomány `jnap` felhasználóját például a kulcscímke fájlban a `jnap@beszreszl.sajatceg.com` képviseli.
  - A **Jelszó** mezőben adja meg a felhasználó jelszavát.
  - A **Jelszó megerősítése** mezőben ellenőrzési céllal adja meg ismét a jelszót.
- A **Kerberos kulcscímke fájl és azonosító** választásakor adja meg a következőket:
  - A **Kulcscímke fájl** mezőben adja meg a rendszer által az EIM műveletek végrehajtásához használt Kerberos azonosítót tartalmazó kulcscímke fájl teljes képzésű elérési útját és nevét. Vagy kattintson a **Tallózás...** gombra, és keresse meg a kulcscímke fájlt az iSeries rendszer integrált fájlrendszerén.
  - Az **Azonosító** mezőben adja meg rendszer által az EIM műveletek végrehajtásához használt Kerberos azonosítót.
  - A **Tartomány** mezőben adja meg annak a Kerberos tartománynak a teljes képzésű nevét, amelynek a fenti azonosító tagja. Az azonosító és a tartomány neve határozza meg egyedi módon a kulcscímke fájlban szereplő Kerberos felhasználókat. A `hoszt.vallalat.hu` tartomány `jnap` felhasználóját például a kulcscímke fájlban a `jnap@beszreszl.sajatceg.com` képviseli.

- A **Kapcsolat ellenőrzése** gombbal győződjön meg róla, hogy a varázsló a megadott felhasználói információk felhasználásával valóban képes-e csatlakozni az EIM tartományvezérlőhöz.
- Kattintson a **Tovább** gombra.

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

Amikor a varázsló befejeződik, hozzáadja a tartományt a **Tartománykezelés** mappához, és a szerveren létrejött egy alapszintű EIM konfiguráció. A tartomány EIM konfigurációjának véglegesítéséhez azonban még el kell végeznie a következő feladatokat is:

1. Szükség szerint adja hozzá a tartományba bevonni kívánt nem iSeries szerverek és alkalmazások nyilvántartás meghatározásait az EIM tartományhoz. Ezek a nyilvántartás meghatározások a tartományban szereplő felhasználói nyilvántartásokra hivatkoznak. Az EIM megvalósítástól függően lehetséges rendszer nyilvántartás meghatározások felvétele vagy alkalmazás nyilvántartás meghatározások hozzáadása.

2. Az EIM megvalósítás függvényében döntsön arról, hogy:

- EIM azonosítók létrehozása és azonosító társítások elkészítése szükséges minden egyes egyedi felhasználó vagy entitás számára a tartományban.
- Irányelv társítások létrehozása szükséges a felhasználók csoportjainak leképezéséhez egyetlen cél felhasználói azonosságra.
- A fentiek kombinációjára van szükség.

3. A leképezés tesztelése EIM funkció segítségével ellenőrizze az EIM konfiguráció azonosság leképezéseit.

4. Ha az egyetlen beállított EIM felhasználó az LDAP adminisztrátor megkülönböztetett neve, akkor az aktuális EIM felhasználó magas szintű hozzáféréssel rendelkezik a címtár szerver adataihoz. Ezért érdemes megfontolni még legalább egy DN létrehozását, amely megfelelő, korlátozott hozzáférés felügyelettel rendelkezik az EIM adatok fölött. A megkülönböztetett nevek létrehozásáról bővebb információkat a Megkülönböztetett nevek témakörben talál az IBM Directory Server for iSeries (LDAP) dokumentációjában. A meghatározandó további EIM felhasználók száma attól függ, hogy a rendszer biztonsági stratégiája mekkora hangsúlyt fektet a biztonsági feladatok és felelőségek elkülönítésére. Általában célszerű létrehozni legalább az alábbi két DN típust:

• **EIM adminisztratori hozzáférés felügyelettel rendelkező felhasználó**

Ez az EIM adminisztratori DN biztosítja a megfelelő szintű jogosultságot az EIM tartomány kezeléséért felelős adminisztrátorok számára. Ezt az EIM adminisztratori megkülönböztetett nevet olyan esetekben lehet használni, amikor az EIM tartomány összes jellemzőjének kezelésére szükség lehet, például amikor az iSeries navigátor kapcsolódik a tartományvezérlőhöz.

• **Legalább egy felhasználó, aki rendelkezik az alábbi hozzáférés felügyelettel:**

- Azonosító adminisztrátor
- Nyilvántartás adminisztrátor
- EIM leképezés műveletek

Ez a felhasználó biztosítja a megfelelő szintű hozzáférés felügyeletet az operációs rendszer nevében EIM műveleteket végrehajtó rendszerfelhasználó számára.

**Megjegyzés:** Ahhoz, hogy ezt az új megkülönböztetett nevet használja a rendszerfelhasználó az LDAP adminisztratori DN helyett, változtassa meg az iSeries szerver EIM konfigurációs tulajdonságait. A rendszerfelhasználó által használt DN megváltoztatásával kapcsolatban lásd az EIM konfigurációs tulajdonságok kezelése témakört.

**Megjegyzés:** Ha alapszintű hálózati hitelesítési szolgáltatás konfigurációt is létrehozott, akkor további feladatokat is el kell végeznie, különösen egyszeri bejelentkezés környezet megvalósítása esetén. Ezekről a további lépésekről bővebb információkat talál a teljes konfigurációs folyamatot példahelyzetben keresztül bemutató Az OS/400 felkészítése egyszeri bejelentkezésre dokumentumban.

## Biztonságos kapcsolat kialakítása az EIM tartományvezérlővel

Az EIM adatok átvitelének biztosítása érdekében szükség esetén beállíthatja a tartományvezérlő biztonságos kapcsolatát a Védett socket réteg (SSL) vagy Szállítási réteg biztonság (TLS) protokollokkal.

Az EIM SSL/TLS támogatásának beállításához tegye a következőket:

1. A Digitális igazolás kezelő (DCM) segítségével hozza létre az igazolást, amely a címtár szervernek az SSL használatához szükséges.
2. Engedélyezze az SSL használatát az EIM tartományvezérlőt kiszolgáló helyi címtár szervernek.
3. Frissítse az EIM konfiguráció tulajdonságait, és adja meg, hogy az iSeries szerver SSL kapcsolatot használ.

Az EIM konfiguráció tulajdonságok frissítéséhez tegye a következőket:

- a. Az iSeries navigátorban válassza ki azt a rendszert, amelyhez beállította az EIM szolgáltatást, és bontsa ki a **Hálózat > Vállalati azonosság leképezés** elemet.
  - b. Kattintson a jobb egérgombbal a **Konfiguráció** elemre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
  - c. A **Tartomány** lapon kapcsolja be a **Biztonságos kapcsolat (SSL vagy TLS) használata**, adja meg a címtár szerver által használt biztonságos portot, vagy fogadja el a **Port** mezőben található alapértelmezett **636** értéket, majd kattintson az **OK** gombra.
4. Frissítse az EIM tartomány tulajdonságait minden EIM tartománynál, és adja meg, hogy az EIM SSL kapcsolatot használ a tartománynak az iSeries navigátorból végzett kezeléséhez.

Az EIM tartomány tulajdonságainak frissítéséhez tegye a következőket:

- a. Az iSeries navigátorban válassza ki azt a rendszert, amelyhez beállította az EIM szolgáltatást, és bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
- b. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg az EIM tartomány hozzáadása a Tartománykezelés mappához című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.
- c. Kattintson a jobb egérgombbal a tesztelni kívánt EIM tartományra, majd válassza az előugró menü **Tulajdonságok** menüpontját.
- d. A **Tartomány** lapon kapcsolja be a **Biztonságos kapcsolat (SSL vagy TLS) használata**, adja meg a címtár szerver által használt biztonságos portot, vagy fogadja el a **Port** mezőben található alapértelmezett **636** értéket, majd kattintson az **OK** gombra.

---

## Vállalati azonosság leképezés (EIM) kezelése

Miután beállította a Vállalati azonosság leképezést az iSeries szerveren, az idők során számos adminisztratív feladatot kell elvégeznie az EIM tartomány és az adatok karbantartásához. Az EIM kezelésével kapcsolatban olvassa el az alábbi fejezeteket.

“**Vállalati azonosság leképezés (EIM) tartományok kezelése**” oldalszám: **80** Ismerje meg az EIM tartományok és tulajdonságaik kezelésének módját.

“**Vállalati azonosság leképezés nyilvántartás meghatározások kezelése**” oldalszám: **84** Ismerje meg, hogyan kell létrehozni és kezelni az EIM tartományban részvevő felhasználói nyilvántartásokhoz tartozó EIM nyilvántartás meghatározásokat.

“**Vállalati azonosság leképezés (EIM) azonosítók kezelése**” oldalszám: **90** Tanulja meg, hogyan kell létrehozni az EIM azonosítókat.

“**Társítások kezelése**” oldalszám: **93** Ismerkedjen meg az azonosító társítások és irányelv társítások létrehozásának és törlésének módjával, illetve a társításokra vonatkozó egyéb információk tulajdonságainak kezelésével a tartományban.

“EIM konfigurációs tulajdonságok kezelése” oldalszám: 109 Ismerje meg, hogyan kezelheti az EIM konfigurációt a rendszeren, beleértve a rendszer felhasználót és egyéb tulajdonságokat.

“EIM hozzáférés felügyelet kezelése” oldalszám: 108 Ismerje meg, hogy szabályozhatja az EIM adatok elérését illetve az EIM adminisztrációs és más feladatok végrehajtását a felhasználói hozzáférés felügyeleti csoportok kezelésével.

## Vállalati azonosság leképezés (EIM) tartományok kezelése

Az iSeries navigátor segítségével az összes Vállalati azonosság leképezés (EIM) tartományt kezelheti. Ahhoz, hogy egy tartomány kezelhető legyen, szerepelnie kell az iSeries navigátor **Hálózat** kategóriájában található **Tartománykezelés** mappában. Amikor az EIM konfigurációs varázsló segítségével létrehoz és konfigurál egy új tartományt, akkor az automatikusan bekerül a **Tartománykezelés** mappába, így kezelheti a tartományt és a benne található információkat.

Az iSeries rendszeren található bármely azonos hálózaton található kapcsolatot felhasználhatja az EIM tartomány kezelésére még akkor is, ha maga az iSeries rendszer nem tagja a tartománynak.

Az alábbi tartománykezelési feladatokat hajthatja végre:

- “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához”
- “Csatlakozás egy Vállalati azonosság leképezés (EIM) tartományhoz” oldalszám: 81
- “Írányelv társítások engedélyezése a tartományban” oldalszám: 81
- “EIM leképezések tesztelése” oldalszám: 82
- “Vállalati azonosság leképezés (EIM) tartomány eltávolítása a Tartománykezelés mappából” oldalszám: 84
- “Vállalati azonosság leképezés (EIM) tartomány és az összes konfigurációs objektum törlése” oldalszám: 84

Ezen kívül kezelheti a felhasználók hozzáférését a tartományhoz és a benne található információkhoz az alábbiak szerint:

- “EIM hozzáférés felügyelet kezelése” oldalszám: 108
- “Vállalati azonosság leképezés nyilvántartás meghatározások kezelése” oldalszám: 84
- “Társítások kezelése” oldalszám: 93
- “Vállalati azonosság leképezés (EIM) azonosítók kezelése” oldalszám: 90

## Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához

Csak létező tartományt lehet hozzáadni a **Tartománykezelés** mappához, továbbá a feladat végrehajtásához \*SECADM különleges jogosultság szükséges.

Egy Vállalati azonosság leképezés (EIM) tartomány felvételéhez a **Tartománykezelés** mappába tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés** elemet.
2. Kattintson a jobb egérgombbal a **Tartománykezelés** elemre, majd válassza az előugró menü **Tartomány hozzáadása...** menüpontját.
3. A **Tartomány hozzáadása** párbeszédablakon adja meg a szükséges tartomány- és kapcsolat információkat. Vagy kattintson **Keresés...** gombbal jelenítse meg a megadott tartományvezérlő által kezelt tartományok listáját.

**Megjegyzés:** Ha a **Keresés...** gombra kattint, akkor megjelenik a **Csatlakozás egy EIM tartományvezérlőhöz** párbeszédablak. A tartományok listájának megjelenítéséhez LDAP adminisztrátor vagy EIM adminisztrátor hozzáférés felügyelettel kell kapcsolódnia a tartományvezérlőhöz. A tartománylista tartalmát befolyásolja a felhasználó EIM hozzáférés felügyelete. Ha LDAP adminisztrátor hozzáférés felügyelettel rendelkezik, akkor a tartományvezérlő által kezelt összes tartomány megjelenik. Egyébként csak azok jelennek meg a listában, amelyekhez EIM adminisztrátor hozzáférés felügyelettel rendelkezik.

4. Amennyiben segítségre szorul a mezők jelentésével kapcsolatban, kattintson a **Súgó** gombra.
5. A tartomány felvételéhez kattintson az **OK** gombra.

## Csatlakozás egy Vállalati azonosság leképezés (EIM) tartományhoz

Mielőtt használatba vehetné a Vállalati azonosság leképezés (EIM) tartományt, először csatlakoznia kell az EIM tartományvezérlőhöz. EIM tartományhoz akkor is csatlakozhat, ha az iSeries szerver jelenleg nincs beállítva a tartomány tagjaként.

A csatlakozáshoz az EIM tartományvezérlőhöz a kapcsolatot létesítő felhasználónak egy tagnak kell lennie egy "EIM hozzáférés felügyelet" oldalszám: 34 csoportban. A felhasználó EIM hozzáférés felügyeleti csoporttagsága határozza meg azt, hogy milyen feladatokat hajthat végre a tartományban, és milyen EIM adatokat jeleníthet meg illetve módosíthat.

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

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Kattintson a jobb egérgombbal arra a tartományra, amelyhez csatlakozni kíván.

**Megjegyzés:** Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor járjon el a "Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához" oldalszám: 80 résznél leírtak alapján.

3. Kattintson a jobb egérgombbal az EIM tartományra, amelyhez csatlakozni kíván, majd válassza az előugró menü **Csatlakozás...** menüpontját.
4. A **Csatlakozás az EIM tartományvezérlőhöz** párbeszédablakon töltsé ki a **Felhasználó típusa** mezőt, adja meg a szükséges azonosítási adatokat a felhasználóhoz, majd válasszon egy jelszó lehetőséget a csatlakozáshoz.
5. Amennyiben segítségre szorul a párbeszédablak mezőinek jelentésével kapcsolatban, kattintson a **Súgó** gombra.
6. Az **OK** gombbal csatlakozzon a tartományvezérlőhöz.

## Irányelv társítások engedélyezése a tartományban

Az irányelv társítások segítségével N-1 leképezéseket hozhatunk létre olyan esetekre, amikor nem létezik társítás a felhasználói azonosságok és egy EIM azonosító között. Az irányelv társítás egyetlen felhasználói azonosság helyett több felhasználói azonosságot rendel egyetlen felhasználói azonossághoz egy megadott felhasználói nyilvántartásban. Mielőtt azonban elkezdené használni az irányelv társításokat, biztosítania kell, hogy a tartományban engedélyezett legyen a használatuk a leképezés kikeresési műveletek során.

Ha engedélyezni szeretné a cél nyilvántartásban az irányelv társítások használatát a leképezés kikeresések támogatás számára a tartományban, akkor csatlakoznia kell a megfelelő EIM tartományhoz, és EIM adminisztrátor hozzáférés felügyelettel kell rendelkeznie.

Amennyiben engedélyezni kívánja a tartományban a leképezés kikeresési támogatás az irányelv társítások használatát, akkor tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Kattintson a jobb egérgombbal a használni kívánt EIM tartományra, majd válassza az előugró menü **Leképezés irányelv...** menüpontját.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a "Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához" oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a **Csatlakozás az EIM tartományvezérlőhöz** című témakörben. (A **Leképezés irányelv...** lehetőség egészen addig tiltott, amíg nem sikerül csatlakozni a tartományhoz.)
3. Az **Általános** lapon válassza ki az **Irányelv társítást használó leképezés kikeresések engedélyezése a tartományban** beállítást.
4. Kattintson az **OK** gombra.

**Megjegyzés:** Engedélyezze a leképezés kikereséseket és az irányelv társítások használatát minden olyan cél nyilvántartás meghatározás számára, amelyhez irányelv társítás van megadva. Ha nincs engedélyezve a leképezés kikeresés a cél nyilvántartás meghatározás számára, akkor az nem vehet részt az EIM

leképezés kikeresési műveletekben. Ha nem engedélyezi a cél nyilvántartás számára az irányelv társítások használatát, akkor az EIM leképezés kikeresési műveletek figyelmen kívül hagyják a nyilvántartáshoz megadott irányelv társításokat.

## EIM leképezések tesztelése

Az EIM leképezés tesztelési támogatás lehetővé teszi EIM leképezés kikeresési műveletek végrehajtását az EIM konfiguráción. A teszttel ellenőrizheti, hogy egy adott forrás felhasználói azonosság megfelelően leképeződik-e a cél felhasználói azonosságra. Ezzel a módszerrel ellenőrizhető, hogy az EIM kikeresési műveletek képesek-e megtalálni a helyes cél felhasználói azonosságot a megadott információk alapján.

A leképezés tesztelése funkció használatához csatlakoznia kell a kívánt EIM tartományhoz, továbbá szüksége van az alábbi EIM hozzáférés felügyelet szintek egyikére:

- EIM adminisztrátor
- Azonosító adminisztrátor
- Nyilvántartás adminisztrátor
- EIM leképezés kikeresési műveletek

Az EIM konfiguráció leképezés teszteléséhez tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg az EIM tartomány hozzáadása a Tartománykezelés mappához című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.
3. Kattintson a jobb egérgombbal a tesztelni kívánt EIM tartományra, majd válassza az előugró menü **Leképezés tesztelése...** menüpontját.
4. A **leképezés tesztelése** párbeszédablakon adja meg az alábbi információkat:
  - A **Forrás nyilvántartás** mezőben adja meg a teszt leképezés kikeresési művelet során forrásként használni kívánt felhasználói nyilvántartásra vonatkozó nyilvántartás meghatározás nevét.
  - A **forrás felhasználó** mezőben adja meg a leképezés kikeresési művelet forrás felhasználói azonosságát.
  - A **Cél nyilvántartás** mezőben adja meg a teszt leképezés kikeresési művelet céljaként használni kívánt felhasználói nyilvántartásra vonatkozó nyilvántartás meghatározás nevét.
  - Választható. A **Kikeresési információk** mezőben adja meg a cél felhasználóra vonatkozó esetleges kikeresési információkat.
5. Ha a párbeszédablak mezőivel kapcsolatban további segítségre van szüksége, akkor kattintson a **Súgó** gombra.
6. Kattintson a **Teszt** gombra, és tekintse át a leképezés kikeresési művelet eredményét.
7. Folytassa a konfiguráció tesztelését, vagy lépjen ki a **Bezár** gombbal.

## Teszteredmények kezelése és a problémák megoldása

A teszt akkor ad vissza egy cél felhasználói azonosságot, ha talál társítást az adminisztrátor által megadott cél felhasználói nyilvántartás és forrás felhasználói azonosság között. Siker esetén a teszt a megtalált társítás típusát is jelzi. Ha a teszt nem talál társítást a megadott információk alapján, akkor a visszaadott cél felhasználói azonosság helyett a **nincs** értékkel tér vissza.

A teszt az összes többi EIM leképezés kikeresési művelethez hasonlóan az alábbi sorrend szerint hajtja végre a cél felhasználói azonosság keresését:

1. Adott azonosító társítás
2. Igazolásszűrő irányelv társítás
3. Alapértelmezett nyilvántartás irányelv társítás



#### 4. Alapértelmezett tartomány irányelv társítás

Bizonyos esetekben a teszt nem ad vissza cél felhasználói azonosságot annak ellenére, hogy a tartományhoz be vannak állítva a megfelelő társítások. Győződjön meg arról, hogy helyes információkat használt a teszt során. Ha az helyes, és a teszt nem ad vissza eredményt, akkor a hiba az alábbi okok egyikéből fakad:

- Az irányelv társítás támogatás nincs engedélyezve tartományi szinten. Engedélyezze az irányelv társítást a tartományban.
- A leképezés kikeresési műveletek támogatása vagy az irányelv társítás támogatás nem engedélyezett az egyedi nyilvántartás szinten. Engedélyezze a leképezés keresés támogatást és az irányelv társítás használatát a cél nyilvántartás számára.
- Egy EIM azonosító forrás vagy cél társítása nincs helyesen beállítva. Például nincs forrás társítás a Kerberos azonosítóhoz (vagy Windows felhasználóhoz), vagy létezik a társítás, de helytelen. Egy másik lehetőség, hogy a cél társítás helytelen felhasználói azonosságot határoz meg. Jelenítse meg az EIM azonosítóhoz tartozó összes azonosító társítást, és ellenőrizze az adott azonosítóhoz tartozó társításokat.
- Egy irányelv társítás beállítása helytelen. Jelenítse meg a tartomány összes irányelv társítását, és ellenőrizze a az összes beállított irányelv társításhoz tartozó forrás és cél információkat.
- A nyilvántartás meghatározások és a felhasználói azonosságok nem egyeznek meg a kis- és nagybetűk megkülönböztetése miatt. Törölheti és a megfelelő kis- vagy nagybetűs írásmóddal újra létrehozhatja a nyilvántartást vagy a társítást.

Más esetekben a teszt kétértelmű eredménnyel érhet véget. Ezt egy hibaüzenet jelzi. A teszt akkor ér véget kétértelmű eredménnyel, ha egynél több felhasználói azonosság felel meg a megadott feltételeknek. Egy leképezés kikeresési művelet akkor talál egynél több cél felhasználói azonosságot, ha az alábbi körülmények közül legalább egy fennáll:

- Egy EIM azonosítóhoz több külön cél társítás tartozik ugyanabban a cél nyilvántartásban.
- Egynél több EIM azonosítónál szerepel forrás társításként ugyanaz a felhasználói azonosság, és noha a cél társításként megadott felhasználói azonosság különbözhet, a cél nyilvántartás szintén megegyezik.
- Egynél több alapértelmezett tartomány irányelv társítás határozza meg ugyanazt a cél nyilvántartást.
- Egynél több alapértelmezett nyilvántartás irányelv társítás határozza meg ugyanazt a forrás nyilvántartást és cél nyilvántartást.
- Egynél több igazolásszűrő irányelv társítás határozza meg ugyanazt az X.509 nyilvántartást, igazolásszűrőt és cél nyilvántartást.

Az egynél több cél felhasználói azonosságot eredményező leképezés kikeresési műveletek problémákat okozhatnak az EIM támogatással rendelkező alkalmazások működésében, beleértve az olyan OS/400 alkalmazásokat és termékeket is. Ezért meg kell találni a kétértelmű eredmény okát, és a helyzet megoldásához szükséges lépéseket. Az probléma okától függően az alábbi lépések segíthetnek a megoldásban:

- A teszt leképezés nem kívánatos többszörös cél azonosságokat eredményez. Ez azt jelzi, hogy a tartomány társítás konfigurációja helytelen, amit az alábbiak okozhatnak:
  - Egy EIM azonosító forrás vagy cél társítása nincs helyesen beállítva. Például nincs forrás társítás a Kerberos azonosítóhoz (vagy Windows felhasználóhoz), vagy létezik a társítás, de helytelen. Egy másik lehetőség, hogy a cél társítás helytelen felhasználói azonosságot határoz meg. Jelenítse meg az EIM azonosítóhoz tartozó összes azonosító társítást, és ellenőrizze az adott azonosítóhoz tartozó társításokat.
  - Egy irányelv társítás beállítása helytelen. Jelenítse meg a tartomány összes irányelv társítását, és ellenőrizze a az összes beállított irányelv társításhoz tartozó forrás és cél információkat.
- Ha a teszt több cél felhasználói azonosságot ad eredményül, és ezek megfelelnek a beállított társításoknak, akkor kikeresési információk megadására van szükség a cél felhasználói azonosságokhoz. A közös forrással (ami lehet EIM azonosító az azonosító társítások esetén vagy forrás felhasználói nyilvántartás az irányelv társítások esetén) rendelkező cél felhasználói azonosságokhoz egyedi kikeresési információkat kell megadni. A kikeresési információk megadásával biztosíthatja, hogy a kikeresési művelet az összes lehetséges cél felhasználói azonosság helyett egyetlen azonosságot eredményezzen. Bővebb információkat a Cél felhasználói azonosság kiegészítése keresési információkkal részben talál. A kikeresési művelet során meg kell adni a kikeresési információkat.

l **Megjegyzés:** Ez a megközelítés csak akkor működik, ha az alkalmazás számára engedélyezett a keresési  
l információk használata. Azonban az alap OS/400 alkalmazások, mint például az iSeries Access for  
l Windows nem használhatják a keresési információkat arra, hogy különbséget tegyenek egy kikeresési  
l művelet több eredménye között. Ebből következően érdemes megfontolni a tartomány társításainak  
l átdefiniálását annak érdekében, hogy a leképezés kikeresési műveletek egyetlen eredménnyel térjenek  
l vissza, és így az alap OS/400 alkalmazások is képesek legyenek kikeresési műveletek végrehajtására  
l és azonosságok leképezésére.

l Az itt leírtakon kívül további lehetséges leképezési problémák és megoldásuk leírását itt találja: “Vállalati azonosság  
l leképezés (EIM) hibaelhárítás: leképezési hibák” oldalszám: 114.

## Vállalati azonosság leképezés (EIM) tartomány eltávolítása a Tartománykezelés mappából

l Amennyiben egy EIM tartományra már nincs szüksége, akkor eltávolíthatja a **Tartománykezelés** mappából. Azonban  
l a tartomány eltávolítása a **Tartománykezelés** mappából **nem** ugyanaz, mintha kitörölné a tartományt, és a  
l tartományadatok nem törlődnek a tartományvezérlőről. Ha a tartományt valójában törölni kívánja az összes adatával  
l együtt, akkor olvassa el a tartomány törlése részt.

l Egy tartomány eltávolításához semmilyen “EIM hozzáférés felügyelet” oldalszám: 34 nem szükséges.

Egy EIM tartomány eltávolításához a **Tartománykezelés** mappából tegye a következőket:

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

## Vállalati azonosság leképezés (EIM) tartomány és az összes konfigurációs objektum törlése

l Egy EIM tartomány törlése előtt az összes nyilvántartás meghatározást és Vállalati azonosság leképezés (EIM)  
l azonosítót törölni kell a tartományból. Ha már nincs szüksége a tartományra, de nem kívánja törölni a benne található  
l adatokkal együtt, akkor inkább távolítsa el a tartományt.

l A tartomány törléséhez szüksége van az alábbi “EIM hozzáférés felügyelet” oldalszám: 34 szintek egyikére:

- l • LDAP adminisztrátor.
- l • EIM adminisztrátor.

EIM tartomány törléséhez tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Ha szükséges, törölje az összes nyilvántartás meghatározást az EIM tartományból.
3. Szükség esetén törölje az összes EIM azonosítót az EIM tartományból.
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.

## Vállalati azonosság leképezés nyilvántartás meghatározások kezelése

l A felhasználói nyilvántartásokat és a bennük található felhasználói azonosságokat nyilvántartás meghatározások  
l segítségével vonhatja be a Vállalati azonosság leképezés (EIM) tartományba. Az EIM nyilvántartás meghatározások  
l segítségével befolyásolhatja azt, hogy a felhasználói nyilvántartások és a bennük található felhasználói azonosságok  
l hogyan vegyenek rész a Vállalati azonosság leképezésben.

Az alábbi nyilvántartás meghatározás kezelési feladatokat hajthatja végre:

- l • “Rendszernyilvántartás meghatározás hozzáadása” oldalszám: 85

- | • “Alkalmazásnyilvántartás meghatározás hozzáadása”
- | • “Álnév hozzáadása nyilvántartás meghatározáshoz” oldalszám: 86
- | • “Saját felhasználói nyilvántartás meghatározása a Vállalati azonosság leképezésben (EIM)” oldalszám: 87
- | • “Leképezés kikeresések és irányelv társítások használatának engedélyezése egy cél nyilvántartásban.” oldalszám: 88
- | • “Nyilvántartás meghatározáshoz tartozó összes irányelv társítás megjelenítése” oldalszám: 106
- | • “nyilvántartás meghatározás álnevének eltávolítása” oldalszám: 90
- | • “Nyilvántartás meghatározás törlése” oldalszám: 89

| Az alábbi kapcsolódó feladatok segítségével lehetnek a nyilvántartás meghatározásokat befolyásoló EIM adatok kezelésében:

- | • “Irányelv társítás létrehozása” oldalszám: 95
- | • “Irányelv társítás törlése” oldalszám: 107

## Rendszernyilvántartás meghatározás hozzáadása

| Rendszer nyilvántartás meghatározás létrehozásához csatlakoznia kell a megfelelő EIM tartományhoz, és EIM adminisztrátor hozzáférés felügyelettel kell rendelkeznie.

Ha a rendszer nyilvántartást szeretne egy EIM tartományhoz hozzáadni, akkor tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a “Csatlakozás egy Vállalati azonosság leképezés (EIM) tartományhoz” oldalszám: 81 című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson a jobb egérgombbal a **Felhasználói nyilvántartások** elemre, majd válassza a **Nyilvántartás hozzáadása**, majd az **Rendszer...** lehetőséget.
5. A **Rendszer nyilvántartás hozzáadása** párbeszédablakon adja meg a rendszer nyilvántartás meghatározásra vonatkozó információkat az alábbiak szerint:
  - A rendszer nyilvántartás meghatározás neve.
  - A nyilvántartás meghatározás típusa.
  - A rendszer nyilvántartás meghatározás leírása.
  - (Választható.) A felhasználói nyilvántartás URL címe.
  - Szükség esetén a rendszer nyilvántartás meghatározáshoz tartozó egy vagy több álnév.
6. Amennyiben segítségre szorul a mezők jelentésével kapcsolatban, kattintson a **Súgó** gombra.
7. Kattintson az **OK** gombra az információk mentéséhez és a nyilvántartás felvételéhez az EIM tartományba.

## Alkalmazásnyilvántartás meghatározás hozzáadása

| Alkalmazás nyilvántartás meghatározás létrehozásához csatlakoznia kell a megfelelő EIM tartományhoz, és EIM adminisztrátor hozzáférés felügyelettel kell rendelkeznie.

| Ha alkalmazás nyilvántartást szeretne egy EIM tartományhoz hozzáadni, akkor tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a “Csatlakozás egy Vállalati azonosság leképezés (EIM) tartományhoz” oldalszám: 81 című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.

4. Kattintson a jobb egérgombbal a **Felhasználói nyilvántartások** elemre, majd válassza a **Nyilvántartás hozzáadása**, majd az **Alkalmazás...** lehetőséget.
5. Az **Alkalmazás nyilvántartás hozzáadása** párbeszédablakon adja meg az alkalmazás nyilvántartás meghatározásra vonatkozó információkat az alábbiak szerint:
  - Az alkalmazás nyilvántartás meghatározás neve.
  - Annak a rendszer nyilvántartás meghatározásnak a neve, amelynek a megadott alkalmazás felhasználói nyilvántartás részhalmaza. A megadott rendszer nyilvántartás meghatározásnak már létezni kell az EIM tartományban, különben az alkalmazás nyilvántartás meghatározás létrehozása meghiúsul.
  - A nyilvántartás meghatározás típusa.
  - Az alkalmazás nyilvántartás meghatározás leírása.
  - Szükség esetén az alkalmazás nyilvántartás meghatározáshoz tartozó egy vagy több álnév.
6. Amennyiben segítségre szorul a mezők jelentésével kapcsolatban, kattintson a **Súgó** gombra.
7. Kattintson az **OK** gombra az információk mentéséhez és a nyilvántartás felvételéhez az EIM tartományba.

### Álnév hozzáadása nyilvántartás meghatározáshoz

Elképzelhető, hogy egy alkalmazásfejlesztő további megkülönböztető információkat szeretne megadni egy nyilvántartás meghatározáshoz. Ezt úgy teheti meg, ha álnevet hoz létre a nyilvántartás meghatározás számára. A nyilvántartás meghatározás álnevek segítségével jobban elkülöníthetők egymástól a felhasználói nyilvántartások.

Az álnév támogatás segítségével a programozók úgy is megírhatnak alkalmazásokat, hogy előzőleg ne kelljen ismerniük az alkalmazást bevezető adminisztrátor által alkalmazott EIM nyilvántartás meghatározás neveket. 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.

Ha egy álnevet kíván hozzáadni egy nyilvántartás meghatározáshoz, akkor csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi "EIM hozzáférés felügyelet" oldalszám: 34 szintek egyikére:

- Nyilvántartás adminisztrátor.
- Kijelölt nyilvántartások adminisztrátora (a módosítani kívánt nyilvántartás)
- EIM adminisztrátor

Ha egy EIM nyilvántartás meghatározáshoz álnevet kíván hozzáadni, akkor tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg a "Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához" oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a "Csatlakozás egy Vállalati azonosság leképezés (EIM) tartományhoz" oldalszám: 81 című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson a **Felhasználói nyilvántartások** elemre a tartományban lévő nyilvántartás meghatározások listájának megjelenítéséhez.

**Megjegyzés:** Ha Kijelölt nyilvántartások adminisztrátora hozzáférés felügyelettel rendelkező felhasználó végzi a műveletet, akkor ez a lista csak azokat a nyilvántartás meghatározásokat tartalmazza, amelyeknek a kezelésére a felhasználó jogosult.

5. Kattintson a jobb egérgombbal arra a nyilvántartás meghatározásra, amelyhez a törölni kívánt álnév tartozik, majd válassza az előugró menü **Tulajdonságok...** menüpontját.
6. Válassza ki az **Álnevek** lapot és adja meg a felvenni kívánt álnév nevét és típusát.

**Megjegyzés:** Olyan álnév típust is meghatározhat, amely nem szerepel a típusok listáján.

7. Amennyiben segítségre szorul a mezők jelentésével kapcsolatban, kattintson a **Súgó** gombra.

8. Kattintson a **Hozzáadás** gombra.
9. Kattintson az **OK** gombra a nyilvántartás meghatározás változásainak elmentéséhez.

## Saját felhasználói nyilvántartás meghatározása a Vállalati azonosság leképezésben (EIM)

- | Egy Vállalati azonosság leképezés (EIM) nyilvántartás meghatározás létrehozása során kiválaszthatja az előre megadott felhasználói azonosság típusok közül azt, amelyik vállalat egyik rendszerén létező aktuális felhasználói nyilvántartást képviseli. Noha az előre meghatározott nyilvántartás meghatározás típusok a legtöbb operációs rendszer felhasználói nyilvántartását lefedik, elképzelhető, hogy olyan nyilvántartás meghatározást kell létrehozni, amelyhez az EIM nem tartalmaz előre meghatározott nyilvántartás típust. Ebben az esetben két választási lehetőség áll rendelkezésre.
- | Használhat egy a kívánt felhasználói nyilvántartás jellemzőinek megfelelő létező nyilvántartás meghatározást vagy létrehozhat saját felhasználói nyilvántartás típust.

Ha olyan felhasználói nyilvántartást kíván meghatározni, amelyet az EIM alapértelmezésben nem ismer, akkor a nyilvántartás típusát **Objektumazonosító-normalizálás** formában kell egy objektum azonosító (OID) segítségével 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). Egy Bejegyzett alkalmazás szolgáltató azonosító (RID) igénylésére szolgáló Microsoft Word formátumú adatlap elérhető az ANSI Nyilvános dokumentum könyvtár webhelyen:

<http://public.ansi.org/ansionline/Documents/> . Az adatlap az **Other Services > Registration Programs** útvonalon érhető el. 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, például: 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/adresse/membodies.html>  helyen található. Az információk között a postacím és az elektronikus levélcím is megtalálható. Több esetben az adott szervezethez tartozó webhely címe is megjelenik.
- 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.

## Leképezés kikeresések és irányelv társítások használatának engedélyezése egy cél nyilvántartásban.

Az EIM leképezés irányelv támogatás segítségével N-1 leképezéseket hozhatunk létre olyan esetekre, amikor nem létezik társítás a felhasználói azonosságok és egy EIM azonosító között. Az irányelv társítás egyetlen felhasználói azonosság helyett több felhasználói azonosságot rendel egyetlen felhasználói azonossághoz egy megadott felhasználói nyilvántartásban.

Mielőtt azonban elkezdené használni az irányelv társításokat, engedélyezze az irányelv társításokat használó leképezés kikereséseket a tartományban. Ezen kívül minden egyes nyilvántartásban engedélyezni kell egy vagy két beállítást:

- **Leképezés kikeresések engedélyezése a nyilvántartásban** Ez a beállítás biztosítja, hogy a nyilvántartás részt vehessen az EIM leképezés kikeresés műveletekben függetlenül attól, hogy van-e megadva hozzá irányelv társítás.
- **Irányelv társítások használata** Ennek a lehetőségnek az engedélyezése kijelöli a nyilvántartást az irányelv társításhoz tartozó cél nyilvántartásnak, és biztosítja, hogy részt tudjon venni az EIM leképezés kikeresési műveletekben.

Ha nincs engedélyezve a leképezés kikeresés a cél nyilvántartás meghatározás számára, akkor az nem vehet részt az EIM leképezés kikeresési műveletekben. Ha nem engedélyezi a nyilvántartás számára az irányelv társítások használatát, akkor az EIM leképezés kikeresési műveletek figyelmen kívül hagyják a nyilvántartáshoz tartozó irányelv társításokat abban az esetben, ha az adott nyilvántartás a művelet célja.

Ha engedélyezni szeretné a cél nyilvántartásban az irányelv társítások használatát a leképezés kikeresések során, akkor csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi "EIM hozzáférés felügyelet" oldalszám: 34 szintek egyikére:

- EIM adminisztrátor
- Nyilvántartás adminisztrátor
- Kijelölt nyilvántartások adminisztrátora (az engedélyezni kívánt nyilvántartás)

A leképezés kikeresés támogatás általános és az irányelv társítások egy adott cél nyilvántartásra vonatkozó engedélyezéséhez tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a "Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához" oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.
3. Kattintson a **Felhasználói nyilvántartások** gombra a tartományban található nyilvántartás meghatározások listájának megjelenítéséhez.

**Megjegyzés:** Ha Kijelölt nyilvántartások adminisztrátora hozzáférés felügyelettel rendelkező felhasználó végzi a műveletet, akkor ez a lista csak azokat a nyilvántartás meghatározásokat tartalmazza, amelyeknek a kezelésére a felhasználó jogosult.

4. Kattintson a jobb egérgombbal arra a nyilvántartás meghatározásra, amelyhez engedélyezni szeretné a leképezés kikeresés támogatást az irányelv társításokhoz, majd válassza az előugró menü **Leképezés irányelv...** menüpontját.
5. Az **Általános** lapon válassza ki az **Irányelv társítások engedélyezése a tartományban** beállítást. A lehetőség kiválasztásával lehetővé teszi a nyilvántartás részvételét az EIM leképezés kikeresési műveletekben. Ha ez a lehetőség nincs be kapcsolva, akkor a leképezés kikeresési műveletek nem adnak vissza eredményt a nyilvántartáshoz attól függetlenül, hogy az adott nyilvántartás forrás vagy cél nyilvántartásként szerepel a kikeresési műveletben.
6. Engedélyezze az **irányelv társítások használata** lehetőséget. A kapcsoló engedélyezésével lehetővé teszi a kikeresési műveletek számára az irányelv társítások használatát abban az esetben, ha a nyilvántartás az adott művelet céljaként szerepel.
7. A módosítások mentéséhez kattintson az **OK** gombra.

**Megjegyzés:** Mielőtt a nyilvántartások használhatnák az irányelv társításokat, engedélyezni kell az irányelv társítások használatát a tartományban.

## Nyilvántartás meghatározás törlése

- | Amikor töröl egy nyilvántartás meghatározást az EIM tartományból, akkor nem befolyásolja azt a felhasználói nyilvántartást, amelyre a nyilvántartás meghatározás hivatkozik, de az adott nyilvántartás a továbbiakban nem vehet részt az EIM tartományban. Azonban tartsa szem előtt az alábbiakat egy nyilvántartás meghatározás törlésekor:
  - | • Ha kitöröl egy nyilvántartás meghatározást, akkor elveszíti az adott felhasználói nyilvántartáshoz tartozó összes társítást. Ha új meghatározást hoz létre a nyilvántartáshoz, akkor újra létre kell hozni a szükséges társításokat is.
  - | • Ha kitöröl egy X.509 nyilvántartás meghatározást, akkor elveszíti a nyilvántartáshoz megadott összes igazolásszűrőt. Ha új meghatározást hoz létre az X.509 nyilvántartáshoz, akkor újra létre kell hozni a szükséges igazolásszűrőket is.
  - | • Nem törölhet egy rendszer nyilvántartás meghatározást akkor, ha vannak olyan alkalmazás nyilvántartás meghatározások, amelyek szülő nyilvántartásként hivatkoznak az adott rendszer nyilvántartás meghatározásra.
- | EIM nyilvántartás meghatározás törléséhez csatlakoznia kell a megfelelő EIM tartományhoz, és EIM adminisztrátor hozzáférés felügyelettel kell rendelkeznie.

EIM nyilvántartás meghatározás törléséhez tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - 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** gombra a tartományban található nyilvántartás meghatározások listájának megjelenítéséhez.

**Megjegyzés:** Ha Kijelölt nyilvántartások adminisztrátora hozzáférés felügyelettel rendelkező felhasználó végzi a műveletet, akkor ez a lista csak azokat a nyilvántartás meghatározásokat tartalmazza, amelyeknek a kezelésére a felhasználó jogosult.

5. Kattintson a jobb egérgombbal a törölni kívánt felhasználói nyilvántartásra, majd válassza az előugró menü **Törlés...** menüpontját.
6. A nyilvántartás meghatározás törléséhez kattintson a **Megerősítés** párbeszédablak **Igen** gombjára.

## nyilvántartás meghatározás álnév eltávolítása

Egy nyilvántartás meghatározáshoz tartozó álnév eltávolításához csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi "EIM hozzáférés felügyelet" oldalszám: 34 szintek egyikére:

- Nyilvántartás adminisztrátor.
- Kijelölt nyilvántartások adminisztrátora (a módosítani kívánt nyilvántartás)
- EIM adminisztrátor

A nyilvántartás meghatározáshoz tartozó álnév eltávolításához tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg a "Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához" oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a "Csatlakozás egy Vállalati azonosság leképezés (EIM) tartományhoz" oldalszám: 81 című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson a **Felhasználói nyilvántartások** elemre a tartományban lévő nyilvántartás meghatározások listájának megjelenítéséhez.

**Megjegyzés:** Ha Kijelölt nyilvántartások adminisztrátora hozzáférés felügyelettel rendelkező felhasználó végzi a műveletet, akkor ez a lista csak azokat a nyilvántartás meghatározásokat tartalmazza, amelyeknek a kezelésére a felhasználó jogosult.

5. Kattintson a jobb egérgombbal az EIM azonosítóra, majd válassza az előugró menü **Tulajdonságok...** menüpontját.
6. Kattintson az **Álnév** lapra.
7. Válassza ki az eltávolítani kívánt álnevet, majd kattintson az **Eltávolítás** gombra.
8. A módosítások mentéséhez kattintson az **OK** gombra.

## Vállalati azonosság leképezés (EIM) azonosítók kezelése

A hálózat felhasználóit képviselő EIM azonosítók létrehozása és használata nagyon hasznos lehet a felhasználók által birtokolt felhasználói azonosságok nyomonkövetéséhez. A vállalati felhasználók folyamatosan mozgásban vannak: újak jönnek, néhányan elmennek vagy munkakört váltanak. Ezek a változások hozzáadódnak a hálózatban található alkalmazásokat és rendszereket használó felhasználói azonosságok és jelszavak nyomon követésének problémájához. Ráadásul egy vállalatnál a jelszókezelés is sok időt igényel. Vállalati azonosság leképezés (EIM) azonosítók létrehozásával és a felhasználói azonosságokhoz társításával leegyszerűsítheti annak nyomon követését, hogy egy adott felhasználói azonosságot pontosan ki birtokol. Ezzel a jelszókezelés is leegyszerűsödik.

Egy egyszeri bejelentkezési környezet a felhasználók számára is könnyebbé teszi a felhasználói azonosságok kezelését, különösen abban az esetben, ha egy másik részleghez vagy területre kerülnek a vállalaton belül. Egyszeri bejelentkezés kialakítása esetén a felhasználóknak az új rendszerekhez nem kell új felhasználói neveket és jelszavakat megjegyezniük.

**Megjegyzés:** Az EIM azonosítók létrehozásának és használatának módja függ az adott szervezet igényeitől. Bővebb információkért olvassa el az "EIM azonosítók elnevezési megállapodásának kialakítása" oldalszám: 56 részt.

A **Tartománykezelés** mappa alatt megtalálható összes EIM tartomány EIM azonosítóit kezelheti. Az EIM azonosítók kezeléséhez az alábbi feladatokat hajthatja vége az EIM tartományban:

- "Vállalati azonosság leképezés (EIM) azonosító létrehozása" oldalszám: 91
- "Álnév hozzáadása egy Vállalati azonosság leképezés azonosítóhoz" oldalszám: 91
- "Vállalati azonosság leképezés azonosító álnév eltávolítása" oldalszám: 92
- "Vállalati azonosság leképezés azonosítók nézetének testreszabása" oldalszám: 93
- "Vállalati azonosság leképezés (EIM) azonosító törlése" oldalszám: 92



A "Társítások kezelése" oldalszám: 93 is hasznosnak fog bizonyulni az EIM azonosítók kezelése során.

## Vállalati azonosság leképezés (EIM) azonosító létrehozása

EIM azonosító létrehozásához csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi "EIM hozzáférés felügyelet" oldalszám: 34 szintek egyikére:

- Azonosító adminisztrátor.
- EIM adminisztrátor

Ha a vállalatban található személy vagy entitás számára EIM azonosítót szeretne létrehozni, akkor tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a "Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához" oldalszám: 80 című részt.
  - 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 az **Azonosítók** elemre, majd válassza az előugró menü **Új azonosító...** menüpontját.
5. Az **Új EIM azonosító** párbeszédablakon adja meg az EIM azonosítóra vonatkozó információkat az alábbiak szerint:
  - Az azonosító neve.
  - Szükség esetén előállítson-e a rendszer egyedi nevet.
  - Az azonosító leírása.
  - Az azonosítóhoz tartozó álnevek, amennyiben szükséges.
6. Amennyiben segítségre szorul a mezők jelentésével kapcsolatban, kattintson a **Súgó** gombra.
7. A szükséges információk megadása után kattintson az **OK** gombra az EIM azonosító létrehozásához.

**Megjegyzés:** Ha a tartományban nagy számú EIM azonosító található, akkor az **Azonosítók** mappa megnyitásakor az azonosítók listájának összeállítása hosszú ideig tart. Ha a tartományban nagy számú EIM azonosító található, akkor a művelet gyorsítása érdekében a "Vállalati azonosság leképezés azonosítók nézetének testreszabása" oldalszám: 93 résznél található információk alapján érdemes szűkíteni a megjelenítendő EIM azonosítók listáját.

## Álnév hozzáadása egy Vállalati azonosság leképezés azonosítóhoz

Elképzelhető, hogy egy "EIM azonosító" oldalszám: 9 részletesebb megkülönböztetéséhez szükség van egy álnév létrehozására. Az álnevek segítséget nyújthatnak egy adott Vállalati azonosság leképezés (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. Ha a vállalatnál két Nap S. János nevű személy dolgozik, akkor érdemes létrehozni például egy Nap Sándor János és egy Nap Sámuel János álnevet a felhasználók azonosságainak egyszerűbb megkülönböztetése érdekében. A további álnevek tartalmazhatják a felhasználók dolgozói kódját, osztályát, munkakörét vagy bármely más megkülönböztető jellemzőt.

Ha egy álnevet kíván hozzáadni egy EIM azonosítóhoz, akkor csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi "EIM hozzáférés felügyelet" oldalszám: 34 szintek egyikére:

- EIM adminisztrátor
- Azonosító adminisztrátor

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

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a “Csatlakozás egy Vállalati azonosság leképezés (EIM) tartományhoz” oldalszám: 81 című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson az **Azonosítók** elemre a tartományban rendelkezésre álló EIM azonosítók listájának megjelenítéséhez a jobboldali ablakrészben.

**Megjegyzés:** Előfordulhat, hogy az **Azonosítók** mappa megnyitásakor az azonosítók listájának összeállítása hosszú ideig tart. Ha a tartományban nagy számú EIM azonosító található, akkor a művelet gyorsítása érdekében a “Vállalati azonosság leképezés azonosítók nézetének testreszabása” oldalszám: 93 résznél található információk alapján érdemes szűkíteni a megjelenítendő EIM azonosítók listáját.

5. Kattintson a jobb egérgombbal arra az EIM azonosítóra, amelyhez a törölni kívánt álnév tartozik, majd válassza az előugró menü **Tulajdonságok...** menüpontját.
6. Az **Álnév** mezőben adja meg az EIM azonosítóhoz felvenni kívánt álnevet, majd kattintson a **Hozzáadás** gombra.
7. Kattintson az **OK** gombra az EIM azonosító változásainak elmentéséhez.

### Vállalati azonosság leképezés azonosító álnév eltávolítása

Ha el akar távolítani egy Vállalati azonosság leképezés azonosítóhoz tartozó álnevet, akkor csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi “EIM hozzáférés felügyelet” oldalszám: 34 szintek egyikére:

- Azonosító adminisztrátor
- EIM adminisztrátor

Az EIM azonosítóhoz tartozó álnév eltávolításához tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a Tartománykezelés mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a “Csatlakozás egy Vállalati azonosság leképezés (EIM) tartományhoz” oldalszám: 81 című témakörben.
3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
4. Kattintson az **Azonosítók** elemre a tartományban rendelkezésre álló EIM azonosítók listájának megjelenítéséhez a jobboldali ablakrészben.

**Megjegyzés:** Előfordulhat, hogy az **Azonosítók** mappa megnyitásakor az azonosítók listájának összeállítása hosszú ideig tart. Ha a tartományban nagy számú EIM azonosító található, akkor a művelet gyorsítása érdekében a “Vállalati azonosság leképezés azonosítók nézetének testreszabása” oldalszám: 93 résznél található információk alapján érdemes szűkíteni a megjelenítendő EIM azonosítók listáját.

5. Kattintson a jobb egérgombbal arra az EIM azonosítóra, amelyhez a törölni kívánt álnév tartozik, majd válassza az előugró menü **Tulajdonságok...** menüpontját.
6. Válassza ki az eltávolítani kívánt álnevet, majd kattintson az **Eltávolítás** gombra.
7. A módosítások mentéséhez kattintson az **OK** gombra.

### Vállalati azonosság leképezés (EIM) azonosító törlése

EIM azonosító létrehozásához csatlakoznia kell a megfelelő Vállalati azonosság leképezés (EIM) tartományhoz, és EIM adminisztrátor hozzáférés felügyelettel kell rendelkeznie.

EIM azonosító törléséhez tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - 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.

**Megjegyzés:** Előfordulhat, hogy az **Azonosítók** mappa megnyitásakor az azonosítók listájának összeállítása hosszú ideig tart. Ha a tartományban nagy számú EIM azonosító található, akkor a művelet gyorsítása érdekében a “Vállalati azonosság leképezés azonosítók nézetének testreszabása” résznel található információk alapján érdemes szűkíteni a megjelenítendő EIM azonosítók listáját.

5. Válassza ki a törölni kívánt EIM azonosítót. Több azonosító törléséhez a **Ctrl** billentyű lenyomása mellett kattintson a megfelelő EIM azonosítókra.
6. Kattintson a jobb egérgombbal a kijelölt EIM azonosítókon, majd válassza az előugró menü **Törlés** menüpontját.
7. A **Törlés megerősítése** párbeszédablakon kattintson az **Igen** gombra a kijelölt EIM azonosítók törléséhez.

### Vállalati azonosság leképezés azonosítók nézetének testreszabása

Előfordulhat, hogy az **Azonosítók** mappa megnyitásakor az azonosítók listájának összeállítása hosszú ideig tart. Ha a tartományban nagy számú EIM azonosító található, akkor érdemes az **Azonosítók** mappa nézetének testreszabásával javítani megjelenítés teljesítményén.

Az **Azonosítók** mappa nézetének testreszabásához tegye a következőket:

1. Bontsa ki a **Hálózat -> Vállalati azonosság leképezés -> Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.
3. Kattintson a jobb egérgombbal az **Azonosítók** mappára, majd válassza az előugró menü **Nézet testreszabása** menüpontját.
4. Adja meg a tartományban található EIM azonosítók megjelenítéséhez használt feltételeket. A megjelenített EIM azonosítók számának csökkentéséhez adja meg az azonosító rendezéséhez használni kívánt karaktereket. Az azonosító nevében egy vagy több helyettesítő karaktert (\*) is megadhat. Például megadhatja a \*NAP\* rendezési feltételt az **Azonosító** mezőben. Az eredményben azok az EIM azonosítók fognak szerepelni, amelyeknek neve vagy egy hozzájuk tartozó álnév tartalmazza a NAP karaktersorozatot.
5. A módosítások mentéséhez kattintson az **OK** gombra.

### Társítások kezelése

Az EIM kétféle társítás létrehozását és kezelését teszi lehetővé: az azonosító társítások közvetett, az irányelv társítások közvetlen viszonyt határoznak meg a felhasználói azonosságok között. Az EIM-ben létrehozható és kezelhető azonosító társítás nem más, mint EIM azonosítók és a hozzájuk tartozó felhasználói azonosságok közötti viszony, melynek segítségével közvetett, egyedi viszony hozható létre a felhasználói azonosságok között. Az EIM-ben létrehozható irányelv társítás segítségével közvetlenül képezhet le több, akár különböző nyilvántartásokban szereplő felhasználói azonosságot egy másik nyilvántartásban található egyetlen cél felhasználói azonosságra. Az irányelv társítások az EIM leképezés irányelv támogatását felhasználva N-1 relációkat hoznak létre felhasználói azonosságok között EIM azonosító közbeiktatása nélkül. Mivel mindkét típusú társítás a vállalatban található felhasználói azonosságok közötti viszony megadására szolgál, a társítások kezelése az EIM kezelésének fontos része.

| A tartományban található társítások karbantartása kulcsfontosságú kérdés a hálózat különféle rendszerein fiókokkal rendelkező felhasználók nyomon követéséhez szükséges adminisztrációs feladatok leegyszerűsítésében. Biztonságos egyszeri bejelentkezést biztosító környezet kialakításakor az azonosító társításoknak folyamatosan naprakésznek kell lenniük.

| Az alábbi társítás kezelési feladatokat hajthatja végre:

- “Társítások létrehozása”
- Bővebb információkat a Cél felhasználói azonosság kiegészítése keresési információkkal részben talál.
- Bővebb információkat a Cél felhasználói azonossághoz tartozó keresési információk eltávolítása részben talál.
- EIM azonosítóhoz tartozó társítások megjelenítése.
- Tartomány összes irányelv társításának megjelenítése
- Nyilvántartás összes irányelv társításának megjelenítése
- “Azonosító társítás törlése” oldalszám: 106
- “Irányelv társítás törlése” oldalszám: 107

## | **Társítások létrehozása**

| Társításokat kétféle módon hozhat létre:

- Létrehozhat egy azonosító társítást egy személy által használt két felhasználói azonosság közötti viszony közvetett megadására. Az azonosító társítások az EIM azonosítók és a felhasználói nyilvántartásban található felhasználói azonosságok közötti kapcsolatot írják le. Az azonosító társítások segítségével egy EIM azonosító és az általa képviselt felhasználóhoz tartozó különböző felhasználói azonosságok között hozhat létre 1-1 leképezést.
- Létrehozhat egy irányelv társítást, melynek segítségével közvetlenül képezhet le több, akár különböző nyilvántartásokban szereplő felhasználói azonosságot egy másik nyilvántartásban található egyetlen cél felhasználói azonosságra. Az irányelv társítások az EIM leképezés irányelv támogatását felhasználva N-1 relációkat hoznak létre felhasználói azonosságok között EIM azonosító közbeiktatása nélkül. Az irányelv társítás segítségével nagy mennyiségű leképezést hozhat létre rövid idő alatt a különböző felhasználói nyilvántartásokban található összetartozó felhasználók között.

| Az EIM megvalósítás által támasztott igényei határozzák meg azt, hogy azonosító társításokat, irányelv társításokat vagy a kettő keverékét szükséges létrehozni. Bővebb információkért nézze meg az Átfogó azonosság leképezés terv elkészítése című témakört.

| **Azonosító társítás létrehozása:** Az azonosító társítás egy vállalati felhasználói azonosság vagy entitás és a hozzá tartozó EIM azonosító között létesít kapcsolatot. Háromféle azonosító társítás hozható létre: cél, forrás és adminisztrációs. A társítások és leképezések későbbi problémáinak megelőzése érdekében a társítások meghatározása előtt szükséges egy átfogó azonosság leképezési terv elkészítése a vállalat számára.

| Azonosító társítás létrehozásához csatlakoznia kell a megfelelő EIM tartományhoz, és egy a társítás típusától függő “EIM hozzáférés felügyelet” oldalszám: 34 is.

| Egy forrás vagy adminisztrációs társítás létrehozásához az alábbi EIM hozzáférés felügyeleti szintek egyikére van szükség:

- Azonosító adminisztrátor.
- EIM adminisztrátor

| Egy cél társítás létrehozásához az alábbi EIM hozzáférés felügyeleti szintek egyikére van szükség:

- Nyilvántartás adminisztrátor.
- Kijelölt nyilvántartások adminisztrátora (az a nyilvántartás meghatározás, amelyik a cél felhasználói azonosságot tartalmazó felhasználói nyilvántartásra vonatkozik)
- EIM adminisztrátor

| Egy azonosító társítás létrehozásához tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - 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 a tartományban található EIM azonosítók listájának megjelenítéséhez.

**Megjegyzés:** Előfordulhat, hogy az **Azonosítók** mappa megnyitásakor az azonosítók listájának összeállítása hosszú ideig tart. Ha a tartományban nagy számú EIM azonosító található, akkor a művelet gyorsítása érdekében a “Vállalati azonosság leképezés azonosítók nézetének testreszabása” oldalszám: 93 résznél található információk alapján érdemes szűkíteni a megjelenítendő EIM azonosítók listáját.

5. Kattintson a jobb egérgombbal arra az EIM azonosítóra, amelyhez létre kívánja hozni a társítást, majd válassza az előugró menü **Tulajdonságok...** menüpontját.
6. A **Társítások** lapon kattintson a **Hozzáadás...** gombra.
7. A **Társítás hozzáadása** párbeszédablakon adja meg társítás meghatározásához szükséges információkat az alábbiak szerint:
  - Az EIM azonosítóval társítandó felhasználói azonosságot tartalmazó nyilvántartás neve. Adja meg egy létező nyilvántartás meghatározás pontos nevét, vagy a tallózás funkcióval keressen meg egy létezőt.
  - Az EIM azonosítóval társítandó felhasználói azonosság neve.
  - A társítás típusa. Az alábbi három típus közül válogathat:
    - Adminisztrációs
    - Forrás
    - Cél
8. Amennyiben segítségre szorul a mezők jelentésével kapcsolatban, kattintson a **Súgó** gombra.
9. Választható. Cél társítás esetén a **Speciális...** gombra kattintva nyissa meg a **Társítás hozzáadása - speciális** párbeszédablakot. Adjon meg kikeresési információkat a cél felhasználói azonossághoz, majd az **OK** gombbal térjen vissza az **Társítás felvétele** párbeszédablakhoz.
10. A szükséges információk megadása után kattintson az **OK** gombra a társítás létrehozásához.

**Irányelv társítás létrehozása:** Az irányelv társítások segítségével közvetlenül képezhet le több, akár különböző nyilvántartásokban szereplő felhasználói azonosságot egy másik nyilvántartásban található egyetlen cél felhasználói azonosságra. Az irányelv társítások az EIM leképezés irányelv támogatását felhasználva N-1 relációkat hoznak létre felhasználói azonosságok között EIM azonosító közbeiktatása nélkül. Mivel az irányelv társítások használatára számos, sokszor egymást átfedő mód létezik, az irányelv társítások létrehozása előtt nagyon fontos megérteni az EIM leképezés irányelv támogatást. Továbbá a társítások és leképezések későbbi problémáinak megelőzése érdekében a társítások meghatározása előtt szükséges egy átfogó azonosság leképezési terv elkészítése a vállalat számára.

Az EIM megvalósítás által támasztott igényei határozzák meg azt, hogy azonosító társításokat, irányelv társításokat vagy a kettő keverékét szükséges létrehozni.

Az irányelv társítás létrehozásának módja a kívánt társítás típustól függ. Az irányelv társítások létrehozásáról bővebben az alábbi részekenél olvashat:

- Alapértelmezett tartomány irányelv társítás létrehozása.
- Alapértelmezett nyilvántartás irányelv társítás létrehozása.
- Igazolásszűrő irányelv társítás létrehozása.

| *Alapértelmezett tartomány irányelv társítás létrehozása:* Alapértelmezett tartomány irányelv társítás létrehozásához  
| csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi “EIM hozzáférés felügyelet”  
| oldalszám: 34 szintek egyikére:

- | • EIM adminisztrátor
- | • Nyilvántartás adminisztrátor

| **Megjegyzés:** Az irányelv társítások több felhasználói azonosság és egy adott cél felhasználói nyilvántartásban  
| található egyetlen felhasználói azonosság közötti viszonyt írják le. Az irányelv társítások segítségével  
| egy felhasználói azonosságokból álló halmaz és egy adott cél felhasználói nyilvántartásban található  
| felhasználói azonosság között írhat le viszonyt. Az irányelv társítások az EIM leképezés irányelv  
| támogatását felhasználva N-1 relációkat hoznak létre felhasználói azonosságok között EIM azonosító  
| közbeiktatása nélkül.

| Mivel az irányelv társítások használatára számos, sokszor egymást átfedő mód létezik, az irányelv  
| társítások létrehozása előtt nagyon fontos megérteni az EIM leképezés irányelv támogatást. Továbbá a  
| társítások és leképezések későbbi problémáinak megelőzése érdekében a társítások meghatározása előtt  
| szükséges egy átfogó azonosság leképezési terv elkészítése a vállalat számára.

| Az alapértelmezett tartomány irányelv társításban a tartományban található összes felhasználó forrása az irányelv  
| társításnak, és leképeződik egyetlen cél nyilvántartásra és cél felhasználóra. A tartományban található összes  
| nyilvántartáshoz megadhat alapértelmezett tartomány irányelv társítást. Ha egy cél nyilvántartásra kettő vagy több  
| tartomány irányelv társítás hivatkozik, akkor egyedi kikeresési információk megadásával biztosíthatja, hogy a  
| leképezés kikeresési műveletek különbséget tudjanak tenni közöttük. Ellenkező esetben a leképezés kikeresési  
| műveletek több felhasználói azonosságot fognak visszaadni. Ezeknek miatt a kétértelmű eredmények miatt  
| előfordulhat, hogy az EIM használatára támaszkodó alkalmazások nem tudják pontosan megállapítani a használandó  
| cél azonosságot.

| Az alapértelmezett tartomány irányelv társítás létrehozásához tegye a következőket:

- | 1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
- | 2. Kattintson a jobb egérgombbal a használni kívánt EIM tartományra, majd válassza az előugró menü **Leképezés**  
| **irányelv...** menüpontját.
  - | • Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati  
| azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - | • Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a  
| Csatlakozás az EIM tartományvezérlőhöz című témakörben.
- | 3. Válassza ki az **Irányelv társítások használatának engedélyezése a leképezés kikeresésekhez a tartományban**  
| lehetőséget az **Általános** lapon.
- | 4. A **Tartomány** lapon kattintson a **Hozzáadás...** gombra.
- | 5. Az **Alapértelmezett tartomány irányelv társítás hozzáadása** párbeszédablakon adja meg az alábbi  
| információkat:
  - | • A **Cél nyilvántartás** mezőben az irányelv társításhoz tartozó cél nyilvántartás meghatározás nevét.
  - | • A **Cél felhasználó** mezőben az irányelv társításhoz tartozó cél felhasználói azonosságot.
- | 6. Ha a párbeszédablak kitöltésével kapcsolatban további segítségre van szüksége, akkor kattintson a **Súgó** gombra.
- | 7. Választható. A **Speciális...** gombra kattintva nyissa meg a **Társítás hozzáadása - speciális** párbeszédablakot. A  
| **Kikeresési információk** mezőben adja meg a kikeresési információkat az irányelv társításhoz, majd az **OK**  
| gombbal térjen vissza a **Alapértelmezett tartomány irányelv társítás hozzáadása** párbeszédablakhoz.

| **Megjegyzés:** Ha egy cél nyilvántartásra kettő vagy több alapértelmezett tartomány irányelv társítás hivatkozik,  
| akkor minden felhasználói azonossághoz egyedi kikeresési információkat kell megadnia. Ebben a  
| helyzetben a kikeresési információk megadásával lehet biztosítani, hogy a leképezés kikeresési  
| műveletek különbséget tudjanak tenni a cél felhasználó azonosságok között. Ellenkező esetben a  
| leképezés kikeresési műveletek több felhasználói azonosságot fognak visszaadni. Ezeknek miatt a

kétértelmű eredmények miatt előfordulhat, hogy az EIM használatára támaszkodó alkalmazások nem tudják pontosan megállapítani a használandó cél azonosságát.

8. Az **OK** gombbal hozza létre az új irányelv társítást és térjen vissza a **Tartomány** lapra. Az új irányelv társítás megjelenik az **Alapértelmezett irányelv társítások** táblázatban.

9. Győződjön meg róla, hogy az új irányelv társítás engedélyezett a cél nyilvántartás számára.

10. A módosítások elmentéséhez és a **Leképezési irányelv** párbeszédablakból kilépéshez kattintson az **OK** gombra.

**Megjegyzés:** Győződjön meg róla, hogy a leképezés irányelv támogatás és az irányelv társítások használata engedélyezett a cél felhasználói nyilvántartás számára. Ha nem engedélyezett, akkor az irányelv társításnak nem lesz hatása.

*Alapértelmezett nyilvántartás irányelv társítás létrehozása:* Alapértelmezett nyilvántartás irányelv társítás létrehozásához csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi "EIM hozzáférés felügyelet" oldalszám: 34 szintek egyikére:

- EIM adminisztrátor
- Nyilvántartás adminisztrátor

**Megjegyzés:** Az irányelv társítások több felhasználói azonosság és egy adott cél felhasználói nyilvántartásban található egyetlen felhasználói azonosság közötti viszonyt írnak le. Az irányelv társítások segítségével egy felhasználói azonosságokból álló halmaz és egy adott cél felhasználói nyilvántartásban található felhasználói azonosság között írhat le viszonyt. Az irányelv társítások az EIM leképezés irányelv támogatását felhasználva N-1 relációkat hoznak létre felhasználói azonosságok között EIM azonosító közbeiktatása nélkül.

Mivel az irányelv társítások használatára számos, sokszor egymást átfedő mód létezik, az irányelv társítások létrehozása előtt nagyon fontos megérteni az EIM leképezés irányelv támogatást. Továbbá a társítások és leképezések későbbi problémáinak megelőzése érdekében a társítások meghatározása előtt szükséges egy átfogó azonosság leképezési terv elkészítése a vállalat számára.

Az alapértelmezett nyilvántartás irányelv társításban a nyilvántartásban található összes felhasználó forrása az irányelv társításnak, és leképeződik egyetlen cél nyilvántartásra és cél felhasználóra. Az alapértelmezett nyilvántartás irányelv társítás engedélyezése a cél nyilvántartás számára biztosítja, hogy a forrás felhasználói azonosságok mindegyike le legyen képezve egy cél nyilvántartásban található cél felhasználóra.

Az alapértelmezett nyilvántartás irányelv társítás létrehozásához tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.

2. Kattintson a jobb egérgombbal a használni kívánt EIM tartományra, majd válassza az előugró menü **Leképezés irányelv...** menüpontját.

- Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a "Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához" oldalszám: 80 című részt.
- Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.

3. Válassza ki az **Irányelv társítások használatának engedélyezése a leképezés kikeresésekhez a tartományban** lehetőséget az **Általános** lapon.

4. A **Nyilvántartás** lapon kattintson a **Hozzáadás...** gombra.

5. Az **Alapértelmezett nyilvántartás irányelv társítás hozzáadása** párbeszédablakon adja meg az alábbi információkat:

- A **Forrás nyilvántartás** mezőben az irányelv társításhoz tartozó forrás nyilvántartás meghatározás nevét.
- A **Cél nyilvántartás** mezőben az irányelv társításhoz tartozó cél nyilvántartás meghatározás nevét.
- A **Cél felhasználó** mezőben az irányelv társításhoz tartozó cél felhasználói azonosságot.

6. Ha a párbeszédablak kitöltésével kapcsolatban további segítségre van szüksége, akkor kattintson a **Súgó** gombra.

7. Választható. A **Speciális...** gombra kattintva nyissa meg a **Társítás hozzáadása - speciális** párbeszédablakot. A **Kikeresési információk** mezőben adja meg a kikeresési információkat az irányelv társításhoz, majd az **OK** gombbal térjen vissza a **Alapértelmezett tartomány irányelv társítás hozzáadása** párbeszédablakhoz.

**Megjegyzés:** Ha egy cél nyilvántartásra kettő vagy több ugyanazzal a forrás nyilvántartással rendelkező irányelv társítás hivatkozik, akkor minden felhasználói azonossághoz egyedi kikeresési információkat kell megadnia. Ebben a helyzetben a kikeresési információk magadásával lehet biztosítani, hogy a leképezés kikeresési műveletek különbséget tudjanak tenni a cél felhasználó azonosságok között. Ellenkező esetben a leképezés kikeresési műveletek több felhasználói azonosságot fognak visszaadni. Ezeknek miatt a kétértelmű eredmények miatt előfordulhat, hogy az EIM használatára támaszkodó alkalmazások nem tudják pontosan megállapítani a használandó cél azonosságot.

8. Az **OK** gombbal hozza létre az új irányelv társítást és térjen vissza a **Nyilvántartás** lapra. Az új alapértelmezett nyilvántartás irányelv társítás megjelenik az **Alapértelmezett irányelv társítások** táblázatban.
9. Győződjön meg róla, hogy az új irányelv társítás engedélyezett a cél nyilvántartás számára.
10. A módosítások elmentéséhez és a **Leképezési irányelv** párbeszédablakból kilépéshez kattintson az **OK** gombra.

**Megjegyzés:** Győződjön meg róla, hogy a leképezés irányelv támogatás és az irányelv társítások használata engedélyezett a cél felhasználói nyilvántartás számára. Ha nem engedélyezett, akkor az irányelv társításnak nem lesz hatása.

*Igazolásszűrő irányelv társítás létrehozása:* Igazolásszűrő irányelv társítás létrehozásához csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi "EIM hozzáférés felügyelet" oldalszám: 34 szintek egyikére:

- EIM adminisztrátor
- Nyilvántartás adminisztrátor

**Megjegyzés:** Egy irányelv társítás egy felhasználói azonosságokból álló halmaz és egy adott cél felhasználói nyilvántartásban található felhasználói azonosság közötti viszonyt ír le. Az irányelv társítások az EIM leképezés irányelv támogatását felhasználva N-1 relációkat hoznak létre felhasználói azonosságok között EIM azonosító közbeiktatása nélkül.

Mivel az irányelv társítások használatára számos, sokszor egymást átfedő mód létezik, az irányelv társítások létrehozása előtt nagyon fontos megérteni az EIM leképezés irányelv támogatást. Továbbá a társítások és leképezések későbbi problémáinak megelőzése érdekében a társítások meghatározása előtt szükséges egy átfogó azonosság leképezési terv elkészítése a vállalat számára.

Az igazolásszűrő irányelv társítások kijelölik egy startégi társítás forrásául szolgáló X.509 nyilvántartásban található igazoláskészletet. Ezeket az igazolásokat a megadott cél nyilvántartásra és felhasználóra képezi le. Az alapértelmezett nyilvántartás irányelv társításhoz képest, amikor egy irányelv társítás forrása a nyilvántartásban található összes felhasználó, az igazolásszűrő irányelv társítás hatóköre jóval rugalmasabb. Forrásként a nyilvántartásban található igazolás egy részhalmazát is megadhatja. Az irányelv társításhoz megadott igazolásszűrő határozza meg a hatókört.

**Megjegyzés:** Ha egy X.509 felhasználói nyilvántartásban található összes igazolást egyetlen cél felhasználói azonosságra kívánja leképezni, akkor hozzon létre egy alapértelmezett nyilvántartás irányelv társítást.

Az igazolásszűrő vezérli azt, hogy az igazolásszűrő irányelv társítás hogyan képezi le a forrás felhasználói azonosságok halmazát (ebben az esetben digitális igazolásokat) egy megadott cél felhasználói azonosságra. Ezért a használni kívánt igazolásszűrőnek léteznie kell az igazolásszűrő irányelv társítás létrehozásakor.

Mielőtt tehát meghatározná egy igazolásszűrő irányelv társítást, először létre kell hoznia egy igazolásszűrőt, ami az irányelv társítás alapjául szolgál.

Az igazolásszűrő irányelv társítás létrehozásához tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.



2. Kattintson a jobb egérgombbal a használni kívánt EIM tartományra, majd válassza az előugró menü **Leképezés irányelv...** menüpontját.
    - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
    - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a **Csatlakozás az EIM tartományvezérlőhöz** című témakörben.
  3. Válassza ki az **Irányelv társítások használatának engedélyezése a leképezés kikeresésekhez a tartományban** lehetőséget az **Általános** lapon.
  4. Az **Igazolásszűrő** lapon kattintson a **Felvez...** gombra az **Igazolásszűrő irányelv társítás felvétele** párbeszédablak megjelenítéséhez.
  5. Ha a párbeszédablak kitöltésével kapcsolatban további segítségre van szüksége, akkor kattintson a **Súgó** gombra.
  6. Az irányelv társítás meghatározásához az alábbi információk megadására van szükség:
    - A **Forrás X.509 nyilvántartás** mezőben adja meg az irányelv társítás forrásául szolgáló X.509 felhasználói nyilvántartás nevét. Ha a tartományhoz megadott nyilvántartás meghatározások közül szeretne választani egyet, akkor kattintson a **Tallózás...** gombra.
    - Kattintson a **Kiválaszt** gombra az **Igazolásszűrő kiválasztása** párbeszédablak megjelenítéséhez. Itt adhatja választhatja ki az új igazolásszűrő irányelv társítás alapjául szolgáló létező igazolásszűrőt.

**Megjegyzés:** **Kötelező** létező igazolásszűrőt használni. Ha a használni kívánt igazolásszűrő nem szerepel a listában, akkor kattintson a **Felvez...** gombra egy új igazolásszűrő létrehozásához.

    - A **Cél nyilvántartás** mezőben adja meg a kívánt nyilvántartás nevét, vagy kattintson a **Tallózás...** gombra, és válasszon egyet a tartományban meglévő nyilvántartás meghatározások listájából.
    - A **Cél felhasználó** mezőben adja meg azt a felhasználói azonosságot, amelyre a **Forrás X.509 nyilvántartás** összes, az igazolásszűrőnek megfelelő igazolását szeretné leképezni. Ha a tartományban felvett felhasználók közül szeretne választani egyet, akkor kattintson a **Tallózás...** gombra.
    - Választható. A **Speciális...** gombra kattintva nyissa meg a **Társítás hozzáadása - speciális** párbeszédablakot. Töltse ki a cél felhasználói azonossághoz tartozó **Kikeresési információk** mezőt, majd az **OK** gombbal térjen vissza az **Igazolásszűrő irányelv társítás felvétele** párbeszédablakhoz.

**Megjegyzés:** Ha egy cél nyilvántartásra kettő vagy több ugyanazzal a forrás X.509 nyilvántartással és igazolásszűrő feltételekkel rendelkező irányelv társítás hivatkozik, akkor minden felhasználói azonossághoz egyedi kikeresési információkat kell megadnia. Ebben a helyzetben a kikeresési információk magadásával lehet biztosítani, hogy a leképezés kikeresési műveletek különbséget tudjanak tenni a cél felhasználó azonosságok között. Ellenkező esetben a leképezés kikeresési műveletek több felhasználói azonosságot fognak visszaadni. Ezeknek miatt a kétértelmű eredmények miatt előfordulhat, hogy az EIM használatára támaszkodó alkalmazások nem tudják pontosan megállapítani a használandó cél azonosságot.
  7. Az **OK** gombbal hozza létre az új igazolásszűrő irányelv társítást és térjen vissza az **Igazolásszűrő** lapra. Az új irányelv társítás megjelenik a listában.
  8. Győződjön meg róla, hogy az új irányelv társítás engedélyezett a cél nyilvántartás számára.
  9. A módosítások elmentéséhez és a **Leképezési irányelv** párbeszédablakból kilépéshez kattintson az **OK** gombra.
- Megjegyzés:** Győződjön meg róla, hogy a leképezés irányelv támogatás és az irányelv társítások használata engedélyezett a cél felhasználói nyilvántartás számára. Ha nem engedélyezett, akkor az irányelv társításnak nem lesz hatása.

*Igazolásszűrő létrehozása:* Az igazolásszűrők megkülönböztetett név igazolás-attribútumok segítségével határozzák meg egy X.509 felhasználói nyilvántartásban a bizonyos szempontból összetartozó felhasználói igazolásokat. Az igazolásszűrők szolgálnak az igazolásszűrő irányelv társítások alapjául. Az igazolásszűrő egy irányelv társításban azt határozza meg, hogy a forrásul szolgáló X.509 nyilvántartásban található igazolások közül melyeket kell leképezni az adott cél felhasználói azonosságra. A szűrő feltételeit kielégítő Tárgy megkülönböztetett név és Kibocsátó megkülönböztetett név információkkal rendelkező igazolás leképezése a megadott cél felhasználóra az EIM kikeresési műveletek során történik meg.

Igazolásszűrő létrehozásához csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi “EIM hozzáférés felügyelet” oldalszám: 34 szintek egyikére:

- EIM adminisztrátor
- Nyilvántartás adminisztrátor
- Kijelölt nyilvántartások adminisztrátora (arra az X.509 felhasználói nyilvántartásra vonatkozó nyilvántartás meghatározás, amelyikhez az igazolásszűrőt kívánja létrehozni)

Az igazolásszűrő alapjául egy digitális igazoláshoz tartozó bizonyos megkülönböztetett név (DN) információk szolgálnak. Ez lehet a tárgy megkülönböztetett név, ami az igazolás tulajdonosát jelöli, vagy a kibocsátó megkülönböztetett név, ami a kibocsátóját határozza meg. Az igazolásszűrőhöz teljes, vagy akár részleges DN információkat is megadhat.

Az igazolásszűrő irányelv társításhoz tartozó igazolásszűrő határozza meg azt, hogy az X.509 nyilvántartásban található igazolások közül melyeket képez le az irányelv társítás a cél felhasználói azonosságra. Ha egy EIM leképezés kikeresési műveletben a forrás felhasználói azonosság egy digitális igazolás (miután a kérést indító alkalmazás az `eimFormatUserIdentity()` EIM API segítségével megformázta a felhasználói azonosság nevet), és az igazolásszűrő irányelv társítás kiértékelése megtörténik, akkor az EIM összehasonlítja az igazolás DN információit a szűrőben megadott teljes vagy részleges DN információkkal. Ha az igazolás DN információi megfelel a szűrőnek, akkor az EIM visszaadja az igazolásszűrő irányelv társítás által meghatározott cél felhasználói azonosságot.

Az igazolásszűrő létrehozása során a szükséges megkülönböztetett név információkat az alábbi módokon adhatja meg:

- Megadhatja egy bizonyos igazoláshoz tartozó teljes vagy részleges **Tárgy DN** vagy **Kibocsátó DN** információkat, szükség esetén mindkettőt.
- Egy adott igazolás megkülönböztetett név információit a vágólapra másolhatja, és a megkülönböztetett név információk alapján létrehozhatja az igazolásszűrő jelölteket tartalmazó listát. Ezután megadhatja, hogy mely DN-ek felhasználásával készüljön el a szűrő.

**Megjegyzés:** Ha ezen a módon kívánja előállítani az igazolásszűrő létrehozásához szükséges megkülönböztetett név információkat, akkor a vágólapra másolást még ennek a feladatnak a végrehajtása előtt el kell végeznie, és az igazolásnak base64 kódolt formában kell lennie. Bővebb információkat az igazolás visszakereséséről a megfelelő formátumban az Igazolásszűrő című témakörnél talál.

- A lehetséges igazolásszűrők listáját az EIM azonosítóhoz tartozó forrás társítással rendelkező digitális igazolások megkülönböztetett név információi alapján hozhatja létre. Ezután megadhatja, hogy mely DN-ek felhasználásával készüljön el a szűrő.

Egy igazolásszűrő irányelv társítás alapjául szolgáló igazolásszűrő létrehozásához tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Kattintson a jobb egérgombbal a használni kívánt EIM tartományra, majd válassza az előugró menü **Léképezés irányelv...** menüpontját.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a **Csatlakozás az EIM tartományvezérlőhöz** című témakörben.
3. Az **Igazolásszűrő** lapon kattintson az **Igazolásszűrők...** gombra az **Igazolásszűrők** párbeszédablak megjelenítéséhez.

**Megjegyzés:** Ha úgy kattint az **Igazolásszűrők...** gombra, hogy nincs irányelv társítás kijelölve, akkor az **EIM nyilvántartások keresése** párbeszédablak jelenik meg. A párbeszédablakon az X.509 nyilvántartás meghatározások listájából kiválaszthat azt az X.509 nyilvántartást, melynek meg szeretné jeleníteni az igazolásszűrőit. A lista tartalmát befolyásolja a felhasználó EIM hozzáférés felügyelete.

4. A **Hozzáadás...** gombra kattintva nyissa meg az **Igazolás hozzáadása** párbeszédablakot.

5. Az **igazolásszűrő hozzáadása** párbeszédablakon eldöntheti, hogy egy különálló igazolásszűrőt kíván felvenni, vagy egy adott digitális igazolás alapján szeretne egy igazolásszűrőt előállítani. Ha a párbeszédablak kitöltésével kapcsolatban további segítségre van szüksége, akkor kattintson a **Súgó** gombra.
  - a. Ha az **Egyetlen igazolásszűrő hozzáadása** lehetőséget választja, akkor megadhatja a teljes vagy részleges **Tárgy DN, Kibocsátó DN** információkat, vagy mindkettőt. Az **OK** gombbal hozza létre az új igazolásszűrőt és térjen vissza az **Igazolásszűrők** párbeszédablakra. A szűrő megjelenik a listában.
  - b. Ha az **Igazolásszűrő előállítása digitális igazolás alapján** lehetőséget választja, akkor az **OK** gombbal megjelenítheti az **Igazolásszűrők előállítása** párbeszédablakot.
    - 1) Illessze be a **Igazolás információk** mezőbe az igazolás vágólapra korábban bemásolt base64 kódolású információit.
    - 2) Kattintson az **OK** gombra az igazolás **Tárgy DN** és **Kibocsátó DN** információi alapján szóba jöhető igazolásszűrők listájának megjelenítéséhez.
    - 3) Az **Igazolásszűrő keresése** párbeszédablakon válasszon ki egy vagy több igazolásszűrőt. Az **OK** gombbal térjen vissza az **Igazolásszűrők kiválasztása** párbeszédablakra, ahol megjelennek a kiválasztott igazolásszűrők.
  - c. Ha az **Igazolásszűrő előállítása forrás társítás alapján** lehetőséget választja, akkor az **OK** gombbal megjelenítheti az **Igazolásszűrők előállítása** párbeszédablakot. Ez a párbeszédablak tartalmaz egy listát azokról az X.509 felhasználói azonosságokról, amelyekhez meg van adva egy tartománybeli EIM azonosítóhoz tartozó forrás társítás.
    - 1) Válassza ki azt az X.509 felhasználói azonosságot, amelynek digitális igazolását fel kívánja használni az igazolásszűrő jelöltek előállításához, majd kattintson az **OK** gombra.
    - 2) Kattintson az **OK** gombra az igazolás **Tárgy DN** és **Kibocsátó DN** információi alapján szóba jöhető igazolásszűrők listájának megjelenítéséhez.
    - 3) Az **Igazolásszűrő keresése** párbeszédablakon válasszon ki egy vagy több igazolásszűrő jelöltet. Az **OK** gombbal térjen vissza az **Igazolásszűrők kiválasztása** párbeszédablakra, ahol megjelennek a kiválasztott igazolásszűrők.

Az új igazolásszűrőt most már felhasználhatja egy igazolásszűrő irányelv társítás létrehozásához.

## Keresési információk hozzáadása a cél felhasználói azonossághoz

A kikeresési információk a társításban megadott cél felhasználói azonossághoz külön megadható egyedi azonosító adatok. Ez a társítás lehet azonosító cél társítás vagy irányelv társítás. A kikeresési információkra akkor van szükség, ha egy leképezés kikeresési művelet egynél több cél felhasználói azonosságot adhat vissza. Ez a körülmény problémákat okozhat az olyan EIM támogatással rendelkező alkalmazások működésében, beleértve az olyan OS/400 alkalmazásokat és termékeket is, amelyek nincsenek felkészítve a kétértelmű eredmények kezelésére.

Szükség esetén a részletesebb leírás érdekében egyedi kikeresési információkat adhat meg minden egyes cél felhasználói azonossághoz. Ha kikeresési információkat ad meg a cél felhasználói azonossághoz, akkor ezeket az információkat elérhetővé kell tenni a felhasználó kikeresés művelet számára annak érdekében, hogy a művelet képes legyen egyedi cél felhasználói azonosságok visszaadására. Ellenkező esetben előfordulhat, hogy az EIM használatára támaszkodó alkalmazások nem tudják pontosan megállapítani a használandó cél azonosságot.

**Megjegyzés:** Ha nem kívánja lehetővé tenni, hogy az EIM kikeresési műveletek képesek legyenek visszaadni egynél több cél felhasználói azonosságot, akkor a kikeresési információk használata helyett alakítsa át az EIM társítások konfigurációját. További információkat az “Vállalati azonosság leképezés (EIM) hibaelhárítás: leképezési hibák” oldalszám: 114 című témakörben talál.

A cél felhasználói azonosság pontosabb leírásához szükséges kikeresési információk megadásának módja attól függ, hogy a cél felhasználói azonosság egy azonosító társításban vagy egy cél társításban szerepel. A kikeresési információk megadásának módjától függetlenül az információk a cél felhasználói azonossághoz vannak tartoznak, nem pedig azokhoz az azonosító- vagy irányelv társításokhoz, amelyekben a felhasználói azonosság szerepel.

## | **Kikeresés információk hozzáadása egy azonosító társításban található cél felhasználói azonossághoz**

| Ha kikeresési információkat kíván megadni az azonosító társításban található felhasználói azonossághoz, akkor csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi "EIM hozzáférés felügyelet" oldalszám: 34 szintek egyikére:

- | • Nyilvántartás adminisztrátor.
- | • Kijelölt nyilvántartások adminisztrátora (az a nyilvántartás meghatározás, amelyik a cél felhasználói azonosságot tartalmazó felhasználói nyilvántartásra vonatkozik).
- | • EIM adminisztrátor

| Ha kikeresési információkat kíván hozzáadni egy azonosító társításban található cél felhasználói azonossághoz, akkor tegye a következőket:

- | 1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
- | 2. Válassza ki a kezelni kívánt EIM tartományt.
  - | • Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a "Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához" oldalszám: 80 című részt.
  - | • 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 a tartományban található EIM azonosítók listájának megjelenítéséhez.

| **Megjegyzés:** Előfordulhat, hogy az **Azonosítók** mappa megnyitásakor az azonosítók listájának összeállítása hosszú ideig tart. Ha a tartományban nagy számú EIM azonosító található, akkor a művelet gyorsítása érdekében az **Azonosítók** mappa testreszabásával érdemes szűkíteni a megjelenítendő EIM azonosítók listáját. Kattintson a jobb egérgombbal az **Azonosítók** mappára, majd válassza az előugró menü **Nézet testreszabása ->Tartalmazás...** menüpontját, és adja meg a listában megjelenítendő EIM azonosítókra vonatkozó feltételeket.

- | 5. Kattintson a jobb egérgombbal az EIM azonosítóra, majd válassza az előugró menü **Tulajdonságok...** menüpontját.
- | 6. A **Társítások** lapon válassza ki azt a cél társítást, amelyhez a kikeresési információkat fel kívánja venni, majd kattintson a **Részletek...** gombra. Amennyiben segítségre szorul a mezők jelentésével kapcsolatban, kattintson a **Súgó** gombra.
- | 7. A **Társítás - részletek** párbeszédablakon a **Kikeresési információk** mezőben adja meg azokat az információkat, amelyek pontosabban azonosítják a felhasználói azonosságot a társításon belül, majd kattintson a **Hozzáadás** gombra.
- | 8. Ismétlje meg az eljárást a társításhoz hozzáadni kívánt összes kikeresési információs bejegyzéshez.
- | 9. A módosítások elmentéséhez és a **Társítás - részletek** párbeszédablakra visszatéréshez kattintson az **OK** gombra.
- | 10. A kilépéshez kattintson az **OK** gombra.

## | **Kikeresés információk hozzáadása egy irányelv társításban található cél felhasználói azonossághoz**

| Ha kikeresési információkat kíván megadni az irányelv társításban található felhasználói azonossághoz, akkor csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi "EIM hozzáférés felügyelet" oldalszám: 34 szintek egyikére:

- | • Nyilvántartás adminisztrátor.
- | • Kijelölt nyilvántartások adminisztrátora (az a nyilvántartás meghatározás, amelyik a cél felhasználói azonosságot (ID) tartalmazó felhasználói nyilvántartásra vonatkozik).
- | • EIM adminisztrátor

| Ha kikeresési információkat kíván hozzáadni egy irányelv társításban található cél felhasználói azonossághoz, akkor tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Kattintson a jobb egérgombbal a használni kívánt EIM tartományra, majd válassza az előugró menü **Leképezés irányelv...** menüpontját.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a **Csatlakozás az EIM tartományvezérlőhöz** című témakörben.
3. Az **Irányelv leképezése** párbeszédablak lapjainak segítségével megtekintheti a tartományban található irányelv társításokat.
4. Keresse meg és jelölje ki cél nyilvántartásban azt az irányelv társítást, amely a kikeresési információkkal bővítendő cél felhasználói azonosságot tartalmazza.
5. Kattintson a **Részletek...** gombra a kiválasztott társítás típusának megfelelő **Irányelv társítás - részletek** párbeszédablak megjelenítéséhez. Amennyiben segítségre szorul a mezők jelentésével kapcsolatban, kattintson a **Súgó** gombra.
6. Adja meg azokat az információkat, amelyek pontosabban azonosítják a felhasználói azonosságot az irányelv társításon belül, majd kattintson a **Hozzáadás** gombra. Ismétlje meg az eljárást a társításhoz hozzáadni kívánt összes kikeresési információs bejegyzéshez.
7. A módosítások elmentéséhez és az **Irányelv társítás - részletek** párbeszédablakra visszatéréshez kattintson az **OK** gombra.
8. A kilépéshez kattintson az **OK** gombra.

## Cél felhasználói azonosság kikeresési információinak eltávolítása

A kikeresési információk a társításban megadott cél felhasználói azonossághoz külön megadható egyedi azonosító adatok. Ez a társítás lehet azonosító cél társítás vagy irányelv társítás. A kikeresési információkra akkor van szükség, ha egy leképezés kikeresési művelet egynél több cél felhasználói azonosságot adhat vissza. Ez a körülmény problémákat okozhat az olyan EIM támogatással rendelkező alkalmazások működésében, beleértve az olyan OS/400 alkalmazásokat és termékeket is, amelyek nincsenek felkészítve a kétértelmű eredmények kezelésére.

Ezeket az információkat elérhetővé kell tenni a felhasználó kikeresés művelet számára annak érdekében, hogy a művelet képes legyen egyedi cél felhasználói azonosságok visszaadására. Azonban ha a korábban megadott kikeresési információk szükségtelenné válnak, akkor felmerülhet az igény az eltávolításukra, mivel már nem kell megadni őket a kikeresési műveletekhez.

A kikeresési információk eltávolításának módja attól függ, hogy a cél felhasználói azonosság egy azonosító társításban vagy egy cél társításban szerepel. A kikeresési információk egy cél felhasználói azonossághoz tartoznak, nem pedig ahhoz az azonosító társításhoz vagy irányelv társításhoz, amelyben a felhasználói azonosság megtalálható. Következésképpen ha kitörli a cél felhasználói azonosságot meghatározó utolsó azonosító társítást vagy irányelv társítást is, akkor a felhasználói azonosság és a kikeresési információk egyaránt törlődnek az EIM tartományból.

### Azonosító társításban található cél felhasználói azonossághoz tartozó kikeresési információk eltávolítása

Ha el kívánja távolítani az azonosító társításban található felhasználói azonossághoz tartozó kikeresési információkat, akkor csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi “EIM hozzáférés felügyelet” oldalszám: 34 szintek egyikére:

- Nyilvántartás adminisztrátor.
- Kijelölt nyilvántartások adminisztrátora (az a nyilvántartás meghatározás, amelyik a cél felhasználói azonosságot tartalmazó felhasználói nyilvántartásra vonatkozik).
- EIM adminisztrátor

Ha egy azonosító társításban található cél felhasználói azonosság A programot kívánja eltávolítani, akkor tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.

2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - 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 a tartományban található EIM azonosítók listájának megjelenítéséhez.
 

**Megjegyzés:** Előfordulhat, hogy az **Azonosítók** mappa megnyitásakor az azonosítók listájának összeállítása hosszú ideig tart. Ha a tartományban nagy számú EIM azonosító található, akkor a művelet gyorsítása érdekében az **Azonosítók** mappa testreszabásával érdemes szűkíteni a megjelenítendő EIM azonosítók listáját. Kattintson a jobb egérgombbal az **Azonosítók** mappára, majd válassza az előugró menü **Nézet testreszabása ->Tartalmazás...** menüpontját, és adja meg a listában megjelenítendő EIM azonosítókra vonatkozó feltételeket.
5. Kattintson a jobb egérgombbal az EIM azonosítóra, majd válassza az előugró menü **Tulajdonságok...** menüpontját.
6. A **Társítások** lapon válassza ki azt a cél felhasználói azonosságot tartalmazó cél társítást, amelytől el kívánja távolítani a kikeresési információkat, majd kattintson a **Részletek...** gombra.
7. A **Társítás - részletek** párbeszédablakon a válassza ki az eltávolítandó kikeresési információkat, majd kattintson az **Eltávolítás** gombra.
 

**Megjegyzés:** A program nem kér megerősítést az **Eltávolítás** gombra kattintás után.
8. A módosítások elmentéséhez és a **Társítás - részletek** párbeszédablakra visszatéréshez kattintson az **OK** gombra.
9. A kilépéshez kattintson az **OK** gombra.

#### **Irányelv társításban található cél felhasználói azonossághoz tartozó kikeresési információk eltávolítása**

Ha el kívánja távolítani az irányelv társításban található felhasználói azonosság kikeresési információit, akkor csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi “EIM hozzáférés felügyelet” oldalszám: 34 szintek egyikére:

- Nyilvántartás adminisztrátor.
- Kijelölt nyilvántartások adminisztrátora (az a nyilvántartás meghatározás, amelyik a cél felhasználói azonosságot (ID) tartalmazó felhasználói nyilvántartásra vonatkozik).
- EIM adminisztrátor

Irányelv társításban található cél felhasználói azonosság kikeresési információinak eltávolításához tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Kattintson a jobb egérgombbal a használni kívánt EIM tartományra, majd válassza az előugró menü **Leképezés irányelv...** menüpontját.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.
3. Az **Irányelv leképezése** párbeszédablak lapjainak segítségével megtekintheti a tartományban található irányelv társításokat.
4. Keresse meg és jelölje ki cél nyilvántartásban azt az irányelv társítást, amely a törlendő információkhoz tartozó cél felhasználói azonosságot tartalmazza.
5. Kattintson a **Részletek...** gombra a kiválasztott társítás típusának megfelelő **Irányelv társítás - részletek** párbeszédablak megjelenítéséhez.
6. Válassza ki az eltávolítandó kikeresési információkat, majd kattintson az **Eltávolítás** gombra.

- | **Megjegyzés:** A program nem kér megerősítést az **Eltávolítás** gombra kattintás után.
- | 7. A módosítások elmentéséhez és az **Irányelv társítás - részletek** párbeszédablakra visszatéréshez kattintson az **OK** gombra.
- | 8. A kilépéshez kattintson az **OK** gombra.

## | **EIM azonosítóhoz tartozó összes azonosító társítás megjelenítése**

| Ha meg kívánja jeleníteni az adott EIM azonosítóhoz megadott összes társítást, akkor csatlakoznia kell a megfelelő EIM tartományhoz, továbbá bizonyos “EIM hozzáférés felügyelet” oldalszám: 34 is szükséges. A Kijelölt nyilvántartások adminisztrátora kivételével bármelyik hozzáférés felügyeleti szint jogosultságot biztosít az összes társítás megtekintésére. Ez a hozzáférés felügyeleti szint csak azon nyilvántartások esetében teszi lehetővé a társítások megjelenítését, amelyekre a jogosultság kimondottan vonatkozik, kivéve ha rendelkezik az EIM leképezés kikeresési műveletek hozzáférés felügyeleti szinttel.

| Az EIM azonosítóhoz megadott társítások megjelenítéséhez tegye a következőket:

| Egy adott azonosítóhoz tartozó társítások megjelenítéséhez tegye a következőket:

- | 1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
- | 2. Válassza ki a kezelni kívánt EIM tartományt.
  - | • Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - | • Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a **Csatlakozás az EIM tartományvezerlőhöz** című témakörben.
- | 3. Bontsa ki az EIM tartományt, amelyhez csatlakozik.
- | 4. Kattintson az **Azonosítók** elemre.

| **Megjegyzés:** Előfordulhat, hogy az **Azonosítók** mappa megnyitásakor az azonosítók listájának összeállítása hosszú ideig tart. Ha a tartományban nagy számú EIM azonosító található, akkor a művelet gyorsítása érdekében az **Azonosítók** mappa testreszabásával érdemes szűkíteni a megjelenítendő EIM azonosítók listáját. Kattintson a jobb egérgombbal az **Azonosítók** mappára, majd válassza az előugró menü **Nézet testreszabása -> Tartalmazás...** menüpontját, és adja meg a listában megjelenítendő EIM azonosítókra vonatkozó feltételeket.

- | 5. Kattintson a jobb egérgombbal egy EIM azonosítóra, majd válassza az előugró menü **Tulajdonságok** menüpontját.
- | 6. Kattintson a **Társítások** lapra a kijelölt EIM azonosítóhoz társított felhasználói azonosságok listájának megjelenítéséhez
- | 7. A befejezéshez kattintson az **OK** gombra.

## | **Tartományban található összes irányelv társítás megjelenítése**

| Ha meg kívánja jeleníteni tartományhoz megadott összes irányelv társítást, akkor csatlakoznia kell a megfelelő EIM tartományhoz, továbbá bizonyos “EIM hozzáférés felügyelet” oldalszám: 34 is szükséges. A Kijelölt nyilvántartások adminisztrátora kivételével bármelyik hozzáférés felügyeleti szint jogosultságot biztosít az összes irányelv társítás megtekintésére. Ez a hozzáférés felügyeleti szint csak azon nyilvántartások esetében teszi lehetővé a társítások megjelenítését, amelyekre a jogosultság kimondottan vonatkozik. Következésképpen ezzel a hozzáférés felügyelettel csak akkor lehet az alapértelmezett tartomány irányelv társításokat megjeleníteni, ha az EIM leképezés kikeresési művelet hozzáférés felügyelet is rendelkezésre áll.

| Egy tartományhoz tartozó összes irányelv társítás megjelenítéséhez tegye a következőket:

- | 1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
- | 2. Kattintson a jobb egérgombbal a használni kívánt EIM tartományra, majd válassza az előugró menü **Leképezés irányelv...** menüpontját.
  - | • Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.

- Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezerlőhöz című témakörben.
3. A különböző lapokon a tartományban megadott irányelv társítások jelennek meg az alábbiak szerint:
    - A **Tartomány** lapon található a tartományban megadott alapértelmezett tartomány irányelv társítások listája, illetve leolvasható az, hogy a társítások engedélyezettek-e nyilvántartás szinten.
    - A **Nyilvántartás** lapon a tartományban megadott alapértelmezett nyilvántartás irányelv társítások vannak felsorolva. Azt is megtekintheti, mely forrás és cél nyilvántartásra vannak hatással az egyes irányelv társítások.
    - Az **Igazolásszűrő** lap a meghatározott és nyilvántartás szinten engedélyezett igazolásszűrő irányelv társításokat tartalmazza.
  4. A befejezéshez kattintson az **OK** gombra.

## Nyilvántartás meghatározáshoz tartozó összes irányelv társítás megjelenítése

Ha meg kívánja jeleníteni az adott nyilvántartáshoz megadott összes irányelv társítást, akkor csatlakoznia kell a megfelelő EIM tartományhoz, továbbá bizonyos “EIM hozzáférés felügyelet” oldalszám: 34 is szükséges. A Kijelölt nyilvántartások adminisztrátora kivételével bármelyik hozzáférés felügyeleti szint jogosultságot biztosít az összes irányelv társítás megtekintésére. Ez a hozzáférés felügyeleti szint csak azon nyilvántartások esetében teszi lehetővé a társítások megjelenítését, amelyekre a jogosultság kimondottan vonatkozik. Következésképpen ezzel a hozzáférés felügyelettel csak akkor lehet az alapértelmezett tartomány irányelv társításokat megjeleníteni, ha az EIM leképezés kikeresési művelet hozzáférés felügyelet is rendelkezésre áll.

Egy nyilvántartás meghatározáshoz tartozó összes irányelv társítás megjelenítéséhez tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Bontsa ki a kezelni kívánt EIM tartományt, majd válassza a **Felhasználói nyilvántartások** lehetőséget a tartományban található nyilvántartás meghatározások listájának megjelenítéséhez.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezerlőhöz című témakörben.
3. Kattintson a jobb egérgombbal a kezelni kívánt nyilvántartás meghatározásra, majd válassza az előugró menü **Leképezési irányelv...** menüpontját.
4. A különböző lapokon a nyilvántartás meghatározáshoz megadott irányelv társítások jelennek meg az alábbiak szerint:
  - A **Tartomány** lapon a nyilvántartáshoz megadott alapértelmezett tartomány irányelv társítások találhatóak.
  - A **Nyilvántartás** lapon a nyilvántartáshoz megadott és engedélyezett alapértelmezett nyilvántartás irányelv társítások vannak felsorolva.
  - Az **Igazolásszűrő** lap a nyilvántartáshoz megadott és engedélyezett igazolásszűrő irányelv társításokat tartalmazza.
5. A befejezéshez kattintson az **OK** gombra.

## Azonosító társítás törlése

Azonosító társítás törléséhez csatlakoznia kell a megfelelő EIM tartományhoz, és egy a társítás típusától függő “EIM hozzáférés felügyelet” oldalszám: 34 is.

Egy forrás vagy adminisztrációs társítás törléséhez az alábbi EIM hozzáférés felügyeleti szintek egyikére van szükség:

- Azonosító adminisztrátor.
- EIM adminisztrátor

Egy cél társítás törléséhez az alábbi EIM hozzáférés felügyeleti szintek egyikére van szükség:

- Nyilvántartás adminisztrátor.
- Kijelölt nyilvántartások adminisztrátora (az a nyilvántartás meghatározás, amelyik a cél felhasználói azonosságot tartalmazó felhasználói nyilvántartásra vonatkozik).



- EIM adminisztrátor

Azonosító társítás törléséhez tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Válassza ki a kezelni kívánt EIM tartományt.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - 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.

**Megjegyzés:** Előfordulhat, hogy az **Azonosítók** mappa megnyitásakor az azonosítók listájának összeállítása hosszú ideig tart. Ha a tartományban nagy számú EIM azonosító található, akkor a művelet gyorsítása érdekében a “Vállalati azonosság leképezés azonosítók nézetének testreszabása” oldalszám: 93 résznél található információk alapján érdemes szűkíteni a megjelenítendő EIM azonosítók listáját.

5. Kattintson a jobb egérgombbal arra az EIM azonosítóra, amelyhez a törölni kívánt társítás tartozik, majd válassza az előugró menü **Tulajdonságok...** menüpontját.
6. Kattintson a **Társítások** lapra az EIM azonosító aktuális társításainak megjelenítéséhez.
7. Válassza ki a törölni kívánt társítást, majd kattintson az **Eltávolítás** gombra a társítás törléséhez.

**Megjegyzés:** A program nem kér megerősítést az **Eltávolítás** gombra kattintás után.

8. A módosítások mentéséhez kattintson az **OK** gombra.

**Megjegyzés:** Ha eltávolít egy cél társítást, és más (irányelv vagy azonosító) társítás nincs megadva az adott cél nyilvántartáshoz, akkor a rá irányuló és a törölt társításon alapuló összes leképezés kikeresési művelet meg fog hiúsulni.

Az EIM számára egyetlen módon határozhat meg felhasználói azonosságot: egy azonosító társítás vagy irányelv társítás létrehozása során kell megadnia. Ebből következően ha egy cél társítás vagy egy irányelv társítás eltávolításával egy törli a felhasználói azonossághoz tartozó utolsó cél társítást is, akkor az adott felhasználó azonosság már nincs meghatározva az EIM számára. Ebből az is következik, hogy a felhasználói azonosság név és kikeresési információk is elvesznek.

## Irányelv társítás törlése

Egy irányelv társítás törléséhez csatlakoznia kell a megfelelő EIM tartományhoz, továbbá szüksége van az alábbi “EIM hozzáférés felügyelet” oldalszám: 34 szintek egyikére:

- Nyilvántartás adminisztrátor.
- EIM adminisztrátor

Egy irányelv társítás törléséhez tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Kattintson a jobb egérgombbal a használni kívánt EIM tartományra, majd válassza az előugró menü **Leképezés irányelv...** menüpontját.
  - Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a “Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához” oldalszám: 80 című részt.
  - Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a Csatlakozás az EIM tartományvezérlőhöz című témakörben.
3. Válassza a törölni kívánt irányelv társításnak megfelelő lapot.
4. A lapon jelölje ki a megfelelő irányelv társítást, majd kattintson az **Eltávolítás** gombra.

**Megjegyzés:** Ha rákattint az **Eltávolítás** gombra, a program nem kér megerősítést az **Eltávolítás** gombra kattintás után.

5. Kattintson az **OK** gombra a **Leképezés irányelv** párbeszédablak bezárásához és a módosítások elmentéséhez.

**Megjegyzés:** Ha eltávolít egy cél irányelv társítást, és más (irányelv vagy azonosító) társítás nincs megadva az adott cél nyilvántartáshoz, akkor a rá irányuló és a törölt irányelv társításon alapuló összes leképezés kikeresési művelet meg fog hiúsulni.

Az EIM számára egyetlen módon határozhat meg felhasználói azonosságot: egy azonosító társítás vagy irányelv társítás létrehozása során kell megadnia. Ebből következően ha egy cél társítás vagy egy irányelv társítás eltávolításával egy törli a felhasználói azonossághoz tartozó utolsó cél társítást is, akkor az adott felhasználó azonosság már nincs meghatározva az EIM számára. Ebből az is következik, hogy a felhasználói azonosság név és kikeresési információk is elvesznek.

## EIM hozzáférés felügyelet kezelése

Az EIM felhasználók olyan felhasználók, akik az előre meghatározott Egyszerűsített címtárhozzáférési protokoll (LDAP) felhasználói csoportbeli tagságuk alapján "EIM hozzáférés felügyelet" oldalszám: 34 birtokosai. Ha EIM hozzáférés felügyeletet ad meg egy felhasználóhoz, akkor a felhasználó belekerül a tartományhoz tartozó egyik LDAP felhasználói csoportba. Minden LDAP csoport különböző EIM adminisztrátori feladatok elvégzésére jogosult az adott tartományban. Az EIM felhasználó által végrehajtható adminisztratív feladatokat (beleértve a kikeresési műveleteket is) az a hozzáférés felügyeleti csoport határozza meg, amelyikbe az adott felhasználó tartozik.

Csak EIM adminisztrátori vagy LDAP adminisztrátori hozzáférés felügyelettel rendelkező felhasználók vehetnek fel más felhasználókat egy EIM hozzáférés felügyeleti csoportba vagy változtathatják meg más felhasználók hozzáférés felügyeleti beállításait. Ahhoz, hogy egy felhasználó tagja lehessen egy EIM hozzáférés felügyeleti csoportnak, rendelkeznie kell egy bejegyzéssel az EIM tartományvezérlőként működő címtár szerveren. Ezen kívül csak adott típusú felhasználók lehetnek egy EIM hozzáférés felügyeleti csoport tagjai: Kerberos azonosítók, megkülönböztetett nevek és OS/400 felhasználói profilok.

**Megjegyzés:** Ahhoz, hogy a Kerberos azonosító típusú felhasználó az rendelkezésre álljon az EIM számára, be kell állítani a hálózati hitelesítési szolgáltatást a rendszeren. Ahhoz, hogy az OS/400 felhasználói profil típus az EIM rendelkezésére álljon, be kell állítani egy rendszerobjektum utótagot a címtár szerveren. Ez lehetővé teszi a címtár szervernek, hogy OS/400 rendszerobjektumokra, például OS/400 felhasználói profilokra hivatkozzon.

Ha egy címtár szerver felhasználó hozzáférés felügyeletét szeretné módosítani vagy egy EIM hozzáférés felügyeleti csoporthoz hozzárendelni, akkor tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.

2. Válassza ki a kezelni kívánt EIM tartományt.

- Ha a kezelni kívánt EIM tartomány nem látható a **Tartománykezelés** mappában, akkor nézze meg a "Vállalati azonosság leképezés (EIM) tartomány hozzáadása a Tartománykezelés mappához" oldalszám: 80 című részt.
- Ha jelenleg nem csatlakozik a kezelni kívánt EIM tartományhoz, akkor nézze meg a szükséges útmutatásokat a **Csatlakozás az EIM tartományvezérlőhöz** című témakörben.

**Megjegyzés:** Győződjön meg róla, hogy a tartományhoz EIM adminisztrátori jogosultsággal rendelkező felhasználóval csatlakozik.

3. Kattintson a jobb egérgombbal a tesztelni kívánt EIM tartományra, majd válassza az előugró menü **Hozzáférés felügyelet...** menüpontját.

4. Az **EIM hozzáférés felügyelet szerkesztése** párbeszédablakon válassza a **Felhasználó típus** lehetőséget a felhasználó azonosítási információinak megadására szolgáló mezők megjelenítéséhez.

5. A szükséges információk megadásával azonosítsa azt a felhasználót, amelynek az EIM hozzáférés felügyeletét kezelni szeretné, majd kattintson az **OK** gombra a **EIM hozzáférés felügyelet szerkesztése** panel megjelenítéséhez. Amennyiben segítségre szorul a mezők jelentésével kapcsolatban, kattintson a **Súgó** gombra.

6. Válasszon ki egy vagy több **Hozzáférés felügyelet** csoportot, majd az **OK** gombbal adja hozzá a felhasználót a kijelölt csoportokhoz. A **Súgó** gombbal további információkhoz juthat az egyes csoportokhoz tartozó jogosultságokkal, illetve a különleges követelményekkel kapcsolatban.
7. A szükséges információk megadása után kattintson az **OK** gombra a módosítások elmentéséhez.

## EIM konfigurációs tulajdonságok kezelése

A szerver számos EIM konfigurációs tulajdonságát kezelheti. Ezt általában nem kell túl gyakran megtenni. Azonban vannak olyan helyzetek, amelyek megkövetelik a konfigurációs tulajdonságok módosítását. Ha például a rendszer leáll, és az EIM konfigurációt újra létre kell hozni, akkor futtathatja újra az EIM konfigurációs varázslót, vagy elvégezheti a módosításokat itt is. Ha például az EIM konfigurációs varázsló futtatása során nem készíti el a nyilvántartás meghatározásokat a helyi nyilvántartásokhoz, akkor ezt a későbbiekben itt teheti meg.

A megváltoztatható tulajdonságok az alábbiak:

- Az az EIM tartomány, amelyben a szerver részt vesz.
- A tartományvezérlő kapcsolat információi.
- A rendszer által az operációs rendszer funkcióinak nevében végrehajtott EIM műveletek során használt felhasználói azonosság.
- A rendszer által az operációs rendszer funkcióinak nevében végrehajtott EIM műveletek során az aktuális nyilvántartásokhoz használt nyilvántartás meghatározás nevek. Ezek a nyilvántartás meghatározás nevek a helyi felhasználói nyilvántartásokra hivatkoznak, és az EIM konfigurációs varázsló futtatása során hozhatja létre őket.

**Megjegyzés:** Ha az EIM konfigurációs varázslóval nem hozta létre a helyi nyilvántartás meghatározás neveket vagy azért, mert a nyilvántartások már meg voltak határozva az EIM számára, vagy mert a későbbi megadásuk mellett döntött, akkor frissíteni kell a rendszerkonfiguráció tulajdonságait az itt található nyilvántartás meghatározás nevekkel. A rendszernek ezekre a nyilvántartás meghatározás információkra az operációs rendszer funkcióinak nevében végrehajtott EIM műveletekhez van szüksége.

Az EIM konfigurációs tulajdonságok módosításához az alábbi különleges jogosultságokra van szüksége:

- Biztonsági adminisztrátor (\*SECADM).
- Minden objektum (\*ALLOBJ).

Az EIM konfigurációs tulajdonságok módosításához az iSeries szerveren tegye a következőket:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés** elemet.
2. Kattintson a jobb egérgombbal a **Konfiguráció** elemre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
3. Módosítsa az EIM konfiguráció információkat.
4. Amennyiben segítségre szorul a párbeszédablak mezőinek jelentésével kapcsolatban, kattintson a **Súgó** gombra.
5. A **Konfiguráció ellenőrzése** gombbal győződjön meg róla, a megadott információk felhasználásával a rendszer valóban képes-e csatlakozni az EIM tartományvezérlőhöz.
6. A módosítások mentéséhez kattintson az **OK** gombra.

**Megjegyzés:** Ha még hozott létre egy új tartományt vagy nem csatlakozott egy meglévőhöz az EIM konfigurációs varázslóval, akkor nem próbálja a konfigurációs tulajdonságok megadásával kézzel beállítani az EIM konfigurációt. A kezdeti EIM konfiguráció elkészítéséhez használja a varázslót, ezzel lehetséges konfigurációs problémákat kerülhet el, mivel a varázsló az itt megadható tulajdonságok beállításán kívül más műveleteket is elvégez.

---

## Vállalati azonosság leképezés (EIM) alkalmazásprogram illesztők

- | A Vállalati azonosság leképezés (EIM) felhasználói azonosság platformok közötti kezelésére biztosít mechanizmust.
- | Az EIM számos alkalmazásprogram illesztővel (API) rendelkezik, amelyekkel az alkalmazások EIM műveleteket hajthatnak végre az alkalmazás vagy az alkalmazás felhasználójának nevében. Az API hívások segítségével azonosság kikeresési műveletekre, különféle EIM kezelési és konfigurációs funkciókra, illetve módosítási és visszakeresési tevékenységekre van lehetőség. Ezen alkalmazásprogram illesztők mindegyike támogatott az IBM platformok között.

Az EIM API hívások 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 hívások 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

Az iSeries szerverhez rendelkezésre álló EIM alkalmazásprogram illesztők listáját és a részletes információkat a Vállalati azonosság leképezés (EIM) API hívások témakörben találja.

---

## Vállalati azonosság leképezés (EIM) hibaelhárítása

A Vállalati azonosság leképezés (EIM) számos technológiát, alkalmazást és funkciót ötvöz. Ebből következően a problémáknak számos forrásuk lehet. Az alábbi témakörökben az EIM használata során gyakran előforduló hibák leírását és az elhárításukra tett javaslatokat olvashatja.

- | • “Tartományvezérlő kapcsolat problémák hibaelhárítása”
- | • “Általános EIM konfigurációs- és tartományproblémák hibaelhárítása” oldalszám: 113
- | • “Vállalati azonosság leképezés (EIM) hibaelhárítás: leképezési hibák” oldalszám: 114

Ha a Vállalati azonosság leképezést (EIM) egyszeri bejelentkezés környezet engedélyezésére használja, akkor az Egyszeri bejelentkezés konfiguráció hibaelhárítása témakörben további hibaelhárítással kapcsolatos tippet talál.

## Tartományvezérlő kapcsolat problémák hibaelhárítása

A tartományvezérlő kapcsolatának sikertelensége számos okra vezethető vissza. Az alábbi táblázat segítségére lehet a tartományvezérlőhöz létesített kapcsolat problémáinak megoldásában.

27. táblázat: Gyakori EIM tartományvezérlő kapcsolat hibák és megoldásuk

Lehetséges hiba	Lehetséges megoldás
<p>Az iSeries navigátorban az EIM kezelése során nem lehet kapcsolódni a tartományvezérlőhöz.</p>	<p>Lehet, hogy a kezelni kívánt tartomány tartományvezérlőjéhez megadott kapcsolat információk hibásak. A tartomány kapcsolat információk ellenőrzéséhez tegye a következőket:</p> <ul style="list-style-type: none"> <li>• Bontsa ki a <b>hálózat--&gt;Vállalati azonosság leképezés--&gt;Tartománykezelés</b> csomópontot. kattintson a jobb egérgombbal a kezelni kívánt tartományra, majd válassza az előugró menü <b>Tulajdonságok</b> menüpontját.</li> <li>• Ellenőrizze, hogy a <b>Tartományvezérlő</b> neve helyesen van-e megadva, és ha a <b>Szülő DN</b> mező tartalmaz értéket, akkor annak helyességét.</li> <li>• Ellenőrizze, hogy helyesek-e a tartományvezérlő <b>Kapcsolat</b> információi. Győződjön meg róla, hogy a <b>Port</b> szám megfelelő. Ha a <b>Biztonságos kapcsolat (SSL vagy TLS) használata</b> lehetőség engedélyezve van, akkor a címtár szerveret be kell állítani az SSL használatához. A <b>Kapcsolat ellenőrzése</b> gombbal ellenőrizze, hogy a varázsló a megadott információk felhasználásával valóban képes-e csatlakozni a tartományvezérlőhöz.</li> <li>• Ellenőrizze, hogy helyesek-e a <b>Csatlakozás a tartományvezérlőhöz</b> panelen található felhasználói információk.</li> </ul>

27. táblázat: Gyakori EIM tartományvezérlő kapcsolat hibák és megoldásuk (Folytatás)

Lehetséges hiba	Lehetséges megoldás
<p>Az operációs rendszer vagy az alkalmazások nem tudnak kapcsolódni a tartományvezérlőhöz az EIM adatok elérése során. Például a rendszer nevében végrehajtott EIM leképezés kikeresési műveletek meghiúsulnak. Ez azért történhet, mert az EIM helytelenül van beállítva a rendszeren.</p>	<p>Ellenőrizze az EIM konfigurációt. Bontsa ki a <b>Hálózat--&gt;Vállalati azonosság leképezés--&gt;Konfiguráció</b> elemet azon a rendszeren, amelyen a hitelesítést próbálja elvégezni. Kattintson a jobb egérgombbal a <b>Konfiguráció</b> mappára majd válassza az előugró menü <b>Tulajdonságok</b> menüpontját és ellenőrizze az alábbiakat:</p> <ul style="list-style-type: none"> <li>• A <b>Tartomány</b> lapon: <ul style="list-style-type: none"> <li>– Ellenőrizze, hogy helyesek-e a portszámok és nincs-e elgépelve a tartományvezérlő neve</li> <li>– Kattintson a <b>Konfiguráció ellenőrzése</b> gombra annak ellenőrzéséhez, hogy a tartományvezérlő aktív-e.</li> <li>– Ellenőrizze, hogy a helyi nyilvántartás neve helyesen van-e megadva</li> <li>– Ellenőrizze, hogy a Kerberos nyilvántartás neve helyesen van-e megadva</li> <li>– Győződjön meg arról, hogy az <b>EIM műveletek engedélyezése ezen a rendszeren</b> lehetőség ki van választva</li> </ul> </li> <li>• A <b>Rendszer felhasználó</b> lapon: <ul style="list-style-type: none"> <li>– Ellenőrizze, hogy a megadott felhasználó számára az EIM hozzáférés felügyelet lehetővé teszi-e a leképezés keresések végrehajtását, és hogy érvényes jelszót adott-e meg a felhasználónak. A felhasználói hitelesítési adatok különböző típusairól az online súgóból tudhat meg többet.</li> </ul> <p><b>Megjegyzés:</b> Ha módosította a megadott rendszer felhasználó jelszavát a címtár szerveren, akkor itt is meg kell változtatnia a jelszót. Ha ezek a jelszavak nem egyeznek meg, akkor a rendszer felhasználó nem használhatja az EIM funkciókat és a leképezés kikeresési műveletek meghiúsulnak.</p> <ul style="list-style-type: none"> <li>– Kattintson a <b>Kapcsolat ellenőrzése</b> gombra a megadott felhasználói információk helyességének ellenőrzéséhez.</li> </ul> </li> </ul>
<p>A konfiguráció hibátlanak tűnik, de nem lehet csatlakozni a tartományvezérlőhöz.</p>	<ul style="list-style-type: none"> <li>• Győződjön meg róla, hogy a tartományvezérlőként szolgáló címtár szerver aktív. Ha a tartományvezérlő egy iSeries szerver, akkor az iSeries navigátorban tegye a következőket: <ol style="list-style-type: none"> <li>1. Bontsa ki a <b>Hálózat &gt; Szerverek &gt; TCP/IP</b> elemet.</li> <li>2. Győződjön meg róla, hogy a Címtár szerver állapota <b>Elindult</b>. Ha a szerver áll, akkor Kattintson a jobb egérgombbal a <b>Címtár szerver</b> bejegyzésre, majd válassza az előugró menü <b>Indítás...</b> menüpontját.</li> </ol> </li> </ul>

Miután meggyőződött róla, hogy a kapcsolat információk helyesek és a címtár szerver aktív, próbáljon meg kapcsolódni a tartományvezérlőhöz az alábbiak szerint:

1. Bontsa ki a **Hálózat > Vállalati azonosság leképezés > Tartománykezelés** elemet.
2. Kattintson a jobb egérgombbal az EIM tartományra, amelyhez csatlakozni kíván, majd válassza az előugró menü **Csatlakozás...** menüpontját.
3. Az EIM tartományvezérlőre csatlakozáshoz adja meg a felhasználó típusát, és a szükséges felhasználói információkat.
4. Kattintson az **OK** gombra.

## Általános EIM konfigurációs- és tartományproblémák hibaelhárítása

Az EIM konfigurálása és az EIM tartomány elérése közben számos általános hiba léphet fel. Az alábbi táblázat segítségével megismerkedhet a gyakori hibákkal, és javaslatokat is talál a megoldásukra.

28. táblázat: Általános EIM konfigurációs és tartomány hibák és megoldásuk

Lehetséges hiba	Lehetséges megoldás
Miután a <b>Befejezés</b> gombra kattintott, az EIM konfigurációs varázsló látszólag lefagy.	Elképzelhető, hogy a varázsló a tartományvezérlő elindulására vár. Ellenőrizze, hogy a címtár szerver indítása során történtek-e hibák. iSeries szerverek esetén ellenőrizze a QSYSWRK alrendszer QDIRSRV munkanaplóját. A munkanapló ellenőrzéséhez tegye a következőket: <ol style="list-style-type: none"> <li>1. Az iSeries navigátorban bontsa ki a <b>Jobkezelés &gt; Alrendszerek &gt; Qsyswrk</b> elemet.</li> <li>2. Kattintson a jobb egérgombbal a <b>Qdirsrv</b> bejegyzésen, majd válassza az előugró menü <b>Munkanapló</b> menüpontját.</li> </ol>
Miközben az EIM konfigurációs varázsló segítségével a tartományt hozza létre egy távoli rendszeren, a következő hibaüzenetet kapja: "A megadott szülő megkülönböztetett név (DN) érvénytelen. A megkülönböztetett névnek léteznie kell a távoli címtár szerveren. Adjon meg vagy válasszon ki egy új vagy létező szülő megkülönböztetett nevet."	A távoli nem tartományhoz megadott szülő DN nem létezik. Az "Új távoli tartomány létrehozása és csatlakozás" oldalszám: 68 részben megismerkedhet az EIM konfigurációs varázsló használatával. Továbbá olvassa el az online súgóban a tartomány létrehozásakor megadandó szülő megkülönböztetett névre vonatkozó részletes információkat.
A kapott üzenet azt jelzi, hogy a tartomány nem létezik.	Ha nem hozott létre EIM tartományt, akkor használja az EIM konfigurációs varázslót. Ez a varázsló létrehoz egy tartományt, vagy lehetővé tesz egy meglévő tartomány beállítását. Ha létrehozott egy tartományt, akkor győződjön meg róla, hogy a megadott felhasználó tagja-e egy megfelelő jogosultságokkal rendelkező "EIM hozzáférés felügyelet" oldalszám: 34 csoportnak.
A kapott üzenet azt jelzi, hogy egy EIM objektum (azonosító, nyilvántartás, társítás, irányelv társítás vagy igazolásszűrő) nem található, vagy hogy nincs jogosultsága az EIM adatok elérésére.	Ellenőrizze, hogy létezik-e az EIM objektum, és hogy a megadott felhasználó tagja-e egy megfelelő jogosultságokkal rendelkező "EIM hozzáférés felügyelet" oldalszám: 34 csoportnak.
Az <b>Azonosítók</b> mappa megnyitásakor az azonosítók listájának összeállítása hosszú ideig tart.	Ez akkor fordulhat elő, ha a tartományban nagy számú EIM azonosító található. Ennek kiküszöböléséhez adjon meg egy keresési feltételt az <b>Azonosítók</b> mappában megjelenítendő azonosítókhoz. Az EIM azonosítók megjelenésének testreszabásához tegye a következőket: <ol style="list-style-type: none"> <li>1. Az iSeries navigátorban bontsa ki a <b>Hálózat &gt; Vállalati azonosság leképezés (EIM) &gt; Tartománykezelés</b> csomópontot.</li> <li>2. Bontsa ki a tartományt, amelynek EIM azonosítóit meg kívánja jeleníteni.</li> <li>3. Kattintson a jobb egérgombbal az <b>Azonosítók</b> mappára, majd válassza az előugró menü <b>Nézet testreszabása &gt; Tartalmazás</b> menüpontját.</li> <li>4. Válassza ki az EIM azonosítók listájának készítése során alkalmazandó megjelenítési feltételeket. <b>Megjegyzés:</b> Helyettesítőkarakterként a csillag (*) használható.</li> <li>5. Kattintson az <b>OK</b> gombra.</li> </ol> <p>Az <b>Azonosítók</b> következő megnyitásakor csak a fent megadott feltételeknek megfelelő EIM azonosítók jelennek meg.</p>

28. táblázat: Általános EIM konfigurációs és tartomány hibák és megoldásuk (Folytatás)

Lehetséges hiba	Lehetséges megoldás
Az EIM kezelése során az iSeries navigátorban olyan hibaüzenetet kap, amely szerint az EIM kapcsolatazonosító a továbbiakban már nem érvényes.	A tartományvezérlő kapcsolata megszakadt. Az újracsatlakozáshoz tegye a következőket: <ol style="list-style-type: none"> <li>1. Az iSeries navigátorban bontsa ki a <b>Hálózat &gt; Vállalati azonosság leképezés (EIM) &gt; Tartománykezelés</b> csomópontot.</li> <li>2. Kattintson a jobb egérgombbal a kezelni kívánt tartományra, majd válassza az előugró menü <b>Újracsatlakozás...</b> menüpontját.</li> <li>3. Adja meg a kapcsolati információkat.</li> <li>4. Kattintson az <b>OK</b> gombra.</li> </ol>
Ha Kerberos protokollt használt az EIM hitelesítéshez, akkor a diagnosztikai üzenet a CPD3E3F munkanaplóba kerül.	Ez az üzenet akkor jön létre, ha a hitelesítés vagy az 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 sűgőjét. Érdemes tanulmányozni az Egyszeri bejelentkezés hibaelhárítás rész is.

## Vállalati azonosság leképezés (EIM) hibaelhárítás: leképezési hibák

Számos olyan gyakori hiba létezik, amelyek ahhoz vezetnek, hogy a Vállalati azonosság leképezés (EIM) egyáltalán nem, vagy nem az elvárt módon végzi a leképezéseket. Az alábbi táblázatban információkat talál arról, hogy milyen problémák okozhatják a hibás EIM leképezéseket, és lehetséges megoldási módokat is talál. Ha az EIM leképezések nem működnek megfelelően, akkor végezze el a táblázatban található összes hibaelhárítás műveletet annak érdekében, hogy az EIM leképezések hibás működésének összes okát megszüntesse.

29. táblázat: Gyakori EIM leképezési hibák és megoldásuk

Lehetséges hiba	Lehetséges megoldás
A tartományvezérlő kapcsolatinformációi hibásak vagy a tartományvezérlő nem aktív.	A Tartományvezérlő kapcsolat problémák fejezetből megtudhatja, hogy hogyan ellenőrizheti a tartományvezérlő kapcsolatinformációit, és azt, hogy aktív-e a tartományvezérlő.



29. táblázat: Gyakori EIM leképezési hibák és megoldásuk (Folytatás)

Lehetséges hiba	Lehetséges megoldás
<p>A rendszer nevében végrehajtott EIM leképezés kikeresési műveletek meghiúsulnak. Ez azért történhet, mert az EIM helytelenül van beállítva a rendszeren.</p>	<p>Ellenőrizze az EIM konfigurációt. Bontsa ki a <b>Hálózat--&gt;Vállalati azonosság leképezés--&gt;Konfiguráció</b> elemet azon a rendszeren, amelyen a hitelesítést próbálja elvégezni. Kattintson a jobb egérgombbal a <b>Konfiguráció</b> mappára majd válassza az előugró menü <b>Tulajdonságok</b> menüpontját és ellenőrizze az alábbiakat:</p> <ul style="list-style-type: none"> <li>• A <b>Tartomány</b> lapon: <ul style="list-style-type: none"> <li>– Ellenőrizze, hogy helyesek-e a portszámok és nincs-e elgépelve a tartományvezérlő neve</li> <li>– Kattintson a <b>Konfiguráció ellenőrzése</b> gombra annak ellenőrzéséhez, hogy a tartományvezérlő aktív-e.</li> <li>– Ellenőrizze, hogy a helyi nyilvántartás neve helyesen van-e megadva</li> <li>– Ellenőrizze, hogy a Kerberos nyilvántartás neve helyesen van-e megadva</li> <li>– Győződjön meg arról, hogy az <b>EIM műveletek engedélyezése ezen a rendszeren</b> lehetőség ki van választva</li> </ul> </li> <li>• A <b>Rendszer felhasználó</b> lapon: <ul style="list-style-type: none"> <li>– Ellenőrizze, hogy a megadott felhasználó számára az EIM hozzáférés felügyelet lehetővé teszi-e a leképezés keresések végrehajtását, és hogy érvényes jelszót adott-e meg a felhasználónak. A felhasználói hitelesítési adatok különböző típusairól az online súgóból tudhat meg többet.</li> </ul> <p><b>Megjegyzés:</b> Ha módosította a megadott rendszer felhasználó jelszavát a címtár szerveren, akkor itt is meg kell változtatnia a jelszót. Ha ezek a jelszavak nem egyeznek meg, akkor a rendszer felhasználó nem használhatja az EIM funkciókat és a leképezés kikeresési műveletek meghiúsulnak.</p> <ul style="list-style-type: none"> <li>– Kattintson a <b>Kapcsolat ellenőrzése</b> gombra a megadott felhasználói információk helyességének ellenőrzéséhez.</li> </ul> </li> </ul>

29. táblázat: Gyakori EIM leképezési hibák és megoldásuk (Folytatás)

Lehetséges hiba	Lehetséges megoldás
<p>Egy leképezés kikeresési művelet több cél felhasználói azonosságot eredményez. Ez a jelenség akkor lép fel, ha az alábbi feltételek valamelyike teljesül:</p> <ul style="list-style-type: none"> <li>• Egy EIM azonosítóhoz több külön cél társítás tartozik ugyanabban a cél nyilvántartásban.</li> <li>• Egynél több EIM azonosítónál szerepel forrás társításként ugyanaz a felhasználói azonosság, és noha a cél társításként megadott felhasználói azonosság különbözhet, a cél nyilvántartás szintén megegyezik.</li> <li>• Egynél több alapértelmezett tartomány irányelv társítás határozza meg ugyanazt a cél nyilvántartást.</li> <li>• Egynél több alapértelmezett nyilvántartás irányelv társítás határozza meg ugyanazt a forrás nyilvántartást és cél nyilvántartást.</li> <li>• Egynél több igazolásszűrő irányelv társítás határozza meg ugyanazt az X.509 nyilvántartást, igazolásszűrőt és cél nyilvántartást.</li> </ul>	<p>Az "EIM leképezések tesztelése" oldalszám: 82 funkcióval ellenőrizheti, hogy egy adott forrás felhasználói azonosság megfelelően leképeződik-e a cél felhasználói azonosságra. A probléma megoldásának módja függ a teszt eredményétől az alábbiak szerint:</p> <ul style="list-style-type: none"> <li>• A teszt leképezés nem kívánatos többszörös cél azonosságokat eredményez. Ez azt jelzi, hogy a tartomány társítás konfigurációja helytelen, amit az alábbiak okozhatnak: <ul style="list-style-type: none"> <li>– Egy EIM azonosító forrás vagy cél társítása nincs helyesen beállítva. Például nincs forrás társítás a Kerberos azonosítóhoz (vagy Windows felhasználóhoz), vagy létezik a társítás, de helytelen. Egy másik lehetőség, hogy a cél társítás helytelen felhasználói azonosságot határoz meg. Jelenítse meg az EIM azonosítóhoz tartozó összes azonosító társítást, és ellenőrizze az adott azonosítóhoz tartozó társításokat.</li> <li>– Egy irányelv társítás beállítása helytelen. Jelenítse meg a tartomány összes irányelv társítását, és ellenőrizze a az összes beállított irányelv társításhoz tartozó forrás és cél információkat.</li> </ul> </li> <li>• A teszt eredménye több cél azonosság, és ezek az eredmények megfelelnek a társítások beállításának. Ebben az esetben ahhoz, hogy a kikeresési művelet az összes lehetséges cél felhasználói azonosság helyett egyetlen azonosságot eredményezzen, az összes cél azonossághoz meg kell adnia a keresési információkat. Bővebb információkat a Cél felhasználói azonosság kiegészítése keresési információkkal részben talál.</li> </ul> <p><b>Megjegyzés:</b> Ez a megközelítés csak akkor működik, ha az alkalmazás számára engedélyezett a keresési információk használata. Azonban az alap OS/400 alkalmazások, mint például az iSeries Access for Windows nem használhatják a keresési információkat arra, hogy különbséget tegyenek egy kikeresési művelet több eredménye között. Ebből következően érdemes megfontolni a tartomány társításainak átdefiniálását annak érdekében, hogy a leképezés kikeresési műveletek egyetlen eredménnyel térjenek vissza, és így az alap OS/400 alkalmazások is képesek legyenek kikeresési műveletek végrehajtására és azonosságok leképezésére.</p>

29. táblázat: Gyakori EIM leképezési hibák és megoldásuk (Folytatás)

Lehetséges hiba	Lehetséges megoldás
Az EIM kikeresési műveletek nem adnak vissza eredményt, és a társítások be vannak állítva a tartományban.	<p>Az "EIM leképezések tesztelése" oldalszám: 82 funkcióval ellenőrizheti, hogy egy adott forrás felhasználói azonosság megfelelően leképeződik-e a cél felhasználói azonosságra. Győződjön meg arról, hogy helyes információkat használt a teszt során. Ha az helyes, és a teszt nem ad vissza eredményt, akkor a hiba az alábbi okok egyikéből fakad:</p> <ul style="list-style-type: none"> <li>• A társítás konfiguráció helytelen. Ellenőrizze a társítás konfigurációt az előző pontban található problémamegoldási információk segítségével.</li> <li>• Az irányelv társítás támogatás nincs engedélyezve tartományi szinten. Engedélyezze az irányelv társítást a tartományban.</li> <li>• A leképezés kikeresési műveletek támogatása vagy az irányelv társítás támogatás nem engedélyezett az egyedi nyilvántartás szinten. Engedélyezze a leképezés keresés támogatást és az irányelv társítás használatát a cél nyilvántartás számára.</li> <li>• A nyilvántartás meghatározások és a felhasználói azonosságok nem egyeznek meg a kis- és nagybetűk megkülönböztetése miatt. Törölheti és a megfelelő kis- vagy nagybetűs írásmóddal újra létrehozhatja a nyilvántartást vagy a társítást.</li> </ul>

## Vállalati azonosság leképezés (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:

- **Egyszeri bejelentkezés** Ez a témakör egyszeri bejelentkezési környezet kialakításáról és kezeléséről szól, és tartalmaz néhány példahelyzetet, amelyek szemléltetik az egyszeri bejelentkezés előnyeit.
- **Hálózati hitelesítési szolgáltatás** Ez a témakör a Hálózati hitelesítési szolgáltatással, a Kerberos protokoll iSeries megvalósításával kapcsolatos konfigurációs és egyéb információkat tartalmazza. Ha a Hálózati hitelesítési szolgáltatást úgy állítja be, hogy képes legyen együttműködni az EIM szolgáltatással, akkor létrehozhat egy egyszeri bejelentkezési környezetet a vállalatban.
- **IBM Directory Server for iSeries (LDAP)** Ez a témakör a IBM Directory Server for iSeries (LDAP) konfigurációs információit és alapelveit tárgyalja. Az EIM a címtárszervert a tartományvezérlő kiszolgálására és az EIM adatok tárolására használja.

## Az információk letöltésére és kinyomtatására vonatkozó feltételek

- | A letöltésre kiválasztott információk használatára vonatkozó engedélyt az alábbi feltételek és kikötések elfogadására szolgáló jelzés alapján kapja meg.
- | **Személyes használat:** Az információk reprodukálhatók személyes, nem kereskedelmi célú használatra, valamennyi tulajdonosi feljegyzés megtartásával. Az IBM kifejezett hozzájárulása nélkül nem szabad a kiadványokat vagy azok részeit terjeszteni, megjeleníteni, illetve belőlük származó munkát készíteni.
- | **Kereskedelmi használat:** Az információk reprodukálhatók, terjeszthetők és megjeleníthetők, de kizárólag a vállalatban belül, és csak az összes tulajdonosi feljegyzés megtartásával. Az IBM kifejezett hozzájárulása nélkül nem készíthetők olyan munkák, amelyek az információkból származnak, továbbá nem reprodukálhatók, nem terjeszthetők és nem jeleníthetők meg, még részben sem, a vállalatban kívül.

| A jelen engedélyben foglalt, kifejezetten megadott engedélyeken túlmenően az információkra, illetve a bennük  
| található adatokra, szoftverekre vagy egyéb szellemi tulajdonra semmilyen más kifejezett vagy vélelmezett engedély  
| nem vonatkozik.

| Az IBM fenntartja magának a jogot, hogy jelen engedélyeket saját belátása szerint bármikor visszavonja, ha úgy ítéli,  
| hogy a Kiadványokat az IBM érdekeit sértő módon használják fel, vagy a fenti útmutatásokat nem megfelelően  
| követik.

| Jelen információk kizárólag valamennyi vonatkozó törvény és előírás betartásával tölthetők le, exportálhatók és  
| reexportálhatók, beleértve az Egyesült Államok exportra vonatkozó törvényeit és előírásait is. AZ IBM SEMMIFÉLE  
| GARANCIÁT NEM NYÚJT AZ INFORMÁCIÓK TARTALMÁRA VONATKOZÓAN. AZ INFORMÁCIÓK  
| "ÖNMAGUKBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA VÁLLALÁSA NÉLKÜL  
| KERÜLNEK KÖZREADÁSRA, IDEÉRTVE, DE NEM KIZÁRÓLAG A KERESKEDELMI  
| ÉRTÉKESÍTHETŐSÉGRE, A SZABÁLYOSSÁGRA ÉS AZ ADOTT CÉLRA VALÓ ALKALMASSÁGRA  
| VONATKOZÓ VÉLELMEZETT GARANCIÁKAT IS.

Valamennyi anyag szerzői jogának birtokosa az IBM Corporation.

| A webhelyen található információk letöltésével vagy nyomtatásával azt jelzi, hogy elfogadja az itt leírt feltételeket és  
| kikötéseket.

---

## Megjegyzések

Ezek az információk az Egyesült Államokban forgalmazott termékekre és szolgáltatásokra vonatkoznak.

Elképzelhető, hogy a dokumentumban szereplő termékeket, szolgáltatásokat vagy lehetőségeket az IBM más országokban nem forgalmazza. Az adott országokban rendelkezésre álló termékekről és szolgáltatásokról a helyi IBM képviselők szolgálnak felvilágosítással. Az IBM termékekre, programokra vagy szolgáltatásokra vonatkozó hivatkozások sem állítani, sem sugallni nem kívánják, hogy az adott helyzetben csak az IBM termékeit, programjait vagy szolgáltatásait lehet alkalmazni. Minden olyan működésében azonos termék, program vagy szolgáltatás alkalmazható, amely nem sérti az IBM szellemi tulajdonjogát. A nem IBM termékek, programok és szolgáltatások működésének megítélése és ellenőrzése természetesen a felhasználó felelőssége.

A dokumentum tartalmával kapcsolatban az IBM-nek bejegyzett, vagy bejegyzés alatt álló szabadalmi lehetnek. Ezen dokumentum nem ad semmiféle jogos licenct ezen szabadalmakhoz. A licenckérelmeket írásban a következő címre küldheti:

- | IBM Director of Licensing
- | IBM Corporation
- | North Castle Drive
- | Armonk, NY 10504-1785
- | U.S.A.

Ha duplabyte-os (DBCS) információkkal kapcsolatban van szüksége licencre, akkor lépjen kapcsolatban az országában az IBM szellemi tulajdon osztályával, vagy írjon a következő címre:

- | IBM World Trade Asia Corporation
- | Licensing
- | 2-31 Roppongi 3-chome, Minato-ku
- | Tokyo 106-0032, Japan

**A következő bekezdés nem vonatkozik az Egyesült Királyságra, valamint azokra az országokra, amelyeknek jogi szabályozása ellentétes a bekezdés tartalmával:** AZ INTERNATIONAL BUSINESS MACHINES CORPORATION JELEN KIADVÁNYT "ÖNMAGÁBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA NÉLKÜL ADJA KÖZRE, IDEÉRTVE, DE NEM KIZÁRÓLAG A JOGSÉRTÉS KIZÁRÁSÁRA, A KERESKEDELMELI ÉRTÉKESÍTHETŐSÉGRE ÉS BIZONYOS CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁT. Bizonyos államok nem engedélyezik egyes tranzakciók kifejezett vagy vélelmezett garanciáinak kizárását, így elképzelhető, hogy az előző bekezdés Önre nem vonatkozik.

Jelen dokumentum tartalmazhat technikai, illetve szerkesztési hibákat. Az itt található információk bizonyos időnként módosításra kerülnek; a módosításokat a kiadvány új kiadásai tartalmazzák. Az IBM mindennemű értesítés nélkül fejlesztheti és/vagy módosíthatja a kiadványban tárgyalt termékeket és/vagy programokat.

A kiadványban a nem IBM webhelyek megjelenése csak kényelmi célokat szolgál, és semmilyen módon nem jelenti ezen webhelyek előnyben részesítését másokhoz képest. Az ilyen webhelyeken található anyagok nem képezik az adott IBM termék dokumentációjának részét, így ezek használata csak saját felelősségre történhet.

- | Az IBM belátása szerint bármilyen formában felhasználhatja és továbbadhatja a felhasználóktól származó információkat anélkül, hogy a felhasználó felé ebből bármilyen kötelezettsége származna.

A programlicenc azon birtokosainak, akik információkat kívánnak szerezni a programról (i) a függetlenül létrehozott programok vagy más programok (beleértve ezt a programot is) közti információcseréhez, illetve (ii) a kicserélt információk kölcsönös használatához, fel kell venniük a kapcsolatot az alábbi címmel:

- | IBM Corporation
- | Software Interoperability Coordinator, Department 49XA

| 3605 Highway 52 N  
| Rochester, MN 55901  
| U.S.A.

Az ilyen információk bizonyos feltételek és kikötések mellett állnak rendelkezésre, ideértve azokat az eseteket is, amikor ez díjfizetéssel jár.

| Az IBM a könyvben tárgyalt licencprogramokat és a hozzájuk tartozó licenc anyagokat IBM Vásárlói megállapodás,  
| IBM nemzetközi programlicenc szerződés, IBM licencszerződés gépi kódra, vagy a felek azonos tartalmú  
| megállapodása alapján biztosítja.

A dokumentumban megadott teljesítményadatok ellenőrzött környezetben kerültek meghatározásra. Ennek következtében a más működési körülmények között kapott adatok jelentősen különbözhetnek a dokumentumban megadottaktól. Egyes mérések fejlesztői szintű rendszereken kerültek végrehajtásra, így nincs garancia arra, hogy ezek a mérések azonosak az általánosan hozzáférhető rendszerek esetében is. Továbbá bizonyos mérések következtetés útján kerültek becslésre. A tényleges értékek eltérhetnek. A dokumentum felhasználóinak ellenőrizni kell az adatok alkalmazhatóságát az adott környezetben.

A nem IBM termékekre vonatkozó információk a termékek szállítójától, illetve azok publikált dokumentációiból, valamint egyéb nyilvánosan hozzáférhető forrásokból származnak. Az IBM nem tesztelte ezeket a termékeket, így a nem IBM termékek esetében nem tudja megerősíteni a teljesítményre és kompatibilitásra vonatkozó, valamint az egyéb állítások pontosságát. A nem IBM termékekkel kapcsolatos kérdéseivel forduljon az adott termék szállítójához.

Az IBM jövőbeli tevékenységére vagy szándékaira vonatkozó állításokat az IBM mindennemű értesítés nélkül módosíthatja, azok csak célokat jelentenek.

Az IBM termékekre vonatkozóan megadott árak ajánlott kiskereskedelmi árak, amelyek előzetes bejelentés nélkül változhatnak. A forgalmazók árai különbözőek lehetnek.

Jelen információk csak tervezési célokat szolgálnak. A leírtak külön értesítés nélkül megváltozhatnak az említett termék elérhetővé válásáig.

Az információk között példaként napi üzleti tevékenységekhez kapcsolódó jelentések és adatok lehetnek. A valóságot a lehető legjobban megközelítő illusztráláshoz a példákban egyének, vállalatok, márkák és termékek nevei szerepelnek. Minden ilyen név a képzelet szüleménye, és valódi üzleti vállalkozások neveivel és címeivel való bármilyen hasonlóságuk teljes egészében a véletlen műve.

Szerzői jogi licenc:

A kiadvány forrásnyelvi alkalmazásokat tartalmaz, amelyek a programozási technikák bemutatására szolgálnak a különböző működési környezetekben. A példaprogramokat tetszőleges formában, az IBM-nek való díjfizetés nélkül másolhatja, módosíthatja és terjesztheti fejlesztési, használati, eladási vagy a példaprogram operációs rendszer alkalmazásprogram illesztőjének megfelelő alkalmazásprogram terjesztési céllal. A példák nem kerültek minden helyzetben tesztelésre. Az IBM így nem tudja garantálni a megbízhatóságukat, javíthatóságukat vagy a program funkcióit.

| Az IBM, A PROGRAMFEJLESZTŐK ÉS A FORGALMAZÓK AZ ÉRVÉNYES JOGSZABÁLYOK ÁLTAL  
| MEGENGEDETT LEGNAGYOBB MÉRTÉKBEN ELHÁRÍTANAK MINDEN KIFEJEZETT VAGY  
| VÉLELMEZETT GARANCIÁT VAGY FELTÉTELT, IDEÉRTVE, DE EZZEL EGYEBEKET NEM KIZÁRVA A  
| FORGALMAZHATÓSÁGRA, HASZNÁLHATÓSÁGRA, EGY ADOTT CÉLRA VALÓ ALKALMASSÁGRA  
| VONATKOZÓ VÉLELMEZETT GARANCIÁKAT ÉS FELTÉTELEKET, FÜGGŐEN A PROGRAMTÓL,  
| ILLETVE A TECHNIKAI TÁMOGATÁSTÓL, AMENNYIBEN ILYEN LÉTEZIK.

| Az IBM, ANNAK PROGRAMFEJLESZTŐI VAGY SZÁLLÍTÓI SEMMILYEN KÖRÜLMÉNYEK KÖZÖTT NEM  
| FELELŐSEK A KÖVETKEZŐKÉRT, MÉG AKKOR SEM, HA TUDOMÁSUK VOLT EZEK  
| BEKÖVETKEZÉSÉNEK LEHETŐSÉGÉRŐL:

- | 1. ADATOK SÉRÜLÉSE VAGY ELVESZTÉSE,
- | 2. KÜLÖNLEGES, JÁRULÉKOS, KÖZVETETT VAGY BÁRMILYEN KÖVETKEZMÉNYES GAZDASÁGI KÁROK, ILLETVE
- | 3. NYERESÉG, ÜZLETMENET, BEVÉTEL, VEVŐKÖZÖNSÉG VAGY VÁRT MEGTAKARÍTÁSOK CSÖKKENÉSE.

| EGYES JOGRENDSZEREK NEM ENGEDÉLYEZIK A JÁRULÉKOS VAGY KÖVETKEZMÉNYES KÁROK KIZÁRÁSÁT VAGY KORLÁTOZÁSÁT, ILYENKOR AZ ÉRINTETT FELHASZNÁLÓRA A FENTI KORLÁTOZÁSOK VAGY KIZÁRÁSOK NÉMELYIKE NEM VONATKOZIK.

Jelen példaprogramok minden másolatának, leszármazottjának vagy kódrészletének tartalmaznia kell a következő szerzői jogi megjegyzést:

© (IBM) (2004). A kód bizonyos részei az IBM Corp. példaprogramjaiból származnak. Példaprogramok. © Copyright IBM Corp. 2004. Minden jog fenntartva.

Ha az információkat elektronikus formában tekinti meg, akkor elképzelhető, hogy a fotók és színes ábrák nem jelennek meg.

---

## Védjegyek

A következő kifejezések az International Business Machines Corporation védjegyei az Egyesült Államokban és/vagy más országokban:

AIX  
Distributed Relational Database Architecture  
Domino  
DRDA  
e(logó)server  
eServer  
IBM  
iSeries  
OS/400  
pSeries  
RACF  
RDN  
Tivoli  
WebSphere  
xSeries  
z/OS  
zSeries

- | A Lotus, a Lotus Notes, a Freelance és a WordPro az International Business Machines Corporation és a Lotus Development Corporation védjegyei az Egyesült Államokban és/vagy más országokban.

A Microsoft, a Windows, a Windows NT és a Windows logó a Microsoft Corporation védjegye az Egyesült Államokban és/vagy más országokban.

A UNIX a The Open Group bejegyzett védjegye az Egyesült Államokban és más országokban.

Más cégek, termékek és szolgáltatások nevei mások védjegyei vagy szolgáltatás védjegyei lehetnek.

---

## Az információk letöltésére és kinyomtatására vonatkozó feltételek

- | A letöltésre kiválasztott információk használatára vonatkozó engedélyt az alábbi feltételek és kikötések elfogadására szolgáló jelzés alapján kapja meg.
- | **Személyes használat:** Az információk reprodukálhatók személyes, nem kereskedelmi célú használatra, valamennyi tulajdonosi feljegyzés megtartásával. Az IBM kifejezett hozzájárulása nélkül nem szabad a kiadványokat vagy azok részeit terjeszteni, megjeleníteni, illetve belőlük származó munkát készíteni.
- | **Kereskedelmi használat:** Az információk reprodukálhatók, terjeszthetők és megjeleníthetők, de kizárólag a vállalaton belül, és csak az összes tulajdonosi feljegyzés megtartásával. Az IBM kifejezett hozzájárulása nélkül nem készíthetők olyan munkák, amelyek az információkból származnak, továbbá nem reprodukálhatók, nem terjeszthetők és nem jeleníthetők meg, még részben sem, a vállalaton kívül.
- | A jelen engedélyben foglalt, kifejezetten megadott engedélyeken túlmenően az információkra, illetve a bennük található adatokra, szoftverekre vagy egyéb szellemi tulajdonra semmilyen más kifejezett vagy vélelmezett engedély nem vonatkozik.
- | Az IBM fenntartja magának a jogot, hogy jelen engedélyeket saját belátása szerint bármikor visszavonja, ha úgy ítéli, hogy a Kiadványokat az IBM érdekeit sértő módon használják fel, vagy a fenti útmutatásokat nem megfelelően követik.
- | Jelen információk kizárólag valamennyi vonatkozó törvény és előírás betartásával tölthetők le, exportálhatók és reexportálhatók, beleértve az Egyesült Államok exportra vonatkozó törvényeit és előírásait is. AZ IBM SEMMIFÉLE GARANCIÁT NEM NYÚJT AZ INFORMÁCIÓK TARTALMÁRA VONATKOZÓAN. AZ INFORMÁCIÓK "ÖNMAGUKBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA VÁLLALÁSA NÉLKÜL KERÜLNEK KÖZREADÁSRA, IDEÉRTVE, DE NEM KIZÁRÓLAG A KERESKEDELMI ÉRTÉKESÍTHETŐSÉGRE, A SZABÁLYOSSÁGRA ÉS AZ ADOTT CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁKAT IS.

Valamennyi anyag szerzői jogának birtokosa az IBM Corporation.

- | A webhelyen található információk letöltésével vagy nyomtatásával azt jelzi, hogy elfogadja az itt leírt feltételeket és kikötéseket.







Nyomtatva Dániában