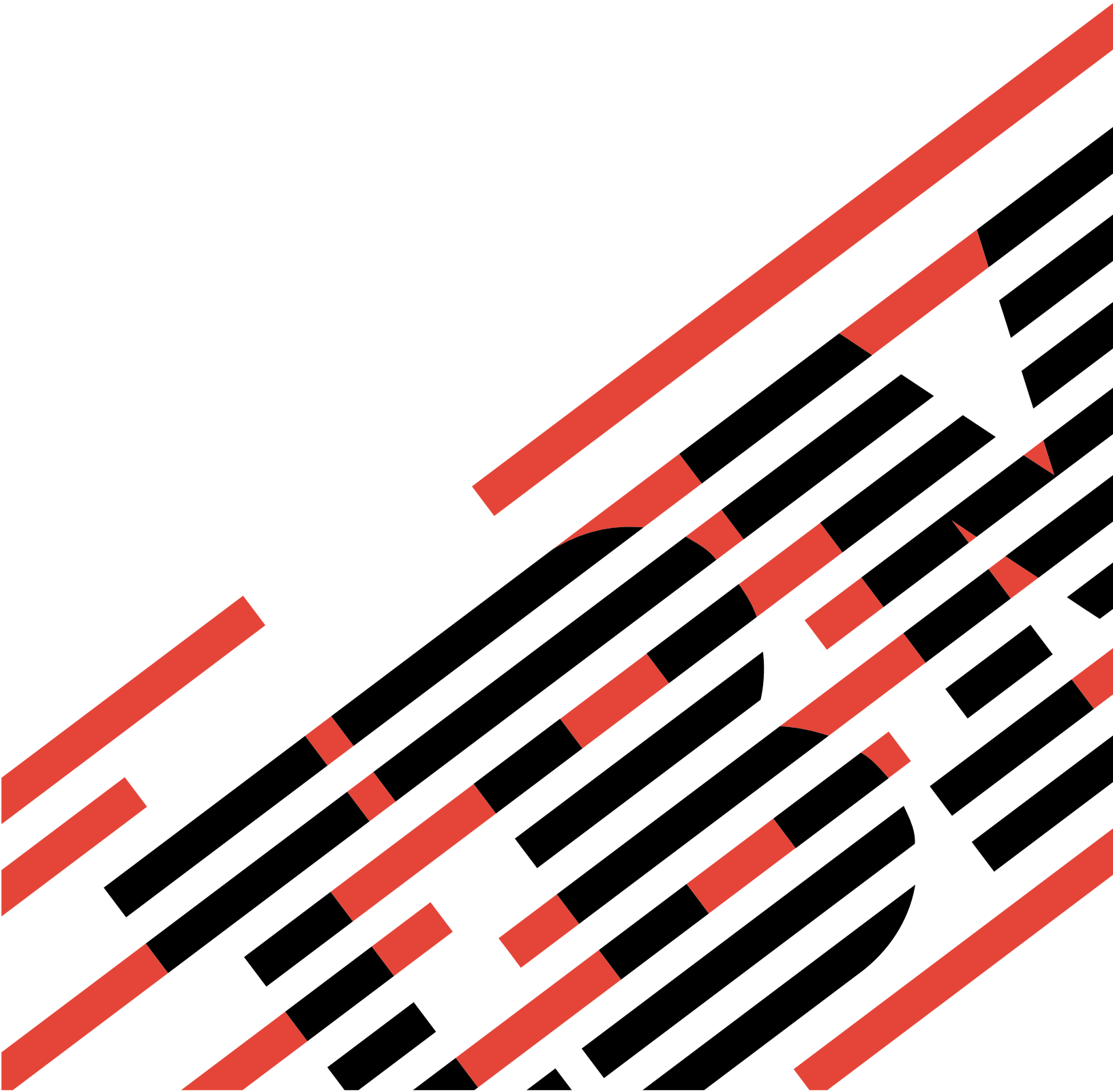
IBM

eserver

iSeries

Címtár szolgáltatások (LDAP)



IBM

@server

iSeries

Címtár szolgáltatások (LDAP)

Tartalom

Rész 1. Címtár szolgáltatások (LDAP)

A Címtár szolgáltatás Lightweight Directory Access Protocol (LDAP) szervert biztosít az iSeries szerveren. Az LDAP TPC/IP (Transmission Control Protocol/Internet Protocol) felett fut, és népszerű címszolgáltatás úgy az Internetre, mint a nem-Internetre készült alkalmazások körében.

Ha ismeri a Címtár szolgáltatás terméket, előfordulhat, hogy először szeretne megismerkedni ezen kiadás újdonságaival. Ha úgy kívánja, kinyomtathatja vagy megjelenítheti a Címtár szolgáltatás információk PDF változatát.

A következő témakörök bemutatják a Címtár szolgáltatás terméket, és információt nyújtanak, melyek segítenek az LDAP szerver adminisztrálásához az iSeries szerveren:

A Címtár szolgáltatás termékről további tájékoztatást kaphat, ha meglátogatja a Címtár szolgáltatás weblapot  .

A Címtár szolgáltatás által nyújtott LDAP szerver valójában egy IBM SecureWay Directory  .

Fejezet 1. A V5R2 újdonságai

A Címtár szolgáltatások a következő továbbfejlesztésekkel és új szolgáltatásokkal rendelkezik:

- A Címtár szolgáltatás az alap operációs rendszer része lett a V5R1 változatban. A V5R2 változattól kezdve a 32-es opció megszűnt.
- A tárolt adatok védelme érdekében új biztonsági javításokkal bővült a címtár szolgáltató.
- Az LDAP címtár szolgáltató tartományvezérlőként működhet az Enterprise Identity Mapping (EIM) tartomány számára.
- A rendszergazdák számára egy új opció van, amivel adminisztrátori hozzáférést adhat a címtár szolgáltatóhoz azoknak a felhasználóknak, akiknek hozzáférése van az operációs rendszer Directory Services Administrator (QIBM_DIRSRV_ADMIN) funkció azonosítójához (ID) az iSeries navigátor alkalmazás támogatásán keresztül.
- Választhat, hogy a címtár szolgáltató adott IP címeket használjon-e, vagy a szerveren konfigurált összes IP címet. “Port vagy IP cím módosítása” oldalszám: 21 helyen további tájékoztatást kaphat.
- Az **ldap_set_option** API új hibakeresési funkcióval bővült a V5R2 változatban. Az LDAP_OPT_DEBUG opcióval segítheti az LDAP C API-kat használó kliensekkel kapcsolatos hibák diagnosztizálását. További információk: “Hibák nyomkövetése az LDAP_OPT_DEBUG opcióval” oldalszám: 67, vagy a Címtár szolgáltatás API-k című témakör az iSeries Információs központban .

Az újdonságok és a változások követése:

A változások könnyebb kikeresése érdekében az alábbi jelzéseket használjuk:

- A » jel ott látható, ahol az új vagy a megváltozott információ kezdődik.
- A « jel ott látható, ahol az új vagy a megváltozott információ véget ér.

Fejezet 2. A témakör nyomtatása

A PDF verzió megtekintéséhez illetve letöltéséhez valassza ki a Címtár szolgáltatások (LDAP) elemet (kb. 323 KB vagy 66 oldal).

Egyéb információk

Megtekintheti, illetve letöltheti a következő anyagokat is:

- *LDAP Implementation Cookbook* .
- *Understanding LDAP* .
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino*
- *Implementation and Practical Use of LDAP on the iSeries Server* .

A PDF fájl mentése munkaállomásra megjelenítés vagy nyomtatás céljából:
1. Nyissa meg a PDF fájlt böngészőjében (kattintson a fenti hivatkozásra).
2. A böngésző menüjében kattintson a **File** menüre.
3. Kattintson a **Save As...** menüpontra.
4. Keresse meg azt az alkönytárt, ahová a PDF fájlt menteni szeretné.
5. Kattintson **Save** menüpontra.

Az Adobe Acrobat Reader letöltése

Ha szüksége van az Adobe Acrobat Reader programra a PDF fájlok megtekintéséhez vagy nyomtatásához, töltse le egy példányát az Adobe webhelyéről (www.adobe.com/products/acrobat/readstep.html) .

Fejezet 3. Első lépések a Címtár szolgáltatás használatában

A Címtár szolgáltatás Lightweight Directory Access Protocol (LDAP) szervert biztosít az iSeries szerveren. Az LDAP TPC/IP (Transmission Control Protocol/Internet Protocol) felett fut, és egyre népszerűbb címszolgáltatás úgy az Internetre, mint a nem-Internetre készült alkalmazások körében. Az OS/400 rendszeren alapuló LDAP címtár szolgáltató legtöbb beállítási és adminisztrációs feladatát az iSeries navigátor grafikus felhasználói felületén (GUI) lehet megoldani. A Címtár szolgáltatás kezeléséhez szükség van arra, hogy az iSeries szerverhez csatlakoztatott PC-n telepítve legyen az iSeries navigátor. A Címtár szolgáltatás szolgáltatásait LDAP-re felkészített alkalmazások használják ki, mint például az olyan levelező rendszerek, amelyek LDAP szerveren keresik ki az e-mail címeket.

Az LDAP szerver mellett a Címtár szolgáltatás az alábbi összetevőket foglalja magában:

- OS/400 rendszeren alapuló LDAP kliens. Ez a kliens egy sor alkalmazásprogram csatolót (application program interface, API) tartalmaz, amelyeket sajátfejlesztésű OS/400 programban is fel lehet használni kliens alkalmazások létrehozásához. Ezekről az API-król információt talál az iSeries Információs központ Programozás fejezetének Címtár szolgáltatások témájánál.
- Az IBM SecureWay Directory Client Software Development Kit (SDK) 3.2 verziója. Az SDK magában foglalja a Windows LDAP klienst és a következő eszközöket:
  - Az IBM SecureWay Directory Management Tool nevű eszközt, ami egy grafikus felhasználói felületet biztosít a címtár tartalmának kezeléséhez.
  - Parancssori segédprogramokat (ldapsearch, ldapadd, stb.)
  - C LDAP API-kat (könyvtári állományokat, fejlécállományokat, és minta forráskódot)
  - IBM JNDI LDAP szerviz szolgáltatót (ibmjndi.jar)
  - Online dokumentációt az összes előző tétel részére. Lásd ezen hely ″readme″ állományát, és ezen HTML állományok nevét.

Ha a Címtár szolgáltatás terméket korábbi verziójú OS/400 rendszerrel használja, akkor olvassa el az “Áttérés V5R2 változatra egy korábbi Címtár szolgáltatás változatról” oldalszám: 11 helyen leírtakat.

Alapvető tájékoztatást nyújt az LDAP szolgáltatásairól “Az LDAP alapjai” oldalszám: 8 fejezet. Ha más platformon használt már LDAP szerveket, célszerű néhány percet az itt leírtak elolvasására szánni, mert több OS/400-specifikus információt tartalmaz.

Az alapvető ismeretek elsajátítása után továbbléphet az “LDAP címtár szolgáltató telepítésének előkészítése” oldalszám: 11 fejezetre.

Címtár szolgáltatások telepítésével és konfigurálásával kapcsolatban további tájékoztatást talál “A Címtár szolgáltatás telepítése és konfigurálása” oldalszám: 14 fejezetben.

Dokumentáció

Az Információs központ Címtár szolgáltatás című témaköre áttekintést nyújt az LDAP szolgáltatásairól, kifejezetten pedig az OS/400 rendszer LDAP címtár szolgáltatójának kezelésével foglalkozik. A dokumentáció a SecureWay Directory Client SDK teljes dokumentációját is magában foglalja. További LDAP információkért nézze meg az LDAP kézikönyveket, mint például a következőket:

- *LDAP Implementation Cookbook* .
- *Understanding LDAP* .
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino* .

- *Implementation and Practical Use of LDAP on the iSeries server* .
- *LDAP: Programming Directory-enabled Applications with Lightweight Directory Access Protocol* - Tim Howes és Mark Smith szerzeménye.
- *Understanding and Deploying LDAP Directory Services* - Mark C. Smith, Gordon S. Good és Tim Howes szerzeménye.

Az iSeries szerveren futó Címtár szolgáltatás termékről további információkat szerezhet az iSeries server Directory Services honlapon .

Megjegyzés: Ezen ismertetésben megjelenő egyes részek a Michigani Egyetemen (University of Michigan) készült LDAP dokumentációból származnak. Szerzői jog © 1992-1996, Regents of the University of Michigan. Minden jog fenntartva.

Az LDAP alapjai

Az egyszerűsített könyvtárhozzáférési protokoll (Lightweight Directory Access Protocol, LDAP) olyan címtár szolgáltatási protokoll, amely TCP/IP (Transmission Control Protocol/Internet Protocol) felett fut. Az LDAP 2. verziója az Internet Engineering Task Force (IETF) Request for Comments (RFC) 1777 alatt lett formálisan meghatározva, *Lightweight Directory Access Protocol*. Az LDAP 3. verziója az IETF RFC 2251, *Lightweight Directory Access Protocol (v3)* alatt van formálisan meghatározva. Ezeket az RFC-ket megtekintheti az Interneten a következő címen:

http://www.ietf.org

Az LDAP címtár szolgáltató kliens/szerver modellt követ. Egy vagy több LDAP szerver tartalmazza a címtár adatait. Az LDAP kliens az LDAP szerverhez kapcsolódik és kérést nyújt be. A szerver választ ad vissza, vagy egy mutatót, amelyik egy másik szerverre utal.

Az LDAP felhasználási lehetőségei:

Mivel az LDAP címtár szolgáltatás és nem adatbázis, az LDAP címtárban található információ általában leíró, attribútum alapú információ. Az LDAP felhasználók általában sokkal gyakrabban olvassák a címtárban lévő információt, mint ahogy azt módosítani szokták. A frissítések jellemzően mindent - vagy - semmit változtatások. Az LDAP címtárak jellemző felhasználása az online telefonkönyvek és e-mail címtárak területén van.

Az LDAP címtár struktúrája:

Az LDAP címtár szolgáltatási modell **bejegyzések**en alapul (amelyeket gyakran **objektumok**nak is nevezünk). Minden egyes bejegyzés egy vagy több **attribútum**ot (mint pl. egy név vagy cím) és egy **típus**t tartalmaz. A típusok általában emlékeztető rövidítésekből állnak, mint pl. cn = common name (általános név) vagy mail = e-mail cím.

A minta címtárban Tim Jones bejegyzése látható, ami egy *mail* és egy *telephoneNumber* attribútumot tartalmaz (Ábra: 1 oldalszám: 10). Néhány más attribútum is lehetne még, például *fax*, *title* (beosztás), *sn* (keresztnév), vagy *jpegPhoto*.

Minden egyes címtárnak van egy **sémája**, ez olyan szabályok gyűjteménye, amelyek meghatározzák a címtár struktúráját és tartalmát. Az LDAP szerver séma fájljait az IBM SecureWay Directory Management Tool (DMT) segítségével szerkesztheti. A Címtár szolgáltatás telepítése után a fájlok helye a /QIBM/UserData/OS400/DirSrv könyvtár.

Megjegyzés: Az alapértelmezés szerint a séma-fájlok eredeti példányainak helye a /QIBM/ProdData/OS400/DirSrv könyvtár. Ha a UserData könyvtárban levő fájlokat kívánja lecserélni, bemásolhatja őket a /QIBM/ProdData/OS400/DirSrv könyvtárba.

Mindegyik címtári bejegyzésnek van egy **objectClass** nevű különleges attribútuma. Ez az attribútum szabályozza, mely attribútumok kötelezőek és megengedettek egy bejegyzésben. Más szóval, az objectClass attribútum értékei határozzák meg azokat a séma-szabályokat, amelyeknek egy bejegyzés engedelmeskedni tartozik.

Minden egyes címtári bejegyzésnek még vannak következő **operációs attribútumai**, melyeket az LDAP szerver automatikusan karbantart:

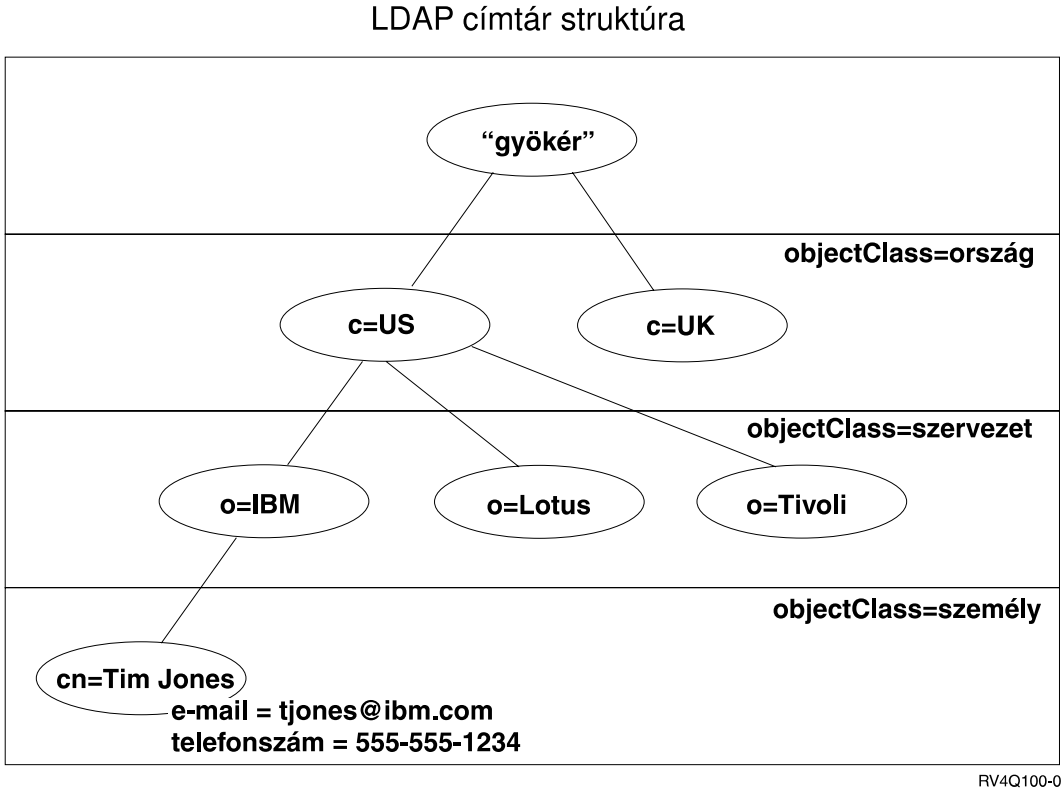
- CreatorsName, amely a bejegyzés létrehozásakor használt kötött DN-t tartalmazza.
- CreateTimestamp, amely a bejegyzés létrehozási időpontját tartalmazza.
- modifiersName, amely a bejegyzés utolsó módosításakor használt kötött DN-t tartalmazza (kezdetben ez megegyezik a CreatorsName nevével).
- modifyTimestamp, amely a bejegyzés utolsó módosításának időpontját tartalmazza (kezdetben ez megegyezik a CreateTimestamp időponttal).

Hagyományosan, az LDAP címtári bejegyzések hierarchikus struktúrába rendeződnek, amely politikai, földrajzi, vagy szervezeti határokat tükröz (Ábra: 1 oldalszám: 10). Az országokat képviselő bejegyzések a hierarchia tetején jelennek meg. Az államokat vagy nemzeti szervezeteket képviselő bejegyzések a hierarchia második szintjét foglalják el. Az alattuk található bejegyzések képviselhetnek embereket, szervezeti egységeket, nyomtatókat, dokumentumokat és más elemeket.

A címtár szerkezetének kialakításakor nincs a hagyományos hierarchiára korlátozva. Például a tartomány komponens struktúra nagyobb népszerűségnek örvend. Az ilyen struktúránál a bejegyzések a TCP/IP tartománynevek részeiből állnak. Például a dc=ibm,dc=com név előnyösebb az o=ibm,c=us névnél.

Az LDAP a bejegyzésekre **megkülönböztető nevekkel (Distinguished Names, DN-ek)** hivatkozik. Egy megkülönböztető név tartalmazza magának a bejegyzésnek a nevét, csakúgy, mint a címtárban felette álló objektumok nevét lentről felfelé. Például, az Ábra: 1 oldalszám: 10 bal alsó sarkában található bejegyzés teljes DN-je cn=Tim Jones, o=IBM, c=US. Mindegyik bejegyzésnek legalább egy attribútuma van, amely a bejegyzést megnevezi. Ezt a megnevező attribútumot a bejegyzés **relatív megkülönböztető nevének** (Relative Distinguished Name, RDN) hívjuk. Az adott RDN feletti bejegyzés neve **szülő megkülönböztető név**. A fenti példában cn=Tim Jones megnevezi a bejegyzést, vagyis ez egy RDN. Az o=IBM, c=US a szülő DN a cn=Tim Jones számára.

Ha azt akarjuk, hogy az LDAP szerver az LDAP címtár egy részét kezelje, meg kell adni a legmagasabb szintű szülő megkülönböztető neveket a szerver konfigurációjában. Ezeket a megkülönböztető neveket **utótagok**nak hívjuk. A szerver az összes olyan objektumot el tudja érni a címtárban, amelyek a megadott utótag alatt vannak a címtár hierarchiájában. Például, ha egy LDAP szerver az Ábra: 1 oldalszám: 10 alatt látható címtárt tartalmazná, akkor az o=ibm, c=us utótagot kellene megadni a konfigurációjában, hogy képes legyen a Tim Jones-ra vonatkozó lekérdezéseket kielégíteni.



Ábra: 1. Alapvető LDAP címtár struktúra

Megjegyzések az LDAP és a Címtár szolgáltatás termékekhez:

- A V4R5 változattól kezdve az OS/400 LDAP szerver és az OS/400 LDAP kliens az LDAP V3 verzión alapszik. A V2 klienst használhatja V3 szerverrel. Azonban nem használhatja a V3 klienst a V2 szerverrel mindaddig, amíg V2 kliensként rendeli hozzá, és csak V2 API-kat használ. További tájékoztatást kaphat az LDAP V2/V3 megfontolások című részben.
- A Windows LDAP kliens ugyancsak az LDAP V3 változaton alapszik.
- Mivel az LDAP egy szabvány, az összes LDAP szerver közös alapvető jellemzőkkel rendelkezik. Azonban megvalósításbeli különbségek miatt nem teljesen kompatíbilisek egymással. A Címtár szolgáltatás által is szolgáltatott LDAP szerver szorosan kompatíbilis az IBM SecureWay Directory és az IBM Directory termékcsaládban rendelkezésre álló szerverekkel. Más LDAP szerverekkel kapcsolatban azonban elképzelhető, hogy nem ennyire kompatíbilis.
- A Címtár szolgáltatás által az LDAP szerver részére szolgáltatott adatok egy OS/400 adatbázisban találhatók.

További információk

LDAP címtárak használatával kapcsolatban a következők tartalmaznak példákat:

- *Understanding LDAP* című vörös könyv 1.6 The Quick Start: A Public LDAP Example szakasza.
- Understanding LDAP című vörös könyv 3.3 Example Scenarios szakasza.

Az LDAP alapfogalmaival kapcsolatban lásd Fejezet 5, “Címtár szolgáltatás: koncepciók és hivatkozások” oldalszám: 35.

Megfontolások az LDAP V2 használatához LDAP V3 esetén

A V4R5 változattól kezdve az OS/400 LDAP szerver és az OS/400 LDAP kliens az LDAP V3 változaton alapul. A V3 klienst nem használhatja a V2 szerverrel. Mindazonáltal használhatja az ldap_set_option() API-t a V3 kliens V2 változatra történő módosításához. Ezt követően sikeresen elküldheti a kliens kéréseit a V2 szervernek.

A V2 klienst használhatja V3 szerverrel. Gondoljon azonban arra, hogy a keresési kérés esetében a V3 szerver az UTF-8 formátum teljes tartományát felölelő adatokat küldhet vissza, miközben a V2 kliens lehet, hogy csak IA5 karakterkészletben lévő adatokat tud kezelni.

Megjegyzés: Az LDAP 2. verziója az Internet Engineering Task Force (IETF) Request for Comments (RFC) 1777 alatt lett formálisan meghatározva, *Lightweight Directory Access Protocol*. Az LDAP 3. verziója az IETF RFC 2251, *Lightweight Directory Access Protocol (v3)* alatt van formálisan meghatározva. Ezeket az RFC-ket megtekintheti az Interneten a következő címen:

http://www.ietf.org

LDAP címtár szolgáltató telepítésének előkészítése

Mielőtt a Címtár szolgáltatás telepítését és az LDAP címtár konfigurálását elkezdené, fordítson egy pár percet a címtár megtervezésére. Célszerű figyelembe venni az alábbi dolgokat:

- **A címtár kialakítása**. Tervezze meg a címtár szerkezetét és döntse el, milyen utótagok és attribútumok szükségesek a címtár szolgáltató működéséhez.
- **A címtár méretének eldöntése**. Megbecsülheti, hogy mekkora tárolóhelyre van szüksége. A címtár mérete a következőktől függ:
  - Az attribútumok száma a szerver sémájában.
  - A címtárban levő bejegyzések száma.
  - A szerveren tárolt információ típusa.

  Például egy üres címtár körülbelül 10 MB tárolóterületet igényel, ha az a Címtár szolgáltatás alapértelmezett sémáját használja. Egy, az alapértelmezett sémát használó címtár, amely 1000 bejegyzést tartalmaz tipikus munkavállalói információval, megközelítőleg 30 MB tárolóterületet igényel. Ez a szám függ a használt attribútumoktól. Sokkal több lesz akkor is, ha nagyméretű objektumokat, pl. képeket, szándékozik tárolni.
- **Az alkalmazandó biztonsági intézkedések eldöntése**. A Címtár szolgáltatás támogatja a Védett socket réteg (SSL) és a digitális igazolások, valamint a kommunikáció biztonsága érdekében a Fordítási réteg biztonság (TLS) használatát. A V5R1 változattól kezdve a Kerberos hitelesítés ugyancsak támogatott.
- A Címtár szolgáltatás megengedi, hogy hozzáférés vezérlési listák (ACL-ek) segítségével szabályozzák a címtár objektumaihoz való hozzáférést. A címtár védelmére használhatja az OS/400 biztonság ellenőrzést.

Áttérés V5R2 változatra egy korábbi Címtár szolgáltatás változatról

Az OS/400 V5R2 verziójában új Címtár szolgáltatássok és lehetőségek kerültek bevezetésre. Ezek a változtatások érintik az LDAP címtár szolgáltatót és az iSeries navigátor grafikus felhasználói kezelőfelületét (GUI-t). Ahhoz, hogy kihasználhassa az új GUI lehetőségeit, telepítenie kell az iSeries navigátor programot egy olyan PC-re, ami TCP/IP-n keresztül kommunikál az iSeries szerverrel. Az iSeries navigátor az iSeries Access for Windows egyik részeleme. Ha telepítve van az iSeries navigátor egy korábbi verziója, akkor azt V5R2 verzióra kell frissíteni.

Az OS/400 V5R2 verziója támogatja a V4R5 és a V5R1 verzió frissítését. Ha az OS/400 V5R2 verziójára történik a frissítés, akkor az LDAP címtári adatok és a címtár séma fájlok úgy kerülnek áthelyezésre, hogy

formátumuk meg fog felelni a V5R2 formátumnak. Ha van egy Címtár szolgáltatás LDAP szervere, ami az OS/400 V4R3 vagy V4R4 verziója alatt működik, és erről akar V5R2 változatra váltani, néhány további áthelyezési feladatot is el kell végeznie.

Ha az OS/400 V5R2 verziójára frissít, pár áthelyezési kérdést kell figyelembe venni:

- Amikor V5R2 verzióra frissít, a Címtár szolgáltatás automatikusan áthelyezi a séma fájlokat a V5R2 verzióba, majd törli a régi séma fájlokat. Azonban, ha törölte vagy átnevezte a séma fájlokat, a Címtár szolgáltatás nem tudja áttelepíteni őket. Lehet, hogy hibaüzenetet kap, vagy a Címtár szolgáltatás feltételezi, hogy a fájlok már áttelepítésre kerültek.
- A Címtár szolgáltatás V5R2 formátumba helyezi át a címtári adatokat a szerver első indításakor vagy egy LDIF fájl importálásakor. Szánjon bizonyos időt az áttelepítés elvégzésére. Ha V4R4 verzióról vagy egy korábbi verzióról frissít, vegye figyelembe, hogy a V5R2 verzióban a címtári adatok elhelyezésére a korábbinál körülbelül kétszer több memória helyre lesz szüksége. Ez azért van, mert a Címtár szolgáltatás csak az IA5 karakterkészletet támogatta a V4R4 és korábbi verzióban, és az adatokat CCSID 37 (egybyte-os formátum) azonosító szerint mentette. A Címtár szolgáltatás támogatja a teljes ISO 10646 karakter készletet.

  Miután V5R2 verzióra frissített, indítsa el legalább egyszer szerverét, hogy a létező adatok áthelyezésre kerüljenek, mielőtt új adatokat importálna. Ha megpróbál adatokat importálni a szerver indítása előtt, és nem rendelkezik elegendő jogosultsággal, akkor az import meghiúsulhat.
- A Címtár szolgáltatás V4R4 verziója és korábbi verziói nem vették figyelembe az időzónákat, amikor létrehozták az időpecséteket. A V4R5 változattól kezdve használják az időzónákat a címtár minden módosításánál és bővítésénél. Ezért, ha V4R4 vagy korábbi verzióról frissít V5R2 verzióra, a Címtár szolgáltatás beállítja a létező createtimestamp és a modifytimestamp attribútumokat, hogy azok tükrözzék a helyes időzónát. Ezt úgy valósítja meg, hogy kivonja az iSeries rendszeren definiált időzónát a címtárban tárolt időzónából. Vegye figyelembe, hogy ha az aktuális időzóna nem egyezik meg azzal az időzónával, amely a bejegyzés eredeti létrehozásakor vagy módosításakor volt aktív, akkor az új időpecsét értékek nem tükrözik az eredeti időzónát.
- Az áthelyezés után az LDAP címtár szolgáltató automatikusan indul a TCP/IP-vel együtt. Ha azt akarja, hogy a címtár szolgáltató ne induljon el automatikusan, akkor a beállításokat módosítsa az iSeries navigátorral.

Áttérés a Címtár szolgáltatás V4R3 vagy V4R4 változatáról V5R2 változatra

A V4R3 változatról nem lehet közvetlenül az OS/400 V5R2 verzióra frissíteni. Ha a Címtár szolgáltatás LDAP szerver V4R3 vagy V4R4 változatáról V5R2 változatára akar frissíteni, az alábbi eljárások valamelyike szerint kell eljárnia:

- OS/400 átmeneti telepítés V4R3 vagy V4R4 változatról egy közbenső változatra
- Adatbázis könyvtár mentése, majd OS/400 V4R3 verzióról teljes (scratch) telepítés V5R2 változatra

OS/400 átmeneti telepítés V4R3 vagy V4R4 változatról egy közbenső változatra

Noha nem támogatott az OS/400 frissítése V4R3 vagy V4R4 változatról V5R2-re, a következő lehetőségek kihasználhatók:

- V4R3 és V4R4 frissíthető V4R5-re
- V4R4 és V4R5 frissíthető V5R1-re
- V4R5 és V5R1 frissíthető V5R2-re

A Címtár szolgáltatás szerver frissítés egyik lehetséges módja, hogy először egy közbenső kiadásra (V4R5 vagy V5R1) tér át, majd onnan V5R2 verzióra. Az OS/400 telepítési eljárásokról részletes információt talál a *Szoftvertelepítés*  című könyvben. Végezze el az áttéréshez a következő műveleteket:

1. Jegyezze be a séma fájlokban megvalósított változtatásokat a /QIBM/UserData/OS400/DirSrv könyvtárba. A séma fájlok költöztetése automatikus.

2. V4R4 vagy V4R3 esetén végezze el az OS/400 V4R5 vagy V5R1 változat átmeneti telepítését.
3. Majd ezután telepítse az OS/400 V5R2 változatát.
4. Indítsa el a címtár szolgáltató szervert, ha nem volt a korábbiakban már elindítva.
5. A Directory Management Tool segítségével módosítsa a séma fájlokat, melyeknek változtatásait a lépés: 1 oldalszám: 12 helyen jegyezte fel.
6. Indítsa el újra a címtár szolgáltató szervert.

Adatbázis könyvtár mentése, majd OS/400 V4R3 verzióról teljes (scratch) telepítés V5R2 változatra

A Címtár szolgáltatás szerverről való áttérés egy másik lehetséges módja, hogy elmenti a Címtár szolgáltatás V4R3 vagy V4R4 változatnál használt adatbázis könyvtárat, majd visszaállítja azt, miután telepítette a V5R2 változatot. Ezzel megtakarítható a közbenső kiadás telepítési fázisa. Azonban ilyenkor a szerver beállításai nincsenek áthelyezve, a szervert újra kell konfigurálni. Az OS/400 telepítési eljárásokról részletes információt talál a *Szoftvertelepítés*  című könyvben. Végezze el az áttéréshez a következő műveleteket:

1. Jegyezze be a séma fájlokban megvalósított változtatásokat a /QIBM/UserData/OS400/DirSrv könyvtárba. A séma fájlok nem kerülnek automatikusan áthelyezésre, ezért ha meg kívánja őrizni a változtatásokat, ezeket kézi úton kell újra létrehozni.
2. Jegyezze be a különböző konfiguráció beállításokat a Címtár szolgáltatás szerver jellemzői közé, természetesen az adatbázis könyvtár nevét is.
3. Mentse el a Címtár szolgáltatás szerver konfigurációban specifikált adatbázis könyvtárat.
4. Jegyezze fel a kiadói konfigurációt.
5. Telepítse a rendszerbe az OS/400 V5R2 változatot.
6. Használja az EZ-Setupot a címtár szolgáltató szerver konfigurálására.
7. Állítsa vissza az adatbázis könyvtárat, amit a 3. lépésben mentett el.
8. A Directory Management Tool segítségével módosítsa a séma fájlokat. Változtatásaikat a lépés: 1 helyen jegyezte fel.
9. Az iSeries navigátorral konfigurálja újra a címtár szolgáltatót. Adja meg az adatbázis könyvtárat, melyet elmentett és visszaállított.
10. Az iSeries navigátorral konfigurálja újra a publikálást.
11. Indítsa el újra a címtár szolgáltató szervert.

Frissítési eredmények

Amikor V4R3 szintről valamilyen későbbi változatra frissít, a következő szempontokra kell figyelni:

- **A kulcstartó fájl átköltöztetése egy kulcs-adatbázisba:**

  A Client Access V3R2 kulcstartó fájlokat használt az LDAP címtár szolgáltatóval történő SSL védett kapcsolat (Secure Sockets Layer) létrehozásakor. Az iSeries Access for Windows ugyanerre a célra igazolástárolókat használ, amelyeket néha kulcs adatbázisnak is hívnak. Ha előzőleg kulcscsomó fájlt használt az LDAP címtár szolgáltatóval kapcsolatban, az SSL használatához azt kulcs adatbázissá kell konvertálni. Amikor az első alkalommal próbál meg SSL védett kapcsolatot felvenni az LDAP címtár szolgáltatóval, az iSeries navigátor figyelmeztetni fogja a konvertálás szükségességére. Amennyiben a konvertálást választja, néhány kérdésre kell válaszolnia a kulcs adatbázissal kapcsolatban, mielőtt megtörténne a konvertálás.

  Az LDAP címtár szolgáltató szintén kulcscsomó fájlt használt a saját SSL kapcsolatai részére a V4R3 verzióban. A V4R4 verziótól kezdődően rendszer igazolástárolót használ. Ha a szervere a V4R3 verzióban SSL kapcsolatra volt beállítva, a kulcstartó fájl tartalma átköltözik a rendszer igazolástárolójába.
- **Két adatfolyam fájl eltávolításra került:**

  A V4R3 változatban a Címtár szolgáltatás által használt következő két folyamfájlra már nincs szükség, és automatikusan eltávolításra kerül, amikor későbbi változatokat telepít:

```
/QIBM/ProdData/OS400/DirSrv/qgldcert.kyr
/QIBM/ProdData/OS400/DirSrv/qgldcert.sth
```

E fájlokkal kapcsolatban semmiféle intézkedésre nincs szükség. Törlésüket csak azért kell megemlíteni, hogy hiányuk ne okozzon félreértést.

Vegye figyelembe, további eredmények is lehetnek, ha az aktuális változatra frissít egy másik változatról.

A Címtár szolgáltatás telepítése és konfigurálása

Az OS/400 telepítésekor a Címtár szolgáltatás (LDAP) is automatikusan telepítésre kerül. A címtár szolgáltató egy alapértelmezés szerinti konfigurációt tartalmaz, ami automatikusan indítja a címtár szolgáltatót, amikor a TCP/IP indításra kerül. A címtár szolgáltató elindítja az OS/400 rendszerből a számítógép információk továbbítását is a címtár szolgáltatónak. Az LDAP címtár szolgáltató beállításainak egyéniesítéséhez futtassa a Címtár szolgáltatás konfigurációs varázslót. A varázsló használatához *ALLOBJ és *IOSYSCFG különleges jogosultságokkal kell rendelkezni.

A Címtár szolgáltatás a V5R1 verziótól kezdve az alap operációs rendszer része, a V5R2 változattól kezdve a 32-es opció megszűnt.

Az LDAP címtár szolgáltató konfigurálása

Ha a rendszere nem úgy lett konfigurálva, hogy képes legyen információkat továbbítani egy másik LDAP szervernek, és a TCP/IP DNS szerver nem ismer LDAP szervereket, akkor a Címtár szolgáltatás automatikusan egy korlátozott alapértelmezés szerinti konfigurációt telepít. A Címtár szolgáltatás egy varázslót biztosít az LDAP címtár szolgáltatónak az egyedi igények szerint történő konfigurálás támogatására. Ez a varázsló az EZ-Setup részeként futtatható, vagy később az iSeries navigátorból. A varázsló használata különösen ajánlott a címtár szolgáltató elsődleges beállításához. Használhatja a varázslót a címtár szolgáltató újrakonfigurálásakor is.

Megjegyzés: Amikor a varázslót a címtár szolgáltató újrakonfigurálása céljából indítja el, akkor a konfigurálás ″tiszta lappal″ indul. Az eredeti konfiguráció törlésre kerül a módosítás helyett. Azonban a címtári adat nem törlődik, helyette abban a könyvtárban marad meg, mely a telepítés alkalmával lett kiválasztva (alapértelmezés szerint ez QUSRDIRDB könyvtár). A változási napló is érintetlen marad az alapértelmezés szerint a QUSRDIRCL könyvtárban.

Ha teljesen alaphelyzetből kíván indulni, akkor a varázsló indítása előtt törölje ezt a két könyvtárat.

Ha módosítani kívánja a címtár szolgáltató konfigurációját, de nem törli ki teljesen azt, akkor kattintson a jobb oldali egérgombbal a **Directory** feliratra, majd válassza a **Properties** lapot. Így megmarad az eredeti beállítás.

A szerver konfigurálásához az *ALLOBJ és *IOSYSCFG különleges jogosultságokkal kell rendelkeznie. Ha az OS/400 biztonsági ellenőrzését akarja konfigurálni, akkor rendelkezni kell az *AUDIT különleges jogosultsággal is.

A Címtár szolgáltatás konfigurációs varázslót az alábbi módon lehet indítani:

1. Nyissa meg az iSeries navigátorban a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, majd válassza a **Configure** menüpontot.

Megjegyzés: Ha már egyszer beállította a címtár szolgáltatót, válassza ki inkább a **Reconfigure** elemet a **Configure** helyett.

Kövesse a címtár szolgáltató beállító varázsló utasításait az LDAP címtár szolgáltató helyes beállításához.

Megjegyzés: Lehet, hogy célszerűnek tartja ezt a könyvtárat (amely a címtár adatait tartalmazza), egy felhasználói kiegészítő tárolókészletben (ASP) tárolni a rendszer ASP helyett. Azonban ez a könyvtár nem tárolható független ASP-ben, és minden olyan kísérlet, amikor független ASP-ben lévő könyvtárral kívánja a szervert konfigurálni, újrakonfigurálni vagy indítani, meghiúsul.

A varázsló működésének befejeztével az LDAP címtár szolgáltató alapszintű konfigurációja készen áll. Ha a rendszerén Lotus Domino terméket futtat, a Domino LDAP funkciója már használhatja az LDAP szerver alapértelmezés szerinti 389-es portját. A következők egyikét teheti:

- Változtassa meg a Lotus Domino által használt portot
- Változtassa meg a Címtár szolgáltatás által használt portot
- Megadott IP címeket használjon

Itt már elindíthatja a szervert. Az indítás előtt azonban célszerű az alábbiakban felsorolt dolgok közül néhányat vagy az összeset elvégezni:

- Adatok importálása a szerverbe
- SSL biztonság (Secure Sockets Layer) engedélyezése
- A Kerberos hitelesítés engedélyezése
- Utalási szerver beállítása

SSL engedélyezése az LDAP címtár szolgáltatón

Ha a Digitális igazolás kezelő telepítve lett a rendszerre, használhatja a védett socket réteg (Secure Sockets Layer SSL) nyújtotta biztonságot, hogy védje az LDAP címtár szolgáltatóhoz való hozzáférést. Mielőtt engedélyezné a címtár szolgáltatón az SSL használatát, érdemes megismerni az SSL és a Címtár szolgáltatás használatáról szóló áttekintést.

Ahhoz, hogy az SSL kapcsolatot használhassa, amikor az LDAP címszolgáltatót az iSeries navigátorból kezeli, vagy ha Windows LDAP klienssel akarja az SSL kapcsolatot használni, akkor valamelyik Client Encryptions terméket (5722CE2 vagy 5722CE3) telepíteni kell a PC-re.

Az SSL engedélyezéséhez LDAP szerveren használja a Digital Certificate Manager (digitális igazolás kezelő) kezelőfelületét. A Digitális igazolás kezelőt indíthatja az iSeries navigátor **Internet** mappájából, vagy a címtár szolgáltató **Properties** párbeszédablakának **Network** lapjáról.

A **Network** lapról az alábbi lépésekkel indítható a Digitális igazolás kezelő:

1. Az iSeries navigátorban nyissa meg a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
5. Kattintson a **Network** fülre.
6. Kattintson a **Digital Certificate Manager** ikonra.

   A Digital Certificate Manager az alapértelmezett Internet böngészőben indul el.

Olvassa el az LDAP címtár szolgáltató biztonsága című részben lévő lépéseket, amelyeket követni kell abból a célból, hogy digitális igazolást rendeljen hozzá a címtár szolgáltatóhoz.

Az SSL engedélyezése után lehetőség nyílik az LDAP címtár szolgáltató által védett kapcsolatok esetén használt port számának megváltoztatására.

A Kerberos hitelesítés engedélyezése az LDAP címtár szolgáltatón

Ha a rendszerén konfigurálta a Hálózati hitelesítés szolgáltatást (Network Authentication Service), akkor üzembe állíthatja az LDAP címtár szolgáltatón a Kerberos hitelesítés használatát. Mielőtt engedélyezné a címtár szolgáltatón a Kerberos használatát, érdemes megismerni a Kerberos és a Címtár szolgáltatás használatáról szóló áttekintést.

A Kerberos hitelesítés engedélyezéséhez végezze el az alábbiakat:
1. Nyissa meg az iSeries navigátorban a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, majd válassza a **Properties** lapot.
5. Kattintson a **Kerberos** fülre.
6. Ellenőrizze a **Kerberos hitelesítés engedélyezését**.
7. Specifikáljon helyzetéhez alkalmazkodva más beállításokat a **Kerberos** oldalon. Az egyes mezőkről további információkat az oldal online súgójában talál.

A Címtár szolgáltatás alapértelmezett konfigurációja

Az LDAP címtár szolgáltató az OS/400 rendszerrel együtt automatikusan telepítésre kerül. Ez a telepítés tartalmaz egy alapértelmezés szerinti konfigurációt. A címtár szolgáltató akkor használja az alapértelmezés szerinti konfigurációt, ha az alábbi feltételek mind igazak:

- A rendszergazdáknak nem kell futtatni a Címtár szolgáltatás konfigurációs varázslóját vagy a tulajdonság lapokkal a megváltozott könyvtári beállításokat.
- A Címtár szolgáltatás kiadója nincs konfigurálva.
- Az LDAP címtár szolgáltató nem képes megtalálni valamilyen LDAP DNS információt.

Ha az LDAP címtár szolgáltató az alapértelmezés szerinti konfigurációt használja, akkor a következők történnek:

- Az LDAP címtár szolgáltató automatikusan indul, ha a TCP/IP elindul.
- A rendszer létrehozza a cn=Administrator alapértelmezés szerinti adminisztrátort. Emellett létrehoz egy jelszót belső használatra. Ha a későbbiek során egy adminisztrátori jelszót kell használni, létrehozható egy új a Címtár szolgáltatás tulajdonság lapról.
- A rendszer IP nevére alapozva kialakításra kerül egy alapértelmezés szerinti utótag. A rendszer neve alapján létre lesz hozva objektum utótag is. Ha például a rendszer IP neve mary.acme.com, az utótag dc=mary,dc=acme,dc=com lesz.
- Az LDAP címtár szolgáltató a QUSRDIRDB alapértelmezés szerinti könyvtárat használja. A rendszer ezt az ASP rendszerben hozza létre.
- A szerver a nem-biztonságos kommunikációra a 389 portot használja. Ha az LDAP részére konfiguráltak egy digitális igazolást, akkor a védett socket réteg (secure socket layer, SSL) engedélyezésre kerül, és a védett kommunikáció a 636-os portot használja.

Az alábbi alapértelmezések érvényesek a Címtár szolgáltatás kiadó számára:

- A rendszer információkat továbbít a helyi LDAP címtár szolgáltató számára.
- A továbbítás nem az SSL segítségével történik.
- A továbbításkor konténereket használnak az alapértelmezés szerinti utótaggal.
- A címtár szolgáltató hitelesítésére az OS/400 a cn=Administrator ID-t és a rendszer által generált jelszót használja.
- A rendszer kizárólag rendszer információkat továbbít.

IBM SecureWay Directory Management Tool

Az IBM SecureWay Directory Management Tool (DMT) grafikus felhasználói kezelőfelületet nyújt az LDAP címtár tartalmának kezeléséhez. A DMT eszközzel végrehajtható feladatok körébe a következők tartoznak:

- Címtár séma böngészése
- Objektum osztályok hozzáadása, szerkesztése és törlése
- Attribútumok hozzáadása, szerkesztése és törlése
- Címtárfa böngészése és keresése
- Bejegyzések hozzáadása, szerkesztése, megjelenítése és törlése

- RDN bejegyzések szerkesztése
- ACL-k kezelése

A DMT a Windows LDAP kliens része, amely tartalmazza a Címtár szolgáltatást. A kliens egy integrált fájlrendszerbeli katalógusban kerül szállításra.

A Windows LDAP kliens PC-re történő telepítéséhez - beleértve a DMT-t is - kövesse ezeket a lépéseket:
1. Az iSeries navigátorban bontsa ki a **File Systems** részt.
2. Bontsa ki a **File Shares** részt.
3. Kattintson duplán a **Qdirsrv** elemre.
4. Kattintson duplán az **UserTools** elemre.
5. Kattintson duplán a **Windows** elemre.
6. Kattintson duplán a **setup.exe** fájlra a DMT telepítéséhez. Kövesse a képernyőn megjelenő utasításokat a telepítés befejezéséhez.

Az IBM SecureWay Directory Management Tool (DMT) dokumentációja a dparent.htm fájlban található. Ez a fájl átmásolásra kerül a PC-n az IBM SecureWay Directory könyvtárba, amikor telepíti a klienst.

Fejezet 4. Az LDAP címtár szolgáltató adminisztrálása

Az LDAP címtár szolgáltató adminisztrálásához a következő jogosultsági csoporttal kell rendelkeznie:

- A szerver konfigurálásához vagy annak megváltoztatásához: All Object (*ALLOBJ) és I/O System Configuration (*IOSYSCFG) különleges jogosultságok
- A szerver indításához vagy leállításához: Job Control (*JOBCTL) és objektum jogosultság az End TCP/IP (ENDTCP), a Start TCP/IP (STRTCP), a Start TCP/IP Server (STRTCPSVR) és az End TCP/IP Server (ENDTCPSVR) parancsokhoz
- A címtár szolgáltató ellenőrzési funkciójának beállításához: Audit (*AUDIT) különleges jogosultság
- A szerver feladatnapló megtekintéséhez: Spool Control (*SPLCTL) különleges jogosultság

A címtár objektumok kezeléséhez (beleértve az elérésvezérlési listákat, az objektum tulajdonjogokat és a replikákat) kapcsolódjon a címlistához adminisztrátori DN-nel vagy olyan DN-nel, amely a megfelelő LDAP jogosultsággal rendelkezik. Ha az ellenőrzési funkciót használja, az adminisztrátor is lehet irányított felhasználó, akinek jogosultsága van a Címtár szolgáltatás adminisztrátori funkció ID-hez.

A címtár szolgáltató adminisztrálása az alábbi feladatokat foglalja magában:

- “Az LDAP címtár szolgáltató indítása”
- “Az LDAP címtár szolgáltató leállítása” oldalszám: 20
- “A címtár szolgáltató állapotának ellenőrzése” oldalszám: 20
- “Jobok ellenőrzése LDAP címtár szolgáltatón” oldalszám: 20
- “Az esemény értesítés engedélyezése” oldalszám: 20
- “A tranzakció beállítások megadása” oldalszám: 21
- “Port vagy IP cím módosítása” oldalszám: 21
- “LDAP címtári adatok átvitele rendszerek között” oldalszám: 22
- “Szerver kijelölése címtári utalások részére” oldalszám: 29
- “Utótagok felvétele az LDAP címtár szolgáltatóba” oldalszám: 29
- “Utótagok eltávolítása a címtár szolgáltatóból” oldalszám: 29
- “A Címtár szolgáltatás információinak mentése és visszaállítása” oldalszám: 30
- “Címtári adatok tulajdonjogának és elérésének kezelése” oldalszám: 30
- “Az LDAP címtár eléréseinek és változásainak nyomon követése” oldalszám: 32
- “Objektum naplózás engedélyezése a címtár szolgáltató számára” oldalszám: 32
- “Az LDAP címtár szolgáltató teljesítményének beállítása” oldalszám: 33

Az LDAP címtár szolgáltató indítása

Az LDAP címtár szolgáltató indításához az alábbi lépésekre van szükség:

1. Az iSeries navigátorban nyissa meg a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Start** gombot.

   A szerver sebességétől és a rendelkezésre álló memória méretétől függően a címtár szolgáltató elindulásához néhány perc szükséges. Első alkalommal a címtár szolgáltató indítása a szokásosnál is hosszabb időt vesz igénybe, mert a szerver új fájlokat hoz létre. Hasonlóképpen, amikor első alkalommal indítja el a címtár szolgáltatót a Címtár szolgáltatás korábbi változatáról történő frissítést követően, az indulás a megszokottnál néhány perccel hosszabb időt vehet igénybe, mivel a szervernek át kell telepíteni a fájlokat. Időről-időre ellenőrizheti a szerver állapotát, hogy megállapítsa, elindult-e már.

Megjegyzés: A címtár szolgáltató elindítható 5250 szekcióból is a STRTCPSVR *DIRSRV parancs segítségével.

Amennyiben a címtár szolgáltatót úgy állította be, hogy a TCP/IP-vel egyidőben induljon, a STRTCP paranccsal is indíthatja azt.

Az LDAP címtár szolgáltató leállítása

A címtár szolgáltató leállítása hatással van az összes olyan alkalmazásra, amely használja a szervert a leállítás pillanatában. Ide tartoznak az Enterprise Identity Mapping (EIM) alkalmazások, amelyek jelenleg igénybe veszik a címtár szolgáltatót az EIM műveletekhez. Az összes alkalmazás lekapcsolódik ugyan a címtár szolgáltatóról, azonban semmi sem akadályozza őket abban, hogy megpróbáljanak újra kapcsolódni a szerverhez.

Az LDAP címtár szolgáltató leállításához az alábbi lépésekre van szükség:
1. Az iSeries navigátorban nyissa meg a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Stop** gombot.

   A címtár szolgáltató leállítása néhány percig is eltarthat a rendszer sebességétől, a szerver tevékenységétől, és a rendelkezésre álló memória méretétől függően. Lehetséges időről-időre a szerver állapotának ellenőrzése, hogy megállapítsuk, leállt-e már.

Megjegyzés: A címtár szolgáltató leállítható 5250 szekcióból is ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL vagy ENDTCP parancsok segítségével. Az ENDTCPSVR *ALL és az ENDTCP parancs hatással van a rendszerben működő összes TCP/IP szerverre. Az ENDTCP parancs leállítja magát a TCP/IP-t is.

A címtár szolgáltató állapotának ellenőrzése

Az iSeries navigátor a jobb keret **Status** oszlopában megjeleníti a címtár szolgáltató állapotát.

A címtár szolgáltató állapotának ellenőrzéséhez az alábbi lépésekre van szükség:
1. Az iSeries navigátorban nyissa meg a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra. Az iSeries navigátor megjeleníti a **Status** oszlopban az összes TCP/IP szerver, közöttük a címtár szolgáltató állapotát. A szerverek állapotának frissítéséhez kattintson a **View** menüre, és ott válassza ki a **Refresh** elemet.
4. Ha további információt szeretne a címtár szolgáltató állapotáról, kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Status** opciót. Ezzel megtekintheti az aktív kapcsolatok számát és más információt, mint pl. az előző és a jelenlegi aktivitási szintet.

   A többletinformáción kívül ezzel a módszerrel időt is takaríthat meg. Anélkül frissítheti a címtár szolgáltató állapotát, hogy a többi TCP/IP szerver állapotfrissítését is ki kellene várnia.

Jobok ellenőrzése LDAP címtár szolgáltatón

Időről-időre szükség lehet egyes jobok megfigyelésére az LDAP címtár szolgáltatón. A szerver jobok ellenőrzéséhez végezze el az alábbi lépéseket:
1. Az iSeries navigátor menüjében nyissa meg a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, majd válassza ki a **Server Jobs** elemet.

Az esemény értesítés engedélyezése

A Címtár szolgáltatás támogatja az esemény értesítést, ami lehetővé teszi, hogy az LDAP szerver értesítse a klienst, ha bekövetkezik egy bizonyos esemény, mint például a címtár kibővítése.

A szerveren az esemény értesítés engedélyezéséhez végezze el az alábbi lépéseket:
1. Nyissa meg az iSeries navigátorban a **Network** ikont.
2. Nyissa meg a **Servers** ikont.

3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, majd válassza a **Properties** lapot.
5. Kattintson az **Events** ikonra.
6. Válassza ki az **Allow clients to register for event notification** parancsot.

Meghatározható egy-egy csatlakozás számára az engedélyezett bejegyzések maximális száma, továbbá a szerver számára engedélyezett összes bejegyzés maximális száma.

Az esemény értesítésről további tájékoztatást az IBM SecureWay Directory V3.2: Client SDK Programming Reference könyv Függelék C. Esemény értesítés című részében talál.  .

A tranzakció beállítások megadása

A Címtár szolgáltatás támogatja a tranzakciókat, ami lehetővé teszi, hogy az LDAP címtári műveletek csoportját a címtár szolgáltató egy egységként kezelje. További információk: “Tranzakciók” oldalszám: 40.

A szerveren a tranzakció beállításokhoz végezze el az alábbi lépéseket:
1. Nyissa meg az iSeries navigátorban a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, majd válassza a **Properties** lapot.
5. Kattintson a **Transactions** gombra.
6. Adja meg a tranzakció beállításokat.

Megjegyzés: Mivel a tranzakció beállítások befolyásolják az LDAP szerver teljesítményét, célszerű megvizsgálni több beállítás hatását.

Port vagy IP cím módosítása

A Címtár szolgáltatás által engedélyezett LDAP címtár szolgáltató a következő alapértelmezett portokat használja:
- 389 nem védett kapcsolatok számára.
- 636 védett kapcsolatok számára (ha a digitális igazoláskezelő - Digital Certificate Manager - segítségével engedélyezte a Címtár szolgáltatás részére a védett port használatát).

Megjegyzés: Alapértelmezés szerint a helyi rendszeren megadott összes IP cím a szerverhez kapcsolódik (bind).

Ha a portokat már más alkalmazás használja, akkor vagy más portot rendel hozzá a Címtár szolgáltatáshoz, vagy különböző IP címeket használ a két szerverre, ha az alkalmazások támogatják az adott IP címhez rendelést.

Ha például a Domino LDAP szerver kerül konfliktusba az iSeries LDAP szerverrel, olvassa el a Hoszt Domino LDAP és Címtár szolgáltatások ugyanazon az iSeries szerveren című részt.

Az LDAP címtár szolgáltató által használt portok megváltoztatásához kövesse az alábbi lépéseket:
1. Az iSeries navigátor menüjében válassza a **Network** pontot.
2. Nyissa meg a **Servers** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Jobb egérgombbal kattintson a **Directory** feliratra, és válassza a **Properties** pontot.
5. Kattintson a **Network** fülre.
6. Írja be a kívánt portszámokat, majd kattintson az **OK** gombra.

Végezze el az alábbi lépéseket, ha IP címet akar módosítani úgy, hogy a címtár szolgáltató elfogadja a kapcsolatokat:

1. Az iSeries navigátor menüjében válassza a **Network** pontot.
2. Nyissa meg a **Servers** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
5. Kattintson a **Network** fülre.
6. Kattintson az **IP Addresses...** gombra.
7. Válassza ki a **Use selected IP addresses** opciót, és válassza ki a szerver számára a kapcsolatok elfogadásakor használandó IP címeket.

LDAP címtári adatok átvitele rendszerek között

A Címtár szolgáltatás LDAP szerver más szerverektől függetlenül is tud futni. Szükség lehet azonban arra, hogy más szerverekkel működjön együtt. Ezek között lehet:
- “LDIF fájl importálása”
- “LDIF fájl importálása”
- “A címtár szolgáltató új replikájának beállítása” oldalszám: 23
- “Információk publikálása a címtár szolgáltatónak” oldalszám: 26

LDIF fájl importálása

Különböző LDAP címtár szolgáltatók között az információcsere LDAP Data Interchange Format (LDIF) formájú fájlokkal lehetséges. Mielőtt elindítaná ezt a műveletet, vigye át adatfolyam fájlként az LDIF fájlt az iSeries szerverre.

Az LDIF fájlnak az LDAP címtár szolgáltatóra történő importálásához a következő lépéseket kell megtenni:
1. Ha a címtár szolgáltató működik, állítsa le azt. “Az LDAP címtár szolgáltató leállítása” oldalszám: 20 részben talál információt a címtár szolgáltató leállítására vonatkozóan.
2. Az iSeries navigátorban nyissa meg a **Network** ikont.
3. Nyissa meg a **Servers** ikont.
4. Kattintson a **TCP/IP** pontra.
5. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Tools**, majd az **Import File** elemet.

Megjegyzés: LDIF fájlok importálásához használhatja az ldapadd segédprogramot is.

LDIF fájl importálása

Különböző LDAP címtár szolgáltatók között az információcsere LDAP Data Interchange Format (LDIF) formájú fájlokkal lehetséges (“LDAP adatcsere formátum” oldalszám: 37). LDIF fájlba lehet menteni az LDAP címtár egészét vagy annak egy részét.

Egy LDIF fájlnak a címtárszolgátatóból történő exportálásához végezze el az alábbi lépéseket:
1. Az iSeries navigátorban nyissa meg a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, majd válassza a **Tools**, majd az **Export File** elemet.

   Megjegyzés: Ha nem adja meg, hogy az LDIF fájl hova legyen exportálva, akkor az OS/400 felhasználói profiljában megadott alapértelmezés szerinti könyvtárba lesz elmentve. Amennyiben még nem módosította az alapértelmezett mappát, az a rendszer főkönyvtára lesz.

Megjegyzések:

1. Ne felejtsen el az LDIF fájlra megfelelő jogosultságot beállítani, hogy megakadályozza a jogosulatlan hozzáférést a címtárhoz. Ehhez az iSeries navigátorban kattintson a jobb oldali egérgombbal a fájlra, majd válassza a **Permission** elemet.
2. Az ldapsearch segédprogrammal teljes vagy részleges LDIF fájlt hozhat létre (“ldapsearch segédprogram” oldalszám: 56). Használja az -L opciót, és irányítsa fájlba a kimenetet.

A címtár szolgáltató új replikájának beállítása

Létrehozhatja az LDAP címtár szolgáltató replikáit más iSeries szerverek címtár szolgáltatóin. A Címtár szolgáltatás a szabványos LDAP 3. verziójú protokollt használja replikálás céljából.

Megjegyzések:

1. Az LDAP verzió 3 és az LDAP verzió 2 szerverek között nem lehetséges replikálni. Ezért a replikát tartalmazó rendszernek ugyanazt az LDAP verziót kell használni, mint amit az a rendszer használ, amelyik replikáltat. Az OS/400 V4R3 és V4R4 verziói támogatják az LDAP 2-es verziót. A V4R5 és a későbbi verziók támogatják az LDAP 3-as verziót.
2. A Címtár szolgáltatás címtára replikálható más platformon működő IBM SecureWay V3.2 vagy újabb szerveren. Ez olyan OS/400 címtár szolgáltatónál lehetséges, melyet az ACI 3.2 eljárással konfiguráltak. Ha probléma merül fel akkor, amikor a szerver megpróbál replikálni, a replikálás leáll. Amennyiben ez előfordul, a replika nem lesz teljes.

A címtár szolgáltató új replikájának létrehozásához kövesse az alábbi lépéseket:

1. Ha még nem konfigurálta a főszervert és a replika szervert, akkor konfigurálja most.

   Megjegyzés: Ellenőrizze, hogy a két szerver utótagja és sémája megegyezik-e egymással.
2. Állítsa le a főszervert.
3. (opcionális) Állítsa be az LDAP adatokat kezdeti replikációhoz. Ha nincs olyan kezdeti adat, amelyet a főszerverről át akar vinni a replika szerverre, akkor kihagyhatja ezt a lépést.
4. (opcionális) Vigye át az LDAP adatokat a főszerverre. Ugorja át ezt a lépést, ha az alábbiak közül valamelyik pont érvényes a replika szerverre:
   - Ez egy új LDAP címtár szolgáltató.
   - Nem tartalmaz olyan adatot, amelyet szándékában áll továbbra is karbantartani.
5. Állítsa be az új replika szervert.
6. Konfigurálja a főszervert az új replikához.
7. Győződjön meg róla, hogy a főszerver engedélyezi a frissítéseket:
   a. Az iSeries navigátorban nyissa meg azt a rendszert, amelyen a főcímtár szolgáltató fut.
   b. Nyissa meg a **Network** ikont.
   c. Nyissa meg a **Servers** ikont.
   d. Kattintson a **TCP/IP** pontra.
   e. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
   f. Ha még nincs bejelölve, jelölje be az **Allow directory updates** jelölőnégyzetet.

Megjegyzés: Ezek az utasítások feltételezik, hogy a főszerver és a replika szerver rendszerét ugyanazon a PC-n működő iSeries navigátorral kezelik. Ha a rendszereket önálló PC-kről kezelik, a két PC között váltani kell ezen feladat végrehajtása közben. Ha a főszerver vagy a replika szerver az OS/400, operációs rendszertől eltérő IBM operációs rendszer felügyelete alatt működik, használja az adott platform dokumentációját a szerver beállításához.

LDAP adatok beállítása kezdeti replikációhoz

Lehet, hogy az LDAP címtár szolgáltatón olyan meglévő adatok vannak, amelyeket egy új replika szerverre kíván átvinni. Ehhez először exportálni kell a címtárat egy LDIF fájlba. Az LDIF fájl exportálása alatt meg kell akadályozni a főszerverben a frissítést. Ezt a következő módszerek egyikével teheti meg:

- Állítsa le az LDAP címtár szolgáltatót. A címtárban lévő adatok mennyiségétől függően lehet, hogy hosszabb időt vesz igénybe a szerver leállítása.

- Változtassa meg a szerver tulajdonságokat úgy, hogy a frissítés ne legyen engedélyezve. Ez lehetővé teszi a szervernek a keresési kérésekre való válaszadás folytatását, miközben az LDIF fájl exportálása folyik. Ehhez az opcióhoz az alábbi lépéseket kell elvégezni:
  1. Az iSeries navigátorban nyissa meg azt a rendszert, amelyen a főcímtár szolgáltató fut.
  2. Válassza a **Network** elemet.
  3. Nyissa meg a **Servers** elemet.
  4. Kattintson a **TCP/IP** pontra.
  5. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
  6. Ha az **Allow directory updates** jelölőnégyzet be van jelölve (x), törölje a kiválasztást. Ez megakadályozza a könyvtár frissítését, amíg a replikációs folyamat be nem fejeződik.
  7. Kattintson az **OK** gombra.
  8. Állítsa le, majd indítsa újra az LDAP címtár szolgáltatót.

Miután leállította a szervert vagy megváltoztatta a szerver tulajdonságokat a címtár frissítések letiltása érdekében, hajtsa végre ezeket a feladatokat:

1. Exportálja a könyvtárt egy LDIF fájlba.
2. Küldje át az LDIF fájlt arra a rendszerre, amelyiken a replika szerver futni fog.

Miután átküldte az LDIF fájlt arra a rendszerre, amelyiken a replika szerver futni fog, importálni kell az adatokat a replika szerverbe:

1. Az iSeries navigátorban nyissa meg azt a rendszert, amelyen a replika címtár szolgáltató fut.
2. Ha a replika szerver még nincs leállítva, állítsa azt most le. Frissítse a szerverek állapotát, amíg az állapot **Stopped** nem lesz.
3. Válassza a **Network** elemet.
4. Nyissa meg a **Servers** elemet.
5. Kattintson a **TCP/IP** pontra.
6. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
7. Ha az **Allow directory updates** jelölőnégyzet üres, jelölje be. Ez lehetővé teszi az adatok importálását.
8. Kattintson az **OK** gombra.
9. Importálja az LDIF fájlt, amelyet a 2. lépésben vitt át.
10. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
11. Törölje ki a **Allow directory updates** jelölőnégyzet kiválasztását.

LDAP adatok átvitele a főszerverre

Amint az LDAP címtár szolgáltatót replika (másodpéldány) szerverré alakította át, nem frissítheti többé a rajta lévő adatokat. Ha vannak meglévő adatai a replika szerverré alakítandó LDAP címtár szolgáltatón, valószínűleg a főszerverre kívánja őket áthelyezni, hogy továbbra is karbantarthassa őket. Ehhez az alábbi lépéseket kell elvégezni:

1. Az iSeries navigátorban nyissa meg a rendszert, amelyen a replika címtár szolgáltató fut.
2. Válassza a **Network** elemet.
3. Nyissa meg a **Servers** elemet.
4. Kattintson a **TCP/IP** pontra.
5. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
6. Ha az **Allow directory updates** jelölőnégyzet be van jelölve (x), törölje a kiválasztást. Ez megakadályozza a könyvtár frissítését, amíg a replikációs folyamat be nem fejeződik.
7. Kattintson az **OK** gombra.
8. Állítsa le az LDAP címtár szolgáltatót.
9. Exportálja a könyvtárt egy LDIF fájlba.
10. Küldje át az LDIF fájlt arra a rendszerre, amelyiken a főszerver futni fog.

Miután átküldte az LDIF fájlt arra a rendszerre, amelyiken a főszerver futni fog, importálni kell az adatokat a replika szerverbe:

1. Az iSeries navigátorban nyissa meg azt a rendszert, amelyen a főcímtár szolgáltató fut.
2. Ha a főcímtár szolgáltató még nincs leállítva, állítsa azt most le. Frissítse a szerverek állapotát, amíg az állapot **Stopped** nem lesz.
3. Válassza a **Network** elemet.

4. Nyissa meg a **Servers** elemet.
5. Kattintson a **TCP/IP** pontra.
6. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
7. Ha az **Allow directory updates** jelölőnégyzet üres, jelölje be. Ez lehetővé teszi az adatok importálását.
8. Kattintson az **OK** gombra.
9. Importálja az LDIF fájlt, amelyet az előző műveletsorban, a lépés: 10 oldalszám: 24 helyen vitt át.
10. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
11. Törölje ki az **Allow directory updates** jelölőnégyzet tartalmát.

Új replika beállítása

Új replika szerver beállításához végezze el az alábbi műveleteket.

Megjegyzés: Mielőtt ehhez az eljáráshoz hozzáfog, győződjön meg arról, hogy a replika szerver konfigurálva van-e, és le lett állítva.

1. Az iSeries navigátorban nyissa meg a rendszert, amelyen a replika címtár szolgáltató fut.
2. Válassza a **Network** elemet.
3. Nyissa meg a **Servers** elemet.
4. Kattintson a **TCP/IP** pontra.
5. Ha a szerver még nincs leállítva, állítsa most le. Frissítse a szerverek állapotát, amíg az állapot **Stopped** nem lesz.
6. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** elemet.
7. Kattintson a **Replication** fülre.
8. Válassza ki az **Use as a replica server** elemet.
9. A **Name used by master server for updates** mezőben jelöljön ki a főszervernek egy nevet. A főszerver naplóz a replika szerverben, amikor frissít. Ez lehet egy megkülönböztető név (DN) vagy egy Kerberos felhasználó.

   Ha egy DN nevet választ:

   - Kattintson a **Name used by master server for updates** mező mellett található **Password** gombra. Adja meg azon főszerver jelszavát, amelyik bejelentkezik a replika szerverhez a frissítések elvégzése céljából.

     Megjegyzés: Jegyezze fel ezt a jelszót és a 9. lépésben megadott nevet. Szüksége lesz rájuk, amikor a replikációhoz használt főszervert konfigurálja.

   Ha az **Add Kerberos User**-t választja:

   - A rendszer kéri, hogy adja meg a Kerberos nevet (LDAP/*hostname* alakban, ahol a *hostname* a főszerver minősített teljes neve), és főszervernek alapértelmezés szerinti adatstruktúráját (úgy mint ACME.COM).

     Megjegyzés: A Kerberos csak akkor használható, ha a főszerveren és a replika szerveren a Kerberos engedélyezve van.
10. A **Master server URL** mezőbe írja be a főszerver nevét URL formátumban. Ha a főszerver az alapértelmezéstől eltérő portot használ, akkor írja be azt az URL cím részeként.
11. Kattintson a **Database/Suffixes** fülre. Ha a replikálni kívánt utótag nem jelenik meg a listán, vegye fel.
12. (opcionális) Amennyiben replikálás közben SSL (Secure Sockets Layer) biztonságot kíván igénybe venni, használja a digitális igazoláskezelőt (Digital Certificate Manager) az SSL engedélyezéséhez a szerveren. A digitális igazoláskezelőt a **Network** elemből indíthatja. Az SSL engedélyezéséről a címtár szolgáltatón további információt talál az “SSL engedélyezése az LDAP címtár szolgáltatón” oldalszám: 15 fejezet alatt.
13. Kattintson az **OK** gombra.

A főszerver beállítása új replikához

A főszerver az alábbi lépésekkel állítható be egy új replikához.

Megjegyzés: A műveletsort csak bekonfigurált és elindított főszerveren lehet végrehajtani.

1. Az iSeries navigátorban nyissa meg azt a rendszert, amelyen a főcímtár szolgáltató fut.

2. Válassza a **Network** elemet.
3. Nyissa meg a **Servers** ikont.
4. Kattintson a **TCP/IP** pontra.
5. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
6. Ha még nincs bejelölve, válassza ki az **Allow directory updates** jelölőnégyzetet.
7. Kattintson az **OK** gombra.
8. Állítsa le, majd indítsa újra az LDAP címtár szolgáltatót. Frissítse a szerverek állapotát, amíg az állapot **Elindítva** nem lesz.
9. Újra kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
10. Kattintson a **Replication** fülre. Az iSeries navigátor kérdéseket tehet fel a kapcsolatról. Válaszoljon a kérdésekre, majd kattintson az **OK** gombra.
11. Kattintson az **Add** gombra.
12. A **Server** mezőben adja meg a replika szerver nevét URL formátumban.
13. Válassza ki a hitelesítési módszert.

    Egy megkülönböztető név (DN) és jelszó használatához:

    a. Válassza ki az **Use DN and password server** elemet.

    b. A **Connect as** mezőben adja meg azt a nevet, amelyet akkor specifikált, amikor beállította a replika szervert (lépés: 9 oldalszám: 25).

    c. Kattintson a **Password** mezőre, és adja meg azt a jelszót, amelyet akkor specifikált, amikor beállította a replika szervert (lépés: 9 oldalszám: 25).

    A Kerberos használatához:

    - Válassza ki a **Use master servers Kerberos account** elemet. A főszerver használni fogja saját Kerberos elsődleges nevét hitelesítésre.

      Megjegyzés: A Kerberos csak akkor használható, ha a főszerveren és a replika szerveren a Kerberos engedélyezve van.
14. Amennyiben replikálás közben SSL (Secure Sockets Layer) biztonságot kíván igénybe venni, használja a szerveren a digitális igazoláskezelőt (Digital Certificate Manager) az SSL engedélyezéséhez. A digitális igazoláskezelőt a **Network** elemből indíthatja. Az SSL engedélyezéséről a címtár szolgáltatón további információt talál az “SSL engedélyezése az LDAP címtár szolgáltatón” oldalszám: 15 fejezetben.
15. Ha a szerver nem az alapértelmezett portot használja, adja meg a portszámot a **Port** mezőben.
16. Amennyiben nem kívánja frissíteni a replika szervert minden alkalommal, amikor a főszerveren megváltozik egy bejegyzés, válassza a **Time** opciót. Itt adhatja meg, milyen gyakran kéri a főszervertől a replika frissítését.
17. Kattintson az **OK** gombra.
18. Kattintson a **Database/Suffixes** fülre. Ha a replikálni kívánt utótag nem jelenik meg a listán, vegye fel.
19. Engedélyezze a könyvtárfrissítést minden replika szerveren:
    a. Az iSeries navigátorban nyissa meg a rendszert, amelyen a replika címtár szolgáltató fut.
    b. Válassza a **Network** elemet.
    c. Nyissa meg a **Servers** elemet.
    d. Kattintson a **TCP/IP** pontra.
    e. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
    f. Ha az **Allow directory updates** jelölőnégyzet üres, jelölje be.
    g. Kattintson az **OK** gombra.
20. Ha a replika szervert még nem indította el, most indítsa el.

Megjegyzés: Egy szerver nem lehet egyszerre főszerver és replika szerver.

Információk publikálása a címtár szolgáltatónak

Rendszerét úgy konfigurálhatja, hogy az bizonyos információkat publikálhasson ugyanazon a rendszeren vagy egy másik rendszeren található LDAP címtár szolgáltató számára. Az OS/400 automatikusan publikálja az LDAP címtár szolgáltató számára ezeket az információkat, amikor az iSeries navigátor használatával

módosítja az OS/400 rendszerben ezeket az információkat. A publikálható információk lehetnek rendszer (több rendszer és nyomtató) információk, nyomtatásmegosztási, felhasználói információk, valamint TCP/IP Qos szabályok. Ha többet szeretne megtudni a Szolgáltatási minőségről, olvassa el az LDAP konfiguráció és a QoS alatt leírtakat.

Ha nem létezik az a DN szülő, aki számára az adatok publikálásra kerülnek, a Címtár szolgáltatás automatikusan létrehozza azt. Más OS/400 alkalmazásokat is telepíthet, melyek információkat publikálhatnak egy LDAP címtárba. Továbbá alkalmazásprogram csatolókat (API-kat) is meghívhat a saját programjából, hogy más típusú adatokat közöljön az LDAP címtárral.

Megjegyzések:

1. Ha úgy konfigurálja az OS/400 rendszerét, hogy Users típusú információkat publikáljon az LDAP címtár szolgáltató számára, akkor a rendszer automatikusan átadja a rendszerterjesztési bejegyzéseket az LDAP szervernek. A QGLDSSDD_search alkalmazási programcsatolón (API) keresztül teszi ezt. Így az LDAP címtárat összehangolja a rendszerterjesztési címtár változásaival. A QGLDSSDD API leírását az iSeries Információs központ Programozás fejezete alatt található OS/400 Címtár szolgáltatások témakör tartalmazza. A rendelkezésre álló tájékoztatás magában foglalja:
   - Hogyan lehet az API-t manuálisan meghívni.
   - Hogyan lehet megakadályozni bizonyos felhasználók exportálva legyenek az LDAP szerverbe.
   - Hogyan exportálja az API a rendszerterjesztési címtár mezőket.
2. Ha úgy konfigurálja az OS/400 rendszerét, hogy System típusú információkat publikáljon az LDAP címtár szolgáltató számára, és kiválaszt publikálás céljaira egy vagy több nyomtatót, a rendszer automatikusan összehangolja az LDAP címtárat azokkal a változtatásokkal, melyeket a rendszer nyomtatóin készítenek. A publikálható nyomtató információk között található a nyomtató elhelyezése, a nyomtatási sebesség lap/perc mértékegységben, a két oldalas illetve színes nyomtatás lehetősége, valamint a nyomtató leírása. Ezek az információk a publikáló rendszer rendszer információiból származnak. Hálózati környezetben ezek az információk megkönnyítik a megfelelő nyomtató kiválasztását.
3. Publikálhat OS/400 információkat olyan LDAP címtár szolgáltató számára is, ami nem OS/400 felügyelete alatt működik, amennyiben ezt a szervert az IBM séma használatára konfigurálták.

Konfigurálja rendszerét az alábbi lépések szerint, ha OS/400 információkat akar egy LDAP címtár szolgáltató számára publikálni:

1. Az iSeries navigátorban a jobb oldali egérgombbal kattintson rendszerére, és válassza a **Properties** lapot.
2. Kattintson a **Directory Services** fülre.
3. Kattintson a publikálni kívánt információtípusokra.

   Javaslat:

   Ha egynél többféle információtípust kíván küldeni ugyanarra a helyre, időt takaríthat meg, ha egyszerre több információtípust választ ki beállítás céljából. A Műveletek navigátor az első információtípushoz beadott értéket alapértelmezett értéknek fogja tekinteni a többi információtípus beállításánál.
4. Kattintson a **Details** ikonra.
5. Kattintson a **Publish system information** jelölőnégyzetre.
6. Adja meg a szerveren használni kívánt **hitelesítési módszert**, továbbá a megfelelő hitelesítési információkat.
7. Kattintson az **Edit** gombra, ami az **(aktív) címtár szolgáltató** mező mellett van. A megjelenő kiugró párbeszéddobozba írja be annak az LDAP címtár szolgáltatónak a nevét, mely felé az OS/400 információt publikálni kívánja, majd kattintson az **OK** gombra.
8. Az **Under DN** mezőben adja meg annak a szülőnek az egyedi nevét (DN) ahonnan információt kíván a címtár szolgáltatónak átadni.
9. Töltse ki a **Server connection** keretben azokat a mezőket, melyek megfelelnek konfigurációjának.

   Megjegyzés: SSL-t vagy Kerberos-t használó címtár szolgáltató számára akkor lehet OS/400 információkat publikálni, ha a címtár szolgáltatót a megfelelő protokoll használatára

konfigurálták. “A Kerberos hitelesítés használata az LDAP címtár szolgáltatóval” oldalszám: 42 további tájékoztatást ad az SSL és a Kerberos használatáról.

10. Ha a címtár szolgáltató nem az alapértelmezett portot használja, adja meg a portszámot a **Port** mezőben.
11. Kattintson a **Verify** ikonra, hogy meggyőződhessen arról, hogy a szerveren létezik a DN szülő, és helyesek-e az összeköttetési információk. Ha a címtár útvonala nem létezik, egy párbeszédpanelen megadhatja azt.

    Megjegyzés: Ha a DN szülő nem létezik, és nem hozza létre azt, a publikálás sikertelen lesz.
12. Kattintson az **OK** gombra.

Megjegyzés: Publikálhat egy másik platformon működő LDAP címtár szolgáltató számára is OS/400 információkat. Csak akkor publikálhat felhasználói és rendszer információkat egy címtár szolgáltatónak, ha az a Címtár szolgáltatás sémával kompatibilis sémát használ. Az IBM SecureWay Directory séma definíciók, amelyek tartalmazzák az iSeries Címtár szolgáltatásokat is, a Directory Services weblapon találhatók.

Csak olyan címtár szolgáltató számára publikálhat nyomtató megosztást, amelyik támogatja a Microsofts Active Directory sémát. Egy Active Directory számára történő nyomtató megosztás publikálás lehetővé teszi, hogy a felhasználó iSeries nyomtatóit közvetlenül a Windows 2000 számítógépről a Windows 2000 Add Printer varázslóval konfigurálja. Ahhoz, hogy ezt az Add Printer varázslóval meg lehessen tenni, meg kell adni, hogy a nyomtató a Windows 2000 Active Directory-ban található.

OS/400 információkat címtár szolgáltatóhoz továbbító API-k

A Címtár szolgáltatás beépített publikálási támogatással rendelkezik, ami a felhasználói és rendszer információk továbbítására szolgál. Az elemek listáját a **Directory Services** tartalmazza a rendszer **Properties** párbeszédablakában. Az LDAP szerver konfigurációjának és a publikáló API-k segítségével OS/400 programok készíthetők más típusú információk publikálására. Ezután ezek az információtípusok is szerepelnek a **Directory Services** oldalon. Ezek a felhasználókhoz és a rendszerekhez hasonlóan először le vannak tiltva, de ugyanazzal az eljárással konfigurálhatók. Azt a programot, amely adatokat visz be az LDAP címtárba, publikációs ügynöknek (publishing agent) nevezzük. A publikált információ típusát, ahogy az megjelenik a **Directory Services** lapon, az ügynök nevével hívjuk.

A következő API-k lehetővé teszik, hogy a publikálást saját programjaiba illeszthesse:

QgldChgDirSvrA
: Az alkalmazás a CSVR0500 formátumot használja a kezdeti ügynöknév hozzáadásához, amely a letiltott tételek között szerepel. Az alkalmazás felhasználóinak szóló leírásokban utasítsa őket, hogy az iSeries navigátoron keresztül menjen a Directory Services tulajdonság lapra a publikációs ügynök konfigurálása céljából. Az ügynöknevekre példák lehetnek a rendszer- és ügynöknevek, melyek **Directory Services** oldalon automatikusan rendelkezésre állnak.

QgldLstDirSvrA
: Az API LSVR0500 formátumot használhatja a rendszerben aktuálisan rendelkezésre álló ügynöklista elkészítéséhez.

QgldPubDirObj
: Ezzel az API-val elvégezheti az információ tényleges publikálását.

Ezekről az API-król további információt az iSeries Információs központ Lightweight Directory Access Protocol (LDAP) témánál a Programozás fejezet alatt talál.

Szerver kijelölése címtári utalások részére

Ha utalási szervereket kíván hozzárendelni a címtár szolgáltatóhoz, kövesse az alábbi lépéseket:
1. Az iSeries navigátorban nyissa meg a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Jobb gombbal kattintson a **Directory** feliratra, majd válassza a **Properties** lapot.
5. Kattintson az **Add** gombra.
6. A parancssorban adja meg az utalási szerver nevét URL formátumban. Az alábbiakban példát talál az elfogadható LDAP URL nevekre:
   - ldap://test.server.com
   - ldap://test.server.com:400
   - ldap://9.9.99.255

   Megjegyzés: Ha az utalási szerver nem az alapértelmezett portot használja, adja meg a helyes portszámot az URL részeként, mint ahogy a 400-as port van megadva a fenti második példában.
7. Kattintson az **OK** gombra.

Utótagok felvétele az LDAP címtár szolgáltatóba

Utótag felvétele az LDAP címtár szolgáltatóba lehetővé teszi, hogy a szerver kezelje a címtárfának ezt az ágát.

Megjegyzés: Sohasem tud olyan utótagot felvenni, amely egy, a szerveren már meglévő utótag alatt van. Ha például o=ibm, c=us egy utótag a címtár szolgáltatóján, nem veheti fel a ou=rochester, o=ibm, c=us utótagot.

Ha utótagot kíván felvenni a címtár szolgáltatóba, kövesse az alábbi lépéseket:
1. Az iSeries navigátorban nyissa meg a **Network** ikont.
2. Válassza a **Servers** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** elemet.
5. Kattintson a **Database/Suffixes** fülre.
6. A **New suffix** mezőbe írja be az új utótag nevét.
7. Kattintson az **Add** gombra.
8. Kattintson az **OK** gombra.

Megjegyzés: A könyvtár egy szekciójának utótag pontokkal történő kiegészítése nem jelenti bármilyen objektumok létrehozását. Ha az új utótagnak egy nem létező objektum felel meg, akkor ezt más objektumokhoz hasonlóan létre kell hozni.

Utótagok eltávolítása a címtár szolgáltatóból

Egy utótag eltávolításához az LDAP címtár szolgáltatóból, kövesse az alábbi lépéseket:
1. Az iSeries navigátor menüjében válassza a **Network** pontot.
2. Nyissa meg a **Servers** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** elemet.
5. Kattintson a **Database/Suffixes** fülre.
6. Kattintással válassza ki azt az utótagot, amelyet törölni kíván.
7. Kattintson a **Remove** gombra.

   Megjegyzés: Választhatja az utótag olyan módon történő törlését is, hogy az alatta lévő címtár objektumok ne törlődjenek. Az adatok elérhetetlenné válnak a címtár szolgáltatóból. Az adatok elérését visszaállíthatja, ha újra felveszi az utótagot.

A Címtár szolgáltatás információinak mentése és visszaállítása

A Címtár szolgáltatás a következő helyeken tárol információt:

- Adatbázis könyvtár (alapértelmezés szerint QUSRDIRDB), amely tartalmazza a címtár szolgáltató tartalmát.
- QDIRSRV2 könyvtár, melyben címtár szolgáltató publikált információt tárolja.
- QUSRSYS könyvtár, melyben a címtároló különböző tételeket objektumokban tárol a QGLD-vel kezdődően (a QUSRSYS/QGLD* paranccsal lehet őket menteni).
- Ha a címtár szolgáltatót úgy konfigurálja, hogy az naplózza a címtár változásait, akkor a változási napló a QUSRDIRCL nevű adatbázis könyvtárat használja.

Ha a könyvtár tartalma gyakran változik, a benne levő adatbázis könyvtárt és az objektumokat rendszeresen kell menteni. A konfigurációs adatok ugyancsak tárolásra kerülnek a következő katalógusban:

```
/QIBM/UserData/OS400/Dirsrv/
```

A katalógusban lévő fájlokat is menteni kell, valahányszor megváltoztatja a konfigurációt vagy PTF-eket alkalmaz.

Olvassa el a Rendszermentés és visszaállítás, SA12-7171 könyvben az OS/400 adatok mentését és visszaállítását.

Címtári adatok tulajdonjogának és elérésének kezelése

A címtári adatok tulajdonjogának és elérésének kezelése az alábbi feladatokat foglalja magában:

- “Címtár objektumok tulajdonjogi jellemzőinek beállítása”
- “Elérésvezérlési listák (ACL-ek) kezelése”
- “ACL csoportok kezelése” oldalszám: 31

Címtár objektumok tulajdonjogi jellemzőinek beállítása

Címtár objektumok tulajdonjogi jellemzőit beállíthatjuk az alábbi módon:

1. Az iSeries navigátorban nyissa meg a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.

   Ha még nincs kapcsolatban a címtár szolgáltatóval, megjelenik a **Connect to Directory Server** párbeszédpanel. Vegye fel a kapcsolatot rendszergazdaként, vagy mint annak az objektumnak a tulajdonosa, amely tulajdonjogának a jellemzőit szeretné beállítani.
5. A címtárfában válassza ki azt az objektumot, amely tulajdonjogának a jellemzőivel kíván dolgozni, majd kattintson az **OK** gombra.

Elérésvezérlési listák (ACL-ek) kezelése

Az elérésvezérlési listák (ACL-ek) használata magában foglalja explicit és implicit ACL-ek hozzárendelését címtár objektumokhoz, felhasználók felvételét ACL-ekbe, felhasználók eltávolítását ACL-ekből, valamint a címtár objektumok tallózását. Ne felejtse el, hogy a V5R1 változattól kezdődően a Címtár szolgáltatás egy új ACL modellt támogat, ezért még ha korábban használt ACL-eket, célszerű velük újra megismerkedni.

ACL-ek használatához végezze el az alábbi lépéseket:

1. Az iSeries navigátorban nyissa meg a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza az **Authority** pontot.

Ha még nincs kapcsolatban a címtár szolgáltatóval, megjelenik a **Connect to Directory Server** párbeszédpanel. Vegye fel a kapcsolatot rendszergazdaként, vagy mint annak az objektumnak a tulajdonosa, amely ACL-jét szeretné kezelni.

5. A címtárfában válassza ki azt az objektumot, amely ACL-jével kíván dolgozni, majd kattintson az **OK** gombra.
6. Kattintson az **ACL** fülre.

ACL csoportok kezelése

Ha ACL (elérésvezérlési lista) csoportokat kíván kezelni, kövesse az alábbi lépéseket:

1. Az iSeries navigátorban válassza a **Network** elemet.
2. Válassza ki a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza az **ACL Groups** elemet.

Adminisztrációs hozzáférés kezelése a jogosult felhasználók számára

A V5R2 változattól kezdve adminisztrátori hozzáférést adhat azoknak a felhasználói profiloknak, amelyeknek hozzáférésük van a Címtár szolgáltatások adminisztrátori (QIBM_DIRSRV_ADMIN) funkció azonosítóhoz (ID).

Például, ha a JOHNSMITH felhasználói profilnak hozzáférése van a Címtár szolgáltatások adminisztrátori funkció azonosítóhoz (ID), és a Directory property párbeszédablakban kiválasztotta a Grant administrator access to authorized users opciót, akkor a JOHNSMITH profil LDAP adminisztrátori jogosultsággal fog rendelkezni. Amikor a profil az ″os400-profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com″ DN beállítással kapcsolódik a címtár szolgáltatóhoz, a felhasználó adminisztrátori jogosultsággal fog rendelkezni. A rendszer objektumok utótagja ebben a példában os400-sys=systemA.acme.com. A tervezett felhasználókról itt olvashat: “Operációs rendszer leképzett háttér objektumai” oldalszám: 43.

Az opció kiválasztásához az alábbi lépéseket kell elvégezni:

1. Az iSeries navigátor menüjében nyissa meg a **Network** ikont.
2. Nyissa meg a **Servers** elemet.
3. Kattintson a jobb egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
4. Az **Administrator information** alatti **General** fülön válassza ki a **Grant administrator access to authorized users** opciót.

Hajtsa végre az alábbi lépéseket, amikor a Címtár szolgáltatások adminisztrátori jogosultságát állítja be a felhasználói profilban:

1. Az iSeries navigátorban kattintson a jobb egérgombbal a rendszernévre, és válassza ki az **Application Administration** elemet.
2. Kattintson a **Host Application** fülre.
3. Bontsa ki az **Operating System/400** elemet.
4. Kattintson a **Directory Services Administrator** elemre, melynek hatására bejelöli (kiemeli) az opciót.
5. Kattintson a **Customize** gombra.
6. Bontsa ki a **Users**, **Groups** vagy **Uses not in a group** részt, amelyiket megfelelőnek tartja a felhasználó számára.
7. Válassza ki az **Access allowed** listához hozzáadandó felhasználót vagy csoportot.
8. Kattintson az **Add** gombra.
9. Kattintson az **OK** gombra a változtatások mentéséhez.
10. Kattintson az **OK** gombra az **Application Administration** párbeszédablakban.

Az LDAP címtár eléréseinek és változásainak nyomon követése

Lehet, hogy tájékoztatást akar kapni az LDAP címtár eléréseiről és változtatásairól. Az LDAP címtár változásait tartalmazó napló segítségével nyomon követheti a címtár változásait. A változási napló módosítása a cn=changelog speciális utótag alatt található meg. Ezt a QUSRDIRCL könyvtár tárolja.

A változási napló engedélyezéséhez kövesse ezeket a lépéseket:
1. Az iSeries navigátor menüjében válassza a **Network** pontot.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
5. Kattintson a **Database/Suffixes** fülre.
6. Válassza ki a **Log directory changes** elemet.
7. (választható) A **Maximum entries** mezőben adja meg a változási naplóban megtartandó bejegyzések maximális számát.

   Megjegyzés: Annak ellenére, hogy ez a paraméter nem kötelező, erősen fontolja meg a bejegyzések maximális számának megadását. Ha nem jelöli ki a bejegyzések maximális számát, a változási napló minden bejegyzést megtart, így a mérete nagyon nagyra nőhet.

A changeLogEntry objektum osztály képviseli a címtár szolgáltatóra vonatkozó változásokat. A changeNumber által megadott módon, a changelog tárolóban lévő összes bejegyzés rendezett készlete adja a változások halmazát. A változás napló csak olvasható.

Bármely felhasználó, aki rajta van a cn=changelog utótagra vonatkozó Access Control List nevű listán, keresheti a változás naplóban lévő bejegyzéseket. A cn=changelog változási napló utótagnál kizárólag kereshet. Ne kíséreljen meg hozzáadni, módosítani vagy törölni a változási napló utótagnál, még akkor sem, ha rendelkezik hozzá jogosultsággal. Ez megjósolhatatlan eredményeket fog okozni.

Példa:

A következő példa az ldapsearch parancssor segédprogramot használja a szerveren naplózott összes változási napló bejegyzés betöltéséhez:

```
ldapsearch -h ldaphost -D cn=rendszergazda -w jelszó -b cn=changelog  (changetype=*)
```

Objektum naplózás engedélyezése a címtár szolgáltató számára

A Címtár szolgáltatás támogatja az OS/400 biztonsági ellenőrzést. Ha a QAUDCTL rendszer értékben *OBJAUD került beállításra, az iSeries navigátor segítségével engedélyezhető az objektum naplózás.

A Címtár szolgáltatás számára az objektum naplózás az alábbi lépésekkel engedélyezhető:
1. Nyissa meg az iSeries navigátorban a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, majd válassza a **Properties** lapot.
5. Kattintson az **Auditing** fülre.
6. Válassza ki a szerverben használni tervezett naplózási beállításokat.

A naplózási beállítások az **OK** gombra történő kattintás után hatályba lépnek. Nem kell az LDAP címtárszolgátatót újraindítani. További információk: “Címtár szolgáltatás biztonsága” oldalszám: 41.

Az LDAP címtár szolgáltató teljesítményének beállítása

Az LDAP címtár szolgáltató teljesítményét az alábbi jellemzők módosításával lehet beállítani:
- A keresés mérete
- A keresésekre megengedett legnagyobb idő
- A szerver tranzakciók beállításai
- Az adatbázis kapcsolatok és a szerver szálak száma

A címtár szolgáltató teljesítményértékeinek beállítását az alábbi módon végezheti el:
1. Az iSeries navigátor menüjében válassza a **Network** elemet.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
5. Kattintson a **Performance** fülre.

A címtár szolgáltató teljesítményét beállíthatja úgy is, hogy megváltoztatja a szerver által használt adatbázis kapcsolatok és szerver szálak számát. Ennek megváltoztatásához az alábbi lépéseket kell elvégezni:
1. Az iSeries navigátor menüjében válassza a **Network** elemet.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **Directory** feliratra, és válassza a **Properties** lapot.
5. Kattintson a **Database/Suffixes** fülre.

Fejezet 5. Címtár szolgáltatás: koncepciók és hivatkozások

Az alábbi helyeken található információk segítenek abban, hogy jobban megismerje és hatékonyabban használja a Címtár szolgáltatás LDAP szervert:
- “LDAP elérésvezérlési listák (ACL-ek)”
- “LDAP adatcsere formátum” oldalszám: 37
- “Nemzeti nyelvek támogatása (NLS)” oldalszám: 39
- “LDAP címtári objektumok tulajdonjoga” oldalszám: 39
- “LDAP címtári utalások” oldalszám: 39
- “Tranzakciók” oldalszám: 40
- “LDAP címtár szolgáltatók replikája” oldalszám: 40
- “Címtár szolgáltatás biztonsága” oldalszám: 41
- “Operációs rendszer leképzett háttér objektumai” oldalszám: 43
- “Címtár szolgáltatás és OS/400 naplózási támogatás” oldalszám: 48

Az LDAP alapjairól és az LDAP szerver üzembeállításáról olvashat az alábbi helyen is: Fejezet 3, “Első lépések a Címtár szolgáltatás használatában” oldalszám: 7.

LDAP elérésvezérlési listák (ACL-ek)

A legtöbb esetben nem szükséges korlátozni a hozzáférést az LDAP címtár szolgáltatón lévő adatokhoz. Vegyünk például egy LDAP címtár szolgáltatót a cége Intranetjén, amely a cég alkalmazottainak telefonszámait tartalmazza. Valószínűleg az a rendeltetése, hogy minden alkalmazott megtekinthesse a címtárban levő adatokat.

Azonban a cég elnöke nem szeretné, ha minden alkalmazott hozzáférhetne az ő telefonszámához. Ezen segít az **elérésvezérlési lista (ACL)**. Egy ACL segítségével korlátozhatja a hozzáférést az elnök címtárbeli bejegyzésénél azokra az alkalmazottakra, akiktől az elnök szívesen veszi a telefonhívást.

Az ACL-ekkel szabályozható, hogy kik kapnak jogosultságot a címtár objektumok felvételére és törlésére. Azt is be lehet állítani, hogy a felhasználók képesek legyenek-e olvasni, írni, keresni és összehasonlítani a címtár attribútumokat. Egy ACL örökölt (inherited) vagy explicit lehet. Tehát, az ACL-eket a következő módok egyike szerint használhatja:
- Explicit módon beállíthat ACL-t egy megadott objektumhoz.
- Meghatározhatja, hogy az objektumok öröklik az ACL-eiket az LDAP címtár hierarchiájában feljebb álló objektumoktól.

Tehát az előző példában a cég elnöke nem szeretné, ha minden alkalmazott hozzáférhetne az ő telefonszámához. Arra viszont szüksége lehet, hogy minden menedzser megtalálja, ha keresi. Ebben az esetben egy **ACL csoport** létrehozása leegyszerűsíti a jogosultság megadását a menedzsereknek. Az ACL csoportok segítségével egyes egyének helyett megadott felhasználói csoportok számára biztosíthat hozzáférést a címtár szolgáltató adataihoz. Különösen hasznos ez, ha a felhasználók egyazon csoportja egynél több objektumhoz kell, hogy hozzáférjen. Ha az elnök telefonszámához hozzáféréssel rendelkező menedzserek csoportjának, például, a jövőben hozzáférést kellene biztosítani a fizetési bejegyzésekhez is, újrahasználhatnánk a meglévő ACL csoportot.

ACL modellek

A Címtár szolgáltatás összes verziója támogatja az osztályszintű elérési engedély modellt. Ebben a modellben minden LDAP attribútum típus rendelkezik Normál (Normal), Érzékeny (Sensitive) vagy Kritikus (Critical) osztályozással. Az attribútum séma fájlok vezérlik ezt a besorolást. Amikor felveszünk egy felhasználót egy objektum ACL listájába, megadjuk, mely besorolást olvashatja, írhatja, keresheti vagy hasonlíthatja össze a felhasználó. A legtöbb sémában a telefonszám Normál attribútumú besorolást kapna. Ezért a fenti példában szereplő menedzserek olvasási hozzáférést kapnának az elnök címjegyzékében levő

objektumok Normál attribútumaihoz, hogy elérhessék az elnök telefonszámát. Azonban még így sem férhetnének hozzá Érzékeny és Kritikus információkhoz. A Címtár szolgáltatás összes verziója támogatja az osztályszintű elérési engedély beállítását.

A Címtár szolgáltatás támogat egy attribútum szintű engedély modellt is. Ebben a modellben speciális attribútumok számára elérési osztályuktól függetlenül olvasás, írás, keresés, és összehasonlítás jogosultságok specifikálhatók. Fontolja meg újra a fenti példát. Az attribútum szintű engedély modellnél a menedzsereknek a telephoneNumber (telefonszám) attribútumhoz olvasási hozzáférés adható, még ha általában nincs is hozzáférésük a Normál attribútumokhoz.

Az attribútum szintű engedély modell csak a SecureWay Címtár szolgáltatás 3.2 és későbbi szerverekkel használható. Alapértelmezés szerint nincs engedélyezve. Engedélyezési opciója akkor áll rendelkezésre, amikor az ACL-eket használják. Ezt követően nincs engedélyezve, a modellt csak a szerver újrakonfigurálásával, vagy az adatbázis visszatöltésével lehet letiltani. Viszont mielőtt ennek a modellnek az engedélyezéséről dönt legyen tisztában azzal, hogy nem képes ezt bármelyik LDAP V2 kliensről (beleértve a V5R1 verzió előtti iSeries navigátorokat is) kezelni. Ha megkísérli ezt megtenni, elronthat ACL bejegyzéseket.

Különleges ACL értékek

Kezdetben minden objektum a Címtár szolgáltatás címtárban rendelkezik egy ACL-lel, amely egy különleges ACL csoportot tartalmaz: CN=Anybody, amelyik az összes címtárhasználót magában foglalja. Alapértelmezés szerint ez a csoport minden objektum normál osztályú attribútumához írási, keresési és összehasonlítási hozzáféréssel rendelkezik.

Szándékában állhat, hogy egyes objektumok elérhetősége ugyanaz legyen az összes olyan felhasználó számára, akiket egy nem névtelen összekapcsolódás a címtár katalógushoz rendelt. Ehhez használja a cn=Authenticated különleges elérésvezérlési lista (ACL) csoportot.

Ha azt akarja specifikálni, hogy milyen elérési engedélyekkel rendelkezik egy objektum önmagával kapcsolatban, akkor a cn=this különleges DN-t használhatja. Ez engedélyezi, hogy az utód bejegyzések, akik öröklik az ACL-eket automatikusan felhatalmazást nyerjenek a műveletek saját objektumaikon való végrehajtásához.

További információk

Ahhoz, hogy az iSeries navigátoron keresztül kezelhesse az ACL-eket, nem szükséges ismerni a Címtár szolgáltatás ACL implementációjának minden részletét. Mindamellett, ha LDIF fájlok használatakor ACL-lel kapcsolatban álló attribútumokat akar megadni, vagy ACL-eket akar az LDAP parancssori segédprogramokkal használni, meg kell ismerkedni az ACL-ek által használt attribútumokkal. Az ACL attribútumokról itt olvashat: Access Control Lists Reference kiadványban  , IBM SecureWay Directory Management Tool dokumentációban  .

ACL-ek és ACL csoportok beállításával és módosításával kapcsolatban kövesse az alábbi hivatkozásokat:

“Elérésvezérlési listák (ACL-ek) kezelése” oldalszám: 30
“ACL csoportok kezelése” oldalszám: 31

LDAP adatcsere formátum

Az LDAP adatcsere formátum (data interchange format, LDIF) leegyszerűsíti a címtár információk átvitelét LDAP címtár szolgáltatók között. Az LDIF fájlok egyszerű szöveges formátumban tartalmazzák az LDAP címtári bejegyzéseket. A címtár szolgáltató által használt LDIF fájlok formátuma kissé megváltozott a Címtár szolgáltatás V4R5 verziótól kezdődően. Az LDIF fájlok olyan sorok sorozatából állnak, amelyek leírják a címtári bejegyzést, vagy a címtári bejegyzésre vonatkozó változtatások halmazát. Mindkettőt nem írhatják le.

Az LDIF bejegyzések általános formátuma az alábbi:

```
version: 1
dn: distinguished name
attrtype1: attrvalue1
...
```

ahol:

- *version* az LDIF fájl formátumának verzióját mutatja. A verziószám 1. Ha hiányzik a verziószám, akkor az LDIF fájl régebbi LDIF fájl formátumként lesz figyelembe véve. Ha az LDIF fájl verziója 1, akkor a tartalmat UTF-8 szerint kell kódolni.
- *distinguished name* a címtári bejegyzés megkülönböztető neve
- *attrtype1* egy LDAP attribútum típus (mint pl. cn vagy ou)
- *attrvalue1* az attribútum értéke

Minden bejegyzésnek több attribútuma lehet. Minden egyes attribútum külön sorban jelenik meg. Ha egy attribútum értéke hosszabb, mint egy egész sor, folytatható a következő sorban, és szóköz vagy tabulátor karakter előzi meg.

Üres sorok választják el a többszörös bejegyzéseket egy LDIF fájlon belül. A font jellel (#) kezdődő sorok kommentár sorok, és figyelmen kívül kell hagyni őket az LDIF fájl elemzésekor.

Minden megkülönböztető név vagy attribútum érték, amely eleget tesz a következő feltételek egyikének, alap-64 szerinti kódolásúnak kell lenni:
- ″Kocsi vissza″ vagy ″soremelés″ karaktert tartalmaz.
- Kettősponttal (:), szóközzel (SPACE) vagy a kisebb, mint (<) jellel kezdődik.
- Szóközzel végződik.

Az alap-64 szerint kódolt attribútumokat az attribútum és az érték közötti két kettőspont használatával jelölheti ki.

A külső hivatkozások a fájlban :// URL formátumban vannak. Az attribútum típusa és a külső hivatkozás között kettőspontnak és kisebb, mint (<) jelnek kell lenni.

Néhány példát találhat itt az LDIF fájlokra:

1. példa: Egyszerű LDAP fájl két bejegyzéssel

```
version: 1
   dn: cn=Barbara Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Barbara Jensen
   cn: Barbara J Jensen
   cn: Babs Jensen
   sn: Jensen
   uid: bjensen
   telephonenumber: +1 408 555 1212
   description: A big sailing fan.
```

```
   dn: cn=Bjorn Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Bjorn Jensen
   sn: Jensen
   telephonenumber: +1 408 555 1212
   description:Babs is a big sailing fan, and travels extensively in
   search of perfect sailing conditions.
   title:Product Manager, Rod and Reel Division
```

2. példa: Alap-64 kódolt értéket tartalmazó fájl

```
version: 1
   dn: cn=Gern Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Gern Jensen
   cn: Gern O Jensen
   sn: Jensen
   uid: gernj
   telephonenumber: +1 408 555 1212
   description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvdSBhcmUhICBUaGlzIHZhbHVlIGlzIGJ
    hc2UtNjQtZW5jb2RlZCBiZWNhdXNlIGl0IGhhcyBhIGNvbnRyb2wgY2hhcmFjdGVyIGluIGl0ICh
    hIENSKS4NICBCeSB0aGUgd2F5LCB5b3Ugc2hvdWxkIHJlYWxseSBnZXQgb3V0IG1vcmUu
```

3. példa: Változási rekordok és megjegyzések sorozatát tartalmazó fájl

Megjegyzés: A változási rekordokat tartalmazó LDIF fájlok nem importálhatók be közvetlenül a szerverre. Mindazonáltal az LDAP parancsértelmező segédprogramok támogatják őket.

```
version: 1
   # új bejegyzés felvétele
   dn: cn=Fiona Jensen, ou=Rochester, o=Big Company, c=US
   changetype: add
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Fiona Jensen
   sn: Jensen
   uid: fiona
   telephonenumber: +1 408 555 1212
   jpegphoto:< file:///usr/local/directory/photos/fiona.jpg

   # meglévő bejegyzés törlése
   dn: cn=Robert Jensen, ou=Rochester, o=Big Company, c=US
   changetype: delete

   # a bejegyzés viszonylagos megkülönböztető nevének módosítása
   dn: cn=Paul Jensen, ou=Rochester, o=Big Company, c=US
   changetype: modrdn
   newrdn: cn=Paula Jensen
   deleteoldrdn: 1
```

Fontos a bejegyzések sorrendje az LDIF fájlon belül. Ahhoz, hogy sikeresen lehessen hozzáadni egy, az LDIF fájlban megadott, bejegyzést az LDAP címtárához, a saját szülő bejegyzésének léteznie kell a címtár névterületén. A fenti példában a második és harmadik bejegyzést nem lehetne felvenni, ha az első nem létezne.

Hasonló módon, egy LDIF fájl importálásához olyan szerverbe, amely bizonyos utótagokat támogat, szükséges, hogy az LDIF fájl minden utótaghoz rendelkezzen saját bejegyzéssel. Így például, ha a szerver a következő utótagokkal rendelkezik: ou=Rochester, o=Big Company, c=US, a fent bemutatott LDIF fájl importálása megvalósítható. Ha azonban ehelyett a szerver utótagjai a következők: o=Big Company, c=US, szükség van egy bejegyzésre az LDIF fájlban elsőként megadott utótaghoz:

```
dn: o=Big Company, c=US
objectclass: organization
o: Big Company
```

Az LDIF fájlok specifikus formátumát és tartalmát az exportáló szerver sémája határozza meg. Egy LDIF fájl importálható minden olyan szerverbe, amely a fájlt exportáló szerverrel azonos sémát használ. A különböző szállítók LDAP szerverei különböző sémát használnak (különböző objektum osztályokkal és attribútumokkal). Az egyik szerveren készült LDIF fájl ezért általában nem vihető át egy másik szerverre.

Az LDIF fájl Request for Comments (RFC) specifikációk a következő URL címen érhetők el:

http://www.ietf.org/rfc/rfc2849.txt 

Kapcsolódó eljárások:

“LDIF fájl importálása” oldalszám: 22
“LDIF fájl importálása” oldalszám: 22

Nemzeti nyelvek támogatása (NLS)

A V4R5 változattól kezdve az OS/400 Directory Services LDAP szerver és az OS/400 LDAP kliens az LDAP V3 verzión alapszik. A következő NLS szempontokra legyen tekintettel:

- Az adatok átvitele UTF-8 formátumban történik az LDAP szerverek és a kliensek között. Az összes ISO 10646 karakter megengedett.
- A címtár szolgáltató LDAP szerver UTF-16 leképezési módszert használ az adatok adatbázisban történő tárolásához.
- A szerver és a kliens kis/nagybetű független karakterlánc összehasonlításokat végez. A nagybetűs algoritmusok nem hibátlanok minden nyelvre (helyi sajátosságok).

Az UCS-2 módszerről további információk az iSeries Információs központ Tervezés fejezete alatt, a Globalizáció témánál találhatók.

LDAP címtári objektumok tulajdonjoga

Az LDAP címtárban minden egyes objektumnak legalább egy tulajdonosa van. Az objektum tulajdonosának joga van azt kitörölni. A tulajdonosokon kívül a szerver adminisztrátora módosíthatja az objektum tulajdonjogi jellemzőit és az elérésvezérlési lista (ACL) attribútumait. Egy objektum tulajdonjoga örökölt (inherited) vagy explicit lehet. Így tulajdonjog hozzárendelése az alábbi módszerekkel lehetséges:

- Explicit módon adhat tulajdonjogot egy megadott objektumra.
- Meghatározhatja, hogy az objektumok öröklik a tulajdonosaikat az LDAP címtár hierarchiájában feljebb álló objektumoktól.

A Címtár szolgáltatás lehetővé teszi, hogy ugyanahhoz az objektumhoz több tulajdonost rendeljen hozzá. Lehetővé teszi továbbá, hogy egy objektum önmaga tulajdonosa legyen. Ennek megvalósítása érdekében a cn=this speciális DN-t kell az objektum tulajdonosok listájába beiktatni. Tegyük fel, például, hogy a cn=A objektum tulajdonosa cn=this. Bármely felhasználónak tulajdonosi hozzáférése lesz a cn=A objektumhoz, ha mint cn=A kapcsolódik a szerverhez.

Kapcsolódó eljárás:

“Címtár objektumok tulajdonjogi jellemzőinek beállítása” oldalszám: 30

LDAP címtári utalások

Az utalások lehetővé teszik, hogy az LDAP címszolgáltatók csoportosan működjenek. Ha a kliens által igényelt DN nem található az egyik címtár szolgáltatón, a szerver automatikusan átküldheti (utalhatja) az igénylést bármely más LDAP szerverre.

A Címtár szolgáltatás rendszeren két különböző típusú utalást lehet használni. Meghatározhatók alapértelmezett utalási szerverek, melyekhez az LDAP szerver utalja a klienseket, amikor egy DN nincs a címtárban. Arra is felhasználható az LDAP kliens, hogy utalás objektumosztályú (objectClass utalás) bejegyzéseket vigyen fel a címtár szolgáltatóra. Így olyan utalások határozhatók meg, melyek a kliens által ígényelt specifikus DN-re alapulnak.

Megjegyzés: A Címtár szolgáltatás utalási objektumainak csak egy megkülönböztető nevet (dn), egy objektum osztályt (objectClass), és egy utalás (ref) attribútumot kell tartalmazni. Az “ldapsearch segédprogram” oldalszám: 56 alatt egy példa illusztrálja a korlátozást.

Az utalási szerverek szorosan kapcsolódnak a replika szerverekhez. Mivel a replika szerveren lévő adatot egy kliens nem módosíthatja, a replika minden címtár módosításra vonatkozó igényt a főszerverre utal.

Tranzakciók

A rendszer LDAP címtár szolgáltatóját konfigurálhatja úgy, hogy megengedje a klienseknek tranzakciók használatát. Egy tranzakció a LDAP címtári műveletek csoportja, amit a címtár szolgáltató egy egységként kezel. A tranzakciót alkotó LDAP műveletek közül egyik sem végleges, míg a tranzakció összes művelete sikeresen véget nem ért, és a címtár szolgáltató a tranzakciót nem nyugtázza. Ha bármelyik művelet sikertelen volt, vagy törölték a tranzakciót, egyetlen művelet sem kerül végrehajtásra. Ez megkönnyíti a felhasználó dolgát, mert szervezetten képes LDAP műveleteket megvalósítani. Például a felhasználó állítson össze a kliensen egy tranzakciót, mellyel több címtári bejegyzést kíván törölni. Ha a tranzakció közben megszakad a kliens és a szerver között a kapcsolat, egyetlen bejegyzés sem kerül törlésre. Ezért a felhasználó újra indíthatja a tranzakciót, nem kell vizsgálnia azt, hogy mely bejegyzés került törlésre.

A következő LDAP műveletek lehetnek egy tranzakció részelemei:

- felvétel
- módosítás
- RDN módosítása
- törlés

Megjegyzés: Tilos a tranzakcióba címtár séma (cn=schema utótag) módosítást beiktatni. Ámbár ilyeneket be lehetne iktatni, de nem lehet őket visszavonni, ha a tranzakció hibázott. Egy hiba a címtár szolgáltatóban előre nem látható problémákat okozhat.

A tranzakciókról itt olvashat: Limited Transaction Support című függelékben az IBM SecureWay Directory Client SDK Programming Reference című könyvben.

LDAP címtár szolgáltatók replikája

A replika (másodpéldány) LDAP címtár szolgáltatón tárolt információ megegyezik a mester vagy fő LDAP címtár szolgáltatón tárolt információval. Két fő előnye van annak, ha az LDAP címtáráról egy vagy két replikát készít:

- A replikák felgyorsítják a címtár kereséseket. Ahelyett, hogy az összes kliens az egyetlen főszerverre irányítaná a keresési kéréseit, megoszthatják a kéréseket a főszerver és replika szerverek között.
- A replikák a főszerver biztonsági mentéséül is szolgálnak. Ha a főszerver nem érhető el, a replika továbbra is teljesítheti a keresési kérelmeket, és hozzáférést bíztosíthat a címtár adataihoz.

A replika szerverek csak olvashatóak. Ha egy jogosult felhasználó megkísérel módosítani egy bejegyzést a replika szerveren, az átutalja a kérelmet a fő címtár szolgáltató felé.

Kapcsolódó eljárás:

“A címtár szolgáltató új replikájának beállítása” oldalszám: 23

Címtár szolgáltatás biztonsága

Biztonsági ellenőrzés

A V5R1 változattól kezdve a Címtár szolgáltatás támogatja az OS/400 biztonsági ellenőrzését. Az ellenőrzésre kerülő elemek a következőek:

- A címtár szolgáltató létrejött és megszűnt kapcsolatai.
- Az LDAP címtár objektumok engedélyének változásai.
- Az LDAP címtár objektumok tulajdonjogának változásai.
- LDAP címtári objektumok létrehozása, törlése és megváltoztatása, továbbá keresés a címtári objektumok között.
- A rendszergazda jelszavának megváltoztatása, és megkülönböztető nevek (DN-ek) frissítése.
- Felhasználói jelszavak megváltoztatása.
- Fájlok importálása és exportálása.

Lehet, hogy meg kell változtatni az OS/400 naplózási beállításait, mielőtt használatba veszi a címtári bejegyzések naplózását. Ha a QAUDCTL rendszer értékbe *OBJAUD lett beállítva, akkor az iSeries navigátor segítségével engedélyezhető az objektum naplózás. A naplózásról további információkat a következő kiadványban talál: *Security - Reference*  vagy az iSeries Információs központ Biztonság ellenőrzése című témakörben.

Összeköttetés hitelesítés és biztonság

A Címtár szolgáltatás a következő eljárásokkal javítja az LDAP címtár szolgáltató és a kliensek közti adatátvitel biztonságát:

- Védett socket réteg (Secure Sockets Layer SSL) kapcsolatok.
- Kerberos hitelesítés.
- CRAM-MD5 jelszó titkosítás.

Védett socket réteg (SSL) és Fordítási réteg biztonság használata LDAP címtár szolgáltatóval

Az LDAP címtár szolgáltatóval történő kapcsolatok biztonságosabbá tételéhez, a Címtár szolgáltatás alkalmazhatja az SSL (Secure Sockets Layer, védett socket réteg) elnevezésű biztonsági eljárást.

Az SSL csak akkor használható a Címtár szolgáltatás szolgáltatással, ha egy Cryptographic Access Provider termék (5722-ACx) a rendszerben telepítésre került. Ha az SSL-t az iSeries navigátorról kívánja használni, telepítenie kell a Client Encryption (5722-CEx) terméket a PC-n. Szüksége lesz erre a szoftverre, ha az alábbiakat kívánja végrehajtani:

- A Címtár szolgáltatás konfigurálása és adminisztrálása egy munkaállomásról SSL kapcsolaton keresztül. Ez magában foglal olyan feladatokat is, amelyek az iSeries navigátor segítségével hajthatók végre.
- SSL kapcsolat használata olyan alkalmazásokban, amelyeket a Windows kliens alkalmazás programillesztők (API-k) segítségével hozott létre.

Az SSL egy szabvány az Internet biztonságához. Az SSL LDAP kliensekkel és replika LDAP szerverekkel történő kapcsolatra egyaránt használható. A szerver hitelesítésen túlmenően használhat kliens hitelesítést is, ami további biztonságot jelent az SSL kapcsolatok számára. A kliens hitelesítés megköveteli, hogy az LDAP kliens bemutassa digitális igazolását, ami megerősíti a kliens azonosságát a szerver számára, mielőtt létrejönne a kapcsolat.

A rendszeren telepíteni kell a Digitális igazolás kezelőt az SSL használatához (az OS/400 34-es opciója). A DCM programtermék lehetővé teszi, hogy digitális igazolásokat állítson elő, kezeljen és tároljon. A digitális igazolásról és a DCM használatáról információt a Digital Certificate Manager dokumentációban talál. Az

iSeries, SSL-jéről információt a Biztonságos alkalmazások SSL segítségével című részben talál. Az iSeries szerverre telepített TLS-ről olvashat az SSL és Szállítási réteg biztonság (TLS) protokollok támogatása részben.

A Kerberos hitelesítés használata az LDAP címtár szolgáltatóval

A Címtár szolgáltatás lehetővé teszi az LDAP címtár szolgáltató olyan beállítását, hogy használja a Kerberos hitelesítést. A Kerberos egy hálózati hitelesítési protokoll, ahol a rejtjelezésre egy titkos kulcsot használnak, ami a kliens-szerver alkalmazásoknál szigorú hitelesítést biztosít.

Kerberos hitelesítés csak akkor használható, ha a rendszerben telepítve lett egy titkosító termék (Cryptographic Service Provider) az 5722AC2 vagy a 5722AC3 típusú. Emellett konfigurálni kell a hálózati hitelesítési szolgáltatást.

A Címtár szolgáltatás Kerberos szolgáltatása támogatást biztosít a GSSAPI SASL eljárás számára. Ez lehetővé teszi, hogy a SecureWay és a Windows 2000 LDAP kliensei az LDAP címtár szolgáltatóval használják a Kerberos hitelesítést.

A szerver a következő alakú **Kerberos elsődleges (principal) nevet** használja:

```
service-name/host-name@realm
```

A service-name az LDAP, a host-name a rendszer teljes TCP/IP neve, a realm a rendszer Kerberos konfigurációjában specifikált alapértelmezés szerinti adatstruktúrája.

Például ha van az acme.com TCP/IP tartományban egy my-as400 nevű rendszer ACME.COM alapértelmezés szerinti Kerberos adatstruktúrával, akkor az LDAP szerver Kerberos elsődleges neve LDAP/my-as400.acme.com@ACME.COM . A Kerberos alapértelmezés szerinti adatstruktúrája a Kerberos konfigurációs fájlban a default_realm direktívával van megadva (default_realm = ACME.COM). A Kerberos konfigurációs fájl alapértelmezés szerint a /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf fájl. Megállapodások szerint a Kerberos adatstruktúra névben nagybetűt, míg a hosztgép névben kisbetűt használnak. Az LDAP/ kötelezően nagybetű. A címtár szolgáltató nem konfigurálható a Kerberos hitelesítés használatára, ha az alapértelmezés szerinti adatstruktúra nem lett a korábban konfigurálva.

Kerberos hitelesítés használata esetén az LDAP címtár szolgáltató egy megkülönböztető nevet (DN-t) társít kapcsolattal, ami meghatározza a címtári adatokhoz a hozzáférést. Kiválasztható, hogy a szerver DN-t a következő módszerek közül melyikkel társítsák:

- A szerver a Kerberos ID alapján hozza létre a DN-t. Ennek az opciónak kiválasztása esetén a principal@realm alakú Kerberos azonosító egy ibm-kn=principal@realm alakú DN-t generál. Az ibm-kn= egyenlő ibm-kerberosName= kifejezéssel.
- A szerver kereshet a címtárban egy megkülönböztetett nevet (DN-t), aminek egyik bejegyzése tartalmazza a Kerberos elsődleges nevet és adatstruktúrát. Ha ezt az opciót választja, a szerver az alábbiakban ismertett módon keres a címtárban egy bejegyzést, ami a Kerberos azonosítót határozza meg:
  - A szerver keresi a címtárban a krbRealm-V2 objektumot, melynek van egy krbRealmName-V2 attribútuma, ami megegyezik a Kerberos adatstruktúrával. Ha talál egy ilyen bejegyzést, akkor keres DN-eket, melyeket princSubtree attribútumban specifikáltak egy krbPrincipalName attribútummal rendelkező bejegyzésnek, ami megegyezik az elsődleges névvel és az adatstruktúra nevével. Ha a krbAliasedObjectName helyen konfigurált DN tartalmazza az előzőleg megtalált bejegyzés DN-jét, akkor a krbAliasedObjectName helyen konfigurált DN-t fogja használni. Egyébként, a bejegyzés DN-je kerül felhasználásra. Ezt a módszert elsősorban akkor használják, amikor egy Kerberos KDC tárol Kerberos elsődleges információkat az LDAP címtárban.
  - Ha a fent ismertetett keresés sikertelen, akkor a szerver keres a címtárban egy bejegyzést, ami az ibm-securityIdentities segédosztályt használja, és rendelkezik egy altSecurityIdentities attribútummal, melynek értéke KERBEROS:principal@realm. Ezzel a módszerrel Kerberos azonosítók társíthatók címtári bejegyzésekkel, amikor a KDC nem tárol elsődleges adatokat a címtárban.

Kell, hogy legyen egy kulcstáblázat (keytab) fájl, ami tartalmaz egy kulcsot az LDAP elsődleges szolgáltatása számára. Olvassa el az Információs központ Biztonság című része alatt található Hálózat hitelesítési szolgáltatást, ha többet akar tudni az iSeries szerveren megvalósítható Kerberos hitelesítésről. A Hálózat hitelesítési szolgáltatás konfigurálása szekcióban tájékoztatást talál a kulcstáblázat fájlok információinak bővítéséről.

Operációs rendszer leképzett háttér objektumai

A rendszer leképzett háttér objektumai funkció leképezi az OS/400 objektumokat LDAP által elérhető katalógusfán belüli bejegyzésekre. A leképzett objektumok az OS/400 objektumok LDAP reprezentánsai, amelyeket az LDAP szerver adatbázisában tárolt tényleges bejegyzés helyett használunk. A V5R2 változattól kezdve csak az OS/400 felhasználói profilok azok az objektumok, amelyeket bejegyzésként hozzárendel vagy leképez a katalógusfán belül. A felhasználói profil objektumok leképezését nevezzük OS/400 felhasználói leképzett háttér objektumnak.

Az LDAP műveletek hozzárendelésre kerülnek az alárendelt OS/400 objektumokhoz, és az LDAP műveletek operációs rendszer funkciókat hajtanak végre az objektumok elérése érdekében. A felhasználói profil összes végrehajtott LDAP művelete a kliens kapcsolathoz tartozó felhasználói profil jogosultságai alapján hajtódik végre.

Az operációs rendszer leképzett háttér objektumairól további tájékoztatást kaphat a következő helyeken:

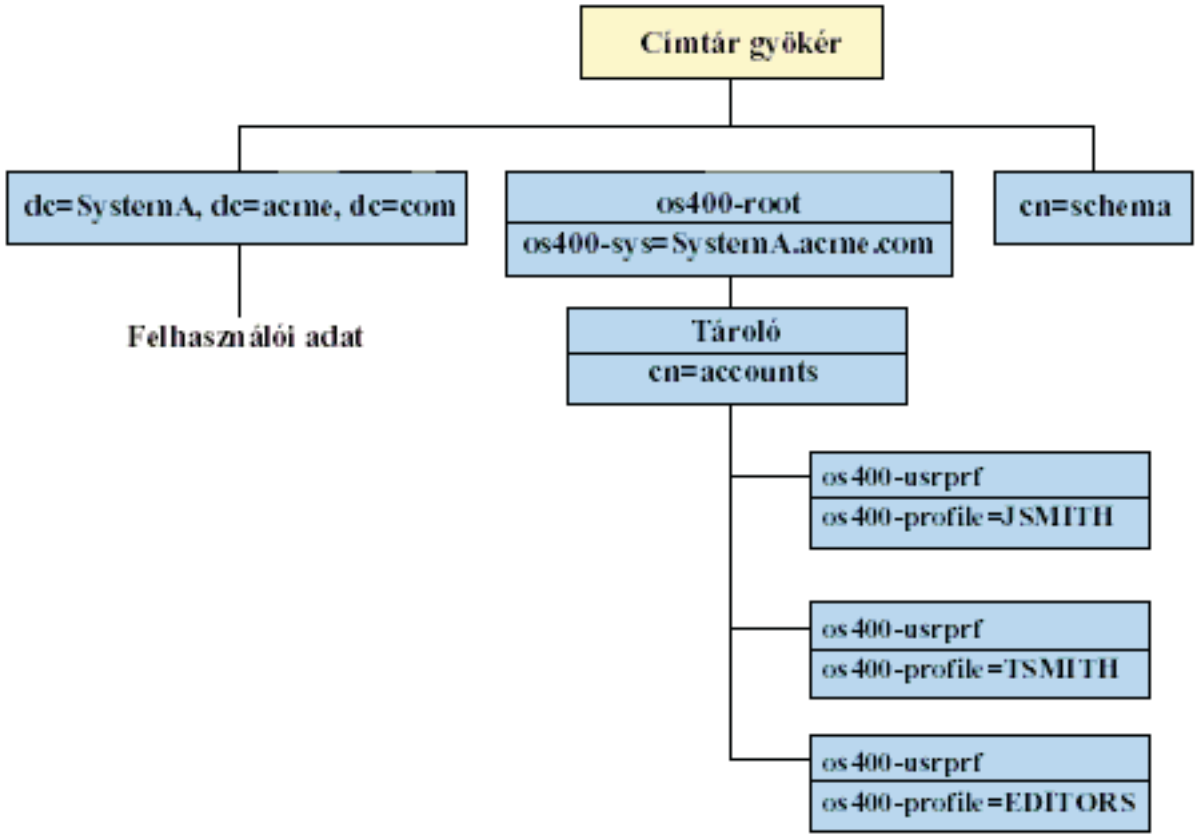
- “OS/400 felhasználói leképzett katalógusfa”
- “LDAP műveletek” oldalszám: 44
- “Adminisztrátori és replika kötés DN” oldalszám: 48
- “OS/400 felhasználói leképzett séma” oldalszám: 48

OS/400 felhasználói leképzett katalógusfa

Az alábbi ábra egy minta katalógus információs fát (DIT) mutat be a felhasználói leképzett háttér objektumokhoz. Az ábrán JSMITH és TSMITH felhasználói profilok, amelyeket csoport azonosító (GID), GID=*NONE (vagy 0) jelez, EDITORS egy csoportprofil, amelyet nem nulla GID jelez.

A dc=SystemA,dc=acme,dc=com utótag hivatkozásként szerepel az ábrán. Ez az utótag képviseli az aktuális adatbázis háttér objektumot, amely további LDAP bejegyzéseket kezel. A cn=schema utótag a

pillanatnyilag használt szerver séma.



A fa gyökere egy utótag, amelynek alapértéke os400-sys=*SystemA.acme.com*, ahol *SystemA.acme.com* a rendszer neve. Az objektumosztály os400-root. A DIT nem módosítható és nem törölhető ugyan, de újrakonfigurálható a rendszer objektumok utótagja. Azonban ellenőrizni kell, hogy az utótagot nem használja-e ACL-ben vagy valahol máshol azon a rendszeren, ahol a bejegyzések módosítása megváltoztatná az utótagot.

Az előző ábrán a cn=accounts tároló látható a gyökér alatt. Ez az objektum nem módosítható. A tároló erre a szintre kerül, megelőzve más típusú információkat vagy objektumokat. A cn=accounts tároló alatt felhasználói profilok vannak, amelyek leképzése objectclass=os400-usrprf-ként történik. A leképzett felhasználói profilokként jelzett felhasználói profilok os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com formában ismertek az LDAP számára.

LDAP műveletek

A leképzett felhasználói profilok révén a következő LDAP műveleteket hajthatja végre.

Kötés (Bind)

Az LDAP kliens kötődhet (hitelesítés) az LDAP szerverhez a leképzett felhasználói profil segítségével. Ez úgy hajtható végre, hogy megadja a leképzett felhasználói profil megkülönböztető nevét (DN) a kötés DN számára, valamint az OS/400 felhasználói profil helyes jelszavát a hitelesítéshez. A kötés kérésben használt DN-re példa az os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com.

A kliensnek leképzett felhasználóként kell kötődnie, hogy hozzáférjen a rendszer leképzett háttér objektumában lévő információkhoz. A szerver végrehajtja az összes műveletet az adott felhasználói profil jogosultságait felhasználva. A leképzett felhasználói profil DN ugyanúgy használható az LDAP ACL-ben,

mint más LDAP bejegyzés DN. Az egyszerű kötés az egyetlen módszer, amely engedélyezett, amikor leképzett felhasználói profilt ad meg a kötési kérésben.

Keresés (Search)

A rendszer leképzett háttér objektuma támogat néhány alapvető keresés szűrőt. Megadhat objectclass, os400-profile és os400-gid attribútumokat a keresési szűrőben. Az os400-profile attribútum támogatja a dzsóker karatereket. Az os400-gid attribútum megadása korlátozott, mégpedig (os400-gid=0), ami egy egyedi felhasználói profil vagy !(os400-gid=0), ami egy csoportprofil. A felhasználói profil összes attribútumát beolvashatja, kivéve a jelszót és a hasonló attribútumokat.

Bizonyos szűrőknél csak a DN objectclass és os400-profile értékeket kaphatja vissza. Azonban, az ezt követő keresések már részletesebb információkat adhatnak vissza.

A következő táblázat leírja, hogyan viselkednek a rendszer leképzett háttér objektumai keresési műveleteknél.

Táblázat: 1. Rendszer leképzett háttér objektumainak viselkedése keresési műveleteknél

Kért keresés	Keresés alapja	Keresés hatásköre	Keresés szűrője	Megjegyzések
Információk kérése az os400-sys=SystemA-ról, (választható), az alatta található tárolóról, valamint (választhatóan) a tárolókban lévő objektumokról.	os400-sys=SystemA.acme.com	base, sub vagy one	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	A megfelelő attribútumok és értékeik visszaadása a megadott hatáskör és szűrő alapján. A hardverkódolt attribútumokat és értékeiket a rendszer objektumok utótagjára és az alatta lévő tárolóra vonatkozóan kapja vissza.
Az összes felhasználói profil visszaadása.	cn=accounts, os400-sys=SystemA.acme.com	one vagy sub	os400-gid=0	Csak a megkülönböztetett név (DN), az objectclass és az os400-profile értékeket kapja vissza a leképzett felhasználói profilokra. Ha bármilyen más szűrőt ad meg, akkor LDAP_UNWILLING_TO_PERFORM üzenetet kap vissza.
Az összes csoport profil visszaadása.	cn=accounts, os400-sys=SystemA.acme.com	one vagy sub	(!(os400-gid=0))	Csak a megkülönböztetett név (DN), az objectclass és az os400-profile értékeket kapja vissza a leképzett felhasználói profilokra. Ha bármilyen más szűrőt ad meg, akkor LDAP_UNWILLING_TO_PERFORM üzenetet kap vissza.

Táblázat: 1. Rendszer leképzett háttér objektumainak viselkedése keresési műveleteknél (Folytatás)

Kért keresés	Keresés alapja	Keresés hatásköre	Keresés szűrője	Megjegyzések
Az összes felhasználói és csoport profil visszaadása.	cn=accounts, os400-sys= SystemA.acme.com	one vagy sub	os400-profile=*	Csak a megkülönböztetett név (DN), az objectclass és az os400-profile értékeket kapja vissza a leképzett felhasználói profilokra. Ha bármilyen más szűrőt ad meg, akkor LDAP_UNWILLING_ TO_PERFORM üzenetet kap vissza.
Egy adott felhasználói vagy csoport profil, mint például JSMITH, visszaadása.	cn=accounts, os400-sys= SystemA.acme.com	one vagy sub	os400-profile=JSMITH	Más visszaadandó attribútumok megadhatók.
Egy adott felhasználói vagy csoport profil, mint például JSMITH, visszaadása.	os400- profile=JSMITH, cn=accounts, os400-sys= SystemA.acme.com	bas, sub vagy one	objectclass=os400- usrprf objectclass=* os400-profile=JSMITH	Más visszaadandó attribútumok megadhatók. Noha egyszintű hatáskör megadható, a keresési eredmények nem adnak vissza értéket, mivel a DIT-ben lévő JSMITH felhasználói profil alatt semmi sincs.
Az összes A-val kezdődő felhasználói és csoport profil visszaadása.	cn=accounts, os400-sys= SystemA.acme.com	one vagy sub	os400-profile=A*	Csak a megkülönböztetett név (DN), az objectclass és az os400-profile értékeket kapja vissza a leképzett felhasználói profilokra. Ha bármilyen más szűrőt ad meg, akkor LDAP_UNWILLING_ TO_PERFORM üzenetet kap vissza.
Az összes G-vel kezdődő csoport profil visszaadása.	cn=accounts, os400-sys= SystemA.acme.com	one vagy sub	(&(!(os400-gid=0)) (os400-profile=G*))	Csak a megkülönböztetett név (DN), az objectclass és az os400-profile értékeket kapja vissza a leképzett felhasználói profilokra. Ha bármilyen más szűrőt ad meg, akkor LDAP_UNWILLING_ TO_PERFORM üzenetet kap vissza.

Táblázat: 1. Rendszer leképzett háttér objektumainak viselkedése keresési műveleteknél (Folytatás)

Kért keresés	Keresés alapja	Keresés hatásköre	Keresés szűrője	Megjegyzések
Az összes A-val kezdődő felhasználói profil visszaadása.	cn=accounts, os400-sys= SystemA.acme.com	one vagy sub	(&(os400-gid=0) (os400-profile=A*))	Csak a megkülönböztetett név (DN), az objectclass és az os400-profile értékeket kapja vissza a leképzett felhasználói profilokra. Ha bármilyen más szűrőt ad meg, akkor LDAP_UNWILLING_ TO_PERFORM üzenetet kap vissza.

Összehasonlítás (Compare)

Az LDAP összehasonlítási művelete révén összehasonlíthatja a leképzett felhasználói profil egy attribútumának értéket. Az os400-aut és os400-docpwd attribútumok nem összehasonlíthatók.

Hozzáadás és módosítás (Add and modify)

Az LDAP hozzáadási művelete révén létrehozhat felhasználói profilokat, míg a módosítási művelettel módosíthatja őket.

Törlés (Delete)

Az LDAP törlési műveletével felhasználói profilokat törölhet. A DLTUSRPRF OWNOBJOPT és a PGPOPT paraméterek viselkedésének megadásához két LDAP szerver vezérlés tartozik. Ezeket a vezérlő információkat az LDAP törlési műveletben adhatja meg. A Delete User Profile (DLTUSRPRF) parancsnál további tájékoztatást talál ezen paraméterek jellemzőiről.

Az LDAP kliens törlési műveletben a következő vezérlések és objektum azonosítók (OID) adhatók meg.

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  A vezérlési érték a következő:
  - controlValue ::= ownObjOpt [newOwner]
  - ownObjOpt ::= *NODLT / *DLT / *CHGOWN

  Az ownObjOpt vezérlési érték kijelöli az elvégzendő műveletet, ha a felhasználói profil birtokol valamilyen objektumot. A *NODLT érték azt jelzi, hogy nem kell törölni a felhasználói profilt, ha a felhasználói profil birtokol valamilyen objektumot. A *DLT érték azt jelzi, hogy törölni kell a birtokolt objektumokat, míg a *CHGOWN érték azt jelzi, hogy át kell adni a tulajdonjogot egy másik profilnak.

  A newOwner érték jelöli ki azt a profilt, akinek át kell adni a tulajdonjogot. Ez az érték akkor szükséges, ha ownObjOpt értéke *CHGOWN.

  A vezérlési értékre talál példákat az alábbiakban:
  - *NODLT: megadja, hogy a profil nem törölhető, ha valamilyen objektumot birtokol
  - *CHGOWN SMITH: megadja, hogy az objektumok tulajdonjogát át kell adni SMITH felhasználói profilnak
- Az ldap.h-ban az objektum azonosító (OID) LDAP_OS400_OWNOBJOPT_CONTROL_OID.
  - os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

A vezérlési érték megadása a következő:

```
controlValue ::=pgpOpt [     newPgp [     newPgpAut ] ]
pgpOpt ::= *NOCHG / *CHGPGP
newPgp ::= *NONE / user-profile-name
newPgpAut ::= *OLDPGP / *PRIVATE / *ALL / *CHANGE / *USE / *EXCLUDE
```

Az pgpOpt érték kijelöli az elvégzendő műveletet, ha a törlés alatt álló profil egy objektumnál is elsődleges csoport. Ha *CHGPGP van megadva, akkor newPgp értéket is meg kell adni. A newPgp értéke az elsődleges csoport profil neve vagy *NONE. Ha új elsődleges csoport profilt ad meg, a newPgpAut értékét ugyancsak megadhatja. A newPgpAut érték kijelöli a jogosultságot azokhoz az objektumokhoz, amelyek az új elsődleges csoportot adják.

A vezérlési értékre talál példákat az alábbiakban:

- *NOCHG: megadja, hogy a profil nem törölhető, ha elsődleges csoport valamilyen objektum számára.
- *CHGPGP *NONE: megadja az objektumokra vonatkozó elsődleges csoport eltávolítását.
- *CHGPGP SMITH *USE: megadja, hogy módosítsa a SMITH felhasználói profil elsődleges csoportját, és adjon *USE jogosultságot az elsődleges csoportnak.

Ha a fenti vezérlések egyikét sem adja meg a törlési műveletben, akkor helyette a QSYS/DLTUSRPRF parancsra pillanatnyilag érvényes alapértelmezéseket használja a rendszer.

ModRDN

A leképzett felhasználói profilokat nem nevezheti át, mivel az operációs rendszer nem támogatja.

Importáló és exportáló API-k

A QgldImportLdif és a QgldExportLdif API-k nem támogatják az adatok importálását és az exportálását a rendszer leképzett háttér objektumain belül.

Adminisztrátori és replika kötés DN

A leképzett felhasználói profilt megadhatja konfigurált adminisztrátori vagy replika kötés DN-nek. A felhasználói profil jelszavát használja a rendszer. A leképzett felhasználói profilok ugyancsak lehetnek LDAP adminisztrátorok, ha jogosultságuk van a Címtár szolgáltatás adminisztrátori funkció azonosítójához (QIBM_DIRSRV_ADMIN). Több felhasználói profil is kaphat adminisztrátori hozzáférést.

További információk: “Adminisztrációs hozzáférés kezelése a jogosult felhasználók számára” oldalszám: 31.

OS/400 felhasználói leképzett séma

A leképzett háttér objektumok objektum osztályai és attribútumai a szerver sugarú sémában találhatók. Az LDAP attribútumok nevei os400–*nnn* formátumúak, ahol *nnn* jellemzően az attribútum kulcsszava (mint például CRTUSRPRF vagy CHGUSRPRF) a felhasználói profil parancsaiban. “OS/400 felhasználói leképzett katalógusfa” oldalszám: 43 helyen további tájékoztatást kaphat.

Címtár szolgáltatás és OS/400 naplózási támogatás

A Címtár szolgáltatás az OS/400 adatbázis támogatását használja a címtár információ tárolásához. A Címtár szolgáltatás a véglegesítés vezérlés alapján tárolja a címtári bejegyzéseket az adatbázisban. Ehhez szükség van az OS/400 naplózási támogatásra.

Amikor a szerver vagy az LDIF importáló segédprogram először indul el, a következőket hozza létre:

- Egy napló
- Egy naplófogadó

- A kezdetben szükséges adatbázis tábla

A QSQJRN napló abban az adatbázis könyvtárban kerül összeállításra, amit a felhasználó konfigurált. A QSQJRN0001 naplófogadó eredetileg abban az adatbázis könyvtárban kerül létrehozásra, amit a felhasználó konfigurált.

Az aktuális környezet: a címtár mérete és szerkezete, valamint a mentési és visszaállítási stratégia megkövetelhet az alapértelmezéstől bizonyos eltéréseket, beleértve ezeknek az objektumoknak a kezelését és a használt méretküszöbüket is. Ha szükséges, megváltoztathatja a naplózási parancs paramétereit. Az LDAP naplózás alapértelmezés szerinti beállítása törli a régi fogadókat. Ha változási naplófájlt állított be, de meg kívánja tartani a régi fogadókat is, hajtsa végre a következő parancsot az OS/400 parancssorból:

```
JRN(QUSRDIRCL/QSQJRN) DLTRCV(*NO)
```

Ha konfigurálásra került a változási naplófájl, a naplófogadó a következő paranccsal törölhető:

```
CHGJRN JRN(QUSRDIRCL/QSQJRN)  DLTRCV(*YES)
```

A naplózási parancsokról további tájékoztatást az OS/400 parancsok témakörben olvashat, amelyet az iSeries Információs központ Programozás című része alatt talál meg.

Fejezet 6. LDAP parancssori segédprogramok

A Címtár szolgáltatás öt segédprogramot tartalmaz, melyekkel az OS/400 Qshell parancsértelmező környezetéből az LDAP címtár szolgáltatón műveletek végeztethetők el. Ezek a segédprogramok az LDAP API-kat használják. Ezeket a segédprogramokat a qsh parancssorból lehet használni, de hívhatók programokból is. Hasznosak lehetnek programozási példákként is. Amikor egy olyan install the Windows LDAP klienst telepít, ami tartalmazza a Címtár szolgáltatást, akkor olyan programkódokat is telepít, melyek nagyon hasonlítanak a parancsértelmező segédprogramok forráskódjához.

A segédprogramok az alábbiak:
- “ldapmodify és ldapadd segédprogramok” LDAP címtári bejegyzéseket vesz fel és módosít.
- “Az ldapdelete segédprogram” oldalszám: 54 LDAP címtári bejegyzéseket töröl.
- “ldapsearch segédprogram” oldalszám: 56 az LDAP címtárban keres bejegyzéseket.
- “ldapmodrdn segédprogram” oldalszám: 61 az LDAP címtári bejegyzések relatív megkülönböztető nevét (Relative Distinguished Name, RDN) módosítja.

A “Megjegyzések az SSL védelem LDAP parancssori segédprogramokkal való használatával kapcsolatban” oldalszám: 63 részben információt talál az SSL biztonság használatáról a segédprogramokkal kapcsolatban.

ldapmodify és ldapadd segédprogramok

Az ldapmodify segédprogrammal a rendszer QSH parancsértelmezőjéből módosíthatja az LDAP címtár szolgáltató bejegyzéseit, illetve bővítheti azt bejegyzésekkel. Az ldap_modify, az ldap_add és az ldap_delete alkalmazási program csatolókat (API) használja. Az ldapmodify segédprogramhoz hasonlóan működik az ldapadd segédprogram, azzal a különbséggel, hogy az -a jelzőt automatikusan bekapcsolja.

Formátum:

ldapmodify [-a] [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn***] [-w** *passwd* **] [-m** *mechanism***] [-O***hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-f** *file***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***]**

ldapadd [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn* **] [-w** *passwd***] [-m** *mechanism***] [-O***hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-f** *file***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***]**

Megjegyzés: Ha nem ad meg bejegyzés információt *fájlban* a **-f** opció használatával, a segédprogram a szabványos bemeneten várja a bejegyzéseket. A várakozásból a SysReq billentyű lenyomásával törhet ki, utána válassza a 2. Előző kérés befejezése pontot.

Diagnosztika:

A kilépési állapot 0, ha nem történt hiba. A hibák nem-zéró kilépési állapotot eredményeznek és diagnosztikai üzenet jelenik meg a szabványos hibakimeneten.

Kattintson ide a segédprogramok használatával kapcsolatos példák megtekintéséhez.

Paraméterek:

-V	Kijelöli az LDAP verziót, amelyet a segédprogram használ az LDAP szerverrel való összekapcsolódáshoz (bind). Alapértelmezés az LDAP V3 kapcsolat használata. Ahhoz, hogy kifejezetten az LDAP V3 legyen kiválasztva, -V 3 kapcsolót kell megadni. Adjon meg -V 2 kapcsolót, ha LDAP V2 alkalmazásként kívánja futtatni.

-a	Csak az ldapmodify használja ezt a paramétert. Azt jelzi, hogy alapértelmezésként a segédprogram bejegyzéseket fog felvenni a meglevők módosítása helyett. E paraméter használata ugyanaz, mint az ldapadd parancs használata.
-b	Tegyük fel, hogy minden érték, amely `/ karakterrel kezdődik, bináris érték, és a tényleges érték egy fájlban található, amelynek elérési útvonalát azon a helyen adták meg, ahol az értékek rendszerint megjelennek.
-c	Folyamatos műveleti üzemmód. Jelenti a hibákat, de az ldapmodify és az ldapadd folytatja a módosításokat vagy felvételeket. Alapértelmezés a hibajelzés után kilépés.
-r	A létező értékek lecserélése alapértelmezés szerinti értékekre.
-M	Utalási objektumokat szabályos bejegyzésként kezelni.
-n	Megmutatja, minek kellene történni, de valójában nem változtatja meg a bejegyzést. Hibakereséskor hasznos a -v paraméterrel együtt.
-v	Bővebb információt ad, részletes diagnosztikai információt ír a szabványos kimenetre.
-F	Az összes módosítás kötelező végrehajtása tekintet nélkül a replikával kezdődő input sorok tartalmára (az alapértelmezés szerinti replika: a sorokat összehasonlítják az LDAP szerver hoszttal és a használt porttal, hogy eldöntésre kerüljön, valóban készüljön-e egy replikációs naplórekord).
-R	Megadja, hogy az utalásokat nem kell automatikusan követni.
-C *charset*	Megadja, hogy a segédprogram inputján a karakterláncok helyi karakterkészletben jelennek meg (*charset*), és ezeket UTF-8 karakterkészletre kell konvertálni. Használja a **-C** charset opciót, ha a bemeneti karakterlánc kódlapja eltér a feladat kódlapjától. Az ldap_set_iconv_local_charset() API dokumentációjában megtalálhatja a támogatott *charset* értékeket.
-d *debuglevel*	Beállítja a hibakeresési szintet a *debuglevel* értékre.
-D *binddn*	Használja a *binddn* értéket az LDAP könyvtárral való összekapcsolódásnál. A *binddn* egy karakterlánccal megadott DN.
-w *passwd*	A *passwd* a hitelesítés jelszavaként használandó.
-m *mechanism*	A *mechanism* az az SASL eljárás, amit a kliens a szerverrel való összekapcsolódásnál használ. A kliens az ldap_sasl_bind_s() API-t használja. Rendelkezésre álló eljárások között található a CRAM-MD5 (titkosító jelszó), az EXTERNAL (SSL-lel használva) és a GSSAPI (Kerberos). A parancs nem használja az **-m** paramétert, ha be van állítva a **-V 2**. Ha nem szerepel az **-m**, egyszerű hitelesítési eljárást használ.
-O*hopcount*	A *hopcount* beállítja azon szakaszoknak maximális számát, amit a kliens könyvtár az utalások keresésénél számba vesz. Az alapértelmezés szerinti érték 10.
-h *ldaphost*	Egy alternatív hoszt megadása, amelyiken az LDAP szerver fut.
-p *ldapport*	Egy alternatív TCP port megadása, amelyiken az LDAP szerver figyel. Az alapértelmezés szerinti LDAP port a 389. Ha másként nincs megadva, és a **-Z** meg van adva, az alapértelmezés szerinti 636 LDAP SSL port használandó.
-f *file*	Bejegyzés módosítási információ beolvasása az LDIF fájlból a szabványos bemenet helyett. Ha nincs egy LDIF fájl megadva, akkor LDIF formátumban a szabványos bemenetet kell használni az LDIF formátumú frissítési rekordok kijelölésére.
-Z	Védett SSL kapcsolat használata az LDAP szerverrel folyó kommunikáció során. A **-Z** opciót ezen eszköznek csak az SSL-engedélyezett verziói támogatják.
-K *keyfile*	Megadja az SSL kulcs adatbázis fájl nevét. Ha a kulcs adatbázis fájl nincs az aktuális könyvtárban, megadja a teljes adatbázis fájlnevet. Ha a segédprogram nem találja meg a kulcs adatbázist, akkor az alapértelmezés szerinti megbízható jogosultság gyökerek hardver-kódolt készletét fogja használni. A kulcs adatbázis fájl általában tartalmaz az igazoló hatóságoktól (CA-któl) egy vagy több olyan igazolást, amit a kliens megbízhatónak tart. Ezeket az X.509 típusú igazolásokat megbízható gyökerekként ismerik. Ez a paraméter hatékonyan engedélyezi a **-Z** kapcsolót.

-P *keyfilepw*	Megadja a kulcs adatbázis jelszót. Ez a jelszó a kulcs adatbázis fájl rejtjelezett tartalma (ide tartozik a privát kulcs is) eléréséhez szükséges. Ha a rejtett jelszófájl társítva lett a kulcs adatbázis fájllal, a jelszó a rejtett fájlból kérdezhető le, ezért erre a paraméterre nincs szükség. Ez a paraméter mellőzésre kerül, ha sem a **-Z**, sem a **-K** nincs megadva.
-N *certificatename*	A kulcs adatbázis fájlban található kliens igazoláshoz tartozó címkét adja meg. Ha az LDAP szerver csak szerver hitelesítésre lett konfigurálva, kliens igazolásra nincs szükség. Ha az LDAP szerver kliens és szerver hitelesítésre lett beállítva, szükséges a kliens igazolás. A *certificatename* (igazolásnév) nem szükséges, ha egy alapértelmezés szerinti igazolás/privát kulcspár alapértelmezés szerintinek lett kijelölve. Hasonlóképpen nincs szükség a*certificatename* paraméterre, ha a kijelölt kulcs adatbázis fájlban van egy egyedi igazolás/privát kulcspár. Ez a paraméter mellőzésre kerül, ha sem a **-Z**, sem a **-K** nincs megadva.

Alternatív bemeneti formátum:

A segédprogram régebbi verzióival való kompatibilitás megőrzése érdekében, az ldapmodify egy alternatív bemeneti formátumot is támogat. Ez a formátum egy vagy több bejegyzésből áll, melyeket üres sorok választanak el egymástól. Minden bejegyzésnek az alábbi formátuma van:

```
Distinguished Name (DN)
attr=value
[attr=value ...]
```

ahol *attr* az attribútum neve, és *value* az értéke. Az alapértelmezés szerint az értékeket fel kell venni. A **-r** parancssori jelző használata esetén a meglévő értékeket le kell cserélni újakra. Megjegyezzük, hogy egy adott attribútum egynél többször is megjelenhet (például egy attribútumnak egynél több érték is adható). Több sorból álló értékeknél egy bevezető fordított per jel (\) használható, hogy az értéket több sorban lehessen megadni, és az új sor magában az értékben megőrzésre kerüljön. Egy érték eltávolításához az *attr* értéket egy mínuszjelnek (-) megelőzni. Az attribútum teljes eltávolításához ki kell hagyni egyenlőségjelet (=) és az értéket. Az *attr* előtt pluszjelnek (+) kell lenni, ha az **-r** jelző megléte esetén értéket kíván megadni.

Példák: ldapmodify és ldapadd

1. példa

Ha a /**tmp**/**entrymods** nevű fájl létezik és tartalma a következő:

```
dn: cn=Modify Me, o=University of Higher Learning, c=US
changetype: modify
replace: mail
mail: modme@student.of.life.edu
-
add: title
title: Grand Poobah
-
add: jpegPhoto
jpegPhoto:< file:///tmp/modme.jpeg
-
delete: description
-
```

Az ldapmodify -b -r -f /tmp/entrymods parancs a következőt végzi el:

- Helyettesíti a Modify Me bejegyzés mail attribútumának tartalmát a modme@student.of.life.edu értékkel.
- Felveszi a Grand Poobah titulust (title).
- Felveszi a /**tmp**/**modme.jpeg** nevű fájl tartalmát jpegPhoto-ként.
- Teljesen eltávolítja a description attribútumot.

A fenti módosítással megegyező eredményt érhető a régebbi ldapmodify bemeneti formátummal:

```
cn=Modify Me, o=University of Higher Learning, c=US
mail=modme@student.of.life.edu
+title=Grand Poobah
+jpegPhoto=/tmp/modme.jpeg
-description
```

A régi formátumot használó parancs az alábbi:

```
ldapmodify -b -r -f /tmp/entrymods
```

2. példa:

Tételezzük fel, hogy a /**tmp**/**newentry** nevű fájl létezik, és tartalma a következő:

```
dn: cn=John Doe, o=University of Higher Learning, c=US
objectClass: person
cn: John Doe
cn: Johnny
sn: Doe
title: Manager
mail: johndoe@student.of.life.edu
uid: jdoe
```

Az ldapadd -f /tmp/entrymods parancs új bejegyzés vesz fel John Doe részére a /tmp/newentry fájlból vett értékek felhasználásával.

3. példa:

Ha a /**tmp**/**newentry** nevű fájl létezik és tartalma a következő:

```
dn: cn=John Doe, o=University of Higher Learning, c=US
changetype: delete
```

Az ldapmodify -f /tmp/entrymods parancs eltávolítja John Doe bejegyzését.

Az ldapdelete segédprogram

Az ldapdelete segédprogram lehetővé teszi, hogy egy vagy több bejegyzést töröljön egy LDAP címtár szolgáltatóról. Az OS/400 rendszeren közvetlenül a QSH parancsértelmezőből fut. Az ldap_delete alkalmazási programcsatolón (API) keresztül működik.

Formátum:

ldapdelete [-V] [-M] [-n] [-v] [-c] [-R] [-C charset] [-d *debuglevel***] [-f** *file***] [-D** *binddn***] [-w** *passwd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***] [***dn***]...**

Megjegyzés: Ha nem ad meg *dn* argumentumokat, az ldapdelete parancs a szabványos bemenetről várja a DN-ek listáját. A várakozásból a SysReq billentyű lenyomásával törhet ki, utána válassza a 2. Előző kérés befejezése pontot.

Diagnosztika:

A kilépési állapot 0, ha nem történt hiba. A hibák nem-zéró kilépési állapotot eredményeznek és diagnosztikai üzenet jelenik meg a szabványos hibakimeneten.

Kattintson ide az ldapdelete segédprogram használatával kapcsolatos példák megtekintéséhez.

Paraméterek:

-V	Kijelöli az LDAP verziót, amelyet a segédprogram használ az LDAP szerverhez való összerendelésnél (bind). Alapértelmezés szerint LDAP V3 kapcsolat lesz használva. Ahhoz, hogy kifejezetten az LDAP V3 legyen kiválasztva, -V 3 kapcsolót kell megadni. Adjon meg -V 2 kapcsolót, ha LDAP V2 alkalmazásként kívánja futtatni.
-M	Utalási objektumokat normál bejegyzésként kezelni.
-n	Megmutatja, mi történne, de valójában nem változtatja meg a bejegyzést. Hibakereséskor hasznos a **-v** paraméterrel együtt.
-v	Bővebb információt ad, részletes diagnosztikát ír a szabványos kimenetre.
-c	Folyamatos műveleti üzemmód. A hibákat jelenti, de az ldapdelete folytatja a törléseket. Alapértelmezés a hiba jelzése után kilépés.
-R	Megadja, hogy a hivatkozásokat nem kell automatikusan követni.
-C *charset*	Megadja, hogy az ldapdelete segédprogram bemeneténél a megkülönböztető nevek (DN) a helyi karakterkészletben (*charset*) vannak ábrázolva. Használja a **-C** *charset* beállítást az alapértelmezés felülbírálására, ahol a karakterláncoknak UTF-8 formátumban kell lenni. Használja a **-C** charset opciót, ha a bemeneti karakterlánc kódlapja eltér a feladat kódlapjától. Az ldap_set_iconv_local_charset() API dokumentációjában megtalálhatja a támogatott *charset* értékeket.
-d *debuglevel*	Beállítja a hibakeresési szintet *debuglevel* értékre.
-f *file*	Egy *fájlból* olvas be sorokat, és a fájl mindegyik soránál végrehajt egy LDAP törlést. Mindegyik sor egyetlen megkülönböztető nevet (DN) tartalmazhat.
-D *binddn*	A *binddn* használata az LDAP könyvtárhoz való kapcsolódáskor. A *binddn* egy karakterlánccal képviselt DN.
-w *passwd*	A *passwd* használata hitelesítési jelszóként.
-m *mechanism*	A *mechanism* kijelöli a szerverhez való hozzárendelés (bind) céljára használandó SASL mechanizmust. Az ldap_sasl_bind_s() API lesz használva. A rendelkezésre álló mechanizmusok között megtalálható a CRAM-MD5 (titkosító jelszó), EXTERNAL (SSL-lel használva) és GSSAPI (Kerberos). A -m paraméter mellőzve van, ha -V 2 be van állítva. Ha a **-m** nincs megadva, akkor egyszerű hitelesítés történik.
-O *hopcount*	A *hopcount* beállítja azoknak a szakaszoknak (hop) a maximális számát, amelyeket a kliens könyvtár az utalások keresésekor számba vesz. Az alapértelmezett érték 10.
-h *ldaphost*	Alternatív hoszt megadása, amelyiken az LDAP szerver fut.
-p *ldapport*	Alternatív TCP port megadása, amelyiken az LDAP szerver figyel. Az alapértelmezett LDAP port a 389. Ha másként nincs megadva, és a **-Z** opció szerepel, az alapértelmezés szerinti 636 LDAP SSL port lesz használva.
-Z	Védett SSL kapcsolat használata az LDAP szerverrel folyó kommunikáció során. A **-Z** opciót csak a segédprogram SSL-engedélyezett verziói támogatják.
-K *keyfile*	Megadja az SSL kulcs adatbázis fájl nevét. Ha a kulcs adatbázis fájl nem az aktuális könyvtárban található, megadja az adatbázis fájl teljes nevet. Ha a segédprogram nem találja meg a kulcs adatbázist, akkor az alapértelmezés szerinti megbízható jogosultság gyökerek hardver-kódolt készletét fogja használni. A kulcs adatbázis fájl általában tartalmaz az igazoló hatóságoktól (CA-któl) egy vagy több olyan igazolást, amit a kliens megbízhatónak tart. Ezeket az X.509 típusú igazolásokat megbízható gyökerekként is ismerik. Ez ez a paraméter hatékonyan engedélyezi a **-Z** kapcsolót.
-P *keyfilepw*	Megadja a kulcs adatbázis jelszavát. A jelszó a kulcs adatbázis fájl rejtjelezett tartalma (ide tartozik a privát kulcs is) eléréséhez szükséges. Ha a rejtett jelszófájl társítva van a kulcs adatbázis fájllal, a jelszó a rejtett fájlból kérdezhető le, ezért erre a paraméterre nincs szükség. Ez a paraméter mellőzve lesz, ha sem **-Z** sem **-K** nincs megadva.

-N *certificatename*	Megadja a kulcs adatbázis fájlban található kliens igazoláshoz tartozó címkét. Amennyiben az LDAP szerver csak szerver hitelesítésre lett beállítva, kliens igazolásra nincs szükség. Ha az LDAP szerver kliens és szerver hitelesítésre lett beállítva, kliens igazolásra szükség van. A *certificatename* (igazolásnév) nem szükséges, ha egy alapértelmezett igazolás/privát kulcspár alapértelmezettként ki lett jelölve. Hasonlóképpen a *certificatename* (igazolásnév) nem szükséges, ha van egy igazolás/privát kulcspár a megjelölt adatbázis fájlban. Ez a paraméter mellőzve lesz, ha sem **-Z** sem **-K** nincs megadva.
dn	Egy vagy több *dn* argumentumot ad meg. Minden egyes *dn* egy karakterlánccal képviselt DN.

Példa: ldapdelete

Az alábbi parancs megkísérli törölni a commonNamemel elnevezett Delete Me bejegyzést közvetlenül a University of Life szervezeti bejegyzés alól:

```
ldapdelete cn=Delete Me, o=University of Life, c=US
```

Lehet, hogy szükséges *binddn* és *passwd* megadása is (lásd a **-D** és **-w** opciókat).

ldapsearch segédprogram

Az ldapsearch segédprogrammal az OS/400 QSH parancsértelmezőből bejegyzések kereshetők az LDAP címtár szolgáltatón. Az ldap_search alkalmazási programcsatolón (API) keresztül működik.

A keresés olyan szűrőt használ, amely megfelel az LDAP szűrők karakterlánc ábrázolásának. Ha többet szeretne megtudni az LDAP keresési szűrőkről, olvassa el az iSeries Információs központ Programozás című fejezete alatt található OS/400 Címtár szolgáltatások témakörben az ldap_search API-ról leírtakat.

Ha az ldapsearch segédprogram egy vagy több bejegyzést talál, beolvassa az *attrs* által meghatározott attribútumokat, és a szabványos kimenetre írja a bejegyzéseket és az értékeket. Ha nem ad meg egy attribútumot sem, az összes attribútumot beolvassa.

Formátum:

ldapsearch [-V] [-n] [-v] [-t] [-A] [-B] [-L] [-M] [-R] [-C *charset***] [-d** *debuglevel***] [-F** *sep***] [-f** *file***] [-D** *binddn***] [-w** *bindpasswd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***] [-b** *searchbase***] [-s** *scope* **] [-a** *deref***] [-l** *time limit***] [-z** *size limit***]** *filter* **[***attrs...***]**

Diagnosztika:

A kilépési állapot 0, ha nem történt hiba. A hibák nem-zéró kilépési állapotot eredményeznek, és diagnosztikai üzenet jelenik meg a szabványos hibakimeneten.

Kimeneti formátum:

Ha az ldapsearch egy vagy több bejegyzést talál, a következő formátumban írja ki mindegyik bejegyzést a szabványos kimenetre:

```
Distinguished Name (DN)
attributename=value
attributename=value
attributename=value
...
```

Az egyes bejegyzéseket egy üres sor választja el egymástól. Ha a **-F** kapcsolóval megad egy elválasztó karaktert, az egyenlőségjel (=) helyett az kerül a kimenetre. Ha a **-t** opciót használja, az ideiglenes fájl neve lecseréli a tényleges értéket. Az **-A** opció segítségével csak az attributename részt jeleníti meg.

Kattintson ide az ldapsearch segédprogram használatával kapcsolatos példák megtekintéséhez.

Paraméterek:

-V	Kijelöli az LDAP verziót, amelyet a segédprogram használ az LDAP szerverhez való összerendelésnél (bind). Alapértelmezés szerint LDAP V3 kapcsolatot használ. Ahhoz, hogy kifejezetten az LDAP V3 legyen kiválasztva, -V 3 kapcsolót kell megadni. Adjon meg -V 2 kapcsolót, ha LDAP V2 alkalmazásként kívánja futtatni.
-n	Megmutatja, mi történne, de valójában nem hajtja végre a keresést. Hibakereséskor hasznos a **-v** paraméterrel együtt.
-v	Bővebb diagnosztikai információt nyújt, amelyet a szabványos kimenetre ír.
-t	A beolvasott értékeket ideiglenes fájlokba írja. Ez hasznos lehet bináris értékek esetében, mint amilyenek a jpegPhoto vagy audio.
-A	Csak az attribútumokat olvassa be (az értékeket nem). Ez akkor lehet hasznos, amikor arra kíváncsi, hogy egy attribútum jelen van-e egy bejegyzésben, de nem kíváncsi annak az értékeire.
-B	Nem nyomja el a bináris érték megjelenítést. Ez hasznos lehet olyan értékek esetében, melyek alternatív karakterkészletekben jelennek meg, amilyen pl. az ISO-8859.1 karakterkészlet. Az **-L** opció ezt magában foglalja.
-L	A keresési eredményeket LDIF formátumban jeleníti meg. Ez a kapcsoló bekapcsolja a **-B** opciót, és mellőzi az **-F** opciót.
-M	Utalási objektumokat normál bejegyzésként kezelni.
-R	Meghatározza, hogy az utalásokat nem kell automatikusan követni.
-C *charset*	Megadja, hogy az ldapsearch segédprogram bemeneteként szolgáló karakterlánc ábrázolása a helyi karakterkészlet (*charset*) szerint történik. A bemeneti karakterlánc magában foglalja a szűrőt, az összerendelési DN-t és az alap DN-t. Ugyanúgy, mint az adatok megjelenítésekor, az ldapsearch segédprogram speciális karakterekre konvertálja az LDAP szervertől kapott adatokat. Használja a **-C** charset opciót, ha a bemeneti karakterlánc kódlapja eltér a job kódlap értékétől. Az ldap_set_iconv_local_charset() API dokumentációjában megtalálhatja a támogatott *charset* értékeket. Ha a -C és az -L opció is meg van adva, akkor feltételezés szerint a bemenet a megadott karakterkészletben jelenik meg, de az ldapsearch programtól jövő kimenetek mindig UTF-8 ábrázolásban, illetve az adatok alap 64-kódolt ábrázolásban örződnek meg, ha nem nyomtatható karaktereket észlel a program. Ez a helyzet azóta, hogy a szabványos LDIF fájlok csak UTF-8 (vagy alap 64-kódolt UTF-8) kódolású karakterlánc adatokat tartalmaznak.
-d *debuglevel*	Beállítja a hibakeresési szintet *debuglevel* értékre.
-F *sep*	A *sep* mező elválasztóként szerepel az attribútum nevek és értékek között. Az alapértelmezett elválasztó mindaddig =, amíg meg nem adja az **-L** jelzőt, amikor is ez az opció mellőzve lesz.
-f *file*	Egy fájlból olvas be sorokat, minden sorra végrehajt egy LDAP keresést. Minden sor egyetlen megkülönböztető nevet (DN) tartalmazhat.
-D *binddn*	A *binddn* használata az LDAP könyvtárhoz való kapcsolódáskor. A *binddn* egy karakterlánccal képviselt DN.
-w *passwd*	A *passwd* használata hitelesítési jelszóként.
-m *mechanism*	A *mechanism* használata kijelöli a szerverhez való hozzárendelés (bind) céljára használandó SASL mechanizmust. Az ldap_sasl_bind_s() API lesz használva. A rendelkezésre álló mechanizmusok között megtalálható a CRAM-MD5 (titkosító jelszó), EXTERNAL (SSL-lel használva) és GSSAPI (Kerberos). Az **-m** paraméter nincs figyelembevéve, ha a **-V** 2 be van állítva. Ha a **-m** nincs megadva, akkor egyszerű hitelesítés történik.
-O *hopcount*	A *hopcount* megadása beállítja azoknak a szakaszoknak (hop) a maximális számát, melyeket a kliens könyvtár számba vesz az utalások keresésekor. Az alapértelmezett érték 10.

-h *ldaphost*	Alternatív hoszt megadása, amelyiken az LDAP szerver fut.
-p *ldapport*	Alternatív TCP port megadása, amelyiken az LDAP szerver figyel. Az alapértelmezett LDAP port a 389. Ha másként nincs megadva, és a **-Z** szerepel, az alapértelmezett 636 LDAP SSL port lesz használva.
-Z	Védett SSL kapcsolat használata az LDAP szerverrel folyó kommunikáció során. A **-Z** opciót csak a segédprogram SSL-t kezelő verziói támogatják.
-K *keyfile*	Megadja az SSL kulcs adatbázis fájl nevét. Ha a kulcs adatbázis fájl nem az aktuális könyvtárban található, megadja az adatbázis fájl teljes nevét. Ha a segédprogram nem találja meg a kulcs adatbázist, akkor az alapértelmezés szerinti megbízható jogosultság gyökerek hardver-kódolt készletét fogja használni. A kulcs adatbázis fájl általában egy vagy több, a kliens által megbízhatónak tartott CA-tól származó igazolást tartalmaz. Ezeket az X.509 típusú igazolásokat megbízható gyökerek is nevezik. Valójában ez a paraméter engedélyezi a **-Z** kapcsolót.
-P *keyfilepw*	Megadja a kulcs adatbázis jelszót. A jelszó a kulcs adatbázis fájl titkosított tartalmának eléréséhez szükséges (beleértve a privát kulcsot is). Ha a kulcs adatbázis fájlhoz rejtett jelszó fájl tartozik, akkor a jelszó a rejtett fájlból kerül lekérdezésre, és ez a paraméter nem szükséges. Ez a paraméter mellőzve lesz, ha sem **-Z** sem **-K** nincs megadva.
-N *certificatename*	A kulcs adatbázis fájlban található kliens igazoláshoz tartozó címkét adja meg. Amennyiben az LDAP szerver csak szerver hitelesítésre lett beállítva, a kliens igazolásra nincs szükség. Ha az LDAP szerver kliens és szerver hitelesítésre lett beállítva, a kliens igazolásra szükség van. A *certificatename* (igazolásnév) nem szükséges, ha egy alapértelmezett igazolás/privát kulcspár alapértelmezettként ki lett jelölve. Hasonlóképpen a *certificatename* (igazolásnév) nem szükséges, ha van egy igazolás/privát kulcspár a megjelölt adatbázis fájlban. Ez a paraméter mellőzve lesz, ha sem **-Z** sem **-K** nincs megadva.
-b *searchbase*	Használja a *searchbase*-t a keresés kezdőpontjaként az alapértelmezés helyett. Ha nem adja meg a **-b** opciót, a segédprogram az LDAP_BASEDN környezeti változóban keresi a *searchbase* definícióját.
-s *scope*	A keresés érvényességi tartományát határozza meg. A *scope* lehetséges értéke base, one vagy sub, ami rendre bázis objektum szintű, egy-szintű vagy alárendelt fa szintű keresést határoz meg. Az alapértelmezés sub.
-a *deref*	Meghatározza az álnevek használatát (alias dereferencing). *deref* lehetséges értéke never (soha), always (mindig), search (keres) vagy find (talál). Rendre azt adja meg, hogy milyen módon történik az álnevek használata, ami lehet soha, mindig, kereséskor vagy a keresés bázis objektumának megtalálásakor. Az alapértelmezés szerint álnevek nincsenek használva (never).
-l *timelimit*	Maximum *timelimit* másodpercet vár a keresés befejezéséig.
-z *sizelimit*	A keresést korlátozza maximum *sizelimit* bejegyzésre. Ezzel megadható a keresési művelet által visszaadott bejegyzések maximális száma.
filter	A keresés által használt szűrő nevét határozza meg.
attrs...	Azokat az attribútumokat határozza meg, amelyeket a segédprogram beolvas, ha egy vagy több bejegyzést talál. Ha nem ad meg értéket az *attrs*-nak, a segédprogram az összes attribútumot beolvassa.

Példák: ldapsearch

1. példa

Az ldapsearch cn=john doe cn telephoneNumber parancs keresést hajt végre egy alárendelt fán (az alapértelmezett keresési kiindulópontot használva) az olyan bejegyzések után, amelyek általános neve (commonName) john doe. A keresés beolvassa a commonName és a telephoneNumber értékeket, és a szabványos kimenetre írja őket. Ha a keresés két bejegyzést talál, a kimenet a következőhöz lesz hasonló:

```
cn=John E Doe, ou=College of Literature, Science, and the Arts,
ou=Students, ou=People, o=University of Higher Learning, c=US
cn=John Doe
cn=John Edward Doe
cn=John E Doe 1
cn=John E Doe
telephoneNumber=+1 313 555-5432

cn=John B Doe, ou=Information Technology Division,
ou=Faculty and Staff,
ou=People, o=University of Higher Learning, c=US
cn=John Doe
cn=John B Doe 1
cn=John B Doe
telephoneNumber=+1 313 555-1111
```

2. példa:

Az ldapsearch -t uid=jed jpegPhoto audio parancs keresést hajt végre egy alárendelt fán (az alapértelmezett keresési kiindulópontot használva) az olyan bejegyzések után, amelyek felhasználói azonosítója (user id) jed. A keresés jpegPhoto és audio értékeket olvas be és ideiglenes fájlokba írja őket. Ha a keresés egy bejegyzést talál egyetlen értékkel mindkét lekérdezett attribútumhoz, akkor a kimenet a következő példához lesz hasonló:

```
cn=John E Doe,
ou=Information Technology Division,
ou=Faculty and Staff,
ou=People, o=University of Higher Learning, c=US
audio=/tmp/ldapsearch-audio-a19924
jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

3. példa:

Az ldapsearch -L -s one -b c=US o=university* o description parancs egyszintű keresést hajt végre a c=US szinten. Ez a keresés az összes olyan szervezetet keresi, amelynek szervezeti neve (organizationName) university szóval kezdődik. A keresés az eredményt LDIF fájl formátumban jeleníti meg. Beolvassa az organizationName attribútum értékét és a leírás (description) attribútum értékét, majd a szabványos kimenetre írja őket az alábbihoz hasonlóan:

```
dn: o=University of Alaska Fairbanks, c=US
o: University of Alaska Fairbanks
description: Preparing Alaska for a brave new tomorrow
description: leaf node only

dn: o=University of Colorado at Boulder, c=US
o: University of Colorado at Boulder
description: No personnel information
description: Institution of education and research

dn: o=University of Colorado at Denver, c=US
o: University of Colorado at Denver
o: UCD
o: CU/Denver
o: CU-Denver
description: Institute for Higher Learning and Research

dn: o=University of Florida, c=US
o: University of Florida
o: UFl
description: Shaper of young minds
...
```

4. példa:

Amint a “LDAP címtári utalások” oldalszám: 39 alatt tárgyaltuk, a Címtár szolgáltatás LDAP címtárak utalási objektumokat is tartalmazhatnak, feltéve, ha csak a következőket tartalmazzák:

- Egy megkülönböztető nevet (dn).
- Egy objektum-osztályt (objectClass).
- Egy utalási (ref) attribútumot.

A következő példa olyan keresést illusztrál, ahol az utalási objektumról van szó.

Tegyük fel, hogy System_A az alábbi utalási bejegyzést tartalmazza:

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
ref: ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US
objectclass: utalás
```

A bejegyzéssel kapcsolatos összes attribútum lelőhelye System_B legyen.

System_B egy bejegyzést tartalmaz:

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
cn: Barb Jensen
objectclass: organizationalPerson
sn: Jensen
telephonenumber: (800) 555 1212
```

Amikor a kliens kérést küld System_A részére, de nem küldi el a manageDsaIT vezérlést, a szerver egy utalással válaszol. Például, az ldapsearch -M esetén a System_A LDAP címtár szolgáltatója a következő URL-lel válaszol a kliensnek:

```
ldap://System_B:389/cn=Barb Jensen,
 ou=Rochester, o=Big Company, c=US
```

A kliens arra használja ezt a választ, hogy System_B felé nyújtson be kérést. Ha System_A-n a bejegyzés más attribútumot is tartalmaz, mint pl. dn, objectclass és ref, a szerver figyelmen kívül hagyja azokat az attribútumokat.

Amikor a kliens egy utalási választ kap a szervertől, újra kiadja a kérést, ezúttal azon szerver felé, amelyre a visszaküldött URL utal. Ha a keresést egyszintű hatáskörrel végezte, az utalás kérés az alap hatáskört használja. A keresés eredménye függ a keresés hatásköreként megadott értéktől (**-b**).

Ha -s sub paramétert ad meg, mint itt:

```
ldapsearch -h System_A -b ou=Rochester, o=Big Company, c=US
     -s sub sn=Jensen
```

a keresés az összes olyan bejegyzésre vonatkozó összes attribútumot beolvassa, ahol sn=Jensen, és amelyek ou=Rochester, o=Big Company, c=US helyen vagy az alatt találhatók System_A-n és System_B-n egyaránt. A kliens utalást kap a System_A-tól, és keresni fog a System_B-n, visszakapva a cn=Barb Jense,ou=Rochester,o=Big Company,c=US adatokat.

Ha -s one paramétert ad meg, mint itt:

```
ldapsearch -h System_A -b ou=Rochester, o=Big Company, c=US
     -s one sn=Jensen
```

a keresés egyik rendszeren sem ad vissza bejegyzést. Helyette a szerver a következő utalási URL-t adja vissza a kliensnek:

```
ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US??base
```

Erre a kliens a következő kérést nyújtja be:

```
ldapsearch -h System_B -b cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
    -s base sn=Jensen
```

Ez a cn=Barb Jensen,ou=Rochester,o=Big Company,c=US bejegyzést adja vissza.

ldapmodrdn segédprogram

Az ldapmodrdn segédprogram lehetővé teszi, hogy az LDAP címtár szolgáltatón a bejegyzések relatív megkülönböztető nevét (Relative Distinguished Name (RDN)) megváltoztathassuk. Az OS/400 rendszeren a QSH parancsértelmezőből használható. Az ldap_modrdn alkalmazási programcsatolón (API) keresztül működik.

Formátum:

ldapmodrdn [-V] [-r] [-M] [-n] [-v] [-c] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn***] [-w** *passwd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***] [-f** *file* **] [***dn rdn***]**

Megjegyzések:

1. A következő parancssori paraméterekkel: *dn* és *rdn*, *rdn* helyettesíti a DN-nel megadott bejegyzés RDN-jét: *dn*. Máskülönben a fájl tartalma (vagy a szabványos bemenet, ha nem adja meg a **-f** jelzőt) egy vagy több bejegyzés legyen.

   ```
   Megkülönböztető név (Distinguished Name, DN)

   Relatív megkülönböztető név (Relative Distinguished Name, RDN)
   ```

   Egy vagy több üres sor választ el minden DN/RDN párt.
2. Ha nem ad meg bejegyzés információt a *fájlban* az **-f** opció használatával (vagy a *dn* és az *rdn* parancssori párral), az ldapmodrdn parancs a szabványos bemeneten várja a bejegyzéseket. A várakozásból a SysReq billentyű lenyomásával törhet ki, utána válassza a 2. Előző kérés befejezése pontot.

Diagnosztikai:

A kilépési állapot 0, ha nem történt hiba. A hibák nem-zéró kilépési állapotot eredményeznek és diagnosztikai üzenet jelenik meg a szabványos hibakimeneten.

Kattintson ide az ldapmodrdn segédprogram megtekintéséhez.

Paraméterek:

-V	Kijelöli az LDAP verzióját, amelyet a segédprogram használ az LDAP szerverhez való összerendeléshez (bind). Alapértelmezés szerint LDAP V3 összeköttetést használ. Ahhoz, hogy kifejezetten az LDAP V3 legyen kiválasztva, -V 3 kapcsolót kell megadni. Adjon meg -V 2 kapcsolót, ha LDAP V2 alkalmazásként kívánja futtatni.
-r	A régi relatív megkülönböztető nevek (RDN) értékének eltávolítása a bejegyzésből. Alapértelmezés: a régi értékek megtartása.
-M	Utalási objektumokat normál bejegyzésként kezel.
-n	Megmutatja, mi történne, de valójában nem változtatja meg a bejegyzést. Hibakereséskor hasznos a **-v** paraméterrel együtt.
-v	Bővebb információt ad, részletes diagnosztikát ír a szabványos kimenetre.
-c	Folyamatos műveleti üzemmód. A hibákat jelenti, de az ldapmodrdn tovább végzi a módosításokat. Alapértelmezés a hiba utáni kilépés.
-R	Meghatározza, hogy utalásokat nem kell automatikusan követni.

-C *charset*	Megadja, hogy a segédprogram bemeneteként szolgáló karakterlánc ábrázolása a helyi karakterkészlet (*charset*) szerint történik, és konvertálni kell az UTF-8 készletre. Használja a **-C** charset opciót, ha a bemeneti karakterlánc kódlapja eltér a job kódlap értékétől. Az ldap_set_iconv_local_charset() API dokumentációjában megtalálhatja a támogatott *charset* értékeket.
-d *debuglevel*	Beállítja a hibakeresési szintet *debuglevel* értékre.
-D *binddn*	A *binddn* használata az LDAP könyvtárhoz való kapcsolódáskor. A *binddn* egy karakterlánccal képviselt DN.
-w *passwd*	A *passwd* használata hitelesítési jelszóként.
-m *mechanism*	A *mechanism* használata kijelöli a szerverhez való hozzárendelés (bind) céljára használandó SASL mechanizmust. Az ldap_sasl_bind_s() API lesz használva. A rendelkezésre álló mechanizmusok között megtalálható a CRAM-MD5 (titkosító jelszó), EXTERNAL (SSL-lel használva) és GSSAPI (Kerberos). Az -m paraméter mellőzve van, ha -V 2 be van állítva. Ha az **-m** nincs megadva, akkor egyszerű hitelesítés történik.
-O *hopcount*	A *hopcount* megadása beállítja azoknak a szakaszoknak (hop) a maximális számát, amelyeket a kliens könyvtár számba vesz az utalások keresésekor. Az alapértelmezett érték 10.
-h *ldaphost*	Alternatív hoszt megadása, amelyiken az LDAP szerver fut.
-p *ldapport*	Alternatív TCP port megadása, amelyiken az LDAP szerver figyel. Az alapértelmezett LDAP port a 389. Ha másként nincs megadva, és a **-Z** szerepel, az alapértelmezett 636 LDAP SSL port 636 lesz használva.
-Z	Védett SSL kapcsolat használata az LDAP szerverrel folyó kommunikáció során. A **-Z** opciót csak a segédprogram SSL-t kezelő verziói támogatják.
-K *keyfile*	Az SSL kulcs adatbázis fájl nevének megadása. Ha a kulcs adatbázis fájl nem az aktuális könyvtárban található, adja meg a teljes adatbázis fájl nevet. Ha a segédprogram nem találja meg a kulcs adatbázist, akkor az alapértelmezés szerinti megbízható jogosultság gyökerek hardver-kódolt készletét fogja használni. A kulcs adatbázis fájl általában egy vagy több, a kliens által megbízhatónak tartott CA-któl származó igazolást tartalmaz. Az X.509 típusú igazolást megbízható gyökérnek is nevezik. Valójában ez a paraméter engedélyezi a **-Z** kapcsolót.
-P *keyfilepw*	Megadja a kulcs adatbázis jelszót. A jelszó a kulcs adatbázis fájl titkosított tartalmának eléréséhez szükséges (beleértve a privát kulcsot is). Ha a rejtett jelszófájl társítva van a kulcs adatbázis fájllal, akkor a rejtett fájlból származó jelszó kerül felhasználásra, és erre a paraméterre nincs szükség. Ez a paraméter mellőzve lesz, ha sem a **-Z**, sem a **-K** nincs megadva.
-N *certificatename*	A kulcs adatbázis fájlban található kliens igazoláshoz tartozó címkét adja meg. Amennyiben az LDAP szerver csak szerver hitelesítésre lett beállítva, a kliens igazolásra nincs szükség. Ha az LDAP szerver kliens és szerver hitelesítésre lett beállítva, a kliens igazolásra szükség van. A *certificatename* (igazolásnév) nem szükséges, ha egy alapértelmezett igazolás/privát kulcspár az alapértelmezettként ki lett jelölve. Hasonlóképpen a *certificatename* (igazolásnév) nem szükséges, ha van egy egyedi igazolás/privát kulcspár a megjelölt adatbázis fájlban. Ez a paraméter mellőzve lesz, ha sem a **-Z**, sem a **-K** nincs megadva.
-f *file*	A bejegyzés módosítási információ beolvasása LDIF fájlból a szabványos bemenet vagy a parancssor helyett (ha *dn* és az új *rdn* van megadva). A szabványos bemenetként egy fájl (< fájl) is megadható.
dn rdn	Egy átnevezendő bejegyzés megkülönböztető nevét, és a bejegyzés új relatív megkülönböztető nevét határozza meg.

Példa: ldapmodrdn

Tegyük fel, hogy létrehozott egy **/tmp/entrymods** nevű szövegfájlt, amely a következőket tartalmazza:

```
cn=Modify Me, o=University of Life, c=US
cn=The New Me
```

A következő parancs:

```
ldapmodrdn -r -f /tmp/entrymods
```

a Modify Me bejegyzés RDN-jét Modify Me-ről The New Me-re változtatja. Az előző cn: Modify Me el lesz távolítva.

Megjegyzések az SSL védelem LDAP parancssori segédprogramokkal való használatával kapcsolatban

Ahhoz, hogy a parancssori segédprogramok védett socket réteg (Secure Sockets Layer, SSL) képességét használni lehessen, telepíteni kell a Cryptographic Access Provider termékek (5722-ACx) egyikét.

A “Védett socket réteg (SSL) és Fordítási réteg biztonság használata LDAP címtár szolgáltatóval” oldalszám: 41 tárgyalja az SSL használatát a Címtár szolgáltatás LDAP szerverrel. Ebbe beleértendő a megbízható CA-k (Certificate Authorities) digitális igazolás kezelővel (Digital Certificate Manager) való létrehozása és kezelése is.

A kliens által elérhető több LDAP szerver is csak szerver hitelesítést alkalmaz. Ezekhez a szerverekhez elegendő egy vagy több megbízható gyökérigazolás meghatározása az igazolástárolóban. Szerver hitelesítésnél a kliens biztos lehet afelől, hogy a megcélzott LDAP szerver egy megbízható CA (Certificate Authority, igazolás kibocsátó hatóság) által kibocsátott igazolással rendelkezik. Emellett minden LDAP tranzakció, amely az SSL kapcsolaton keresztül megy végbe, titkosítva lesz. Titkosítva lesz többek között az alkalmazásprogram csatolók (API-k) által szolgáltatott LDAP igazoló levelek is, amelyek a címtár szolgáltatóhoz történő összekapcsolódásra (bind) szolgálnak. Amennyiben az LDAP szerver egy feltétlenül megbízható Verisign igazolást használ, az alábbiak a teendők:

1. Beszerezni egy CA igazolást a Verisign cégtől.
2. A DCM használatával importálni azt az igazolástárolóba.
3. A DCM segítségével kijelölni azt megbízhatónak.

Amennyiben az LDAP szerver egy saját kibocsátású szerver igazolást használ, a szerver adminisztrátorától kell kérni egy szerver igazolást igénylő fájlt. Importálja az igazolást igénylő fájlt az igazolástárolóba, és jelölje meg azt megbízhatónak.

Amennyiben a kliens- és a szerver hitelesítését egyaránt igénylő segédprogramokat használ az LDAP szerver eléréséhez, az alábbiakat kell tennie:

- Definiáljon egy vagy több megbízható gyökér-igazolást a rendszer igazolástárolójában. Ez biztosítja a klienst afelől, hogy a megcélzott LDAP szerver egy megbízható CA (Certificate Authority, igazolás kibocsátó hatóság) által kibocsátott igazolással rendelkezik. Emellett minden LDAP tranzakció, amely az SSL kapcsolaton keresztül megy végbe, titkosítva lesz. Titkosítva lesz többek között az alkalmazásprogram csatolók (API-k) által szolgáltatott LDAP igazoló levelek is, amelyek a címtár szolgáltatóhoz történő összekapcsolódásra (bind) szolgálnak.
- Hozzon létre egy kulcspárt és igényeljen egy kliens igazolást egy CA-tól. Miután a CA-tól megkapta az aláírt igazolást, tárolja azt el a kliens kulcstartó fájljában.

Fejezet 7. A Címtár szolgáltatás hibaelhárítása

Sajnos, még az olyan megbízható szerverekkel, mint amilyen a Címtár szolgáltatás LDAP szervere, alkalmanként problémák adódhatnak. Amikor az LDAP címtár szolgáltató problémákkal találkozik, segíthet az alábbi információ a hiba okának kiderítésében és a hiba kiküszöbölésében.

- “Alapvető hibakeresési eljárások Címtár szolgáltatás esetében”
- “Általános LDAP kliens hibák” oldalszám: 67

Az általános Címtár szolgáltatás problémákról további információkat kaphat a Címtár szolgáltatás honlapon

`http://www.iseries.ibm.com/ldap`

Alapvető hibakeresési eljárások Címtár szolgáltatás esetében

Az LDAP hibák visszadott hibakódjai az ldap.h fájlban találhatók, ami a rendszer QSYSINC/H.LDAP könyvtárban helyezkedik el.

Ha az LDAP címtár szolgáltatón hiba fordul elő, és részletesebb tájékoztatást akar, egy másik lehetőség a QDIRSRV feladatnapló megtekintése. Reprodukálható hibák esetén a Trace TCP/IP Application (TRCTCPAPP APP(*DIRSRV)) parancs segítségével futtathatja a hibák nyomkövetését. “Hibakeresés TRCTCPAPP segítségével” oldalszám: 66 helyen további tájékoztatást kaphat.

A Címtár szolgáltatás több SQL (Structured Query Language, strukturált lekérdezési nyelvi) szervert használ. SQL hiba esetén a QDIRSRV üzenetnapló a következő üzenetet tartalmazza:

```
SQL error -1 occurred (SQL hiba -1 lépett fel)
```

Ilyen esetekben a QDIRSRV feladatnapló az SQL szerver feladatnaplójára fog hivatkozni. Egyes esetekben azonban a QDIRSRV nem tartalmazza ezt az üzenetet és a hivatkozást akkor sem, ha valójában az SQL szerver probléma oka. Ilyen esetekben segíthet az, ha tudjuk, hogy melyik SQL szervereket kell elindítani és mire használja őket a Címtár szolgáltatás.

Amikor az LDAP címtár szolgáltató szabályosan indul el, az alábbihoz hasonló üzenetet generál.

Megjegyzés: Az üzenetek és az elindított SQL szerver jobok száma eltérhet a következő esetekben:

- A szervert első alkalommal indítja.
- Költöztetésnek kell történnie.
- A szerver a változási naplót használja.
- A szerver úgy van beállítva, hogy nagyobb számú adatbázis kapcsolatot engedjen meg.

```
                                                    System:   WARMERS
 Job . . :   QDIRSRV       User . . :   QDIRSRV       Number . . . :   174440

  >> CALL PGM(QSYS/QGLDSVR)
     Job 057448/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057340/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057448/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057166/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057279/QUSER/QSQSRVR used for SQL server mode processing.
  Job 057288/QUSER/QSQSRVR used for SQL server mode processing.
     Directory Services server started successfully.
```

A Címtár szolgáltatás az első SQL szervert használja az LDAP szerver indításakor: 057448/QUSER/QSQSRVR. Szükség szerint a Címtár szolgáltatás további SQL szervereket indíthat el az LDAP szerver indítása során, ha a szervert első alkalommal indítja, ha költöztetésnek kell történnie, vagy ha a szerver a változási naplót használja. Az indítást követően ezek az SQL szerverek mellőzve lesznek.

A példában nem használt további SQL szervereket a költöztetéshez vagy a szerver indításhoz, valamint a változási napló sem volt konfigurálva. A Címtár szolgáltatás a következő SQL szervert (057340/QUSER/QSQSRVR) használja a replikáláshoz.

A példában található legutolsó kapcsolatot (057288/QUSER/QSQSRVR) az add, modify, modrdn és delete műveletekhez használja. A többi kapcsolat search, bind és compare műveletekhez használatos.

Az iSeries navigátorban a címtár szolgáltató **Database**/**Suffixes** nevű tulajdonságok lapján megadhatja az SQL szerverek maximális számát, amelyeket a Címtár szolgáltatás használ fel a címtár műveletekhez a szerver elindítása után. Továbbá, egy SQL szervert mindig a replikációhoz kell konfigurálni.

Hibafigyelés és hozzáférés követés a Címtár szolgáltatás feladatnapló segítségével

Az LDAP címtár szolgáltató feladatnaplójának megtekintése hibákra hívhatja fel a figyelmet, és segít nyomonkövetni a szerver elérését.

Ha a szerver már elindult, az alábbi lépéseket követve megtekintheti a QDIRSRV feladatnaplót:
1. Az iSeries navigátorban nyissa meg a **Network** ikont.
2. Nyissa meg a **Servers** ikont.
3. Kattintson a **TCP/IP** pontra.
4. Jobb gombbal kattintson a **Directory** feliratra, és válassza a **Server Jobs** elemet.
5. A **File** menüből válassza a **Job Log** elemet.

Ha a szerver még nem indult el, kövesse az alábbi lépéseket a QDIRSRV feladatnapló megtekintéséhez:
1. Az iSeries navigátorban nyissa meg a **Basic Operations** pontot.
2. Kattintson a **Printer Output** pontra.
3. A QDIRSRV a **User** oszlopban jelenik meg az iSeries navigátor jobboldali keretén. A job napló megtekintéséhez kattintson kétszer a **Qpjoblog** pontra ugyanabban a sorban a QDIRSRV-től balra.

   Megjegyzés: Lehetséges, hogy az iSeries navigátor pillanatnyi beállítása csak a zsilipelt állományokat mutatja meg. Ha a QDIRSRV nem jelenik meg a listán, kattintson a **Printer Output** pontra, majd válassza az **Include** pontot az **Options** menüből. Válassza az **All** értéket az **User** mezőben, majd kattintson az **OK** gombra.

Megjegyzés: A Címtár szolgáltatás egyes feladatok végrehajtásához más rendszererőforrásokat vesz igénybe. Ha ezen erőforrásokkal kapcsolatban fordul elő hiba, a feladatnapló jelzi, hova lehet információért fordulni. Néhány esetben a Címtár szolgáltatás nem képes meghatározni a hiba forrását. Ilyenkor tekintse meg az SQL (Structured Query Language) szerver feladatnaplóját, hátha a hiba az SQL szerverekkel kapcsolatos.

Hibakeresés TRCTCPAPP segítségével

A szerver nyomkövetési funkciót nyújt a kommunikációs vonalra vonatkozó adatok összegyűjtésére, mint például a helyi hálózat (LAN) vagy a távolsági hálózat (WAN) interfésze. Az átlagos felhasználó nem feltétlenül érti meg a nyomkövetési adatok teljes tartalmát. Azonban, a nyomkövetési bejegyzések segítségével meghatározhatja, hogy az adatcsere két pont között valójában megtörtént-e.

A Trace TCP/IP Application (TRCTCPAPP) parancsot *DIRSRV opcióval az LDAP címtár szolgáltató használhatja a kliensekkel vagy az alkalmazásokkal kapcsolatos problémák megtalálásához.

A TRCTCPAPP parancs LDAP szerverrel való használatáról és a szükséges jogosultságok korlátozásáról olvassa el a TRCTCPAPP (Trace TCP/IP Application) parancs leírást.

A kommunikációs nyomkövetés használatáról szóló általános tájékoztatót a Kommunikációs nyomkövetés tartalmazza.

Hibák nyomkövetése az LDAP_OPT_DEBUG opcióval

A V5R2 változattól kezdve az **ldap_set_option()** API program LDAP_OPT_DEBUG opciója révén nyomon követheti az LDAP C API-kat használó kliensekkel kapcsolatos problémákat. A hibakeresési opció több hibakeresési szinttel rendelkezik, amelyek nagyban segítik az ilyen alkalmazások problémáinak hibakeresését.

A következő sorok a kliens nyomkövetés engedélyezésére mutatnak be példát.

```
int  debugvalue=  LDAP_DEBUG_TRACE  |  LDAP_DEBUG_PACKETS;
ldap_set_option(    1d,  LDAP_OPT_DEBUG,  &debugvalue);
```

A hibakeresési szint beállításának másik módja az, ha ugyanazt a számértéket adja meg a kliens alkalmazást futtató job leírásában az LDAP_DEBUG környezeti változóra, mint ami a debugvalue értéke lenne, ha az **ldap_set_option()** API-t használná.

A következő példában a kliens nyomkövetést engedélyezi az LDAP_DEBUG környezeti változó segítségével:

```
ADDENVVAR  ENVVAR(LDAP_DEBUG)  VALUE(0x0003)
```

A jelentkező hibát előállító kliens futtatása után gépelje be az iSeries parancssorba a következő parancsot:

```
DMPUSRTRC    ClientJobNumber
```

ahol ClientJobNumber a kliens feladat száma.

Az információ párbeszédes megjelenítéséhez írja be az iSeries parancssorba:

```
DSPPFM  QAPOZDMP  QPOZnnnnnn
```

ahol nnnnnn a feladat száma.

Hajtsa végre a következő lépéseket, hogy mentse az információkat, és elküldje a szerviznek:

1. Hozzon létre egy SAVF fájlt a Create SAVF (CRTSAVF) parancs segítségével.
2. Írja be a következőt az iSeries parancssorba.

   ```
   SAVOBJ  OBJ(QAPOZDMP  LIB(QTEMP)  DEV(*SAVF)  SAVF(xxx)
   ```

   ahol *xxx* a SAVF fájl megadott neve.

Általános LDAP kliens hibák

Az általános LDAP kliens hibák ismerete segít a szerverrel kapcsolatos problémák megoldásában. Az iSeries Információs központ Programozás című fejezetének OS/400 Címtár szolgáltatások témaköre nyújt teljes listát az LDAP kliens hibaállapotairól.

A kliens hibaüzenetek az alábbi formátumban jelennek meg:

```
[Hibás LDAP művelet]:[LDAP kliens API hibafeltétel]
```

Megjegyzés: A hibák magyarázata feltételezi, hogy a kliens OS/400 alatt futó LDAP szerverrel kommunikál. Más platformon futó szerverrel kommunikáló kliens is hasonló hibaüzeneteket kaphat, de azok oka és megoldása az alábbiaktól eltérő lehet.

Az általános hibaüzenetek a következők:

- “ldap_search: Timelimit exceeded (Időhatár túllépés)”
- “[Failing LDAP operation]: Operations error (Műveleti hiba)”
- “ldap_bind: No such object (Nem létező objektum)”
- “ldap_bind: Inappropriate authentication (Nem megfelelő hitelesítés)”
- “[Failing LDAP operation]: Insufficient access (Nem elegendő elérés)” oldalszám: 69
- “[failing LDAP operation]: Cannot contact LDAP server (Nem lehet az LDAP szerverhez kapcsolódni)” oldalszám: 69
- “[failing LDAP operation]: Failed to connect to ssl server (Meghiúsult az ssl szerverhez a kapcsolat)” oldalszám: 69

ldap_search: Timelimit exceeded (Időhatár túllépés)

Ez a hiba akkor lép fel, ha az ldapsearches (ldap-keresések) lassan hajtódnak végre. A hiba kiküszöbölésére az alábbi lépések közül egyet vagy mindkettőt végezze el:

- Növelje meg az LDAP címtár szolgáltató keresési idejét. “Az LDAP címtár szolgáltató teljesítményének beállítása” oldalszám: 33 részben megtalálja a szükséges információt.
- Csökkentse rendszerében a tevékenységet. Az éppen futó aktív LDAP kliens jobok számát is csökkentheti.

[Failing LDAP operation]: Operations error (Műveleti hiba)

Több körülmény is okozhatja ezt a hibát. Adott feltételek mellett a hiba okáról információt kaphat, ha megtekinti az QDIRSRV és az SQL (Structured Query Language, strukturált lekérdezési nyelv) szerver feladatnaplóját, amint az “Alapvető hibakeresési eljárások Címtár szolgáltatás esetében” oldalszám: 65 részben ismertetve van.

ldap_bind: No such object (Nem létező objektum)

A hiba általános oka az, hogy a felhasználó gépelési hibát vét, amikor végrehajt egy műveletet. Egy másik jellemző oka, ha az LDAP kliens egy nem létező DN-nel kisérel meg összekapcsolódni. Ez gyakran előfordul, amikor a felhasználó tévesen azt gondolja, hogy ő DN adminisztrátor. Például a felhasználó megadhatja a QSECOFR vagy Administrator értéket, amikor az adminisztrátor tényleges DN-je cn=Administrator értékhez hasonló érték lehet.

A hibáról további részleteket a QDIRSRV feladatnaplóban talál, erről volt szó a következő helyen: “Alapvető hibakeresési eljárások Címtár szolgáltatás esetében” oldalszám: 65.

ldap_bind: Inappropriate authentication (Nem megfelelő hitelesítés)

A szerver érvénytelen megbízó levelet adott vissza, amikor a jelszó vagy a bind DN helytelen. A szerver nem megfelelő hitelesítést küld vissza, amikor a kliens a következők egyike szerint próbál kapcsolódni:

- A bejegyzés nem rendelkezik userpassword attribútummal
- Az OS/400 felhasználót képviselő bejegyzés rendelkezik UID attribútummal, de nem rendelkezik userpassword attribútummal. Ez összehasonlítást eredményez a megadott jelszó és az OS/400 felhasználói jelszó között, amelyek nem egyeznek meg.
- Olyan bejegyzésre van szükség, ami egy irányított felhasználót képvisel, és az összekapcsolódási módszer eltér az egyszerűtől.

Ez a hiba általában akkor lép fel, ha a kliens érvénytelen jelszóval kisérel meg összekapcsolódni. A hiba részleteivel kapcsolatban tekintse meg a QDIRSRV feladatnaplót, amint ezt az “Alapvető hibakeresési eljárások Címtár szolgáltatás esetében” oldalszám: 65 részben ismertetjük.

[Failing LDAP operation]: Insufficient access (Nem elegendő elérés)

Ezt a hibát általában egy összekapcsolódó DN okozza, amely nem rendelkezik megfelelő jogosultsággal a kliens által igényelt művelet (mint pl. felvétel vagy törlés) végrehajtásához. A hiba részleteivel kapcsolatban tekintse meg a QDIRSRV feladatnaplóját, amint azt az “Alapvető hibakeresési eljárások Címtár szolgáltatás esetében” oldalszám: 65 részben ismertetjük.

[failing LDAP operation]: Cannot contact LDAP server (Nem lehet az LDAP szerverhez kapcsolódni)

A hiba leggyakoribb okai az alábbiak:

- Egy LDAP kliens azelőtt intéz egy kérést a szerverhez, mielőtt a megadott rendszerben a LDAP szerver be lenne kapcsolva, és várakozó állapotban lenne.
- A felhasználó érvénytelen portszámot adott meg. A szerver, például, a 386-as porton figyel, de a kliens a 387-es portot kísérli meg használni.

A hiba részleteivel kapcsolatban tekintse meg a QDIRSRV feladatnaplóját, amint azt az “Alapvető hibakeresési eljárások Címtár szolgáltatás esetében” oldalszám: 65 részben ismertetjük. Ha a Címtár szolgáltató szerver sikeresen felállt, a QDIRSRV feladatnaplójában a Directory Services server started successfully (A Címtár szolgáltató szerver sikeresen elindult) szövegű üzenet található.

[failing LDAP operation]: Failed to connect to ssl server (Meghiúsult az ssl szerverhez a kapcsolat)

Ez a hiba akkor lép fel, amikor az LDAP szerver visszautasítja a kliens kapcsolatfelvételi kísérletét, mert védett (SSL) kapcsolatot nem lehet létrehozni. Ezt okozhatja az alábbiak valamelyike:

- Az Igazoláskezelő támogatás (Certificate Management support) visszautasítja a kliensnek a szerverrel való kapcsolatfelvételi kísérletét. Használja a digitális igazoláskezelőt (Digital Certificate Manager) azért, hogy megbizonyosodjon arról, igazolásai megfelelően vannak összeállítva, majd indítsa újra a szervert, és kísérelje meg újból a kapcsolatfelvételt.
- A felhasználó nem rendelkelkezik a *SYTEM igazolástárhoz (ez alapértelmezés szerint /QIBM/userdata/ICSS/Cert/Server/default.kdb) olvasási hozzáférési joggal.

OS/400 C alkalmazások esetében további SSL hiba információk állnak rendelkezésre. Részleteket lásd az egyedi Címtár szolgáltatás API-k dokumentációjában.

Nyomtatva Dániában