



IBM Systems - iSeries

IBM Directory Server (LDAP)

V5R4





IBM Systems - iSeries

IBM Directory Server (LDAP)

V5R4

Megjegyzés

Jelen leírás és a tárgyalt termék használatba vétele előtt olvassa el a “Nyilatkozatok” oldalszám: 281 helyen lévő tájékoztatót és az *IBM eServer Safety Information* című kiadványt.

Nyolcadik kiadás (2006. február)

Ez a kiadás a V5R4M0 szintű IBM i5/OS (száma: 5722-SS1) termékre, és minden azt követő változatra és módosításra vonatkozik, amíg ez másképpen nincs jelezve. Ez a verzió nem fut minden csökkentett utasításkészletű (RISC) rendszeren és CISC modellen.

© Szerzői jog IBM Corporation 1998, 2006. Minden jog fenntartva

Tartalom

1. fejezet IBM Directory Server for iSeries (LDAP)	1
2. fejezet A V5R4 újdonságai	3
3. fejezet Nyomtatható PDF	5
4. fejezet Directory Server - Alapfogalmak	7
Címtárak	7
Megkülönböztetett nevek (DN)	11
Utótag (névkontextus)	14
Séma	15
IBM Directory Server sémája	16
Általános séma támogatása	17
Objektumosztályok	18
Attribútumok	19
Objektumazonosító (OID)	26
Alséma-bejegyzések	27
Az IBMsubschema objektumosztály	27
Sémalekérdezések	27
Dinamikus séma	27
Nem engedélyezett sémamódosítások	28
Sémaellenőrzés	31
iPlanet-kompatibilitás	33
Generalized time és UTC time	33
Közzététel	35
Replikáció	36
Replikáció áttekintés	36
Replikációs szakkifejezések	39
Replikációs megállapodások	40
Hogyan tárolódnak a replikációs információk a szerveren?	41
Biztonsági megfontolások a replikációs információkkal kapcsolatban	41
Replikáció nagy rendelkezésre állású környezetben	42
Tartományok és felhasználói sablonok	42
Keresési paraméterek	43
Nemzeti nyelvek támogatása (NLS)	44
Nyelvi címkék	44
LDAP címtárutalások	46
Tranzakciók	46
Directory Server biztonsága	46
Ellenőrzés	47
Védett socket réteg (SSL) és Fordítási réteg biztonság (TLS) használata LDAP Directory Serverrel	47
Kerberos hitelesítés használata Directory Server-rel	48
Csoportok és szerepek	48
Adminisztratív hozzáférés	55
Proxy hitelesítés	55
Hozzáférés-felügyeleti listák	56
LDAP címtárobjektumok tulajdonjoga	67
Jelszó-irányelvek	68
Hitelesítés	71
Szolgáltatás megbénítása	74
Operációs rendszer leképezett háttér objektumai	75
Felhasználói leképezett címtár-információs fa	75
LDAP műveletek	76
Adminisztrátori és replika csatlakozási DN	80
Felhasználói leképezett séma	80
Directory Server és i5/OS naplózási támogatás	80
Egyedi attribútumok	81
Műveleti attribútumok	81
Szerver gyorsítótárak	82
Attribútum-gyorsítótár	82
Szűrő gyorsítótár	83
Bejegyzés gyorsítótár	83
ACL gyorsítótár	83
Vezérlőelemek és kiterjesztett műveletek	84
5. fejezet Első lépések a Directory Server használatában	85
Áttérési megfontolások	85
Átállás V5R4 kiadásra V5R3 vagy V5R2 rendszerekről	85
Adatok átállítása V4R4, V4R5 vagy V5R1 kiadásokról a V5R4 kiadásra	86
Replikált szerverek hálózatának átállítása	87
Kerberos szolgáltatás megváltozott neve	89
Directory Server megtervezése	90
Directory Server beállítása	90
A Directory Server alapértelmezett konfigurációja	91
A címtár feltöltése	92
Információk publikálása a címtárszervernek	92
LDIF fájl importálása/exportálása	93
Felhasználók másolása HTTP szerver ellenőrzési listából a Directory Serverbe	94
Javasolt példák a címtár felépítésére	96
Webes adminisztráció	98
Webes adminisztráció első beállítása	99
Webes adminisztrációs eszköz	100
6. fejezet Példahelyzet: Directory Server beállítása	103
Példahelyzet részletek: A Directory Server telepítése	104
Példahelyzet részletek: A címtár-adatbázis létrehozása	105
Példahelyzet részletek: Az iSeries adatok közzététele a címtár-adatbázisban	107
Példahelyzet részletek: Információk beírása a címtár-adatbázisba	108
Példahelyzet részletek: A címtár-adatbázis tesztelése	109
7. fejezet Directory Server felügyelete	111
Directory Server indítása/leállítása	112
A címtárszerver állapotának ellenőrzése	113
Jobok ellenőrzése a Directory Server-en	113
Szerverkapcsolatok kezelése	113
Kapcsolat tulajdonságainak kezelése	114
Az eseményértesítés engedélyezése	116
Tranzakció-beállítások megadása	117

Port vagy IP cím módosítása	117	Objektumosztály másolása	161
Szerver kijelölése címtári utalások részére	118	Objektumosztály törlése.	162
Directory Server utótagok felvétele és eltávolítása	118	Attribútumok megjelenítése	162
A Directory Server információinak mentése és visszaállítása	119	Attribútum hozzáadása	163
Adminisztrátori hozzáférés megadása leképezett felhasználóknak	119	Attribútum módosítása	164
Adminisztrációs csoport kezelése	120	Attribútum másolása.	165
Az adminisztrációs csoport engedélyezése	121	Attribútum törlése	167
Adminisztrációs csoport tagjainak hozzáadása, módosítása és eltávolítása	121	Séma átmásolása más szerverekre	167
Keresésikorlát-csoportok kezelése.	122	Címtárbejegyzések kezelése	168
Keresésikorlát-csoport létrehozása	122	Címtárfa tallózása	168
Keresésikorlát-csoport módosítása	123	Bejegyzés hozzáadása	169
Keresésikorlát-csoportok másolása	123	Nyelvi címkékkel ellátott attribútumokat tartalmazó bejegyzés hozzáadása	169
Keresésikorlát-csoport eltávolítása	123	Bejegyzés törlése.	170
Proxy hitelesítési csoport kezelése.	123	Bejegyzés módosítása	170
Proxy hitelesítési csoport létrehozása	124	Bejegyzés másolása	171
Proxy hitelesítési csoport módosítása	124	Hozzáférés-felügyeleti listák módosítása	171
Proxy hitelesítési csoport másolása	125	Kiegészítő objektumosztály hozzáadása	171
Proxy hitelesítési csoport eltávolítása	125	Kiegészítő osztály törlése	172
Egyedi attribútumok kezelése	125	Csoporttagságok módosítása	172
Egyedi attribútumlista létrehozása.	125	Címtárbejegyzések keresése	172
Bejegyzés eltávolítása az egyedi attribútumlistából	126	Bináris attribútumok módosítása	174
Az LDAP címtár eléréseinek és változásainak nyomon követése	126	Felhasználók és csoportok kezelése	175
Objektum naplózás engedélyezése a Directory Server számára	127	Felhasználók kezelése	175
Keresési beállítások módosítása	127	Csoportok kezelése	176
Teljesítménnyel kapcsolatos beállítások módosítása	128	Tartományok és felhasználói sablonok kezelése.	178
Adatbázis-kapcsolatok és gyorsítótár-beállítások megadása	128	Tartomány létrehozása	178
Attribútum-gyorsítótár beállítása	129	Tartományadminisztrátor létrehozása	178
Tranzakciós beállítások megadása.	131	Sablon létrehozása	179
Replikáció kezelése	131	Sablon felvétele egy tartományba	181
Elsődleges és replikaszerverekből álló topológia létrehozása	132	Csoportok létrehozása	181
Elsődleges és továbbító szerverekből álló topológia létrehozása	137	Felhasználó felvétele a tartományba	181
Összetett replikációs topológia készítésének áttekintése.	138	Tartományok kezelése	182
Összetett topológia létrehozása egyenrangú replikációval	139	Sablonok kezelése	183
Átjárótopológia beállítása	141	Hozzáférés-felügyeleti listák (ACL-ek) kezelése	185
Topológiák kezelése	143	Hatályos ACL-ek.	186
Replikációs tulajdonságok módosítása	146	Hatályos tulajdonosok	186
Replikációs ütemezések létrehozása	147	Nem szűrt ACL-ek	186
Sorok kezelése	149	Szűrt ACL-ek.	188
Replikáció beállítása biztonságos kapcsolaton keresztül	149	Tulajdonosok	189
Biztonsági tulajdonságok kezelése	150	8. fejezet Referencia 191	
Jelszavak kezelése	150	Parancssori segédprogramok	191
SSL és TSL engedélyezése a Directory Serveren	154	ldapmodify és ldapadd	191
Kerberos hitelesítés engedélyezése a Directory Server-hez.	156	ldapdelete	195
DIGEST-MD5 hitelesítés beállítása a Directory Serveren	157	ldapexop	198
Séma kezelése	157	ldapmodrtn	203
Objektumosztályok megjelenítése.	158	ldapsearch	206
Objektumosztály hozzáadása	158	ldapchangepwd	215
Objektumosztály módosítása	159	ldapdiff	217
		Az SSL védelem LDAP parancssori segédprogramok használata	220
		LDAP adatsere formátum (LDIF)	220
		Példa: LDIF	221
		Version 1 LDIF támogatás	222
		Példák: 1. változat LDIF	222
		Directory Server konfigurációs séma	223
		Címtár-információs fa	223
		Attribútumok	232
		Objektumazonosítók (OID).	261

9. fejezet A Directory Server hibaelhárítása 269

Hibafigyelés és hozzáférés követés a Directory Server feladatnapló segítségével	270
Hibakeresés TRCTCPAPP segítségével	270
Hibák nyomkövetése az LDAP_OPT_DEBUG kapcsolóval	271
GLEnnnn üzenetazonosítók	271
Általános LDAP klienshibák	274
ldap_search: Timelimit exceeded (Időhatár túllépés) [Hibás LDAP művelet]: Operations error (Műveleti hiba)	275
ldap_bind: No such object (Nem létező objektum)	275
ldap_bind: Inappropriate authentication (Nem megfelelő hitelesítés)	275

[Hibás LDAP művelet]: Insufficient access (Nem elegendő elérés)	275
[Hibás LDAP művelet]: Nem lehet az LDAP szerverhez kapcsolódni	275
[Hibás LDAP művelet]: Meghiúsult az SSL szerverhez a kapcsolat	276
Jelszóirányelvekkel kapcsolatos hibák	276
A QGLDCPYVL API hibaelhárítása	276

10. fejezet Kapcsolódó információk 279

Nyilatkozatok	281
Védjegyek	282
Feltételek és kikötések	283

1. fejezet IBM Directory Server for iSeries (LDAP)

Az IBM Directory Server for iSeries, az i5/OS funkciója (a továbbiakban Directory Server) Lightweight Directory Access Protocol (LDAP) szerveret 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.

A következő témakörök segítenek a Directory Server megismerésében és az iSeries szerveren használatában:

2. fejezet, “A V5R4 újdonságai”, oldalszám: 3

Információk a Directory Server terméknek a legutolsó kiadás óta történt módosításairól és továbbfejlesztéseiről.

3. fejezet, “Nyomtatható PDF”, oldalszám: 5

A jelen információs témakör PDF változata.

4. fejezet, “Directory Server - Alapfogalmak”, oldalszám: 7

Információk a Directory Server alapfogalmairól.

5. fejezet, “Első lépések a Directory Server használatában”, oldalszám: 85

Információk a Directory Server beállításával kapcsolatban.

6. fejezet, “Példahelyzet: Directory Server beállítása”, oldalszám: 103

Példa arra, hogyan alakítható ki egy LDAP címtár a Directory Server segítségével.

7. fejezet, “Directory Server felügyelete”, oldalszám: 111

Információk a Directory Server kezelésével kapcsolatban.

8. fejezet, “Referencia”, oldalszám: 191

A Directory Server-rel kapcsolatos referenciaanyag, többek között a parancssori segédprogramok és LDIF információk.

9. fejezet, “A Directory Server hibaelhárítása”, oldalszám: 269

Információk a problémák megoldásával kapcsolatban. Javaslatok szervizadatok begyűjtésére és bizonyos problémák megoldására.

10. fejezet, “Kapcsolódó információk”, oldalszám: 279

A Directory Server-rel kapcsolatos további információk.

2. fejezet A V5R4 újdonságai

A Directory Server for iSeries a következő továbbfejlesztéseket és új funkciókat tartalmazza a V5R4 kiadáshoz:

Replikáció

- **Átjárón keresztüli replikáció:** A replikáció történhet hálózatok között is, átjárószerverek használatával. Az átjárószerverek hatékonyabban gyűjtik össze és továbbítják az információkat, ugyanakkor csökkentik a hálózati forgalmat. További információk: “Replikáció áttekintés” oldalszám: 36, Átjárón keresztüli replikáció fejezet.
- **cn=IBMpolicies:** Egy új tárolóobjektum a replikáló szerverek közötti bejegyzések megosztására. Szemben a cn=localhost objektummal (ez egy olyan bejegyzéstároló, amely nem kerül replikálásra), a cn=IBMpolicies konfigurációszerű adatokat tartalmaz, amelyek replikálására szükség lehet. Részletek: “Utótag (névkontextus)” oldalszám: 14.

Biztonság

- **DIGEST-MD5 hitelesítés:** A DIGEST-MD5 az egyszerű hitelesítési biztonsági réteg (SASL) körébe tartozó hitelesítési mechanizmus. Amikor egy kliens Digest-MD5 hitelesítést használ, a jelszó nem kerül továbbításra nyílt szövegben, és a protokoll megakadályozza az újrakódolás típusú támadásokat is. Részletek: “Hitelesítés” oldalszám: 71.
- **Szállítási réteg biztonság (TLS):** Bekerült egy StartTLS kiterjesztett művelet annak érdekében, hogy a kliens egy nem biztonságos kapcsolatot TLS segítségével biztosíthatóvá módosíthasson. Ezenfelül a szerver támogatja egy 256 bites AES TLS rejtjelkészlet használatát is. Részletek: “Védett socket réteg (SSL) és Fordítási réteg biztonság (TLS) használata LDAP Directory Serverrel” oldalszám: 47.

Keresés (Search)

- **Részfa keresése üres alappal:** A konfigurációs fájlban megadott összes utótag kereshető egyetlen keresési kéréssel. Nincs tehát szükség több keresésre (mindegyikre a keresési alaptól eltérő utótaggal) a teljes címtárban kereséshez. Részletek: “Címtárbejegyzések keresése” oldalszám: 172.
- **Csoportok keresési korlátjai:** E funkció segítségével a rendszergazda különböző keresési korlátokat rendelhet egyes csoportokhoz, az összes felhasználóra megadott általános keresési korlátokon túl. Rugalmasságot biztosít a rendszergazdák számára annak meghatározásában, hogy egy adott szerveren kihez milyen keresési korlát tartozik. Részletek: “Keresési paraméterek” oldalszám: 43.
- **Álnévshivatkozás-feloldás feldolgozás továbbfejlesztései:** A feloldási beállításokat használó keresések teljesítménye lényegesen javul, ha a címtár nem tartalmaz álneveket. Ezenfelül most már léteznek konfigurációs beállítások a kliens keresési kéréseiben megadott hivatkozásfeloldási beállítások felülbírálásához. Részletek: “Keresési paraméterek” oldalszám: 43.
- **Attribútum-gyorsítótár:** Az attribútum-gyorsítótár funkció a teljesítmény növelésére szolgál. Lehetővé teszi, hogy a keresési szűrő feloldása memóriában történjen, nem pedig úgy, hogy a kezdeti feloldás az adatbázisban történik, és az tárolódik a szűrő-gyorsítótárban. Az attribútum-gyorsítótár, szemben a szűrő-gyorsítótárral, nem kerül minden egyes LDAP hozzáadás, módosítás vagy törlés művelet végrehajtása után kiürítésre. Beállítása esetén a szerver automatikusan módosítja a beállított időközönként az attribútum-gyorsítótárakat és a gyorsítótárba helyezi a leghasznosabbnak ítélt attribútumokat - természetesen mindezt az attribútumok gyorsítótárazására megszabott maximális memória keretein belül. Részletek: “Attribútum-gyorsítótár” oldalszám: 82.

Attribútumok

- **Egyedi attribútumok:** Az egyedi attribútumok funkció biztosítja, hogy a megadott attribútum értéke egyedi maradjon a címtárban belül. Például egy rendszergazda előírhatja, hogy a tárolt TAJ-számok egyediek legyenek, hiszen törvény írja elő, hogy két emberhez nem tartozhat ugyanaz az érték. Részletek: “Egyedi attribútumok” oldalszám: 81.

- **Műveleti attribútumok megőrzése:** A creatorsName, createTimestamp, modifiersName és modifyTimestamp műveleti attribútumok most már a fogyasztó szerverekre is továbbreplikálódnak, valamint importálásra/exportálásra kerülnek LDIF fájlalba. Részletek: “Műveleti attribútumok” oldalszám: 81.
- **Nyelvi címkék:** A nyelvi címkék nevű mechanizmus segítségével természetes nyelvek kódjai rendelhetők a címtárban tárolt értékekhez és a kliensek lekérdezhetik a bizonyos természetes nyelvi feltételeknek megfelelő értékeket. Részletek: “Nyelvi címkék” oldalszám: 44.

Csoportok

- **Adminisztrátor felhasználók csoportja:** Több felhasználói megkülönböztetett név (DN) is rendelkezhet szinte ugyanazzal az adminisztrátori jogkörrel, mint az LDAP szerver rendszergazdája. E funkció használatával több felhasználó is képes elvégezni az adminisztrációs feladatokat anélkül, hogy osztozniuk kellene egy felhasználói azonosítón és jelszón. Részletek: “Adminisztratív hozzáférés” oldalszám: 55.
- **Proxy felhatalmazás:** A proxy felhatalmazás lehetővé teszi, hogy egy LDAP kliens egy adott felhasználó nevében csatlakozzon, de egy másik felhasználó nevében érje el a cél könyvtárat. Ez javítja a kliensalkalmazások rugalmasságát, mivel több felhasználó nevében is képesek műveleteket végezni anélkül, hogy minden egyes felhasználó nevében újra kellene csatlakozni. Részletek: “Proxy hitelesítés” oldalszám: 55.

Egyéb

- **Figyelési továbbfejlesztések:** A webes adminisztrációs eszközzel most már a szerver- és kapcsolati információk is megtekinthetők. A figyelés javítására a következő továbbfejlesztések történtek:
 - Javíthatóság és szolgáltatás megbénítása
 - Új információkkal bővült a figyelő kimenete. Megtekinthető az elvégzett műveletek száma típusonként (BIND, MODIFY, COMPARE, SEARCH stb.), a munkasor mélysége, a rendelkezésre álló dolgozó szálak száma, a szervernaplóba beírt üzenetek száma, a felügyeleti napló, a CLI hibák, az SSL és TLS kapcsolatok száma, az üres kapcsolatok információi, valamint a végszálak statisztikái.
 - Egy új keresési alap (“cn=workers,cn=monitor”) szolgál a dolgozó szálak információinak visszaadására.
 - Attribútum-gyorsítótár
 - A gyorsítótárral és a gyorsítótárban található attribútumokkal kapcsolatos információk (beállított méret, összméret, találati arány) rögzítésre kerülnek.
 - Egy új keresési alap (“cn=changelog,cn=monitor”) szolgál a változásnapló attribútum-gyorsítótár információinak visszaadására.
- **Kliensalkalmazások az aktuális felhasználóként hitelesítésének támogatása:** Az LDAP kliens és a parancssori segédprogramok bővítésre kerültek, és támogatják az aktuális felhasználó nevében történő hitelesítést a helyi címtárszerver felé. Ez akkor különösen hasznos például, ha adminisztrációs feladatokat kell elvégezni egy olyan i5/OS felhasználóként bejelentkezve, amelyik rendelkezik adminisztrátori jogkörrel a címtárra vonatkozóan.
- **Rendszer- és korlátozott attribútumok hozzáférés-felügyelete:** Most már az LDAP bejegyzéseknek a hozzáférés-felügyelettel kapcsolatos és a szerver által kezelt rendszer- és korlátozott attribútumainak hozzáférése is felügyelhető.
- **Felhasználók átmásolása egy ellenőrzési listából egy LDAP címtárba:** A címtárszerver feltölthető címtárobjektumokkal egy felhasználó által megadott, HTTP-szerű ellenőrzési listában felsorolt felhasználók alapján is. A címtárszerver ezenfelül képes hitelesíteni a felhasználókat egy HTTP ellenőrzési listából átmásolt hitelesítési adatok alapján is. Ezt a folyamatot új alkalmazás programozási felületek (API) támogatják. Részletek: “Felhasználók másolása HTTP szerver ellenőrzési listából a Directory Serverbe” oldalszám: 94.
- **Szolgáltatás megbénítása és kötött DN leválasztása:** Új funkciók szolgálnak a szolgáltatás megbénítása típusú támadások azonosítására, az ilyen támadások átvészelésére és az utánuk történő helyreállításra. Ilyen továbbfejlesztés például az, hogy a rendszergazda nagyobb szabadságot kap a szerver kezeléséhez, illetve különféle automatikus igazítások. Részletek: “Szolgáltatás megbénítása” oldalszám: 74.
- **Még szélesebb körű webes adminisztrációs funkcionalitás:** Még több feladat elvégezhető a webes adminisztrációs eszközzel. Az új funkciók nagy része az új **Szerveradminisztráció** kategória alatt található.

3. fejezet Nyomtatható PDF

A dokumentum PDF változatának megtekintéséhez vagy letöltéséhez válassza ki a Directory Server (LDAP) dokumentumot (megközelítőleg 2700 KB).

Egyéb információk


A vonatkozó kézikönyvek PDF fájljainak, illetve a Redbook kiadványok megtekintése és nyomtatása: 10. fejezet, "Kapcsolódó információk", oldalszám: 279.

PDF fájlok mentése

A PDF fájl mentése a munkaállomáson megjelenítés vagy nyomtatás céljából:

1. Kattintson a jobb egérgombbal a PDF fájlra a böngészőben (a fenti hivatkozás).
2. Kattintson az opcióra, amely helyi lemezre menti a PDF-et.
3. Válassza ki azt a könyvtárat, ahová a PDF fájlt mentenie kívánja.
4. Kattintson a **Mentés** gombra.

Adobe Reader letöltése

- | A PDF fájlok megjelenítéséhez vagy nyomtatásához telepíteni kell az Adobe Acrobat Reader programot a rendszeren.
- | A programot ingyen letöltheti az Adobe honlapjáról (www.adobe.com/products/acrobat/readstep.html)  .

4. fejezet Directory Server - Alapfogalmak

A Directory Server az Internet Engineering Task Force (IETF) LDAP V3 ajánlásait valósítja meg. A funkcionalitás és a teljesítmény terén tartalmazza az IBM kiegészítéseit. A jelen verzió az IBM DB2 Universal Database for iSeries adatbázis-kezelőjét használja háttértárként az LDAP műveletek tranzakciós integritása, a nagyteljesítményű működés, valamint az üzem közbeni mentési és visszaállítási lehetőségek érdekében. Együttműködik az IETF LDAP V3 szabványnak megfelelő kliensekkel. A Directory Server alapfogalmaival és megfontolásával kapcsolatos témakörök:

- “Címtárak”
- “Megkülönböztetett nevek (DN)” oldalszám: 11
- “Utótag (névkontextus)” oldalszám: 14
- “Séma” oldalszám: 15
- “Közzététel” oldalszám: 35
- “Replikáció” oldalszám: 36
- “Tartományok és felhasználói sablonok” oldalszám: 42
- “Keresési paraméterek” oldalszám: 43
- “Nemzeti nyelvek támogatása (NLS)” oldalszám: 44
- “Nyelvi címkék” oldalszám: 44
- “LDAP címtárutalások” oldalszám: 46
- “Tranzakciók” oldalszám: 46
- “Directory Server biztonsága” oldalszám: 46
- “Operációs rendszer leképzett háttér objektumai” oldalszám: 75
- “Directory Server és i5/OS naplózási támogatás” oldalszám: 80
- “Egyedi attribútumok” oldalszám: 81
- “Műveleti attribútumok” oldalszám: 81
- “Szerver gyorsítótárak” oldalszám: 82
- “Vezérlőelemek és kiterjesztett műveletek” oldalszám: 84

Címtárak

A Directory Server (címtárszerver) segítségével egy olyan adatbázistípus érhető el, amely az információkat az i5/OS integrált fájlrendszerének felépítéséhez hasonló, hierarchikus struktúrába szervezve tárolja.

Ha ismert az objektum neve, jellemzői lekérhetők. Ha egy adott objektum neve nem ismert, akkor a címtárból kikereshetők egy adott feltételrendszernek megfelelő objektumok. A címtárakat általában meghatározott feltételek, nemcsak kategóriák előre megadott halmaza alapján szokás keresni.

A címtár egy speciális adatbázis, amelynek jellemzői valamelyest eltérnek az általános célú relációs adatbázisokétól. Ilyen jellemző például, hogy egy címtárat általában sokkal sűrűbben érnek el (olvasnak vagy keresnek benne), mint frissítik (írják). Mivel a címtáraknak nagyon nagy mennyiségű olvasási kérést kell kiszolgálniuk, általában olvasási hozzáféréshez is vannak optimalizálva. Mivel a címtáraknak nem kell olyan sokféle funkciót biztosítaniuk, mint az általános célú adatbázisoknak, optimalizálhatók arra, hogy gazdaságos módon, több alkalmazást is kiszolgáljanak címtáradatokkal nagy, elosztott környezetekben is.

A címtár lehet központosított vagy elosztott. Az első esetben egyetlen címtárszerver (vagy szerverfürt) szolgálja ki az összes címtárkérést. Ha a címtár elosztott, akkor több, földrajzilag általában távol is első szerver biztosít hozzáférést a címtárhoz.

A címtár elosztása esetén a címtárban tárolt adatok feloszthatók, particionálhatók vagy replikálhatók. A particionálás azt jelenti, hogy minden egyes címtárszerver az adatok külön, egyedi, nem összefüggő részhalmozását tárolják. Más szavakkal, egy címtárbejegyzés csak egy szerveren tárolódik. A címtár ilyen módon felosztása esetén úgynevezett LDAP utalásokat kell használni. Az LDAP utalások segítségével az ugyanazon vagy más névtérre vonatkozó Egyszerűsített címtárhozzáférési protokoll (LDAP) kérések átirányíthatók egy másik (vagy akár ugyanazon) szerverre. Az információk replikálása esetén egynél több szerver is tárolja ugyanazokat az adatokat. Egy elosztott címtárban az is előfordulhat, hogy az adatok egy része particionálva van, más részük pedig replikálva.

Az LDAP címtárszerver modell bejegyzésekre (más néven objektumokra) épül. Minden egyes bejegyzés egy vagy több attribútumot (mint pl. egy név vagy cím) és egy típust tartalmaz. A típusok általában emlékeztető karakter sorozatokkal vannak megadva: a cn jelenti a közönséges nevet (common name), a mail pedig az e-mail címet.

A példacímtárban (1. ábra: oldalszám: 9) található egy bejegyzés Tim Jones számára, amely mail és telephoneNumber (telefonszám) tulajdonságai vannak. További szokásos attribútumok: fax, title (beosztás), sn (surname, azaz vezetéknév) és jpegPhoto.

Minden egyes címtárnak van egy sémája. A séma szabályok gyűjteménye, amelyek meghatározzák a címtár struktúráját és tartalmát. A séma a webes adminisztrációs eszközzel tekinthető meg. További információ a sémáról: "Séma" oldalszám: 15.

Mindegyik címtárbejegyzésnek 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 sémaszabályokat, amelyeknek egy bejegyzés engedelmessé kell tartoznia.

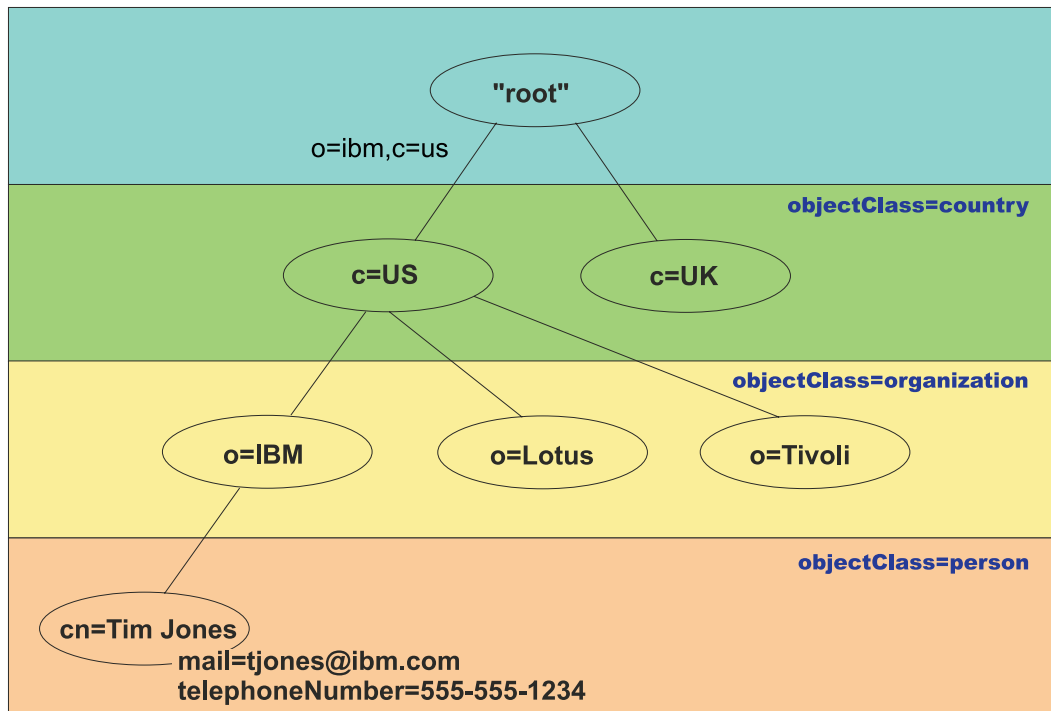
A séma által megadott attribútumok mellett vannak a szerver által kezelt attribútumok is. Ezek közt az úgynevezett működési attribútumok közt olyan dolgok találhatók, mint például mikor lett létrehozva a bejegyzés, hozzáférés-felügyeleti információk és hasonlóak. A működési attribútumokról további információk: "Műveleti attribútumok" oldalszám: 81.

Hagyományosan, az LDAP címtárbejegyzések hierarchikus struktúrába rendeződnek, amely politikai, földrajzi, vagy szervezeti határokat tükröz (1. ábra: oldalszám: 9). Az országokat vagy régiókat 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.

Az LDAP a bejegyzésekre megkülönböztetett nevekkkel (Distinguished Names, DN-ek) hivatkozik. Egy megkülönböztetett név tartalmazza magának a bejegyzésnek a nevét, csakúgy, mint a címtárban felette álló objektumok nevét letről felfelé. Például, az 1. ábra: oldalszám: 9 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 nevezi meg a bejegyzést, vagyis ez egy RDN. Az o=IBM, c=US a szülő DN a cn=Tim Jones számára. További információk a DN-ekről: "Megkülönböztetett nevek (DN)" oldalszám: 11.

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 utótagoknak 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 1. ábra: oldalszám: 9 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.

LDAP címtárstruktúra



RV4Q100-1

1. ábra: LDAP címtárstruktúra

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

Tegyük fel, hogy létre akar hozni egy címtárt tartomány komponens struktúra alapján, különféle alkalmazotti adatokkal (név, telefonszám és e-mail cím). A TCP/IP tartomány alapján meghatározott utótagot vagy névkontextust fogja használni. Ez a címtár valahogy így néz ki:

```
/
|
+- ibm.com
  |
  +- employees
    |
    +- Tim Jones
      |
      | 555-555-1234
      | tjones@ibm.com
    +- John Smith
      |
      | 555-555-1235
      | jsmith@ibm.com
```

Ténylegesen beírva a Directory Server-be, az adatok ilyen formát öltenek:

```
# ibm.com utótag
dn: dc=ibm,dc=com
objectclass: top
objectclass: domain
dc: ibm
```

```
# employees (alkalmazottak) címtár
dn: cn=employees,dc=ibm,dc=com
objectclass: top
```

```

objectclass: container
cn: employees

# Tim Jones alkalmazott
dn: cn=Tim Jones,cn=employees,dc=ibm,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: publisher
objectclass: ePerson
cn: Tim Jones
cn: "Jones, Tim"
sn: Jones
givenname: Tim
telephonenumber: 555-555-1234
mail: tjones@ibm.com

# John Smith alkalmazott
dn: cn=John Smith,cn=employees,dc=ibm,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: publisher
objectclass: ePerson
cn: John Smith
cn: "Smith, John"
sn: Smith
givenname: John
telephonenumber: 555-555-1235
mail: jsmith@ibm.com

```

Bizonyára feltűnt, hogy minden bejegyzésben vannak objectclass nevű attribútumok. Az objectclass értékek határozzák meg, hogy a bejegyzésben milyen tulajdonságok használhatók (például telephonenumber vagy givenname). Az engedélyezett objektumosztályok a sémában vannak meghatározva. A séma az a szabályhalmaz, amelyik megadja, milyen bejegyzéstípusok fordulhatnak elő az adatbázisban.

Címtárkliensek és -szerverek

A címtárak hozzáférése általában az úgynevezett kliens-szerver típusú kommunikációval történik. A kliens- és a szerverfolyamatoknak nem kell ugyanazonokon a gépeken futniuk. Egy szerver számos klienst képes egyszerre kiszolgálni. Egy alkalmazásnak, amelyik a címtár adatait akarja olvasni vagy írni, nem kell közvetlenül elérnie a címtárat. Ehelyett meghív egy funkciót vagy alkalmazásprogram illesztőt (API), amelynek hatására egy másik folyamat küld el egy üzenetet. Ez a második folyamat éri el a címtár adatait a kérő alkalmazás nevében. Az írási vagy olvasási művelet eredményeit utána visszaadja a kérő alkalmazásnak.

Egy API egy adott programozási nyelven programozási felületet biztosít egy adott szolgáltatás eléréséhez. A kliens és a szerver között haladó üzenetek formátumának és tartalmának meg kell felelnie egy előre meghatározott protokollnak. Az LDAP címtárkliensek és címtárszerverek közötti üzenetek protokollját határozza meg. Tartozik hozzá egy LDAP API C nyelven, valamint a címtár elérési lehetősége Java alkalmazásokból a Java Naming and Directory Interface (JNDI) nevű illesztőn keresztül.

Címtárbiztonság

Egy címtárnak biztosítania kell legalább alapszintű funkciókat egy biztonsági rendszer kialakításához. Előfordul, hogy a címtár nem maga biztosítja a biztonsági funkciókat, hanem integrálva van egy megbízható hálózati biztonsági szolgáltatással, és az végzi a biztonsági szolgáltatásokat. Először is, szükség van a felhasználók hitelesítésére. A hitelesítés során derül ki, hogy a felhasználó valóban az-e, akinek mondja magát. A legalapvetőbb hitelesítési megoldás egy felhasználónév és egy jelszó bekérése. A felhasználók hitelesítése után meg kell állapítani, hogy rendelkeznek-e megfelelő jogosultságokkal vagy engedélyekkel az adott objektum kért műveletének elvégzésére.

A felhatalmazás gyakran hozzáférés-felügyeleti listák (ACL) használatával történik. Az ACL tulajdonképpen jogosultságok egy listája, amely a címtárobjektumaihoz és attribútumaihoz kapcsolható. Az ACL felsorolja, hogy az egyes felhasználók vagy csoportok milyen típusú hozzáférésre jogosultak (vagy hogy milyenre nem). Az ACL-ek leegyszerűsítése és kezelhetőbbé tétele érdekében ugyanazon hozzáférési jogok gyakran csoportokba vannak szervezve.

Megkülönböztetett nevek (DN)

A címtár minden bejegyzésének vagy egy megkülönböztetett neve (DN). A DN az a név, amelyik egyedi módon azonosítja a címtárbejegyzést. A DN vesszőkkel elválasztott attribútum=érték párokból épül fel, például:

```
cn=Ben Gray,ou=editing,o=New York Times,c=US
cn=Lucille White,ou=editing,o=New York Times,c=US
cn=Tom Brown,ou=reporting,o=New York Times,c=US
```

A címtársémában megadott bármelyik attribútum használható DN kialakítására. Az egyes attribútum=érték párok sorrendje számít. A DN a címtárhierarchia minden szintjéről egy elemet tartalmaz, a fa gyökerétől egészen le addig a szintig, ahol a bejegyzés található. Az LDAP DN-ek a legkonkrétabb attribútummal kezdődnek (jellemzően valamiféle névvel), majd egyre szélesebb körű attribútumok következnek, a végén gyakran például az országot jelző értékkel. A DN első elemét szokás relatív megkülönböztetett névként (Relative Distinguished Name, RDN) emlegetni. Ez különbözteti meg a bejegyzés az összes többi olyantól, amelyeknek ugyanaz a szülője. A fenti második példában a "cn=Ben Gray" RDN különbözteti meg az első bejegyzést a másodiktól ("cn=Lucille White" RDN). Összes többi elemükben egyébként megegyeznek. Az RDN attribútum=érték párjának szintén benne kell lenni a bejegyzésben. (Ez a DN többi elemére nem feltétlenül igaz.)

Tekintse meg az alábbi példát egy személy bejegyzéséről:

```
dn: cn=Tim Jones,o=ibm,c=us
objectclass: top
objectclass: person
cn: Tim Jones
sn: Jones
telephonenumber: 555-555-1234
```

Speciális karakterek a DN-ekben

Bizonyos karakterek speciális jelentéssel bírnak a DN-eken belül. Először is, az = (egyenlőségjel) választja el az attribútumneveket az értékektől, a , (vessző) pedig az attribútum=érték párokat választja el. A speciális karakterek: , (vessző), = (egyenlőségjel), + (plusz), < (kisebb mint), > (nagyobb mint), # (kettőskereszt), ; (pontosvessző), \ (balra döntött törtvonal) és " (idézőjel, ASCII 34).

A speciális karakterek megfelelő jelzőkarakterekkel megelőzve elveszítik speciális jelentésüket. A speciális karakterek névértéken beírásához egy DN karaktersorozatba, használja a következő lehetőségeket:

1. Speciális karakterek elé írjon egy balra döntött törtvonalat (` ASCII 92). A következő példa egy vesszőt tartalmazó szervezeti név beírását mutatja:

```
CN=L. Eagle,o=Sue\, Grabbit and Runn,C=GB
```

Ez a javasolt módszer.

2. Másik megoldás, ha a balra döntött törtvonal után két hexadecimális számjegyet ír, amelyek együttesen a karakter kódját adják. A karakter kódjának **muszáj** UTF-8 kódolásúnak lennie.

```
CN=L.
Eagle,o=Sue\2C Grabbit and Runn,C=GB
```

3. A teljes attribútumértéket "" (idézőjelek, ASCII 34) közé teszi, amelyek nem képezik az érték részét. Az idézőjel-karakter párok közt minden karakter névértéken kerül figyelembe vételre, kivéve a \ (balra döntött törtvonal) karaktert. A \ (balra döntött törtvonal) használható egy másik balra döntött törtvonal (ASCII 92) előtt, idézőjelek (ASCII 34) előtt és belül, az előbb említett többi speciális karakter, illetve hexadecimális párok előtt (fenti 2. számú módszer). Ha tehát be akarjuk vinni a cn=xyz"qrs"abc nevet idézőjelestül, akkor cn=xyz\"qrs\"abc vagy \ formában kell beírni:

```
"egy balra döntött törtvonal így írható be: \\"
```

Egy másik példa: "\Zoo" érvénytelen, mert a 'Z' elé nem kell és nem is írható jelentésmódosító karakter.

Pszeudo DN-ek

A pszeudo DN-eket a hozzáférés-felügyeletben és a kiértékeléseknél használja a rendszer. Az LDAP címtár számos pszeudo DN használatát lehetővé teszi (például "group:CN=THIS" vagy "access-id:CN=ANYBODY"). Ezek célja, hogy nagyszámú, hasonló jellemzőkkel bíró DN-re hivatkozzanak, amelyek valamilyen jellemzője közös, akár az elvégzett művelettel, akár a művelet alanyául szolgáló objektummal kapcsolatban. További információk a hozzáférés-felügyeletről: "Directory Server biztonsága" oldalszám: 46.

A Directory Server három pszeudo DN használatát támogatja:

- access-id: CN=THIS

Egy ACL részeként megadva ez a DN a bindDN attribútumra vonatkozik, amelyik azzal a DN-nel egyezik meg, amelyiken a művelet végrehajtásra kerül. Ha például egy művelet a "cn=personA, ou=IBM, c=US" objektumon kerül végrehajtásra és a bindDn attribútum értéke "cn=personA, ou=IBM, c=US", akkor a megadott jogosultságok a "CN=THIS"-nek és a "cn=personA, ou=IBM, c=US"-nek megadott jogosultságok együttese lesz.

- group: CN=ANYBODY

Egy ACL részeként megadva ez a DN az összes felhasználót jelenti, még azokat is, akik nincsenek hitelesítve. A felhasználók nem törölhetők ebből a csoportból, és ez a csoport nem törölhető az adatbázisból.

- group: CN=AUTHENTICATED

Ez a DN az összes olyan DN-t tartalmazza, amelyek hitelesítve lettek a címtár által (be vannak jelentkezve). A hitelesítés módszere nem számít.

Megjegyzés: A "CN=AUTHENTICATED" azokat a DN-eket jelenti, amelyek hitelesítették magukat a szerveren bárhol, függetlenül attól, hogy a DN-hez tartozó objektum ténylegesen hol is található. Célszerű azonban óvatosan bánni ezzel a pszeudo DN-nel. Tegyük fel például, hogy egy adott utótag, a "cn=Secret" alatt található egy "cn=Bizalmas anyag", amelynek az ACL attribútuma (aclentry) "group:CN=AUTHENTICATED:normal:rsc". Egy másik utótag, a "cn=Common" alatt meg legyen egy "cn=Nyilvános anyag". Ha ez a kettő ugyanazon a szerveren található, akkor a "cn=Public Material"-hoz kapcsolódás hitelesítettnek számít, és a fenti ACL használata esetén jogosultságot kap a "cn=Bizalmas anyag" objektum normál osztályához is.

Néhány példa pszeudo DN-ekre:

1. példa

Legyen a cn=personA, c=US objektum ACL-je

AclEntry: access-id: CN=THIS:critical:rwsc

AclEntry: group: CN=ANYBODY: normal:rsc

AclEntry: group: CN=AUTHENTICATED: sensitive:rcs

Az így kapcsolódó felhasználó	Ezt kapja
cn=personA, c=US	normal:rsc:sensitive:rcs:critical:rwsc
cn=personB, c=US	normal:rsc:sensitive:rsc
Anonymous	normal:rsc

Ebben a példában personA a "CN=THIS" azonosítóhoz, továbbá a "CN=ANYBODY" és "CN=AUTHENTICATED" pszeudo DN csoportokhoz rendelt jogosultságokat kapja.

2. példa

Legyen a cn=personA, c=US cn=personA, c=US AclEntry: access-id:cn=personA, c=US: object:ad objektum ACL-je

AclEntry:

access-id: CN=THIS:critical:rwsc

AclEntry: group: CN=ANYBODY: normal:rsc

AclEntry: group: CN=AUTHENTICATED: sensitive:rcs

A cn=personA, c=US objektumon végzett művelet esetében:

Az így kapcsolódó felhasználó	Ezt kapja
cn=personA, c=US	object:ad:critical:rwsc
cn=personB, c=US	normal:rsc:sensitive:rsc
Anonymous	normal:rsc

Ebben a példában personA a "CN=THIS" azonosítóhoz, továbbá a DN-nek ("cn=personA, c=US") magának adott jogosultságokat kapja. Figyelje meg, hogy csoportos jogosultságok a bind DN ("cn=personA, c=US") specifikusabb acentry attribútuma ("access-id:cn=personA, c=US") miatt nem kerülnek kiadásra.

Kibővített DN feldolgozás

Egy DN összetett RDN-je több, egymással '+' operátorral elválasztott összetevőből áll. A szerver kibővíti az ilyen DN-nel rendelkező bejegyzések kereséseit. Összetett RDN bármilyen sorrendben megadható a keresés alapjául.

```
ldapsearch -b
"cn=mike+ou=austin,o=ibm,c=us" "(objectclass=*)"
```

A szerver támogatja a DN normalizálás kiterjesztett műveletet. A DN normalizálás kiterjesztett művelet a DN-eket a serverséma alapján normalizálja. Ez a kiterjesztett művelet hasznos lehet a DN-eket használó alkalmazások esetén. További információk a kiterjesztett műveletekről: "Vezérlőelemek és kiterjesztett műveletek" oldalszám: 84.

Megkülönböztetett nevek szintaxisa

A megkülönböztetett nevek (DN) szintaxisa az RFC 2253 szerinti. A Backus-Naur formátumú szintaxis (BNF) a következő:

```
<név> ::= <név-összetevő> ( <köz-elválasztó> )
        | <név-összetevő> <köz-elválasztó> <név>

<köz-elválasztó> ::= <elhagyható-köz>
                   <elválasztó>
                   <elhagyható-köz>

<elválasztó> ::= ", " | ";"

<elhagyható-köz> ::= ( <CR> ) *( " " )

<név-összetevő> ::= <attribútum>
                  | <attribútum> <elhagyható-köz> "+"
                  | <elhagyható-köz> <név-összetevő>

<attribútum> ::= <karaktersorozat>
                | <kulcs> <elhagyható-köz> "=" <elhagyható-köz> <karaktersorozat>

<kulcs> ::= 1*( <kulcskarakter> ) | "OID." <oid> | "oid." <oid>
<kulcskarakter> ::= betűk, számok és szóköz

<oid> ::= <számsor> | <számsor> "." <oid>
<számsor> ::= 1*<számjegy>
<számjegy> ::= 0-9 számjegyek

<karaktersorozat> ::= *( <karakter> | <pár> )
                   | ''' *( <karakter> | <speciális> | <pár> ) '''
                   | "#" <hexa>

<speciális> ::= ", " | "=" | <CR> | "+" | "<" | ">"
              | "#" | ";"

<pár> ::= "\" ( <speciális> | "\" | "'" )
<karakter> ::= bármilyen karakter, kivéve a <speciális> vagy "\" vagy "'"
```

```
<hexa> ::= 2*<hexa-karakter>
<hexa-karakter> ::= 0-9, a-f, A-F
```

Pontosvessző (;) karakterrel is elválaszthatók a külön RDN-ek egy megkülönböztetett névben, bár a vessző (,) karakter a szokásos jelölés.

Szóköszerű karakterek (szóközök) szerepelhetnek a vessző vagy pontosvessző bármelyik oldalán. A szóköszerű karakterek figyelmen kívül maradnak, a pontosvessző pedig vesszőre cserélődik.

Ezenfelül szóköz (' ' ASCII 32) karakterek szerepelhetnek a '+' és '=' előtt vagy után. Elemzéskor ezek a szóköz karakterek figyelmen kívül maradnak.

A következő példa megkülönböztetett neve egy olyan formában van írva, amely kényelmesen használható a nevek szokásos formájához. Az első rész egy három részből álló név. Az első rész egy összetett RDN. Az összetett RDN egynél több attribútum-érték párból áll és arra használható, hogy azonosítsa egy adott bejegyzést olyan esetben, amikor egyetlen sima CN érték kétértelmű lenne:

```
OU=Sales+CN=J. Smith,O=Widget Inc.,C=US
```

Utótag (névkontextus)

Az utótag (más néven névkontextus) egy olyan DN, amely egy helyileg tárolt címtárhierarchia legfelső bejegyzését azonosítja. Az LDAP relatív elnevezési sémája miatt ez a DN az adott címtárhierarchia minden más bejegyzésének az utótagja is. Egy címtárszerver több utótagot is kezelhet, amelyek mindegyike egy helyileg tárolt címtárhierarchiát azonosít, mint például az o=ibm,c=us.

Az utótaggal megegyező bejegyzést kötelező felvenni a címtárba. A létrehozott bejegyzésnek egy olyan objectclass értékkel kell rendelkeznie, amely tartalmazza a használt névattribútumot. Az utótagnak megfelelő bejegyzés létrehozásához használható akár a webes adminisztrációs eszköz, akár a Qshell ldapadd segédprogramja. További információk: "Címtárbejegyzések kezelése" oldalszám: 168 vagy "ldapmodify és ldapadd" oldalszám: 191.

Elméletileg létezik egy globális LDAP névtér. A globális LDAP névtérben ilyen DN-ek fordulhatnak elő:

- cn=John Smith,ou=Rochester,o=IBM
- cn=Jane Doe,o=My Company,c=US
- cn=rendszergazda,dc=myco,dc=com

Az "o=IBM" utótag azt jelzi a szerver számára, hogy csak az első DN található a szerveren tárolt névtérben. Az olyan objektumokra hivatkozás, amelyek nem, "nincs ilyen objektum" hibákat eredményeznek, vagy utalást egy másik címtárszerverre.

Egy szerver több utótagot is kezelhet. A Directory Server számos előre megadott utótagot biztosít, amely az adott megvalósításra vonatkozó adatokat tárol:

- A cn=schema a séma LDAP-n keresztül elérhető ábrázolását tartalmazza
- A cn=changelog a szerver változtatási naplóját tartalmazza (már ha be van kapcsolva)
- A cn=localhost nem replikált, a szerver működését valamilyen módon befolyásoló információkat tartalmaz, például a replikáció-konfigurációs objektumokat
- A cn=IBMpolicies olyan információkat tartalmaz a szerver működésével kapcsolatban, amelyek *replikálásra* *kerülnek*.
- A cn=pwdpolicy a szerverre kiterjedő jelszó-irányelvet tartalmazza
- Az "os400-sys=system-name.mydomain.com" utótag az i5/OS objektumok LDAP-n keresztüli elérését biztosítja (egyelőre csak felhasználói profilok és csoportok)

A Directory Server az egyszerűbb beüzemelés érdekében előre beállításra kerül egy alapértelmezett utótaggal: `dc=rendszer_neve,dc=tartomány_neve`. Nem kötelező ezt az utótagot használni. Saját utótagok is felvehetők, az előre megadott utótag pedig törölhető.

Az utótagokra vonatkozóan kétféle szokásos elnevezési megállapodás létezik. Az egyik a szervezet TCP/IP tartományára épül. A másik a szervezet nevét és helyét használja.

Ha tehát a cég TCP/IP tartományának neve `mycompany.com`, akkor választható például a `dc=mycompany,dc=com` értékhez hasonló utótag (a `dc` attribútum a tartománykomponensre utal). Ebben az esetben a címtárban létrehozott legmagasabb szintű bejegyzés az alábbihoz hasonló lehet (LDIF, az LDAP bejegyzéseket ábrázoló szöveges fájlformátum használata esetén):

```
dn: dc=mycompany,dc=com
objectclass: domain
dc: mycompany
```

A `domain` objektumosztály néhány egyéb attribútummal is rendelkezik. Tekintse meg a sémát vagy módosítsa a bejegyzést a webes adminisztrációs eszközzel és tekintse meg, milyen egyéb attribútumokat használhat. További információk: "Séma kezelése" oldalszám: 157.

Ha a cég neve `Retroimpex` és Magyarországon működik, akkor például használhat az alábbihoz hasonló utótagot:

```
o=Retroimpex
o=Retroimpex,c=HU
ou=Kattantyú részleg,o=Retroimpex,c=HU
```

ahol `OU` az `organizationalUnit` (szervezeti egység) objektumosztály neve, `O` a szervezet neve az `organization` (szervezet) objektumosztályban, a `C` pedig a szabványos kétbetűs rövidítése az ország nevének a `country` (ország) objektumosztályban. Ebben az esetben a létrehozandó legfelső szintű bejegyzés így néz ki:

```
dn: o=Retroimpex,c=HU
objectclass: organization
o: Retroimpex
```

Lehetnek olyan alkalmazások, amelyek megkövetelik bizonyos utótagok létrehozását, illetve egy bizonyos elnevezési megállapodás használatát. Ha például a címtár digitális igazolásokat is kezel, akkor kötelező lehet a címtár egy részét úgy szervezni, hogy a bejegyzések nevei megegyezzenek a tárolt igazolások tárgy DN-jeivel.

A címtárba felvett bejegyzések utótagjának egyeznie kell a DN értékével (például `ou=Marketing,o=ibm,c=us`). Ha egy lekérdezés olyan utótagot tartalmaz, amelyik a helyi adatbázishoz beállított utótagok egyikének sem felel meg, akkor a lekérdezés továbbításra kerül az alapértelmezett utalásként (referral) megjelölt LDAP szerverhez. Ha nincs kijelölve LDAP alapértelmezett hivatkozás, akkor egy "objektum nem található" hibaüzenet kerül visszaadásra.

Az utótagok felvételével és törlésével kapcsolatos további információk: "Directory Server utótagok felvétele és eltávolítása" oldalszám: 118.

Séma

A séma az a szabályhalmaz, amelyik szabályozza, milyen adatok tárolhatók a címtárban. A séma határozza meg az engedélyezett bejegyzések típusát, attribútumaik szerkezetét és szintaxisát.

A címtár adatai címtárbejegyzésekben tárolódnak. Egy bejegyzés egy kötelező objektumosztályból, valamint attribútumokból áll. Az attribútumok lehetnek kötelezők és elhagyhatók. Az objektumosztályok határozzák meg a bejegyzést leíró információk fajtáját és a tartalmazott attribútumok halmazát. Minden egyes attribútumhoz egy vagy több érték tartozik. A bejegyzések kezelésével kapcsolatos további információk: "Címtárbejegyzések kezelése" oldalszám: 168.

A sémákkal kapcsolatos további információk:

- "IBM Directory Server sémája" oldalszám: 16

- “Általános séma támogatása” oldalszám: 17
- “Objektumosztályok” oldalszám: 18
- “Attribútumok” oldalszám: 19
- “Objektumazonosító (OID)” oldalszám: 26
- “Alséma-bejegyzések” oldalszám: 27
- “Az IBMsubschema objektumosztály” oldalszám: 27
- “Sémalekérdések” oldalszám: 27
- “Dinamikus séma” oldalszám: 27
- “Nem engedélyezett sémamódosítások” oldalszám: 28
- “Sémaellenőrzés” oldalszám: 31
- “iPlanet-kompatibilitás” oldalszám: 33
- “Generalized time és UTC time” oldalszám: 33

IBM Directory Server sémája

A Directory Server sémája előre meghatározott, azonban az igényeknek megfelelően a séma módosítható. További információ a séma módosításáról: “Séma kezelése” oldalszám: 157.

A Directory Server képes dinamikus sémakezelésre. A séma a címtár adatok részeként kerül közzétételre és a Subschema bejegyzésben (DN="cn=schema") érhető el. A séma az ldap_search() API függvénnyel kérdezhető le és az ldap_modify() függvénnyel módosítható. Az API-hívásokkal kapcsolatos további információkat a “Directory Server API-k” témakörben talál.

A séma több konfigurációs adatot tartalmaz, mint amit az LDAP Version 3 Request For Comments (RFC) dokumentum vagy a szabványmeghatározások előírnak. Például egy adott attribútumhoz megjelölhető, milyen indexeket kell tárolni. Ez a kiegészítő konfigurációs jellemző, amennyiben lehetséges, a subschema bejegyzésben tárolódik. Az IBMsubschema nevű subschema bejegyzéshez egy további objektumosztály van meghatározva, amelynek "MAY" attribútumai tárolják a kiterjesztett sémainformációkat.

A Directory Server egyetlen sémát ad meg az egész szerverhez, amely egy speciális címtárbejegyzés ("cn=schema") alól érhető el. Ez a bejegyzés tartalmazza a szerverhez megadott teljes sémát. A sémainformációk lekéréséhez hajtson végre egy ldap_search hívást az alábbi módon:

```
DN: "cn=schema", keresési hatókör: base, szűrő: objectclass=subschema
vagy objectclass=*
```

A séma az alábbi attribútumtípusokhoz biztosít értékeket:

- objectClass (az objektumosztályokkal kapcsolatos további információk: “Objektumosztályok” oldalszám: 18.)
- attributeType (az attribútumtípusokkal kapcsolatos további információk: “Attribútumok” oldalszám: 19.)
- IBMAttributeTypes (Az IBMAttributeTypes attribútummal kapcsolatos további információk: “Az IBMAttributeTypes attribútum” oldalszám: 21.)
- megfeleltetési szabályok (a megfeleltetési szabályokkal kapcsolatos további információk: “Megfeleltetési szabályok” oldalszám: 22).
- ldap szintaxis (további információk az LDAP szintaxisról: “Attribútum-szintaxis” oldalszám: 25).

Az alábbi sémameghatározások szintaxisa az LDAP Version 3 RFC-ire épül.

Egy példa sémabejegyzés az alábbiakat tartalmazhatja:

```
objectclasses=( 1.3.6.1.4.1.1466.101.120.111
                NAME 'extensibleObject'
                SUP top AUXILIARY )

objectclasses=( 2.5.20.1
                NAME 'subschema'
                AUXILIARY MAY
```



```

        ( dITStructureRules
        $ nameForms
        $ ditContentRules
        $ objectClasses
        $ attributeTypes
        $ matchingRules
        $ matchingRuleUse ) )
objectclasses=( 2.5.6.1
    NAME 'alias'
    SUP top STRUCTURAL
    MUST aliasedObjectName )

attributeTypes=( 2.5.18.10
    NAME 'subschemaSubentry'
    EQUALITY distinguishedNameMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
    NO-USER-MODIFICATION
    SINGLE-VALUE USAGE directoryOperation )
attributeTypes=( 2.5.21.5 NAME 'attributeTypes'
    EQUALITY objectIdentifierFirstComponentMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.3
    USAGE directoryOperation )
attributeTypes=( 2.5.21.6 NAME 'objectClasses'
    EQUALITY objectIdentifierFirstComponentMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.37
    USAGE directoryOperation
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    USAGE directoryOperation )

ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.5 DESC 'Binary' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.7 DESC 'Boolean' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.12 DESC 'DN' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.15 DESC 'Directory String' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.24 DESC 'Generalized Time' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.26 DESC 'IA5 String' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.27 DESC 'INTEGER' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.50 DESC 'Telephone Number' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.53 DESC 'UTC Time' )




matchingRules=( 2.5.13.2 NAME 'caseIgnoreMatch'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
matchingRules=( 2.5.13.0 NAME 'objectIdentifierMatch'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
matchingRules=( 2.5.13.30 NAME 'objectIdentifierFirstComponentMatch'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
matchingRules=( 2.5.13.4 NAME 'caseIgnoreSubstringsMatch'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.58 )

```

A sémainformációk az ldap_modify API-hívás segítségével módosíthatók. További információkat a “Directory Server API-k” témakörben talál. A “cn=schema” DN használatával felvehet, törölhet és lecserélhet attribútumtípusokat és objektumosztályokat. További információk: “Dinamikus séma” oldalszám: 27 és “Séma kezelése” oldalszám: 157. Teljes leírást is megadhat. A sémabejegyzést felveheti vagy lecserélheti akár LDAP Version 3 meghatározás, akár IBM attribútum-kiterjesztés meghatározás használatával, vagy akár mindkettővel.

Általános séma támogatása

Az IBM Directory támogatja az alábbiak szerinti szabványos címtárséma használatát:

- Az Internet Engineering Task Force (IETF)  LDAP Version 3 RFC-kben, például az RFC 2252 és 2256 dokumentumok.
- A Directory Enabled Network (DEN) 
- A Desktop Management Task Force (DMTF) Common Information Model ajánlása (egységes információs modell, CIM) 

- A Network Application Consortium Lightweight Internet Person Schema (könnyűsúlyú internetes személyi séma, LIPS) ajánlása 

Ez az LDAP változat az alapértelmezett sémakonfigurációjában tartalmazza az LDAP Version 3 szabvány által megadott sémát. Tartalmazza továbbá a DEN sémameghatározásokat.

Az IBM biztosít egy sor kiterjesztett, általános sémameghatározást is, amelyeket más IBM termékek használnak, amikor az LDAP címtárhoz fordulnak. Ilyenek például:

- Objektumok telefonkönyv-alkalmazásokhoz: például `eperson`, `group` (csoport), `country` (ország), `organization` (szervezet), `organization unit` (szervezeti egység), `organization role` (szervezeti szerep), `locality` (hely), `state` (állam) stb.
- Objektumok más alrendszerhez, például fiókok, szolgáltatások és hozzáférési pontok, felhatalmazás, hitelesítés, biztonsági irányelvek és még sokminden más.

Objektumosztályok

Az objektumosztályok határozzák meg, hogy egy adott objektumtípust milyen attribútumok írják le. Ha például létrehozunk egy `tempEmployee` nevű objektumosztályt, az tartalmazhat olyan attribútumokat, amelyek az ideiglenes alkalmazottakra jellemzők, mint például `idNumber` (azonosító), `dateOfHire` (felvétel napja) vagy `assignmentLength` (megbízás időtartama). A címtár szabadon bővíthető egyedi objektumosztályokkal a szervezet igényeinek megfelelően. Az IBM Directory Server sémája bizonyos alapvető objektumosztály-típusokat maga is tartalmaz:

- Csoportok
- Helyek
- Szervezetek
- Emberek

Megjegyzés: A csak a Directory Server-re jellemző objektumosztály neve az `'ibm-'` előtaggal kezdődik.

Az objektumosztályokat a típus, az öröklődés és az attribútumok jellemzői határozzák meg.

Objektumosztály-típusok

Egy objektumosztály háromféle típusú lehet:

Strukturális:

Minden bejegyzésnek egy és csakis egy strukturális objektumosztályhoz kell tartoznia, amely meghatározza a bejegyzés alapvető tartalmát. Ez az objektumosztály egy valós világbeli objektumot reprezentál. Mivel minden bejegyzésnek tartoznia kell egy strukturális objektumosztályhoz, ez a leggyakoribb típusú objektumosztály.

Absztrakt:

Ez a típus más (strukturális) objektumosztályok szülőosztálya, vagy sablonja. Egy sor olyan attribútumot határoz meg, amelyek közősek strukturális objektumosztályok egy adott részalmazára. Ezek az objektumosztályok, amelyek az absztrakt osztály alosztályaiként vannak megadva, megöröklik annak megadott attribútumait. Az attribútumokat ezután nem kell még egyszer külön definiálni az alárendelt objektumosztályok mindegyikében.

Kiegészítő:

Ez a típus további attribútumokat tartalmaz, amelyek hozzáadhatók egy adott strukturális objektumosztályhoz tartozó bejegyzéshez. Bár egy bejegyzés csak egy strukturális objektumosztályhoz tartozhat, kiegészítő objektumosztályhoz akárhányhoz.

Objektumosztályok öröklődése

A Directory Server e változata támogatja az objektumosztályok és az attribútum-meghatározások objektum-öröklődését. Egy új objektumosztály megadható szülőosztályokkal (többszörös öröklődés), valamint a további, vagy módosított attribútumokkal.

Minden bejegyzés egyetlen strukturális objektumosztályhoz van rendelve. Minden objektumosztály az absztrakt, **top** nevű objektumosztályból öröklődik. Más objektumosztályokból is öröklődhetnek. Az objektumosztály-struktúra határozza meg egy adott bejegyzés kötelező és lehetséges attribútumainak listáját. Az objektumosztály-öröklődés függ az objektumosztály-meghatározások sorrendjétől. Egy objektumosztály csak az öt megelőző objektumosztályoktól öröklődhet. Egy személy bejegyzés objektumosztály-struktúrája például így adható meg az LDIF fájlban:

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
```

Ebben a struktúrában az `organizationalPerson` a `person` és a `top` objektumosztályokból öröklődik, míg a `person` objektumosztály csak a `top` objektumosztályból. Ez azt jelenti, hogy ha egy bejegyzéshez az `organizationalPerson` objektumosztályt rendeli, akkor az automatikusan megörökli a felsőbb szintű objektumosztályok (adott esetben tehát a `person` objektumosztály) kötelező és lehetséges attribútumait.

A sémafrissítési műveleteket a rendszer feldolgozás és véglegesítés előtt összeveti a sémaosztály-hierarchiával.

Attribútumok

Minden objektumosztály tartalmaz egy sor kötelező és elhagyható attribútumot. A kötelező attribútumok azok, amelyeknek feltétlenül szerepelniük kell az adott objektumosztályhoz rendelt bejegyzésekben. Az elhagyható attribútumoknak nem kell feltétlenül szerepelniük az adott objektumosztályhoz rendelt bejegyzésekben.

Attribútumok

Minden címtárbejegyzéshez tartozik egy sor attribútum, az objektumosztály meghatározása alapján. Az objektumosztály írja le, hogy milyen típusú információkat tartalmaz egy bejegyzés, az attribútumok pedig a tényleges adatokat tartalmazzák. Egy attribútumot egy vagy több név-érték pár ábrázol, amelyek meghatározott adatelemeket adnak meg, például nevet, címet vagy telefonszámot. A Directory Server az adatokat név-érték párokként jeleníti meg: egy leíró attribútumnévvel (például `commonName`, `cn`) és egy meghatározott információdarabbal (például Gipsz Jakab).

Gipsz Jakab bejegyzése több név-érték párt is tartalmazhat:

```
dn: uid=jgipsz, ou=people, ou=mycompany, c=us
objectClass: top
objectClass: person
objectClass: organizationalPerson
cn: John Doe
sn: Doe
givenName: János
givenName: Jakab
```

Bár a szabványos attribútumok már meg vannak adva a sémában, szabadon vehetők fel, módosíthatók, másolhatók át és törölhetők attribútumok a szervezet igényeinek megfelelően.

További információk:

- “Szokásos alséma-elemek”
- “Az `objectclass` attribútum” oldalszám: 20
- “Az `attributetypes` attribútum” oldalszám: 20
- “Az `IBMAttributeTypes` attribútum” oldalszám: 21
- “Megfeleltetési szabályok” oldalszám: 22
- “Indexelési szabályok” oldalszám: 24
- “Attribútum-szintaxis” oldalszám: 25

Szokásos alséma-elemek

Az alséma attribútumértékeinek megadására az alábbi elemek használatosak:

- `alpha = 'a' - 'z', 'A' - 'Z'`

- number = '0' - '9'
- anh = alpha / number / '-' / ','
- anhstring = 1 * anh
- keystack = alpha [anhstring]
- numericstring = 1 * number
- oid = descr / numericoid
- descr = keystack
- numericoid = numericstring * ("." numericstring)
- woid = whsp oid whsp ; oid-k halmaza valamelyik formátumban (numerikus OID-k vagy nevek)
- oids = woid / ("(" oidlist ")")
- oidlist = woid * ("\$" woid) ; objektumleírók, mint sémaelem-nevek
- qdescrs = qdescr / (whsp "(" qdesclist ")" whsp)
- qdesclist = [qdescr * (qdescr)]
- whsp "" descr "" whsp

Az objectclass attribútum

Az objectclasses attribútumlista sorolja fel a szerver által támogatott objektumosztályokat. Az attribútum minden egyes értéke egy külön objektumosztály-meghatározást ábrázol. Az objektumosztály-meghatározások a cn=schema objectclasses attribútumának megfelelő módosításaival vehetők fel, törölhetők és módosíthatók. Az objectclasses attribútum értékeinek az alábbi szintaxist kell követniük, az RFC 2252-ben meghatározott módon:

```
ObjectClassDescription = "(" whsp
    numericoid whsp ; Objectclass azonosító
    [ "NAME" qdescrs ]
    [ "DESC" qdstring ]
    [ "OBSOLETE" whsp ]
    [ "SUP" oids ] ; felsőbb objektumosztályok
    [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ] ; az alapértelmezés a structural
    [ "MUST" oid-k ] ; attribútumtípusok
    [ "MAY" oid-k ] ; attribútumtípusok
whsp ")"
```

A person objektumosztály meghatározása például az alábbi:

```
( 2.5.6.6 NAME 'person' DESC 'Jellemzően embereket ábrázoló bejegyzéseket határoz meg.'
STRUCTURAL SUP top MUST ( cn $ sn ) MAY ( userPassword $ telephoneNumber $ seeAlso $ description
))
```

- Az osztály OID-je 2.5.6.6
- A neve "person"
- Ez egy strukturális objektumosztály
- A "top" objektumosztálytól örököl
- A következő attribútumok kötelezők: cn, sn
- A következő attribútumok elhagyhatók: userPassword, telephoneNumber, seeAlso, description

További információ arról, hogyan módosíthatók a szerver által támogatott objektumosztályok: "Séma kezelése" oldalszám: 157.

Az attributetypes attribútum

Az attributetypes attribútum sorolja fel a szerver által támogatott attribútumokat. Az attribútum minden egyes értéke egy külön attribútum-meghatározást ábrázol. Az attribútum-meghatározások a cn=schema attributetypes attribútumának megfelelő módosításaival vehetők fel, törölhetők és módosíthatók. Az attributetypes attribútum értékeinek az alábbi szintaxist kell követniük, az RFC 2252-ben meghatározott módon:

```
AttributeTypeDescription = "(" whsp
    numericoid whsp ; attribútumtípus azonosító
    [ "NAME" qdescrs ] ; az attribútumtípus neve
    [ "DESC" qdstring ] ; leírás
    [ "OBSOLETE" whsp ]
    [ "SUP" woid ] ; ebből a másik attribútumtípusból származik
    [ "EQUALITY" woid ; Megfeleltetési szabály neve
    [ "ORDERING" woid ; Megfeleltetési szabály neve
    [ "SUBSTR" woid ] ; Megfeleltetési szabály neve
    [ "SYNTAX" whsp noidlen whsp ]
    [ "SINGLE-VALUE" whsp ] ; alapértelmezés: multi-valued (többértékű)
    [ "COLLECTIVE" whsp ] ; alapértelmezés: nem kollektív
    [ "NO-USER-MODIFICATION" whsp ] ; alapértelmezés: felhasználó módosíthatja
    [ "USAGE" whsp AttributeUsage ] ; alapértelmezés: userApplications
    whsp ")"
```

```
AttributeUsage =
    "userApplications" /
    "directoryOperation" /
    "distributedOperation" / ; DSA-megosztott
    "dSAOperation" ; DSA-specifikus, az érték a szervertől függ
```

A megfeleltetési szabályok és szintaxisértékek az alábbiak egyike által meghatározott értékek kell, hogy legyenek:

- “Megfeleltetési szabályok” oldalszám: 22
- “Attribútum-szintaxis” oldalszám: 25

A sémában csak az "userApplications" attribútumok módosíthatók. A "directoryOperation", "distributedOperation" és "dSAOperation" attribútumokat a szerver definiálta, és speciális jelentéssel bírnak a szerver működésére vonatkozóan.

A "description" attribútum például az alábbi meghatározással bír:

(2.5.4.13 NAME 'description' DESC 'A CIM és LDAP sémában egyaránt megtalálható attribútum, amely feladata, hogy hosszabb leírást biztosítson egy címtárobjektum-bejegyzésről.' EQUALITY caselgnoreMatch SUBSTR caselgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications)

- OID-je 2.5.4.13
- Neve: "description"
- Szintaxisa: 1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

További információ arról, hogyan módosíthatók a szerver által támogatott attribútumtípusok: “Séma kezelése” oldalszám: 157.

Az IBMAttributeTypes attribútum

Az IBMAttributeTypes attribútum használható az LDAP Version 3 szabvány által nem szabályozott attribútumok sémainformációinak megadásához. Az IBMAttributeTypes értékek az alábbi szintaxist kell, hogy kövessék:

```
IBMAttributeTypesDescription = "(" whsp
    numericoid whsp
    [ "DBNAME" qdescrs ] ; legfeljebb 2 név (tábla, oszlop)
    [ "ACCESS-CLASS" whsp IBMAccessClass whsp ]
    [ "LENGTH" wlen whsp ] ; az attribútum maximális hossza
    [ "EQUALITY" [ IBMwlen ] whsp ] ; index létrehozása a megfeleltetési szabályhoz
    [ "ORDERING" [ IBMwlen ] whsp ] ; index létrehozása a megfeleltetési szabályhoz
    [ "APPROX" [ IBMwlen ] whsp ] ; index létrehozása a megfeleltetési szabályhoz
    [ "SUBSTR" [ IBMwlen ] whsp ] ; index létrehozása a megfeleltetési szabályhoz
    [ "REVERSE" [ IBMwlen ] whsp ] ; fordított index a rész-karakter sorozathoz
    whsp ")"
```

```
IBMAccessClass =
    "NORMAL" / ; ez az alapértelmezés
    "SENSITIVE" /
    "CRITICAL" /
    "RESTRICTED" /
```

```
"SYSTEM"      /  
"OBJECT"
```

IBMwlen = whsp len

Numericoid

Az IBMAttributeTypes értékének és az attributetypes értékének összeegyeztetésére szolgál.

DBNAME

Legfeljebb 2 nevet adhat meg, már ha egyáltalán kettőt megad. Az első az attribútumhoz használt tábla neve. A második az attribútum teljesen normalizált értékéhez használt oszlopnév a táblában. Ha csak egy nevet ad meg, azt használja a rendszer tábla- és oszlopnévnek egyaránt. Ha nem ad meg egy DBNAME értéket sem, akkor az attribútumnév első tizenhét karaktere alapján kerül kialakításra egy név (amelynek egyedinek kell lennie). Az adatbázistáblák és -oszlopok nevei legfeljebb tizenhét karakteresek lehetnek.

ACCESS-CLASS

Az attribútum hozzáférési besorolása. Ha az ACCESS-CLASS ki van hagyva, akkor alapértelmezés szerint értéke normal (szokásos).

LENGTH

Az attribútum maximális hossza. A hossz byte-ok számában van megadva. A Directory Server lehetővé teszi egy attribútum hosszának megadását. Az attributetypes értékben az:

```
( attr-oid ...  
SYNTAX syntax-oid{len} ... )
```

attribútum használható annak jelzésére, hogy az attr-oid OID-jű attribútumtípusnak van maximális hossza.

EQUALITY, ORDERING, APPROX, SUBSTR, REVERSE

Ha ezen attribútumok bármelyike használatra kerül, index készül a megfelelő megfeleltetési szabályhoz. Az elhagyható hossz paraméter adja meg az indexelt oszlop szélességét. Egy indexet használ a rendszer több megfeleltetési szabály megvalósítására is. Ha nem ad meg hosszt, a Directory Server 500-at feltételez. A szerver használhat a felhasználó által kértnél rövidebb hosszt is, ha annak van értelme. Ha például az index hossza meghaladja az attribútum hosszát, akkor az indexhossz figyelmen kívül marad.

Megfeleltetési szabályok

A megfeleltetési szabályok határozzák meg, hogyan történjen a karaktersorozatok összehasonlítása a keresési műveletek közben. A szabályok három kategóriába esnek:

- Egyenlőség
- Sorrendezés
- Rész-karaktersorozat

| A címtárszerver a bináris kivételével mindenféle szintaxishoz engedi egyenlőségi illesztések megadását. Bináris
| szintaxissal megadott attribútumok esetén a szerver csak létezésvizsgálatot támogat (például "(jpegphoto=*)"). Az IA5
| String és Directory String szintaxisok esetén az attribútumok meghatározása sokkal kifinomultabb lehet, például a kis-
| és nagybetűk különbségei figyelhetők vagy figyelmen kívül hagyhatók. A cn attribútum például a caseIgnoreMatch
| illesztési szabályt használja, vagyis a "Kiss Elek" és "kiss elek" értékek egyenlőnek számítanak. A kis- és nagybetűk
| különbségeit figyelmen kívül hagyó illesztési szabályok esetén az összehasonlítás az értékek nagybetűssé átalakítása
| után történik meg. A nagybetűssé alakító algoritmus nem figyeli a területi beállításokat, és lehet, hogy nem is minden
| területi beállítás esetén működik helyesen.

| A címtárszerver Directory String, IA5 String, és Distinguished name (megkülönböztetett név) szintaxisú attribútumok
| esetén támogatja a rész-karaktersorozatok illesztését. A rész-karaktersorozatok egyezésének keresési szűrői a "*"
| karaktert használják egy karaktersorozat nulla vagy több karakterének illesztéséhez. A "(cn=*smith)" keresési szűrő
| például minden értéket megtalál, amely a "smith" karaktersorozatra végződik.

| Integer (egész), Directory String (címtár-karaktersorozat), IA5 String és Distinguished name (megkülönböztetett név)
| szintaxisú attribútumok esetén támogatott a találatok sorbarendezése. Karaktersorozat típusú szintaxisok esetén a
| sorbarendezés az UTF-8 karakterértékek byte-jainak egyszerű sorbarendezésén alapszik. Ha az attribútum a kis- és

l nagybetűket figyelmen kívül hagyó szabállyal lett megadva, akkor a sorbarendezés a nagybetűre konvertált értékek
l alapján történik. Amint korábban már írtuk, a nagybetűssé alakító algoritmus lehet, hogy nem minden területi beállítás
l esetén működik helyesen.

l Az IBM Directory Serverben a rész-karakter sorozat és a rendezésillesztés viselkedését az illesztési szabály határozza
l meg impliciten: a rész-karakter sorozat illesztést támogató szintaxisokban van egy beleértett rész-karakter sorozat
l illesztési szabály is, a rendezésillesztést támogató szintaxisokban pedig egy beleértett rendezésillesztési szabály. A kis-
l és nagybetűk különbségét figyelmen kívül hagyó illesztési szabállyal megadott attribútumok esetén a beleértett
l rész-karakter sorozat és rendezésillesztési szabályok is figyelmen kívül hagyják a kis- és nagybetűk különbségét.

Egyenlőséget meghatározó szabályok		
Megfeleltetési szabály	OID	Szintaxis
caseExactIA5Match	1.3.6.1.4.1.1466.109.114.1	Directory String szintaxis
caseExactMatch	2.5.13.5 IA5	String szintaxis
caseIgnoreIA5Match	1.3.6.1.4.1.1466.109.114.2	IA5 String szintaxis
caseIgnoreMatch	2.5.13.2	Directory String szintaxis
distinguishedNameMatch	2.5.13.1	DN - megkülönböztetett név
generalizedTimeMatch	2.5.13.27	Generalized Time szintaxis
ibm-entryUuidMatch	1.3.18.0.2.22.2	Directory String szintaxis
integerFirstComponentMatch	2.5.13.29	Integer szintaxis - egész szám
integerMatch	2.5.13.14	Integer szintaxis - egész szám
objectIdentifierFirstComponentMatch	2.5.13.30	OID-ket tartalmazó String. Az OID egy számokból (0-9) és pontokból (.) álló karakter sorozat.
objectIdentifierMatch	2.5.13.0	OID-ket tartalmazó String. Az OID egy számokból (0-9) és pontokból (.) álló karakter sorozat
octetStringMatch	2.5.13.17	Directory String szintaxis
telephoneNumberMatch	2.5.13.20	Telephone Number szintaxis
uTCTimeMatch	2.5.13.25	UTC Time szintaxis

Sorbarendezést meghatározó szabályok		
Megfeleltetési szabály	OID	Szintaxis
caseExactOrderingMatch	2.5.13.6	Directory String szintaxis
caseIgnoreOrderingMatch	2.5.13.3	Directory String szintaxis
distinguishedNameOrderingMatch	1.3.18.0.2.4.405	DN - megkülönböztetett név
generalizedTimeOrderingMatch	2.5.13.28	Generalized Time szintaxis

Rész-karakter sorozatok keresését meghatározó szabályok		
Megfeleltetési szabály	OID	Szintaxis
caseExactSubstringsMatch	2.5.13.7	Directory String szintaxis
caseIgnoreSubstringsMatch	2.5.13.4	Directory String szintaxis
telephoneNumberSubstringsMatch	2.5.13.21	Telephone Number szintaxis

Megjegyzés: Az UTC-Time az ASN.1 szabvány szerinti formátumú idő. Lásd még ISO 8601 és X680. Ez a szintaxis UTC-Time formátumú időértékek tárolására használható. Lásd még: "Generalized time és UTC time" oldalszám: 33.

Indexelési szabályok

Az attribútumokhoz rendelt indexelési szabályok segítségével lehetséges az információkat gyorsabban kinyerni. Ha csak egy attribútum kerül megadásra, nem készül index. A Directory Server az alábbi típusú indexelési szabályokat biztosítja:

- Egyenlőség
- Sorrendezés
- Közelítés
- Rész-karaktorsorozat
- Fordított

Indexelési szabályok specifikációi az egyes attribútumhoz: Indexelési szabályt megadva egy attribútumhoz szabályozható az attribútumértékek alapján készített speciális indexek létrehozása és karbantartása. Ez nagymértékben javítja az ezekre az attribútumokra szűrő keresések válaszüdejét. Az indexelési szabályok ötféle lehetséges típusa a keresési szűrőn végzett műveletekkel kapcsolatosak.

Egyenlőség

A következő keresési műveletekre vonatkozik:

- equalityMatch '='

Például:

```
"cn = John Doe"
```

Sorrendezés

A következő keresési műveletekre vonatkozik:

- greaterOrEqual '>='
- lessOrEqual '<='

Például:

```
"sn >= Doe"
```

Közelítés

A következő keresési műveletekre vonatkozik:

- approxMatch '~='

Például:

```
"sn ~= doe"
```

Rész-karaktorsorozat

A substring (rész-karaktorsorozat) szintaxist használó keresési műveletekre vonatkozik:

- substring '*'

Például:

```
"sn = McC*"
"cn = J*Doe"
```

Fordított

A következő keresési műveletekre vonatkozik:

- '*' substring

Például:

```
"sn = *baugh"
```

Célszerű legalább egyenlőségi index készítését megadni a keresési szűrőkben használt attribútumokra.

Attribútum-szintaxis

Az attribútum-szintaxis határozza meg egy attribútum lehetséges értékeit. A szerver az attribútum szintaxis-meghatározása alapján érvényesíti az adatokat és határozza meg az értékek megfeleltetését. Egy "Boolean" típusú attribútum például csak a "TRUE" és "FALSE" értékeket veheti fel.

Az attribútum lehetnek egy- és többértékűek. A többértékű attribútumok nincsenek sorba rendezve, tehát egy alkalmazás nem számíthat arra, hogy egy adott attribútum értékei bármilyen sorrendben érkezzenek vissza. Ha rendezett értékhalmozra van szükség, akkor érdemes lehet egyértékű attribútumokba tenni az értékek listáját:

```
kedvencek: elsokedvenc  
masodikkedvenc harmadikkedvenc
```

Vagy érdemes lehet sorrendiséget jelölő információkat tárolni az értéken belül:

```
kedvencek: 2 yyy  
kedvencek: 1 xxx  
kedvencek: 3 zzz
```

A többértékű attribútumok akkor hasznosak, ha a bejegyzés több néven is ismert. A cn (közönséges név) attribútum például többértékű. Egy bejegyzés megadható így:

```
dn: cn=Beke Antal,o=Retroimpex,c=HU  
objectclass: inetorgperson  
sn: Beke  
cn: Beke Antal  
cn: Beke Anti  
cn: Beke Tóni
```

Ennek eredményeképpen a Beke Antal és Beke Tóni nevekre vonatkozó keresések ugyanazokat az információkat adják vissza.

A bináris attribútumok tetszés szerinti byte-sorozatot tartalmazhatnak, akár egy JPEG formátumú képet is. Ezek nem használhatók bejegyzések keresésére.

A logikai (boolean) attribútumok a TRUE vagy FALSE értékeket vehetik fel.

A DN attribútumok LDAP megkülönböztetett neveket tartalmaznak. Az értékeknek nem kell feltétlenül létező bejegyzések DN-jeinek lenniük, de érvényes DN szintaxis szerint kell, hogy formálva legyenek.

A Directory String (címtár-karaktorsorozat) attribútumok UTF-8 kódú karaktereket tartalmazó szöveges karaktorsorozatokat tartalmaznak. A attribútumban a keresésekre vonatkozóan megadható (az attribútum megfeleltetési szabályában), hogy számítsanak-e külön a kis- és nagybetűk; mindazonáltal az érték eredeti, beírt formájában kerül visszaadásra.

A Generalized Time (általános időformátumú) attribútumok egy 2000-álló dátum és idő karakteres ábrázolását tartalmazzák, GMT idők és opcionális GMT időzóna-eltolások használatával. Az értékek szintaxisáról további részletek: "Generalized time és UTC time" oldalszám: 33.

Az IA5 String attribútumok IA5 kódolású (7 bites US ASCII) karaktorsorozatokat tartalmaznak. A attribútumban a keresésekre vonatkozóan megadható (az attribútum megfeleltetési szabályában), hogy számítsanak-e külön a kis- és nagybetűk; mindazonáltal az érték eredeti, beírt formájában kerül visszaadásra. Az IA5 String formátum lehetővé teszi helyettesítő karakterek megadását rész-karaktorsorozatok keresésekor.

Az Integer (egész) attribútumok az érték szöveges ábrázolását tartalmazzák. Ilyen például a 0 vagy 1000. Az Egész szintaxisú attribútumok a -2147483648 - 2147483647 tartományba kell, hogy essenek.

A Telephone Number (telefonszám) attribútumok egy telefonszám szöveges ábrázolását tartalmazzák. A Directory Server nem követeli meg semmilyen meghatározott szintaxis használatát ezekben az értékekben. Az alábbiak mind érvényes telefonszámok: (555)555-5555, 555.555.5555 és +1 43 555 555 5555.

Az UTC Time (UTC idő) attribútumok egy korábbi, nem 2000-álló, szöveges dátum- és időformátumot használnak. További részletek: “Generalized time és UTC time” oldalszám: 33.

A címtársémában egy attribútum szintaxisát az egyes szintaxisokhoz rendelt objektumazonosítókkal (OID) lehet megadni. A következő táblázat felsorolja a címtárszerver és az OID-k által támogatott szintaxisokat.

Szintaxis	OID
Attribute Type Description (attribútumtípus-leírás) szintaxis	1.3.6.1.4.1.1466.115.121.1.3
Binary - byte-sorozat	1.3.6.1.4.1.1466.115.121.1.5
Boolean - TRUE/FALSE	1.3.6.1.4.1.1466.115.121.1.7
Directory String szintaxis	1.3.6.1.4.1.1466.115.121.1.15
DIT Content Rule Description (tartalomszabály-leírás) szintaxis	1.3.6.1.4.1.1466.115.121.1.16
DIT Structure Rule Description (struktúraszabály-leírás) szintaxis	1.3.6.1.4.1.1466.115.121.1.17
DN - megkülönböztetett név	1.3.6.1.4.1.1466.115.121.1.12
Generalized Time szintaxis	1.3.6.1.4.1.1466.115.121.1.24
IA5 String szintaxis	1.3.6.1.4.1.1466.115.121.1.26
IBM Attribute Type Description (attribútumtípus-leírás)	1.3.18.0.2.8.1
Integer szintaxis - egész szám	1.3.6.1.4.1.1466.115.121.1.27
LDAP Syntax Description (szintaxisleírás) szintaxis	1.3.6.1.4.1.1466.115.121.1.54
Matching Rule Description (megfeleltetésiszabály-leírás)	1.3.6.1.4.1.1466.115.121.1.30
Matching Rule Use Description (megfeleltetésiszabály-használat leírás)	1.3.6.1.4.1.1466.115.121.1.31
Name Form Description (névformátum leírás)	1.3.6.1.4.1.1466.115.121.1.35
Object Class Description (objektumosztály-leírás) szintaxis	1.3.6.1.4.1.1466.115.121.1.37
OID-ket tartalmazó String. Az OID egy számközből (0-9) és pontokból (.) álló karaktersorozat. Lásd még: “Objektumazonosító (OID)”.	1.3.6.1.4.1.1466.115.121.1.38
Telephone Number szintaxis	1.3.6.1.4.1.1466.115.121.1.50
UTC Time szintaxis. Az UTC-Time az ASN.1 szabvány szerinti formátumú idő. Lásd még ISO 8601 és X680. Ez a szintaxis UTC-Time formátumú időértékek tárolására használható. Lásd még: “Generalized time és UTC time” oldalszám: 33.	1.3.6.1.4.1.1466.115.121.1.53

Objektumazonosító (OID)


Az objektumazonosító (OID) egy decimális számokból álló karaktersorozat, amely egyedi módon azonosít egy objektumot. Ezek az objektumok általában vagy egy objektumosztály, vagy egy attribútum.


Ha nincs még OID, akkor megadható úgy is, hogy az objektumosztály vagy attribútum nevéhez az **-oid** betűket fűzi. Ha például létrehozott egy tempID nevű attribútumot, annak az OID-je lehet **tempID-oid**.


Kritikus fontosságú, hogy a saját OID-ket jogos forrásokból szerezze be. Jogos OID-k beszerzésére két fő stratégia létezik:

- Jegyeztesse be az objektumokat egy hatósággal. Ez a stratégia akkor kényelmes, ha csak kevés OID-t kell használni.
- Igényeljen egy ívet (ívnek hívják az OID fa egy egyéni részfáját) egy hatóságtól és azon belül maga bocsáthatja ki az OID-ket. Ez a stratégia akkor hasznos, ha sok OID-re van szükség, vagy az OID-hozzárendelések nem tartósak.

Az Amerikai Nemzeti Szabványügyi Hivatal (ANSI) a Nemzetközi Szabványosítási Szervezet (ISO) és a Nemzetközi Telekommunikációs Unió (ITU) által kialakított regisztrációs folyamat keretében az Egyesült Államokon belül kibocsátott szervezeti nevekért felelős regisztrációs hatóság. A szervezeti nevek bejegyzésével kapcsolatos további

információk az ANSI webhelyén  (www.ansi.org) található. Az ANSI OID íve szervezetek számára a 2.16.840.1. Az ANSI egy számot (NEWNUM) ad ki, amellyel létrehoz egy új OID ívet: 2.16.840.1.NEWNUM.

A legtöbb országban és régióban a helyi szabványhatóság látja el az OID regisztráció feladatát. Csakúgy, mint az ANSI ív esetében, itt is általában az OID 2.16 alatti ívekről van szó. Némi utánjárást igényelhet egy adott ország vagy régió OID hatóságának fellelése. Az ország vagy régió helyi szabványszervezete valószínűleg ISO-tag. Az ISO-tagok nevei és elérhetőségei az ISO webhelyén  (www.iso.ch) található.

Az Internet Assigned Numbers Authority (IANA) nevű szervezet bocsát ki magántulajdonú vállalati számokat, amelyek az 1.3.6.1.4.1 íven belüli OID-k. Az IANA kiad egy új számot (NEWNUM), vagyis az új OID ív az 1.3.6.1.4.1.NEWNUM lesz. Ezek a számok az IANA webhelyén  (www.iana.org) igényelhetők.

Ha a szervezet kapott egy OID-t, akkor hozzáláthat a saját OID-k készítéséhez, az OID végéhez fűzve további számokat. Tegyük fel például, hogy a cég megkapta a (képzelt) 1.1.1 OID-t. Más szervezet már nem kaphat olyan OID-t, amelyik az "1.1.1" számokkal kezdődik. Az LDAP számára létrehozható egy tartomány az ".1" tag hozzáadásával, az eredmény az 1.1.1.1. Később ez a tartomány még tovább osztható, például kaphatnak egy tartományt az objektumosztályok (1.1.1.1.1), az attribútumtípusok (1.1.1.1.2) és így tovább, és mondjuk az 1.1.1.1.2.34 OID-t kaphatja a "foo" attribútum.

Alséma-bejegyzések

Szerverenként egy alséma-bejegyzés található. A címtár összes bejegyzésének kell, hogy legyen egy implicit subschemaSubentry attribútumtípusa. A subschemaSubentry attribútumtípus értéke a bejegyzésnek megfelelő alséma-bejegyzés DN-je. Egy adott szerver összes bejegyzésének osztoznia kell ugyanazon alséma-bejegyzésen, és subschemaSubentry attribútumtípusuk értéke is meg kell, hogy egyezzen. Az alséma-bejegyzés DN-je gyárilag beállított módon 'cn=schema'.

Az alséma-bejegyzés a 'top', a 'subschema' és az 'IBMsubschema' objektumosztályokhoz tartozik. Az 'IBMsubschema' objektumosztálynak nincs MUST (kötelező) attribútuma és csak egy MAY attribútumtípusa van ('IBMattributeTypes').

Az IBMsubschema objektumosztály

Az IBMsubschema objektumosztályt csak az alséma-bejegyzés használja, az alábbi módon:

```
( 1.3.18.0.2.6.174
NAME 'ibmSubSchema'
DESC 'IBM-specifikus objektumosztály, amely egy adott címtárszerver összes
attribútumát és objektumosztályát tárolja.' SUP 'subschema'
STRUCTURAL MAY ( IBMAttributeTypes ) )
```

Sémalekérdezések

Az alséma-bejegyzés lekérdezésére az ldap_search() API-hívás használható, amint az alábbi példa is mutatja:

```
DN          : "cn=schema"
search scope : base
filter      : objectclass=subschema vagy objectclass=*
```

Ez a példa a teljes sémát lekéri. Adott attribútumtípusok összes értékének lekéréséhez használja az ldap_search attrs paraméterét. Nem lehet lekérni csak egy adott attribútumtípus csak egy adott értékét.

Az ldap_search API-hívással kapcsolatos további információkat a "Directory Server API-k" témakörben talál.

Dinamikus séma

Dinamikus sémamódosítás elvégzéséhez az ldap_modify API-hívást kell használnia "cn=schema" DN-nel. Egyszerre csak egy sémaelem (például attribútumtípus vagy objektumosztály) vehető fel, törölhető vagy cserélhető le.

Egy sémabejegyzés törléséhez adja meg azt a sémaattribútumot, amelyik meghatározza a sémabejegyzést (objectclasses vagy attributetypes), majd az értékét, az OID-t, zárójelben. Például az <attr-oid> OID-jú attribútum törlése:

```
dn: cn=schema
changetype: modify
delete: attributetypes
attributetypes: ( <attr-oid> )
```

Teljes leírást is megadhat. Akárhogy is legyen, a törlendő sémaelem kikereséséhez használt megfeleltetési szabály az objectIdentifierFirstComponentMatch.

Egy sémaelem felvételéhez vagy cseréjéhez **KÖTELEZŐ** megadni LDAP Version 3 meghatározást és **LEHETSÉGES** megadni az IBM meghatározást. Mindkét esetben a sémaelemnek csak azt a részét kell megadni, amelyik módosításra kerül.

Például a 'cn' attribútumtípus (OID-je 2.5.4.3) törléséhez használja az ldap_modify() hívást:

```
LDAPMod attr;
LDAPMod *attrs[] = { &attr, NULL };
char *vals[] = { "( 2.5.4.3 )", NULL };
attr.mod_op = LDAP_MOD_DELETE;
attr.mod_type = "attributeTypes";
attr.mod_values = vals;
ldap_modify_s(ldap_session_handle, "cn=schema", attrs);
```

Egy új típusor felvételéhez, ha az OID 20.20.20, a "name" attribútumtól örököl és a hossza 20 karakter:

```
char *vals1[] = { "( 20.20.20 NAME 'bar' SUP name )" NULL };
char *vals2[] = { "( 20.20.20 LENGTH 20 )", NULL };
LDAPMod attr1;
LDAPMod attr2;
LDAPMod *attrs[] = { &attr1, &attr2, NULL };
attr1.mod_op = LDAP_MOD_ADD;
attr1.mod_type = "attributeTypes";
attr1.mod_values = vals1;
attr2.mod_op = LDAP_MOD_ADD;
attr2.mod_type = "IBMattributeTypes";
attr2.mod_values = vals2;
ldap_modify_s(ldap_session_handle, "cn=schema", attrs);
```

A fentiek LDIF verziója:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( 20.20.20 NAME 'bar' SUP name )
-
add: ibmattributetypes
ibmattributetypes: (20.20.20 LENGTH 20)
```

Hozáférés-felügyelet

A dinamikus sémamódosításokat csak egy replikáció-biztosító vagy az adminisztrátor DN végezheti el.

Replikáció

Dinamikus sémamódosítás esetén a változások replikálódnak.

Nem engedélyezett sémamódosítások

Nem minden sémamódosítás megengedett. A módosítások korlátozásai:

- Csak úgy módosítható a séma, hogy összefüggő állapotban maradjon.

- Olyan attribútum, amelyik másik attribútum szülő típusa, nem törölhető. Egy objektumosztály "MAY" vagy "MUST" attribútum típusa szintén nem törölhető.
- Egy olyan objektumosztály, amelyik egy másik osztály szülője, nem törölhető.
- Nem létező elemekre (például szintaxisokra vagy objektumosztályokra) hivatkozó attribútum típusok és objektumosztályok nem vehetők fel.
- Nem módosíthatók úgy attribútum típusok és objektumosztályok, hogy nem létező elemekre (például szintaxisokra vagy objektumosztályokra) hivatkozzanak.
- Az új attribútumok IBMAttributeType meghatározásaikban nem használhatják a meglévő adatbázistáblákat.
- A meglévő címtárbejegyzésekben használt attribútumok nem törölhetők.
- Az attribútumok hossza és szintaxisa nem módosítható.
- Az attribútumokhoz rendelt adatbázistábla vagy -oszlop nem módosítható.
- A meglévő objektumosztályok meghatározásánál használt attribútumok nem törölhetők.
- A meglévő címtárbejegyzésekben használt objektumosztályok nem törölhetők.

A sémának a szerver állapotát befolyásoló módosításai nem engedélyezettek. A címtárszerver megköveteli az alábbi sémameghatározások meglétét. Ezek nem változtathatók meg.

Objektumosztályok:

- accessGroup
- accessRole
- alias
- os400-usrprf
- referral
- replicaObject
- top

Attribútumok:

- aclEntry
- aclPropagate
- aclSource
- aliasedObjectName, aliasedentryName
- businessCategory
- cn, commonName
- createTimeStamp
- creatorsName
- description
- dn, distinguishedName
- entryOwner
- hasSubordinates
- ibm-entryChecksum
- ibm-entryChecksumOp
- ibm-entryUuid
- member
- modifiersName
- modifyTimeStamp
- name
- o, organizationName, organization
- objectClass

- os400-acgcde
- os400-astlvl
- os400-atnpgm
- os400-audlvl
- os400-aut
- os400-ccsid
- os400-chridctl
- os400-cntryid
- os400-curlib
- os400-dlvry
- os400-docpwd
- os400-dspsgninf
- os400-eimassoc
- os400-gid
- os400-groupmember
- os400-grpaut
- os400-grpauttyp
- os400-grpprf
- os400-homedir
- os400-IaspStorageInformation
- os400-inlmnu
- os400-inlpgm
- os400-invalidSignonCount
- os400-jobd
- os400-kbdbuf
- os400-langid
- os400-lclpwdmgt
- os400-lmtcpb
- os400-lmtdevssn
- os400-locale
- os400-maxstg
- os400-msgq
- os400-objaud
- os400-outq
- os400-owner
- os400-password
- os400-passwordExpirationDate
- os400-passwordLastChanged
- os400-previousSignon
- os400-profile
- os400-prtdev
- os400-ptylmt
- os400-pwdexp
- os400-pwdexpitv
- os400-setjobatr

- os400-sev
- os400-spcaut
- os400-spcenv
- os400-srtseq
- os400-status
- os400-storageUsed
- os400-storageUsedOnIasp
- os400-supgrprpf
- os400-sys os400-text
- os400-uid
- os400-usrcls
- os400-usropt
- ou, organizationalUnit, organizationalUnitName
- owner
- ownerPropagate
- ownerSource
- ref
- replicaBindDN
- replicaBindMethod
- replicaCredentials, replicaBindCredentials
- replicaHost
- replicaPort
- replicaUpdateTimeInterval
- replicaUseSSL
- seeAlso

Szintaxisok:

Mind

Megfeleltetési szabályok:

Mind

Sémaellenőrzés

A szerver inicializálásakor a sémafájlokat beolvassa és ellenőrzi, hogy következetesek és helyesek-e. Ha az ellenőrzések sikertelenek, akkor az inicializálás megghiúsul és a szerver hibüzenetet ad. A rendszer minden dinamikus sémamódosítás esetén ellenőrzi, hogy az eredményül kapott séma következetes és helyes-e. Ha az ellenőrzések sikertelenek, akkor hibajelzés történik és a módosítás megghiúsul. Bizonyos ellenőrzések a nyelvtan rész (egy attribútumtípusnak például legfeljebb egy szülőtípusa lehet, egy objektumosztálynak viszont akárhány szülőosztálya).

Attribútumtípusokkal kapcsolatban a rendszer az alábbi ellenőrzéseket végzi:

- Két különböző attribútumtípusnak nem lehet ugyanaz a neve vagy OID-je.
- Az attribútumtípusok öröklődési hierarchiájában nem lehet ciklus.
- Egy attribútum szülőtípusának szintén léteznie kell, bár maga a meghatározás megjelenhet később, vagy akár külön fájlban is.
- Ha egy attribútumtípus egy másik altípusa, akkor mindkettőhöz ugyanaz a USAGE (használati mód) tartozik.
- Minden attribútumtípus szintaxisát vagy meg kell meghatározni, vagy örököltetni kell.
- NO-USER-MODIFICATION tulajdonság csak a működéssel kapcsolatos attribútumokhoz adható meg.

Az objektumosztályokkal kapcsolatban a rendszer az alábbi ellenőrzéseket végzi:

- Két különböző objektumosztálynak nem lehet ugyanaz a neve vagy OID-je.
- Az objektumosztályok öröklődési hierarchiájában nem lehet ciklus.
- Egy objektumosztály szülőosztályának szintén léteznie kell, bár maga a meghatározás megjelenhet később, vagy akár külön fájlban is.
- Egy objektumosztály "MUST" és "MAY" attribútumtípusait szintén meg kell adni, bár maga a meghatározás megjelenhet később, vagy akár külön fájlban is.
- Minden strukturális objektumosztály közvetve vagy közvetlenül a top objektumosztály leszármazottja.
- Ha egy absztrakt osztálynak van szülőosztálya, akkor a szülőosztályoknak szintén absztraktnak kell lenniük.

Bejegyzés ellenőrzése a séma alapján

Amikor egy bejegyzés felvételre vagy módosításra kerül egy LDAP művelettel, a bejegyzést a rendszer ellenőrzi a séma alapján. Alapértelmezés szerint az itt felsorolt összes ellenőrzés végrehajtásra kerül. Igény szerint azonban letilthető a sémaellenőrzés egy része a sémaellenőrzési szint módosításával. Ehhez az iSeries navigátorban módosítani kell a Directory Server tulajdonságai között az **Adatbázis/utótagok** oldalon a **Sémaellenőrzés** mező értékét. A sémakonfigurációs attribútumokkal kapcsolatos további információk: "Directory Server konfigurációs séma" oldalszám: 223.

A sémának való megfelelést a rendszer az alábbi szempontok szerint végzi:

Objektumosztályokra vonatkozóan:

- Léteznie kell legalább egy "objectClass" attribútumtípus-értéknek.
- Kiegészítő objektumosztály akárhány lehet, nulla is. Ez nem ellenőrzés, csak pontosítás. Kikapcsolni sem lehet.
- Akárhány absztrakt objektumosztály szerepelhet, de csak osztályöröklődés eredményeképp. Ez azt jelenti, hogy a bejegyzés minden absztrakt objektumosztályához léteznie kell egy strukturális vagy absztrakt objektumosztálynak, amely örököl közvetve vagy közvetlenül az adott absztrakt objektumosztálytól.
- Legalább egy strukturális objektumosztálynak léteznie kell.
- Pontosan egy azonnali vagy alap strukturális objektumosztálynak kell léteznie. Ez azt jelenti, hogy a bejegyzésben megadott összes strukturális objektumosztály pontosan egynek kell, hogy szülőosztálya legyen. A "legjobban leszármazott" objektumosztályt hívjuk a bejegyzés "azonnali" vagy "alap strukturális" objektumosztályának.
- Nem módosítható az azonnali strukturális objektumosztály (ldap_modify hívással).
- A bejegyzés minden egyes objektumosztályára vonatkozóan kiszámításra kerül az közvetett és közvetlen szülőosztályok halmaza; ha e szülőosztályok bármelyike nincs megadva a bejegyzésnél, akkor automatikusan felvételre kerül.
- Ha a sémaellenőrzési szint **Version 3 (szigorú)**, akkor az összes strukturális szülőosztályt meg kell adni. Ha például egy inetorgperson objektumosztályú bejegyzést kíván létrehozni, akkor meg kell adni a person, organizationalperson és inetorgperson objektumosztályokat.

A bejegyzés attribútumtípusainak érvényessége az alábbi módon kerül ellenőrzésre:

- A bejegyzés MUST attribútumtípusainak halmaza az összes objektumosztályának MUST attribútumtípusaiból képzett halmazok uniójaként kerül kiszámítva (beleértve a közvetve örökölt objektumosztályokat is). Ha a bejegyzés MUST attribútumtípusainak halmaza nem részhalmaza a bejegyzésben megadott attribútumtípusok halmazának, akkor a bejegyzés visszautasításra kerül.
- A bejegyzés MAY attribútumtípusainak halmaza az összes objektumosztályának MAY attribútumtípusaiból képzett halmazok uniójaként kerül kiszámítva (beleértve a közvetve örökölt objektumosztályokat is). Ha a bejegyzés attribútumtípusainak halmaza nem részhalmaza a bejegyzés MUST és MAY attribútumtípusaiból képzett halmazok uniójának, akkor a bejegyzés visszautasításra kerül.
- Ha a bejegyzéshez megadott attribútumtípusok bármelyike NO-USER-MODIFICATION tulajdonságúként van megjelölve, akkor a bejegyzés visszautasításra kerül.

A bejegyzés attribútumtípus-értékeinek érvényessége az alábbi módon kerül ellenőrzésre:

- A bejegyzés minden egyes attribútumtípusára vonatkozóan, ha az attribútumtípus egyértékű és egynél több érték van megadva, akkor a bejegyzés visszautasításra kerül.
- A bejegyzés minden egyes attribútumtípusának minden egyes attribútumértékére vonatkozóan, ha a szintaxisa nem felel meg az adott attribútum szintaxis-ellenőrzési eljárásának, akkor a bejegyzés visszautasításra kerül.
- A bejegyzés minden egyes attribútumtípusának minden egyes attribútumértékére vonatkozóan, ha a hossza nagyobb, mint az adott attribútumhoz rendelt maximális hossz, akkor a bejegyzés visszautasításra kerül.

A DN érvényességének ellenőrzési módja:

- A szintaxisnak meg kell felelnie a DistinguishedName-ek BNF szabályainak. Ha nem felel meg, akkor a bejegyzés visszautasításra kerül.
- A rendszer ellenőrzi, hogy az RDN csak a bejegyzésben érvényes attribútumtípusokból épül fel.
- A rendszer ellenőrzi, hogy az RDN-ben használt attribútumtípusok értékei megtalálhatók-e a bejegyzésben.

iPlanet-kompatibilitás

A Directory Server elemzője lehetővé teszi a séma attribútumtípusainak (objectClass és attributeType) megadását iPlanet szintaxis szerint. A descr és numeric-oid értékek megadhatók aposztrófokkal határolva (mintha qdescr értékek lennének). A sémainformációk azonban mindig az ldap_search híváson keresztül érhetők el. Amint egyetlen dinamikus módosítás történik (ldap_modify híváson keresztül) egy fájl attribútumértékén, a teljes fájl kicserélődik egy olyanra, amelyikben az összes attribútumérték a Directory Server előírásainak megfelelően van megadva. Mivel a fájlokhoz és az ldap_modify kérésekhez használt elemző ugyanaz, ezért az iPlanet szintaxisát követő attribútumértékeket használó ldap_modify hívások is helyesen kerülnek feldolgozásra.

Egy iPlanet szerver subschema bejegyzésére vonatkozó lekérdezés egy adott OID-hez egynél több értéket is visszaadhat. Ha például egy bizonyos attribútumtípusnak két neve van (például 'cn' és 'commonName'), akkor az attribútumtípus leírása kétszer kerül megadásra, egyszer minden egyes névhez. A Directory Server képes elemezni az olyan sémákat is, ahol egy attribútumtípus vagy objektumosztály leírása egynél többször szerepel (kivéve a NAME és DESCR) mezőket. Amikor viszont a Directory Server közzéteszi a sémát, akkor az ilyen attribútumtípusokhoz csak egyetlen leírást biztosít, az összes nevet felsorolva (a rövid név szerepel előbb). Egy példa, hogyan írja le az iPlanet a "közönséges név" attribútumot:

```
( 2.5.4.3 NAME 'cn'
  DESC 'Szabványos attribútum'
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

( 2.5.4.3 NAME 'commonName'
  DESC 'Szabványos attribútum, másik név a cn helyett'
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

És így írja le a Directory Server:

```
( 2.5.4.3 NAME ( 'cn' 'commonName' ) SUP name )
```

A Directory Server altípusokat is kezel. Ha nem akarja, hogy a 'cn' a name altípusa legyen (ami eltérés a szabványtól), akkor deklarálhatja az alábbiakat:

```
( 2.5.4.3 NAME ( 'cn' 'commonName' )
  DESC 'Szabványos attribútum'
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Ebben az esetben az első név ('cn') a preferált vagy rövid név, és a 'cn' utáni minden más név alternatívának számít. E ponttól kezdve a '2.3.4.3', a 'cn' és a 'commonName' karaktersorozatokat (illetve a csak kis- és nagybetűkben eltérő megfelelőik) szabadon felcserélve használhatók a sémán, illetve a címtárba felvett bejegyzéseken belül.

Generalized time és UTC time

Többféle módon is jelölhetők a dátumokkal és idővel kapcsolatos információk. 1999. február negyediké például leírható így:

2/4/99
4/2/99
99/2/4
4.2.1999
04-FEB-1999

és még rengeteg más módon.

A Directory Server szabványosítja az időbélyegek megjelenítését, ugyanis csak kétféle szintaxist engedélyez az LDAP szerverek számára:

- Generalized Time szintaxis, az alábbi formátumban:

ÉÉÉÉHHNNÓÓPPMM[. | , tört] [(+ | -)ÓÓPP] | Z]

4 számjegy jelzi az évet, 2 a hónapot, napot, órát, percet és másodpercet, és nem kötelező, de a másodperc törtrésze is megadható. További adatok híján a rendszer feltételezi, hogy a dátum és idő a helyi időzónában lett megadva. Azt, hogy az idő Coordinated Universal Time (UTC) formátumú megadásához írjon egy Z betűt az idő végére vagy a helyi időeltolást. Például:

"19991106210627.3"

a helyi idő 6 perccel és 27.3 másodperccel este 9 után 1999. november 6-án.

"19991106210627.3Z"

a koordinált egyetemes idő.

"19991106210627.3-0500"

a helyi idő az első példával megegyező, 5 óra különbséggel az UTC időhöz képest.

Ha megad tört másodpercet, akkor tizedespontot vagy -vesszőt kell használnia. Helyi időkülönbség megadása esetén a '+' vagy '-' jel az óra-perc érték előtt kell, hogy álljon

- Az Universal time szintaxis, amely a következő formátumú:

ÉÉHHNNÓÓPP[MM] [(+ | -)ÓÓPP] | Z]

2 számjegy jelzi az év, hónap, nap, óra, perc és az elhagyható másodperce mezőt. A GeneralizedTime szintaxishoz hasonlóan, itt is megadható egy időeltolás. Ha például a helyi idő reggel 7 1999. január másodikán, a koordinált univerzális idő pedig 1999. január 2, déli 12 óra, akkor az UTCTime értéke vagy:

"9901021200Z"

vagy

"9901020700-0500"

Ha például a helyi idő reggel 7 2001. január másodikán, a koordinált univerzális idő pedig 2001. január 2, déli 12 óra, akkor az UTCTime értéke vagy:

"0101021200Z"

vagy

"0101020700-0500"

Az UTCTime csak 2 számjegyen adja meg az év értékét, ezért használatát nem ajánljuk.

A hozzájuk tartozó megfeleltetési szabályok a generalizedTimeMatch egyenlőség vizsgálatára és a generalizedTimeOrderingMatch a nem egyezés megállapítására. Rész-karakter sorozatok nem kereshetők. A következő szűrők például érvényesek:

```
generalized-timestamp-attribute=199910061030  
utc-timestamp-attribute>=991006  
generalized-timestamp-attribute=*
```

A következő szűrők viszont nem érvényesek:

```
generalized-timestamp-attribute=1999*  
utc-timestamp-attribute>=*1010
```

Közzététel

Az i5/OS lehetővé teszi a rendszer bizonyos információinak közzétételét egy LDAP címtárban. Ez azt jelenti, hogy a rendszer képes létrehozni és frissíteni bizonyos adattípusokat ábrázoló LDAP bejegyzéseket.

Az i5/OS az alábbi információkat képes közzétenni egy LDAP szerveren:

Felhasználók

Beállítva az operációs rendszert, hogy a felhasználók adatait közzétegye a Directory Server-en, automatikusan exportálja a rendszer terjesztési címtárából a bejegyzéseket a Directory Server-re. Ezt a QGLDSSDD_search alkalmazási programcsatlón (API) keresztül teszi. Így az LDAP címtárat összehangolja a rendszer terjesztési címtárának változásaival. A QGLDSSDD API leírását a Programozás fejezet alatt található "Directory Server API-k" témakörben találja meg.

A felhasználók közzététele hasznos, ha LDAP keresési hozzáférést kíván biztosítani a rendszer terjesztési címtárhoz (például egy LDAP címjegyzék-elérést az LDAP-re felkészített POP3 levelezőprogramok számára, mint a Netscape Communicator vagy a Microsoft Outlook Express).

A közzétett felhasználók használhatók LDAP hitelesítés támogatására is; egyes felhasználók a rendszer terjesztési címtárából vannak közzétéve, mások pedig máshogyan kerülnek be a címtárba. A közzétett felhasználók uid attribútuma nevezi meg a felhasználói profilt, userPassword attribútuma pedig nincs. Ha a szerver ilyen bejegyzésre vonatkozó kapcsolódási kérést fogad, akkor meghívja az operációs rendszer biztonsági rendszerét, hogy ellenőrizze az uid-t és a megadott jelszót, mint érvényes felhasználói profilt és az ahhoz tartozó jelszót. Ha LDAP hitelesítést akar használni, és azt akarja, hogy a meglévő operációs rendszer felhasználói képesek legyenek hitelesíteni magukat az operációs rendszer jelszavaikkal, a nem i5/OS felhasználókat pedig felveszi a címtárba kézzel, akkor érdemes lehet megfontolni ezt a funkciót.

A felhasználók közzétételének másik módja a bejegyzések átvétele egy meglévő HTTP ellenőrzőlistából és a megfelelő LDAP bejegyzések létrehozása a címtárszerveren. Ez a QGLDPUBVL alkalmazásprogramozási felület (API) használatával hajtható végre. Ez az API inetOrgPerson címtárbejegyzéseket és jelszavakat hoz létre, amelyek az eredeti ellenőrzőlista bejegyzéseivel kapcsolódnak. Az API futhat egyszer is, illetve rendszeresen is a címtárszerverhez hozzáadandó új bejegyzések megkeresésére.

Megjegyzés: Ez az API csak az Apache alapú HTTP szerverrel használhatóra készült ellenőrzőlista-bejegyzéseket támogatja. A címtárszerver meglévő bejegyzései nem kerülnek frissítésre. Az ellenőrzőlistából törölt felhasználókat a rendszer nem észleli.

Ha a felhasználók egyszer már hozzáadásra kerültek a címtárhoz, akkor hitelesíthetők az ellenőrzést használó alkalmazásokhoz is, és azokhoz is, amelyek támogatják az LDAP hitelesítést. A QGLDPUBVL API leírását a Programozás fejezet alatt található "Directory Server API-k" témakörben találja meg.

Rendszerinformációk

Beállítva az operációs rendszert, hogy a felhasználók adatait közzétegye a Directory Server-en, a következő adatok kerülnek közzétételre:

- Alapszintű információk a gépről és az operációs rendszer kiadásáról.
- Kiválaszthat közzététel céljaira egy vagy több nyomtatót is. Ebben az esetben a rendszer automatikusan összehangolja az LDAP címtárat a rendszer nyomtatóin végrehajtott változtatásokkal.

A nyomtatók közzétehető információi:

- Hely
- Sebesség (lap/perc)
- Kétoldalas és színes nyomtatás támogatása
- Típus és modell

- Leírás

Ezek az információk a közzétevő rendszer információiból származnak. Hálózati környezetben ezek az információk megkönnyítik a megfelelő nyomtató kiválasztását. Az információk első alkalommal akkor kerülnek közzétételre, amikor a nyomtatón engedélyezik a közzétételt, majd minden alkalommal frissülnek az adatok, amikor a nyomtatóíró leáll vagy elindul, illetve amikor a nyomtatási eszköz leírása megváltozik.

Nyomtatómegosztások

Ha beállítja, hogy az operációs rendszer közzétegye a nyomtatómegosztásokat, akkor a kiválasztott iSeries Hálózati szerver nyomtatómegosztások adatai közzétételre kerülnek a beállított Active Directory szerveren. A nyomtatómegosztások Active Directory címtáron keresztüli közzétételével a felhasználók felvehetik az iSeries nyomtatókat Windows 2000 asztali gépeikre a Windows 2000 Nyomtató hozzáadása varázslójával. Ahhoz, hogy a Nyomtató hozzáadása varázsló használható legyen, a nyomtatót meg kell adni a Windows 2000 Active Directory címtárában. A nyomtatómegosztásokat egy olyan címtárszerveren kell közzétenni, amely támogatja a Microsoft Active Directory sémáját.

TCP/IP Szolgáltatási minőség)

A TCP/IP Szolgáltatási minőség (QoS) szerver beállítható, hogy egy, az LDAP címtárban az IBM sémájával megadott, megosztott QOS irányelvet használjon. A TCP/IP QOS közzétételi ügynököt a QOS szerver arra használja, hogy kiolvassa az irányelv-információkat: a szerver meghatározását, a hitelesítési információkat, valamint hogy a címtárban hol vannak tárolva az irányelv-információk.

A keretrendszerrel készíthető más alkalmazás is az LDAP címtár egyéb adatainak kereséséhez: további közzétételi ügynököket kell megadni, valamint használni kell a címtár közzétételi API-jait. További információkat a Programozási fejezet alatt található a “Információk publikálása a címtárszervernek” oldalszám: 92 és a Directory Server APIs témakörökben talál.

Replikáció

A címtárszerverek a replikáció nevű technikát használják a teljesítmény és a megbízhatóság javítására. A replikációs folyamat feladata, hogy szinkronban tartsa több címtár adatait.

További információk a replikáció kezeléséről: “Replikáció kezelése” oldalszám: 131. További információk a replikációról:

- “Replikáció áttekintés”
- “Replikációs szakkifejezések” oldalszám: 39
- “Replikációs megállapodások” oldalszám: 40
- “Hogyan tárolódnak a replikációs információk a szerveren?” oldalszám: 41
- “Biztonsági megfontolások a replikációs információkkal kapcsolatban” oldalszám: 41
- “Replikáció nagy rendelkezésre állású környezetben” oldalszám: 42

Replikáció áttekintés

A replikáció két fő előnyt biztosít:

- Redundánsan tárolt információk - a másolatok a fő szerver biztonsági tartalékaként szolgálnak.
- Gyorsabb keresés - a keresési kérések eloszthatók egy helyett több szerver között, amelyek ugyanazt a tartalmat tárolják. Ez javítja a kérés kiszolgálásának válaszidejét.

A címtár egyes bejegyzései a replikált részfák gyökérelemeként vannak azonosítva, kiegészítve az `ibm-replicationContext` objektumostállyal. Minden egyes részfa replikálása függetlenül történik. A részfa lefelé folytatódik a címtár-információs fán (DIT), egészen le a levél bejegyzésekig vagy más replikált részfáig. A replikált részfa gyökere alatti bejegyzések tárolják a replikációs topológia adatait. Ez egy vagy több replikációs csoport bejegyzés,

amelyek alatt a másolatok albejegyzései találhatóak. Az egyes replika részbejegyzésekhez replikációs megállapodások vannak rendelve, amelyek azonosítják az ellátó (replikált) szervereket, valamint meghatározzák a hitelesítési adatokat és az ütemezés jellemzőit.

A replikáció biztosítja, hogy az egyik címtárban elvégzett módosítás megtörténjen egy vagy több másik címtárban is. Más szavakkal, egy címtár módosítása több különböző címtárban is megjelenik. Az IBM Directory egy kibővített elsődleges-alárendelt replikációs modellt használ. A replikációs topológiák ki lettek bővítve és a következőket is biztosítják:

- A címtár-információs fa (DIT) részfáinak replikálása adott szerverekre
- Többrétegű topológia (lépcsőzetes replikáció)
- A szerverszerep (elsődleges vagy replika) részfánkenti megadása.
- Több elsődleges szerver, egyenrangú replikációhoz.
- Átjáróreplikáció hálózatok között.

A részfánkenti replikálás előnye, hogy egy replikának nem kell az egész címtárat tartalmaznia. Lehet a címtár csak egy részének, részfájának másolata.

A kibővített modell módosítja az elsődleges és replika kifejezések értelmét. Ezek a fogalmak már nem a szerverekre vonatkoznak, hanem a szerver szerepére az egyes replikált részfákat illetően. Egy szerver lehet bizonyos replikákat illetően elsődleges, míg másokra vonatkozóan replika (alárendelt). Az "elsődleges" egy olyan szervert jelent, amely elfogadja a kliensek egy replikált részfa frissítésére vonatkozó kéréseit. A "replika" pedig egy olyan szerver, amelyik csak a replikált részfa ellátójaként megjelölt más szerverektől fogad el frissítéseket.

A funkcióként meghatározott szervertípusok a következők: *master/peer*, *cascading*, *gateway* és *replica*.

1. táblázat: Szerverszerepek

Címtár	Leírás
Elsődleges/ egyenrangú	<p>Az elsődleges/egyenrangú szerver tartalmazza az elsődleges címtár adatait, amelynek frissítései továbbításra kerülnek a replikák felé. Minden módosítás az elsődleges szerveren történik, és az elsődleges szerver felelős azért, hogy a változások továbbításra kerüljenek a replikák felé.</p> <p>Több elsődleges szerver is működhet, és mindegyik elsődleges szervernek feladata, hogy frissítse a többi elsődleges és replikaszervert. Ezt egyenrangú replikációnak hívjuk. Az egyenrangú replikáció javíthatja a teljesítményt és a megbízhatóságot. A teljesítmény azért javul, mert helyi szerverek végzik az elosztott hálózaton belüli frissítéseket. A megbízhatóság pedig azért, mert egy tartalék elsődleges szerver bármikor át tudja venni az esetleg meghibásodott fő elsődleges szerver feladatát.</p> <p>Megjegyzések:</p> <ol style="list-style-type: none"> 1. Az elsődleges szerver replikálja a kliensektől érkező összes frissítést, de nem replikálja a más elsődleges szerverektől kapott frissítéseket. 2. Ha ugyanazon bejegyzés több szerveren is módosításra kerül, akkor inkonzisztenssé válhatnak a címtár adatok, mivel nincs mechanizmus az ütközések feloldására.
Lépcsőzetes felépítés (továbbítás)	<p>Lépcsőzetesnek az olyan replikaservert nevezzük, amely továbbreplikálja a neki küldött változásokat. Ez ellentétben áll az elsődleges/egyenrangú szerverre épülő rendszerrel, ahol csak az elsődleges/egyenrangú szerver replikálja a szerverhez csatlakozó kliensek módosításait. Egy lépcsőzetes szerver csökkentheti az elsődleges szerverek replikációs terhelését egy olyan hálózatban, amely sok, nagymértékben elosztott replikát tartalmaz.</p>
Átjáró	<p>Az átjáróreplikáció az átjárószervereket használja a replikációs információk hatékony összegyűjtésére és szétosztására a replikációs hálózatban. Az átjáróreplikáció elsődleges előnye a hálózati forgalom mérséklése.</p>
Replika (csak olvasható)	<p>A replika egy címtár-információk másolatát tartalmazó szerver. A replikák az elsődleges másolatok további példányai (a teljes címtáré vagy egy részfáé). A replika a replikált részfa tartalmát is képezi.</p>

Ha a replikáció meghiúsul, akkor megismétlésre kerül, még akkor is, ha közben az elsődleges szerver újraindításra került. A webes adminisztrációs eszköz Sorok kezelése ablakában ellenőrizhető a hibás replikáció.

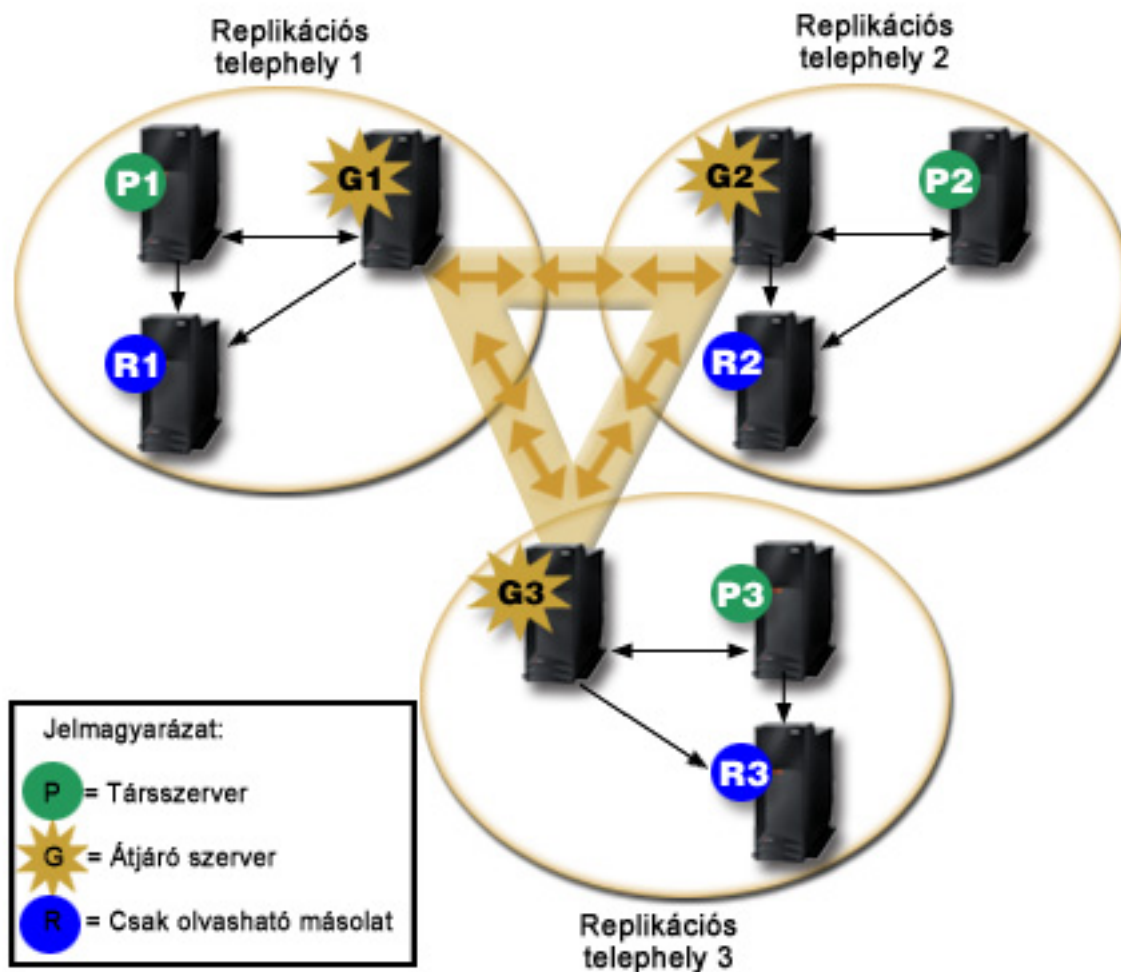
A replikaszerveren frissítések is kérhetők, de a frissítés ténylegesen az elsődleges szerverhez kerül továbbításra, visszaadva egy utalást a kliensre. Ha a frissítés sikeres, akkor az elsődleges szerver továbbküldi a frissített adatokat a replikáknak. A változások addig nem jelennek meg a kérést eredetileg intéző replikaszerveren, amíg az elsődleges szerver nem fejezte be a frissítés replikálását. A módosítások abban a sorrendben kerülnek replikálásra, amilyen sorrendben az elsődleges szerveren megtörténtek.

Ha már nem használ egy replikát, törölni kell a replikációs megállapodást az ellátó rendszeren. A definíció törlésének elfelejtése esetén a szerverben gyűlnek a felesleges frissítések és feleslegesen foglal el helyet a lemezen. Ezenfelül az ellátó továbbra is próbálkozik fog, hogy elérje a hiányzó fogyasztót; újra és újra megkísérli elküldeni az adatokat.

Átjáróreplikáció

Az átjáróreplikáció az átjárószervereket használja a replikációs információk hatékony összegyűjtésére és szétosztására a replikációs hálózatban. Az átjáróreplikáció elsődleges előnye a hálózati forgalom mérséklése. Az átjárószervereknek elsődleges (írható) szervereknek kell lenniük.

A következő ábrán az átjáróreplikáció működése látható:



2. ábra: Egy replikációs hálózat átjárószerverrel

Az előző ábrán látható replikációs hálózat három replikációs helyet tartalmaz, amelyek mindegyikében van egy átjárószerver. Az átjárószerver összegyűjti a replikációs frissítéseket a saját replikációs helye társ-/elsődleges

- | szervereiről, és a replikációs hálózaton belül elküldi ezeket az összes többi átjárószervernek. Együttal összegyűjti a replikációs hálózat többi átjárószerverén található replikációs frissítéseket, és elküldi ezeket a saját replikációs helye társ-/elsődleges és replikaszervereinek.
- | Az átjárószerverek szerverazonosítókat és ügyfélazonosítókat használnak annak meghatározására, hogy melyik frissítések kerüljenek átküldésre a replikációs hálózat átjárószerverének és melyik frissítések továbbítódjanak a replikációs hely helyi szerverei felé.
- | Az átjáróreplikáció beállításához létre kell hozni legalább egy átjárószerveret. Az átjárószerver létrehozásával létrejön egy replikációs hely. Ezután létre kell hozni a replikációs megállapodásokat az átjárószerver, valamint az ahhoz tartozó replikációs hely összes elsődleges/társszervere és replikációs szervere között.
- | Az átjárószervereknek elsődleges (írható) szervereknek kell lenniük. Ha olyan albejegyzéshez próbálja meg hozzáadni az átjáró-objektumostályt (ibm-replicaGateway), amely nem elsődleges, hibaüzenetet fog kapni.
- | Átjárószerver kétféleképpen hozható létre. Az alábbiakat teheti:
 - Létrehozhat egy új átjárószerveret
 - Egy meglévő társszervert átjárószerverre alakíthat
- | **Megjegyzés:** Nagyon fontos, hogy replikációs helyenként csak egy átjárószerveret rendeljen hozzá.

Replikációs szakkifejezések

Néhány szakkifejezés a replikáció leírásával kapcsolatban:

Lépcsőzetes replikáció

Szerverek több rétegeből álló replikációs topológia. Egy egyenrangú/elsődleges szerver az adatokat egy sor csak olvasható (továbbító) szervernek küldi el, amelyek azokat utána továbbreplikálják más szerverekre. Egy ilyen topológia csökkenti az elsődleges szerverek replikációs terhelését.

Fogyasztó szerver

Egy olyan szerver, amely a módosításokat egy másik (ellátó) szervertől kapja.

Hitelesítési adatok

Meghatározzák azt a módszert és megadják a szükséges adatokat, amelyek használatával az ellátó csatlakozik a fogyasztóhoz. Egyszerű kapcsolódás esetén ez a DN és a jelszó. A hitelesítési adatok a DN egyik bejegyzésében tárolódnak, amelyet a replikációs megállapodás azonosít.

Továbbító szerver

Egy csak olvasható szerver, amely továbbreplikálja az elsődleges vagy egyenrangú szerver által küldött összes változást. A kliensek frissítési kérései esetén utalás történik az elsődleges vagy egyenrangú szerverre.

Átjárószerver

- | Egy olyan szerver, amely a saját helyi replikációs helyének minden forgalmát továbbítja a replikációs hálózat többi átjárószervere felé. Az átjárószerverek fogadják a replikációs hálózat többi szerveréről érkező forgalmat, és továbbítják a saját helyi replikációs helyük felé. Az átjárószervereknek elsődleges (írható) szervereknek kell lenniük.

Elsődleges szerver

Egy adott részfára vonatkozóan írható (frissíthető) szerver.

Beágyazott részfa

A címtár replikált részfáján belüli részfa.

Egyenrangú szerver

Elsődleges szerver egy olyan rendszerben, ahol egy adott részfához egynél több elsődleges szerver tartozik.

Replikacsoport

Egy replikációs kontextus alatti első bejegyzésnek rendelkeznie kell az `ibm-replicaGroup` objektumostálllyal, amelyben leírja a replikációban részvevő szerverek csoportját. Praktikus helyet biztosít az ACL beállításához a

replikációs topológia információinak védelméhez. A jelenleg rendelkezésre álló adminisztrációs eszközök replikációs kontextusonként egyetlen, **ibm-replicagroup=default** nevű replikacsoport használatát engedik meg.

Replika albejegyzés

Egy replikacsoport bejegyzés alatt egy vagy több `ibm-replicaSubentry` objektumosztályú bejegyzés hozható létre; egy a replikációban ellátóként részvevő minden egyes szerver számára. A replika albejegyzés azonosítja a szerver által a replikációban betöltött szerepet: elsődleges vagy csak olvasható. Egy csak olvasható szervernek például lehetnek replikációs megállapodásai lépcsőzetes replikációhoz.

Replikált részfa

A címtár-információs fa (DIT) egy része, amely az egyik szerverről replikálásra kerül egy másikra. Ebben az esetben egy adott részfa bizonyos szerverekre replikálható, másokra nem. A részfa írható lehet bizonyos szervereken, míg másokon lehet csak olvasható.

Replikációs hálózat

Egy összekapcsolt replikációs helyekből álló hálózat.

Replikációs megállapodás

A címtárban tárolt információk, amelyek két szerver közötti "kapcsolatot" vagy "replikációs utat" határozzák meg. Az egyik szerver az ellátó (az, amelyik küldi a változásokat), a másik a fogyasztó (az, amelyik fogadja a változásokat). A megállapodás tartalmaz minden adatot, amelyre szükség van az ellátó és fogyasztó közötti kapcsolat létrehozásához és a replikáció időzítéséhez.

Replikációs kontextus

A replikált részfa gyökere. Az `ibm-replicationContext` segéd-objektumosztály felvehető bejegyzésként a replikált terület kezdőpontjának megadásához. A replikációs topológiával kapcsolatos információk a replikációs kontextus alatti bejegyzésekben tárolódnak.

| Replikációs hely

| Egy átjárószerver és minden olyan elsődleges, társ- vagy replikaserver, amely egymás replikálására van beállítva.

Ütemezés

A replikáció ütemezhető, hogy csak meghatározott időközönként történjen, és az ellátón addig felgyült módosítások egy kötegben kerüljenek továbbításra. A replikációs megállapodás tartalmazza az ütemezést leíró bejegyzésnek a DN-jét.

Ellátó szerver

Szerver, amely a változásokat továbbküldi egy másik (fogyasztó) szervernek.

Replikációs megállapodások

A replikációs megállapodás a címtár **ibm-replicationAgreement** objektumosztályú, egy replika albejegyzés alatt létrehozott bejegyzése, amely meghatározza az albejegyzés által azonosított szerver és egy másik szerver közötti replikáció módját. Ezek az objektumok hasonlítanak a Directory Server korábbi változataiban használt `replicaObject` bejegyzésekhez. A replikációs megállapodás a következő elemeket tartalmazza:

- Egy felhasználóbarát név, a megállapodás névtribútuma.
- Egy LDAP URL, amely megadja a szervert, a portszámot és hogy kell-e használni SSL-t.
- Ha ismert, akkor a fogyasztó azonosítója. A V5R3 előtti címtárszervereknek nincs szerverazonosítója.
- Az ellátónak a fogyasztóhoz kapcsolódása során használt hitelesítési adatokat tartalmazó objektum DN-je.
- Egy nem kötelező DN mutató a replikáció ütemezési információját tartalmazó objektumra. Ha nincs ilyen attribútum, akkor a változások azonnal replikálásra kerülnek.

Egy felhasználóbarát név, a fogyasztó szerver neve vagy valami más leíró karaktersorozat.

A fogyasztó szerver azonosítóját az adminisztrációs felület használja a topológia bejárásához. A fogyasztó szerver azonosítója alapján képes az adminisztrációs felület megtalálni a megfelelő albejegyzést és annak megállapodásait. Az

adatok pontosságának biztosítása érdekében, amikor az ellátó hozzákapcsolódik a fogyasztóhoz, lekéri a szerver azonosítóját a gyökér DSE-ből és összehasonlítja a megállapodásban szereplő értékkel. Ha a két szerverazonosító nem egyezik, akkor egy figyelmeztetés kerül naplózásra.

Mivel a replikációs megállapodás is replikálható, a hitelesítési objektum DN-jét használja a rendszer. Így a hitelesítési adatok a címtár egy nem replikált területén tárolhatók. A hitelesítési adatok replikálása (amelyekből "nyílt szöveggel" lekérhető a hitelesítési adatok) potenciális biztonsági rést jelentenek. A cn=localhost utótag megfelelő hely a hitelesítési adat objektumok létrehozására.

Objektumosztályok vannak definiálva a támogatott hitelesítési módszerekhez:

- Egyszerű kapcsolódás
- SASL
- EXTERNAL mechanizmus SSL használatával
- Kerberos alapú hitelesítés

Megadható, hogy egy replikált részfa egy része ne kerüljön replikálásra. Ehhez az ibm-replicationContext segédosztályt kell felvenni a részfa gyökerébe, további replika albejegyzések megadása nélkül.

Megjegyzés: A webes adminisztrációs eszköz a megállapodásokra mint "sorokra" hivatkozik, amikor egy adott megállapodás értelmében replikálásra várakozó módosításokra utal.

Hogyan tárolódnak a replikációs információk a szerveren?

A replikációs információk a címtárban három helyen tárolódnak:

- A szerver beállításai között, ahol fel van sorolva, hogyan hitelesíthetik magukat más szerverek ehhez a szerverhez replikáció elvégzésére (tehát például kit enged ez a szerver ellátóként viselkedni).
 - A címtárban egy replikált részfa tetején. Ha az "o=my company" egy replikált részfa teteje, akkor egy "ibm-replicagroup=default" nevű objektum kerül közvetlenül alatta létrehozásra (ibm-replicagroup=default,o=my company). Az "ibm-replicagroup=default" objektum alatt további objektumok írják le a részfa replikáit tartalmazó szervereket és a szerverek közötti megállapodásokat.
 - Egy "cn=replication,cn=localhost" nevű objektum szolgál a kizárólag egy szerver által használt replikációs információk tárolására. Például az ellátó szerver által használt hitelesítési adatokat tartalmazó objektumra csak az ellátó szervernek van szüksége. A hitelesítési adatokat a "cn=replication,cn=localhost" bejegyzés alatt tárolva csak az adott szerver érheti el őket.
- l
- Egy "cn=replication,cn=IBMpolicies" nevű objektum tartalmazza a többi szerverre replikált információkat.


Biztonsági megfontolások a replikációs információkkal kapcsolatban

Tekintse át a következő objektumok biztonsági megfontolásait:

- **ibm-replicagroup=default:** Ennek az objektumnak a hozzáférés-felügyelete szabályozza, hogy ki tekintheti meg vagy módosíthatja az itt tárolt replikációs információkat. Alapértelmezés szerint az objektum hozzáférés-felügyeleti beállításait a szülőjétől örökli. Érdemes lehet beállítani ezen az objektumon külön a hozzáférési jogosultságokat a replikációs információk elérésének korlátozása érdekében. Megadható például egy csoport, amelynek tagjai felelősek a replikáció kezeléséért. Ez a csoport legyen a tulajdonosa az "ibm-replicagroup=default" objektumnak, más felhasználók pedig ne is érhessek el az objektumot.
- **cn=replication,cn=localhost:** Ezzel az objektummal kapcsolatban két biztonsági szempontot kell szem előtt tartani:
 - Ennek az objektumnak a hozzáférés-felügyelete szabályozza, hogy kik tekinthetik meg és módosíthatják az itt tárolt objektumokat. Az alapértelmezett hozzáférés-felügyeleti beállítások engedik a név nélküli felhasználók számára a legtöbb információ kiolvasását (a jelszavak kivételével) és adminisztrátori jogosultságot követelnek meg az objektumok felvételéhez, módosításához és törléséhez.
 - A "cn=localhost" alatt található objektumok soha nem kerülnek replikálásra más szerverekre. A szerver által használt replikációs hitelesítési adatokat ide helyezve, más szerverek nem fogják azokat elérni. Alternatív megoldásként a hitelesítési adatok az "ibm-replicagroup=default" objektum alá is helyezhetők, hogy több szerver használja ugyanazokat a hitelesítési adatokat.

- cn=IBMPolicies: Ebben a tárolóban elhelyezhet replikációs hitelesítési adatokat, de a benne található adatok a szerver minden ügyfele számára replikálásra kerülnek. A hitelesítési adatok a cn=replication,cn=localhost alatti elhelyezése biztonságosabb megoldás.

Replikáció nagy rendelkezésre állású környezetben

- A Directory Servert gyakran használják egyszeri bejelentkezési megoldásokban, aminek következtében egyetlen meghibásodási pont keletkezhet. A Directory Server magas rendelkezésre állásúra is készíthető a replikáció használatával, mégpedig kétféleképpen: az IBM Load Balancer használatával vagy IP-cím átvétellel. Ezzel a témakörrel kapcsolatban további információk találhatóak az IBM WebSphere V5.1 Performance, Scalability, and High Availability.  című IBM Redbook kiadvány 13.2 fejezetében.

Tartományok és felhasználói sablonok

A webes adminisztrációs eszköz tartomány és sablon objektumainak célja, hogy megkönnyítse a felhasználó dolgát és ne kelljen részletesen foglalkoznia az LDAP rendszer kérdéseivel.

Egy tartomány felhasználók és csoportok gyűjteménye. Egy lapos címtárstruktúrában megadja, hol található a felhasználók és a csoportok. Egy tartomány egy helyet (például "cn=users,o=acme,c=us") ad meg a felhasználók számára és a felhasználókat közvetlenül e bejegyzés alatt hozza létre (tehát Kő Pál mint "cn=Kő Pál,cn=users,o=acme,c=us") kerül létrehozásra. Több tartomány is megadható és ismerős nevek adhatók nekik (például Webes felhasználók). Az ismerős neveket használhatják a felhasználókat létrehozó és karbantartó személyek is.

A sablonok a felhasználók adatainak formátumát írják le. Megadják, hogy milyen objektumosztályokat használ a rendszer a felhasználók létrehozásakor (mind a strukturális, mind a kiegészítő osztályokat). A sablonok megadják továbbá a felhasználók létrehozásakor használt ablakok szerkezetét (például a lapok nevét, az alapértelmezett értékeket és a lapokon megjelenő attribútumokat).

Egy új tartomány létrehozásakor egy ibm-realm objektum kerül létrehozásra a címtárban. Az ibm-realm objektum rögzíti a tartomány tulajdonságait, például hogy hol kerülnek létrehozásra a felhasználók és csoportok, illetve melyik sablont kell használni. Az ibm-realm objektum rámutathat egy meglévő címtárbejegyzésre, mint a felhasználók szülőobjektumára, de mutathat magára is, és ekkor ő maga az új felhasználók tárolója (ez az alapértelmezés). Lehet például egy meglévő cn=users,o=acme,c=us tároló és létrehozható a címtárban más helyen egy users nevű tartomány (például egy cn=realms,cn=admin stuff,o=acme,c=us tárolóobjektumban), amely megadja, hogy az új felhasználókat és csoportokat a cn=users,o=acme,c=us helyen kell létrehozni. Ennek hatására létrejön az alábbi ibm-realm objektum:

```
dn: cn=users,cn=realms,cn=admin stuff,o=acme,c=us
objectclass: top
objectclass: ibm-realm
objectclass: ibm-staticGroup
ibm-realmUserTemplate: cn=users template,cn=realms,cn=admin stuff,o=acme,c=us
ibm-realmUserContainer: cn=users,o=acme,c=us
ibm-realmGroupContainer: cn=users,o=acme,c=us
ibm-realmAdminGroup: cn=users,cn=realms,cn=admin stuff,o=acme,c=us
ibm-realmUserSearchFilter:
cn: users
```

Vagy ha nem létezett cn=users,o=acme,c=us objektum, akkor a users tartomány létrehozható az o=acme,c=us helyen és mutathat saját magára.

A címtár rendszergazda felelős a felhasználói sablonok, tartományok és tartományadminisztrátori csoportok kezeléséért. Egy tartomány létrehozása után a tartomány adminisztrátori csoportjának tagjai lesznek felelősek az adott tartomány felhasználóinak és csoportjainak kezeléséért.

További információ a tartományok és a felhasználói sablonok kezeléséről: "Tartományok és felhasználói sablonok kezelése" oldalszám: 178.

Keresési paraméterek

A szerver által használt erőforrások mennyiségének korlátozásához az adminisztrátor beállíthatja a keresési paramétereket a felhasználók keresési lehetőségeinek korlátozására. A keresési lehetőségek egyes különleges felhasználók számára ki is bővíthetők. A felhasználói keresések a következő módszerekkel korlátozhatók és bővíthetők ki:

Keresés korlátozása

- Oldalakra bontott keresés
- Rendezett keresés
- Álnév-hivatkozás-feloldás letiltása

Keresés kibővítése

- Keresésikorlát-csoportok

Oldalakra bontott keresés

Az oldalakra bontott keresési funkcióval szabályozható az egy keresési kérésből egyszerre visszakapott adatok mennyisége. A szerverről kérhető a bejegyzések egy részhalma (egy oldal), vagy kérhető a teljes eredményhalmaz egyszerre. A további keresési kérések az eredmények következő oldalát adják vissza, addig, amíg a kérés visszavonásra nem kerül, vagy az utolsó eredmény is ki nem lett szolgáltatva. A rendszergazda korlátozhatja ennek használatát azzal, hogy csak az adminisztrátorok számára teszi elérhetővé.

Rendezett keresés

A rendezett keresés eredményeit a kliens egy feltételista szerint rendezett formában kapja vissza, ahol az egyes feltételek rendezési kulcsokat reprezentálnak. A rendezés feladata ily módon átterhelhető a kliensről a szerverre. A rendszergazda korlátozhatja ennek használatát azzal, hogy csak az adminisztrátorok számára teszi elérhetővé.

Álnév-hivatkozás-feloldás letiltása

Egy alias vagy aliasObject objektumostállyal rendelkező címtárbejegyzés tartalmazza az aliasedObjectName attribútumot, amellyel a címtár másik bejegyzésére lehet hivatkozni. Hogy az álnévek feloldásra kerüljenek-e, az csak keresési kérésekben adható meg. A *feloldás* az álnév visszakövetését jelenti az eredeti bejegyzésig. A **mindig** vagy **kereséskor** álnév-hivatkozás-feloldási beállításokkal rendelkező IBM Directory Server keresési válaszeje jelentősen hosszabb lehet, mint a **soha** beállítással rendelkezőé, még akkor is, ha a címtárban nincsenek álnévbejegyzések. Két beállítás határozza meg a szerver álnév-hivatkozás-feloldási működési módját: a kliens keresési kérésben megadott feloldási beállítás, illetve a szerveren az adminisztrátor által beállított feloldási beállítás. Ha arra van beállítva, a szerver automatikusan kihagyja az álnév-hivatkozás-feloldást, ha a címtárban nincs alias objektum, valamint felülírja a kliens keresési kérésben megadott feloldási beállításokat. A következő táblázat mutatja a kliens és a szerver közötti álnév-hivatkozás-feloldás kivonatos működését:

2. táblázat: Tényleges álnév-hivatkozás-feloldás a kliens és a szerver beállításai alapján

Szerver	Kliens	Tényleges
soha	bármilyen beállítás	soha
mindig	bármilyen beállítás	a kliens beállítása
bármilyen beállítás	mindig	a szerver beállítása
keresés	találat	soha
találat	keresés	soha

Keresésikorlát-csoportok

| Az adminisztrátorok az általános felhasználóknál sokkal rugalmasabb keresési korlátokkal rendelkező
| keresésikorlát-csoportokat hozhatnak létre. A keresésikorlát-csoportban szereplő egyedi tagok vagy csoportok számára
| kevésbé szoros keresési korlátok hozhatók létre, mint amilyenek az általános felhasználók számára szabhatók.

| Amikor egy felhasználó keresést indít, akkor először a keresési kérés korlátai kerülnek ellenőrzésre. Ha a felhasználó
| keresésikorlát-csoport tagja, akkor a korlátok összehasonlításra kerülnek. Ha a keresésikorlát-csoport megszorításai
| kevésbé szigorúak, mint a keresési kérései, akkor a keresési kérés korlátai kerülnek felhasználásra. Ha a keresési kérés
| megszorításai kevésbé szigorúak, mint a keresésikorlát-csoportéi, akkor a keresésikorlát-csoport korlátai kerülnek
| felhasználásra. Ha a rendszer nem talál keresésikorlát-csoport bejegyzést, akkor ugyanez az összehasonlítás a szerver
| keresési korlátozásaival kapcsolatban zajlik le. Ha nincs szerver keresési korlát beállítva, akkor az összehasonlítás az
| alapértelmezett szerverbeállításhoz képest történik. A felhasznált korlátozások mindig az összehasonlításban szereplő
| legenyhébb korlátozások.

| Ha egy felhasználó több keresésikorlát-csoportba is tartozik, akkor számára a legmagasabb szintű keresési lehetőség
| kerül biztosításra. Ha például a felhasználó beletartozik az 1. keresési csoportba, amely 2000 bejegyzés keresésénél és
| 4000 másodpercnél húzza meg a határt, valamint beletartozik a 2. csoportba, amely korlátlan számú bejegyzés
| keresésére ad módot 3000 másodpercig, akkor a felhasználó keresési korlátja korlátlan számú bejegyzésre és 4000
| másodpercre fog vonatkozni.

| A keresésikorlát-csoportok a localhost vagy az IBMpolicies alatt is tárolhatók. Az IBMpolicies alatt tárolt
| keresésikorlát-csoportok replikálásra kerülnek, a localhost alattiak nem. Ugyanaz a keresésikorlát-csoport a localhost és
| az IBMpolicies alatt is tárolható. Ha a keresésikorlát-csoport ezen megkülönböztetett nevek egyike alatt sincs tárolva,
| akkor a szerver figyelmen kívül hagyja a csoport keresési korlát részét, és normál csoportként kezeli azt.

| Amikor egy felhasználó keresést indít, akkor a rendszer először a localhost alatt található keresésikorlát-csoport
| bejegyzéseket ellenőrzi. Ha nem talál a felhasználóra vonatkozó bejegyzést, akkor végignézi az IBMpolicies alatti
| keresésikorlát-csoport bejegyzéseket is. Ha a localhost alatt talál bejegyzést, akkor az IBMpolicies alatti
| keresésikorlát-csoport bejegyzéseket már nem vizsgálja. A localhost alatti keresésikorlát-csoport bejegyzéseknek
| prioritásuk van az IBMpolicies alattiakkal szemben.

| A keresési paraméterekkel kapcsolatban további információk:

- “Keresési beállítások módosítása” oldalszám: 127
- “Címtárbejegyzések keresése” oldalszám: 172
- “Keresésikorlát-csoportok kezelése” oldalszám: 122

Nemzeti nyelvek támogatása (NLS)

Ügyeljen a nemzeti nyelvek támogatásával kapcsolatos alábbi szempontokra:

- Az adatok átvitele UTF-8 formátumban történik az LDAP szerverek és a kliensek között. Az összes ISO 10646 karakter megengedett.
- A Directory Server 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 nyelv esetén (helyi sajátosságok).

Az UCS-2 módszerről további információk a Tervezés fejezete alatt, a “Globalizáció” témánál találhatók.

Nyelvi címkék

| A *nyelvi címkék* meghatározzák azt a mechanizmust, amelynek segítségével természetes nyelvek kódjai rendelkeznek a
| címtárban tárolt értékekhez és a kliensek lekérdezhetik a bizonyos természetes nyelvi feltételeknek megfelelő értékeket.
| A nyelv címkéje egy attribútumleírás egyik összetevője. A nyelv címkéje egy karaktersorozat, amely egy lang- előtagból,
| betűkarakterek elsődleges részcímkéjéből, és esetleg kötőjellel (-) csatlakozó részcímkékből áll. Az egymás után
| következő részcímkék betű- és számkarakterek bármilyen kombinációi lehetnek; csak az elsődleges részcímkének kell
| betűkből állnia. A részcímkék bármilyen hosszúak lehetnek; az egyetlen korlátozás, hogy a címke teljes hossza nem
| haladhatja meg a 240 karaktert. A nyelv címkékben a kis- és a nagybetűk nem számítanak eltérőnek; az en-us, en-US

| és EN-US azonosak. A nyelvi címkék használata nem megengedett a DN vagy RDN összetevőiben.
| Attribútumleírásonként csak egy nyelvi címke használata engedélyezett.

| **Megjegyzés:** Attribútumonként a nyelvi címkék közösen kizárják egymást az egyedi attribútumokkal. Ha egy adott
| attribútum egyedi attribútumként van megjelölve, akkor nem lehet hozzárendelve nyelvi címke.

| Ha egy adat címtárhoz rendelésekor nyelvi címkék is vannak, akkor ezek a keresési műveletekben használhatók arra,
| hogy az adott nyelvekben szelektíven attribútumértékek legyenek lekérdezhetők. Ha egy nyelvi címke meg van adva
| egy keresés kért attribútumainak listáján belül egy attribútumleírásban, akkor csak az azonos nyelvi címkével
| rendelkező címtárbejegyzés attribútumértékei kerülnek visszaadásra. Így a következőhöz hasonló keresés esetében:
| `ldapsearch -b "o=ibm,c=us" (objectclass=organization) description;lang-en`

| a szerver visszaadja a "description;lang-en" attribútum értékeit, de nem adja vissza a "description" vagy
| "description;lang-fr" értékeit.

| Ha egy kérés egy attribútum megadásával, de egy nyelvi címke megadása nélkül érkezett, akkor minden
| attribútumérték visszaadásra kerül, függetlenül a nyelvi címkéktől.

| Az attribútumtípus és a nyelvi címke pontosvesszővel (;) van elválasztva.

| **Megjegyzés:** A pontosvessző karakter az AttributeType "NAME" részében is használható. Mivel azonban ez a
| karakter a nyelvi címke AttributeType értékétől külön kerül használatra, használata az AttributeType
| "NAME" részében nem engedélyezett.

| Ha például a kliens egy "description" attribútumot kér, és a megfelelő bejegyzés a következőket tartalmazza:

```
| objectclass: top  
| objectclass: organization  
| o: Software GmbH  
| description: software  
| description;lang-en: software products  
| description;lang-de: Softwareprodukte  
| postalAddress: Berlin 8001 Germany  
| postalAddress;lang-de: Berlin 8001 Deutschland
```

| akkor a szerver a következőket adja vissza:

```
| description: software  
| description;lang-en: software products  
| description;lang-de: Softwareprodukte
```

| Ha a keresés egy "description;lang-de" attribútumot kér, akkor a szerver a következőt adja vissza:

```
| description;lang-de: Softwareprodukte
```

| A nyelvi címkék használata módot ad arra, hogy a címtárakban többnyelvű adatok legyenek, amivel lehetővé válik a
| kliensek számára a többféle nyelvű működés. A nyelvi címkék használatával egy alkalmazás megírható úgy, hogy egy
| német kliens csak a lang-de attribútummal beírt adatokat lássa, egy francia pedig csak a lang-fr attribútumúakat.

| Annak meghatározásához, hogy egy nyelvi címke működése engedélyezve van-e, indítson egy root DSE keresést az
| "ibm-enabledCapabilities" attribútum megadásával.

```
| ldapsearch -b "" -s base objectclass=* ibm-enabledCapabilities
```

| Ha a visszaérkező OID "1.3.6.1.4.1.4203.1.5.4", akkor a funkció engedélyezve van.

| Ha a nyelvi címkék támogatása nem engedélyezett, akkor minden olyan LDAP-kérés, amely nyelvi címkét rendel egy
| attribútumhoz, hibaüzenettel visszautasításra fog kerülni.

| Bizonyos attribútumokhoz rendelhető nyelvi címke, míg másokhoz nem. Annak eldöntésére, hogy egy attribútum
| megengedi-e a nyelvi címkék használatát, az `ldapexop` parancs használható:

- | • A nyelvi címkék használatát megengedő attribútumokhoz: `ldapexop -op getattributes -attrType language_tag -matches true`
- | • A nyelvi címkék használatát nem megengedő attribútumokhoz: `ldapexop -op getattributes -attrType language_tag -matches false`
- | További információk: “Nyelvi címkékkel ellátott attribútumokat tartalmazó bejegyzés hozzáadása” oldalszám: 169.

LDAP címtárutalások

Az utalások lehetővé teszik, hogy a Directory Server szerverek csoportosan működjenek. Ha a kliens által igényelt DN nem található az egyik címtárban, a szerver automatikusan átküldheti (utalhatja) a kérést bármely más LDAP szerverre.

A Directory Server rendszeren két különböző típusú utalást lehet használni. Meghatározhatók alapértelmezett utalási szerverek, amelyekhez az LDAP szerver a klienseket utalja, ha egy DN nem található a címtárban. Arra is felhasználható az LDAP kliens, hogy utalás objektumosztályú (objectClass utalás) bejegyzéseket vigyen fel a címtárszerverre. Így olyan utalások határozhatók meg, melyek a kliens által igényelt specifikus DN-re alapulnak.

Megjegyzés: A Directory Server utalási objektumainak csak egy megkülönböztető nevet (dn), egy objektumosztályt (objectClass), és egy utalás (ref) attribútumot kell tartalmazni. Példa a korlátozás illusztrálására: “ldapsearch” oldalszám: 206.

Az utalási szerverek szorosan kapcsolódnak a replikaszerverekhez. Mivel a replikaszerveren lévő adatot egy kliens nem módosíthatja, a replika minden címtármódosítási igényt az elsődleges szerverre utal.

Tranzakciók

A Directory Server beállítható úgy, hogy megengedje a klienseknek tranzakciók használatát. A tranzakciók beállításaival kapcsolatos további információk: “Tranzakció-beállítások megadása” oldalszám: 117. Egy tranzakció LDAP címtárműveletek csoportja, amit a címtár egyetlen egységként kezel. A tranzakciót alkotó LDAP műveletek közül egyik sem végleges, amíg a tranzakció összes művelete sikeresen véget nem ért, és a címtárszolgáltató a tranzakciót nem nyugtázza. Ha bármelyik művelet sikertelen volt, vagy törölték a tranzakciót, egyetlen művelet sem kerül végrehajtásra. Ez megkönnyíti a felhasználó dolgát, mert szervezeten képes LDAP műveleteket megvalósítani. Például a felhasználó állítson össze a kliensen egy tranzakciót, mellyel több címtárbejegyzést kíván törölni. Ha a tranzakció közben megszakad a kliens és a szerver között a kapcsolat, egyetlen bejegyzés sem kerül törlésre. Ezért a felhasználó újraindíthatja a tranzakciót, nem kell vizsgálnia azt, hogy mely bejegyzés került törlésre.

A következő LDAP műveletek lehetnek egy tranzakció részelei:

- felvétel
- módosítás
- RDN módosítása
- törlés

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

Directory Server biztonsága

A Directory Server biztonságával az alábbi témakörök foglalkoznak:

- “Ellenőrzés” oldalszám: 47
- “Védett socket réteg (SSL) és Fordítási réteg biztonság (TLS) használata LDAP Directory Serverrel” oldalszám: 47
- “Kerberos hitelesítés használata Directory Server-rel” oldalszám: 48
- “Csoportok és szerepek” oldalszám: 48

- “Adminisztratív hozzáférés” oldalszám: 55
- “Proxy hitelesítés” oldalszám: 55
- “Hozzáférés-felügyeleti listák” oldalszám: 56
- “LDAP címtárobjektumok tulajdonjoga” oldalszám: 67
- “Jelszó-irányelvek” oldalszám: 68
- “Hitelesítés” oldalszám: 71
- “Szolgáltatás megbénítása” oldalszám: 74

Kapcsolódó fogalmak

“Biztonsági tulajdonságok kezelése” oldalszám: 150

Ellenőrzés

A Directory Server támogatja az i5/OS biztonsági ellenőrzést. Az ellenőrzésre kerülő elemek a következők:

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

Lehet, hogy meg kell változtatni az naplózási beállításait, mielőtt használatba veszi a címtárbejegyzések naplózását. Ha a QAUDCTL rendszer értékbe *OBJAUD lett beállítva, akkor az iSeries navigátor segítségével engedélyezhető az objektumnaplózás. A naplózásról további információkat a következő kiadványban talál: *Biztonsági referenciakönyv*



vagy a “Biztonság ellenőrzése” című témakörben.

Védett socket réteg (SSL) és Fordítási réteg biztonság (TLS) használata LDAP Directory Serverrel

A Directory Server kapcsolatainak biztonságosabbá tételéhez a Directory Server alkalmazhatja az SSL (Secure Sockets Layer, védett socket réteg) és a Transport Layer Security (TLS) elnevezésű biztonsági eljárásokat.

Az SSL egy szabvány az Internet biztonságához. Az SSL LDAP kliensekhez és LDAP replikaszerverekhez kapcsolódásra egyaránt használható. A szerverhitelesítésen túlmenően használható klienshitelesítés is, ami további biztonságot jelent az SSL kapcsolatok számára. A klienshitelesítés 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 i5/OS 34-es lehetősége). A DCM program lehetővé teszi, hogy digitális igazolásokat állítson elő, kezeljen és tároljon. A DCM használatával és a digitális igazolásokkal kapcsolatos információkat a “Digitális igazolás kezelő” témakörben talál. Az iSeries, SSL-jéről információt a “Védett socket réteg (SSL)” részben talál.

- | A TLS az SSL utódául készült, és ugyanazt a kriptográfiai eljárást használja, de több kriptográfiai algoritmust támogat.
- | Az iSeries szerverre telepített TLS-ről olvashat az SSL és Szállítási réteg biztonság (TLS) protokollok támogatása részben. A TLS módot ad arra, hogy a szerver fogadja a kliens felől érkező biztonságos és nem biztonságos kommunikációt az alapértelmezett 389-es porton keresztül. A biztonságos kommunikációhoz a kliensnek használnia kell a StartTLS kibővített műveletet.

Annak érdekében, hogy a kliens használhassa a TLS-t:

1. A Directory Servernek beállítva kell lennie a TLS vagy SSLTLS használatára. Részletek: “SSL és TSL engedélyezése a Directory Serveren” oldalszám: 154.

2. A kliens parancssoros segédprogramjaiban meg kell adni az -Y paramétert.

Megjegyzés: A TLS és az SSL nem működik együtt kölcsönösen. A TLS indítási kérés (a -Y paraméter) kiadása egy SSL port felett működési hibát okoz.

Egy kliens akár a TSL, akár az SSL használatával kapcsolódhat a biztonságos portra (636). A StartTLS egy LDAP szolgáltatás, amellyel lehetőséget ad a biztonságos kommunikációra egy meglévő nem biztonságos kapcsolaton (pl. a 389-es porton) keresztül. Így a StartTLS (vagy a parancssoros segédprogramban megadott -Y paraméter) csak a szabványos nem biztonságos (389) porttal használható, biztonságos kapcsolattal nem.

További információk: "SSL és TSL engedélyezése a Directory Serveren" oldalszám: 154.

Kerberos hitelesítés használata Directory Server-rel

A Directory Server rendszer lehetővé teszi Kerberos hitelesítés használatát. A Kerberos egy hálózati hitelesítési protokoll, amely titkos kulcsú kriptográfiai megoldást használ erős hitelesítés biztosításához kliens-szerver alkalmazások számára.

Kerberos hitelesítés engedélyezéséhez konfigurálni kell a hálózati hitelesítési szolgáltatást.

A Directory Server Kerberos szolgáltatása támogatást biztosít a GSSAPI SASL eljárásához. Ez lehetővé teszi, hogy a Directory Server és a Windows 2000 LDAP kliensei a Directory Server-rel együtt Kerberos hitelesítést használjanak.

A szerver a következő alakú **Kerberos azonosítót** használja:

szolgáltatásnév/hosztnév@tartomány

A szolgáltatásnév paraméter értéke ldap (kisbetűvel), a hostnév a rendszer teljes TCP/IP neve, a tartomány pedig a rendszer Kerberos konfigurációjában specifikált alapértelmezés szerinti tartománya.

Például ha van az acme.com TCP/IP tartományban egy my-as400 nevű rendszer ACME.COM alapértelmezés szerinti Kerberos tartománnyal, akkor az LDAP szerver Kerberos azonosítója ldap/my-as400.acme.com@ACME.COM. A Kerberos alapértelmezés szerinti tartománya 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. A címtárszerver nem konfigurálható a Kerberos hitelesítés használatára, ha az alapértelmezés szerinti tartomány nem lett korábban beállítva.

Kerberos hitelesítés használata esetén a Directory Server egy megkülönböztető nevet (DN-t) társít a kapcsolathoz, amely szabályozza a címtárakatok elérését. Kiválasztható, hogy a szerver DN-t a következő módszerek közül melyikhez legyen társítva:

- A szerver a Kerberos ID alapján hozza létre a DN-t. Ennek a lehetőségnek a kiválasztása esetén az azonosító@tartomány alakú Kerberos azonosító egy ibm-kn=azonosító@tartomány alakú DN-t generál. Az ibm-kn= egyenlő az ibm-kerberosName= kifejezéssel.
- A szerver kereshet a címtárban egy megkülönböztetett nevet (DN-t), aminek egyik bejegyzése tartalmazza a Kerberos azonosítót és tartományt. Ha ezt a lehetőséget választja, a szerver az alábbiakban ismertetett módon keres a címtárban egy bejegyzést, amely a Kerberos azonosítót határozza meg:

Kell, hogy legyen egy kulcstáblázat (keytab) fájl, ami tartalmaz egy kulcsot az LDAP szolgáltatás (Kerberos) azonosítója 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.

Csoportok és szerepek

A csoportok lényegében listák, nevek gyűjteménye. A csoportok az **aclentry**, **ibm-filterAclEntry** és **entryowner** attribútumokban használhatók a hozzáférés korlátozására, illetve alkalmazáspecifikus feladatokra, mint a

levelezőlisták. További részletek: “Hozzáférés-felügyeleti listák” oldalszám: 56. A csoportok lehetnek statikusak, dinamikusak és egymásba ágyazottak. A csoportok kezelésével kapcsolatos információk: “Felhasználók és csoportok kezelése” oldalszám: 175.

A szerepek hasonlítanak abban a csoportokra, hogy szintén objektumként jelennek meg a címtárban. A szerepek azonban DN-ek csoportját is tartalmazzák.

További információk:

- “Statikus csoportok”
- “Dinamikus csoportok”
- “Beágyazott csoportok” oldalszám: 50
- “Hibrid csoportok” oldalszám: 51
- “Csoporttagság meghatározása” oldalszám: 51
- “Csoport objektumosztályok beágyazott és dinamikus csoportokhoz” oldalszám: 53
- “Csoport attribútum típusok” oldalszám: 54
- “Szerepek” oldalszám: 54

Statikus csoportok

Egy statikus csoport minden egyes tagját külön határozza meg a strukturális **groupOfNames**, **groupOfUniqueNames**, **accessGroup** vagy **accessRole** objektumosztály segítségével; illetve a kiegészítő **ibm-staticgroup** használatával. Egy **groupOfNames** vagy **groupOfUniqueNames** strukturális objektumosztályt használó csoportnak legalább egy tagja kell, hogy legyen. Az **accessGroup** vagy **accessRole** strukturális objektumosztályt használó csoport lehet üres is. Statikus csoportok kiegészítő objektumosztályokkal is megadhatók: az **ibm-staticGroup**, nem követeli meg a **member** attribútum használatát, ezért lehet üres is.

Egy szokásos csoport bejegyzés:

```
DN: cn=Dev.Staff,ou=Austin,c=US
   objectclass: accessGroup
   cn: Dev.Staff
   member: cn=John Doe,o=IBM,c=US
   member: cn=Jane Smith,o=IBM,c=US
   member: cn=James Smith,o=IBM,c=US
```

Minden egyes csoportnak van egy többértékű attribútuma, amely a csoport DN-jeit sorolja fel.

Egy hozzáférési csoport törlése esetén a hozzáférési csoport is törlésre kerül minden ACL-ből, amelyhez korábban rendelve volt.

Dinamikus csoportok

A dinamikus csoportok másképp határozzák meg tagjaikat, mint a statikus csoportok. Ahelyett, hogy felsorolná őket, a dinamikus csoport tagjait egy LDAP kereséssel határozza meg. A dinamikus csoport a **groupOfURLs** strukturális objektumosztályt (vagy az **ibm-dynamicGroup** kiegészítő objektumosztályt) és a **memberURL** attribútumot használja a keresés megadásához egy egyszerűsített LDAP URL szintaxis segítségével.

```
ldap:///<keresés alap DN-je> ? ? <keresés hatóköre> ? <keresési szűrő>
```

Megjegyzés: Amint a fenti példából is látható, a hosztnév nem kötelező eleme a szintaxisnak. A többi paraméter ugyanolyan, mint a szokásos LDAP URL szintaxis esetében. Minden egyes paramétermezőt egy kérdőjel (?) karakterrel kell elválasztani, akkor is, ha nincs egy paraméter sem megadva. Normál esetben meg szokás adni a visszaadandó attribútumok listáját az alap DN és a keresés hatóköre között. Erre a paraméterre azonban szintén nincs szükség a dinamikus tagság megállapításához, ugyanakkor az elválasztó ? karakter nem hiányozhat.

ahol:

keresés alap DN-je

Az a pont, ahol a keresés elkezdődik a címtárban. Ez lehet egy utótag, vagy a címtár gyökere, például **ou=Szolnok**. Ez a paraméter kötelező.

keresés hatóköre

A keresés kiterjedését adja meg. Az alapértelmezett hatókör a "base".

base Csak az URL-ben megadott alap DN információit adja vissza.

one Az URL-ben megadott alap DN-nél egy szinttel mélyebben levő bejegyzések információit adja vissza. Az alap bejegyzést nem tartalmazza.

sub Az összes lejjebb lévő szint információit visszaadja, az alap DN-nel együtt.

keresési szűrő

Az a szűrő, amelyet a keresés hatókörébe eső bejegyzéseken alkalmazni kíván. A keresési szűrő szintaxisának leírását az alábbi helyen találja: "az ldapsearch szűrési beállítás" oldalszám: 210. Az alapértelmezett érték az `objectclass=*`

A dinamikus tagkeresés mindig a szerveren belüli művelet, ezért szemben a teljes LDAP URL-lel, itt sosem kell megadni a hosztnévet és a portszámot, és a használt protokoll is mindig **ldap** (és nem **ldaps**). A **memberURL** tartalmazhat bármilyen URL-t, de a szerver csak az **ldap:///** karakterekkel kezdődő **memberURL** értékeket használja a dinamikus tagság meghatározásához.

Példák

Egyetlen bejegyzés, amelyben a hatókör a "base" és a szűrő az alapértelmezett "objectclass=*":

```
ldap:///cn=Kis Csaba, cn=Employees, o=Acme, c=US
```

Az összes bejegyzés, amely egy szinttel a cn=Employees alatt található és a szűrő az alapértelmezett "objectclass=*":

```
ldap:///cn=Employees, o=Acme, c=US??one
```

Minden "person" objektumosztályú bejegyzés az o=Acme alatt:

```
ldap:///o=Acme, c=US??sub?objectclass=person
```

A felhasználói bejegyzésekhez használt objektumosztályoktól függően előfordulhat, hogy a bejegyzések nem tartalmazzák a csoporttagság megállapításához szükséges attribútumokat. Az **ibm-dynamicMember** kiegészítő objektumosztály használatával a felhasználói bejegyzések kiterjeszthetők, hogy tartalmazzák az **ibm-group** attribútumot is. Ezzel az attribútummal tetszőleges értékek vehetők fel a felhasználói bejegyzésekbe, amelyek szintén használhatók szűrésre a dinamikus csoporttagság meghatározásához. Például:

Legyenek a dinamikus csoport tagjai azok a bejegyzések, amelyek közvetlenül a cn=users,ou=Austin bejegyzés alatt találhatóak és **ibm-group** attribútumuk értéke **GROUP1**:

```
dn: cn=GROUP1,ou=Austin
objectclass: groupOfURLs
cn: GROUP1
memberURL: ldap:///cn=users,ou=Austin??one?(ibm-group=GROUP1)
```

A cn=GROUP1,ou=Austin csoport egy tagja:

```
dn: cn=Group 1 tag, cn=users, ou=austin
objectclass: person
objectclass: ibm-dynamicMember
sn: tag_neve
userpassword: tag_jelszava
ibm-group: GROUP1
```

Beágyazott csoportok

A csoportok egymásba ágyazásával kialakíthatók hierarchikus viszonyok, amelyekkel örökölt csoporttagság adható meg. A beágyazott csoport egy leszármazott csoport bejegyzése, amelynek DN-jére hivatkozik egy attribútum a szülő

csoporthozzáadásban. Szülőcsoport a meglévő strukturális objektumosztályok (**groupOfNames**, **groupOfUniqueNames**, **accessGroup**, **accessRole** és **groupOfURLs**) kiterjesztésével, az **ibm-nestedGroup** kiegészítő objektumosztály felvételével hozható létre. A beágyazott csoport kiterjesztés után nulla vagy több **ibm-memberGroup** attribútum vehető fel, amelyek a beágyazott, leszármazott csoportok DN-jeit tartalmazzák. Például:

```
dn: cn=Group 2, cn=Groups, o=IBM, c=US
objectclass: groupOfNames
objectclass: ibm-nestedGroup
objectclass: top
cn: Group 2
description: Statikus és beágyazott tagokat tartalmazó csoport.
member: cn=Person 2.1, cn=Dept 2, cn=Employees, o=IBM, c=US
member: cn=Person 2.2, cn=Dept 2, cn=Employees, o=IBM, c=US
ibm-memberGroup: cn=Group 8, cn=Nested Static, cn=Groups, o=IBM, c=US
```

A beágyazott csoportok hierarchiáján belül ciklikusság nem alakítható ki. Amennyiben kiderül, hogy egy beágyazott csoport művelet körkörös hivatkozást eredményezne, akár közvetlenül, akár öröklődés útján, ez az előírások megsértésének számít, és ezért a bejegyzés frissítése nem történik meg.

Hibrid csoportok

Bármelyik strukturális objektumosztály kiterjeszthető, hogy a csoporttagság statikus, dinamikus és beágyazott tagtípusok kombinációjával legyen leírható. Például:

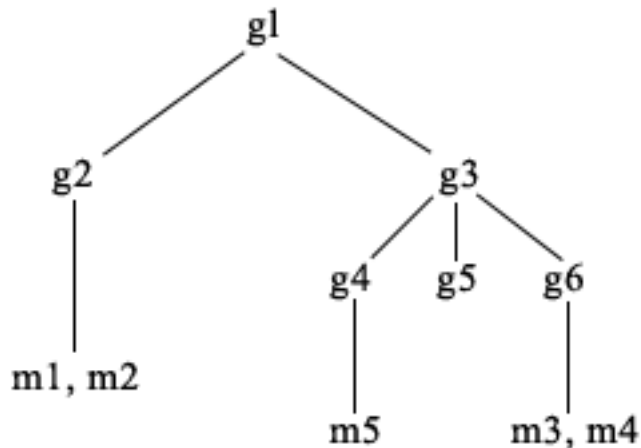
```
dn: cn=Group 10, cn=Groups, o=IBM, c=US
objectclass: groupOfURLs
objectclass: ibm-nestedGroup
objectclass: ibm-staticGroup
objectclass: top
cn: Group 10
description: Statikus, dinamikus és beágyazott tagokból álló csoport.
memberURL: ldap:///cn=Austin, cn=Employees, o=IBM, c=US??one?objectClass=person
ibm-memberGroup: cn=Group 9, cn=Nested Dynamic, cn=Groups, o=IBM, c=US
member: cn=Person 10.1, cn=Dept 2, cn=Employees, o=IBM, c=US
member: cn=Person 10.2, cn=Dept 2, cn=Employees, o=IBM, c=US
```

Csoporttagság meghatározása

Két műveleti attribútum használható az összesített csoporttagság lekérdezésére. Egy adott csoport bejegyzés esetén az **ibm-allMembers** műveleti attribútum számlálja meg az összesített csoporttagságot, beleértve a statikus, dinamikus és beágyazott tagokat, a beágyazott csoportok hierarchiájánál leírt módon. Egy adott felhasználói bejegyzés esetén az **ibm-allGroups** műveleti attribútum számlálja meg az összes olyan csoportot, beleértve az őt csoportokat is, amelyeknek a felhasználó tagja.

Egy kérő lehet, hogy csak a kért adatok egy részét kapja meg, attól függően, hogyan vannak beállítva az ACL-ek az adatokon. Bárki lekérdezheti az **ibm-allMembers** és **ibm-allGroups** műveleti attribútumokat, de a visszaadott adathalmaz csak azon LDAP bejegyzéseket és attribútumokat tartalmazza, amelyekhez a kérő megfelelő jogokkal rendelkezik. Az **ibm-allMembers** vagy **ibm-allGroups** attribútumot kérő felhasználónak jogosultsága kell, hogy legyen a csoport és a beágyazott csoportok **member** vagy **uniquemember** attribútumértékeihez ahhoz, hogy lássa a statikus tagokat, és végre kell tudnia hajtani a **memberURL** attribútum értékeként megadott keresést a dinamikus tagok megjelenítéséhez. Példák:

Hierarchia példák



Ebben a példában **m1** és **m2** a **g2** csoport member (tag) attribútumai. **g2** ACL-je a **user1** felhasználó számára engedi a "member" attribútum kiolvasását, de a **user 2** felhasználó nem éri el a "member" attribútum. A **g2** bejegyzés LDIF alakban így néz ki:

```

dn: cn=g2,cn=groups,o=ibm,c=us
objectclass: accessGroup
cn: g2
member: cn=m1,cn=users,o=ibm,c=us
member: cn=m2,cn=users,o=ibm,c=us
aclentry: access-id:cn=user1,cn=users,o=ibm,c=us:normal:rsc
aclentry: access-id:cn=user2,cn=users,o=ibm,c=us:normal:rsc:at.member:deny:rsc
  
```

A **g4** bejegyzés az alapértelmezett aclentry attribútumot használja, amely engedi **user1** és **user2** számára is, hogy kiolvassa a member attribútumát. A **g4** bejegyzés LDIF alakban:

```

dn: cn=g4, cn=groups,o=ibm,c=us
objectclass: accessGroup
cn: g4
member: cn=m5, cn=users,o=ibm,c=us
  
```

A **g5** bejegyzés egy dinamikus csoport, amely két tagját a memberURL attribútum alapján szerzi. A **g5** bejegyzés LDIF alakban:

```

dn: cn=g5, cn=groups,o=ibm,c=us
objectclass: container
objectclass: ibm-dynamicGroup
cn: g5
memberURL: ldap:///cn=users,o=ibm,c=us??sub?(|(cn=m3)(cn=m4))
  
```

Az **m3** és **m4** bejegyzések a **g5** csoport tagjai, mivel megfelelnek a **memberURL** attribútumnak. Az **m3** bejegyzés ACL-je engedi mind a **user1**, mind a **user2** felhasználó számára, hogy keresse. Az **m4** bejegyzés ACL-je nem engedi a **user2** felhasználó számára, hogy kikeresse. Az **m4** bejegyzés LDIF alakban:

```

dn: cn=m4, cn=users,o=ibm,c=us
objectclass: person
cn: m4
sn: four
aclentry: access-id:cn=user1,cn=users,o=ibm,c=us:normal:rsc
aclentry: access-id:cn=user2,cn=users,o=ibm,c=us
  
```

1. példa:

Az 1. felhasználó (user1) keresést hajt végre a **g1** csoport összes tagjának kikereséséhez. Mivel az 1. felhasználó jogosult az összes tag elérésére, mindegyiket vissza is kapja.

```

ldapsearch -D cn=user1,cn=users,o=ibm,c=us -w user1pwd -s base -b cn=g1,
cn=groups,o=ibm,c=us objectclass=* ibm-allmembers
  
```

```
cn=g1,cn=groups,o=ibm,c=us
ibm-allmembers: CN=M1,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M2,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M3,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M4,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M5,CN=USERS,O=IBM,C=US
```

2. példa:

A 2. felhasználó (user2) keresést hajt végre a **g1** csoport összes tagjának kikereséséhez. A 2. felhasználó nem jogosult az **m1** és **m2** tagok elérésére, ugyanis nem jogosult a **g2** csoport member attribútumának kiolvasására. A 2. felhasználó jogosult megtekinteni a **g4** csoport member attribútumát, ezért eléri az **m5** tagot. A 2. felhasználó végrehajthatja a **g5** csoport memberURL attribútumában megadott keresést az **m3** bejegyzés kikereséséhez, így ezt a tagot vissza is kapja, de nem hajthatja végre **m4** kikeresését.

```
ldapsearch -D cn=user2,cn=users,o=ibm,c=us -w user2pwd -s base -b cn=g1,
cn=groups,o=ibm,c=us objectclass=* ibm-allmembers
```

```
cn=g1,cn=groups,o=ibm,c=us
ibm-allmembers: CN=M3,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M5,CN=USERS,O=IBM,C=US
```

3. példa:

A 2. felhasználó végrehajt egy keresést, hogy megállapítsa, **m3** tagja-e a **g1** csoportnak. Mivel a 2. felhasználó jogosult e keresés végrehajtására, eredményül azt kapja, hogy **m3** valóban tagja a **g1** csoportnak.

```
ldapsearch -D cn=user2,cn=users,o=ibm,c=us -w user2pwd -s base -b cn=m3,
cn=users,o=ibm,c=us objectclass=* ibm-allgroups
```

```
cn=m3,cn=users,o=ibm,c=us
ibm-allgroups: CN=G1,CN=GROUPS,O=IBM,C=US
```

4. példa:

A 2. felhasználó végrehajt egy keresést, hogy megállapítsa, **m1** tagja-e a **g1** csoportnak. A 2. felhasználó nem jogosult a member attribútum kiolvasására, ezért a keresésből nem derül ki, hogy **m1** tagja-e a **g1** csoportnak.

```
ldapsearch -D cn=user2,cn=users,o=ibm,c=us -w user2pwd -s base -b
cn=m1,cn=users,o=ibm,c=us objectclass=* ibm-allgroups
```

```
cn=m1,cn=users,o=ibm,c=us
```

Csoport objektumosztályok beágyazott és dinamikus csoportokhoz

ibm-dynamicGroup

Ez a kiegészítő osztály lehetővé teszi a választható **memberURL** attribútum használatát. Egy strukturális osztállyal, például a **groupOfNames** osztállyal együtt használva egy statikus és dinamikus tagokat is tartalmazó hibrid csoport hozható létre.

ibm-dynamicMember

Ez a kiegészítő osztály lehetővé teszi a választható **ibm-group** attribútum használatát. Használja szűrőattribútumként dinamikus csoportok létrehozásához.

ibm-nestedGroup

Ez a kiegészítő osztály lehetővé teszi a választható **ibm-memberGroup** attribútum használatát. Egy strukturális osztállyal, például a **groupOfNames** osztállyal együtt használva a szülő csoport alá beágyazható alcsoportok hozhatók létre.

ibm-staticGroup

Ez a kiegészítő osztály lehetővé teszi a választható **member** attribútum használatát. Egy strukturális osztállyal, például a **groupOfURLs** osztállyal együtt használva egy statikus és dinamikus tagokat is tartalmazó hibrid csoport hozható létre.

Megjegyzés: Az **ibm-staticGroup** az egyetlen olyan osztály, amelyben a **member** attribútum *választható*, minden más osztályban a **member** attribútum legalább 1 tagot meg kell, hogy adjon.

Csoport attribútum típusok

ibm-allGroups

Jelzi, hogy egy bejegyzés mely csoportokhoz tartozik. Egy bejegyzés lehet tag közvetlenül a **member**, **uniqueMember** vagy **memberURL** attribútumokban felsorolva, vagy közvetve, az **ibm-memberGroup** attribútumon keresztül. Ez a **csak olvasható** műveleti attribútum nem használható keresési szűrőkben. Az **ibm-allGroups** attribútum összehasonlítási kérésekben használható, annak meghatározására, hogy egy adott bejegyzés tagja-e egy bizonyos csoportnak. Például annak megállapítása, hogy "cn=john smith,cn=users,o=my company" tagja-e a "cn=system administrators, o=my company" csoportnak:

```
rc = ldap_compare_s(ld, "cn=john smith,cn=users,o=my company", "ibm-allgroups",
    "cn=system administrators,o=my company");
```

ibm-allMembers

Egy csoport összes tagját tartalmazza. Egy bejegyzés lehet tag közvetlenül a **member**, **uniqueMember** vagy **memberURL** attribútumokban felsorolva, vagy közvetve, az **ibm-memberGroup** attribútumon keresztül. Ez a **csak olvasható** műveleti attribútum nem használható keresési szűrőkben. Az **ibm-allMembers** attribútum összehasonlítási kérésekben használható, annak meghatározására, hogy egy adott DN tagja-e egy bizonyos csoportnak. Például annak megállapítása, hogy "cn=john smith,cn=users,o=my company" tagja-e a "cn=system administrators, o=my company" csoportnak:

```
rc = ldap_compare_s(ld, "cn=system administrators,o=my company", "ibm-allmembers",
    "cn=john smith,cn=users,o=my company");
```

ibm-group

Az **ibm-dynamicMember** kiegészítő osztály által használt attribútum. Használatával tetszőleges értékek adhatók meg dinamikus csoportok tagságának szabályozásához. Például a "Biciklistak" érték felvételével a bejegyzés felvehető egy olyan dinamikus csoportba, amelynek **memberURL** attribútuma tartalmazza az "ibm-group=Biciklistak" szűrőt.

ibm-memberGroup

Az **ibm-nestedGroup** kiegészítő osztály által használt attribútum. Egy szülő csoport bejegyzés alcsoportjait azonosítja. Az ilyen alcsoportok tagjai a szülőcsoport tagjainak is számítanak az ACL-ek feldolgozásakor, illetve az **ibm-allMembers** és **ibm-allGroups** műveleti attribútumok szempontjából. Az alcsoport bejegyzések maguk *nem* tagok. A beágyazott tagság rekurzív.

member

A csoport egyes tagjainak megkülönböztetett nevét tartalmazza. Példa: member: cn=John Smith, dc=ibm, dc=com.

memberURL

A csoport egy tagjához rendelt URL-t határoz meg. Mindenféle típusú címkézett URL használható. Példa: memberURL: ldap:///cn=jsmith,dc=ibm,dc=com.

uniqueMember

Egy bejegyzéshez tartozó nevek egy csoportját azonosítja, ahol minden egyes névhez meg lett adva egy uniqueIdentifier (egyedi azonosító) az egyediség biztosítása érdekében. A uniqueMember értéke egy DN, amelyet a uniqueIdentifier követ. Példa: uniqueMember: cn=John Smith, dc=ibm, dc=com 17.

Szerepek

A szerep alapú felhatalmazás elvi kiegészítése a csoport alapú felhatalmazásnak, és sok esetben igen hasznos. A szerep tagjaként jogosultságot kap az illető egy adott feladat elvégzéséhez. Szemben a csoportokkal, a szerepek engedélyek implicit halmazát kapják. Nincs semmilyen beépített feltételezés, hogy milyen engedélyeket szerez meg (vagy veszít el) valaki egy csoport tagjaként.

A szerepek hasonlítanak abban a csoportokra, hogy szintén objektumként jelennek meg a címtárban. A szerepek azonban DN-ek csoportját is tartalmazzák. A hozzáférés-felügyeletben használt szerepeknek rendelkezniük kell egy 'AccessRole' nevű objektumosztállyal. Az 'Accessrole' objektumosztály a 'GroupOfNames' objektumosztály alosztálya.

Ha például van egy sor DN, mint mondjuk a "sys admin", akkor az ember azt gondolhatja elsősre, hogy ők a "sys admin csoport" (lévén a csoportok és a felhasználók a jogosultság-kezelésben legmegszokottabb típusok). Mivel azonban van egy sor engedély, amelyet a felhasználó a "sys admin" tagjaként várhatóan megkap, pontosabb "sys admin szerepként" emlegetni ezt a DN-halmazt.

Adminisztratív hozzáférés

Az IBM címtárszerver a következő fajta adminisztratív hozzáféréseket engedi meg:

- **Leképezett i5/OS adminisztrátor:** Egy leképezett felhasználóként hitelesített kliens (egy operációsrendszeri felhasználói profilt jelentő LDAP bejegyzés) *ALLOBJ és *IOSYSCFG speciális jogosultságokkal módosíthatja a címtárbeállításokat az LDAP csatolók (a cn=configuration subtree vagy a webadminisztrációs eszköz "Server administration" feladatai) segítségével, valamint LDAP adminisztrátorként működik az egyéb címtárbejegyzések (a DB2 valamelyik utótagjában vagy sémájában tárolt bejegyzések) tekintetében. Csak a leképezett i5/OS adminisztrátorok módosíthatják a szerverbeállításokat.
- **LDAP adminisztrátor:** Az IBM Directory Server megengedi egyetlen felhasználói azonosító (DN) használatát elsődleges LDAP szerveradminisztrátorként. Az iSeries szintén módot ad arra, hogy leképezett operációsrendszeri felhasználói profilok LDAP adminisztrátorok legyenek. Az LDAP szerveradminisztrátorok sokféle adminisztrációs feladatot hajthatnak végre, például kezelhetik a replikációs, séma- és címtárbejegyzéseket. További információk: "Adminisztrátori hozzáférés megadása leképezett felhasználóknak" oldalszám: 119.
- **Adminisztratív felhasználók csoportja:** Egy leképezett i5/OS adminisztrátor kijelölhet egyes felhasználókat, hogy azok tagjai legyenek az adminisztrációs csoportnak. A csoport tagjai bármilyen feladatot végrehajthatnak, mivel ugyanolyan adminisztrációs hozzáféréssel rendelkeznek, mint az LDAP szerveradminisztrátor.

Megjegyzés: Webes adminisztráció használatakor az adminisztrációs csoport tagjaihoz hozzá nem adott feladatok letiltásra kerülnek.

Az LDAP adminisztrátorok vagy adminisztrációs csoport tagok a következő szerveradminisztrációs feladatokat végezhetik el:

- Módosíthatják a saját jelszavukat
- Lezárhatják a kapcsolatokat
- Engedélyezhetik és módosíthatják a jelszó-irányelveket, kivéve a jelszótitkosítást, amelyet csak a leképezett i5/OS adminisztrátorok módosíthatnak.
- Kezelhetik az egyedi attribútumokat
- Kezelhetik a szerversémát
- Kezelhetik a replikációt, kivéve a replikációs tulajdonság feladatot (beleértve az elsődleges szerver kapcsolati megkülönböztetett nevét és jelszavát, valamint az alapértelmezett hivatkozást) - ezt csak a leképezett i5/OS adminisztrátor végezheti.

Az adminisztrációs csoport létrehozásával kapcsolatban információért lásd: "Adminisztrációs csoport kezelése" oldalszám: 120.

Proxy hitelesítés

A proxy hitelesítés a hitelesítés egy speciális formája. A proxy hitelesítési mechanizmus használatával egy kliensalkalmazás saját azonosságával is kapcsolódhat egy másik címtárhoz, de egy másik felhasználó nevében is hajthat végre műveleteket a cél címtár elérésére. A megbízható alkalmazások vagy felhasználók halmaza több felhasználó nevében is hozzáférhet a Directory Serverhez.

A proxy hitelesítési csoport tagjai bármelyik hitelesített jogosultságot felvehetik, kivéve az adminisztrátorét vagy az adminisztrációs csoport tagjait.

A proxy hitelesítési csoport a localhost vagy az IBMpolicies alatt is tárolható. Az IBMpolicies alatt tárolt proxy hitelesítési csoport replikálásra kerül, a localhost alatt tárolt nem. A proxy hitelesítési csoport a localhost és az IBMpolicies alatt is tárolható. Ha a proxy hitelesítési csoport ezen megkülönböztetett nevek egyike alatt sincs tárolva, akkor a szerver figyelmen kívül hagyja a csoport proxy részét, és normál csoportként kezeli azt.

| Példa: a client1 alkalmazáscsoport magas hozzáférési jogosultságokkal köthető a Directory Serverhez. A korlátozott
| jogosultságokkal rendelkező A felhasználó küld egy kérést a kliensalkalmazáshoz. Ha a kliens tagja a proxy hitelesítési
| csoportnak, akkor ahelyett, hogy client1 néven továbbítaná a kérést a Directory Servernek, A felhasználó néven fogja
| továbbítani, sokkal korlátozottabb jogosultsági szintek használatával. Ez azt jelenti, hogy ahelyett, hogy client1 néven
| hajtaná végre a kérést, az alkalmazáserver csak azokat az információkat érheti el vagy azokat a műveleteket hajthatja
| végre, amelyekre A felhasználó jogosult. A felhasználó proxyjaként vagy A felhasználó nevében fogja végrehajtani a
| kérést.

| **Megjegyzés:** Az attribútum tagnak rendelkeznie kell saját értékkel egy megkülönböztetett név formájában.
| Máskülönb érvénytelen DN szintaxis üzenet érkezik. Csoport DN nem lehet tag proxy hitelesítési
| csoportban.

| Adminisztrátorok vagy adminisztrációs csoporttagok nem lehetnek tagok proxy hitelesítési csoportban. A
| felülvizsgáló napló egyaránt feljegyzi a kapcsolati és proxy DN proxy hitelesítés használatával végrehajtott összes
| műveletét.

| További információk: "Proxy hitelesítési csoport kezelése" oldalszám: 123.

Hozzáférés-felügyeleti listák

A hozzáférés-felügyeleti listák (ACL-ek) az LDAP címtárban tárolt információ védelméhez biztosítanak eszközöket. A rendszergazdák az ACL-ek segítségével korlátozhatják a címtár különböző részeinek, vagy az egyes címtárbejegyzéseknek az elérését. A címtár egyes bejegyzéseinek és attribútumainak módosításai vezérelhetők ACL-ekkel. Egy adott bejegyzésre vagy attribútumra vonatkozó ACL megörökölhető a szülő bejegyzéstől, illetve megadható közvetlenül.

Célszerű a hozzáférés-felügyeleti stratégiát az objektumok és attribútumok elérésének beállításakor használható felhasználói csoportok létrehozásával kialakítani. A tulajdonjogot és a hozzáférést a fa lehető legmagasabb részén célszerű beállítani, és hagyni, hogy a vezérlési szabályok lefelé öröklődjenek a címtárfában.

A hozzáférés-felügyelethez kapcsolódó műveleti attribútumok - például az entryOwner, ownerSource, ownerPropagate, aclEntry, aclSource és aclPropagate attribútumok - szokatlanok abban az értelemben, hogy bár az egyes objektumokhoz vannak logikailag rendelve, értékeik függhetnek a címtárfa felsőbb részében található objektumoktól. Létrehozásuk módjától függően ezek az attribútumértékek lehetnek expliciten megadottak az objektumhoz, de öröklődhetnek is magasabb szintről.

A hozzáférés-felügyeleti modell kétféle attribútumot határoz meg: a Hozzáférés-felügyeleti információk (Access Control Information, ACI) és az entryOwner (bejegyzés tulajdonosa) adatokat. Az ACI határozza meg egy adott elemhez rendelt hozzáférési jogokat: azt, hogy milyen műveleteket hajthat végre a vonatkozó objektumokon. Az aclEntry és aclPropagate attribútumok az ACI meghatározásra vonatkoznak. Az entryOwner adatok határozzák meg, mely alanyok definiálják a társított bejegyzés objektum ACI-ját. Az entryOwner és ownerPropagate attribútumok az entryOwner meghatározásra vonatkoznak.

Kétféle hozzáférés-felügyeleti listából lehet választani: a szűrő alapú és a nem szűrő ACL-ek közül. A nem szűrő ACL-ek közvetlenül arra a címtárbejegyzésre vonatkoznak, amely őket tartalmazza, de továbbterjeszthetők nulla, vagy akár az összes leszármazott bejegyzésre. A szűrő alapú ACL-ek eltérnek abban, hogy szűrő alapú összehasonlítást használnak egy meghatározott objektumszűrő segítségével, hogy azonosítsák a célobjektumokat a tényleges rájuk vonatkozó hozzáférési jogosultságokkal.

ACL-ek használatával a rendszergazdák korlátozhatják a címtár egyes részeinek, akár meghatározott címtárbejegyzések elérését, illetve az attribútumnév vagy attribútum-hozzáférés osztály alapján az egyes bejegyzések attribútumaihoz hozzáférést. Az LDAP címtár minden egyes bejegyzéséhez tartozik egy sor hozzárendelt ACI. Az LDAP modellnek megfelelően az ACI és entryOwner információk is attribútum-érték párokként vannak reprezentálva. Az LDIF szintaxis használható ezen értékek leírására is. Az attribútumok:

- aclEntry
- aclPropagate

- `ibm-filterAclEntry`
- `ibm-filterAclInherit`
- `entryOwner`
- `ownerPropagate`

Az ACL-ek kezelésével kapcsolatos információk: "Hozzáférés-felügyeleti listák (ACL-ek) kezelése" oldalszám: 185.
További információk:

- "Szűrt ACL-ek"
- "Hozzáférés-felügyeleti attribútumok szintaxisa"
- "AclEntry és `ibm-filterAclEntry`" oldalszám: 58
- "EntryOwner" oldalszám: 61
- "Továbbadás" oldalszám: 61
- "Hozzáférés kiértékelése" oldalszám: 62
- "ACI-k és bejegyzéstulajdonosok megadása" oldalszám: 63
- "Az ACI és a bejegyzéstulajdonos értékek módosítása" oldalszám: 64
- "Az ACI és a bejegyzéstulajdonos értékek törlése" oldalszám: 67
- "Az ACI és a bejegyzéstulajdonos értékek lekérése" oldalszám: 67
- "Részfa-replikációs megfontolások" oldalszám: 67

Szűrt ACL-ek

A szűrő alapú ACL-ek szűrő alapú összehasonlítást használnak egy meghatározott objektumszűrő segítségével, hogy azonosítsák a célobjektumokat a tényleges rájuk vonatkozó hozzáférési jogosultságokkal.

A szűrő alapú ACL-ek jellegükénél fogva tovaterjednek minden összehasonlítással megfeleltetett objektumra a társított részében. Éppen ezért az `aclPropagate` attribútum, amely arra szolgál, hogy megállítsa a tovaterjedést a nem szűrt ACL-ek esetén, nem alkalmazható az új, szűrő alapú ACL-ekre.

Egy szűrő alapú ACL alapértelmezett viselkedése az, hogy összegyűlik a legalacsonyabb tartalmazó bejegyzéstől felfelé az öröklődési láncon, a DIT legmagasabb tartalmazó bejegyzéséig. A tényleges hozzáférési jogok az öt bejegyzésekhez megadott és elvett összes jog uniójaként kerülnek kiszámításra. Egy kivétel van erre a viselkedésre. A részfa-replikációs funkció használata és a jobb adminisztrációs irányítás érdekében létezik egy "plafon" (ceiling) attribútum, amelynek a szerepe, hogy megállítsa a jogok gyűjtését annál a bejegyzésnél, amely őt tartalmazza.

Egy új sor hozzáférés-felügyeleti attribútum szolgál kifejezetten a szűrő alapú ACL-ek támogatására ahelyett, hogy a szűrő alapú jellegzetességeket összeolvasztaná a rendszer a nem szűrt ACL-ekkel. Ezek az attribútumok:

- `ibm-filterAclEntry`
- `ibm-filterAclInherit`

Az `ibm-filterAclEntry` attribútum formátuma ugyanaz, mint az `aclEntry` attribútumé, de szerepel benne egy objektumszűrő elem. A hozzá tartozó "plafon" attribútum az `ibm-filterAclInherit`. Alapértelmezés szerint ez igaz értéket kap. Hamis értékre állítva megakadályozza a jogok további összegzését.

Hozzáférés-felügyeleti attribútumok szintaxisa

Az attribútumok mindegyike kezelhető az LDIF jelölés használatával. Az új, szűrő alapú ACL attribútumok a meglévő, nem szűrő alapú ACL attribútumok módosított változatai. Az alábbiakban megadjuk az ACI és az `entryOwner` attribútumok definícióját BNF formátumban:

```
<aclEntry> ::= <subject> [ ":" <rights> ]
```

```
<aclPropagate> ::= "true" | "false"
```

```
<ibm-filterAclEntry> ::= <subject> ":" <object filter> [ ":" <rights> ]
```

```
<ibm-filterAclInherit> ::= "true" | "false"
```

```

<entryOwner> ::= <subject>
<ownerPropagate> ::= "true" | "false"
<subject> ::= <subjectDnType> ':' <subjectDn> |
              <pseudoDn>
<subjectDnType> ::= "role" | "group" | "access-id"
<subjectDn> ::= <DN>
<DN> ::= megkülönböztetett név az RFC 2251, 4.1.3 rész szerint
<pseudoDn> ::= "group:cn=anybody" | "group:cn=authenticated" |
              "access-id:cn=this"
<object filter> ::= karaktorsorozat kereső szűrő az RFC 2254, 4. rész szerint
                  (a bővíthető illesztés nem támogatott).
<rights> ::= <accessList> [":" <rights> ]
<accessList> ::= <objectAccess> | <attributeAccess> |
                 <attributeClassAccess>
<objectAccess> ::= "object:" [<action> ":"] <objectPermissions>
<action> ::= "grant" | "deny"
<objectPermissions> ::= <objectPermission> [ <objectPermissions> ]
<objectPermission> ::= "a" | "d" | ""
<attributeAccess> ::= "at." <attributeName> ":" [<action> ":"]
                    <attributePermissions>
<attributeName> ::= attributeType név az RFC 2251, 4.1.4 rész szerint
                  (OID vagy alfanumerikus karaktorsorozat vezető
                  betűvel, "-" és ";" karakterek engedélyezettek)
<attributePermissions> ::= <attributePermission>
                          [<attributePermissions>]
<attributePermission> ::= "r" | "w" | "s" | "c" | ""
<attributeClassAccess> ::= <class> ":" [<action> ":"]
                          <attributePermissions>
<class> ::= "normal" | "sensitive" | "critical" | "system" | "restricted"

```

AclEntry és ibm-filterAclEntry

Alany: Egy alany (az objektumon műveletvégzéshez hozzáférést kérő entitás) egy DN (megkülönböztetett név) típus és egy DN kombinációjából áll. Az érvényes DN típusok: access-id, Group és Role.

A DN egy megadott access-id (hozzáférési azonosító), role (szerep) vagy group (csoport) bejegyzést azonosít. Például az alany lehet access-id: cn=personA, o=IBM, vagy group: cn=deptXYZ, o=IBM.

Mivel a mezők határoló karaktere a kettőspont (:), egy kettőspontokat tartalmazó DN-t idézőjelek ("") közé kell írni. Ha a DN már tartalmaz idézőjelek közötti karaktereket, akkor ezeknek a karaktereknek a beírásához balra döntött törtvonalakat (\) kell használni.

Minden címtárcsoport használható hozzáférés-felügyeletre.

Megjegyzés: Az **AccessGroup**, **GroupOfNames**, **GroupofUniqueNames** vagy **groupOfURLs** strukturális objektumosztályok, illetve az **ibm-dynamicGroup**, **ibm-staticGroup** kiegészítő objektumosztály bármely csoportja használható hozzáférés-felügyeletre.

A hozzáférés-felügyelet terén használt másik DN típus a szerep. Bár a szerepek és a csoportok megvalósításukban hasonlóak, elvben különböznek. Amikor egy felhasználó hozzáférhető egy szerephez, akkor közvetetten elvárja, hogy a szerephez tartozó feladat elvégzéséhez a szükséges jogosultságok be vannak már állítva. Egy csoport tagjaként nincs semmilyen beépített feltételezés, hogy valaki milyen engedélyeket szerez meg (vagy veszít el).

A szerepek hasonlítanak abban a csoportokra, hogy szintén objektumként jelennek meg a címtárban. A szerepek azonban DN-ek csoportját is tartalmazzák. A hozzáférés-felügyeletben használt szerepeknek rendelkezniük kell egy **AccessRole** nevű objektumosztállyal.

Pszedo DN: Az LDAP címtár számos pszedo DN-t tartalmaz. Ezek célja, hogy nagyszámú, hasonló jellemzőkkel bíró DN-re hivatkozzanak, amelyek valamilyen jellemzője közös, akár az elvégzett művelettel, akár a művelet céljául szolgáló objektummal kapcsolatosan.

Jelenleg három pszedo DN használható:

group:cn=anybody

Minden alany, azok is, amelyek még nincsenek hitelesítve. Egy csoportba minden felhasználó automatikusan beletartozik.

group:cn=authenticated

A címtárhoz még nem hitelesített DN-ek csoportja. A hitelesítés módszere nem számít.

access-id:cn=this

Ez a DN a bindDN attribútumra vonatkozik, amelyik annak a célobjektumnak a DN-jével egyezik meg, amilyen a művelet végrehajtásra kerül.

Objektumszűrő: Ez a paraméter csak a szűrt ACL-ekre vonatkozik. Az objektumszűrő formátuma az RFC 2254-ben definiált karaktersorozat keresési szűrő. Mivel a célobjektum már ismert, a karaktersorozat nem kerül használatra tényleges keresés végrehajtásához. Ehelyett a kérdéses célobjektumon végrehajtott szűrő alapú keresés szolgál annak meghatározására, hogy egy adott **ibm-filterAclEntry** érték halmaz vonatkozik-e rá.

Jogok: A hozzáférési jogok vonatkozhatnak egy teljes objektumra vagy az objektum egy attribútumára. Az LDAP hozzáférési jogok elhatároltak. Egy jog nem von maga után semmilyen másik jogot. A jogok együttesen is megadhatók, hogy biztosítsák a kívánt jogosultságokat (lásd az alábbi listát). A jogok értelme lehet nem megadott, amely azt jelzi, hogy a az alany nem kapott a célobjektumhoz hozzáférési jogokat. A jogok három részből állnak:

Művelet:

A lehetséges értékek **grant** (megad) és a **deny** (tagad). Ha ez a mező nincs jelen, akkor az alapértelmezett érték a **grant**.

Jogosultságok:

Egy címtárobjektumon hat alapművelet végezhető el. E műveletek mindegyikéhez a rendszer fogja az ACI jogosultságok alap halmazát. Ezek az alábbiak: bejegyzés felvétele, bejegyzés törlése, attribútumérték olvasása és írása, attribútum keresése, illetve egy másik attribútumértékkel összehasonlítása.

A lehetséges attribútum-jogosultságok a következők: olvasás (read, r), írás (write, w), keresés (search, s) és összehasonlítás (compare, c). Az objektumjogok pedig az objektum teljes egészére vonatkoznak. Ezek a következők: leszármazott bejegyzések felvétele (add child entries, a) és a jelen bejegyzés törlése (delete this entry, d).

Az alábbi táblázat összefoglalja, milyen jogosultságokra van szükség az egyes LDAP műveletek elvégzéséhez.

Művelet	Szükséges engedély
ldapadd	hozzáadás (a szülőhöz)
ldapdelete	törlés (az objektumhoz)

Művelet	Szükséges engedély
ldapmodify	írás (a módosított attribútumokhoz)
ldapsearch	<ul style="list-style-type: none"> • keresés, olvasás (az RDN attribútumaihoz) • keresés (a keresési szűrőben megadott attribútumokhoz) • keresés (a csak nevekkkel visszaadott attribútumokhoz) • keresés, olvasás (az értékekkel visszaadott attribútumokhoz)
ldapmodrdn	írás (az RDN attribútumokhoz)
ldapcompare	összehasonlítás (az összehasonlított attribútumokhoz)

Megjegyzés: Keresési műveletek esetén az alannak keresési jogokkal kell rendelkeznie a keresési szűrő összes attribútumához, vagy különben egy bejegyzés sem kerül visszaadásra. A keresésből visszaadott bejegyzésekre az alannak keresés és olvasás jogokkal kell rendelkeznie a visszaadott bejegyzések RDN-jének összes attribútumához, vagy különben a bejegyzések nem kerülnek visszaadásra.

Hozzáférési cél:

Ezek a jogok vonatkozhatnak a teljes objektumra (leszármazott bejegyzések felvétele, jelen bejegyzés törlése), a bejegyzés egy egyedi attribútumára, vagy attribútumok csoportjára (attribútum-hozzáférési osztályokra), az alábbiakban leírtak szerint.

A hasonló hozzáférési jogosultságokat igénylő attribútumok csoportokba vannak szervezve. Az attribútumok a címtárséma fájl attribútumosztályaira vannak leképezve. Ezek az osztályok diszkréték: az egyik osztály elérése nem jelent hozzáférést egy másik osztályhoz. A jogosultságok beállítása az attribútumosztály egészére vonatkozóan történik. Egy adott attribútumosztályhoz megadott jogok az osztály összes attribútumára érvényesek lesznek, kivéve, ha az egyes attribútumokhoz külön lettek megadva jogok.

Az IBM három attribútumosztályt határozott meg a felhasználói attribútumok kiértékeléséhez: a **normal** (normál), a **sensitive** (érzékeny) és a **critical** (kritikus) osztályokat. Például a **commonName** attribútum a normál osztályba tartozik, míg a **userpassword** (jelszó) attribútum a kritikusba. A felhasználó által megadott attribútumok a normál osztályba tartoznak, kivéve, ha másképp lettek megadva.

Két további osztály is definiálva van: a **system** (rendszer) és a **restricted** (korlátozott). A **system** osztály attribútumai:

- **creatorsName**
- **modifiersName**
- **createTimestamp**
- **modifyTimestamp**
- **ownerSource**
- **aclSource**

Ezeket az attribútumokat az LDAP szerver kezeli és a címtárfelhasználók csak olvashatják őket. Az **OwnerSource** és az **aclSource** a Terjesztés fejezetben vannak leírva ("Továbbadás" oldalszám: 61).

A **restricted** attribútumosztály a hozzáférés-felügyeletet határozza meg:

- **aclEntry**
- **aclPropagate**
- **entryOwner**
- **ownerPropagate**
- **ibm-filterAclEntry**
- **ibm-filterAclInherit**
- **ibm-effectiveAcl**

Minden felhasználó olvashatja a restricted (korlátozott) attribútumokat, de csak az **entryOwner** felhasználók hozhatják létre, módosíthatják és törölhetik ezeket az attribútumokat.

Megjegyzés: Az **ibm-effectiveAcl** attribútum csak olvasható.

EntryOwner

A bejegyzések tulajdonosai teljeskörű jogosultsággal rendelkeznek: minden műveletet végrehajthatnak az objektumon, az **aclEntry** attribútum értékétől függetlenül. Ezenfelül a bejegyzéstulajdonosok az egyetlenek, akik jogosultak az objektum **aclEntry** attribútumainak kezelésére. Az **EntryOwner** egy hozzáférés-felügyeleti alany, megadható egyénekkkel, csoportokkal vagy szerepekkel.

Megjegyzés: A címtáradminisztrátor az egyik **entryOwner**, aki a címtár összes bejegyzésének tulajdonosa alapértelmezés szerint és a címtáradminisztrátor **entryOwnership** tulajdonsága nem is törölhető egyetlen objektumból sem.

Továbbadás

Az **aclEntry** tulajdonsággal rendelkező bejegyzéseket úgy tekintjük, hogy explicit **aclEntry** attribútummal bírnak. Hasonlóan, ha egy adott bejegyzéshez van megadva **entryOwner** attribútum, akkor a bejegyzésnek van explicit tulajdonosa. A kettő nincs összekapcsolva: egy explicit tulajdonosú bejegyzésnek nincs feltétlenül explicit **aclEntry** attribútuma, és egy explicit **aclEntry** attribútummal bíró bejegyzésnek nem biztos, hogy van explicit tulajdonosa. Ha az értékek valamelyike nincs explicite megadva egy bejegyzéshez, akkor az a hiányzó értéket öröklő a címtárfa egy felsőbb szintű (ős-) csomópontjától.

Az egyes explicit **aclEntry** és **entryOwner** attribútumok azokra a bejegyzésekre vonatkoznak, amelyekre be lettek állítva. Ezenfelül az értékek minden olyan leszármazottra is érvényesek, amelyekhez nincs külön megadva más érték. Ilyenkor arról beszélünk, hogy az értékek "terjednek"; tovaterjednek a címtárfán belül. Egy adott érték terjedése addig tart, amíg egy másik terjedő értékbe nem ütközik.

Megjegyzés: A szűrő alapú ACL-ek nem terjednek a nem szűrő alapúakhoz hasonló módon. Jelleműknél fogva tovaterjednek minden összehasonlítással megfeleltetett objektumra a társított részfában. A különbségekről további információk: "Szűrő ACL-ek" oldalszám: 57.

Az **aclEntry** és az **entryOwner** attribútumok beállíthatók csak egy adott bejegyzésre, a terjedést "false" értékre állítva, vagy egy bejegyzésre és az alatta levő részfára, a terjedést "true" értékre állítva. Bár az **aclEntry** és az **entryOwner** is tovaterjedhet, nincsenek összekapcsolva e téren semmilyen módon.

Az **aclEntry** és az **entryOwner** attribútumok engedik több érték használatát, de a terjedési attribútumok (az **aclPropagate** és az **ownerPropagate**) csak egy értéket tartalmazhatnak ugyanazon bejegyzés összes **aclEntry** és **entryOwner** attribútumértékéhez.

Az **aclSource** és **ownerSource** rendszerattribútumok tartalmazzák annak a csomópontnak a DN-jét, amelytől kezdve az **aclEntry** illetve **entryOwner** attribútumok kiértékelésre kerülnek. Ha nincs ilyen csomópont, akkor a **default** érték kerül hozzárendelésre.

Egy objektum hatályos hozzáférés-felügyeleti meghatározásai a következő módon állapíthatók meg:

- Ha van az objektumhoz rendelve explicit hozzáférés-felügyeleti attribútumok egy halmaza, akkor ezek képezik az objektum hozzáférés-felügyeleti meghatározását.
- Ha nincsenek explicit módon megadott hozzáférés-felügyeleti attribútumok, akkor el kell indulni a címtárfán felfelé, amíg találunk egy szülő (ős-) csomópontot, amelyhez tartoznak tovaterjedő hozzáférés-felügyeleti attribútumok.
- Ha nincs ilyen ős csomópont, akkor az alany az alábbi leírt alapértelmezett hozzáférési jogokat kapja meg.

A bejegyzés tulajdonosa a címtár adminisztrátora. A **cn=anybody** (összes felhasználó) pszeudocsoport olvasási, keresési és összehasonlítási hozzáférést kap a **normal** hozzáférési osztályhoz.

Hozzáférés kiértékelése

Egy adott művelet hozzáféréseinek megadása vagy megtagadása attól függ, hogy az alany kapcsolódási (bind) DN-je milyen jogokkal rendelkezik a célobjektumhoz. A feldolgozás azonnal leáll, ha a hozzáférés megállapítható.

A hozzáférés ellenőrzése először a hatályos **entryOwnership** és **ACI** meghatározás kikeresésével kezdődik, a bejegyzés tulajdonosának ellenőrzésével, majd az ACI értékeinek kiszámításával.

A szűrő alapú ACL-ek összegyűjtik a jogokat a legalacsonyabb tartalmazó bejegyzéstől felfelé az öröklődési láncon, a DIT legmagasabb tartalmazó bejegyzéséig. A tényleges hozzáférési jogok az ős bejegyzésekhez megadott és elvett összes jog uniójaként kerülnek kiszámításra. A szűrő alapú ACL-ek hatályos hozzáférési jogosultságának kiszámítása a meglévő egyediségi és összegzési szabályok alapján történik.

A szűrő alapú és a nem szűrő alapú attribútumok kölcsönösen kizárják egymást az őket tartalmazó címtárbejegyzésen belül. Mindkét fajta attribútumtípus nem helyezhető el ugyanazon a bejegyzésen, ez a megszorítások megsértésének számít. Ha ez az állapot lépne fel, akkor a címtárbejegyzés létrehozása vagy frissítése meghiúsul.

A hatályos hozzáférési jogok kiszámításakor az ősök láncában elsőként felismert ACL típus fogja meghatározni a számítás módját. Szűrő alapú módban a nem szűrő alapú ACL-ek figyelmen kívül maradnak a hatályos hozzáférési jogok kiszámítása során. Hasonlóan, nem szűrő alapú módban a szűrő alapú ACL-ek figyelmen kívül maradnak a hatályos hozzáférési jogok kiszámítása során.

A szűrő alapú ACL-ek összeadódásának korlátozása érdekében beállítható az **ibm-filterAclInherit** attribútum "false" értékkel egy adott részfán belül az **ibm-filterAclEntry** attribútum legmagasabb és legalacsonyabb előfordulása közötti bármely bejegyzésen. Ennek hatására a célobjektum őseinek láncában a bejegyzés felett található **ibm-filterAclEntry** attribútumok figyelmen kívül maradnak.

Szűrő alapú ACL módban, ha egy szűrő alapú ACL sem vonatkozik a bejegyzésre, akkor az alapértelmezett ACL-t használja a rendszer (a cn=anybody pszeudocsoport olvasási, keresési és összehasonlítási hozzáférést kap a normal hozzáférési osztályhoz). Ez a helyzet akkor fordulhat elő, ha az elért bejegyzés nem felel meg az **ibm-filterAclEntry** értékekben megadott szűrők egyikének sem. Ha nem akarja, hogy ez az alapértelmezett hozzáférés-felügyelet bekapcsoljon, akkor adjon meg egy alapértelmezett szűrő ACL-t:

```
ibm-filterAclEntry: group:cn=anybody:(objectclass=*):
```

Ez a példa semmilyen hozzáférést nem engedélyez. Módosítsa tetszés szerint, hogy a kívánt jogokat adja meg.

Alapértelmezés szerint a címtáradminisztrátor, az elsődleges szerver és az egyenrangú szerver (replikációhoz) teljes hozzáférést kap a címtárhoz, kivéve a rendszerattribútumok írását. Más bejegyzéstulajdonosok (**entryOwner**) teljes hozzáférést kapnak a saját objektumaikhoz, kivéve a rendszerattribútumok írását. Minden felhasználó olvasási hozzáférést kap a rendszer (system) és a korlátozott (restricted) attribútumokhoz. Ezek az előre meghatározott jogok nem módosíthatók. Ha a kérő alany **entryOwnership** tulajdonsággal rendelkezik, akkor a hozzáférés a fenti alapértelmezett beállítások alapján kerül meghatározásra, és a feldolgozás leáll.

Ha a kérő alany nem bejegyzéstulajdonos (entryOwner), akkor a rendszer ellenőrzi az objektumbejegyzések ACI értékeit. A célobjektumnak az ACI-k által meghatározott hozzáférési jogainak kiszámítása az egyediségi és az összegzési szabályok által történik.

Egyediségi szabály

A leegyedibb aclEntry meghatározások kerülnek használatra a felhasználónak megadott/tőle megtagadott jogok kiértékelésében. Az egyediségi szintek:

- Az Access-id egyedibb, mint a csoport vagy szerep. A csoportok és szerepek azonos szintnek számítanak.
- Ugyanazon **dnType** szinten belül az egyedi attribútumszintű jogok egyedibbnek számítanak, mint az attribútumosztály szintű jogok.
- Ugyanazon attribútumon vagy attribútumosztályon belül a **deny** (tiltás) egyedibbnek számít, mint a **grant** (engedélyezés).

Összegzési szabály

Az alanyok adott egyforma egyediségű jogok összegződnek. Ha nem állapítható meg ugyanazon az egyediségi szinten belül a hozzáférés, akkor a kevésbé egyedi szint hozzáférési definícióit alkalmazza a rendszer. Ha a hozzáférés nem állapítható meg az összes megadott ACI után sem, akkor a hozzáférés megtagadásra kerül.

Megjegyzés: Ha a rendszer talál egy access-id szintű **aclEntry** attribútumot a hozzáférés kiértékelése közben, akkor a csoport szintű **aclEntry** attribútumok már nem kerülnek kiértékelésre. Kivétel, ha az egyező access-id szint **aclEntry** attribútumai mind `cn=this` mellett vannak megadva. Ebben az esetben az összes egyező csoport **aclEntry** is bekerül a kiértékelésbe.

Más szavakkal, ha az objektumbejegyzésen belül egy megadott ACI bejegyzés tartalmaz a kapcsolódási (bind) DN-nel egyező access-id alany DN-t, akkor a jogok először ezen **aclEntry** alapján kerülnek kiértékelésre. Ugyanazon alany DN esetében, ha egyező attribútumszintű jogok vannak megadva, akkor azok felülbírálják az attribútumosztály szintű jogokat. Ugyanazon attribútum vagy attribútumosztály szintű meghatározáson belül, ha ütközések vannak, akkor a jogok tiltása erősebb a jogok megadásánál.

Megjegyzés: Egy megadott nullértékű jog megakadályozza a kevésbé egyedi jogmeghatározások kiértékelését.

Ha a hozzáférés még mindig nem állapítható meg, és az összes megtalált egyező **aclEntry** attribútum `"cn=this"` névvel van megadva, akkor a csoporttagságok is kiértékelésre kerülnek. Ha a felhasználó egynél több csoporthoz tartozik, akkor az összes csoport összesített jogait kapja meg. Ezenfelül a felhasználó automatikusan tagja a `cn=Anybody` csoportnak és - hitelesített csatlakozás esetén - a `cn=Authenticated` csoportnak is. Ha a csoportokhoz jogok vannak adva, akkor a felhasználó megkapja ezeket a megadott jogokat.

Megjegyzés: A csoport- és szereptagság kapcsolódáskor kerül kiértékelésre, és a következő kapcsolódásig, vagy a szétkapcsolási kérésig tart. A beágyazott csoportok és szerepek (vagyis amikor egy csoport vagy szerep egy másik csoport vagy szerep tagja) nem kerülnek feloldásra a tagság megállapításakor, sem a hozzáférés kiértékelésekor.

Tegyük fel például, hogy `attribute1` a `"sensitive"` attribútumosztályba tartozik, és a `cn=Person A, o=IBM` felhasználó pedig a `group1` és `group2` csoportok tagja, valamint a következő **aclEntry** attribútumok kerültek megadásra:

1. **aclEntry:** `access-id: cn=Person A, o=IBM: at.attribute1:grant:rsc:sensitive:deny:rsc`
2. **aclEntry:** `group: cn=group1, o=IBM:critical:deny:rwc`
3. **aclEntry:** `group: cn=group2, o=IBM:critical:grant:r:normal:grant:rsc`

Ez a felhasználó a következő jogokat kapja:

- `'rsc'` szintű hozzáférést az `attribute1` attribútumhoz (az 1. attribútumszintű meghatározás felülbírálja az attribútumosztály szintű meghatározást).
- Semmilyen egyéb hozzáférést nem kap a célobjektum többi `"sensitive"` osztályú attribútumához (1. miatt).
- Semmilyen egyéb jogot nem kap (2 és 3 NEM kerülnek be a hozzáférés kiértékelésébe).

Egy másik példa, a következő **aclEntry** attribútumokkal:

1. **aclEntry:** `access-id: cn=this: sensitive`
2. **aclEntry:** `group: cn=group1, o=IBM: sensitive:grant:rsc: normal:grant:rsc`

A felhasználó jogai:

- hozzáférés tiltva a `"sensitive"` osztályú attribútumokhoz (1. miatt: az access-id-hez adott nullérték megakadályozza a `group1` csoportnak a `"sensitive"` osztályú attribútumokhoz adott jogainak érvényesülését).
- `'rsc'` hozzáférés a `normal` osztályú attribútumokhoz (2. miatt).

ACI-k és bejegyzéstulajdonosok megadása

A következő két példa bemutatja egy adminisztrációs altartomány kialakítását. Az első példában egyetlen felhasználó lesz a teljes tartomány tulajdonosa (`entryOwner`). A második példában egy csoport kapja az `entryOwner` attribútumot.

```
entryOwner: access-id:cn=Person A,o=IBM
ownerPropagate: true
```

```
entryOwner: group:cn=System Owners, o=IBM
ownerPropagate: true
```

A következő példa azt mutatja be, hogy egy "cn=Person 1, o=IBM" access-id olvasási, keresési és összehasonlítási jogokat kap az attribute1 attribútumhoz. A jog a teljes részfa (a jelen ACI alatt) összes olyan csomópontjára kiterjed, amelyre teljesül az "(objectclass=groupOfNames)" összehasonlítási szűrő. Az ős csomópontok egyező ibm-filteraclentry attribútumainak összeadódása le lett tiltva ennél a bejegyzésnél (az ibm-filterAclInherit attribútum "false" értékre lett állítva).

```
ibm-filterAclEntry: access-id:cn=Person 1,o=IBM:(objectclass=groupOfNames):
                    at.attribute1:grant:rsc
```

```
ibm-filterAclInherit: false
```

A következő példa azt mutatja be, hogy a "cn=Dept XYZ, o=IBM" csoport olvasási, keresési és összehasonlítási jogokat kap az attribute1 attribútumhoz. A jogok a jelen ACI-t tartalmazó csomópont alatti teljes részfára vonatkoznak.

```
aclEntry: group:cn=Dept XYZ,o=IBM:at.attribute1:grant:rsc
aclPropagate: true
```

A következő példa azt mutatja be, hogy a "cn=System Admins,o=IBM" szerep jogokat kap az adott csomópont alatt objektumok felvételére, valamint olvasási, keresési és összehasonlítási jogokat kap az attribute2 attribútumhoz és a "critical" attribútumosztályhoz. A jogosultság csak a jelen ACI-t tartalmazó csomópontra vonatkozik.

```
aclEntry: role:cn=System Admins,o=IBM:object:grant:a:at.
          attribute2:grant:rsc:critical:grant:rsc
aclPropagate: false
```

Az ACI és a bejegyzéstulajdonos értékek módosítása

Modify-replace

A modify-replace a többi attribútumhoz hasonlóan működik. Ha az attribútumérték nem létezik, akkor létrehozza az értéket. Ha az attribútumérték létezik, akkor lecseréli az értékét.

Rendelkezzen egy bejegyzés a következő ACI-kkel:

```
aclEntry: group:cn=Dept ABC,o=IBM:normal:grant:rsc
aclPropagate: true
```

és hajtsuk végre a következő változást:

```
dn:
cn=valamilyen bejegyzés
changetype: modify
replace: aclEntry
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

Az eredményül kapott ACI:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
aclPropagate: true
```

A Dept ABC ACI értékei a csere miatt elvesztek.

Rendelkezzen egy bejegyzés a következő ACI-kkel:

```
ibm-filterAclEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC):normal
                    :grant:rsc
ibm-filterAclInherit: true
```

és hajtsuk végre a következő változásokat:

```
dn: cn=valamilyen bejegyzés
changetype: modify
replace: ibm-filterAclEntry
```



```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                    :grant:rsc
```

```
dn: cn=valamilyen bejegyzés
changetype: modify
replace: ibm-filterAclInherit
ibm-filterAclInherit: false
```

Az eredményül kapott ACI:

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                    :grant:rsc
ibm-filterAclInherit: false
```

A Dept ABC ACI értékei a csere miatt elvesztek.

Modify-add

Egy ldapmodify-add művelet során, ha az ACI vagy az entryOwner nem létezik, akkor az ACI vagy entryOwner létrehozásra kerül a megadott értékekkel. Ha az ACI vagy az entryOwner létezik, akkor a megadott értékek hozzáadásra kerülnek a megadott ACI vagy entryOwner attribútumhoz. Például az alábbi ACI esetén:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

a következő módosítás:

```
dn: cn=valamilyen bejegyzés
changetype: modify
add: aclEntry
aclEntry: group:cn=Dept ABC,o=IBM:at.attribute1:grant:rsc
```

a következő többértékű aclEntry attribútumot eredményezi:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
aclEntry: group:cn=Dept ABC,o=IBM:at.attribute1:grant:rsc
```

Például az alábbi ACI esetén:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                    :grant:rsc
```

a következő módosítás:

```
dn: cn=valamilyen bejegyzés
changetype: modify
add: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC)
                    :at.attribute1:grant:rsc
```

a következő többértékű aclEntry attribútumot eredményezi:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                    :grant:rsc
ibm-filterAclEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC):at.attribute1
                    :grant:rsc
```

Az ugyanazon az attribútumnak vagy attribútumosztálynak megadott jogok alapvető építőelemnek számítanak és a műveletek a minősítőik. Ha ugyanaz a jog egynél többször kerül megadásra, csak egy érték tárolódik. Ha ugyanaz a jog egynél többször kerül megadásra más értékekkel, akkor csak az utolsó érték tárolódik. Ha az eredményül kapott jog mező üres (""), akkor ez a jog érték nullértékre lesz állítva, a művelet érték pedig **grant** (megadás) lesz..

Például az alábbi ACI esetén:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

a következő módosítás:

```
dn: cn=valamilyen bejegyzés
changetype: modify
add: aclEntry
aclEntry: group:cn=Dept XYZ,o=IBM:normal:deny:r:critical:deny::sensitive
:grant:r
```

a következő aclEntry attribútumot eredményezi:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:sc:normal:deny:r:critical
:grant::sensitive:grant:r
```

Például az alábbi ACI esetén:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
:grant:rsc
```

a következő módosítás:

```
dn: cn=valamilyen bejegyzés
changetype: modify
add: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
:deny:r:critical:deny::sensitive:grant:r
```

a következő aclEntry attribútumot eredményezi:

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
:grant:sc:normal:deny:r:critical:grant::sensitive
:grant:r
```

Modify-delete

Egy adott ACI érték törléséhez használja a szabályos ldapmodify-delete szintaxist.

A következő ACI esetén:

```
aclEntry: group:cn=Dept XYZ,o=IBM:object:grant:ad
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rWSC
```

```
dn: cn=valamilyen bejegyzés
changetype: modify
delete: aclEntry
aclEntry: group:cn=Dept XYZ,o=IBM:object:grant:ad
```

az alábbi maradék ACI-t eredményezi:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rWSC
```

A következő ACI esetén:

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):object
:grant:ad
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
:grant:rWSC
```

```
dn: cn=valamilyen bejegyzés
changetype: modify
delete: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):object
:grant:ad
```

az alábbi maradék ACI-t eredményezi:

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
:grant:rWSC
```

Egy nem létező ACI vagy entryOwner érték törlése, változatlan ACI vagy entryOwner értéket eredményez, valamint egy visszatérési kódot, hogy az attribútumérték nem létezik.

Az ACI és a bejegyzéstulajdonos értékek törlése

Az entryOwner az ldapmodify-delete művelettel törölhető:

```
dn: cn=valamilyen bejegyzés
changetype: modify
delete: entryOwner
```

Ebben az esetben a bejegyzésnek ezután nem lesz explicit módon megadott entryOwner attribútuma. Automatikusan törlésre kerül az ownerPropagate attribútum is. Ez a bejegyzés ezután tulajdonosát (entryOwner) a címtárfa felsőbb szintjéről, a terjedési szabályoknak megfelelően kapja meg.

Ugyanígy a teljes aclEntry is törölhető:

```
dn: cn=valamilyen bejegyzés
changetype: modify
delete: aclEntry
```

Egy bejegyzés utolsó ACI vagy entryOwner értékének törlése nem ugyanaz, mint az ACI vagy az entryOwner attribútum törlése. Egy bejegyzésnek lehet ACI vagy entryOwner attribútuma értékek nélkül. Ebben az esetben semmi nem kerül visszaadásra a kliensnek, ha az lekérdezi az ACI vagy az entryOwner értékét és a beállítás tovább is terjed a leszármazott csomópontokra, amíg felül nem bírálódik. A senki által el nem érhető, összeköttetés nélküli bejegyzések elkerülése érdekében a címtáradminisztrátornak mindig teljeskörű jogosultsága van egy bejegyzéshez, még akkor is, ha a bejegyzés ACI vagy entryOwner értéke egyébként üres.

Az ACI és a bejegyzéstulajdonos értékek lekérése

A hatályos ACI és entryOwner értékek lekérhetők a kívánt ACL vagy entryOwner attribútumok megadásával egy keresésben. Például az alábbi keresés:

```
ldapsearch -b "cn=object A, o=ibm" -s base "objectclass=*"
aclentry aclpropagate aclsource entryowner ownerpropagate ownersource
ibm-filterAclEntry ibm-filterAclInherit ibm-effectiveAcl
```

visszaadja az összes ACL és entryOwner információkat, amelyek az "object A" nevű objektum hozzáféréseinek kiértékelésében felhasználásra kerülnek. Ügyeljen arra, hogy a visszaadott értékek nem feltétlenül néznek ki pontosan ugyanúgy, mint ahogy először megadásra kerültek. Az értékek az eredeti forma egyenértékű megfelelői.

Csak az ibm-filterAclEntry attribútumra keresve kizárólag az adott bejegyzés egyedi értékei kerülnek visszaadásra.

Az ibm-effectiveAcl nevű csak olvasható attribútum szolgál az összesített hatályos hozzáférési jogok megjelenítésére. Az ibm-effectiveAcl attribútumra megadott keresés a célobjektumra érvényes hatályos hozzáférési jogokat adja vissza, szűrő vagy nem szűrő ACL-ek alapján, attól függően, hogyan kerültek terjesztésre a címtár-információs fán (DIT) belül.

Mivel a szűrő alapú ACL-ek számos ősből származhatnak, az aclSource attribútum a társított források listáját adja vissza.

Részfa-replikációs megfontolások

Ahhoz, hogy a szűrő alapú hozzáférés bekerüljön a részfa replikációjába, az összes ibm-filterAclEntry attribútumnak a hozzá tartozó ibm-replicationContext bejegyzés szintjén vagy alatta kell szerepelnie.

Mivel a hatályos hozzáférés nem összegezhető a replikált részfa feletti szülő (ős) bejegyzések alapján, az ibm-filterAclInherit attribútumot **false** értékre kell állítani és a hozzá tartozó ibm-replicationContext bejegyzésben kell lennie.

LDAP címtárobjektumok 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 hozzáférés-felügyeleti 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 Directory Server 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.

A tulajdonosi jellemzők kezelésével kapcsolatos további információk: "Címtárbejegyzések kezelése" oldalszám: 168.

Jelszó-irányelvek

LDAP szervereket használva hitelesítéshez, fontos, hogy az LDAP szerver támogasson a jelszavak lejáratára, a meghiúsult bejelentkezési kísérletekre, valamint a jelszósabályokra vonatkozó irányelveket. A Directory Server konfigurálható támogatást nyújt mindhárom fajta irányelvhez. Az irányelv minden címtárbejegyzésre alkalmazható, amelynek van `userPassword` attribútuma. Nem adható meg egyfajta irányelv egy felhasználócsoporthoz és másfajta irányelvek egy másikhoz. A Directory Server ezenfelül biztosít egy mechanizmust a kliensek számára a jelszó-irányelvekkel kapcsolatos feltételek (például hogy a jelszó három nap múlva lejár) megismeréséhez, valamint egy sor műveleti attribútumot, amelyek alapján az adminisztrátor keresni tud például olyan dolgokat, mint a lejárt jelszavú felhasználók vagy a letiltott fiókok.

További információk a jelszó-irányelv tulajdonságokról: "Jelszavak kezelése" oldalszám: 150.

Beállítások

A szerver jelszavakkal kapcsolatos viselkedése az alábbi területeken állítható be:

- Egy globális "be/ki" kapcsoló a jelszó-irányelvek be- és kikapcsolásához
- Szabályok a jelszavak módosításához:
 - A felhasználók maguk módosíthatják saját jelszavaikat. Ez az irányelv a hozzáférés-felügyeleti beállítások mellett érvényesül. Vagyis a hozzáférés-felügyeletnek jogokat kell adnia a felhasználónak a `userPassword` attribútum módosításához, valamint a jelszó-irányelvnek engednie kell, hogy a felhasználók módosíthassák saját jelszavaikat. Ha az irányelv ki van kapcsolva, akkor a felhasználók nem tudják módosítani saját jelszavaikat. Csak egy adminisztrátor vagy más, megfelelő jogokkal rendelkező felhasználó tudja módosítani a bejegyzések `userPassword` attribútumát a jelszavak megváltoztatásához.
 - A jelszavakat visszaállítás után meg kell változtatni. Ha ez az irányelv be van kapcsolva, akkor ha a jelszót az adott felhasználón kívül bárki más módosítja, akkor a jelszó visszaállítottnak minősül, és a felhasználó köteles megváltoztatni bármilyen egyéb címtárművelet elvégzése előtt. A visszaállított jelszóval végrehajtott csatlakozási kérés sikeres. Ahhoz, hogy értesítést kapjon a jelszó visszaállításáról, az alkalmazásnak képesnek kell lennie az irányelvek kezelésére.
 - A felhasználóknak meg kell adniuk a régi jelszavakat a jelszóváltáskor. Ha ez az irányelv be van kapcsolva, akkor egy jelszó csak egy olyan módosítási kéressel változtatható meg, amely tartalmazza mind a `userPassword` attribútum törlendő értékét (a régi értéket) és a felveendő új `userPassword` értéket (az új jelszót). Ez biztosítja, hogy a jelszót csak a jelszavát ismerő felhasználó változtathassa meg. A rendszergazda, illetve a `userPassword` attribútum módosítására jogosult egyéb felhasználók mindig módosíthatják a jelszót.
- Szabályok a jelszó lejáratával kapcsolatban:
 - A jelszavak soha nem járnak le, vagy a jelszavak a legutolsó módosítástól számított beállítható idő eltelte után lejárnak.
 - A felhasználók nem kapnak figyelmeztetést a jelszavak lejártáról, vagy figyelmeztetést kapnak egy beállítható idővel a jelszó lejárat előtt. Ahhoz, hogy figyelmeztetést kapjon a jelszó lejártáról, az alkalmazásnak képesnek kell lennie az irányelvek kezelésére.

- Meghatározott számú "grátisz" bejelentkezés engedélyezése a felhasználó jelszavának lejáta után. Az irányelvek kezelésére képes alkalmazás értesítést kap a maradék grátisz bejelentkezések számáról. Ha egy grátisz bejelentkezés sincs engedélyezve, akkor a felhasználó nem tudja sem hitelesíteni magát, sem módosítani a jelszavát, ha az egyszer lejárt.
- Szabályok a jelszavak ellenőrzésével kapcsolatban:
 - Beállítható jelszótörténet-méret, amely azt jelenti, hogy a szerver megőrzi a legutolsó N darab jelszót és visszautasítja a korábban már használtakat.
 - Jelszósyntaxis-ellenőrzés, többek között annak beállítása, hogyan viselkedjen a szerver a kivonatolt jelszavakkal. Ez a beállítás azt befolyásolja, hogy a szerver figyelmen kívül hagyja-e az irányelvet az alábbi feltételek teljesülése esetén:
 - A szerver kivonatolt jelszavakat tárol.
 - Egy kliens kivonatolt jelszót küld a szervernek (ez történhet például, ha LDIF fájlon keresztül továbbítanak szerverek egymásnak bejegyzéseket és a forrásszerver kivonatolt jelszavakat tárol).

A fenti esetekben a szerver nem biztos, hogy képes az összes szintaktikai szabály érvényesítésére. A következő szintaktikai szabályok támogatottak: minimális hossz, betű karakterek minimális száma, numerikus vagy speciális karakterek minimális száma, megismételt karakterek száma, valamint azon karakterek száma, amennyiben a jelszónak különböznie kell a korábbi jelszótól.
- Szabályok a meghíúsult bejelentkezésekkel kapcsolatban:
 - Minimális időköz két jelszóváltás között. Ez megakadályozza a felhasználókat abban, hogy gyorsan végigpörgessenek néhány jelszót és újra a régit állítsák be.
 - A meghíúsult bejelentkezések maximális száma. Utána a fiók letiltásra kerül.
 - Beállítható jelszó-kizárási időtartam. Ennyi idő után a letiltott fiók újra használható. Ez segít abban, hogy egy betörő ne tudja megtörni a jelszót, ugyanakkor segít annak a felhasználónak, aki elfelejtette a jelszavát.
 - Beállítható időtartam, amíg a szerver nyilvántartja a meghíúsult bejelentkezési kísérleteket. Ha ennyi időn belül megtörténik a maximális számú meghíúsult kísérlet, akkor a fiók letiltásra kerül. Ennyi idő után a szerver eldobja a fiók meghíúsult bejelentkezési kísérleteivel kapcsolatos információkat.

A címtárszerver jelszó-irányelv beállításai a "cn=pwdpolicy" objektumban tárolódnak, amely az alábbihoz hasonlóan néz ki:

```
cn=pwdpolicy
objectclass=container
objectclass=pwdPolicy
objectclass=ibm-pwdPolicyExt
objectclass=top
cn=pwdPolicy
pwdExpireWarning=0
pwdGraceLoginLimit=0
passwordMaxRepeatedChars=0
pwdSafeModify=false
pwdattribute=userpassword
pwdinhistory=0
pwdchecksyntax=0
passwordminotherchars=0
passwordminalphachars=0
pwdminlength=0
passwordmindiffchars=0
pwdminage=0
pwdmaxage=0
pwdallowuserchange=true
pwdlockoutduration=0
ibm-pwdpolicy=true
pwdlockout=true
pwdmaxfailure=2
pwdfailurecountinterval=0
pwdmustchange=false
```

Jelszó-irányelvek kezelésére képes alkalmazások

A Directory Server for iSeries jelszó-irányelv támogatásának része egy sor LDAP vezérlőelem, amelyek használatával egy, a jelszó-irányelvek kezelésére felkészített alkalmazás értesítéseket kaphat további, a jelszó-irányelvekkel kapcsolatos feltételekről.

Az alkalmazások az alábbi figyelmeztető állapotokról kaphatnak értesítést:

- Maradék idő a jelszó lejártáig
- Maradék grátisz bejelentkezések száma a jelszó lejárta után

Az alkalmazások az alábbi hibaállapotokról is kaphatnak értesítést:

- A jelszó lejárt
- A fiók le van tiltva
- A jelszó vissza lett állítva és meg kell változtatni
- A felhasználó számára nem engedélyezett a saját jelszó módosítása
- A régi jelszót meg kell adni a jelszó módosításához
- Az új jelszó sérti a szintaktikai szabályokat
- Az új jelszó túl rövid
- A jelszó túl gyakran lett módosítva
- Az új jelszó a megjegyzett korábbiak egyike

Kétféle vezérlőelem használható. A jelszó-irányelv-kérési vezérlőelem szolgál a szerver értesítésére, hogy az alkalmazás a jelszó-irányelvekkel kapcsolatos állapotokról kér információkat. Ezt a vezérlőelemet az alkalmazásnak minden művelethez meg kell adnia, jellemzően a kezdeti csatlakozási kéréshez, valamint minden jelszó módosítási kéréshez. Ha van jelszó-irányelv kérési vezérlőelem, akkor a szerver egy jelszó-irányelv válasz vezérlőelemet ad vissza, ha a fenti hibás állapotok bármelyike fennáll.

A Directory Server kliens API-jai között található egy sor olyan, amelyek használatával C nyelvű alkalmazások használhatják ezeket a vezérlőelemeket. Ezek az API-k a következők:

- ldap_parse_pwdpolicy_response
- ldap_pwdpolicy_err2string

Azoknak az alkalmazásoknak a vezérlőelemeit, amelyek nem használják ezeket az API-kat, az alábbiakban írjuk le. A vezérlőelemek feldolgozásához az LDAP kliens API-k által biztosított szolgáltatásokat kell használni. Például a Java Naming and Directory Interface (JNDI) beépített támogatást tartalmaz néhány jól ismert vezérlőelemhez, valamint egy keretrendszert azon vezérlőelemek támogatásához, amelyet a JNDI nem ismer fel.

Jelszó-irányelv kérés vezérlőelem

Vezérlőelem neve: 1.3.6.1.4.1.42.2.27.8.5.1

Vezérlőelem kritikussága: FALSE

Vezérlőelem értéke: None

Jelszó-irányelv válasz vezérlőelem

Vezérlőelem neve: 1.3.6.1.4.1.42.2.27.8.5.1 (ugyanaz, mint a kérésé)

Vezérlőelem kritikussága: FALSE

Vezérlőelem értéke: Az ASN.1 specifikáció szerinti BER-kódolású érték, az alábbi:

```
PasswordPolicyResponseValue ::= SEQUENCE {
  warning [0] CHOICE OPTIONAL {
    timeBeforeExpiration [0] INTEGER (0 .. MaxInt),
    graceLoginsRemaining [1] INTEGER (0 .. maxInt) }
  error [1] ENUMERATED OPTIONAL {
    passwordExpired (0),
    accountLocked (1),
    changeAfterReset (2),
    passwordModNotAllowed (3),
    mustSupplyOldPassword (4),
```

```
invalidPasswordSyntax (5),
passwordTooShort      (6),
passwordTooYoung      (7),
passwordInHistory     (8) } }
```

Csakúgy, mint más LDAP protokollelemek, a BER-kódolás is implicit címkézést alkalmaz.

Jelszó-írányelv műveleti attribútumok

A Directory Server egy sor műveleti attribútumot használ minden egyes bejegyzéshez, amelyik rendelkezik userPassword attribútummal. Az arra jogosult felhasználók kereshetnek ezen attribútumok között, akár keresési szűrőkben használva őket, akár keresési kérésben visszaadva. Ezek az attribútumok az alábbiak:

- pwdChangedTime - Egy GeneralizedTime típusú attribútum, amelyik a jelszó legutolsó módosításának idejét tartalmazza.
- pwdAccountLockedTime - Egy GeneralizedTime típusú attribútum, amelyik a fiók legutolsó letiltásának idejét tartalmazza. Ha a fiók nincs letiltva, akkor ez az attribútum nem szerepel.
- pwdExpirationWarned - Egy GeneralizedTime típusú attribútum, amelyik azt az időt tartalmazza, amikor első alkalommal figyelmeztetés lett küldve a kliensnek a jelszó közelgő lejáratáról.
- pwdFailureTime - Egy többértékű, GeneralizedTime típusú attribútum, amely a korábbi egymás utáni bejelentkezési hibák idejét tartalmazza. Ha a legutolsó bejelentkezés sikeres volt, akkor ez az attribútum nem szerepel.
- pwdGraceUseTime - Egy többértékű, GeneralizedTime típusú attribútum, amely a korábbi grátisz bejelentkezések idejét tartalmazza.
- pwdReset - Egy logikai attribútum, amely akkor TRUE értékű, ha a jelszó meg lett változtatva és a felhasználónak ezért most módosítania kell.
- ibm-pwdAccountLocked - Logikai attribútum, amely azt jelzi, hogy a fiók adminisztratív módon zárolásra került.

Jelszó-írányelvek replikációja

A jelszó-írányelvek replikálásra kerülnek az ellátó és fogyasztó szerverek között. A cn=pwdpolicy módosításai globális módosításokként kerülnek replikálásra, csakúgy, mint a séma módosításai. Az egyes bejegyzések jelszó-írányelv állapotinformációi is replikálásra kerülnek, vagyis ha például egy bejegyzés ki van tiltva egy ellátó szerveren, akkor ez a művelet a fogyasztókra is átkerül. A csak olvasható replikák jelszó-írányelv változásai azonban nem replikálódnak más szerverekre.

Hitelesítés

A Directory Server-en belüli hozzáférés-felügyelet az egyes kapcsolatokhoz tartozó megkülönböztetett névre (DN) épül. A DN a Directory Server-hez kapcsolódás (rá bejelentkezés) alapján kerül megállapításra.

A Directory Server első beállításakor az alábbi azonosságok használhatók a szerverre bejelentkezésre:

- Anonymous
- a címtáradminisztrátor (alapértelmezés szerint cn=administrator)
- egy leképzett i5/OS felhasználói profil (lásd: "Operációs rendszer leképzett háttér objektumai" oldalszám: 75)

Jó ötlet további felhasználókat létrehozni, amelyek jogosultságokat kaphatnak a címtár különböző részeihez anélkül, hogy osztozni kellene a címtáradminisztratori azonosságon.

| További információk: "Felhasználók kezelése" oldalszám: 175.

LDAP szemszögből nézve az alábbi keretrendszerek szolgálnak hitelesítésre az LDAP szerverhez:

- Egyszerű csatlakozás, amikor is az alkalmazás megad egy DN-t és hozzá nyílt szövegben a DN-hez tartozó jelszót
- | • Simple Authentication and Security Layer (SASL), amely számos további hitelesítési eljárást biztosít (például
- | • CRAM-MD5, EXTERNAL, GSSAPI, és OS400-PRFTKN).

Egyszerű csatlakozás és CRAM-MD5

Egyszerű csatlakozás esetén a kliensnek meg kell adnia egy már létező LDAP bejegyzés DN-jét és a bejegyzés userPassword attribútumának értékével egyező jelszót. Például létrehozható egy bejegyzés John Smith számára:

```
sample.ldif:
  dn: cn=John Smith,cn=users,o=acme,c=us
  objectclass: inetorgperson
  cn: John Smith
  sn: smith
  userPassword: jelszavam
```

```
ldapadd -D cn=administrator -w secret -f sample.ldif
```

Most már használható a "cn=John Smith,cn=users,o=acme,c=us" DN a hozzáférés-felügyeleten belül, vagy tagjává tehető a hozzáférés-felügyelet egyik csoportjának.

Számos előre meghatározott objektumosztály teszi lehetővé az userPassword attribútum megadását. Ilyen például (de nem kizárólag) a person, az organizationalperson, az inetorgperson, az organization, az organizationalunit és még sok más.

A Directory Server jelszavaiban a kis- és nagybetűk különbözőnek számítanak. Ha létrehoz egy bejegyzést a secret userPassword értékkel, akkor a SECRET jelszót megadó csatlakozás meghiúsul.

Egyszerű csatlakozás használata esetén a kliens a nyílt szövegű jelszót a csatlakozási kérés részeként küldi el a szervernek. Emiatt azonban a jelszó lehallgathatóvá válik protokollszinten. A jelszó védhető egy SSL kapcsolattal (az SSL kapcsolaton keresztül haladó információk titkosítottak). Alternatívaként használható a DIGEST-MD5 vagy a CRAM-MD5 SASL eljárás.

A CRAM-MD5 módszer használata esetén a szervernek hozzá kell férnie a nyílt szövegű jelszóhoz (a jelszóvédelem szintje nincs kell, hogy legyen - ez a gyakorlatban azt jelenti, hogy a jelszó visszafejthető módon tárolódik és kereséskor nyílt szövegben kerül visszaadásra), továbbá a QRETSVRSEC (szerverbiztonsági adatok megtartása) rendszerértéknek 1-nek kell lennie (adatmegtartás). A kliens elküldi a DN-t a szervernek. A szerver visszaadja a bejegyzés userPassword értékét, majd generál egy véletlen karaktersorozatot. A kliens a véletlen karaktersorozatot kapja meg. A jelszót kulcsként használva mind a kliens, mind a szerver kivonatot készít a véletlen karaktersorozatból, majd a kliens visszaküldi az eredményt a szervernek. Ha a két kivonatos karaktersorozat egyezik, akkor a kapcsolódási kérés sikeres, és a jelszó sosem került elküldésre a szerverhez.

| A DIGEST-MD5 metódus hasonlít a CRAM-MD5-höz. Ebben az esetben a szervernek hozzá kell férnie a nyílt
| szövegű jelszóhoz (a jelszóvédelem szintje nincs kell, hogy legyen), és a QRETSVRSEC rendszerértéknek 1-nek kell
| lennie. A megkülönböztetett név elküldése helyett a szerverre a DIGEST-MD5 azt igényli, hogy a kliens küldjön egy
| felhasználónév-értéket a szerverre. Hogy a DIGEST-MD5 használható legyen egy normál felhasználó (nem az admin)
| számára, az szükséges, hogy a címtár egyetlen más bejegyzése se rendelkezzen ugyanazzal a felhasználónév-attribútum
| értékkel. A DIGEST-MD5-tel kapcsolatban eltérés az is, hogy több beállítási lehetőséget tartalmaz: szervertartomány,
| felhasználónév, adminisztrátori jelszó. Az iSeries lehetőséget ad a felhasználó leképezett vagy közzétett
| felhasználóként végzett kapcsolódására, ahol a szerver ellenőrzi a megadott jelszót a rendszeren megadott felhasználói
| profil jelszához képest. Mivel a felhasználói profilok nyílt szöveges jelszava nem elérhető a szerver számára, a
| DIGEST-MD5 nem használható leképezett vagy közzétett felhasználókhoz.

További információk: "DIGEST-MD5 hitelesítés beállítása a Directory Serveren" oldalszám: 157.

Csatlakozás közzétett felhasználóként

A Directory Server lehetőséget ad olyan LDAP bejegyzések használatára, amelyek jelszava megegyezik ugyanazon rendszer egy operációs rendszer felhasználói profiljával. Ehhez az alábbiakra van szükség:

- egy UID attribútum, amelynek értéke az operációs rendszer felhasználói profil neve
- ne legyen userPassword attribútum

Ha a szerver csatlakozási kérést kap egy olyan bejegyzéssel, amelynek van UID, de nincs userPassword értéke, akkor a szerver meghívja az operációs rendszer biztonsági rendszerét, hogy ellenőrizze: a megadott UID valóban egy érvényes felhasználói profil neve-e és a megadott jelszó valóban az adott felhasználói profil helyes jelszava-e. Az ilyen bejegyzést közzétett felhasználónak hívjuk, mivel arról van szó, hogy a rendszer terjesztési címtára (SDD) közzétételre kerül az LDAP címtárban, amely létrehozza a megfelelő bejegyzéseket.

Csatlakozás leképzett felhasználóként

Az operációs rendszer felhasználói profilt reprezentáló LDAP bejegyzéseket leképzett felhasználóknak nevezzük. A leképzett felhasználó DN-je a felhasználói profil jelszavával együtt használható egy egyszerű csatlakozás során. A my-system.acme.com JSMITH nevű felhasználójának DN-je például a következő:

```
os400-profile=JSMITH,cn=accounts,os400-sys=my-system.acme.com
```

SASL EXTERNAL csatlakozás

Ha a kliens hitelesítése során SSL vagy TLS kapcsolatot használ a rendszer (például mert a kliensnek van saját igazolása), akkor használható az SASL EXTERNAL módszer. E módszer esetén a szerver a kliens azonosságát egy külső forrásból, jelen esetben az SSL kapcsolatból veszi. A szerver lekéri a kliens igazolásának nyilvános részét (a kliens igazolást az SSL kapcsolat létrehozása során kapta meg), és kinyeri az alany DN-jét. Ezt a DN-t rendeli az LDAP szerver a kapcsolathoz.

Ha például az alábbi személy rendelkezik igazolással:

```
név: John Smith
szervezeti egység: Engineering
szervezet: ACME
hely: Minneapolis
állam: MN
ország: US
```

akkor az alany DN-je a következő lesz:

```
cn=John Smith,ou=Engineering,o=acme,l=Minneapolis,st=MN,c=US
```

Ügyeljen rá, hogy a cn, ou, o, l, st és c elemek a megadott sorrendben alkotják az alany DN-jét.

SASL GSSAPI csatlakozás

Az SASL GSSAPI csatlakozási mechanizmus esetén a szerverre hitelesítés Kerberos jegy segítségével történik. Ez akkor hasznos, ha a kliens KINIT vagy más Kerberos hitelesítést (például Windows 2000 tartomány bejelentkezést) végzett. Ebben az esetben a szerver ellenőrzi a kliens jegyét, majd bekéri a Kerberos azonosító és tartomány nevét: a realm acme.com tartomány jsmith azonosítója általában jsmith@acme.com formában kerül megjelenítésre. A szerver kétféleképpen állítható be az azonosság DN-re leképezésére:

- `ibm-kn=jsmith@acme.com` formátumú pszeudo DN-t generál
- Kikeresi azt a bejegyzést, amelynek létezik `ibm-securityidentities` kiegészítő osztálya és `KERBEROS:<azonosító>@<tartomány>` formátumú `altsecurityidentities` értéke.

A `jsmith@acme.com` azonosítóhoz tartozó bejegyzés például így nézhet ki:

```
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
objectclass: ibm-securityidentities
cn: John Smith
sn: Smith
altsecurityidentities: kerberos:jsmith@acme.com
```

A Kerberos hitelesítés engedélyezésével kapcsolatos információk: “Kerberos hitelesítés engedélyezése a Directory Server-hez” oldalszám: 156.

OS400-PRFTKN csatlakozás

Az OS400-PRFTKN SASL csatlakozási mechanizmus esetén a szerverre hitelesítés egy profil jelsor alapján történik (a részleteket a Profil jelsor generálási API-ban találja). E mechanizmus használata esetén a szerver ellenőrzi a profil jelsort, majd a leképzett felhasználói profil DN-jét rendeli a kapcsolathoz (például os400-profile=JSMITH,cn=accounts,os400-system=my-as400.mycompany.com). Ha az alkalmazásnak már van profil jelsora, akkor a mechanizmus nem kéri le még egyszer a felhasználói profilt és a felhasználói jelszót az egyszerű csatlakozás végrehajtásához. A mechanizmus használatához az ldap_sasl_bind s API-ra van szükség, adjon meg egy üres DN-t, az OS400-PRFTKN mechanizmust, valamint alapszintű kódolási szabályokkal kódolt bináris adatként ("berval") adja meg a hitelesítési adatokhoz tartozó 32 byte-os profil jelsort. Ha az LDAP API-k i5/OS-ben kerülnek használatra vagy a helyi címtárszerver elérése QSH parancs segédprogramok (például ldapsearch) használatával történik, a jelszó kihagyható, és a kliens API-k a szervert mint a feladat aktuális felhasználói profilját fogják azonosítani. Például: az

```
> ldapsearch -m OS400-PRFTKN -b "o=ibm,c=us" "(uid=johndoe)"
```

végre fogja hajtani a keresést az aktuális felhasználói profil jogosultsága alatt, mintha a következőt használta volna:

```
> ldapsearch -D os400-profile=myprofile,cn=accounts,os400-sys=mssystem -w mypassword -b "o=ibm,c=us" "(uid=johndoe)"
```

LDAP mint hitelesítési szolgáltatás

Az LDAP címtárak sokszor biztosítanak hitelesítési szolgáltatást. Beállítható például a webszerver, hogy LDAP segítségével hitelesítse a felhasználókat. Több LDAP hitelesítést használó webszerver (vagy alkalmazás) üzemeltetése esetén elegendő egyetlen felhasználói nyilvántartást működtetni, nem kell minden egyes alkalmazásban és webszerver-példányban külön-külön megadni őket.

Hogyan működik mindez? Röviden úgy, hogy a webszerver bekéri a felhasználó nevét és jelszavát. Ezek alapján keresést hajt végre az LDAP címtárban a megadott nevű bejegyzésre (beállítható a webszerver úgy is, hogy a felhasználó nevét például az LDAP 'uid' vagy 'mail' attribútumainak feleltesse meg). Ha pontosan egy bejegyzést talál, akkor a webszerver kiad egy csatlakozási kérést a megtalált bejegyzés DN-jével és a felhasználó által megadott jelszóval. Ha a csatlakozás sikeres, akkor a felhasználó hitelesítve van. A protokollszerű lehallgatás elleni védekezésként SSL kapcsolatokat is használhat a rendszer.

A webszerver nyomon követheti a felhasznált DN-t, vagyis egy adott alkalmazás használhatja ezt a DN-t, például arra, hogy egyedi adatokat mentsen el a bejegyzésbe, egy másik, hozzá tartozó bejegyzésbe, vagy éppen használhatja egy adatbázis kulcsaként a DN-t bizonyos információk kikereséséhez.

A csatlakozási kérés szokásos alternatívája egy LDAP "összehasonlítás" (compare) művelet kiadása. Például: ldap_compare(ldap_session, dn, "userPassword", beírt_jelszó). Így az alkalmazásnak elegendő egyetlen LDAP munkamenetet használnia, nem kell állandóan újakat nyitnia és lezárnia minden egyes hitelesítési kéréshez.

| Szolgáltatás megbénítása

| A címtárszerver a következő fajta szolgáltatásbénító (DOS) támadások ellen véd:

- | • Kliensek, amelyek lassan küldenek adatokat, részleges adatokat küldenek vagy nem küldenek adatokat
- | • Kliensek, amelyek nem vagy lassan olvassák az adateredményeket
- | • Le nem választható kliensek
- | • Kliensek, amelyek hosszan futó adatbázislekérdezési kéréseket készítenek
- | • Névtelenül kapcsolódó kliensek
- | • Szerverterhelések, amelyek megakadályozzák az adminisztrátort a szerver adminisztrálásában

| A címtárszerver számos eljárást kínál az adminisztrátorok számára a szolgáltatásbénítós támadások elleni védekezéshez. Egy vészszál használatával mindig hozzáférhetnek a szerverhez, még akkor is, ha az éppen hosszan futó műveletekkel van leterhelve. Emellett az adminisztrátorok felügyelhetik a szerver elérését, így lehetőségük van

| lecsatlakoztatni egy adott kapcsolati DN-nel vagy IP-címmel rendelkező klienst, illetve beállítani a szerveret, hogy ne engedélyezzen névtelen hozzáférést. Más konfigurációs beállítások is üzembe helyezhetők, amelyekkel a szerver aktívan megelőzheti a szolgáltatásbénítós támadásokat.

| További információk:

- | • “Szerverkapcsolatok kezelése” oldalszám: 113
- | • “Kapcsolat tulajdonságainak kezelése” oldalszám: 114

Operációs rendszer leképzett háttér objektumai

A rendszer leképzett háttér objektumai funkció leképezi az i5/OS objektumokat LDAP által elérhető katalógusfán belüli bejegyzésekre. A leképzett objektumok az operációs rendszer objektumok LDAP reprezentánsai, amelyeket az LDAP szerver adatbázisában tárolt tényleges bejegyzés helyett használunk. Kizárólag a felhasználói profilok azok az objektumok, amelyeket a rendszer bejegyzésként hozzárendel vagy leképez a katalógusfán belül. A felhasználói profil objektumok leképezését nevezzük az operációs rendszer felhasználói leképzett háttér objektumnak.

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

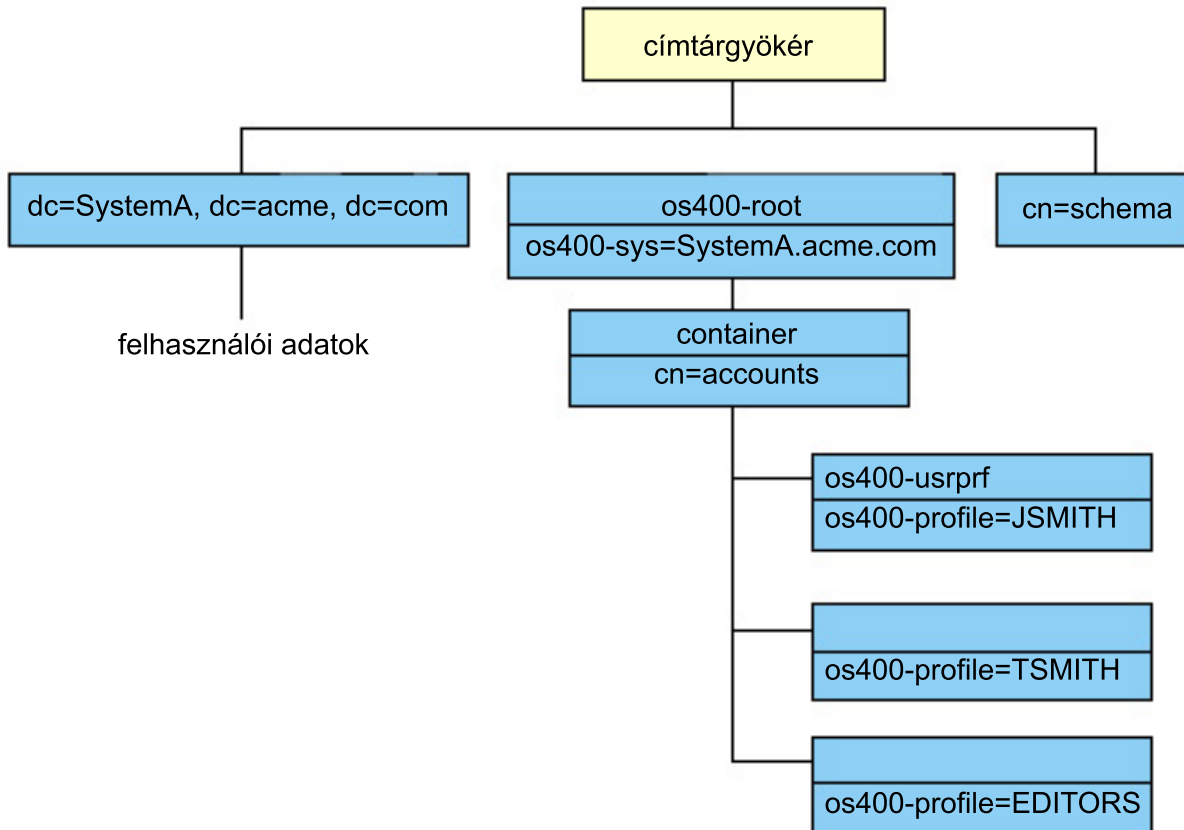
Az operációs rendszer leképzett háttér objektumairól további tájékoztatást kaphat a következő helyeken:

- “Felhasználói leképezett címtár-információs fa”
- “LDAP műveletek” oldalszám: 76
- “Adminisztrátori és replika csatlakozási DN” oldalszám: 80
- “Felhasználói leképezett séma” oldalszám: 80

Felhasználói leképezett címtár-információs fa

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 segítségével a következő LDAP műveleteket hajthatja végre.

Csatlakozás (Bind)

Az LDAP kliens csatlakozhat (hitelesítheti magát) az LDAP szerverhez a leképzett felhasználói profil segítségével. Ez úgy hajtható végre, hogy bind DN értéként a leképzett felhasználói profil megkülönböztetett nevét (DN) adja meg, valamint a felhasználói profil helyes jelszavát a hitelesítéshez. Példa a csatlakozási kérésben használt DN-re: `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.

Két további mechanizmus áll rendelkezésre a címtárszerverre leképzett felhasználókénti hitelesítéshez:

- GSSAPI SASL csatlakozás. Ha az operációs rendszer úgy van beállítva, hogy a Vállalati azonosság leképezés (EIM) rendszert használja, akkor a címtárszerver lekérdezi az EIM rendszert annak megállapításához, hogy van-e rendelve helyi felhasználói profil a kezdeti Kerberos azonossághoz. Ha van ilyen összerendelés, akkor a szerver hozzárendeli a felhasználói profilt a kapcsolathoz és az használható a rendszer leképezési háttérének elérésére. További információkat az EIM rendszerről az EIM témakörben talál.
- OS400-PRFTKN SASL csatlakozás. A címtárszerverre csatlakozáshoz profil jelsor használható. A szerver a profil jelsor felhasználói profilját rendeli a kapcsolathoz.

A szerver az összes műveletet az adott felhasználói profil jogosultságait felhasználva hajtja végre. A leképzett felhasználói profil DN ugyanúgy használható az LDAP ACL-ben, mint más LDAP bejegyzés DN. Az egyszerű csatlakozás az egyetlen módszer, amely engedélyezett, amikor leképzett felhasználói profilt ad meg a csatlakozási 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 helyettesítő karakterek használatát. Az os400-gid attribútum megadása korlátozott, mégpedig (os400-gid=0), amely egy egyedi felhasználói profil vagy !(os400-gid=0), amely 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. Az ezt követő keresések azonban már részletesebb információkat adhatnak vissza.

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

3. táblázat: 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 értékek 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.

3. táblázat: Rendszer leképzett háttér objektumainak viselkedése keresési műveleteknél (Folytatás)

Kért keresés	Keresés alapja	Keresés hatásköre	Keresés szűrője	Megjegyzések
Az összes csoportprofil 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 felhasználói és csoportprofil 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 csoportprofil, 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 csoportprofil, mint például JSMITH, visszaadása.	os400-profile=JSMITH, cn=accounts, os400-sys=SystemA.acme.com	bas, sub vagy one	objectclass=os400-usrprf objectclass=*	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 csoportprofil 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 csoportprofil 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.

3. táblázat: 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 értékét. 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 OWNBOBJOPT 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 az alábbi formátumú karaktersorozat:

- 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 az alábbi formátumú karaktersorozattal van megadva:

```
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 csoportprofil neve vagy `*NONE`. Ha új elsődleges csoportprofil 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.

Importálási és exportálási API-k

A `QglImportLdif` és a `QglExportLdif` API-k nem támogatják az adatok importálását és az exportálását a rendszer leképzett háttér objektumain belül.

Adminisztrátori és replika csatlakozási DN

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

További információk: “Adminisztratív hozzáférés” oldalszám: 55.

Felhasználói leképezett séma

A leképzett háttér objektumok objektum osztályai és attribútumai egy, az egész szerverre kiterjedő sémában található. Az LDAP attribútumok nevei `os400-nnn` formátumúak, ahol *nnn* jellemzően az attribútum kulcsszava a felhasználói profil parancsaiban. Az `os400-usrcls` attribútum például a `CRTUSRPRF` parancs `USRCLS` paraméterének felel meg. Az attribútumok értékei a `CRTUSRPRF` és `CHGUSRPRF` parancsok által elfogadott paraméterértékeknek, illetve a felhasználói profil megjelenítésekor látható értékeknek felelnek meg. Az `os400-usrprf` objektumosztályt és a hozzá tartozó `os400-xxx` attribútumokat a webes adminisztrációs eszközzel vagy más alkalmazással tekintheti meg.

Directory Server és i5/OS naplózási támogatás

A Directory Server az i5/OS adatbázis támogatását használja a címtár-információk tárolásához. A Directory Server a véglegesítés vezérlés alapján tárolja a címtárbejegyzéseket az adatbázisban. Ehhez szükség van az i5/OS 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 QSQRN napló abban az adatbázis könyvtárban kerül összeállításra, amit a felhasználó konfigurált. A QSQRN0001 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 változtatási naplófájlt állított be, de meg kívánja tartani a régi fogadókat is, hajtsa végre a következő parancsot az i5/OS parancssorból:

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

Ha konfigurálásra került a változtatási naplófájl, a régi naplófogadók a következő paranccsal törölhetők:

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

További információkat a naplózási parancsokról a Programozás témakör "OS/400 parancsok" részében talál.

Egyedi attribútumok

Egyedi attribútumok: Az egyedi attribútumok funkció biztosítja, hogy a megadott attribútum értéke egyedi maradjon a címtáron belül. Ezek az attribútumok csak két bejegyzésben határozhatók meg, ezek a `cn=uniqueattribute,cn=localhost` valamint a `cn=uniqueattribute,cn=IBMpolicias`. Az egyedi attribútumok keresési eredményei csak az adott szerver adatbázisára vonatkozóan egyediek. Az utalásokból származó keresési eredmények nem lehetnek egyediek.

Megjegyzés: A bináris, műveleti, konfigurációs és objektumosztály attribútumok nem lehetnek egyedi jelölésűek.

Nem minden attribútum adható meg egyediként. Annak eldöntésére, hogy egy attribútum megadható-e egyedi attribútumként, az `ldapexop` parancs használható:

- Azokhoz az attribútumokhoz, amelyek lehetnek egyediek: `ldapexop -op getattributes -attrType unique -matches true`
- Azokhoz az attribútumokhoz, amelyek nem lehetnek egyediek: `ldapexop -op getattributes -attrType unique -matches false`

További információk az egyedi attribútumokkal kapcsolatban: "Egyedi attribútumok kezelése" oldalszám: 125.

Műveleti attribútumok

Több olyan attribútum is van, amelyek speciális jelentéssel bírnak a Directory Server számára. Ezek a műveleti attribútumok. Ezeket az attribútumokat a szerver tartja karban és vagy azzal kapcsolatos információkat tartalmaznak, hogyan kezeli a bejegyzést a szerver, vagy pedig a szerver működését befolyásolják. Ezek az attribútumok különleges jellemzőkkel bírnak:

- Az attribútumok nem kerülnek visszaadásra a keresési kérések során, kivéve, ha kifejezetten, névvel meg lettek adva
- Az attribútumok egyetlen objektumosztálynak sem részei. Azt, hogy mely bejegyzéseknek van ilyen attribútumuk, a szerver szabályozza.

A Directory Server többek közt az alábbi műveleti attribútumhalmazokat kezeli:

- A `creatorsName`, `createTimestamp`, `modifiersName`, `modifyTimestamp` minden bejegyzésben benne van. Ezek az attribútumok jelzik a kapcsolódási DN-t és az időt, amikor a bejegyzés első alkalommal létrehozásra került, illetve legutoljára módosítva lett. Ezek az attribútumok keresési szűrőkben is használhatók, például egy megadott idő után módosított bejegyzések kikereséséhez. Ezeket az attribútumokat egyetlen felhasználó sem módosíthatja. Ezek az attribútumok replikálásra kerülnek a fogyasztó szerverekre, valamint importálódnak és exportálódnak az LDIF fájlokból/fájlokba.
- `ibm-entryuuid`. Minden olyan bejegyzésben megtalálható, amely V5R3 vagy frissebb kiadású szerveren került létrehozásra. Ez az attribútum egy univerzálisan egyedi karaktersorozat azonosító, amelyet a szerver rendel a bejegyzéshez annak létrehozásakor. Hasznos olyan alkalmazások esetén, amelyeknek különbséget kell tenniük

különböző szerverek egyforma nevű bejegyzései között. Az attribútum a DCE UUID algoritmus alapján előállított értéket tartalmaz, amely egyedi minden szerver minden bejegyzésére vonatkozóan, ugyanis az időbélyeg, az adapter címe és hasonló elemekből épül fel.

- entryowner, ownersource, ownerpropagate, aclentry, aclsource, aclpropagate, ibm-filteracl, ibm-filteraclinherit, ibm-effectiveAcl. További információk: “Hozzáférés-felügyeleti listák” oldalszám: 56.
- hasSubordinates. Minden bejegyzés tartalmazza, és TRUE az értéke, ha a bejegyzésnek vannak alárendeltjei.
- numSubordinates. Minden bejegyzés tartalmazza, és az értéke az adott bejegyzés leszármazott bejegyzéseinek száma.
- pwdChangedTime, pwdAccountLockedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdReset, pwdHistory. További információk: “Jelszó-irányelvek” oldalszám: 68.
- subschemasubentry - Minden bejegyzés tartalmazza, és az adott címtárfarész sémájának helyét azonosítja. Ez hasznos olyan szerverek esetén, amelyek több sémát is tartalmaznak és éppen ki kell keresni az adott címtárfarészhez tartozó sémát.

A műveleti attribútumok teljes listája a következő kiterjesztett művelettel kérhető le: `ldapexop -op getattributes -attrType operational -matches true`.

Szerver gyorsítótárak

Az LDAP gyorsítótárak gyors tárolópufferek a memóriában, amelyek olyan LDAP információk tárolására szolgálnak a jövőbeli használathoz, mint amilyenek a lekérdezések, válaszok és felhasználói hitelesítések. Az LDAP gyorsítótárak hangolása rendkívül fontos a teljesítmény fokozásában.

Az LDAP gyorsítótárat elérő LDAP-keresés gyorsabb lehet, mint az, aminek DB2 kapcsolatra van szüksége, még akkor is, ha az információt a DB2 gyorsítótárazza. Emiatt az LDAP-gyorsítótárak hangolása fokozza a teljesítményt azzal, hogy megelőzi az adatbázishívásokat. Az LDAP gyorsítótárak különösen az olyan alkalmazásoknál hasznosak, amelyek gyakran kérdeznek le ismétlődő gyorsítótári információkat.

A következő rész az egyes LDAP gyorsítótárakról szól, és bemutatja, hogyan határozhatók meg és adhatók meg a legjobb gyorsítótári beállítások a rendszerhez.

- “Attribútum-gyorsítótár”
- “Szűrő gyorsítótár” oldalszám: 83
- “Bejegyzés gyorsítótár” oldalszám: 83
- “ACL gyorsítótár” oldalszám: 83

A gyorsítótárak beállításával kapcsolatban lásd: “Teljesítménnyel kapcsolatos beállítások módosítása” oldalszám: 128.

Attribútum-gyorsítótár

Az attribútum-gyorsítótárnak az az előnye, hogy lehetőséget ad a szűrők feloldására a memóriában az adatbázis helyett. Az is előny, hogy minden alkalommal frissül egy LDAP add, delete, modify vagy modrdn művelet végrehajtásakor.

Annak eldöntéséhez, hogy mely attribútumokat kívánja gyorsítótárban tárolni, a következőket kell figyelembe vennie:

- A szerverben rendelkezésre álló memória mennyiségét
- A címtár méretét
- Az alkalmazás által általában használt keresési szűrők típusát

Megjegyzés: Az attribútum gyorsítótár kezelő az egyszerű szűrők következő típusait képes feloldani: pontos illeszkedés szűrők és jelenlét szűrők. Fel tudja oldani az összekötő és szétválasztó összetett szűrőket; a részszűrőknek pontos illeszkedés, jelenlét, összekötő vagy szétválasztó típusúaknak kell lenniük.

Nem minden attribútum adható hozzá az attribútum-gyorsítótárhoz. Annak eldöntéséhez, hogy egy attribútum hozzáadható-e a gyorsítótárhoz, az `ldapexop` parancs használható:

- Hozzáadható attribútumok esetén: `ldapexop -op getattributes -attrType attribute_cache -matches true`
- Hozzá nem adható attribútumok esetén: `ldapexop -op getattributes -attrType attribute_cache -matches false`

Az attribútum-gyorsítótárazás kétféle módon állítható be: kézzel és automatikusan. Az attribútum-gyorsítótárazás kézi beállításához az adminisztrátornak `cn=monitor` kereséseket kell végeznie annak felderítésére, hogy hogyan teheti az attribútum-gyorsítótárazást a leghatékonyabbá. Ezek a keresések aktuális információt adnak vissza arról, hogy mely attribútumok vannak a gyorsítótárban, melyikhez mennyi memória van felhasználva, az attribútum-gyorsítótárazás összesen mennyi memóriát használ fel és mennyi memória van beállítva az attribútum-gyorsítótárazáshoz, illetve felsorolják a keresési szűrőkben leggyakrabban használt attribútumokat. Ennek az információnak a felhasználásával az adminisztrátorok módosíthatják, hogy mennyi memóriát lehet felhasználni az attribútum-gyorsítótárazáshoz, valamint hogy mely attribútumokat kell gyorsítótárazni, ahányszor az új `cn=monitor` keresések alapján szükséges.

A másik módszer az automatikus attribútum-gyorsítótárazás beállítása. Ha az automatikus attribútum-gyorsítótárazás engedélyezve van, a Directory Server nyomon követi, hogy az attribútumok mely kombinációját volna leghasznosabb gyorsítótárban tárolni az adminisztrátor által megadott memóriakorlátokon belül. Ezután, szintén az adminisztrátor által beállított időben és időközönként frissíti az attribútum-gyorsítótárat.

Szűrő gyorsítótár

Ha a kliens kibocsát egy adatkérést és azt az attribútum-gyorsítótár kezelő nem tudja feloldani a memóriában, akkor a kérés a szűrő gyorsítótárba jut. Ez tartalmazza a gyorsítótárba helyezett bejegyzésazonosítókat. Amikor a kérés megérkezik a szűrő gyorsítótárhoz, két dolog történhet:

- **A kérésben használt, a szűrőbeállításoknak megfelelő azonosítók megtalálhatók a szűrő gyorsítótárban.** Ebben az esetben a megfelelő bejegyzésazonosítók átküldésre kerülnek a bejegyzés gyorsítótárnak.
- **A megfelelő bejegyzésazonosítók nincsenek a szűrő gyorsítótárban.** Ebben az esetben a lekérdezésnek el kell érnie a DB2-t a kívánt adatok lekérdezésekor.

Annak eldöntésére, hogy mekkora legyen a szűrő gyorsítótár, futtassa a terhelést a szűrő gyorsítótár különböző értékre állítása mellett, és mérje meg a műveletek közötti különbségeket másodpercben.

A szűrő gyorsítótár kihagyási korlát változó korlátozza a szűrő gyorsítótárhoz hozzáadható bejegyzések számát. Ha például a kihagyási korlát változó 1000-re van állítva, akkor az ezernél több bejegyzésnek megfelelő keresési szűrők nem kerülnek hozzáadásra a szűrő gyorsítótárhoz. Ez megvédi a rendszert attól, hogy nagy, szokatlan keresések felülírják a hasznos gyorsítótári bejegyzéseket. A szűrő gyorsítótár kihagyási korlát legmegfelelőbb beállításához futtassa le többször a terhelést és mérje a teljesítményt.

Bejegyzés gyorsítótár

A bejegyzés gyorsítótár a bejegyzések adatait tartalmazza. A bejegyzésazonosítók elküldésre kerülnek a bejegyzés gyorsítótárhoz. Ha az ezekhez illeszkedő bejegyzések benne vannak a gyorsítótárban, akkor az eredmény visszaadásra kerül a kliensnek. Ha a bejegyzés gyorsítótár nem tartalmazza a bejegyzésazonosítónak megfelelő bejegyzéseket, a lekérdezés átkerül a DB2-be a megfelelő bejegyzések keresésére.

Annak eldöntésére, hogy mekkora legyen a bejegyzés gyorsítótár, futtassa a terhelést a bejegyzés gyorsítótár különböző méretre állítása mellett, és mérje meg a műveletek közötti különbségeket másodpercben.

ACL gyorsítótár

Az ACL gyorsítótár hozzáférés-vezérlési információkat tartalmaz, például a közelmúltban elért bejegyzések tulajdonosát és jogosultságait. Ez a gyorsítótár a bejegyzések hozzáadásakor, törlésekor és keresésekor a hozzáférés-kiértékelés teljesítményének növelésére szolgál. Ha egy bejegyzés nem található az ACL gyorsítótárban, a hozzáférés-vezérlési információk az adatbázisból kerülnek lekérésre. A megfelelő ACL gyorsítótári méret meghatározására mérje meg a szerverteljesítményt úgy, hogy egy jellemző terheléshez többféle ACL gyorsítótár-méretet állít be.

Vezérlőelemek és kiterjesztett műveletek

Vezérlőelemek

A vezérlőelemek további információkat biztosítanak a szerver számára. Például a **delete subtree** (részfá törlése) vezérlőelem megadható egy LDAP törlési kérés részeként, azt jelezvén, hogy a szerver a bejegyzést és összes alárendelt bejegyzését is törölje (és ne csak a megadott bejegyzést). A vezérlőelemek három részből állnak:

- A vezérlőelem típusa, amely a vezérlőelemet azonosító OID.
- Egy "fontosságjelző", amely azt szabályozza, hogyan viselkedjen a szerver, ha nem támogatja az adott vezérlőelem használatát. Ez egy logikai érték. A FALSE érték azt jelzi, hogy az érték nem kritikus fontosságú, és ha a szerver nem támogatja a használatát, akkor hagyja figyelmen kívül. A TRUE érték azt jelzi, hogy a vezérlőelem kritikus fontosságú, és a teljes kérés legyen sikertelen (nem támogatott kritikus kiterjesztés hibával), ha a szerver nem képes azt teljes egészében kiszolgálni.
- Egy elhagyható vezérlőelem érték, amely az adott vezérlőelemre jellemző további információkat tartalmaz. A vezérlőelem értéket ASN.1 jelölésmóddal kell megadni. Az érték maga a vezérlőelem adat BER kódolással.

Kiterjesztett műveletek

A kiterjesztett műveletek célja az alap LDAP műveleteken kívüli lehetőségek biztosítása. Kiterjesztett műveletek léteznek például meghatározott műveletek egyetlen tranzakcióvá szervezésére. Egy kiterjesztett művelet az alábbiakból áll:

- A kérés neve, az adott műveletet azonosító OID.
- Egy elhagyható kérés érték, amely az adott műveletre jellemző további információkat tartalmaz. A kérés értékét ASN.1 jelölésmóddal kell megadni. Az érték maga a kérés adat BER kódolással.

A kiterjesztett műveletekhez általában kiterjesztett válaszok is tartoznak. A válasz az alábbi részekből áll:

- A normál LDAP eredmény elemei (hibakód, egyező DN és hibaüzenet)
- A válasz neve, az adott kéréstípust azonosító OID.
- Egy elhagyható érték, amely a válaszra jellemző további információkat tartalmaz. A válaszártékét ASN.1 jelölésmóddal kell megadni. Az érték maga a válasz adat BER kódolással.

A vezérlőelemek és a kiterjesztett műveletek teljes listája és a megfelelő objektumazonosítók (OID-k) és leírások ismertetése a következő helyen található: "Objektumazonosítók (OID)" oldalszám: 261.

5. fejezet Első lépések a Directory Server használatában

A Directory Server az i5/OS rendszerrel együtt automatikusan telepítésre kerül. A Directory Server része egy alapértelmezés szerinti konfiguráció. A Directory Server használatának első lépései:

1. Ha V5R4 kiadást telepít, és a Directory Server-t használta már egy korábbi kiadásban, akkor tekintse át az áttéréssel kapcsolatos megfontolásokat. További információk: “Áttérési megfontolások”.
2. Tervezze meg a Directory Server rendszert. További információk: “Directory Server megtervezése” oldalszám: 90.
3. A Directory Server beállításainak testreszabásához futtassa le a Directory Server beállítási varázslóját. További információk: “Directory Server beállítása” oldalszám: 90.
4. Indítsa el a szerveret. További információk: “Directory Server indítása/leállítása” oldalszám: 112.
5. A webes adminisztrációs eszközzel hozzon létre vagy módosítson meglévő LDAP címtárakat. További információk: “Webes adminisztráció” oldalszám: 98.
6. A különféle Directory Server feladatok elvégzésével kapcsolatban tekintse meg a 7. fejezet, “Directory Server felügyelete”, oldalszám: 111 részben található további információkat.

Áttérési megfontolások

A Directory Server az i5/OS rendszerrel együtt automatikusan telepítésre kerül. A szerver első elindításakor átállít minden meglévő beállítást és adatot. Ez a szerver első indításakor jó ideig eltarthat.

Megjegyzés: A beállítási és sémafájlok átállítása a telepítés és az első szerverindítás során történik. Ha egyszer ez az első szerverindítás megtörtént, akkor ha a /qibm/userdata/os400/dirsrv könyvtárban található konfigurációs és sémafájlok visszaállításra kerültek az előző kiadás mentéséből, az új kiadás konfigurációs és sémafájljai átfedésben lesznek az előző kiadás fájljaival, amelyek nem állíthatók át újra. Az előző kiadás séma- és konfigurációs fájljainak visszaállítása az átállás után azt okozhatja, hogy a szerver nem indul el vagy más megjósolhatatlan hibák jelentkeznek. Ha a szerverkonfiguráció és a séma mentése kívánatos, akkor ezeket az adatokat azután érdemes menteni, hogy a szerver sikeresen elindult.

Ha van V5R3 vagy V5R2 kiadás alatt futó Directory Server-e, akkor tekintse meg a következő részt: “Átállás V5R4 kiadásra V5R3 vagy V5R2 rendszerekről”.

Ha van V4R4, V4R5 vagy V5R1 kiadás alatt futó Directory Server-e, akkor az adatokat átállíthatja V5R4 szintre. További információk: “Adatok átállítása V4R4, V4R5 vagy V5R1 kiadásokról a V5R4 kiadásra” oldalszám: 86.

Ha replikált szerverek hálózatát használja, akkor itt talál további információkat: “Replikált szerverek hálózatának átállítása” oldalszám: 87.

Ha Kerberosot használ: “Kerberos szolgáltatás megváltozott neve” oldalszám: 89.

Átállás V5R4 kiadásra V5R3 vagy V5R2 rendszerekről

Az i5/OS V5R3 kiadása számos új funkcióval és lehetőséggel bővíti a Directory Server rendszert. Ezek a változtatások érintik az LDAP címtárszerveret és az iSeries navigátor grafikus felhasználói kezelőfelületét (GUI-t). Ahhoz, hogy kihasználhassa az új GUI funkcióit, 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 V5R4 változatra kell frissíteni.

Az i5/OS V5R4 támogatja a közvetlen frissítéseket V5R2 és V5R3 változatról. Ha az V5R4 i5/OS verziójára történik a frissítés, akkor az LDAP címtárakat és a címtárséma-fájlokat úgy kerülnek átállításra, hogy megfeleljenek a V5R4 formátumnak.

Az i5/OS V5R3 verziójára frissítéskor figyelembe kell venni néhány szempontot:

- A V5R4 verzióra frissítéskor, a Directory Server automatikusan áthelyezi a sémafájlokat a V5R4 verzióba, majd törli a régi sémafájlokat. Ha Ön már törölte vagy átnevezte a sémafájlokat, akkor a Directory Server nem fogja tudni áttelepíteni őket. Lehet, hogy hibaüzenetet kap, vagy a Directory Server feltételezheti, hogy a fájlok már áttelepítésre kerültek.
- A V5R4 kiadásra frissítés után indítsa el legalább egyszer szerverét, hogy a létező adatok átállításra kerüljenek, mielőtt új adatokat importálna. Ha megpróbál adatokat importálni a szerver indítása előtt, és nem rendelkezik elegendő jogosultsággal, akkor az import meghiúsulhat. A Directory Server V5R4 formátumba állítja át a címtáradatokat a szerver első indításakor vagy egy LDIF fájl importálásakor. Szánjon némi időt az áttelepítés elvégzésére.
- Az áthelyezés után az LDAP címtárszerver automatikusan elindul a TCP/IP alrendszerrel együtt. Ha azt akarja, hogy a címtárszerver ne induljon el automatikusan, akkor a beállításokat módosítsa az iSeries navigátorral.

Adatok átállítása V4R4 ,V4R5 vagy V5R1 kiadásokról a V5R4 kiadásra

A V4R4, V4R5 és V5R1 változatokról nem lehet közvetlenül az i5/OS V5R4 változatra frissíteni. Ha ezeket a kiadásokat kívánja frissíteni a V5R4 kiadásra, akkor az alábbi eljárások szerint kell eljárnia:

- “frissítése V4R4, V4R5 vagy V5R1 kiadásokról köztes kiadásra”
- “Adatbáziskönyvtár elmentése és a V5R4 kiadás telepítése” oldalszám: 87

V4R4 kiadásról bármelyik későbbi változatra frissítéskor a következő szempontokra kell figyelni:


- A Directory Server V4R4 verziója és korábbi verziói nem vették figyelembe az időzónákat, amikor létrehozták az időbélyegeket. A V4R5 változattól kezdve a rendszer figyelembe veszi az időzónákat a címtár minden módosításánál és bővítésénél. Ezért, ha V4R4 vagy korábbi verzióról frissít V5R3 verzióra, a Directory Server 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 időbélyeg értékek nem tükrözik az eredeti időzónát.
- Ha V4R4 verzióról vagy egy korábbi verzióról frissít adatokat, vegye figyelembe, hogy a címtáradatok elhelyezésére a korábbinál körülbelül kétszer több tárolóhelyre lesz szüksége. Ez azért van, mert a Directory Server csak az IA5 karakterkészletet támogatta a V4R4 és korábbi verzióban, és az adatokat CCSID 37 (egybyte-os formátum) azonosító szerint mentette. A Directory Server támogatja a teljes ISO 10646 karakter készletet. Frissítés után 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.

frissítése V4R4, V4R5 vagy V5R1 kiadásokról köztes kiadásra

Noha nem támogatott a V4R4, V4R5 és V5R1 frissítése a V5R4 változatra, a következő lehetőségek kihasználhatók:

- V4R4 és V4R5 frissíthető V5R1-re
- V4R5 és V5R1 frissíthető V5R2-re
- V5R1 és V5R2 frissíthető V5R3-ra
- V5R2 és V5R3 frissíthető V5R4-re

A Directory Server szerver frissítés egyik lehetséges módja, hogy először egy közbenső kiadásra (V5R2 vagy V5R3)

tér át, majd onnan V5R4 változatra. Az i5/OS telepítési eljárásokról részletes információt a *Szoftvertelepítés*  című könyvben talál. Az átállítás a következő lépések végrehajtásával történik. A sémamódosításokat érdemes automatikusan átállítani. Minden telepítés után ellenőrizze, hogy a sémamódosítások megvannak-e még.

1. V4R4 esetén hajtsa végre a V5R1 telepítését. Majd hajtsa végre a V5R3 kiadás telepítését.
2. V4R5 esetén hajtsa végre a V5R1 vagy V5R2 kiadás telepítését. Ha a V5R1-et telepíti, akkor eztán telepítenie kell a V5R2 vagy V5R3 változatot.
3. V5R1 esetén végezze el a V5R3 telepítését.
4. Ha a V5R2 vagy V5R3 fent van, végezze el a V5R4 telepítését.
5. Ha még nem indított el eddig, akkor indítsa el a Directory Servert.

Adatbáziskönyvtár elmentése és a V5R4 kiadás telepítése

A Directory Server állítható úgy is, hogy elmenti a Directory Server által használt adatbáziskönyvtárat a V4R4 vagy V4R5 kiadásban, majd visszaállítja a V5R4 változat telepítése után. Ezzel megtakarítható a közbenső kiadás telepítési fázisa. Ilyenkor azonban a szerver beállításai nem helyeződnek át, így a szervert újra kell konfigurálni. Az i5/OS

telepítési eljárásokról részletes információt a *Szoftvertelepítés*  című könyvben talál. Az áttéréshez a következő műveleteket végezze el:

1. Jegyezzen fel minden, a /QIBM/UserData/OS400/DirSrv katalógusban a sémafájlokban végrehajtott változtatást. A sémafájlok nem kerülnek automatikusan áthelyezésre, ezért ha meg kívánja őrizni a változtatásokat, ezeket kézi úton kell újra létrehozni. Ha a sémafrissítések LDIF fájlok és az ldapmodify segédprogram használatával készültek, akkor keresse meg ezeket a fájlokat, hogy miután a szerver elindult az új kiadással, használhassa őket. A címtárkezelő eszköz vagy a webadminisztrációs eszköz (más V5R4 rendszeren futtatva) használható az egyedi attribútumtípus és objektumoszály-definíciók megjelenítésére. Ha a módosítások csak új attribútumtípusok és objektumoszályok hozzáadására terjednek ki, készítsen egy másolatot a /qibm/userdata/os400/dirsrv/v3.modifieschema fájlról. Ennek a fájlnek a felhasználásával hozhatók létre a sémafrissítéseket tartalmazó LDIF fájlok. További információk: "Séma" oldalszám: 15.
2. Jegyezze fel a Directory Server különböző konfigurációs beállításait, többek között az adatbáziskönyvtár nevét is.
3. Mentse el a Directory Server konfigurációban megadott adatbáziskönyvtárat. Ha beállította a változásnaplót, akkor el kell mentenie a QUSRDIRCL könyvtárat is.
4. Jegyezze fel a közzétételi konfigurációt. A közzétételi információk (kivéve a jelszó-információt) az iSeries Navigator használatával tekinthetők meg a rendszerre vonatkozó **Tulajdonságok** kiválasztásával, majd a **Címtárszolgáltatások** lapra kattintva.
5. Telepítse az i5/OS V5R4 kiadását a rendszeren.
6. Használja az EZ-Setup programot a címtárszerver konfigurálására.
7. Állítsa vissza az 3. lépésben elmentett adatbáziskönyvtárat. Ha a 3. lépésben elmentette a QUSRDIRCL könyvtárat, akkor állítsa azt is vissza.
8. Az iSeries navigátorral konfigurálja újra a Directory Server-t. Adja meg a korábban beállított adatbázis-könyvtárat, amelyet az előző lépésekben elmentett és visszaállított.
9. Az iSeries navigátorral állítsa be újra a közzétételt.
10. Indítsa újra a Directory Server-t.
11. A webes adminisztrációs eszközzel hajtsa végre a 1 lépésben feljegyzett sémafájl-módosításokat.

Replikált szerverek hálózatának átállítása

Az elsődleges szerver első elindításakor átmozgatja a replikációt vezérlő címtár információit. A cn=localhost alatti, replicaObject objektumoszályú bejegyzéseket felváltják az új replikációs modell által használt bejegyzések (további információk: "Replikáció" oldalszám: 36). Az elsődleges szerver beállításra kerül, hogy a címtár összes utótagját replikálja. A megállapodás bejegyzései létrejönnek, ibm-replicationOnHold attribútumukat true értékre állítja a rendszer. Ez lehetővé teszi, hogy a replikához tartozó módosítások gyűljenek az elsődleges szerveren addig, amíg a replika rendelkezésre nem áll.

Ezeket a bejegyzéseket szokás replikációs topológia néven említeni. Az új elsődleges szerver használható a korábbi változatokat futtató replikákkal együtt is; az új funkciókkal kapcsolatos adatok egyszerűen nem kerülnek replikálásra az alacsonyabb szintű szerverekre. A replikaszerver átállítása után exportálni kell a replikációs topológia bejegyzéseit az elsődleges szerverről és fel kell venni őket mindegyik replikába. A bejegyzések exportálásához használja a Qshell parancsori eszközt "ldapsearch" oldalszám: 206 és mentse el a kimenetet egy fájlba. A keresési parancs az alábbihoz hasonló lesz:

```
ldapsearch -h elsődleges_szerver_hosztnev -p elsődleges_szerver_port \  
-D elsődleges_szerver_admin_DN -w  
elsődleges_szerver_admin_jelszo \  
-b ibm-replicagroup=default,utótag_bejegyzés_DN \  
-L "(|(objectclass=ibm-replicaSubEntry)(objectclass=ibm-replicationAgreement))" \  
> replication.topology.ldif
```

Ez a parancs létrehoz egy replication.topology.ldif nevű LDIF kimeneti fájlt az aktuális munkakönyvtárban. A fájl csak az új bejegyzéseket tartalmazza.

Megjegyzés: Ne vegye be az alábbi utótagokat:

- cn=changelog
- cn=localhost
- cn=pwdpolicy
- cn=schema
- cn=configuration

Csak a felhasználó által létrehozott utótagokat használja.

Ismételje meg a parancsot az elsődleges szerver mindegyik utótagjára, de “>” helyett “>>” karaktereket írjon, hogy a további keresések során az adatok ne felülírják a kimeneti fájlt, hanem hozzáfűzésre kerüljenek. A fájlt elkészülte után másolja át a replikaszerverekre.

A replikaszerverekre átállításuk után vegye fel a fájlt; véletlenül se adja azonban hozzá a fájlt a címtárszerver korábbi változatait futtató szerverekhez. A fájl felvétele előtt el kell indítania és le kell állítania a szervert.

A szerver elindításához használja az iSeries navigátor **Indítás** parancsát. További információk: “Directory Server indítása/leállítása” oldalszám: 112.

A szerver leállításához használja az iSeries navigátor **Leállítás** parancsát. További információk: “Directory Server indítása/leállítása” oldalszám: 112.

Amikor felveszi a fájlt a replikaszerverre, ügyeljen rá, hogy a replikaszerver ne működjön. Az adatok felhasználásához használja az iSeries navigátor **Fájl importálása** parancsát.

A replikációs topológia bejegyzéseinek betöltése után indítsa el újra a replikaszervert, majd folytassa a replikációt. A replikáció folytatásának módjai:

- Az elsődleges szerveren használja a webes adminisztrációs eszköz **Replikációkezelés sorainak kezelése** parancsát.
- Használja az **ldapexop** parancssori segédprogramot. Például:

```
ldapexop -h elsődleges_szerver_hozstnév -p elsődleges_szerver_port \  
-D elsődleges_szerver_admin_DN -w elsődleges_szerver_admin_jelszó \  
-op controlrepl -action resume -ra replika_megállapodás_DN
```

Ez a parancs újra elindítja a megadott DN-ű bejegyzésben meghatározott szerver replikációját.

Az, hogy melyik replikációs megállapodás DN tartozik egy replikaszerverhez, a replication.topology.ldif fájl alapján állapítható meg. Az elsődleges szerver egy üzenetet naplóz, amikor elindul a replikáció egy adott replikával és egy figyelmeztetést, ha a replikaszervernek a megállapodásban megadott azonosítója nem egyezik a replikaszerver tényleges azonosítójával. A replikációs megállapodás frissítéséhez, hogy a megfelelő szerverazonosítót használja, alkalmazza a webes adminisztrációs eszköz **Replikációkezelés** részét, vagy használja az **ldapmodify** parancssori eszközt. Például:

```
ldapmodify -h elsődleges_szerver_hozstnév -p elsődleges_szerver_port \  
-D elsődleges_szerver_admin_DN -w elsődleges_szerver_admin_jelszó \  
dn: replikációs_megállapodás_DN \  
changetype: modify \  
replace: ibm-replicaConsumerID \  
ibm-replicaConsumerID: replikaszerver_ID
```


Ezeket a parancsokat beírhatja közvetlenül a parancssorban, vagy elmentheti őket egy LDIF fájlba és megadhatja az **-i fájl** paraméterrel. A parancs leállításához az **Előző kérés leállítása** lehetőséget használhatja.

Ezzel a replika átállítása befejeződött.

Ha egy korábbi változattal akarja használni tovább a replikát, akkor is vissza kell állítania a replikáció működését az **ldapexop** parancssori eszközzel vagy a webes adminisztrációs eszköz **Replikációkezelés** részének használatával. Ha egy korábbi változatot futtató replika később átállításra kerül, használja az **ldapdiff** parancssori eszközt a címtár adatok szinkronizálására. Ez garantálja, hogy a nem replikált bejegyzések vagy attribútumok is frissítésre kerüljenek a replikán.

Kerberos szolgáltatás megváltozott neve

A V5R3 kiadásban módosult a címtárszerver és a kliens API-k által a GSSAPI (Kerberos) hitelesítéshez használt szolgáltatás neve. E módosítás eredményeképp a rendszer nem működik együtt a V5R3 előtt használt szolgáltatásnévvel (a V5R2M0 PTF 5722SS1-SI08487 már ugyanezt a módosítást tartalmazza).

A V5R3 kiadás előtt a Directory Server és kliens API-jai egy LDAP/dns-hoztnév@Kerberos-tartomány formátumú szolgáltatásnevet használtak, ha a hitelesítés a GSSAPI mechanizmussal (Kerberoszal) történt. Ez a név nem felel meg a GSSAPI hitelesítést leíró szabványoknak, amely szerint az azonosító neve kisbetűs "ldap" karakterekkel kell, hogy kezdődjön. Ennek eredményeképpen előfordulhat, hogy a Directory Server és kliens API-jai nem működnek együtt más gyártók termékeivel. Ez különösen igaz akkor, ha a Kerberos kulcsterjesztő központ (KDC) érzékeny a kis- és nagybetűk különbségére az azonosítóknak. A JNDI LDAP szolgáltatója, ez a gyakran használt Java LDAP kliens API például olyan kliens, amelyik része az operációs rendszernek és a helyes szolgáltatásnevet használja.

A V5R3M0 kiadásban a szolgáltatás neve módosult, hogy megfeleljen a szabványoknak. Ez azonban saját kompatibilitási problémákat vet fel.

- A GSSAPI hitelesítés használatára beállított címtárszerver nem fog elindulni e kiadás telepítése után. Ez azért történik meg, mert a szerver által használt keytab fájlban a régi szolgáltatásnévnek (LDAP/mysys.ibm.com@IBM.COM) megfelelő hitelesítési adatok találhatók, a szerver viszont már az új szolgáltatásnéven (ldap/mysys.ibm.com@IBM.COM) keresi a hitelesítési adatokat.
- Előfordulhat, hogy a V5R3M0 kiadás LDAP API-jait használó címtárszerver vagy LDAP alkalmazás nem képes hitelesíteni magát régebbi OS/400 szerverekhez és kliensekhez. Ez az alábbi módon orvosolható:
 1. Ha a KDC megkülönbözteti a kis- és nagybetűket, akkor hozzon létre egy fiókot a helyes szolgáltatásnévvel (ldap/mysys.ibm.com@IBM.COM).
 2. Frissítse az Directory Server által használt keytab fájlt, hogy az már az új szolgáltatásnév hitelesítési adatait tartalmazza. Érdemes lehet törölni a régi hitelesítési adatokat. A keytab fájl frissítéséhez a Qshell keytab segédprogram használható. Alapértelmezés szerint a címtárszerver /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab fájlt használja. A V5R3M0 iSeries navigátorának Hálózati hitelesítési szolgáltatás (Kerberos) varázslója szintén tartalmaz keytab bejegyzéseket az új szolgáltatáshoz.
 3. Frissítse a V5R2M0 kiadású, GSSAPI-t használó OS/400 rendszereket a 5722SS1-SI08487 sorszámú PTF-fel.

Alternatív megoldásként használhatja a címtár szerver és kliens API-jaiban a régi szolgáltatásnevet. Ez akkor lehet célszerű, ha vegyes rendszerben használ Kerberos hitelesítést, amelyben vannak is telepítve PTF-ek meg nem is. Ehhez állítsa be a LDAP_KRB_SERVICE_NAME környezeti változót. A teljes rendszerre vonatkozóan az alábbi paranccsal állíthatja be (szükséges ahhoz, hogy a szolgáltatás nevét be tudja állítani a szerveren):

```
ADDENVVAR ENVVAR(LDAP_KRB_SERVICE_NAME)
```

vagy a QSH-n belül (az adott QSH szekción belüli LDAP segédprogramokat befolyásolja):

```
export LDAP_KRB_SERVICE_NAME=1
```

Directory Server megtervezése

Mielőtt nekilátna a Directory Server telepítésének és az LDAP címtár konfigurálásának, szánjon 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 címtárszerver működéséhez. További információk: “Javasolt példák a címtár felépítésére” oldalszám: 96, “Címtárak” oldalszám: 7, “Utótag (névkontextus)” oldalszám: 14 és “Attribútumok” oldalszám: 19.
- **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 Directory Server 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 is. Sokkal több lesz akkor is, ha nagyméretű objektumokat, pl. képeket szándékozik tárolni.

- **Az alkalmazandó biztonsági intézkedések eldöntése.**

A Directory Server lehetővé teszi egy jelszó irányelv kialakítását, amely kényszeríti a felhasználókat a jelszavak időszakos cseréjére, valamint megköveteli, hogy a szervezeten belül használt jelszavak megfeleljenek bizonyos szintaktikai követelményeknek.

A Directory Server támogatja a Védett socket réteg (SSL) és a digitális igazolások, valamint a kommunikáció biztonsága érdekében a Fordítási réteg biztonság (TLS) használatát. A Kerberos hitelesítés ugyancsak támogatott.

A Directory Server megengedi, hogy hozzáférés vezérlési listák (ACL-ek) segítségével szabályozza a címtár objektumaihoz való hozzáférést. A címtár védelmére használhatja az operációs rendszer biztonsági ellenőrzést is. Továbbá eldöntheti, melyik jelszó irányelvet alkalmazza.

- **Adminisztrátori DN és jelszó választása.** Az alapértelmezett adminisztrátori DN a `cn=admin`. A szerver első beállításakor ez az egyetlen olyan azonosság, amelyik jogosult címtárbejegyzéseket létrehozni és módosítani. Használhatja az alapértelmezett adminisztrátori DN-t, vagy megadhat egy másikat. Az adminisztrátori DN-hez jelszót is meg kell adni.
- **Directory Server webes adminisztrációs eszköz előfeltétel szoftvereinek telepítése.** A Directory Server webes adminisztrációs eszközhöz az alábbi termékeknek kell telepítve lenniük az iSeries szerveren.
 - IBM HTTP Server for iSeries (5722-DG1)
 - IBM WebSphere Application Server - Express (5722-IWE Base and Option 2)

Az IBM HTTP Server for iSeries és IBM WebSphere Application Server - Express termékekkel kapcsolatos további információkat az IBM HTTP Server témakörben talál.

Directory Server beállítása

1. 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 Directory Server automatikusan egy korlátozott alapértelmezés szerinti konfigurációt telepít. “A Directory Server alapértelmezett konfigurációja” oldalszám: 91 helyen további tájékoztatást kaphat. A Directory Server egy varázslót biztosít a Directory Server az egyedi igények szerint történő konfigurálásának támogatására. Ez a varázsló az EZ-Setup részeként futtatható, vagy később az iSeries navigátorból. A varázsló használata különösen ajánlott a címtárszerver elsődleges beállításához. Használhatja a varázslót a címtárszerver újrakonfigurálásakor is.

Megjegyzés: Amikor a varázslót a címtárszerver újrakonfigurálása céljából indítja el, akkor a konfigurálás “tisztalappal” indul. Az eredeti konfiguráció törlésre kerül a módosítás helyett. Azonban a címtár adatok nem törölődnek, hanem abban a könyvtárban maradnak meg, amely a telepítés alkalmával lett kiválasztva (alapértelmezés szerint ez QUSRDIRDB könyvtár). A változtatási 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 címtárszerver konfigurációját, de nem törli ki teljesen azt, akkor kattintson a jobb oldali egérgombbal a **Címtár** felíratra, majd válassza a **Tulajdonságok** lapot. Így megmarad az eredeti beállítás.

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

2. A Directory Server konfigurációs varázsló az alábbi módokon indítható:
 - a. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
 - b. Bontsa ki a **Szerverek** elemet.
 - c. Kattintson a **TCP/IP** pontra.
 - d. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** felíratra, majd válassza a **Beállítás** menüpontot.

Megjegyzés: Ha már egyszer beállította a címtárszervert, akkor a **Beállítás** elem helyett az **Újrakonfigurálás** lehetőséget válassza.

3. Kövesse a Címtárszerver beállító varázsló utasításait a Directory Server helyes beállításához.

Megjegyzés: Érdeemes lehet ezt a könyvtárat (amely a címtár adatait tartalmazza), egy felhasználói lemeztárban (ASP) tárolni a rendszer ASP helyett. Nem tárolható azonban a könyvtár független ASP-ben, és minden olyan kísérlet, amikor független ASP-ben lévő könyvtárral kívánja a szervert konfigurálni, újrakonfigurálni vagy indítani, meghiúsul.

4. A varázsló működésének befejeztével a Directory Server alapszintű konfigurációja készen áll. Ha a rendszeren Lotus Domino fut, akkor lehet, hogy a 389-es portot (az LDAP szerver alapértelmezett portját) már használja a Domino LDAP funkciója. A következők egyikét teheti:
 - Megváltoztatja a Lotus Domino által használt portot. További információkat az E-mail témakörben, a “Domino LDAP és Directory Server működtetése ugyanazon az iSeries szerveren” részben talál.
 - Megváltoztatja a Directory Server által használt portot. További információk: “Port vagy IP cím módosítása” oldalszám: 117.
 - Megadott IP címekeket használ. További információk: “Port vagy IP cím módosítása” oldalszám: 117.
5. A beállított utótagoknak megfelelő bejegyzéseket készít. További információk: “Directory Server utótagok felvétele és eltávolítása” oldalszám: 118.

A folytatás előtt azonban célszerű az alábbiakban felsorolt dolgok közül néhányat vagy az összeset elvégezni:

- Adatok importálása a szerverre. Részletek: “LDIF fájl importálása/exportálása” oldalszám: 93.
- SSL (Védett socket réteg) biztonság engedélyezése. Részletek: “SSL és TSL engedélyezése a Directory Serveren” oldalszám: 154.
- Kerberos hitelesítés engedélyezése. Részletek: “Kerberos hitelesítés engedélyezése a Directory Server-hez” oldalszám: 156.
- Utalás beállítása. Részletek: “Szerver kijelölése címtári utalások részére” oldalszám: 118.

A Directory Server alapértelmezett konfigurációja

A Directory Server az i5/OS rendszerrel együtt automatikusan telepítésre kerül. Ez a telepítés tartalmaz egy alapértelmezés szerinti konfigurációt. A Directory Server akkor használja az alapértelmezés szerinti konfigurációt, ha az alábbi feltételek mind teljesülnek:

- A rendszergazdák nem futtatták a Directory Server konfigurációs varázslóját és nem módosították a tulajdonságlapokon a címtár beállításait.
- A Directory Server közzététel nincs beállítva.
- A Directory Server nem talál LDAP DNS információkat.

Ha a Directory Server az alapértelmezés szerinti konfigurációt használja, akkor a következők történnek:

- A Directory Server automatikusan elindul a TCP/IP alrendszerrel.

- 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 Directory Server tulajdonságlapon.
- 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.
- A Directory Server 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 be lett állítva egy digitális igazolás, akkor a Védett socket réteg (SSL) engedélyezésre kerül, és a védett kommunikáció a 636-os portot használja.

A cím tár feltöltése

A cím tár feltöltésére számos út kínálkozik. További információk:

- “Információk publikálása a cím társzervernek”
- “LDIF fájl importálása/exportálása” oldalszám: 93
- “Felhasználók másolása HTTP szerver ellenőrzési listából a Directory Serverbe” oldalszám: 94

Információk publikálása a cím társzervernek

Rendszerét úgy konfigurálhatja, hogy az bizonyos információkat, , valamint a felhasználó által megadott információkat közlétegyen ugyanazon a rendszeren vagy egy másik rendszeren található Directory Server számára. Az operációs rendszer automatikusan publikálja a Directory Server számára ezeket az információkat, amikor az iSeries navigátor használatával módosítja az i5/OS rendszerben ezeket az információkat. A közzétehető információk lehetnek rendszer (több rendszer és nyomtató) információk, nyomtatásmegosztási, felhasználói információk, valamint TCP/IP QoS szabályok (további információk: “Közzététel” oldalszám: 35).

Ha nem létezik az a szülő DN, amely számára az adatok közzétételre kerülnek, a Directory Server automatikusan létrehozza azt. Más i5/OS alkalmazásokat is telepíthet, amelyek információkat tehetnek közzé egy LDAP cím tárba. Továbbá alkalmazásprogram csatolókat (API-kat) is meghívhat a saját programjából, hogy más típusú adatokat tegyen közzé az LDAP cím tárban.

Megjegyzés: Publikálhat i5/OS információkat olyan cím társzerver számára is, amely nem i5/OS felügyelete alatt működik, amennyiben ez a szerver be van állítva az IBM séma használatára.

Konfigurálja rendszerét az alábbi lépések szerint, ha i5/OS információkat akar egy cím társzerver számára közzétenni:

1. Az iSeries navigátorban a jobb oldali egérgombbal kattintson rendszerére, és válassza a **Tulajdonságok** lapot.
2. Kattintson a **Directory Server** lapra.
3. Válassza ki a közzétenni kívánt információ típusokra.

Java s lat:

Ha egynél többféle információ típus t kíván küldeni ugyanarra a helyre, idő t takaríthat meg, ha egyszerre több információ típus t választ ki beállítás céljából. A Műveletek navigátor az első információ típus hoz beadott értéket alapértelmezett értéknek fogja tekinteni a többi információ típus beállításánál.

4. Kattintson a **Részletek** ikonra.
5. Kattintson a **Rendszer információk közzététele** jelölőnégyzetre.
6. Adja meg a szerveren használni kívánt **hitelesítési módszert**, továbbá a megfelelő hitelesítési információkat.
7. Kattintson az **(aktív) cím társzerver** mező melletti **Módosítás** gombra. A megjelenő kiugró párbeszéd dobozba írja be annak a cím társzervernek a nevét, amelyen az i5/OS információt közzétenni kívánja, majd kattintson az **OK** gombra.
8. Az **Under DN** mezőben adja meg annak a szülő nek az egyedi nevét (DN), ahonnan információt kíván a cím társzervernek átadni.
9. Töltse ki a **Szerver kapcsolat** keretben azokat a mezőket, melyek megfelelnek konfigurációjának.

Megjegyzés: SSL-t vagy Kerberos-t használó címtárszerver számára akkor lehet i5/OS információkat közzétenni, ha a címtárszerver be lett állítva a megfelelő protokoll használatára. További információk az SSL és Kerberos használatával kapcsolatban: “Kerberos hitelesítés használata Directory Server-rel” oldalszám: 48.

10. Ha a címtárszerver nem az alapértelmezett portot használja, adja meg a portszámot a **Port** mezőben.

11. Kattintson az **Ellenőrzés** ikonra, hogy meggyőződhessen arról, hogy a szerveren létezik-e a DN szülő, és helyesek-e a kapcsolódási információk. Ha a címtár elérési útja nem létezik, egy párbeszédpanelen megadhatja azt.

Megjegyzés: Ha a DN szülő nem létezik, és nem hozza létre azt, a közzététel sikertelen lesz.

12. Kattintson az **OK** gombra.

Megjegyzés: Közzétehető egy másik platformon működő címtárszerver számára is i5/OS információkat. Csak akkor tehető közzé felhasználói és rendszer információkat egy címtárszerveren, ha az a IBM Directory Server sémával kompatibilis sémát használ. Az IBM címtár sémájával kapcsolatos további információk: “IBM Directory Server sémája” oldalszám: 16.

API-k i5/OS információk címtárszerveren közzétételéhez

A Directory Server beépített közzétételi támogatást biztosít a felhasználói és rendszerinformációkhoz. Az elemek listáját a rendszerek **Directory Server** oldalának **Tulajdonság** párbeszédablaka tartalmazza. Az LDAP szerver konfigurációjának és a közzétételi API-k segítségével i5/OS programok készíthetők más típusú információk közzétételére. Ezután ezek az információ típusok is szerepelnek a **Directory Server** 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, közzétételi ügynöknek (publishing agent) nevezzük. A közzétett információ típusára, ahogy az megjelenik a **Directory Server** lapon, az ügynök nevével hivatkozunk.

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

QgldChgDirSvrA

Az alkalmazás a CSVSR0500 formátumot használja a kezdeti ügynöknev hozzáadásához, amely a letiltott tételek között szerepel. Az alkalmazás felhasználóinak szóló leírásokban utasítsa őket, hogy az iSeries navigátoron keresztül menjen a Directory Server tulajdonságlapra a közzétételi ügynök konfigurálása céljából. Az ügynöknevekre példák lehetnek a rendszer- és ügynöknevek, amelyek **Directory Server** oldalon automatikusan rendelkezésre állnak.

QgldLstDirSvrA

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

QgldPubDirObj

Ezzel az API-val végezheti el az információ tényleges közzétételét.

Ezekről az API-król további információt az iSeries Információs központ Egyszerűsített címtárhozzáférési protokoll (LDAP) témánál a Programozás fejezet alatt talál.

LDIF fájl importálása/exportálása

LDIF fájl importálása

Különböző Directory Server-ek között az információcserére LDAP Data Interchange Format (LDIF) formátumú fájlokkal lehetséges. További információk: “LDAP adatcsere formátum (LDIF)” oldalszám: 220. Mielőtt elindítaná ezt a műveletet, vigye át adatfolyam fájlként az LDIF fájlt az iSeries szerverre.

Az LDIF fájlt az alábbi lépésekkel importálhatja a Directory Server-re:

1. Ha a címtárszerver működik, állítsa le azt. Információk a címtár szolgáltató leállítására vonatkozóan: “Directory Server indítása/leállítása” oldalszám: 112.
2. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.

3. Bontsa ki a **Szerverek** elemet.
4. Kattintson a **TCP/IP** pontra.
5. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, és válassza a **Eszközök**, majd a **Fájl importálása** elemet.

Az **Importált adatok replikálása** négyzet megjelölésével beállíthatja azt is, hogy a szerver a frissen importált adatokat replikálja, amikor legközelebb bekapcsolásra kerül. Ez hasznos például, ha új bejegyzéseket vesz fel a címtárfába az elsődleges szerveren. Ha adatokat importál, mert inicializálni akar egy replika- (vagy egy egyenrangú) szerveret, akkor általában nincs szükség az adatok replikálására, mivel azok már megtalálhatók lehetnek azokon a szervereken, amelyek számára ez az adott szerver szolgáltató.

Megjegyzés: Az LDIF fájlok importálásához használhatja az ldapadd segédprogramot is (részletek: "ldapmodify és ldapadd" oldalszám: 191).

LDIF fájl importálása

Különböző Directory Server-ek között az információcsere LDAP Data Interchange Format (LDIF) formájú fájlokkal lehetséges ("LDAP adatcsere formátum (LDIF)" oldalszám: 220). LDIF fájlba menthető az LDAP címtár egésze vagy csak egy része.

Egy LDIF fájl exportálása a címtárszerverből:

1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, és válassza a **Eszközök**, majd a **Fájl exportálása** elemet.

Megjegyzés: Ha nem ad meg egy teljes képzésű elérési utat, hogy az LDIF fájl hova exportáljon adatokat, akkor a fájl az operációs rendszer felhasználói profiljában megadott saját könyvtárba készül.

5. Adja meg, hogy a **Teljes címtár exportálása** vagy a **Kiválasztott részfa exportálása** a feladat, illetve hogy szükséges-e a **Műveleti attribútumok exportálása**. Az exportált műveleti attribútumok a creatorsName, createTimestamp, modifiersName és modifyTimestamp.

Megjegyzések:

1. Ha az adatokat azért exportálja, hogy V5R3 vagy korábbi címtárba importálja, akkor ne válassza ki a **Műveleti attribútumok exportálása** lehetőséget. Ezek a műveleti attribútumok nem importálhatók V5R3 vagy korábbi címtárszerverekbe.
2. Az ldapsearch segédprogrammal teljes vagy részleges LDIF fájlt hozhat létre ("ldapsearch" oldalszám: 206). Használja az -L kapcsolót és irányítsa fájlba a kimenetet.
3. Ne felejtse 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 az **Engedély** elemet.

Felhasználók másolása HTTP szerver ellenőrzési listából a Directory Serverbe

Ha HTTP szervert használ vagy azt használt a múltban, lehet, hogy létrehozta az ellenőrzőlistákat az internetes felhasználók és jelszavaik tárolására. Amikor WebSphere alkalmazáskiszolgálóra, portálszerverre vagy más, az LDAP hitelesítést támogató alkalmazásra áll át, akkor lehet, hogy továbbra is használni kívánja a meglévő internetes felhasználókat és jelszavakat. Ez az "Ellenőrzőlista címtárba másolása" API, QGLDCPYVL használatával tehető meg.

A QGLDCPYVL kiolvassa az ellenőrzőlista bejegyzéseit és létrehozza a megfelelő LDAP objektumokat a helyi címtárszerverből. Az objektumok userPassword attribútummal rendelkező váz inetOrgPerson bejegyzések lesznek, amelyek az ellenőrzőlista-bejegyzések jelszó-információinak másolatát tartalmazzák. Megadható, hogy hogyan és mikor kerüljön meghívásra ez az API. Egyszeri műveletként is használhatja ezt nem módosítandó ellenőrzőlista esetén, vagy ütemezett feladatként is beállíthatja, hogy a címtárszerver frissüljön, és tükrözze az ellenőrzőlista új bejegyzéseit.

| A QGLDCPYVL API teljesebb leírását lásd: Directory Server API-k. Ha érdeklí egy példa egy API használatáról, tekintse meg a következő részt: "Példahelyzet: Felhasználók másolása HTTP szerver ellenőrzési listából a Directory Serverbe".

| **Példahelyzet: Felhasználók másolása HTTP szerver ellenőrzési listából a Directory Serverbe**

| **Körülmények és áttekintés**

| Van egy jelenleg (Apache) HTTP szerveren futó alkalmazása, amely a MYLIB/HTTPVLDL ellenőrzőlistában található internetes felhasználókkal dolgozik. Ugyanezeket az internetes felhasználókat használhatja a WebSphere alkalmazáskiszolgálóban (WAS) LDAP hitelesítéssel. Hogy a felhasználói információkat ne kelljen duplán karbantartani az ellenőrzőlistában és az LDAP-ban, a HTTP szerveralkalmazás is beállítható az LDAP hitelesítés használatára.

| Ennek megvalósításához a következőket kell tenni:

- | 1. Másolja át a meglévő ellenőrzőlista-felhasználókat a helyi cím társzerverre.
- | 2. Állítsa be a WAS szerveret az LDAP hitelesítés használatára.
- | 3. Állítsa át a HTTP szerveret, hogy az LDAP hitelesítést használja az ellenőrzőlista helyett.

| **1. lépés: A meglévő ellenőrzőlista-felhasználók átmásolása a helyi cím társzerverre**

| Ez a lépés feltételezi, hogy a cím társzerver előzőleg az "o=my company" utótaggal volt beállítva, és fut. Az LDAP felhasználóknak a "cn=users,o=my company" részében kell lenniük. A cím társzerver adminisztrátorának megkülönböztetett neve "cn=administrator" és az adminisztrátori jelszó "secret".

| Hívja meg az API-t a parancssorból a következők szerint:

```
| CALL PGM(QSYS/QGLDCPYVL) PARM('HTTPVLDL MYLIB ' 'cn=administrator' X'00000000' 'secret'  
| X'00000000' 'cn=users,o=my company' X'00000000' ' X'00000000' X'00000000')
```

| Ha kész, a cím társzerver inetorgperson bejegyzéseket fog tartalmazni az ellenőrzőlista bejegyzései alapján. A következő ellenőrzőlista-felhasználó esetében például:

```
| Felhasználónév: jsmith  
| Leírás: John Smith  
| Jelszó: *****
```

| a következő cím társzerverbejegyzés keletkezik:

```
| dn: uid=jsmith,cn=users,o=my company  
| objectclass: top  
| objectclass: person  
| objectclass: organizationalperson  
| objectclass: inetorgperson  
| uid: jsmith  
| sn: jsmith  
| cn: jsmith  
| description: John Smith  
| userpassword: *****
```

| Ez a bejegyzés most már felhasználható a hitelesítésre a cím társzerverhez. Az alábbi QSH ldapsearch parancs például ki fogja olvasni a kiszolgáló root DSE bejegyzését:

```
| > ldapsearch -D "uid=jsmith,cn=users,o=my company" -w ***** -s base "(objectclass=*)"
```


| Ha a cím társzerverbejegyzések létrejöttek, akkor módosíthatók, hogy további információkat is tartalmazzanak. Lehet például, hogy módosítani kívánja a cn és sn értékeket a felhasználó teljes nevére és vezetéknévére, vagy fel szeretne venni egy telefonszámot és egy e-mail címet.

| **2. lépés: Állítsa be a WAS szerveret az LDAP hitelesítés használatára.**

| A WAS LDAP biztonsági szolgáltatást be kell állítani, hogy megkeresse a dn "cn=users,o=my company" alatti bejegyzéseket egy keresési szűrő használatával, amely a beírt felhasználónevet az uid attribútumértéket tartalmazó inetOrgPerson bejegyzésekre képezi le. A jsmith néven végzett hitelesítés a WAS kiszolgálóhoz például az "(uid=jsmith)" keresési szűrőnek megfelelő bejegyzések keresését fogja eredményezni. További információkért lásd a WebSphere Application Server for iSeries információs központ LDAP keresési szűrők beállítása c. anyagát.

| A HTTP szerver átállítása, hogy az LDAP hitelesítést használja az ellenőrzőlista helyett

| **Megjegyzés:** Az alábbiakban leírt eljárás a példahelyzetben leírt példák illusztrálását szolgálja azáltal, hogy magas szintű áttekintést nyújt a HTTP szerver beállításáról az LDAP hitelesítés használatára. Részletesebb információkat talál az Implementation and Practical Use of LDAP on the IBM eServer iSeries Server,

| SG24-6193  IBM Redbook kiadvány 6.3.2. fejezetében: "Setting up LDAP authentication for the powered by Apache server", valamint a Jelszavas védelem beállítása (Apache) HTTP szerveren című dokumentumban.

- | 1. Kattintson a **Beállítás** lap **Alapszintű hitelesítés** menüpontjára HTTP szervere eléréséhez a HTTP adminisztrációs eszközben.
- | 2. A **Felhasználói hitelesítési módszer** alatt módosítsa az **Internetes felhasználók alkalmazása az ellenőrzőlistában** lehetőséget az **LDAP szerver felhasználói bejegyzéseinek alkalmazása** lehetőségre, majd kattintson az **OK** gombra.
- | 3. Térjen vissza a **Beállítás** lapra és kattintson a **Hozzáférés felügyelete** menüpontra. Állítsa be ezt a fent hivatkozott Redbook kiadványban leírtaknak megfelelően, és kattintson az **OK** gombra.
- | 4. A **Beállítás** lapon kattintson az **LDAP hitelesítés** lehetőségre.
 - | a. Adja meg az LDAP szerver hosztnevét és portját. A **Felhasználói keresés alapszintű megkülönböztetett név**-hez írja be: cn=users,o=my company.
 - | b. Az **Egyedi LDAP DN létrehozása felhasználói hitelesítéshez** alatt adja meg a következő szűrőt: (&objectclass=person)(uid=%v1)).
 - | c. Adja meg a csoportinformációkat és kattintson az **OK** gombra.
- | 5. Állítsa be a kapcsolatot az LDAP szerverrel a fent hivatkozott Redbook kiadványban leírtaknak megfelelően.

| Javasolt példák a címtár felépítésére

| A Directory Servert gyakran használják felhasználók és csoportok lerakataként is. Ebben a részben néhány ajánlott gyakorlati módszerről lesz szó egy felhasználók és csoportok felügyeletére optimalizált struktúra beállításához. Ez a struktúra és a hozzátartozó biztonsági modell a címtár más használati módjaira is kiterjeszthető.

| A felhasználók általában egyetlen vagy nagyon kevés helyen tárolódnak. Lehet, hogy csak egyetlen tárolója van, a cn=users, és ez az összes felhasználó szülőbejegyzése, vagy külön tárolók vannak felhasználók különböző, külön adminisztrált halmazaihoz. Az alkalmazottak, szállítók és a saját magukat bejegyző internetes felhasználók például elhelyezhetők a cn=employees, cn=vendors és cn=internet users objektumok alatt. Csábító lehet az embereket azok alatt a szervezetek alatt elhelyezni, amelyekhez tartoznak, ez azonban nehézségeket okozhat, amikor más szervezetekhez kerülnek, mivel ekkor a címtárbejegyzést is át kell helyezni, és frissíteni a csoportokat vagy más (a címtárban külsőnek vagy belsőnek számító) adatforrásokat, hogy az új megkülönböztetett nevet tükrözzék. A felhasználók és a szervezeti felépítés közötti viszony a felhasználói bejegyzésen belül is megfogható az olyan címtárattribútumok használatával, mint az "o" (szervezet neve), "ou" (szervezeti egység neve), illetve a departmentNumber, amely a szabványos séma része az organizationalPerson és inetOrgPerson esetében.

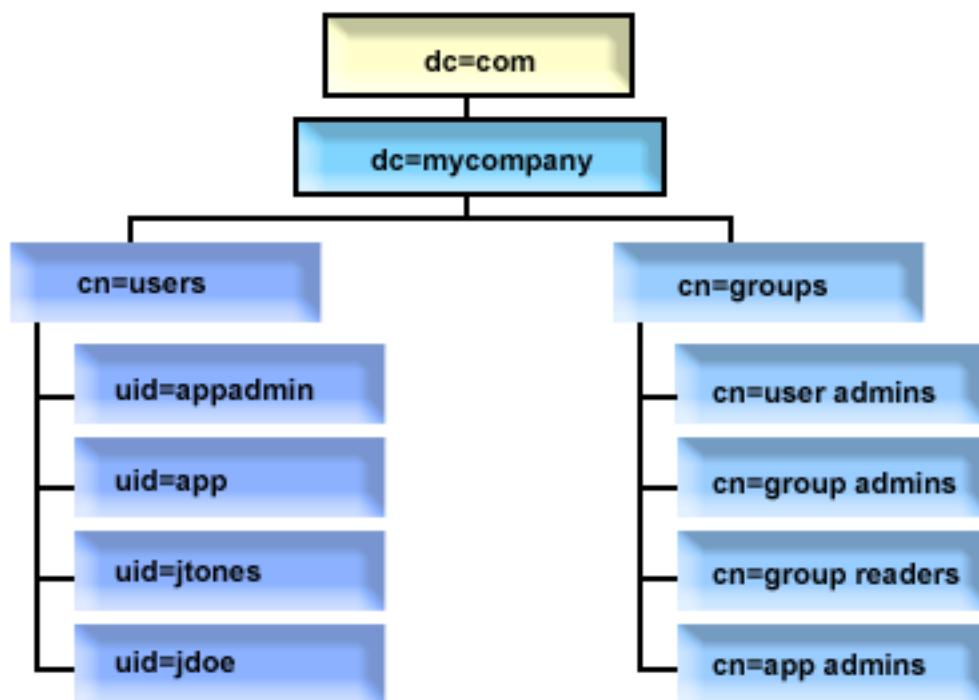
| Ugyanígy, a csoportok általában egy külön tárolóban (például "cn=groups") találhatóak.

| A felhasználók és csoportok ilyen szervezésével csak néhány hely van, ahol a hozzáférés-felügyeleti listákat (ACL-eket) be kell állítani.

| A címtárszerver használatának és a csoportok felügyeletének módjától függően esetleg használni kívánja a következő hozzáférés-felügyeleti minták valamelyikét:

- Ha a címtár címjegyzékként szolgál az alkalmazásokhoz, akkor érdemes lehet a speciális `cn=anybody` csoportnak olvasási és keresési jogosultságokat adni a `cn=users` tárolóban és szülőobjektumaiban található "normál" attribútumokhoz.
- Gyakran csak bizonyos alkalmazások és csoportadminisztrátorok által használt megkülönböztetett neveknek kell elérniük a `cn=groups` tárolót. Érdemes lehet létrehozni egy csoportot, amely a csoportadminisztrátorok megkülönböztetett neveit tartalmazza, és ezt a `cn=groups` és alárendeltjei tulajdonosává tenni. Érdemes létrehozni egy másik csoportot is, amely az alkalmazások által a csoportinformációk kiolvasására használt DN-eket tartalmazza, és ennek olvasási és keresési jogosultságokat adni a `cn=groups` objektumhoz.
- Ha a felhasználó objektumokat közvetlenül a felhasználók frissítik, akkor a speciális `cn=this` hozzáférési azonosítóhoz valószínűleg hozzá kívánja rendelni a megfelelő olvasási, írási és keresési jogosultságokat.
- Ha a felhasználók az alkalmazásokból kerülnek frissítésre, akkor az alkalmazások gyakran saját azonosságuk alatt futnak, és csak az alkalmazásoknak van szükségük jogosultságokra a felhasználó objektumok frissítéséhez. Mégegyszer, kényelmes ezeket a megkülönböztetett neveket hozzáadni egy csoporthoz (pl. `cn=user administrators`), és a csoportnak megfelelő jogosultságokat adni a `cn=users` objektumhoz.

Ezt a fajta felépítést és hozzáférés-felügyeletet alkalmazva az induló címtár az alábbihoz hasonló lehet:



3. ábra: Példa címtárstruktúra

- A `cn=mycompany`, `dc=com` tulajdonosa a címtáradminisztrátor vagy a csoport más felhasználója, aki elegendő jogosultsággal rendelkezik a címtár legfelsőbb szintjének kezeléséhez. A kiegészítő ACL bejegyzések olvasási hozzáférést biztosítanak valamelyik `cn=anybody` vagy `cn=authenticated` objektum normál attribútumaikhoz, vagy akár néhány más csoporthoz is, ha korlátozóbb ACL-re van szükség.
- A `cn=users` objektumnak az alábbiakban leírtakon túl is vannak ACL bejegyzései a felhasználók megfelelő hozzáféréseinek biztosítására. Az ACL-ek lehetnek:
 - olvasási és keresési hozzáférések a `cn=anybody` vagy `cn=authenticated` objektumok normál attribútumaihoz
 - olvasási és keresési hozzáférések a kezelők normál és érzékeny attribútumaihoz
 - más kívánt ACL bejegyzések, amelyek esetleg írási hozzáférést adnak egyes személyeknek saját bejegyzésükhöz.

Megjegyzés:

- Az olvashatóság fokozására a bejegyzések RDN bejegyzéseit kell használni a teljes megkülönböztetett nevek helyett. A "user admins" csoport teljes megkülönböztetett neve tagként például uid=app,cn=users,dc=mycompany,dc=com, nem pedig a rövidebb uid=app.
- Bizonyos felhasználók és csoportok kombinálhatók. Ha az alkalmazás adminisztrátorának például jogosultságokra volt szüksége a felhasználók kezeléséhez, az alkalmazás futhat az alkalmazás adminisztrátorának megkülönböztetett neve alatt. Ez azonban korlátozhatja például azt a lehetőséget, hogy az alkalmazás adminisztrátori jelszava módosítható legyen anélkül, hogy az alkalmazásban is új jelszót kéne beállítani.
- Miközben a fentiekben bemutattunk néhány jó gyakorlati módszert a csak egyetlen alkalmazás által használt címtárakhoz, talán sokkal célszerűbb, ha minden frissítés címtáradminisztrátori hitelesítéssel zajlik. Ez a gyakorlat korábban tárgyalt okokból nem javasolt.

Webes adminisztráció

A webes adminisztrációs konzolról egy vagy több Directory Server felügyelhető. A webes adminisztrációs konzolon a következő feladatok végezhetők el:

- A felügyelt Directory Server-ek listájának felvétele és módosítása.
- Egy Directory Server adminisztrációja a webes adminisztrációs eszközzel.
- A webes adminisztrációs konzol jellemzőinek módosítása.

A webes adminisztrációs konzol használatának módja:

1. Ha első alkalommal használja a Directory Server webes adminisztrációját, akkor először be kell állítania a Web Administration rendszert (részletek: "Webes adminisztráció első beállítása" oldalszám: 99), majd ezután folytassa a következő lépéssel.
2. Jelentkezzen be a Directory Server webes adminisztrációs rendszerében az alábbi módok valamelyikével:
 - Az iSeries navigátorban válassza ki a szerveret és kattintson a **Hálózat > Szerverek > TCP/IP** elemekre, ezután kattintson a jobb egérgombbal az **IBM Directory szerver elemre**, majd válassza a megjelenő menü **Szerveradminisztráció** menüpontját.
 - Az iSeries Feladatok oldalon (http://saját_szerver:2001) kattintson az **IBM Directory Server** elemre.
3. A Directory Server adminisztrációja:
 - a. Válassza ki az adminisztrálni kívánt Directory Server-t az **LDAP hosztnév** mezőben.
 - b. Írja be az adminisztrátor bejelentkezési DN-jét, amellyel csatlakozni kíván a címtárszerverhez.
 - c. Írja be az adminisztrátor jelszavát.
 - d. Kattintson a **Bejelentkezés** lehetőségre. Megjelenik az IBM Directory Server webes adminisztrációs eszközének oldala. Az IBM Directory Server webes adminisztrációs eszköz oldallal kapcsolatos további információk: "Webes adminisztrációs eszköz" oldalszám: 100.
4. A felügyelt Directory Server-ek listájának felvétele és módosítása, illetve a webes adminisztrációs konzol jellemzőinek módosítása:
 - a. Válassza ki az **LDAP hosztnév** mezőben a **Konzol admin** lehetőséget.
 - b. Írja be a konzoladminisztrátor bejelentkezési nevét.
 - c. Írja be a konzoladminisztrátor jelszavát.
 - d. Kattintson a **Bejelentkezés** lehetőségre. Megjelenik az IBM Directory Server webes adminisztrációs eszközének oldala. Az IBM Directory Server webes adminisztrációs eszköz oldallal kapcsolatos további információk: "Webes adminisztrációs eszköz" oldalszám: 100.
 - e. Kattintson a **Konzoladminisztráció** lehetőségre, majd válassza az alábbiak valamelyikét:
 - A **Konzoladminisztrátor bejelentkezési nevének módosítása** elemmel módosíthatja a konzoladminisztrátor bejelentkezési nevét.
 - A **Konzoladminisztrátor jelszavának módosítása** lehetőséggel módosíthatja a konzoladminisztrátor jelszavát.

- A **Konzolszerverek kezelése** lehetőséggel változtathatja meg, mely Directory Server-ek adminisztrálhatók a webes adminisztrációs konzollal.
- A **Konzoltulajdonságok kezelése** lehetőséggel állíthatja be a webes adminisztrációs konzol tulajdonságait.

Webes adminisztráció első beállítása

A Directory Server webes adminisztrációját első alkalommal így állíthatja be:

1. Ha még nincsenek telepítve, akkor telepítse az IBM WebSphere Application Server - Express 5.1 (5722E51 alaptermék és 2. opció) terméket és a hozzá tartozó előfeltétel-szoftvereket.
2. Kapcsolja be a rendszer alkalmazásszerver példányt a HTTP ADMIN szerverben. További információkat az IBM HTTP Server témakörben talál.

a. A HTTP ADMIN szerver az alábbi módokon indítható:

- Az iSeries navigátorban kattintson a **Hálózat -> Szerverek -> TCP/IP** menüpontokra, majd kattintson a jobb egérgombbal a **HTTP adminisztráció** elemre. Ezután kattintson a **Start** lehetőségre.
- Egy parancssorba írja be az STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN) parancsot.

b. Jelentkezzen be az IBM Web Administration for iSeries rendszerbe. A felhasználói profillal és jelszóval jelentkezzen be az iSeries Feladatok lapon ([http:// saját_szerver:2001](http://saját_szerver:2001)), majd kattintson az **IBM Web Administration for iSeries** elemre.

c. A HTTP szerver adminisztráció *saját_szerver* lapon kattintson a **Kezel**, majd a **HTTP szerverek** fülre. Győződjön meg róla, hogy az **ADMIN – Apache** ki van választva a **Szerver** legördülő listában, és hogy a **/QIBM/UserData/HTTPPA/admin/conf/admin-cust.conf** tartalmazott ki van választva a **Szerverterület** legördülő listában.

d. A lap bal keretén lévő opciók közül kattintson az **Általános szerver konfigurációra**.

Megjegyzés: Lehet, hogy ki kell bontani a **Szerver tulajdonságok** szakaszt, hogy láthassa az **Általános szerver konfiguráció** opciót.

e. Állítsa be a **Rendszer alkalmazás szerverpéldány indítása az 'Admin' szerver indulásakor** opciót **Igen** értékre.

f. Kattintson az **OK** gombra.

g. Indítsa újra a HTTP ADMIN szerverpéldányt az Újraindít gombra történő kattintással (a második gomb a **HTTP szerverek** fül alatt). Az iSeries navigátorból vagy a parancssorból is leállíthatja és elindíthatja a HTTP ADMIN szerverpéldányt.

Az alábbi módszerek valamelyikével ugyancsak leállíthatja a HTTP ADMIN szerverpéldányt.

- Az iSeries navigátorban kattintson a **Hálózat -> Szerverek -> TCP/IP** menüpontokra, majd kattintson a jobb egérgombbal a **HTTP adminisztráció** elemre. Ezután kattintson a **Stop** lehetőségre.
- Egy parancssorba írja be az ENDTCPSPV SERVER(*HTTP) HTTPSVR(*ADMIN) parancsot.

Az alábbi módszerek valamelyikével ugyancsak elindíthatja a HTTP ADMIN szerverpéldányt.

- Az iSeries navigátorban kattintson a **Hálózat -> Szerverek -> TCP/IP** menüpontokra, majd kattintson a jobb egérgombbal a **HTTP adminisztráció** elemre. Ezután kattintson a **Start** lehetőségre.
- Egy parancssorba írja be az STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN) parancsot.

További információkat az IBM HTTP Server témakörben talál.

3. Jelentkezzen be a Directory Server webes adminisztrációs eszközre.

a. A **Bejelentkezési lap** az alábbi módszerek valamelyikével jöhet elő.

- Az iSeries navigátorban válassza ki a szervert és kattintson a **Hálózat -> Szerverek -> TCP/IP** elemekre, ezután kattintson a jobb egérgombbal az **IBM címtár elemre**, majd válassza a **Szerveradminisztráció** menüpontot.
- Az iSeries Feladatok oldalon ([http:// saját_szerver:2001](http://saját_szerver:2001)) kattintson az **IBM Directory Server for iSeries** elemre.

b. Válassza ki az **LDAP hosztnév** mezőben a **Konzol admin** lehetőséget.

c. A **Felhasználónév** mezőbe írja be, hogy **superadmin**.

- d. A **Jelszó** mezőbe írja be, hogy **secret**.
 - e. Kattintson a **Bejelentkezés** lehetőségre. Megjelenik az IBM Directory Server webes adminisztrációs eszközének oldala.
4. Változtassa meg a konzoladminisztrátor bejelentkezési nevét.
 - a. Kattintson a **Konzol adminisztrációra** a baloldali kereten az adott rész kibontásához, majd kattintson a **Konzoladminisztrátori bejelentkezés módosítása** elemre.
 - b. A **Konzoladminisztrátor bejelentkezési név** mezőbe írja be a konzoladminisztrátor új bejelentkezési nevét.
 - c. Írja be a jelenlegi jelszót (**secret**) a **Jelenlegi jelszó** mezőbe.
 - d. Kattintson az **OK** gombra.
 5. Változtassa meg a konzoladminisztrátor jelszavát. Kattintson a **Konzoladminisztrátori jelszó módosítása** lehetőségre.
 6. Adja meg az adminisztrálni kívánt Directory Server-t. Kattintson a **Konzolszerverek kezelése** lehetőségre a baloldali kereten.

Megjegyzés: Egy Directory Server felvételekor az **Adminisztrációs port** lehetőséget nem használja a rendszer és figyelmen kívül is hagyja az értékét.

7. Ha meg kívánja változtatni a konzol tulajdonságait. Kattintson a **Konzoltulajdonságok kezelése** lehetőségre a baloldali kereten.
8. Kattintson a **Kijelentkezés** lehetőségre. A Sikeres kijelentkezés képernyő megjelenése után kattintson **ide**, ha vissza akar térni a webes adminisztráció bejelentkezési oldalára.

A konzol első beállítása után bármikor visszatérhet a konzolhoz, hogy:

- Megváltoztassa a konzoladminisztrátor bejelentkezési nevét és jelszavát.
- Megváltoztassa, mely Directory Server-ek adminisztrálhatók a webes adminisztrációs konzollal.
- Módosítsa a konzol tulajdonságait.

Webes adminisztrációs eszköz

Bejelentkezve a webes adminisztrációs eszközre, egy öt részből álló alkalmazásablakkal találkozunk:

Csikterület

A csikterület az ablak felső részén található. Az alkalmazás nevét, illetve az IBM logót tartalmazza.

Navigációs terület

Az ablak bal szélén található navigációs területen a szervertartalommal kapcsolatos különböző feladatok kibontható csoportjai találhatók, mint például:

Felhasználói tulajdonságok

Ezzel a feladattal módosítható a jelenlegi felhasználó jelszava.

Sémakezelés

Ezzel a feladattal kezelhetők az objektumosztályok, attribútumok, megfeleltetési szabályok és szintaxisok.

Címtárkezelés

Ezzel a feladattal kezelhetők a címtárbejegyzések.

Replikációkezelés

Ezzel a feladattal kezelhetők a hitelesítési adatok, a topológia, az ütemezések és a sorok.

Tartományok és sablonok

Ezzel a feladattal kezelhetők a felhasználói sablonok és tartományok.

Felhasználók és csoportok

Ezzel a feladattal kezelhetők a megadott tartományok felhasználói és csoportjai. Ha például létre kíván hozni egy új webes felhasználót, akkor a **Felhasználók és csoportok** feladattal egyetlen groupOfNames objektumosztály kezelhető. A csoport támogatás nem szabható testre.

Szerveradminisztráció

Ezzel a feladattal módosítható a szerverbeállítás és a biztonsági beállítások.

Munkaterület

A munkaterületen jelennek meg a navigációs területen kiválasztott feladatkörrel kapcsolatos feladatok. Ha például a navigációs területen a Szerverbiztonság kezelése feladatkört választja ki, akkor a munkaterületen megjelenik a Szerverbiztonság oldal, a szerver biztonságával kapcsolatos feladatok lapjaira bontva.

Szerverállapot terület

A szerverállapot terület a munkaterület legtetején található. A szerverállapot terület bal szélén látható ikon a szerver pillanatnyi állapotát jelzi. Az ikon mellett a felügyelt szerver neve látható. A szerverállapot terület jobb szélén látható ikon az online súgóra nyújt hivatkozást.

Feladatállapot terület

A munkaterület alatt található feladatállapot terület az aktuális feladat állapotát jelzi.

6. fejezet Példahelyzet: Directory Server beállítása

Helyzet

Mint a cég számítógéprendszereiért felelős rendszergazda, az alkalmazottak információit, például a szervezeti telefonszámokat és e-mail címeket egy központi LDAP lerakatba kívánja gyűjteni.

Célok

Ebben a példahelyzetben a MyCo Rt. üzembe kíván helyezni egy Directory Server-t és létre akar hozni egy cím tár-adatbázist az alkalmazottak adataival (név, e-mail cím, telefonszám és hasonló).

A példahelyzet céljai a következők:

- Az alkalmazottak információinak elérhetővé tétele a céges hálózat teljes egészén egy Lotus Notes vagy Microsoft Outlook Express levelező klienssel.
- A vezetők módosíthassák az alkalmazottak adatait a cím tár-adatbázisban, ugyanakkor a nem vezetők ezt ne tehesék meg.
- Az iSeries szerver legyen képes az alkalmazottak adatait közzétenni a cím tár-adatbázisban.

Részletek

A Directory Server a myiSeries nevű iSeries szerveren fog futni.

Az alábbi példa bemutatja, hogy a MyCo Rt. milyen adatokat kíván tárolni az egyes alkalmazottakról a cím tár-adatbázisban.

Név: Jose Alvirez
Osztály: DEPTA
Telefonszám: 999 999 9999
Email-cím: jalvirez@my_co.com

A példahelyzethez alkalmazható cím tár szerkezete valahogy így néz ki:

```
/
|
+- my_co.com
  |
  +- employees
    |
    +- Jose Alvirez
      |
      DEPTA
      999-555-1234
      jalvirez@my_co.com
    +- John Smith
      |
      DEPTA
      999-555-1235
      jsmith@my_co.com
    + Vezetők csoport
      Jose Alvirez
      myiSeries.my_co.com
  .
  .
  .
```

Minden alkalmazott (vezetők és nem vezetők egyaránt) az employees cím tár fában található. A vezetők a managers csoport tagjai. A managers csoport tagjai jogosultak az alkalmazottak adatainak módosítására.

Az iSeries szerver (myiSeries) szintén jogosultsággal kell, hogy rendelkezzen az alkalmazottak adatainak módosításához. A példahelyzetben az iSeries szerver is bekerül az employees címtárfába és a managers csoport tagja.

Ha az alkalmazottak bejegyzéseit külön akarja választani az iSeries szerver bejegyzésétől, akkor létrehozhat egy másik címtárfát (például "computers" néven) és felveheti abba az iSeries szervert. Az iSeries szervernek mindazonáltal ugyanazokat a jogokat kell adni, mint a vezetőknek.

Előfeltételek és feltételezések

A webes adminisztrációs eszköz megfelelően be van állítva és fut. További információk: "Webes adminisztráció" oldalszám: 98.

Beállítási lépések

Hajtsa végre az alábbiakat:

1. "Példahelyzet részletek: A Directory Server telepítése".
2. "Példahelyzet részletek: A címtár-adatbázis létrehozása" oldalszám: 105.
3. "Példahelyzet részletek: Az iSeries adatok közzététele a címtár-adatbázisban" oldalszám: 107.
4. "Példahelyzet részletek: Információk beírása a címtár-adatbázisba" oldalszám: 108.
5. "Példahelyzet részletek: A címtár-adatbázis tesztelése" oldalszám: 109.

Példahelyzet részletek: A Directory Server telepítése

1. lépés: A Directory Server beállítása

Megjegyzés: A szerver konfigurálásához *ALLOBJ és *IOSYSCFG különleges jogosultságokkal kell rendelkeznie.

1. Az iSeries navigátorban kattintson a **Hálózat** → **Szerverek** → **TCP/IP** elemekre.
2. Kattintson az iSeries navigátor jobb alsó részében, a **Szerverkonfigurációs feladatok** ablak **jo Rendszer címtárszerverként konfigurálása** lehetőségére.
3. Megjelenik a **Directory Server beállítási varázsló**.
4. Kattintson az **IBM Directory Server beállítási varázsló - üdvözlő** ablak **Helyi LDAP címtárszerver beállítása** lehetőségére.
5. Kattintson az **IBM Directory Server beállítási varázsló - üdvözlő** ablak **Tovább** lehetőségére.
6. Az **IBM Directory Server beállítási varázsló - Beállítások megadása** ablakban válassza ki a **Nem** lehetőséget. Így konfigurálhatja az LDAP szerveret az alapértelmezett beállítások nélkül.
7. Kattintson az **IBM Directory Server beállítási varázsló - Beállítások megadása** ablak **Tovább** lehetőségére.
8. Szüntesse meg az **IBM Directory Server beállítási varázsló - Adminisztrátor DN megadása** ablak **Rendszer által előállított** lehetőségének kijelölését.

Adminisztrátori DN	cn=administrator
Jelszó	secret
Jelszó megerősítése	secret

Megjegyzés: A jelen példahelyzet összes jelszava kizárólag példa. A rendszer és a hálózat biztonsága érdekében soha ne használja ténylegesen ezeket a jelszavakat a saját konfigurációjában.

9. Kattintson az **IBM Directory Server beállítási varázsló - Adminisztrátor DN megadása** ablak **Tovább** lehetőségére.
10. Az **IBM Directory Server beállítási varázsló - Utótagok megadása** ablakának **Utótag** mezéjébe írja be, hogy dc=my_co,dc=com.
11. Kattintson az **IBM Directory Server beállítási varázsló - Utótagok megadása** ablak **Hozzáadás** lehetőségére.
12. Kattintson az **IBM Directory Server beállítási varázsló - Utótagok megadása** ablak **Tovább** lehetőségére.

13. Válassza ki az **IBM Directory Server beállítási varázsló - IP címek kiválasztása** ablak **Igen**, az **összes IP cím használata** lehetőséget.
14. Kattintson az **IBM Directory Server beállítási varázsló - IP címek kiválasztása** ablak **Tovább** lehetőségére.
15. Válassza ki az **IBM Directory Server beállítási varázsló - TCP/IP preferencia megadása** ablakban az **Igen** értéket.
16. Kattintson az **IBM Directory Server beállítási varázsló - TCP/IP preferencia megadása** ablak **Tovább** lehetőségére.
17. Kattintson az **IBM Directory Server beállítási varázsló - Összegzés** ablak **Befejezés** lehetőségére.
18. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** elemre és nyomja meg az **Indítás** gombot.

2. lépés: A Directory Server webes adminisztrációs eszközének beállítása

1. Irányítsa a böngészőt a http://myiSeries.my_co.com:9080/IDSWebApp/IDSjsp/Login.jsp oldalra, ahol a *myiSeries.my_co.com* az iSeries szerverre utal.
2. Egy bejelentkező oldalnak kell megjelennie. Kattintson az **LDAP hosztnév** listára és válassza ki a **Konzol admin** lehetőséget. Felhasználónévként írja be, hogy **superadmin**, jelszónak pedig, hogy **secret**. Kattintson a **Bejelentkezés** menüpontra.
3. Állítsa be a webes adminisztrációs eszközt, hogy csatlakozzon az iSeries rendszeren futó LDAP szerverre. Válassza ki a **Konzoladminisztráció** → **Konzolszerverek kezelése** elemeket a baloldali navigációs területen.
4. Kattintson a **Hozzáadás** gombra.
5. A **Szerver hozzáadása** mezőbe írja be, hogy *myiSeries.my_co.com*.
6. Kattintson az **OK** gombra. Az új szerver megjelenik a **Konzolszerverek kezelése** listában.
7. Kattintson a baloldali navigációs terület **Kijelentkezés** elemére.
8. A webes adminisztrációs eszköz bejelentkezési oldalán kattintson az **LDAP hosztnév** listára, majd válassza ki az imént beállított szervert (**myiSeries.my_co.com**).
9. A **Felhasználónév** mezőbe írja be, hogy **cn=admin**, a **Jelszó** mezőbe pedig, hogy **secret**. Kattintson a **Bejelentkezés** lehetőségre. Meg kell, hogy jelenjen az IBM Directory Server webes adminisztrációs eszközének főoldala.

Példahelyzet részletek: A címtár-adatbázis létrehozása

Az adatok bevitelének megkezdése előtt létre kell hoznia egy helyet az adatok tárolásához.

1. lépés: Alap DN objektum létrehozása

1. A webes adminisztrációs eszközben kattintson a **Címtárkezelés** → **Bejegyzések kezelése** menüpontokra. A címtár alap szintjén megjelenik objektumok egy listája. Mivel a szerver még új, csak a konfigurációs információkat tartalmazó strukturális objektumok láthatók.
2. Létre kívánunk hozni egy új objektumot a MyCo Rt. adatainak tárolásához. Először kattintson az ablak jobb oldalán a **Hozzáadás...** lehetőségére. A következő ablak **Objektumosztály** listájában keresse ki a **tartomány** osztályt, majd kattintson a **Tovább** gombra.
3. Nem akarunk felvenni kiegészítő objektumosztályokat, így kattintson újra a **Tovább** gombra.
4. Az **Attribútumok beírása** ablakban írja be a varázsló korábbi lépésében létrehozott utótagnak megfelelő adatokat. Hagyja az **Objektumosztály** legördülő listát a **tartomány** elemen. A **Relatív DN** mezőbe írja be, hogy **dc=my_co**. A **Szülő DN** mezőbe írja be, hogy **dc=com**. A **dc** mezőbe pedig írja be, hogy **my_co**.
5. Kattintson az ablak alján látható **Befejezés** lehetőségre. Visszakerül az alapszintre, ahol most már látszania kell az új alap DN-nek.

2. lépés: Felhasználói sablon létrehozása

A felhasználói sablon segít a MyCo Rt. alkalmazottak adatainak beírásában.

1. A webes adminisztrációs eszközben kattintson a **Tartományok és sablonok** → **Felhasználói sablon hozzáadása** lehetőségekre.

2. A **Felhasználói sablon neve** mezőbe írja be, hogy **Alkalmazott**.
3. Kattintson a **Szülő DN** mező melletti **Tallózás...** gombra. Kattintson a korábbi részben létrehozott alap DN-re (**dc=my_co,dc=com**), majd kattintson az ablak jobb oldalán látható **Kiválasztás** lehetőségre.
4. Kattintson a **Tovább** gombra.
5. A **Strukturális objektumosztály** legördülő
6. listából válassza ki az **inetOrgPerson** elemet, majd kattintson a **Tovább** gombra.
7. Az **Elnevezési tulajdonság** legördülő listából válassza ki a **cn** elemet.
8. A **Lapok** listából válassza ki a **Kötelező** elemet és kattintson a **Módosítás** lehetőségre.
9. A **Lap módosítása** ablakban adhatja meg, hogy a felhasználói sablon milyen mezőket tartalmazzon. Az **sn** és **cn** mezők kötelezők.
10. Az **Attribútumok** listából válassza ki a **departmentNumber** elemet, majd kattintson a **Hozzáadás >>>** elemre.
11. Válassza ki a **telephoneNumber** elemet, majd kattintson a **Hozzáadás >>>** elemre.
12. Válassza ki a **mail** elemet, majd kattintson a **Hozzáadás >>>** elemre.
13. Válassza ki a **userPassword** elemet, majd kattintson a **Hozzáadás >>>** elemre.
14. Kattintson az **OK**, majd a **Befejezés** lehetőségre a felhasználói sablon létrehozásához.

3. lépés: Tartomány létrehozása

1. A webes adminisztrációs eszközben kattintson a **Tartományok és sablonok** —> **Tartomány hozzáadása** lehetőségekre.
2. A **Tartomány neve** mezőbe írja be, hogy **employees**.
3. Kattintson a **Szülő DN** mező melletti **Tallózás...** gombra.
4. Válassza ki a létrehozott szülő DN-t (**dc=my_co,dc=com**), majd kattintson az ablak jobb szélén látható **Kiválasztás** lehetőségre.
5. Kattintson a **Tovább** gombra.
6. A következő ablakban csak a **Felhasználói sablon** legördülő listát kell módosítania. Válassza ki a létrehozott felhasználói sablont (**cn=employees,dc=my_co,dc=com**).
7. Kattintson a **Befejezés** gombra.

4. lépés: Vezetői csoport kialakítása

1. Hozza létre a vezetői csoportot.
 - a. A webes adminisztrációs eszközben kattintson a **Felhasználók és csoportok** —> **Csoportok hozzáadása** lehetőségekre.
 - b. A **Csoport neve** mezőbe írja be, hogy **managers**.
 - c. Ügyeljen rá, hogy a **Tartomány** legördülő listából az **employees** érték legyen kiválasztva.
 - d. Kattintson a **Befejezés** gombra.
2. Állítsa be a vezetői csoport adminisztrátorát az **employees** tartományra vonatkozóan.
 - a. Kattintson a **Tartományok és sablonok** —> **Tartományok kezelése** lehetőségekre.
 - b. Válassza ki a létrehozott tartományt (**cn=employees,dc=my_co,dc=com**), majd kattintson a **Módosítás** lehetőségre.
 - c. Az **Adminisztrátor csoport** mező jobb oldalán kattintson a **Tallózás...** lehetőségre.
 - d. Válassza ki a **dc=my_co,dc=com** értéket, majd kattintson a **Kibontás** lehetőségre.
 - e. Válassza ki a **cn=employees** elemet, majd kattintson a **Kibontás** lehetőségre.
 - f. Válassza ki a **cn=managers** elemet, majd kattintson a **Kiválasztás** lehetőségre.
 - g. A **Tartomány módosítása** ablakban kattintson az **OK** gombra.
3. Adjon a managers nevű csoportnak jogosultságot a **dc=my_co,dc=com** utótaghoz.
 - a. Kattintson a **Címtárkezelés** —> **Bejegyzések kezelése** menüpontra.
 - b. Válassza ki a **dc=my_co,dc=com** értéket, majd kattintson az **ACL módosítása...** lehetőségre.

- c. Az **ACL módosítása** ablakban kattintson az **Tulajdonosok** lehetőségre.
- d. Jelölje meg a **Tulajdonos továbbadása** négyzetet. A managers csoport minden tagja a **dc=my_co,dc=com** adatfa tulajdonosa is lesz.
- e. A **Típus** legördülő listából válassza ki a **Csoport** lehetőséget.
- f. A **DN (megkülönböztetett név)** mezőbe írja be, hogy **cn=managers,cn=employees,dc=my_co,dc=com**.
- g. Kattintson a **Hozzáadás** gombra.
- h. Kattintson az **OK** gombra.

5. lépés: Egy vezető felhasználó felvétele

1. A webes adminisztrációs eszközben kattintson a **Felhasználók és csoportok** → **Felhasználó hozzáadása** lehetőségekre.
2. A **Tartomány** legördülő menüből válassza ki a létrehozott tartományt (**employees**), majd kattintson a **Tovább** gombra.
3. A **cn** mezőbe írja be, hogy **Jose Alvarez**.
4. A ***sn** (vezetéknév) mezőbe írja be, hogy **Alvarez**.
5. A ***cn** (teljes név) mezőbe írja be, hogy **Jose Alvarez**. A **cn** szükséges a bejegyzés DN-jének létrehozásához. A ***cn** az objektum egyik attribútuma.
6. A **telephoneNumber** mezőbe írja be, hogy **999 555 1234**.
7. A **departmentNumber** mezőbe írja be, hogy **DEPTA**.
8. A **mail** mezőbe írja be, hogy **jalvarez@my_co.com**.
9. A **userPassword** mezőbe írja be, hogy **secret**.
10. Kattintson a **Felhasználói csoportok** lapra.
11. A **Rendelkezésre álló csoportok** listából válassza ki a **managers** nevűt, majd kattintson a **Hozzáadás** → lehetőségre.
12. Az ablak alján kattintson a **Befejezés** gombra.
13. Jelentkezzen ki a webes adminisztrációs eszközből a baloldali navigációs terület **Kijelentkezés** elemére kattintva.

Példahelyzet részletek: Az iSeries adatok közzététele a címtár-adatbázisban

A közzététel beállításával az iSeries szerver automatikusan beírja a felhasználói adatokat az LDAP címtárba. A rendszer terjesztési címtárának felhasználói információi közzétételre kerülnek az LDAP címtárban.

Megjegyzés: Az iSeries navigátorban létrehozott felhasználók kapnak egy felhasználói profilt, valamint a rendszer terjesztési címtárában egy bejegyzést. Ha CL parancsokkal hoz létre felhasználókat, akkor külön kell létrehoznia a felhasználói profilt (**CRTUSRPRF**) és a rendszer terjesztési címtárában a bejegyzést (**WRKDIRE**). Ha a felhasználókhoz csak felhasználói profilok léteznek, és mégis közzé akarja tenni őket az LDAP címtárban, akkor előbb bejegyzéseket kell készítenie hozzájuk a rendszer terjesztési címtárában.

1. lépés: Az iSeries szerver felvétele Directory Server felhasználóként

1. Jelentkezzen be a webes adminisztrációs eszközbe (http://myiSeries.my_co.com:9080/IDSWebApp/IDSjsp/Login.jsp) adminisztrátorként.
 - a. Válassza ki az **LDAP hosztnév** lista **myiSeries.my_co.com** elemét.
 - b. A **Felhasználónév** mezőbe írja be, hogy **cn=administrator**.
 - c. A **Jelszó** mezőbe írja be, hogy **secret**.
 - d. Kattintson a **Bejelentkezés** lehetőségre.
2. Válassza ki a **Felhasználók és csoportok** → **csoport hozzáadása** lehetőségeket.
3. Válassza ki a **Tartomány** lista **employees** elemét.

4. Kattintson a **Tovább** gombra.
5. A **cn** mezőbe írja be, hogy myiSeries.my_co.com.
6. A ***sn** mezőbe írja be, hogy myiSeries.my_co.com.
7. A ***cn** mezőbe írja be, hogy myiSeries.my_co.com.
8. A **userPassword** mezőbe írja be, hogy secret.
9. Kattintson a **Felhasználói csoportok** lapra.
10. Válassza ki a **managers** csoportot.
11. Kattintson a **Hozzáadás** —> lehetőségre.
12. Kattintson a **Befejezés** gombra.

2. lépés Az iSeries szerver beállítása adatok közzétételére

1. Az iSeries navigátorban kattintson a jobb egérgombbal a baloldali navigációs területen az iSeries szerverre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
2. A **Tulajdonságok** párbeszédablakban válassza ki a **Directory Server** lapot.
3. Válassza ki a **Felhasználók** lehetőséget, majd kattintson a **Részletek** elemre.
4. Jelölje meg a **Felhasználói információk közzététele** négyzetet.
5. A **Közzététel helye** szakaszban kattintson a **Módosítás** gombra. Megjelenik egy ablak.
6. Írja be, hogy myiSeries.my_co.com.
7. A **Mely DN alatt** mezőbe írja be, hogy cn=employees,dc=my_co,dc=com.
8. A **Szerverkapcsolat** szakaszban győződjön meg róla, hogy a **Port** mezőben az alapértelmezett portszám, a **389** látható. A **Hitelesítési módszer** legördülő listából válassza ki a **Megkülönböztetett név** elemet, majd a **Megkülönböztetett név** mezőbe írja be, hogy cn=myiSeries,cn=employees,dc=my_co,dc=com.
9. Kattintson a **Jelszó** mezőre.
10. A **Jelszó** mezőbe írja be, hogy secret.
11. A **Jelszó megerősítése** mezőbe is írja be, hogy secret.
12. Kattintson az **OK** gombra.
13. Kattintson az **Ellenőrzés** gombra. A rendszer megvizsgálja, hogy a beírt adatok helyesek-e és hogy az iSeries rendszer tud-e csatlakozni az LDAP címtárhoz.
14. Kattintson az **OK** gombra.
15. Kattintson az **OK** gombra.

Példahelyzet részletek: Információk beírása a címtár-adatbázisba

Vezetőként Jose Alvarez most beírja és frissíti a saját osztályán dolgozók adatait. Jane Doe-ról további információkra is szüksége van. Jane Doe az iSeries szerver egyik felhasználója, és információi közzétételre kerültek. Jose Alvarez John Smithről is be akar írni adatokat. John Smith is not a user on the iSeries server. Jose Alvarez a következőket teszi:

1. lépés: Bejelentkezik a webes adminisztrációs eszközre

Jelentkezzen be a webes adminisztrációs eszközre. (http://myiSeries.my_co.com:9080/IDSWebApp/IDSjsp/Login.) az alábbi módon:

1. Válassza ki az **LDAP hosztnév** lista **myiSeries.my_co.com** elemét.
2. A **Felhasználónév** mezőbe írja be, hogy cn=Jose Alvarez,cn=myco employees,dc=my_co,dc=com.
3. A **Jelszó** mezőbe írja be, hogy secret.
4. Kattintson a **Bejelentkezés** menüpontra.

2. lépés: Az alkalmazott adatainak módosítása

1. Kattintson a **Felhasználók és csoportok** —> **Felhasználók kezelése** lehetőségekre.
2. Válassza ki a **Tartomány** lista **employees** elemét, majd kattintson a **Felhasználók megjelenítése** lehetőségre.

3. Válassza ki **Jane Doe**-t a felhasználók listájából, majd kattintson a **Módosítás** lehetőségre.
4. A **departmentNumber** mezőbe írja be, hogy DEPTA.
5. Kattintson az **OK** gombra.
6. Kattintson a **Bezárás** gombra.

3. lépés: Alkalmazottak adatainak felvitele

1. Kattintson a **Felhasználók és csoportok** —> **csoport hozzáadása** lehetőségekre.
2. Válassza ki a **Tartomány** legördülő menü **employees** elemét, majd kattintson a **Tovább** gombra.
3. A **cn** mezőbe írja be, hogy John Smith.
4. A ***sn** mezőbe írja be, hogy Smith.
5. A ***cn** mezőbe írja be, hogy John Smith.
6. A **telephoneNumber** mezőbe írja be, hogy 999 555 1235.
7. A **departmentNumber** mezőbe írja be, hogy DEPTA.
8. A **mail** mezőbe írja be, hogy jsmith@my_co.com.
9. Kattintson az ablak alján látható **Befejezés** lehetőségre.

Példahelyzet részletek: A címtár-adatbázis tesztelése

Miután beírta az adatokat a címtár-adatbázisba, ellenőrizze le a címtár-adatbázist és a Directory Server-t az alábbi módok egyikével:

Keresés a címtár-adatbázisban az e-mail címjegyzékkel

Az LDAP címtárban egyszerű a keresés az LDAP használatára felkészített programokkal. Számos e-mail kliensprogram képes keresni LDAP címtárszervereken saját címjegyzék funkciójuk részeként. Az alábbiakban bemutatjuk, hogyan kell beállítani a Lotus Notes 6 és a Microsoft Outlook Express 6 levelezőprogramokat. Más e-mail kliensek esetén is hasonló az eljárás.

Lotus Notes

1. Nyissa meg a címjegyzéket.
2. Kattintson a **Tevékenységek** —> **Új** —> **Fiók** menüpontra.
3. A **Fióknév** mezőbe írja be, hogy myiSeries.
4. A **Fiókszerver neve** mezőbe írja be, hogy myiSeries.my_co.com.
5. Válassza ki a **Protokoll** mező **LDAP** elemét.
6. Kattintson a **Protokoll beállítások** lapra.
7. A **Keresés alapja** mező értéke dc=my_co,dc=com legyen.
8. Kattintson a **Mentés és bezárás** menüpontra.
9. Kattintson a **Létrehozás** —> **Levél** —> **Memo** menüpontra.
10. Kattintson a **Cím...** gombra.
11. Válassza ki a **Címjegyzék kiválasztása** mező myiSeries elemét.
12. A **Keresett érték** mezőbe írja be, hogy Alvirez.
13. Kattintson a **Keresés** gombra. Megjelennek Jose Alvirez adatai.

Microsoft Outlook Express

1. Kattintson az **Eszközök** —> **Fiókok** menüpontra.
2. Kattintson a **Hozzáadás** —> **Címtárszolgáltatás** gombokra.
3. Az **Internetes címtár (LDAP) szerver** mezőbe írja be az iSeries webes címét (myiSeries.my_co.com).
4. Szüntesse meg **Az LDAP szerver megköveteli a bejelentkezést** jelölőnégyzet kijelölését.

5. Kattintson a **Tovább** gombra.
6. Kattintson a **Tovább** gombra.
7. Kattintson a **Befejezés** gombra.
8. Válassza ki a **mySeries.my_co.com** elemet (az imént beállított címtárszolgáltatást), majd kattintson a **Tulajdonságok** gombra.
9. Kattintson a **Speciális** gombra.
10. A **Keresés alapja** mező értéke **dc=my_co,dc=com** legyen.
11. Kattintson az **OK** gombra.
12. Kattintson a **Bezárás** gombra.
13. A **Ctrl+E** billentyűk lenyomásával hívja meg a **Személy keresése** ablakot.
14. Válassza ki a **Keresett adatok** lista **mySeries.my_co.com** elemét.
15. A **Név** mezőbe írja be, hogy **Alvirez**.
16. Kattintson a **Keresés** gombra. Megjelennek Jose Alvirez adatai.

Keresés a címtár-adatbázisban az **ldapsearch** parancssori paranccsal

1. A karakteres felületen írja be a **QSH CL** parancsot egy Qshell szekció megnyitásához.
2. Az alábbi paranccsal lekérheti az adatbázis összes LDAP bejegyzését.

```
ldapsearch -h mySeries.my_co.com -b dc=my_co,dc=com objectclass=*
```

ahol:

-h az LDAP szerver futtató hosztgép neve.

-b az alap DN, amely alatt a keresés történik.

objectclass=*

a címtár összes bejegyzését visszaadja.

A parancs eredménye az alábbihoz hasonló lesz:

```
dc=my_co,dc=com
dc=my_co
objectclass=domain
objectclass=top
```

```
cn=MyCo employee,dc=my_co,dc=com
```

```
.
.
.
```

```
cn=Jose Alvirez,cn=MyCo Employees,dc=my_co,dc=com
```

```
sn=Alvirez
departmentNumber=DEPTA
mail=jalvirez@my_co.com
telephoneNumber=999 999 9999
objectclass=top
objectclass=inetOrgPerson
objectclass=organizationalPerson
objectclass=person
cn=Jose Alvirez
```

```
.
.
.
```

Az egyes bejegyzések első sora a megkülönböztetett név (DN). A DN-ek a teljes fájlnevhez hasonlóan, egyedi módon azonosítják az egyes bejegyzéseket. Egyes bejegyzések nem tartalmaznak adatokat és kizárólag strukturális szerepük van. Az **objectclass=inetOrgPerson** sort tartalmazó bejegyzések felelnek meg az embereknek. Jose Alvirez DN-je **cn=Jose Alvirez,cn=MyCo Employees,dc=my_co,dc=com**.

7. fejezet Directory Server felügyelete

A Directory Server adminisztrálásához az Ön által használt felhasználói profilnak a következő jogosultságot kell használnia:

- 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 címtárszerver ellenőrzési funkciójának beállításához: Audit (*AUDIT) különleges jogosultság
- A szerver feladatnapló megtekintéséhez: Spool Control (*SPLCTL) különleges jogosultság

A címtárobjektumok 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 (lásd: “Operációs rendszer leképzett háttér objektumai” oldalszám: 75), aki jogosultsággal bír a Directory Server adminisztrátori funkció azonosítójához. A legtöbb adminisztrációs feladatot az adminisztrációs csoportban található felhasználók is elvégezhetik (lásd: “Adminisztratív hozzáférés” oldalszám: 55).

Általános adminisztrációs feladatok

- “Directory Server indítása/leállítása” oldalszám: 112
- “A címtárszerver állapotának ellenőrzése” oldalszám: 113
- “Jobok ellenőrzése a Directory Server-en” oldalszám: 113
- “Szerverkapcsolatok kezelése” oldalszám: 113
- “Kapcsolat tulajdonságainak kezelése” oldalszám: 114
- “Az eseményértesítés engedélyezése” oldalszám: 116
- “Tranzakció-beállítások megadása” oldalszám: 117
- “Port vagy IP cím módosítása” oldalszám: 117
- “LDIF fájl importálása/exportálása” oldalszám: 93
- “Szerver kijelölése címtári utalások részére” oldalszám: 118
- “Directory Server utótagok felvétele és eltávolítása” oldalszám: 118
- “A Directory Server információinak mentése és visszaállítása” oldalszám: 119
- “Adminisztrátori hozzáférés megadása leképezett felhasználóknak” oldalszám: 119
- “Adminisztrációs csoport kezelése” oldalszám: 120
- “Keresésikorlát-csoportok kezelése” oldalszám: 122
- “Proxy hitelesítési csoport kezelése” oldalszám: 123
- “Egyedi attribútumok kezelése” oldalszám: 125
- “Az LDAP címtár eléréseinek és változásainak nyomon követése” oldalszám: 126
- “Objektum naplózás engedélyezése a Directory Server számára” oldalszám: 127
- “Keresési beállítások módosítása” oldalszám: 127
- “Teljesítménnyel kapcsolatos beállítások módosítása” oldalszám: 128
- “Replikáció kezelése” oldalszám: 131

Biztonsági feladatok

- “Jelszavak kezelése” oldalszám: 150
- “SSL és TSL engedélyezése a Directory Serveren” oldalszám: 154

- “Kerberos hitelesítés engedélyezése a Directory Server-hez” oldalszám: 156
- “DIGEST-MD5 hitelesítés beállítása a Directory Serveren” oldalszám: 157

A címtár tartalmával kapcsolatos feladatok

- “Séma kezelése” oldalszám: 157
- “Címtárbejegyzések kezelése” oldalszám: 168
- “Felhasználók és csoportok kezelése” oldalszám: 175
- “Tartományok és felhasználói sablonok kezelése” oldalszám: 178
- “Hozzáférés-felügyeleti listák (ACL-ek) kezelése” oldalszám: 185

Közzétételi feladatok

- “Információk publikálása a címtárszervernek” oldalszám: 92

Directory Server indítása/leállítása

A Directory Server elindításának lépései:

1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Start** menüpontot.

A szerver sebességétől és a rendelkezésre álló memória méretétől függően a címtárszerver elindulásához néhány perc szükséges. Első alkalommal a címtárszerver 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 Directory Server korábbi változatáról történő frissítést követően, az indulás a megszokottnál néhány perccel hosszabb időt vehet igénybe, mivel a szervernek át kell állítania a fájlokat. Időről-időre ellenőrizheti a szerver állapotát (részletek: “A címtárszerver állapotának ellenőrzése” oldalszám: 113), hogy megállapítsa, leállt-e már.

A címtárszerver elindítható a karakteres felületről is a `STRTCPSVR *DIRSRV` parancs segítségével. Amennyiben a címtárszervert úgy állította be, hogy a TCP/IP-vel egyidőben induljon, a `STRTCP` paranccsal is indíthatja azt.

Csak konfigurációs mód

A címtár szolgáltató elindítható a karakteres felületről csak konfigurációs módban is a `TRCTCPAPP APP(*DIRSRV) ARGLIST(SAFEMODE)` parancs segítségével.

Csak konfigurációs módban a szerver úgy indul el, hogy csak a `cn=configuration` utótag aktív és nem függ az adatbázis-háttér sikeres inicializálásától a működése.

A directory server leállításának lépései:

A címtárszerver leállítása hatással van az összes olyan alkalmazásra, amely használja a szervert a leállítás pillanatában. Ide tartoznak a Vállalati azonosság leképezés (EIM) alkalmazások, amelyek éppen igénybe veszik a címtárszervert az EIM műveletekhez. Az összes alkalmazás lekapcsolódik ugyan a címtárszerverről, azonban semmi sem akadályozza őket abban, hogy megpróbáljanak újra kapcsolódni a szerverhez.

A Directory Server leállításának lépései:

1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Leállítás** menüpontot.

A címtárszerver leállítása néhány percig is eltarthat a rendszer sebességétől, a szerver tevékenységétől, és a rendelkezésre álló memória méretétől függően. Időről-időre ellenőrizheti a szerver állapotát (részletek: “A címtárszerver állapotának ellenőrzése” oldalszám: 113), hogy megállapítsa, leállt-e már.

Megjegyzés: A címtárszerver leállítható 5250 szekcióból is, az ENDTCP SVR *DIRSRV, ENDTCP SVR *ALL vagy ENDTCP parancsok segítségével. Az ENDTCP SVR *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 címtárszerver állapotának ellenőrzése

Az alapvető állapotinformációk az iSeries Navigatorban találhatóak. Ennél bővebb információk is találhatóak a webadminisztrációs eszköz használatával.

Az iSeries navigátor a jobb keret **Állapot** oszlopában megjeleníti a címtárszerver állapotát.

A címtárszerver állapotának ellenőrzéséhez az iSeries Navigatorban tegye a következőket:

1. Bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** lehetőségre. Az iSeries navigátor megjeleníti az **Állapot** oszlopban az összes TCP/IP szerver, közöttük a címtárszerver állapotát. A szerverek állapotának frissítéséhez kattintson a **Megjelenítés** menüre, és ott válassza ki a **Frissítés** elemet.
4. Ha további információt szeretne a címtárszerver állapotáról, kattintson a jobb oldali egérgombbal a **IBM Directory Server** felírára, és válassza a **Állapot** lehetőséget. 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 címtárszerver állapotát, hogy a többi TCP/IP szerver állapotfrissítését is ki kellene várnia.

| A címtárszerver állapotának ellenőrzéséhez a webadminisztrációs eszközben tegye a következőket:

1. Bontsa ki a **Szerveradminisztráció** kategóriát a navigációs területen.

| **Megjegyzés:** A szerver konfigurációs beállításainak módosításához a webadminisztrációs eszköz

| Szerveradminisztrációs kategóriájának használatával hitelesítenie kell magát a szerverhez egy i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultságokkal. Ez úgy történhet, hogy hitelesíti magát leképezett felhasználóként az adott profil jelszavával. A kapcsolódáshoz a webes adminisztrációs eszközhöz leképezett felhasználóként adjon meg egy felhasználónevet a következő formában: os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, ahol a MYUSERNAME és MYSYSTEM.COM karaktersorozatokat a saját felhasználói profiljának nevével és a beállított rendszerlekepezési utótaggal helyettesíti.

2. Kattintson a **Szerverállapot megjelenítése** menüpontra.

3. A **Szerverállapot megjelenítése** panelben válassza ki a különféle lapokat az állapotinformációk megjelenítésére.

Jobok ellenőrzése a Directory Server-en

Időről-időre szükség lehet egyes jobok megfigyelésére a Directory Server-en. A szerverjobok a következő lépésekkel ellenőrizhetők az iSeries Navigatorban:

1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** felírára, majd válassza a **Szerver feladatok** menüpontot.

Szerverkapcsolatok kezelése

| Az adminisztrátorok számára gyakran szükséges, hogy lássák a szerverrel fennálló kapcsolatokat és az azokon zajló műveleteket. Az adminisztrátor ezután döntéseket tud hozni a hozzáférés felügyeletével és a szolgáltatásbénítással (DOS) támadások megelőzésével kapcsolatban. Erre a webes adminisztrációs eszköz ad lehetőséget.

| Bontsa ki a **Szerveradminisztráció** kategóriát a navigációs területen. Kattintson a **Szerverkapcsolatok kezelése** lehetőségre. Megjelenik egy táblázat, amely a következő információkat tartalmazza az egyes kapcsolatokról:

| **Megjegyzés:** A szerver konfigurációs beállításainak módosításához a webadminisztrációs eszköz
| Szerveradminisztrációs kategóriájának használatával hitelesítenie kell magát a szerverhez egy i5/OS
| felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultságokkal. Ez úgy
| történhet, hogy hitelesíti magát leképezett felhasználóként az adott profil jelszavával. A kapcsolódáshoz
| a webes adminisztrációs eszközhöz leképezett felhasználóként adjon meg egy felhasználónevet a
| következő formában: os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM,
| ahol a MYUSERNAME és MYSYSTEM.COM karaktersorozatokat a saját felhasználói profiljának
| nevével és a beállított rendszerleképezési utótaggal helyettesíti.

| **DN** Megadja a szerverre csatlakozó kliens megkülönböztetett nevét.

| **IP címek**

| Megadja a szerverre csatlakozó kliens IP-címét.

| **Kezdési idő**

| Megadja azt az időpontot és dátumot (a szerver helyi ideje szerint), amikor a kapcsolat létrejött.

| **Állapot**

| Megadja, hogy a kapcsolat aktív vagy tétlen. A kapcsolat akkor számít aktívnek, ha valamilyen művelet
| folyamatban van.

| **Kezdeményezett műveletek**

| Megadja a kapcsolat létrehozása óta kért műveletek számát.

| **Befejezett műveletek**

| Megadja az egyes kapcsolatokon belül befejezett műveletek számát.

| **Típus** Megadja, hogy a kapcsolat SSL vagy TLS használatával került-e biztosításra. Egyéb esetekben a mező üres.

| **Megjegyzés:** A táblázatban egyidőben akár 20 kapcsolat is látható.

| A panel tetején lévő legördülő menü kibontásával és egy kiválasztással megadható, hogy a táblázatot DN vagy IP-cím
| szerint szeretné-e megjeleníteni. Az alapértelmezett kiválasztás a DN. Ugyanígy az is megadható, hogy a táblázat
| elemei csökkenő vagy növekvő sorrendben legyenek-e rendezve.

| Az aktuális kapcsolati információk frissítéséhez kattintson a **Frissítés** gombra.

| Ha adminisztrátorként vagy az adminisztrációs csoport tagjaként van bejelentkezve, akkor további választási
| lehetőségei is vannak a panelben rendelkezésre álló szerverkapcsolatok megszüntetésére. Ez a lehetőség módot ad arra,
| hogy megszüntesse a szolgáltatásmegbénítós (DOS) támadásokat és közben tarthassa a szerver elérését. Egy
| kapcsolat megszüntetéséhez bontsa ki a legördülő menüket és válasszon ki egy DN-t, egy IP-címet vagy mindkettőt, és
| kattintson a **Megszakítás** lehetőségre.

| Ha minden szerverkapcsolatot meg szeretne szakítani azon kívül, amin a kérés történik, kattintson az **Összes**
| **megszakítása** lehetőségre. Megjelenik egy megerősítést kérő üzenet. Kattintson az **OK** gombra a szétkapcsolási
| művelet végrehajtásához vagy a **Mégse** gombra a művelet befejezéséhez és a visszatéréshez a **Szerverkapcsolatok**
| **kezelése** panelbe.

| A szolgáltatásbénítós támadások elleni védekezéssel kapcsolatban további információk: “Kapcsolat tulajdonságainak
| kezelése”.

| **Kapcsolat tulajdonságainak kezelése**

| A kapcsolati tulajdonságok felügyeletének lehetősége módot ad annak megakadályozására, hogy a kliensek záróják a
| szervert. Ez biztosítja azt is, hogy az adminisztrátor mindig elérheti a szerveret azokban az esetekben, ha a háttér
| valamilyen hosszan futó feladat miatt túlterhelt. A kapcsolati tulajdonságok felügyelete a webes adminisztrációs
| eszközzel történik.

Megjegyzés: Ezek a kiválasztások csak akkor jelennek meg, ha adminisztrátorként vagy az adminisztrációs csoport tagjaként van bejelentkezve egy olyan szerveren, amely támogatja ezeket a funkciókat.

A kapcsolati tulajdonságok beállításához a következő lépéseket kell elvégeznie.

1. Bontsa ki a navigációs terület **Szerveradminisztráció** kategóriáját, majd kattintson a **Kapcsolati tulajdonságok kezelése** lehetőségre.

Megjegyzés: A szerver konfigurációs beállításainak módosításához a webadminisztrációs eszköz Szerveradminisztrációs kategóriájának használatával hitelesítenie kell magát a szerverhez egy i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultságokkal. Ez úgy történhet, hogy hitelesíti magát leképezett felhasználóként az adott profil jelszavával. A kapcsolódáshoz a webes adminisztrációs eszközhöz leképezett felhasználóként adjon meg egy felhasználónevet a következő formában: **os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM**, ahol a MYUSERNAME és MYSYSTEM.COM karaktersorozatokat a saját felhasználói profiljának nevével és a beállított rendszerleképezési utótaggal helyettesíti.

2. Válassza ki az **Általános** lapot.
3. Adja meg a névtelen kapcsolat beállításait. A **Névtelen kapcsolatok engedélyezése** jelölőnégyzet már ki van választva, vagyis a névtelen kapcsolatok engedélyezettek. Ez az alapértelmezett beállítás. A jelölőnégyzetre kattintva megszüntetheti a **Névtelen kapcsolatok engedélyezése** lehetőség kiválasztását. Ennek az lesz a következménye, hogy a szerver minden névtelen kapcsolatot megszakít.

Megjegyzés: Bizonyos alkalmazások meghiúsulhatnak a névtelen kapcsolatok letiltásakor.

4. A **Névtelen kapcsolatok törlési küszöbértéke** mezőben adjon meg egy küszöbértéket a névtelen kapcsolatok leválasztásának megkezdéséhez. 0 és 65535 közötti szám adható meg.

Megjegyzés: A tényleges maximális számot a folyamatonként engedélyezett fájlok száma korlátozza. UNIX rendszereken a korlátok megadására az **ulimit -a** parancs használható. Windows rendszereken a szám rögzített.

Az alapértelmezett beállítás 0. Amikor a névtelen kapcsolatok számának ez a korlátja meghaladásra kerül, akkor a kapcsolatok az **Üresjáratú időkorlát** mezőben megadott határérték alapján törlésre kerülnek.

5. A **Hitelesített kapcsolatok törlési küszöbértéke** mezőben adjon meg egy küszöbértéket a hitelesített kapcsolatok leválasztásának megkezdéséhez. 0 és 65535 közötti szám adható meg.

Megjegyzés: A tényleges maximális számot a folyamatonként engedélyezett fájlok száma korlátozza. UNIX rendszereken a korlátok megadására az **ulimit -a** parancs használható. Windows rendszereken a szám rögzített.

Az alapértelmezett beállítás 1100. Amikor a hitelesített kapcsolatok számának ez a korlátja meghaladásra kerül, akkor a kapcsolatok az **Üresjáratú időkorlát** mezőben megadott határérték alapján törlésre kerülnek.

6. Az **Összes kapcsolat törlési küszöbértéke** mezőben adjon meg egy küszöbértéket az összes kapcsolat leválasztásának megkezdéséhez. 0 és 65535 közötti szám adható meg.

Megjegyzés: A tényleges maximális számot a folyamatonként engedélyezett fájlok száma korlátozza. UNIX rendszereken a korlátok megadására az **ulimit -a** parancs használható. Windows rendszereken a szám rögzített.

Az alapértelmezett beállítás 1200. Amikor az összes kapcsolat számának ez a korlátja meghaladásra kerül, akkor a kapcsolatok az **Üresjáratú időkorlát** mezőben megadott határérték alapján törlésre kerülnek.

7. Az **Üresjáratú időkorlát** mezőben állítsa be, hogy egy kapcsolat hány másodpercig lehet tétlen, mielőtt azt egy törlési művelet bezárná. 0 és 65535 közötti szám adható meg.

Megjegyzés: A tényleges maximális számot a folyamatonként engedélyezett fájlok száma korlátozza. UNIX rendszereken a korlátok megadására az **ulimit -a** parancs használható. Windows rendszereken a

szám rögzített.

Az alapértelmezett beállítás 300. Amikor a törlési folyamat működésbe lép, minden ezáltal érintett, a korlátot meghaladó kapcsolat lezárásra kerül.

8. Az **Eredmény időkorlát** mezőben állítsa be, hogy hány másodperc várakozás lehet az írási kísérletek között. 0 és 65535 közötti szám adható meg. Az alapértelmezett beállítás 120. A korlátot meghaladó minden kapcsolat lezárásra kerül.

Megjegyzés: Ez csak a Windows rendszerekre érvényes. A 30 másodpercen túli kapcsolatok az operációs rendszer automatikusan eldobja. Ennek következtében ezt az **Eredmény időkorlátot** az operációs rendszer 30 másodperc után hatályon kívül helyezi.

9. Kattintson a **Vésszál** lapra.
10. Adja meg a vésszál beállításait. A **Vésszál engedélyezése** jelölőnégyzet már ki van választva, vagyis a vésszál engedélyezett. Ez az alapértelmezett beállítás. A jelölőnégyzetre kattintva megszüntetheti a **Vésszál engedélyezése** lehetőség kiválasztását. Ezzel a művelettel megelőzhető a vésszál aktiválása.
11. A **Függőben lévő kérések küszöbértéke** mezőben állítsa be a vésszálát aktiváló kérések számának korlátját. Adjon meg egy 0 és 65535 közötti számot, amellyel beállítja, hogy hány feladatkérés lehet a várakozási sorban, mielőtt a vésszál aktiválásra kerül. Az alapértelmezett beállítás az 50. Ha a megadott korlát meghaladásra kerül, a vésszál aktiválásra kerül.
12. Az **Időkorlát** mezőben állítsa be, hogy hány perc telhet el, miután az utolsó munka is eltávolításra került a sorból. Ha a sorban munkafeladatok vannak és ez az időkorlát meghaladásra került, akkor a vésszál aktiválásra kerül. 0 és 240 közötti szám adható meg. Az alapértelmezett beállítás 5.
13. Válassza ki a legördülő menüből a vésszál aktiválására használt feltételeket. A következők közül választhat:
 - **Csak méret:** A vésszál csak akkor kerül aktiválásra, ha a várakozási sorban a függőben lévő munkák meghaladják a megadott mennyiséget.
 - **Csak idő:** A vésszál csak akkor kerül aktiválásra, ha az eltávolított feladatok időkorlátja meghaladja a megadott mennyiséget.
 - **Méret vagy idő:** A vésszál akkor kerül aktiválásra, ha vagy a sorméret, vagy az időkorlát meghaladja a megadott mennyiséget.
 - **Méret és idő:** A vésszál akkor kerül aktiválásra, ha a sorméret és az időkorlát meghaladja a megadott mennyiséget.

Az alapértelmezett beállítás a Méret és idő.

14. Kattintson az **OK** gombra

További információk: "Szerverkapcsolatok kezelése" oldalszám: 113.

Az eseményértesítés engedélyezése

A Directory Server támogatja az eseményértesítést, ami lehetővé teszi, hogy az LDAP szerver értesítse a klienst, ha bekövetkezik egy bizonyos esemény, mint például a címtár kibővítése.


A szerveren az eseményértesítés engedélyezésének lépései:

1. Bontsa ki a webes adminisztrációs eszköz navigációs területének **Szervertulajdonságok kezelése** kategóriáját, és válassza az **Eseményértesítések** oldalt.
2. Válassza ki az **Eseményértesítések engedélyezése** jelölőnégyzetet az eseményértesítések engedélyezésére. Ha az **Eseményértesítések engedélyezése** ki van kapcsolva, akkor a szerver a panel összes többi beállítását figyelmen kívül hagyja.
3. Állítsa be a **Regisztrációk maximális száma kapcsolatonként** értéket. Kattintson vagy a **Regisztrációk** vagy a **Korlátlan** választógombra. Ha a **Regisztrációk** lehetőséget választotta, akkor meg kell adni a mezőben az egyes kapcsolatokhoz engedélyezett regisztrációk maximális számát. A tranzakciók maximális száma 2 147 483 647. Az alapértelmezett beállítás 100.
4. Állítsa be a **Regisztrációk maximális száma összesen** értéket. Ez a kiválasztás szabja meg, hogy a szerveren egy időben hány regisztráció lehet. Kattintson vagy a **Regisztrációk** vagy a **Korlátlan** választógombra. Ha a

Regisztrációk lehetőséget választotta, akkor meg kell adni a mezőben az egyes kapcsolatokhoz engedélyezett regisztrációk maximális számát. A tranzakciók maximális száma 2 147 483 647. A regisztrációk alapértelmezett száma **Korlátlan**.

5. Ha végzett, kattintson az **ALKalmazás** gombra, ha kilépés nélkül kívánja menteni a változásokat, illetve az **OK** gombra, ha menteni szeretne és kilépni, esetleg a **Mégse** gombra, ha változások nélkül szeretné elhagyni a panelt.
6. Ha engedélyezte az eseményértesítéseket, akkor a szervert újra kell indítani ahhoz, hogy a változások életbe lépjenek. Ha csak ezeket a beállításokat módosította, akkor a szervert nem kell újraindítani.

Megjegyzés: Az eseményértesítések kikapcsolásához szüntesse meg az **Eseményértesítések engedélyezése** jelölőnégyzet kijelölését és indítsa újra a szervert.

- | Az eseményértesítésekkel kapcsolatos további információkat az IBM Directory Server Version 5.2 Programozási kézikönyv  Eseményértesítés szakaszában talál.

Tranzakció-beállítások megadása

A Directory Server támogatja a tranzakciók használatát, amelynek segítségével a címtárszerver az LDAP címtárműveletek egy adott csoportját egy egységként kezeli. További információk: “Tranzakciók” oldalszám: 46.

A szerveren a tranzakciókezelés beállításokhoz végezze el az alábbi lépéseket:

1. Bontsa ki a webes adminisztrációs eszköz navigációs területének **Szervertulajdonságok kezelése** kategóriáját, és válassza a **Tranzakciók** oldalt.
2. A tranzakciókezelés engedélyezéséhez válassza ki a **Tranzakciókezelés engedélyezése** jelölőnégyzetet. Ha a **Tranzakciókezelés engedélyezése** ki van kapcsolva, akkor a panel többi beállítását (például a **Műveletek maximális száma tranzakciónként** vagy a **Függőben lévő tranzakciók időkorlátja**) a szerver figyelmen kívül hagyja.
3. Állítsa be a **Tranzakciók maximális száma** értéket. Kattintson vagy a **Tranzakciók** vagy a **Korlátlan** választógombra. Ha a **Tranzakciók** lehetőséget választotta, akkor meg kell adni a mezőben a tranzakciók maximális számát. A tranzakciók maximális száma 2 147 483 647. Az alapértelmezett beállítás 20 tranzakció.
4. Állítsa be a **Tranzakciónkénti műveletek maximális száma** értéket. Kattintson vagy a **Műveletek** vagy a **Korlátlan** választógombra. Ha a **Műveletek** lehetőséget választotta, akkor meg kell adni a mezőben az egyes tranzakciókhoz engedélyezett műveletek maximális számát. A műveletek maximális száma 2 147 483 647. Minél kisebb a szám, annál jobb a teljesítmény. A műveletek alapértelmezett száma 5.
5. Állítsa be a **Függőben lévő tranzakciók időkorlátja** értéket. Ez a kiválasztás a függőben lévő tranzakciók maximális időkorlát-értékét adja meg másodpercben. Kattintson vagy a **Másodpercek** vagy a **Korlátlan** választógombra. Ha a **Másodperc** lehetőséget választotta, akkor meg kell adni a mezőben az egyes tranzakciókhoz engedélyezett időt másodpercben. A másodpercek maximális száma 2 147 483 647. Az ezután az idő után még mindig elvégzetlen tranzakciók befejezés nélkül maradnak (visszagörgetésre kerülnek). Az alapértelmezett érték 300 másodperc.
6. Ha végzett, kattintson az **ALKalmazás** gombra, ha kilépés nélkül kívánja menteni a változásokat, illetve az **OK** gombra, ha menteni szeretne és kilépni, esetleg a **Mégse** gombra, ha változások nélkül szeretné elhagyni a panelt.
7. Ha engedélyezte a tranzakciók támogatását, akkor a szervert újra kell indítani ahhoz, hogy a változások életbe lépjenek. Ha csak ezeket a beállításokat módosította, akkor a szervert nem kell újraindítani.

Megjegyzés: A tranzakciókezelés kikapcsolásához szüntesse meg a **Tranzakciókezelés engedélyezése** jelölőnégyzet kiválasztását és indítsa újra a szervert.

Port vagy IP cím módosítása

A Directory Server az alábbi alapértelmezés szerinti portokat használja:

- 389 a nem védett kapcsolatok számára.
- 636 a védett kapcsolatok számára (ha a Digitális igazolás kezelő segítségével engedélyezte a Directory Server részére a védett port használatát).

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

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

Ha például a Domino LDAP szerver kerül ütközésbe a Directory Server-rel, akkor olvassa el a Domino LDAP és Directory Server üzemeltetése ugyanazon az iSeries rendszeren részt.

A Directory Server által használt portok megváltoztatásának lépései:

1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Properties** menüpontot.
5. Kattintson a **Hálózat** lapra.
6. Írja be a kívánt portszámokat, majd kattintson az **OK** gombra.

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

1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Properties** menüpontot.
5. Kattintson a **Hálózat** lapra.
6. Kattintson az **IP címek...** gombra.
7. Válassza ki a **Megjelölt IP címek használata** lehetőséget, majd válassza ki a szerver számára a kapcsolatok elfogadásakor használandó IP címeket.

Szerver kijelölése címtári utalások részére

Ha utalási szervereket kíván hozzárendelni a címtárszerverhez, kövesse az alábbi lépéseket:

1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Properties** menüpontot.
5. Válassza ki az **Általános** tulajdonságlapot.
6. Az **Új utalás** mezőben adja meg az utalási szerver URL-jét.
7. 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.

8. Kattintson a **Hozzáadás** gombra.
9. Kattintson az **OK** gombra.

Directory Server utótagok felvétele és eltávolítása

Egy 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 címtárszerveren, nem veheti fel a ou=rochester, o=ibm, c=us utótagot.

Ha utótagot kíván felvenni a címtárszerverbe, kövesse az alábbi lépéseket:

1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Properties** menüpontot.
5. Kattintson az **Adatbázis/utótagok** lapra.
6. Az **Új utótag** mezőbe írja be az új utótag nevét.
7. Kattintson a **Hozzáadás** gombra.
8. Kattintson az **OK** gombra.

Megjegyzés: Egy utótag felvétele rámutat a címtár egy szakaszára, de objektumokat nem hoz létre. Ha az új utótagnak egy nem létező objektum felel meg, akkor ezt más objektumokhoz hasonlóan létre kell hozni.

A Directory Server egy utótagjának eltávolítása:

1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Properties** menüpontot.
5. Kattintson az **Adatbázis/utótagok** lapra.
6. Kattintással válassza ki azt az utótagot, amelyet törölni kíván.
7. Kattintson a **Törlés** gombra.

Megjegyzés: Választhatja az utótag olyan módon történő törlését is, hogy az alatta lévő címtárobjektumok ne töröljenek. Az adatok ilyenkor elérhetetlenné válnak a címtárszerverből. Az adatok elérését visszaállíthatja, ha újra felveszi az utótagot.

A Directory Server információinak mentése és visszaállítása

A Directory Server a következő helyeken tárol információt:

- Adatbáziskönyvtár (alapértelmezés szerint a QUSRDIRDB), amely tartalmazza a címtárszerver tartalmát.


Megjegyzés: Hogy melyik adatbázis-könyvtárat használja, azt az IBM Directory Server **Adatbázis/utótag** lapjának használatával nézheti meg az iSeries Navigatorban.

- QDIRSRV2 könyvtár, melyben címtárszerver publikált információt tárolja.
- QUSRSYS könyvtár, amely különböző tételeket objektumokban tárol a QGLD-vel kezdődően (a QUSRSYS/QGLD* paranccsal lehet őket menteni).
- Ha a címtárszervert úgy állítja be, hogy az naplózza a címtár változásait, akkor a változtatási napló a QUSRDIRCL nevű adatbáziskönyvtárat használja.

Ha a könyvtár tartalma gyakran változik, a benne levő adatbáziskönyvtárt 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 adatok mentését és visszaállítását.

Adminisztrátori hozzáférés megadása leképezett felhasználóknak

Adminisztrátori hozzáférést is adhat azoknak a felhasználói profiloknak, amelyeknek hozzáférésük van a Directory Server adminisztrátori (QIBM_DIRSRV_ADMIN) funkció azonosítóhoz (ID).

Például, ha a JOHNSMITH felhasználói profilnak hozzáférése van a Directory Server adminisztrátori funkció azonosítóhoz (ID), és a Címtár tulajdonságok párbeszédablakban kiválasztotta a Adminisztrátori hozzáférés megadása a hitelesített felhasználók számára lehetőséget, 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 címtárszerverhez, a felhasználó adminisztrátori jogosultsággal fog rendelkezni. A rendszerobjektumok utótagja ebben a példában os400-sys=systemA.acme.com. A leképzett felhasználókról itt olvashat: "Operációs rendszer leképzett háttér objektumai" oldalszám: 75.

A beállítás kiválasztásához az alábbi lépéseket kell elvégezni:

1. az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a jobb oldali egérgombbal a **Címtár** felírra, és válassza a **Tulajdonságok** lapot.
4. Az **Adminisztrátor információk** alatti **Általános** lapon válassza ki az **Adminisztrátori hozzáférés megadása a hitelesített felhasználók számára** lehetőséget.

Hajtsa végre az alábbi lépéseket, amikor a Directory Server adminisztrátori jogosultságát állítja be a felhasználói profilban:

1. Az iSeries navigátorban kattintson a jobb egérgombbal a rendszernévre, és válassza ki az **Alkalmazások adminisztrációja** lehetőséget.
2. Kattintson a **Hosztalkalmazás** lapra.
3. Bontsa ki az **Operating System/400** elemet.
4. Kattintson a **Directory Server Administrator** elemre, melynek hatására az megjelölődik.
5. Kattintson a **Testreszabás** gombra.
6. Bontsa ki a **Felhasználók, Csoportok** vagy a **Nem csoporttag felhasználók** részt, amelyik megfelelő a felhasználó esetében.
7. Válassza ki a **Hozzáférés engedélyezett** listához hozzáadandó felhasználót vagy csoportot.
8. Kattintson a **Hozzáadás** gombra.
9. Kattintson az **OK** gombra a változtatások mentéséhez.
10. Kattintson az **OK** gombra az **Alkalmazás-adminisztráció** párbeszédablakban.

Adminisztrációs csoport kezelése

A adminisztrációs csoport lehetőséget ad az adminisztrációs szolgáltatások ellátására anélkül, hogy az adminisztrátoroknak egyetlen azonosítón és jelszón kellene osztozniuk. Az adminisztrációs csoport tagjainak saját azonosítójuk és jelszavuk van. Az adminisztrációs csoporttagok megkülönböztetett neve nem egyezhet meg egymással, és ugyanígy nem egyezhetnek meg az IBM Directory Server adminisztrátor DN-jeivel. Ennek megfelelően az IBM Directory Server adminisztrációs DN-nek sem egyezhetnek meg egyetlen adminisztrációs csoporttag megkülönböztetett nevével sem.

Ez a szabály az IBM Directory Server adminisztrátorok és az adminisztrációs csoporttagok Kerberos vagy Digest-MD5 azonosítóira is vonatkozik. Ezeknek a megkülönböztetett neveknek nem szabad megegyezniük az IBM Directory Server replikációszoigálató DN-jeivel. Ez azt is jelenti, hogy az IBM Directory Server replikációszoigálató DN-jeinek nem szabad egyezniük egyetlen adminisztrációs csoporttag vagy az IBM Directory Server adminisztrátor DN-jével sem.

Megjegyzés: Az IBM Directory Server replikációszoigálató DN-jei megegyezhetnek egymással.

További információk:

- "Az adminisztrációs csoport engedélyezése" oldalszám: 121
- "Adminisztrációs csoport tagjainak hozzáadása, módosítása és eltávolítása" oldalszám: 121

Kapcsolódó információk

"Adminisztratív hozzáférés" oldalszám: 55

Az adminisztrációs csoport engedélyezése

Ennek a műveletnek az elvégzéséhez IBM Directory Server adminisztrátornak kell lennie.

1. Bontsa ki a **Szerveradminisztráció** kategóriát a webadminisztrációs eszköz navigációs területén, és kattintson az **Adminisztrációs csoportok kezelése** lehetőségre.

Megjegyzés: A szerver konfigurációs beállításainak módosításához a webadminisztrációs eszköz Szerveradminisztrációs kategóriájának használatával hitelesítenie kell magát a szerverhez egy i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultságokkal. Ez úgy történhet, hogy hitelesíti magát leképezett felhasználóként az adott profil jelszavával. A kapcsolódáshoz a webes adminisztrációs eszközhöz leképezett felhasználóként adjon meg egy felhasználónevet a következő formában: `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, ahol a MYUSERNAME és MYSYSTEM.COM karaktersorozatokat a saját felhasználói profiljának nevével és a beállított rendszerleképezési utótaggal helyettesíti.

2. Az adminisztrációs csoport engedélyezéséhez vagy letiltásához kattintson az **Adminisztrációs csoport engedélyezése** melletti jelölőnégyzetre. Ha a jelölőnégyzet ki van jelölve, akkor az adminisztrációs csoport engedélyezett.
3. Kattintson az **OK** gombra.

Megjegyzés: Ha letiltja az adminisztrációs csoportot, akkor annak bejelentkezett tagjai továbbra is végezhetnek adminisztrációs műveleteket, egészen addig, amíg újra be nem kell jelentkezniük.

Adminisztrációs csoport tagjainak hozzáadása, módosítása és eltávolítása

Előfeltétel: Ennek a műveletnek az elvégzéséhez IBM Directory Server adminisztrátornak kell lennie.

1. Bontsa ki a **Szerveradminisztráció** kategóriát a webadminisztrációs eszköz navigációs területén, és kattintson az **Adminisztrációs csoportok kezelése** lehetőségre.

Megjegyzés: A szerver konfigurációs beállításainak módosításához a webadminisztrációs eszköz Szerveradminisztrációs kategóriájának használatával hitelesítenie kell magát a szerverhez egy i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultságokkal. Ez úgy történhet, hogy hitelesíti magát leképezett felhasználóként az adott profil jelszavával. A kapcsolódáshoz a webes adminisztrációs eszközhöz leképezett felhasználóként adjon meg egy felhasználónevet a következő formában: `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, ahol a MYUSERNAME és MYSYSTEM.COM karaktersorozatokat a saját felhasználói profiljának nevével és a beállított rendszerleképezési utótaggal helyettesíti.

2. Az **Adminisztrációs csoport kezelése** panelben kattintson a **Hozzáadás** lehetőségre.
3. Az **Adminisztrációs csoport tagjának hozzáadása** panelben:
 - a. Adja meg a tag adminisztrátori megkülönböztetett nevét (ennek érvényes megkülönböztetett név szintaxisnak kell lennie).
 - b. Adja meg a tag jelszavát.
 - c. A megerősítéshez adja meg ismét a tag jelszavát.
 - d. Nem kötelező: Adja meg a tag Kerberos azonosítóját. A kerberos azonosító formátuma vagy `ibm-kn`, vagy `ibm-KerberosName`. Az értékekben a kis- és a nagybetűk nem számítanak eltérőnek, vagyis például az `ibm-kn=root@TEST.ROCHESTER.IBM.COM` egyenlő az `ibm-kn=ROOT@TEST.ROCHESTER.IBM.COM` értékkel.
4. Nem kötelező: adja meg a tag **Digest-MD5 felhasználónevet**.

Megjegyzés: A Digest-MD5 felhasználónévben a kis- és nagybetűk különbözőnek számítanak.

5. Kattintson az **OK** gombra.
6. Ismételve meg az eljárást minden, az adminisztrációs csoportba felvenni kívánt tagnál.

- | A tag adminisztrátori megkülönböztetett neve, Digest-MD5 felhasználóneve és (ha meg van adva) Kerberos azonosítója megjelenik az Adminisztrációs csoport tagjai listában.
- | Az adminisztrációs csoport tagjainak módosításához vagy eltávolításához is a fent leírtakat kell tennie, de az **Adminisztrációs csoport** panelben használja a **Szerkesztés** és **Törlés** gombokat.

| Keresésikorlát-csoportok kezelése

- | Annak megelőzésére, hogy a felhasználók kérései túl sok erőforrást foglaljanak le és ennek következményeképp lerontsák a szerver teljesítményét, keresési korlátokat kell szabni ezekre a kérésekre minden megadott szerveren. Ezeket a méretet és időtartamot megadó keresési korlátokat az adminisztrátor adja meg a szerver beállítása során.
- | Ezekre a minden más felhasználóra vonatkozó korlátok alól csak az adminisztrátor és az adminisztrációs csoport tagjai mentesülnek. Az igényektől függően azonban adminisztrátorok az általános felhasználóknál sokkal rugalmasabb keresési korlátokkal rendelkező keresésikorlát-csoportokat hozhatnak létre. Ezen a módon az adminisztrátor speciális keresési jogosultságokat adhat felhasználói csoportoknak.
- | További információk:
 - | • “Keresésikorlát-csoport létrehozása”
 - | • “Keresésikorlát-csoport módosítása” oldalszám: 123
 - | • “Keresésikorlát-csoportok másolása” oldalszám: 123
 - | • “Keresésikorlát-csoport eltávolítása” oldalszám: 123

- | A keresésikorlát-csoportok felügyeletére a webes adminisztrációs eszköz használható.

| Kapcsolódó fogalmak

- | “Keresési paraméterek” oldalszám: 43

| Keresésikorlát-csoport létrehozása

- | Egy keresésikorlát-csoport létrehozásához létre kell hozni egy csoportbejegyzést a webes adminisztrációs eszköz segítségével.
 - | 1. Bontsa ki a navigációs terület **Címtárfelügyelet** kategóriáját, majd kattintson a **Bejegyzés hozzáadása** lehetőségre. A **Bejegyzések kezelése** menüpontra is kattinthat; ekkor válassza ki a helyet (cn=IBMpolicies vagy cn=localhost), és kattintson a **Hozzáadás** lehetőségre. A cn=IBMpolicies alatt található bejegyzések replikálásra fognak kerülni, a cn=localhost alattiak nem.
 - | 2. Válasszon ki egy csoportobjektum-osztályt a **Strukturális objektumosztály** menüből.
 - | 3. Kattintson a **Tovább** gombra.
 - | 4. Válasszon ki egy **ibm-searchLimits** kiegészítő objektumosztályt a **Rendelkezésre álló** menüből, és kattintson a **Hozzáadás** gombra. Ismételje meg ezt az eljárást minden hozzáadandó kiegészítő objektumosztálynál. A **Kiválasztott** menüből egy kiegészítő objektumosztály úgy távolítható el, ha kiválasztja, és az **Eltávolítás** gombra kattint.
 - | 5. Kattintson a **Tovább** gombra.
 - | 6. A **Relatív DN** mezőben írja be a felvenni kívánt csoport viszonylagos megkülönböztető nevét (RDN-jét). Például: cn=Search Group1.
 - | 7. A **Szülő DN** mezőbe írja be a kiválasztott fabejegyzés nevét. Például: cn=localhost. Kattinthat a **Tallózás** gombra is, ha a Szülő DN-t listából akarja kiválasztani. Jelöljön ki egy lehetőséget és kattintson a **Kiválasztás** gombra egy szülő DN megadásához. A **Szülő DN** alapértelmezés szerint a fában kijelölt bejegyzés.

- | **Megjegyzés:** Ha ezt a feladatot a **Bejegyzések kezelése** ablakból indította, akkor ez a mező már előre ki van töltve. A **szülő DN** ki volt választva, mielőtt a bejegyzéshozzáadási művelet megkezdéséhez a **Hozzáadás** lehetőségre kattintott.

8. A **Kötelező attribútumok** lapon írja be a kötelező attribútumok értékeit.
 - A **cn** a korábban már megadott relatív megkülönböztetett név.
 - Az **ibm-searchSizeLimit** mezőben adja meg a bejegyzések számát, amelyek szerint a keresés méretét korlátozni kell. Ez a szám 0 és 2 147 483 647 között lehet. A 0 érték megadása ugyanaz, mint a **Korlátlan**.
 - Az **ibm-searchTimeLimit** mezőben adja meg a másodpercek számát, amelyek szerint a keresés időtartamát korlátozni kell. Ez a szám 0 és 2 147 483 647 között lehet. A 0 érték megadása ugyanaz, mint a **Korlátlan**.
 - A kiválasztott objektumosztálytól függően egy **Member** vagy egy **uniqueMember** mezőt láthat. Ezek az éppen létrehozott csoport tagjai. A bejegyzés formátuma egy DN, például cn=Bob Garcia,ou=austin,o=ibm,c=us.
9. Ha egynél több értéket akar megadni egy adott attribútumnak, akkor kattintson a **Többszörös érték** gombra, és írja be egyesével az értékeket. Ha végzett a több érték megadásával, kattintson az **OK** gombra. Az értékek bekerülnek egy kibontható menübe, amely az attribútum mellett jelenik meg.
10. Ha a szerveren vannak nyelvi címkék engedélyezve, akkor kattintson a **Nyelvi címke érték** lehetőségre a nyelvi címkék leírónak hozzáadásához vagy eltávolításához.
11. Kattintson az **Egyéb attribútumok** menüpontra.
12. Az **Egyéb attribútumok** lapon írja be az attribútumokhoz megfelelő értékeket. További információk: “Bináris attribútumok módosítása” oldalszám: 174.
13. A bejegyzés létrehozásához kattintson a **Befejezés** lehetőségre.

Keresésikorlát-csoport módosítása

Módosíthatja a keresésikorlát-csoportok méret- vagy időkorlát-attribútumait. Csoporttagokat is felvehet és törölhet. A webes adminisztrációs eszközzel módosíthat egy keresésikorlát-csoportot.

A keresésikorlát-csoportok módosításával kapcsolatban lásd: “Bejegyzés módosítása” oldalszám: 170.

Keresésikorlát-csoportok másolása

Hasznos a keresésikorlát-csoportok lemásolása, ha ugyanazt a localhost és az IBMpolicies alatt is tárolni szeretné. Ezt akkor is érdemes megtenni, ha létre szeretne hozni egy új csoportot, amely azonos információkat tartalmaz, mint egy meglévő csoport, de kismértékben eltér attól.

Keresésikorlát-csoport másolása. További információk: “Bejegyzés másolása” oldalszám: 171.

Keresésikorlát-csoport eltávolítása

Keresésikorlát-csoport eltávolítása. További információk: “Bejegyzés törlése” oldalszám: 170.

Proxy hitelesítési csoport kezelése

A proxy hitelesítési csoport a tagjai elérhetik a Directory Servert és számos feladatot végezhetnek el több felhasználó nevében anélkül, hogy minden egyes felhasználó nevében újra kellene csatlakozni. A proxy hitelesítési csoport tagjai bármelyik hitelesített jogosultságot felvehetik, kivéve az adminisztrátorét vagy az adminisztrációs csoport tagjait. További információk: “Proxy hitelesítés” oldalszám: 55.

A proxy hitelesítés felügyeletére a webes adminisztrációs eszköz használható.

További információk:

- “Proxy hitelesítési csoport létrehozása” oldalszám: 124
- “Proxy hitelesítési csoport módosítása” oldalszám: 124
- “Proxy hitelesítési csoport másolása” oldalszám: 125
- “Proxy hitelesítési csoport eltávolítása” oldalszám: 125

Proxy hitelesítési csoport létrehozása

1. Bontsa ki a navigációs terület **Címtárfelügyelet** kategóriáját, majd kattintson a **Bejegyzés hozzáadása** lehetőségre. A **Bejegyzések kezelése** menüpontra is kattinthat; ekkor válassza ki a helyet (cn=ibmPolicies vagy cn=localhost), és kattintson a **Hozzáadás** lehetőségre.
2. Válassza ki a **groupof Names** objektumosztályokat a **Strukturális objektumosztály** menüből.
3. Kattintson a **Tovább** gombra.
4. Válassza ki az **ibm-proxyGroup** kiegészítő objektumosztályt a **Rendelkezésre álló** menüből és kattintson a **Hozzáadás** gombra. Ismétlje ezt meg minden további felvenni kívánt kiegészítő objektumosztálynál.
5. Kattintson a **Tovább** gombra.
6. A **Relatív megkülönböztetett név** mezőben adja meg a cn=proxyGroup értéket.
7. A **Szülő DN** mezőbe írja be a kiválasztott fabejegyzés nevét, például cn=localhost. A **Tallózás** gombra kattintva ki is választhatja a **szülő DN**-t a listából. Adja meg a kiválasztott elemet, majd kattintson a **Kiválasztás** gombra a kívánt szülő DN megadásához. A szülő DN alapértelmezett értéke a fában kiválasztott bejegyzést.

Megjegyzés: Ha ezt a feladatot a Bejegyzések kezelése ablakból indította, akkor ez a mező már előre ki van töltve. A szülő DNt már kiválasztotta, mielőtt a Hozzáadás gombbal elindította volna a bejegyzés felvételi folyamatát.

8. A **Kötelező attribútumok** lapon adja meg a kötelező attribútumok értékeit.
 - A **cn** a proxyGroup .
 - A **Tag** formátuma egy DN, például cn=Bob Garcia,ou=austin,o=ibm,c=us.
A bináris értékek felvételével kapcsolatos további információk: “Bináris attribútumok módosítása” oldalszám: 174.
9. Ha egynél több értéket akar megadni egy adott attribútumnak, akkor kattintson a **Többszörös érték** gombra, és írja be egyesével az értékeket.

Megjegyzés: Ne hozzon létre több értéket egy cn értékhez. A proxy hitelesítési csoport nevének a jólismert névnek, a proxyGroup-nak kell lennie.
Ha végzett a több érték megadásával, kattintson az **OK** gombra. Az értékek bekerülnek egy kibontható menübe, amely az attribútum mellett jelenik meg.

10. Ha a szerveren vannak nyelvi címkék engedélyezve, akkor kattintson a **Nyelvi címke érték** lehetőségre a nyelvi címkék leíróinak hozzáadásához vagy eltávolításához.
11. Kattintson az **Egyéb attribútumok** menüpontra.
12. Az **Egyéb attribútumok** lapon írja be az attribútumokhoz megfelelő értékeket. A bináris értékek felvételével kapcsolatos további információk: “Bináris attribútumok módosítása” oldalszám: 174.
13. Ha egynél több értéket akar megadni egy adott attribútumnak, akkor kattintson a **Többszörös érték** gombra, és írja be egyesével az értékeket. Ha végzett a több érték megadásával, kattintson az **OK** gombra. Az értékek bekerülnek egy kibontható menübe, amely az attribútum mellett jelenik meg.
14. Ha a szerveren vannak nyelvi címkék engedélyezve, akkor kattintson a **Nyelvi címke érték** lehetőségre a nyelvi címkék leíróinak hozzáadásához vagy eltávolításához.
15. A bejegyzés létrehozásához kattintson a **Befejezés** lehetőségre.

Proxy hitelesítési csoport módosítása

A proxy hitelesítési csoport módosításához (például tagok hozzáadásához vagy törléséhez) a webes adminisztrációs eszköz használható.

A proxy hitelesítési csoportok módosításához lásd: “Bejegyzés módosítása” oldalszám: 170.

Proxy hitelesítési csoport másolása

Hasznos a proxy hitelesítési csoportok lemásolása, ha ugyanazt a localhost és az IBMpolicies alatt is tárolni szeretné.

A proxy hitelesítési csoportok másolásához lásd: “Bejegyzés másolása” oldalszám: 171.

Proxy hitelesítési csoport eltávolítása

A proxy hitelesítési csoport egy tagjának eltávolításához webes adminisztrációs eszköz használatával lásd: “Bejegyzés törlése” oldalszám: 170.

Egyedi attribútumok kezelése

Az egyedi attribútumok kezelése a webes adminisztrációs eszköz **Szerveradminisztráció** kategóriájának használatával történik. További információk:

- “Egyedi attribútumlista létrehozása”
- “Bejegyzés eltávolítása az egyedi attribútumlistából” oldalszám: 126

Megjegyzés: Attribútumonként a nyelvi címkék közösen kizárják egymást az egyedi attribútumokkal. Ha egy adott attribútum egyedi attribútumként van megjelölve, akkor nem lehet hozzárendelve nyelvi címke.

Megjegyzés: A szerver konfigurációs beállításainak módosításához a webadminisztrációs eszköz Szerveradminisztráció kategóriájának használatával hitelesítenie kell magát a szerverhez egy i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultságokkal. Ez úgy történhet, hogy hitelesíti magát leképezett felhasználóként az adott profil jelszavával. A kapcsolódáshoz a webes adminisztrációs eszközhöz leképezett felhasználóként adjon meg egy felhasználónevet a következő formában: `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, ahol a MYUSERNAME és MYSYSTEM.COM karaktersorozatokat a saját felhasználói profiljának nevével és a beállított rendszerlekepezési utótaggal helyettesíti.

Egyedi attribútumlista létrehozása

1. Bontsa ki a **Szerveradminisztráció** kategóriát a navigációs területen. Kattintson az **Egyedi attribútumok kezelése** lehetőségre.
2. Válassza ki azt az attribútumot, amelyet egyedi attribútumként hozzá szeretne adni a **Rendelkezésre álló attribútumok** menüből. A felsorolt rendelkezésre álló attribútumok azok, amelyek egyediként vannak megjelölve; pl.: `sn`.
3. Kattintson vagy a **Hozzáadás: cn=localhost** vagy a **Hozzáadás: cn=IBMpolicies** lehetőségre. A két tároló között az a különbség, hogy a `cn=IBMpolicies` bejegyzései replikálásra kerülnek, míg a `cn=localhost` bejegyzései nem. Az attribútum a megfelelő listájában jelenik meg. Ugyanazt az attribútumot mindkét tárolóban kilistázhatja.

Megjegyzés: Ha egy bejegyzés mind a `cn=localhost`, mind a `cn=IBMpolicies` alatt létrehozásra került, a két bejegyzés egyesült eredménye az egyedi attribútumok listája. Ha például a `cn` és `employeeNumber` attribútumok egyediként vannak megjelölve a `cn=localhost` objektumban, a `cn` és a `telephoneNumber` pedig a `cn=IBMpolicies` objektumban, a szerver a `cn`, `employeeNumber` és `telephoneNumber` attribútumokat kezeli egyediékként.

4. Ismétlje meg ezt a műveletet minden egyediként felvenni kívánt attribútumnál.
5. Kattintson az **OK** gombra a változtatások mentéséhez.

Egy egyedi attribútum bejegyzés hozzáadásakor vagy módosításakor, ha a felsorolt egyedi attribútumtípusok bármelyikénél egy egyedi megszorítás hibát okoz, akkor az a bejegyzés nem kerül hozzáadásra illetve létrehozásra a címtárban. A bejegyzés létrehozásához vagy módosításához először meg kell oldani a gondot és újra ki kell adni a hozzáadás vagy módosítás parancsot. Például: egyedi attribútumbejegyzések címtárhoz adása közben ha a felsorolt egyedi attribútumtípusok valamelyikének táblázatában egy egyedi megszorítás létrehozása meghiúsul (például azért, mert többször szereplő értékek vannak az adatbázisban), akkor az egyedi attribútum-bejegyzések nem kerülnek hozzáadásra a címtárhoz. Hibaüzenet érkezik.

| Ha egy alkalmazás megkísérel hozzáadni egy bejegyzést a cím tárhoz egy olyan attribútumértékkel, amely megegyezik a
| meglévő cím tárbejegyzéssel, akkor az LDAP szerverről egy 20. eredménykódú hibaüzenet érkezik (LDAP: error code 20
| - Attribute or Value Exists).

| A szerver elindulásakor ellenőrzi az egyedi attribútumok listáját és meghatározza, hogy van-e valamelyikhez DB2
| megszorítás. Ha nincs megszorítás egy attribútumhoz, mivel azt a tömegterhelési segédprogram törölte vagy a
| felhasználó kézzel eltávolította, akkor eltávolításra kerül az egyedi attribútumok listájából és a hibnaplóba
| (ibmslapd.log) bekerül egy hibaüzenet. Ha a cn attribútum egyediként van megjelölve a
| cn=uniqueattributes,cn=localhost objektumban, és nincs hozzá DB2 megszorítás, akkor a következő üzenet kerül a
| naplóba:

| A CN attribútum értékei nem egyediek.
| A CN attribútum törlésre került az egyedi attribútumok közül.
| bejegyzés: CN=UNIQUEATTRIBUTES,CN=LOCALHOST

| **Bejegyzés eltávolítása az egyedi attribútumlistából**

| Ha egy egyedi attribútum mind a cn=uniqueattribute,cn=localhost, mind pedig a cn=uniqueattribute,cn=IBMpolicies
| objektumban létezik és csak az egyik bejegyzésből kerül törlésre, akkor a szerver továbbra is egyedi attribútumként
| fogja kezelni. Az attribútum akkor válik nem egyedivé, amikor mindkét bejegyzésből eltávolításra kerül.

- | 1. Bontsa ki a navigációs terület **Szerveradminisztráció** kategóriáját, majd kattintson az **Egyedi attribútumok**
| **kezelése** lehetőségre.
- | 2. Válassza ki az egyedi attribútumok listájából eltávolítani kívánt attribútumot azzal, hogy a megfelelő listában
| rákattint az attribútumra.
- | 3. Kattintson a **Törlés** gombra.
- | 4. Ismétlje meg ezt a műveletet minden attribútumnál, amelyet el kíván távolítani a listából.
- | 5. Kattintson az **OK** gombra a változtatások mentéséhez.

| **Megjegyzés:** Ha az utolsó egyedi attribútumot is eltávolítja a cn=localhost vagy a cn=IBMpolicies listából akkor a
| cn=uniqueattribute,cn=localhost vagy a cn=uniqueattribute,cn=IBMpolicies lista tárolóbejegyzése
| automatikusan törlésre kerül.

| **Az LDAP cím tár eléréseinek és változásainak nyomon követése**

| Hasznos lehet tájékoztatást kapni az LDAP cím tár eléréseiről és módosításairól. Az LDAP cím táruk változásait
| tartalmazó napló segítségével nyomon követheti a cím tár változásait. A változtatási napló a cn=changelog speciális
| utótag alatt található meg. Ezt a QUSRDIRCL könyvtár tárolja.

| A változtatási napló engedélyezéséhez kövesse ezeket a lépéseket:

- | 1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
- | 2. Bontsa ki a **Szerverek** elemet.
- | 3. Kattintson a **TCP/IP** pontra.
- | 4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Properties** menüpontot.
- | 5. Kattintson a **Változtatási napló** lapra.
- | 6. Válassza ki a **Cím tár változások naplózása** elemet.
- | 7. Választható: A **Maximum entries** mezőben adja meg a változtatási naplóban megtartandó bejegyzések maximális
| számát. A **Maximális kor** mezőben adja meg, hogy mennyi ideig tárolódjanak a változtatási napló bejegyzései.

| **Megjegyzés:** Annak ellenére, hogy ezek a paraméterek nem kötelezők, erősen fontolja meg a bejegyzések
| maximális számának vagy a maximális kor megadását. Ha egyiket sem adja meg, a változtatási napló
| minden bejegyzést megtart, így a mérete túl nagyra nőhet.

| A changeLogEntry objektumosztály képviseli a cím társzerverre vonatkozó változásokat. A changeNumber által
| megadott módon, a changelog tárolóban lévő összes bejegyzés rendezett készlete adja a változások halmazát. A
| változtatási napló csak olvasható.

Bármely felhasználó, aki rajta van a `cn=changelog` utótag hozzáférés-felügyeleti listáján, kereshet a változtatási napló bejegyzéseiben. A `cn=changelog` változtatási napló utótag alatt kizárólag kereshet. Ne kíséreljen meg hozzáadni, módosítani vagy törölni a változtatási napló utótag alatt, 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 változtatási napló bejegyzés betöltéséhez:

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

Objektum naplózás engedélyezése a Directory Server számára

Directory Server támogatja az i5/OS biztonsági ellenőrzést. Ha a QAUDCTL rendszer értékben `*OBJAUD` került beállításra, az iSeries navigátor segítségével engedélyezhető az objektumok naplózása.

A Directory Server számára az objektumnaplózás az alábbi lépésekkel engedélyezhető:

1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Properties** menüpontot.
5. Kattintson az **Ellenőrzések** lapra.
6. Válassza ki a szerverben használni tervezett naplózási beállításokat.
7. Kattintson az **OK** gombra

A naplózási beállítások az **OK** gombra történő kattintás után hatályba lépnek. Nincs szükség a Directory Server újraindítására. További információk: "Directory Server biztonsága" oldalszám: 46.

Keresési beállítások módosítása

A webes adminisztrációs eszköz használatával beállíthatók keresési paraméterek a felhasználók keresési lehetőségeinek (például az oldalakra bontott és sorba rendezett keresések, méret- és időkorlátok és álnévhivatkozás-feloldási beállítások) szabályozása érdekében.

Az oldalakra bontott keresési funkcióval szabályozható az egy keresési kérésből egyszerre visszakapott adatok mennyisége. A kliens kérheti a bejegyzések egy részhalmazát (egy oldal), vagy kérheti a teljes eredményhalmazt egyszerre. A további keresési kérések az eredmények következő oldalát adják vissza, addig, amíg a kérés visszavonásra nem kerül, vagy az utolsó eredmény is ki nem lett szolgáltatva.

A rendezett keresés eredményeit a kliens egy feltételista szerint rendezett formában kapja vissza, ahol az egyes feltételek rendezési kulcsokat reprezentálnak. A rendezés feladata így módon átterhelhető a kliensről a szerverre.

A címtárszerver keresési beállításainak pontosításához tegye a következőket:

1. Bontsa ki a navigációs terület **Szerveradminisztráció** kategóriáját, majd kattintson a **Szervertulajdonságok kezelése** lehetőségre.

Megjegyzés: A szerver konfigurációs beállításainak módosításához a webadminisztrációs eszköz Szerveradminisztrációs kategóriájának használatával hitelesítenie kell magát a szerverhez egy i5/OS felhasználói profillal, amely rendelkezik a speciális `*ALLOBJ` és `IOSYSCFG` jogosultságokkal. Ez úgy történhet, hogy hitelesíti magát leképezett felhasználóként az adott profil jelszavával. A kapcsolódáshoz a webes adminisztrációs eszközhöz leképezett felhasználóként adjon meg egy felhasználónevet a következő formában: `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, ahol a `MYUSERNAME` és `MYSYSTEM.COM` karaktersorozatokat a saját felhasználói profiljának nevével és a beállított rendszerleképezési utótaggal helyettesíti.

2. Válassza ki a **Keresési beállítások** lapot.

3. Állítsa be a **Keresési méretkorlát** értéket. Kattintson vagy a **Bejegyzések** vagy a **Korlátlan** választógombra. Ha a **Bejegyzések** lehetőséget választotta, akkor meg kell adni a mezőben a bejegyzések maximális számát. Az alapértelmezett beállítás 500. Ha a keresési feltételnek több bejegyzés felel meg, akkor azok nem kerülnek visszaadásra. Ez a korlát nem vonatkozik az adminisztrátorokra vagy azoknak a kereséskorlát-csoportoknak a tagjaira, akik nagyobb keresési méretkorlátot kaptak.
4. Állítsa be a **Keresési időkorlát** értéket. Kattintson vagy a **Másodpercek** vagy a **Korlátlan** választógombra. Ha a **Másodperc** lehetőséget választotta, akkor meg kell adni a mezőben, hogy a szerver maximum mennyi időt tölthet a keresés feldolgozásával. Az alapértelmezett beállítás 900. Ez a korlát nem vonatkozik az adminisztrátorokra vagy azoknak a kereséskorlát-csoportoknak a tagjaira, akik nagyobb keresési időkorlátot kaptak.
5. Ha a keresésrendezési funkciót csak az adminisztrátorokra szeretné korlátozni, akkor válassza ki a **Csak az adminisztrátorok számára engedélyezett a keresések rendezése** jelölőnégyzetet.
6. Ha a kereséslapozási funkciót csak az adminisztrátorokra szeretné korlátozni, akkor válassza ki a **Csak az adminisztrátorok számára engedélyezett a keresések lapozása** jelölőnégyzetet.
7. Bontsa ki az **Álnévhibavizsgálás-feloldás** menüpontot és válassza ki a következők valamelyikét. Az alapértelmezett beállítás a **Mindig**.

Soha Az álnevek soha nem kerülnek feloldásra.

Találat Az álnevek akkor kerülnek feloldásra, amikor a rendszer megtalálja a keresés kiindulópontját, nem pedig az induló bejegyzés alatti kereséskor.

keresés

Az álnevek a keresési kiindulópont alatti kereséskor kerülnek feloldásra, nem pedig akkor, amikor a kiinduló bejegyzést a rendszer megtalálja.

Mindig

Az álnevek mindig feloldásra kerülnek, a keresés kiindulópontjának megtalálásakor és az induló bejegyzés alatt végzett kereséskor is. A Mindig az alapértelmezett beállítás.

További információk: "Keresési paraméterek" oldalszám: 43 és "Címtárbejegyzések keresése" oldalszám: 172.

Teljesítménnyel kapcsolatos beállítások módosítása

A Directory Server teljesítménye az alábbi jellemzők módosításával állítható be:

- Az ACL gyorsítótár mérete, a bejegyzés-gyorsítótár mérete, a szűrő gyorsítótárban tárolt keresések maximális száma, valamint a szűrő gyorsítótárban tárolt legnagyobb keresés.
- Az adatbázis-kapcsolatok és a szerverszálak száma
- Az attribútum-gyorsítótár beállításai
- A szerver tranzakciós beállításai

További információk:

- "Adatbázis-kapcsolatok és gyorsítótár-beállítások megadása"
- "Attribútum-gyorsítótár beállítása" oldalszám: 129
- "Tranzakciós beállítások megadása" oldalszám: 131

Adatbázis-kapcsolatok és gyorsítótár-beállítások megadása

Az adatbázis-kapcsolatok és gyorsítótári beállítások megadásához tegye a következőket:

1. Bontsa ki a **Szervertulajdonságok kezelése** kategóriát a webes adminisztrációs eszköz navigációs területén, és kattintson a jobboldali ablakrész **Teljesítmény** lapjára.
2. Adja meg az **Adatbázis-kapcsolatok számát**. Ezzel állítható be a szerveren használt DB2 kapcsolatok száma. A minimális megadandó érték 4, az alapértelmezett beállítás 15. Ha az LDAP szerver nagymennyiségű klienskerést fogad vagy a kliensek "kapcsolat visszautasítva" üzeneteket kapnak, akkor lehet, hogy jobb eredményekhez vezethet a szerverre indított DB2 kapcsolatok számának emelése. A kapcsolatok maximális számát a DB2 adatbázis beállításai szabják meg. Miközben a megadható kapcsolatok számát a szerver nem korlátozza, a kapcsolatok erőforrásokat fogyasztanak.

- Adja meg az **Adatbáziskapcsolatok száma replikációhoz** értékét. Ezzel állítható be a szerveren replikációhoz használt DB2 kapcsolatok száma. A minimális megadandó érték 1, az alapértelmezett beállítás 4.

Megjegyzés: A megadott adatbáziskapcsolatok teljes száma a replikációhoz beállított kapcsolatokkal együtt nem haladhatja meg azt a számot, amely a DB2 adatbázisban meg van adva.

- A következő ACL gyorsítótári beállítások használatához válassza ki az **ACL információk gyorsítótárazása** lehetőséget.
- Adja meg az **ACL gyorsítótárban található elemek maximális száma** értékét. Az alapértelmezett érték 25 000.
- Adja meg a **Bejegyzés-gyorsítótárban található elemek maximális száma** értékét. Az alapértelmezett érték 25 000.
- Adja meg az **Keresési szűrő gyorsítótárban található elemek maximális száma** értékét. Az alapértelmezett érték 25 000. A keresési szűrő gyorsítótár a kért attribútumszűrők aktuális lekérdezéseit, valamint az eredményül kapott megfelelő azonosítókat tartalmazza. Egy frissítési műveletnél minden szűrő gyorsítótári bejegyzés érvénytelenítésre kerül.
- Adja meg az **Elemek maximális száma egyetlen, a keresési szűrő gyorsítótárhoz hozzáadott keresésnél** értéket. Ha az **Elemek** lehetőséget választja, meg kell adnia egy számot. Az alapértelmezett érték 100. A másik választási lehetőség a **Korlátlan**. Az itt megadottnál több bejegyzésnek megfelelő keresési bejegyzések nem kerülnek hozzáadásra a keresési szűrő gyorsítótárhoz.
- Ha kész, kattintson az **OK** gombra.
- Ha beállította az adatbáziskapcsolatok számát, akkor a szervert újra kell indítani ahhoz, hogy a változások életbe lépjenek. Ha csak a gyorsítótári beállításokat módosította, akkor a szervert nem kell újraindítani.

Attribútum-gyorsítótár beállítása

Az attribútum-gyorsítótár beállításai a webes adminisztrációs eszközben és az iSeries Navigatorban is megadhatók.

Az attribútum-gyorsítótár kézi beállításához a webes adminisztrációs eszközből tegye a következőket:

- Bontsa ki a **Szerveradminisztráció** kategóriát a webes adminisztrációs eszköz navigációs területén, majd válassza a jobboldali ablakrész **Attribútum-gyorsítótár** lapját.

Megjegyzés: A szerver konfigurációs beállításainak módosításához a webadminisztrációs eszköz Szerveradminisztrációs kategóriájának használatával hitelesítenie kell magát a szerverhez egy i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultságokkal. Ez úgy történhet, hogy hitelesíti magát leképezett felhasználóként az adott profil jelszavával. A kapcsolódáshoz a webes adminisztrációs eszközhöz leképezett felhasználóként adjon meg egy felhasználónevet a következő formában: `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, ahol a MYUSERNAME és MYSYSTEM.COM karaktersorozatokat a saját felhasználói profiljának nevével és a beállított rendszerleképezési utótaggal helyettesíti.

- Módosítsa, hogy hány kilobyte memória álljon a címtár gyorsítótár rendelkezésére. Az alapértelmezett érték 16 384 kilobyte (16 MB).
- Módosítsa, hogy hány kilobyte memória álljon a változásnapló gyorsítótár rendelkezésére. Az alapértelmezett érték 16 384 kilobyte (16 MB).

Megjegyzés: Ez a választási lehetőség le van tiltva, ha a változásnapló nincs beállítva. A változásnaplók esetében az attribútum-gyorsítótárazást 0 értékre érdemes állítani és semmilyen attribútumot nem kell beállítani, hacsak nem keres sűrűn a változásnaplókban és ezeknek a kereséseknek nem kritikus a sebessége.

- Válassza ki azt az attribútumot a **Rendelkezésre álló attribútumok** menüből, amelyet gyorsítótárazni kíván. Csak az ebben a menüben megjelenő attribútumok gyorsítótárazhatók (pl.: sn).

Megjegyzés: Egy attribútum a rendelkezésre álló attribútumok listájában marad addig, amíg nem kerül elhelyezésre mind a `cn=directory` és `cn=changelog` tárolókban.

- Kattintson vagy a **Hozzáadás: cn=directory** vagy a **Hozzáadás: cn=changelog** lehetőségre. Az attribútum a megfelelő listájában jelenik meg. Ugyanazt az attribútumot mindkét tárolóban kilistázhatja.

Megjegyzés: A **Hozzáadás: cn=changelog** lehetőség nem engedélyezett, ha a változásnapló nincs beállítva. A változásnaplók esetében az attribútum-gyorsítárást 0 értékre érdemes állítani és semmilyen attribútumot nem kell beállítani, hacsak nem keres sűrűn a változásnaplókban és ezeknek a kereséseknek nem kritikus a sebessége.

6. Ismétlje meg ezt the műveletet minden attribútumnál, amelyet hozzá kíván adni az attribútum-gyorsítótárhoz.
7. Ha kész, kattintson az **OK** gombra.

Az automatikus attribútum-gyorsítótárazás engedélyezéséhez az iSeries Navigatorban tegye a következőket:

1. iSeries Navigatorban bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Properties** menüpontot.
5. Kattintson a **Teljesítmény** lapra.
6. Válassza ki az **Automatikus attribútum-gyorsítótárazás engedélyezése** lehetőséget vagy az **Adatbázis**, vagy a **Változásnapló**, esetleg mindkettő esetében. Az automatikus attribútum-gyorsítótárazást nem érdemes engedélyezni a változásnaplóhoz, hacsak nem keres gyakran a változásnaplóban, és ezeknek a kereséseknek a teljesítménye nem kritikus.
7. Adja meg a **Kezdési idő** (a szerver helyi idejében) és az **Időköz** értékét minden kiválasztott gyorsítótár-típushoz. Ha például engedélyezte az adatbázis-gyorsítótárazást, reggel 6 órára állította a kezdési időt és hatórára az időközöt, akkor a gyorsítótár automatikusan beállításra fog kerülni reggel hatkor, délben, délután hatkor és éjjelkor, függetlenül attól, hogy a szerver mikor került elindításra vagy hogy mikor konfigurálták be az automatikus beállítást.

Megjegyzés: Az automatikus attribútum-gyorsítótárazás a webes adminisztrációs eszközben gyorsítótárazáshoz megadott maximális memóriaméretig fogja betárazni az attribútumokat.

4. táblázat: Az attribútum-gyorsítótári beállítások interakciója

Tevékenység	Mi történik
Szerverindulás	Ha az automatikus attribútum-gyorsítótárazás pillanatnyilag engedélyezett és akkor is az volt, amikor a szerver utoljára leállt, akkor a leálláskor a gyorsítótárban található attribútumok létrejönnek a szerver újraindulásakor. Ha az attribútum-gyorsítótárazáshoz még további memória is rendelkezésre áll, akkor a kézzel beállított attribútumok is gyorsítótárba kerülnek. Ha az automatikus attribútum-gyorsítótárazás pillanatnyilag engedélyezett, de nem volt az, amikor a szerver utoljára leállt, akkor a gyorsítótárazáshoz kézzel beállított attribútumok kerülnek a gyorsítótárba. Bizonyos esetekben a szerver ezután automatikusan beállítja az attribútum-gyorsítótárazást a megadott kezdési idő és időköz alapján. Ha az automatikus gyorsítótárazás nincs engedélyezve, akkor a kézzel beállított gyorsítótári beállítások lépnek érvénybe.
Engedélyezett automatikus attribútum-gyorsítótárazás szerverindítás után	Az automatikus attribútum-gyorsítótárazás a szerverindításnál leírtak szerint fog történni. Minden olyan kézzel beállított attribútum-gyorsítótár, ami nem fér bele az attribútum-gyorsítótárazáshoz beállított memóriába, törlésre kerül.
Letiltott automatikus attribútum-gyorsítótárazás szerverindítás után	Csak a kézzel beállított attribútumok kerülnek gyorsítótárba.
A kézzel beállított gyorsítótárba kerülő attribútumok módosítása szerverindításkor engedélyezett automatikus gyorsítótárazásnál	Semmi sem fog történni. A kézi beállítás csak akkor fog érvénybe lépni, ha az automatikus gyorsítótárazás ki van kapcsolva.
A gyorsítótárazásra rendelkezésre álló memória mennyiségének módosítása szerverindítás után	Ha az automatikus gyorsítótárazás engedélyezve van, akkor a szerver az új méret alapján azonnal újra elvégzi a gyorsítótár feltöltését. Ha az automatikus gyorsítótárazás le van tiltva, akkor a szerver a kézzel beállított attribútumokat fogja gyorsítótárba helyezni az új méretig.

4. táblázat: Az attribútum-gyorsítótári beállítások interakciója (Folytatás)

Tevékenység	Mi történik
A kezdési idő vagy az időköz módosítása szerverindítás után	Ha az automatikus gyorsítótárazás engedélyezve van, akkor az új beállítások a megadott kezdési időpont vagy időköz leteltékor érvénybe lépnek. Ha az automatikus gyorsítótárazás le van tiltva, akkor a beállítások tárolásra kerülnek és az automatikus gyorsítótárazás engedélyezésekor lépnek hatályba.

Tranzakciós beállítások megadása

Tranzakciós beállítások megadásához tegye a következőket:

1. Bontsa ki a **Szervertulajdonságok kezelése** kategóriát a webes adminisztrációs eszköz navigációs területén, majd válassza a jobboldali ablakrész **Tranzakciók** lapját.
2. A tranzakciókezelés engedélyezéséhez válassza ki a **Tranzakciókezelés engedélyezése** jelölőnégyzetet. Ha a **Tranzakciókezelés engedélyezése** ki van kapcsolva, akkor a panel többi beállítását a szerver figyelmen kívül hagyja.
3. Állítsa be a **Tranzakciók maximális száma** értéket. Kattintson vagy a **Tranzakciók** vagy a **Korlátlan** választógombra. Ha a **Tranzakciók** lehetőséget választotta, akkor adja meg a tranzakciók maximális számát. A tranzakciók maximális száma 2 147 483 647. Az alapértelmezett beállítás 20 tranzakció.
4. Állítsa be a **Tranzakciónkénti műveletek maximális száma** értéket. Kattintson vagy a **Műveletek** vagy a **Korlátlan** választógombra. Ha a **Műveletek** lehetőséget választotta, akkor adja meg az egyes tranzakciókhoz engedélyezett műveletek maximális számát. A műveletek maximális száma 2 147 483 647. Minél kisebb a szám, annál jobb a teljesítmény. A műveletek alapértelmezett száma 5.
5. Állítsa be a **Függőben lévő tranzakciók időkorlátja** értéket. Ez a kiválasztás a függőben lévő tranzakciók maximális időkorlát-értékét adja meg másodpercben. Kattintson vagy a **Másodpercek** vagy a **Korlátlan** választógombra. Ha a **Másodperc** lehetőséget választotta, akkor adja meg az egyes tranzakciókhoz engedélyezett időt másodpercben. A másodpercek maximális száma 2 147 483 647. Az ezután az idő után még mindig elvégzetlen tranzakciók befejezés nélkül maradnak (visszagörgetésre kerülnek). Az alapértelmezett érték 300 másodperc.
6. Ha kész, kattintson az **OK** gombra.
7. Ha engedélyezte a tranzakciók támogatását, akkor indítsa újra a szervert, hogy a változások életbe lépjenek. Ha csak ezeket a beállításokat módosította, akkor a szervert nem kell újraindítani.

Replikáció kezelése

A replikáció kezeléséhez bontsa ki a webes adminisztrációs eszköz **Replikáció kezelése** kategóriáját. A replikáció alapfogalmairól itt olvashat: “Replikáció” oldalszám: 36.

További információk:

- “Elsődleges és replikaserverekből álló topológia létrehozása” oldalszám: 132
- “Elsődleges és továbbító szerverekből álló topológia létrehozása” oldalszám: 137
- “Összetett replikációs topológia készítésének áttekintése” oldalszám: 138
- “Összetett topológia létrehozása egyenrangú replikációval” oldalszám: 139
- “Átjárótopológia beállítása” oldalszám: 141
- “Topológiák kezelése” oldalszám: 143
- “Replikációs tulajdonságok módosítása” oldalszám: 146
- “Replikációs ütemezések létrehozása” oldalszám: 147
- “Sorok kezelése” oldalszám: 149
- “Replikáció beállítása biztonság kapcsolatán keresztül” oldalszám: 149

Elsődleges és replikaszerverekből álló topológia létrehozása

Egy elsődleges és replikaszerverekből álló topológia létrehozása az alábbi lépésekből áll:

1. Egy elsődleges szerver létrehozása és tartalmának megadása. Válassza ki a replikálni kívánt részfát, majd adja meg, hogy melyik szerver az elsődleges. Részletek: “Elsődleges szerver (replikált részfa) létrehozása”.
2. Hozza létre az ellátó által használt hitelesítési adatokat. Részletek: “Hitelesítési adatok létrehozása” oldalszám: 133.
3. Hozzon létre egy replikaszervert. Részletek: “Replikaszerver létrehozása” oldalszám: 135.
4. Exportálja a topológiát az elsődleges szerverről a replikára. Részletek: “Adatok másolása a replikába” oldalszám: 136.
5. Módosítsa a replika konfigurációját és adja meg, ki jogosult replikálni a változásait. Adjon meg továbbá egy utalást az elsődleges szerverre. Részletek: “Ellátó információk felvétele a replikaszerveren” oldalszám: 136.

Megjegyzés:

Ha a replikálni kívánt részfa gyökérobjektuma nem a szerver egyik utótagja, akkor a **Részfa hozzáadása** funkció használatához előbb biztosítani kell, hogy annak ACL-jei is meg legyenek adva:

Nem szűrt ACL-ek esetén:

```
ownsource: <a bejegyzés DN-jével megegyező>  
ownerpropagate: TRUE
```

```
aclsource: <a bejegyzés DN-jével megegyező>  
aclpropagate: TRUE
```

Szűrt ACL-ek esetén:

```
ibm-filteraclinherit: FALSE
```

Az ACL követelmények teljesítéséhez, ha a bejegyzés nem utótag a szerveren, akkor módosítsa a bejegyzés ACL-jét a **Bejegyzések kezelése** ablakban. Válassza ki a bejegyzést, majd kattintson az **ACL módosítása** lehetőségre. Ha nem szűrt ACL-eket akar felvenni, akkor válassza ki azt a lapot és jelölje meg a négyzetet annak megadásához, hogy az ACL-ek explicitek vagy sem, az ACL-ekhez és a tulajdonosokhoz egyaránt. Győződjön meg róla, hogy az **ACL-ek továbbadása** és a **Tulajdonos továbbadása** négyzetek be vannak jelölve. Ha szűrt ACL-eket akar felvenni, akkor válassza ki azt a lapot és vegyen fel egy **cn=this** bejegyzést **access-id** szereppel az ACL-ekhez és a tulajdonosokhoz egyaránt. Győződjön meg róla, hogy a **Szűrt ACL-ek gyűjtése** nincs megjelölve, a **Tulajdonos továbbadása** viszont igen. További információk: “Hozzáférés-felügyeleti listák (ACL-ek) kezelése” oldalszám: 185.

Kezdetben a folyamat által létrehozott **ibm-replicagroup** objektum megörökli a replikált részfa gyökér bejegyzésnek ACL-jét. Ezek az ACL-ek nem feltétlenül alkalmasak a címtár replikációs információinak hozzáférés-vezérléséhez.

Elsődleges szerver (replikált részfa) létrehozása

Megjegyzés: E feladat végrehajtásához a szervernek futnia kell.

E feladat megjelöl egy bejegyzést egy függetlenül replikált részfa gyökereként és létrehoz egy, a szervert a részfa egyetlen elsődleges szervereként reprezentáló **ibm-replicasubentry** bejegyzést. A replikált részfa létrehozásához meg kell adni a részfát, amelyet a szerver replikálni fog.

Bontsa ki a navigációs terület Replikációkezelés kategóriáját, majd kattintson a **Topológia kezelése** lehetőségre.

1. Kattintson a **Részfa hozzáadása** lehetőségre.
2. Írja be a replikálni kívánt részfa gyökerének DN-jét, vagy kattintson a **Tallózás** lehetőségre a részfa gyökereként megjelölt bejegyzés kiválasztásához.
3. Az elsődleges szerver utalási URL-je LDAP URL-ként jelenik meg, például:
`ldap://<myservername>.<mylocation>.<mycompany>.com`

Megjegyzés: Az elsődleges szerver utalási URL megadása nem kötelező. Csak a következő esetekben van rá szükség:

- Ha a szerver csak olvasható részfákat tartalmaz (vagy fog tartalmazni).
- Egy olyan utalási URL megadásához, amely visszaadásra kerül a szerver bármelyik csak olvasható részfájának frissítése esetén.

4. Kattintson az **OK** gombra.

5. Az új szerver megjelenik a Topológia kezelése ablakban, a **Replikált részfák** címsor alatt.

Hitelesítési adatok létrehozása

Bontsa ki a navigációs terület Replikációkezelés kategóriáját, majd kattintson a **Hitelesítési adatok kezelése** lehetőségre.

1. Válassza ki a helyet a részfák listájából, ahol a hitelesítési adatokat tárolni kívánja. A webes adminisztrációs eszköz az alábbi helyeken teszi lehetővé a hitelesítési adatok tárolását:

- **cn=replication,cn=localhost**, amely esetben a hitelesítési adatok csak az adott szerveren maradnak.

Megjegyzés: A legtöbb replikációs esetben célszerű a hitelesítési adatokat a **cn=replication,cn=localhost** helyen tárolni, mivel nagyobb biztonságot kínál, mint a részfában található, replikált hitelesítési adatok. Bizonyos esetekben azonban a hitelesítési adatok nem tehetők a **cn=replication,cn=localhost** helyre.

Ha egy replikát vesz fel egy szerverre (mondjuk serverA) és egy másik szerverre (serverB) csatlakozik a webes adminisztrációs eszközzel, akkor a **Hitelesítési adatok kiválasztása** mezőben nem jelenik meg a **cn=replication,cn=localhost** lehetőség. Ez azért van így, mert nem olvasható ki és nem frissíthető a serverA semmilyen **cn=localhost** alatti adata a serverB szerverre csatlakozás közben.

A **cn=replication,cn=localhost** lehetőség csak akkor áll rendelkezésre, ha a szerver (amelyikre éppen replikát próbál felvenni) ugyanaz a szerver, mint amelyikre a webes adminisztrációs eszközzel csatlakozik.

- A replikált részfán belül, amely esetben a hitelesítési adatok a részfa maradékával együtt kerülnek replikálásra. A replikált részfában tárolt hitelesítési adatok az adott részfa **ibm-replicagroup=default** bejegyzése alatt kerülnek létrehozásra.

Megjegyzés: Ha egyetlen részfa sem jelenik meg, akkor az “Elsődleges szerver (replikált részfa) létrehozása” oldalszám: 132 rész tartalmazza a replikálni kívánt részfa létrehozásával kapcsolatos utasításokat.

2. Kattintson a **Hozzáadás** gombra.

3. Írja be a létrehozni kívánt hitelesítési adatok nevét, például **mycreds**. A rendszer előre kitölti a mezőben a **cn=** értéket.

4. Adja meg a használni kívánt hitelesítési módszert, majd kattintson a **Tovább** gombra.

- Ha egyszerű csatlakozásos hitelesítést választott:
 - a. Írja be a szerver által a replikához kapcsolódáshoz használt DN-t. Például: **cn=akarmi**
 - b. Írja be a szerver által a replikához kapcsolódáshoz használt jelszót. Például: **titok**.
 - c. A hibák elkerülése érdekében megerősítésként írja be még egyszer a jelszót.
 - d. Ha akarja, megadhat egy rövid leírást a hitelesítési adatok mellé.
 - e. Kattintson a **Befejezés** gombra.

Megjegyzés: Érdemes lehet biztonságos helyen rögzíteni a hitelesítési adatokhoz tartozó kapcsolódási DN-t és jelszót. A jelszóra szükség lesz a replikációs megállapodás létrehozásakor.

- Ha Kerberos alapú hitelesítést választott:
 - a. Adja meg a Kerberos kapcsolódási DN-t.
 - b. Adja meg a kulcslap fájl nevét.

- c. Ha akarja, megadhat egy rövid leírást a hitelesítési adatok mellé. Egyéb információkra nincs szükség. További információk: “Kerberos hitelesítés engedélyezése a Directory Server-hez” oldalszám: 156.
- d. Kattintson a **Befejezés** gombra.

A **Kerberos hitelesítési adatok hozzáadása** panel vesz egy választható kapcsolati DN-t `ibm-kn=felhasználó@tartomány` formában, valamint egy választható (kulcsfájlként hivatkozott) kulcscímké fájlnevet. Ha van megadva kapcsolati DN, akkor a szerver a megadott hitelesítési adat nevét használja a fogyasztó szerver hitelesítésére. Ha nincs, akkor a szerver Kerberos szolgáltatásneve (`ldap/host-name@realm`) kerül használatra. Ha van használatban lévő kulcscímké fájl, akkor a szerver ezt használja a hitelesítési adatok lekérdezésére a megadott azonosítónévhez. Ha nincs megadott kulcscímké fájl, akkor a szerver a Kerberos konfigurációjában megadott kulcscímké fájlt használja. Ha egynél több ellátó működik, akkor meg kell adni az azonosítót és kulcscímkét, amelyet az összes ellátó használ.

Azon a szerveren, amelyiken létrehozta a hitelesítési adatokat:

- a. Bontsa ki a **Címtárkezelés** kategóriát, majd kattintson a **Bejegyzések kezelése** menüpontra.
- b. Válassza ki a részfát, ahol a hitelesítési adatokat tárolta (például **cn=localhost**), majd kattintson a **Kibontás** menüpontra.
- c. Válassza ki a **cn=replication** elemet, majd kattintson a **Kibontás** menüpontra.
- d. Válassza ki a Kerberos hitelesítési adatokat (`ibm-replicationCredentialsKerberos`), majd kattintson az **Attribútumok módosítása** lehetőségre.
- e. Kattintson az **Egyéb attribútumok** lapra.
- f. Írja be a **replicaBindDN** attribútum értékét (például **ibm-kn=myprincipal@SOME.REALM**).
- g. Írja be a **replicaCredentials** attribútum értékét. Ez a **myprincipal** azonosítóhoz használt kulcscímké fájlnev.

Megjegyzés: Ez az azonosító és jelszó meg kell, hogy egyezzen azokkal, amelyek segítségével a **kinit** programot futtatta a paranassorból.

A replikán

- a. Kattintson a navigációs terület **Replikációs tulajdonságok kezelése** kategóriájára.
 - b. Válasszon ki az **Ellátó információk** legördülő menüből egy ellátót, vagy írja be annak a replikált részfának a nevét, amelyhez be kívánja állítani az ellátó hitelesítési adatait.
 - c. Kattintson a **Módosítás** gombra.
 - d. Adja meg a replikációs bindDN-t. Ez a jelen példában **ibm-kn=myprincipal@SOME.REALM**).
 - e. Írja be és erősítse meg a **Replikációs kapcsolódási jelszót**. Ez a **myprincipal** azonosítóhoz használt KDC jelszó.
- Ha SSL használatát választotta igazolással hitelesítéssel és a szerver igazolását használja, akkor nem kell megadnia további információkat. Ha nem a szerver igazolását használja:
 - a. Adja meg a kulcsfájl nevét.
 - b. Adja meg a kulcsfájl jelszavát.
 - c. Írja be újra a kulcsfájl jelszavát megerősítésként.
 - d. Írja be a kulcs címkéjét.
 - e. Ha akarja, megadhat egy rövid leírást.
 - f. Kattintson a **Befejezés** gombra.

További információk: “SSL és TSL engedélyezése a Directory Serveren” oldalszám: 154.

5. Azon a szerveren, amelyen létrehozta a hitelesítési adatokat, állítsa be a Szerver biztonsági információk megtartása (QRETSVRSEC) rendszerváltozó értékét 1-re (adatok megtartása). Mivel a replikációs hitelesítési adatok egy ellenőrzési listában tárolódnak, a szerver le tudja kérni a hitelesítési adatokat az ellenőrzési listából, amikor a replikához kapcsolódik.

Replikaszerver létrehozása

Megjegyzés: E feladat végrehajtásához a szervernek futnia kell.

Bontsa ki a navigációs terület **Replikációkezelés** kategóriáját, majd kattintson a **Topológia kezelése** lehetőségre.

1. Válassza ki a replikálni kívánt részfát, majd kattintson a **Topológia megjelenítése** lehetőségre.
2. Kattintson a **Replikációs topológia** kijelölés melletti nyílra az ellátó szerverek listájának kibontásához.
3. Válassza ki az ellátó szerveret, majd kattintson a **Replika hozzáadása** lehetőségre.

A **Replika hozzáadása** ablak **Szerver** lapján:

- Írja be a létrehozandó replika hosztnevét és portszámát. Az alapértelmezett port a 389 nem SSL és 636 SSL kapcsolatok esetén. Ezek kötelező mezők.
- Állítsa be, hogy engedélyezi-e az SSL alapú kommunikációt.
- Írja be a replika nevét, vagy hagyja üresen (ekkor a hosztnevet használja a rendszer).
- Írja be a replika azonosítóját. Ha a szerver, amelyen a replikát éppen létrehozza, már fut, akkor kattintson a **Replikaazonosító lekérése** lehetőségre a mező automatikus kitöltéséhez. Ez egy kötelező mező, ha a felvenni kívánt szerver egyenrangú vagy továbbító szerver lesz. Célszerű minden szerveren ugyanazt a kiadást futtatni.
- Adja meg a replikaszerver leírását.

A **Kiegészítések** lapon:

1. Adja meg a hitelesítési adatokat, amelyek segítségével a replika kommunikál az elsődleges szerverrel.

Megjegyzés: A webes adminisztrációs eszköz az alábbi helyeken teszi lehetővé a hitelesítési adatok tárolását:

- **cn=replication,cn=localhost**, amely esetben a hitelesítési adatok csak az őket használó szerveren maradnak.
- A replikált részfán belül, amely esetben a hitelesítési adatok a részfa maradékával együtt kerülnek replikálásra. A replikált részfában tárolt hitelesítési adatok az adott részfa **ibm-replicagroup=default** bejegyzése alatt kerülnek létrehozásra.

A hitelesítési adatok a **cn=replication,cn=localhost** alatti elhelyezése biztonságosabb megoldás.

- a. Kattintson a **Kiválasztás** lehetőségre.
- b. Válassza ki a hitelesítési adatok helyét. Célszerűen ez a **cn=replication,cn=localhost** legyen.
- c. Kattintson a **Hitelesítési adatok megjelenítése** lehetőségre.
- d. Bontsa ki a hitelesítési adatok listáját és válassza ki a használni kívántakat.
- e. Kattintson az **OK** gombra.

További információk a megállapodás hitelesítési adataival kapcsolatban: "Hitelesítési adatok létrehozása" oldalszám: 133.

2. Válasszon ki egy replikációs ütemezést legördülő listából, vagy hozzon létre egyet a **Hozzáadás** gomb megnyomásával. Részletek: "Replikációs ütemezések létrehozása" oldalszám: 147.
3. Az ellátó funkcióinak listájában kikapcsolhat bármilyen olyan funkciót, amelyet nem kíván replikálni a fogyasztó felé.

Ha a szerveren különböző kiadású szerverek futnak, akkor az újabb kiadások egyes funkciói el sem érhetők a régebbi kiadásokon. Bizonyos funkciók, például az ACL-ek szűrése és a jelszó-irányelvek más változások miatt replikált műveleti attribútumokat használnak. A legtöbb esetben az a legjobb, ha minden szerver támogatja a használt funkciókat. Ha nem mindegyik szerver támogatja a funkciót, akkor érdemesebb nem is használni. Nem hasznos például különböző ACL-eket használni a különböző szervereken. Ugyanakkor előfordulhatnak esetek, amikor egyes funkciókat ki akar használni az azt támogató szervereken, a többin pedig nem. Ilyen esetekben a funkciólistában jelölheti meg a replikálni nem kívánt funkciókat.

4. Kattintson az **OK** gombra a replika létrehozásához.
5. Megjelenik egy üzenet, hogy további teendőkre is szükség van még. Kattintson az **OK** gombra.

Megjegyzés: Ha további szervereket is felvesz, vagy egy összetett topológiát alakít ki, akkor előbb fejezze be a topológia megadását az elsődleges szerveren, és csak utána folytassa a következő résszel: “Adatok másolása a replikába” vagy “Ellátó információk felvétele a replikaszerveren”. A topológia elkészítése után létrehozott *masterfile.ldif* fájl tartalmazza az elsődleges szerver címtárbejegyzéseit és a topológiai megállapodások teljes másolatát. A fájlt a többi szerver mindegyikén betöltve, minden szerver ugyanazokkal az információkkal fog rendelkezni.

Adatok másolása a replikába

A replika létrehozása után exportálnia kell a topológiát az elsődleges szerverről a replikára.

1. Az elsődleges szerveren hozzon létre egy LDIF fájlt az adatoknak. Az elsődleges szerver összes adatának átmásolása:
 - a. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
 - b. Bontsa ki a **Szerverek** elemet.
 - c. Kattintson a **TCP/IP** pontra.
 - d. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** lehetőségre, majd válassza az előugró menü **Eszközök**, majd a **Fájl exportálása** menüpontját.
 - e. Adja meg a kimeneti LDIF fájl nevét (például *masterfile.ldif*), opcionálisan megadhat egy exportálandó részfát (például *subtreeDN*). Ezután kattintson az **OK** gombra.
2. A gépen, amelyen létre kívánja hozni a replikát, hajtja végre az alábbiakat:
 - a. Győződjön meg róla, hogy a replikált utótagok valóban meg vannak adva a replikaszerver konfigurációjában.
 - b. Állítsa le a replikaszervert.
 - c. Másolja át az LDIF fájlt a replikaszerverre, majd tegye a következőket:
 - 1) Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
 - 2) Bontsa ki a **Szerverek** elemet.
 - 3) Kattintson a **TCP/IP** pontra.
 - 4) Kattintson a jobb oldali egérgombbal a **IBM Directory Server** lehetőségre, majd válassza az előugró menü **Eszközök**, majd a **Fájl importálása** menüpontját.
 - 5) Adja meg a bemeneti LDIF fájl nevét (például *masterfile.ldif*), opcionálisan adja meg, hogy replikálni kívánja-e az adatokat, majd kattintson az **OK** gombra.

A replikációs megállapodások, az ütemezések és a hitelesítési adatok (már amennyiben a replikált részében tárolódnak) betöltésre kerülnek a replikaszerveren.

- d. Indítsa el a szervert.

Ellátó információk felvétele a replikaszerveren

Módosítania kell a replika konfigurációját és meg kell adnia, ki jogosult replikálni a változásait. Meg kell továbbá adnia egy utalást az elsődleges szerverre.

A gépen, amelyen létre kívánja hozni a replikát:

1. Bontsa ki a navigációs terület **Replikációkezelés** kategóriáját, majd kattintson a **Replikációs tulajdonságok kezelése** lehetőségre.

Megjegyzés: Ahhoz, hogy a **Replikációtulajdonságok kezelése** panelekben módosíthassa a beállításokat, *ALLOBJ és *IOSYSCFG különleges jogosultságokkal rendelkező leképezett OS/400 felhasználóként kell bejelentkeznie a webes adminisztrációs eszközbe.

2. Kattintson a **Hozzáadás** gombra.
3. Válasszon ki a **Replikált részfa** legördülő menüből egy ellátót, vagy írja be annak a replikált részfának a nevét, amelyhez be kívánja állítani az ellátó hitelesítési adatait. Ha módosítja az ellátó hitelesítési adatait, akkor ez a mező nem szerkeszthető.
4. Adja meg a replikációs bindDN-t. Ez a jelen példában *cn=akarmi*.

Megjegyzés: A két lehetőség bármelyikét használhatja a helyzettől függően.

- Állítsa be a replikáció kapcsolódási DN-jét (és jelszavát), valamint egy alapértelmezett utalást a szerver összes replikált részfájához az "alapértelmezett hitelesítési adatok és utalás" lehetőséggel. Ezt akkor lehet használni, ha az összes részfa ugyanarról az ellátóról replikálódik.
 - Adja meg a replikáció kapcsolódási DN-jét (és jelszavát) külön minden egyes replikált részfához: vegye fel az ellátó információit minden egyes részfához. Ezt akkor kell használni, ha az egyes részfák ellátója eltér (vagyis minden részfához más elsődleges szerver tartozik).
5. A hitelesítési adatok típusától függően írja be és erősítse meg a hitelesítési adatok jelszavát. (Ez az, amit korábban felírt.)
- **Egyszerű kapcsolódás** - Adja meg a DN-t és a jelszót
 - **Kerberos** - Ha az ellátó hitelesítési adatai nem azonosítják az azonosítót és jelszót, vagyis a szerver saját szolgáltatási hitelesítési adatait használja, akkor a kapcsolódási DN az `ibm-kn=ldap/<sajátservernév@sajáttartomány>`. Ha a hitelesítési adatokban az azonosító neve `<azonosító@tartomány>` formátumú, akkor ezt használja DN-ként. Jelszóra egyik esetben sincs szükség.
 - **SSL külső csatlakozással** - Adja meg az igazolás alany DN-jét, jelszóra nincs szükség
- Részletek: "Hitelesítési adatok létrehozása" oldalszám: 133.
6. Kattintson az **OK** gombra.
7. A replikaszervert újra kell indítani a változtatások érvénybe léptetéséhez.
- További információk: "Replikációs tulajdonságok módosítása" oldalszám: 146.

A replika felfüggesztett állapotban van és nem történik replikáció. A replikációs topológia beállításának befejezése után kattintson a **Sorok kezelése** lehetőségre, válassza ki a replikát, majd kattintson a **Felfüggesztés/visszaállítás** gombra a replikáció elindításához. További információk: "Sorok kezelése" oldalszám: 149. A replika most már fogadja a frissítéseket az elsődleges szervertől.

Elsődleges és továbbító szerverekből álló topológia létrehozása

Egy elsődleges és továbbító szerverekből álló topológia létrehozása az alábbi lépésekből áll:

1. Egy elsődleges és egy replikaszerver létrehozása. Részletek: "Elsődleges és replikaszerverekből álló topológia létrehozása" oldalszám: 132.
2. Hozzon létre egy új replikaszervert az eredeti replikához. Részletek: "Új replikaszerver létrehozása".
3. Másolja át az adatokat a replikákba. Részletek: "Adatok másolása a replikába" oldalszám: 136.

Új replikaszerver létrehozása

Ha már beállított egy replikációs topológiát (részletek: "Elsődleges szerver (replikált részfa) létrehozása" oldalszám: 132) egy elsődleges (server1) és egy replikaszerverrel (server2), akkor módosíthatja server2 szerepét, hogy továbbító szerver legyen. Ehhez azonban egy újabb replikát kell (server3) létrehozni server2 alatt.

1. Kapcsolódjon a webes adminisztrációs eszközzel az elsődleges szerverhez (server1)
2. Bontsa ki a navigációs terület Replikációkezelés kategóriáját, majd kattintson a **Topológia kezelése** lehetőségre.
3. Válassza ki a replikálni kívánt részfát, majd kattintson a **Topológia megjelenítése** lehetőségre.
4. Kattintson a **Replikációs topológia** kijelölés melletti nyílra az ellátó szerverek listájának kibontásához.
5. Kattintson a **server1** kijelölés melletti nyílra a szerverek listájának kibontásához.
6. Válassza ki a server2 szervert, majd kattintson a **Replika hozzáadása** lehetőségre.
7. A **Replika hozzáadása** ablak **Szerver** lapján:
 - Írja be a létrehozandó replika (server3) hosztnevét és portszámát. Az alapértelmezett port a 389 nem SSL és 636 SSL kapcsolatok esetén. Ezek kötelező mezők.
 - Állítsa be, hogy engedélyezi-e az SSL alapú kommunikációt.
 - Írja be a replika nevét, vagy hagyja üresen (ekkor a hosztnevet használja a rendszer).
 - Írja be a replika azonosítóját. Ha a szerver, amelyen a replikát éppen létrehozza, már fut, akkor kattintson a **Replikaazonosító lekérése** lehetőségre a mező automatikus kitöltéséhez. Ez egy kötelező mező, ha a felvenni kívánt szerver egyenrangú vagy továbbító szerver lesz. Célszerű minden szerveren ugyanazt a kiadást futtatni.

- Adja meg a replikaszerver leírását.

A **Kiegészítések** lapon:

- a. Adja meg a hitelesítési adatokat, amelyek segítségével a replika kommunikál az elsődleges szerverrel.

Megjegyzés: A webes adminisztrációs eszköz két helyen teszi lehetővé a hitelesítési adatok tárolását:

- **cn=replication,cn=localhost**, amely esetben a hitelesítési adatok csak az őket használó szerveren maradnak.
- A replikált részfán belül, amely esetben a hitelesítési adatok a részfa maradékával együtt kerülnek replikálásra.

A hitelesítési adatok a **cn=replication,cn=localhost** alatti elhelyezése biztonságosabb megoldás. A replikált részfában tárolt hitelesítési adatok az adott részfa **ibm-replicagroup=default** bejegyzése alatt kerülnek létrehozásra.

- 1) Kattintson a **Kiválasztás** lehetőségre.
- 2) Válassza ki a hitelesítési adatok helyét. Célszerűen ez a **cn=replication,cn=localhost** legyen.
- 3) Kattintson a **Hitelesítési adatok megjelenítése** lehetőségre.
- 4) Bontsa ki a hitelesítési adatok listáját és válassza ki a használni kívántakat.
- 5) Kattintson az **OK** gombra.

További információk a megállapodás hitelesítési adataival kapcsolatban: "Hitelesítési adatok létrehozása" oldalszám: 133.

- b. Válasszon ki egy replikációs ütemezést legördülő listából, vagy hozzon létre egyet a **Hozzáadás** gomb megnyomásával. Részletek: "Replikációs ütemezések létrehozása" oldalszám: 147.
- c. Az ellátó funkcióinak listájában kikapcsolhat bármilyen olyan funkciót, amelyet nem kíván replikálni a fogyasztó felé.

Ha a szerveren különböző kiadású szerverek futnak, akkor az újabb kiadások egyes funkciói el sem érhetők a régebbi kiadásokon. Bizonyos funkciók, például az ACL-ek szűrése és a jelszó-irányelvek más változások miatt replikált műveleti attribútumokat használnak. A legtöbb esetben az a legjobb, ha minden szerver támogatja a használt funkciókat. Ha nem mindegyik szerver támogatja a funkciót, akkor érdemesebb nem is használni. Nem hasznos például különböző ACL-eket használni a különböző szervereken. Ugyanakkor előfordulhatnak esetek, amikor egyes funkciókat ki akar használni az azt támogató szervereken, a többin pedig nem. Ilyen esetekben a funkciólistában jelölheti meg a replikálni nem kívánt funkciókat.

- d. Kattintson az **OK** gombra a replika létrehozásához.

8. Másolja át az adatokat a server2 szerverről az új replikára (server3). Ezzel kapcsolatban további információk: "Adatok másolása a replikába" oldalszám: 136.
9. Vegyen fel egy ellátó megállapodást a server3 szerverre, amelynek értelmében server2 a server3 szerver ellátója, server3 pedig server2 fogyasztója. Ezzel kapcsolatban további információk: "Ellátó információk felvétele a replikaszerveren" oldalszám: 136.

A szerverek szerepeit ikonok jelzik a webes adminisztrációs eszközben. A topológia most így néz ki:

- server1 (elsődleges)
 - server2 (továbbító)
 - server3 (replika)

Összetett replikációs topológia készítésének áttekintése

Összetett replikációs topológia kialakításához használja az alábbi áttekintést.

1. Indítson el minden egyenrangú szervert és leendő replikát. Ez azért szükséges, hogy a webes adminisztrációs eszköz információkat gyűjthessen a szerverekről.
2. Indítsa el az "első" elsődleges szervert, majd állítsa be, mint a kontextus elsődleges szerverét.
3. Ha még nincsenek betöltve, töltsse be a "első" elsődleges szerverről replikált részfa adatait.
4. Válassza ki a replikálandó részfát.

5. Vegye fel az összes leendő egyenrangú szervert az "első" elsődleges szerver replikájaként.
6. Vegye fel a többi replikát is.
7. Léptesse elő a többi egyenrangú elsődleges szervert.
8. Vegye fel a többi egyenrangú elsődleges szerverre a replikákra vonatkozó replikációs megállapodásokat.

Megjegyzés: Ha a hitelesítési adatok a **cn=replication,cn=localhost** bejegyzés alatt kerülnek létrehozásra, akkor a hitelesítési adatokat létre kell hozni mindegyik szerveren újraindításuk után. Az egyenrangú szerverek replikációja sikertelen, ha nincsenek létrehozva a hitelesítési objektumok.

9. Vegye fel a többi egyenrangú elsődleges szerverre az egyes egyenrangú elsődleges szerverekre vonatkozó replikációs megállapodásokat. Az "első" elsődleges szerveren már megvannak ezek az információk.
10. Zárolja a replikált részfát. Ez megakadályozza, hogy frissítések történjenek a szerverek közötti adatmásolás alatt.
11. Az egyes sorok a Sorkezelés kategória parancsaival hagyhatók ki.
12. Exportálja a replikált részfa adatait az "első" elsődleges szerverről.
13. Oldja fel a részfa zárolását.
14. Állítsa le a replikaszervert és importálja mindegyik replikán és egyenrangú elsődleges szerveren a replikált részfa adatait. Ezután indítsa újra a szervert.
15. Állítsa be a replikáció tulajdonságait mindegyik replikán és egyenrangú elsődleges szerveren: adja meg az ellátók által használt hitelesítési adatokat.

Összetett topológia létrehozása egyenrangú replikációval

Az egyenrangú replikáció egy olyan replikációs topológia, amelyben több szerver is elsődleges. Szemben a "multimaster" környezetekkel, az egyenrangú szerverek között nem történik ütközésfeloldás. Az LDAP szerverek elfogadják az egyenrangú szerverek által küldött frissítéseket és frissítik saját adataikat. Semmilyen megfontolás nem történik a frissítések fogadási sorrendjével vagy a többszörös frissítési konfliktusokkal kapcsolatban.

További elsődleges (egyenrangú) szerverek felvételéhez először a meglévő elsődleges szerverek csak olvasható replikájaként kell felvenni az újakat (részletek: "Replikaszerver létrehozása" oldalszám: 135), inicializálni kell a címtáradatokat, majd elő kell léptetni a szervert elsődlegessé (részletek: "Szerver áthelyezése vagy előléptetése" oldalszám: 144).

Kezdetben a folyamat által létrehozott **ibm-replicagroup** objektum megőröklí a replikált részfa gyökér bejegyzésnek ACL-jét. Ezek az ACL-ek nem feltétlenül alkalmasak a címtár replikációs információinak hozzáférés-vezérléséhez.

Ahhoz, hogy a Részfa hozzáadása művelet sikeres legyen, a felvett bejegyzés DN-jének - ha nem a szerver egyik utótagja - helyes ACL-ekkel kell rendelkeznie.

Nem szűrt ACL-ek esetén:

- ownersource : <a bejegyzés DN-je>
- ownerpropagate : TRUE
- aclsource : <a bejegyzés DN-je>
- aclpropagate: TRUE

Szűrt ACL-ek esetén:

- ownersource : <a bejegyzés DN-je>
- ownerpropagate : TRUE
- ibm-filteraclinherit : FALSE
- ibm-filteraclentry : <tetszés szerinti érték>

Az újonnan létrehozott replikált részfához társított replikációs információk ACL-jeinek beállításához használja a webes adminisztrációs eszköz **ACL-ek módosítása** funkcióját (részletek: "Hozzáférés-felügyeleti listák módosítása" oldalszám: 146).

A replika felfüggesztett állapotban van és nem történik replikáció. A replikációs topológia beállításának befejezése után kattintson a **Sorok kezelése** lehetőségre, válassza ki a replikát, majd kattintson a **Felfüggesztés/visszaállítás** gombra a replikáció elindításához. További információk: “Sorok kezelése” oldalszám: 149. A replika most már fogadja a frissítéseket az elsődleges szervertől.

Az egyenrangú replikációt csak olyan környezetekben használja, amelyben a címtárfrissítések mintája jól ismert. A címtáron belül az egyes objektumok frissítése csak egy szerveren történjen. Ez azért fontos, nehogy előálljon az a helyzet, hogy az egyik szerver kitöröl egy objektumot, majd egy másik utána módosítja. Ilyenkor ugyanis előfordulhat, hogy egy egyenrangú szerver egy törlési parancsot kap, majd közvetlenül utána egy módosítást; ez pedig ütközést okoz.

Egy két egyenrangú-elsődleges és négy replikaszervertől álló egyenrangú-továbbító-replika topológia kialakítása az alábbi lépésekből áll:

1. Egy elsődleges és egy replikaszervert létrehozása. Részletek: “Elsődleges és replikaszervekből álló topológia létrehozása” oldalszám: 132.
2. Két további replikaszervert létrehozása az elsődleges szerverhez. Részletek: “Replikaszerver létrehozása” oldalszám: 135.
3. Két replika létrehozása az újonnan létrehozott replikaszervertől.
4. Az eredeti replikák előléptetése elsődlegessé. Részletek: “Szerver előléptetése egyenrangúvá”.

Megjegyzés: Az elsődlegessé előléptetni kívánt szervernek levélreplikának kell lennie, amely alatt nincsenek további replikák.

5. Az adatok átmásolása az elsődleges szerverről az új elsődleges és a replikaszervertre. Részletek: “Adatok másolása a replikába” oldalszám: 136.

Szerver előléptetése egyenrangúvá

Az “Elsődleges és továbbító szerverekből álló topológia létrehozása” oldalszám: 137 részben létrehozott továbbítási topológia használatával egy szerver előléptethető egyenrangú szerverre. Az alábbi példában a replikát (server3) léptetjük elő az elsődleges szerver (server1) egyenrangú társává.

1. Kapcsolódjon a webes adminisztrációs eszközzel az elsődleges szerverhez (server1).
2. Bontsa ki a navigációs terület Replikációkezelés kategóriáját, majd kattintson a **Topológia kezelése** lehetőségre.
3. Válassza ki a replikálni kívánt részét, majd kattintson a **Topológia megjelenítése** lehetőségre.
4. Kattintson a **Replikációs topológia** kijelölés melletti nyílra a szerverek listájának kibontásához.
5. Kattintson a **server1** kijelölés melletti nyílra a szerverek listájának kibontásához.
6. Kattintson a **server2** kijelölés melletti nyílra a szerverek listájának kibontásához.
7. Kattintson a **server1** elemre, majd kattintson a **Replika hozzáadása** lehetőségre. Hozza létre a server4 nevű szervert. Részletek: “Replikaszerver létrehozása” oldalszám: 135. Ugyanezzel az eljárással hozza létre a server5 szervert. A szerverek szerepeit ikonok jelzik a webes adminisztrációs eszközben. A topológia most így néz ki:
 - server1 (elsődleges)
 - server2 (továbbító)
 - server3 (replika)
 - server4 (replika)
 - server5 (replika)
8. Kattintson a **server2** szerverre, majd kattintson a **Replika hozzáadása** lehetőségre a server6 szerver létrehozásához.
9. Kattintson a **server4** szerverre, majd kattintson a **Replika hozzáadása** lehetőségre a server7 szerver létrehozásához. Ugyanezzel az eljárással hozza létre a server8 szervert. A topológia most így néz ki:
 - server1 (elsődleges)
 - server2 (továbbító)
 - server3 (replika)

- server6 (replika)
- server4 (továbbító)
- server7 (replika)
- server8 (replika)
- server5 (replika)

10. Válassza ki a **server5** szervert, majd kattintson az **Áthelyezés** lehetőségre.

Megjegyzés: Az áthelyezni kívánt szervernek levélreplikának kell lennie, amely alatt nincsenek további replikák.

11. A replika elsődlegessé előléptetéséhez kattintson a **Replikációs topológia** lehetőségre. Kattintson az **Áthelyezés** gombra.
12. Megjelenik a **További ellátói megállapodások** ablak. Az egyenrangú replikációhoz az szükséges, hogy minden egyes elsődleges szerver ellátója és fogyasztója legyen a topológia összes többi elsődleges szerverének, valamint az első szintű replikáknak (server2 és server4). A server5 már server1 fogyasztója, úgyhogy most server1, server2 és server4 ellátójává kell tenni. Gondoskodjék róla, hogy az alábbi ellátói megállapodás négyzetek meg legyenek jelölve:

5. táblázat:

	Ellátó	Fogyasztó
✓	server5	server1
✓	server5	server2
✓	server5	server4

Kattintson a **Folytatás** gombra.

Megjegyzés: Egyes esetekben megjelenhet a Hitelesítési adatok kiválasztása ablak, és bekéri a `cn=replication,cn=localhost` helytől eltérő helyen tárolt hitelesítési adatokat. Ilyenkor meg kell adnia egy, a `cn=replication,cn=localhost` helytől eltérő helyen tárolt hitelesítési objektumot. Válassza ki a részfa által használt hitelesítési adatokat a meglévők közül, vagy adjon meg újakat. Részletek: "Hitelesítési adatok létrehozása" oldalszám: 133.

13. Kattintson az **OK** gombra. A topológia most így néz ki:

- server1 (elsődleges)
 - server2 (továbbító)
 - server3 (replika)
 - server6 (replika)
- server4 (továbbító)
 - server7 (replika)
 - server8 (replika)
- server5 (elsődleges)
- server5 (elsődleges)
 - server1 (elsődleges)
 - server2 (továbbító)
 - server4 (továbbító)

14. Másolja át az adatokat a server1 szerverről az összes többi szerverre. Ezzel kapcsolatban további információk: "Adatok másolása a replikába" oldalszám: 136.

Átjárótopológia beállítása

A replikációs topológia beállítása előtt készítsen biztonsági másolatot az eredeti `ibmslapd.conf` fájlról. Ez az eredeti beállítások visszaállítására használható, ha valami gond lenne a replikációval.

l Egy átjáró beállításához a(z) “Szerver előléptetése egyenrangúvá” oldalszám: 140 részben leírt összetett, társreplikációs topológia használatával tegye a következőket:

- l • Alakítson át egy meglévő társszervert (peer 1) átjárószerverre az 1. replikációs hely létrehozásához.
- l • Hozzon létre egy új replikációs szervert a 2. replikációs helyhez és egyeztesse a peer 1 szerverrel.
- l • Hozza létre a 2. replikációs hely topológiáját (ebben a példában nincs szemléltetve).
- l • Másolja át az adatokat az elsődleges szerverről a topológia összes többi gépére.

l **Alakítson át egy meglévő társszervert átjárószerverre**

- l 1. A webes adminisztrációs eszköz használatával lépjen be az elsődleges szerverre (server1).
- l 2. Bontsa ki a navigációs terület **Replikációkezelés** kategóriáját, majd kattintson a **Topológia kezelése** lehetőségre.
- l 3. Válassza ki a replikálni kívánt részfát, majd kattintson a **Topológia megjelenítése** lehetőségre.
- l 4. Kattintson a **Replikációs topológia** kijelölés melletti nyílra a szerverek listájának kibontásához.
- l 5. Egy meglévő szerver átjárószerverre alakításához válassza ki a **server1**-et vagy társát, a **server5**-öt. Ebben a példában használja a **server1**-et.
- l 6. Kattintson a **Szerverek módosítása** lehetőségre.
- l 7. Ellenőrizze, hogy az **Elsődleges szerver** jelölőnégyzet meg van jelölve, majd jelölje ki az **Átjárószerver** lehetőséget.
- l 8. Kattintson az **OK** gombra.

l **Megjegyzés:** Ha az átjáróként használni kívánt szerver már nem elsődleges, akkor annak egy levélreplikának kell lennie alárendelt replikák nélkül, amelyet először elsődlegesé kell előléptetni, és azután jelölhető meg átjárószerverként.

l **Hozzon létre egy átjárószervert és másolja az adatokat az elsődleges szerverről a topológia minden gépére.**

- l 1. Válassza ki a **server1**-et, majd kattintson a **Replika hozzáadása** lehetőségre.
- l 2. Hozza létre az új replikát, a **server9**-et. További információk a replikák létrehozásával, a hitelesítési adatok megadásával és az ellátói információkkal kapcsolatban: “Replikaszerver létrehozása” oldalszám: 135.
- l 3. Válassza ki a **server9** szervert, majd kattintson az **Áthelyezés** lehetőségre.
- l 4. A replika elsődlegessé előléptetéséhez kattintson a **Replikációs topológia** lehetőségre. Kattintson az **Áthelyezés** gombra.
- l 5. Megjelenik a **További ellátói megállapodások** ablak. Ebben az ablakban, gondoskodjék róla, hogy az alábbi ellátói megállapodás négyzetek meg legyenek jelölve:

	Ellátó	Fogyasztó
✓	server9	server1
	server9	server2
	server9	server4
	server9	server5

l Kattintson a **Folytatás** gombra.

l **Megjegyzés:** Egyes esetekben megjelenhet a **Hitelesítési adatok kiválasztása** ablak, és bekéri a `cn=replication,cn=localhost` helytől eltérő helyen tárolt hitelesítési adatokat. Ilyenkor meg kell adnia egy, a `cn=replication,cn=localhost` helytől eltérő helyen tárolt hitelesítési objektumot. Válassza ki a részfa által használt hitelesítési adatokat a meglévők közül, vagy adjon meg újakat. Részletek: “Hitelesítési adatok létrehozása” oldalszám: 133.

- l 6. Kattintson az **OK** gombra.
- l 7. Válassza ki a **server9** értéket, majd kattintson a **Szerver módosítása** lehetőségre.
- l 8. Ellenőrizze, hogy az **Elsődleges szerver** jelölőnégyzet meg van jelölve, majd jelölje ki az **Átjárószerver** lehetőséget.

9. Kattintson az **OK** gombra. A szerverek szerepeit ikonok jelzik a webes adminisztrációs eszközben. A topológia most így néz ki:
- server1 (elsődleges átjáró a site1 számára)
 - server2 (továbbító)
 - server3 (replika)
 - server6 (replika)
 - server4 (továbbító)
 - server7 (replika)
 - server8 (replika)
 - server5 (elsődleges)
 - server9 (elsődleges átjáró a 2. replikációs hely számára)
 - server5 (elsődleges)
 - server1 (elsődleges)
 - server2 (továbbító)
 - server4 (továbbító)
 - server9 (elsődleges átjáró)
 - server1 (elsődleges átjáró)
10. Adjon hozzá replikaszervereket a **server9**-hez a 2. replikációs hely topológiájának kialakításához.
11. Ismétlje meg ezt a folyamatot további replikációs helyek létrehozására. Ne felejtse el, hogy replikációs helyenként csak egy átjárószervert készíthet.
12. Ha végzett a topológia kialakításával, másolja át a server1-ről az adatokat az összes replikációs hely összes gépére és adja hozzá az ellátó információkat az összes új szerverhez. Ezzel kapcsolatos további információk: “Adatok másolása a replikába” oldalszám: 136 és “Ellátó információk felvétele a replikaszerveren” oldalszám: 136.

Topológiák kezelése

A topológiák az egyes replikált részfákra vonatkoznak.

- “Topológia megjelenítése”
- “Replika hozzáadása” oldalszám: 144
- “Megállapodás módosítása” oldalszám: 144
- “Szerver áthelyezése vagy előléptetése” oldalszám: 144
- “Elsődleges szerver lejjebb sorolása” oldalszám: 144
- “Részfa replikálása” oldalszám: 145
- “Részfa módosítása” oldalszám: 145
- “Részfa eltávolítása” oldalszám: 145
- “Részfa zárolása” oldalszám: 145
- “Hozzáférés-felügyeleti listák módosítása” oldalszám: 146

Topológia megjelenítése

Megjegyzés: E feladat végrehajtásához a szervernek futnia kell.

Bontsa ki a navigációs terület **Replikációkezelés** kategóriáját, majd kattintson a **Topológia kezelése** lehetőségre.

1. Válassza ki a megjeleníteni kívánt részfát, majd kattintson a **Topológia megjelenítése** lehetőségre.

A topológia megjelenik a Replikációs topológia listában. A topológiákat a kék háromszögekre kattintva bonthatja ki. A listában az alábbi műveleteket végezheti el:

- Replika hozzáadása.
- Meglévő replika információinak módosítása.

- Átváltás egy másik ellátó szerverre, vagy a replika elsődleges szerverre előléptetése.
- Replika törlése.

Replika hozzáadása

Részletek: “Replikaszerver létrehozása” oldalszám: 135.

Megállapodás módosítása

A replika alábbi információi módosíthatók:

A **Szerver** lapon csak az alábbiak módosíthatók:

- Hozsnév
- Port
- SSL engedélyezése
- Leírás

A **Kiegészítések** lapon az alábbiak módosíthatók:

- Hitelesítési adatok - lásd: “Hitelesítési adatok létrehozása” oldalszám: 133.
- Replikációs ütemezések - lásd: “Replikációs ütemezések létrehozása” oldalszám: 147.
- A fogyasztó replikához replikált funkciók módosítása. Az ellátó funkcióinak listájában kikapcsolhat bármilyen olyan funkciót, amelyet nem kíván replikálni a fogyasztó felé.
- Ha kész, kattintson az **OK** gombra.

Szerver áthelyezése vagy előléptetése

1. Válassza ki a kívánt szervert, majd kattintson az **Áthelyezés** lehetőségre.
2. Válassza ki a szervert, amelyre át akarja helyezni a replikát, vagy a replika elsődleges szerverre előléptetéséhez kattintson a **Replikációs topológia** lehetőségre. Kattintson az **Áthelyezés** gombra.
3. Egyes esetekben megjelenhet a Hitelesítési adatok kiválasztása ablak, és bekéri a cn=replication,cn=localhost helytől eltérő helyen tárolt hitelesítési adatokat. Ilyenkor meg kell adnia egy, a cn=replication,cn=localhost helytől eltérő helyen tárolt hitelesítési objektumot. Válassza ki a részfa által használt hitelesítési adatokat a meglévők közül, vagy adjon meg újakat. Részletek: “Hitelesítési adatok létrehozása” oldalszám: 133.
4. Megjelenik a **További ellátói megállapodások** ablak. Válassza ki a szerver szerepének megfelelő ellátói megállapodásokat. Ha például egy replikaszervert egyenrangú szerverre léptet elő, akkor ellátói megállapodásokat kell létrehoznia az összes többi szerverrel és azok első szintű replikáival. Ezek a megállapodások teszik lehetővé, hogy az előléptetett szerver ellátója legyen a többi szervernek és replikáiknak. Az újonnan előléptetett szerver más szerverekkel meglévő ellátói megállapodásai továbbra is érvényben vannak, és nem kell őket újra létrehozni.
5. Kattintson az **OK** gombra.

A topológia megváltozik, hogy tükrözze a szerver áthelyezését.

További információk: “Összetett topológia létrehozása egyenrangú replikációval” oldalszám: 139.

Elsődleges szerver lejjebb sorolása

Egy szerver elsődlegesből replikaszerverre alakításának lépései:

1. Kapcsolódjon a webes adminisztrációs eszközzel ahhoz a szerverhez, amelyet lejjebb akar sorolni.
2. Kattintson a **Topológia kezelése** lehetőségre.
3. Válassza ki a részfát, majd kattintson a **Topológia megjelenítése** lehetőségre.
4. Törölje a lejjebb sorolni kívánt szerver összes megállapodását.
5. Válassza ki a lejjebb sorolni kívánt szervert, majd kattintson az **Áthelyezés** lehetőségre.
6. Válassza ki a szervert, amely alá át kívánja helyezni a lejjebb sorolt szervert, majd kattintson az **Áthelyezés** lehetőségre.

7. Ugyanúgy, ahogy egy új replika esetében tenné, hozza létre az új ellátói megállapodásokat a lejjebb sorolt szerver és ellátói között. További részletek: “Replikaszerver létrehozása” oldalszám: 135.

Részfa replikálása

Megjegyzés: E feladat végrehajtásához a szervernek futnia kell.

Bontsa ki a navigációs terület **Replikációkezelés** kategóriáját, majd kattintson a **Topológia kezelése** lehetőségre.

- Kattintson a **Részfa hozzáadása** lehetőségre.
- Írja be a replikálni kívánt részfa DN-jét, vagy kattintson a **Tallózás** lehetőségre a részfa gyökereként megjelölt bejegyzés kiválasztásához.
- Írja be az elsődleges szerver utalási URL-jét. Ezt LDAP URL-ként kell megadni, például:
`ldap://<myservername>.<mylocation>.<mycompany>.com`
- Kattintson az **OK** gombra.
- Az új szerver megjelenik a Topológia kezelése ablakban, a **Replikált részfák** címsor alatt.

Részfa módosítása

Ezzel a funkcióval módosíthatja az elsődleges szerver URL-jét, amelyre ez a részfa és replikái küldik a frissítéseket. Ezt akkor kell elvégeznie, ha megváltoztatta az elsődleges szerver portszámát vagy hosztnevét, illetve áthelyezte az elsődleges szervert egy másik szerverre.

1. Válassza ki a módosítani kívánt részfát.
2. Kattintson a **Részfa módosítása** gombra.
3. Írja be az elsődleges szerver utalási URL-jét. Ezt LDAP URL-ként kell megadni, például:
`ldap://<mynewservername>.<mylocation>.<mycompany>.com`

A szerver által betöltött szereptől (elsődleges, replika, vagy továbbító) függően az ablakban más címkék és gombok jelennek meg.

- Ha a részfa szerepe replika, akkor egy megjelenik egy címke, amely azt jelzi, hogy a szerver replikaként vagy továbbítóként működik, és egy gomb a **Szerver elsődlegessé előléptetése** felirattal. Erre a gombra kattintva a szerver, amelyhez a webes adminisztrációs eszköz csatlakozik, előlép elsődleges szerverre.
- Ha a részfa csak a kiegészítő osztály felvételével van beállítva replikációra (nincs alapértelmezett csoport és albejegyzés), akkor megjelenik az **Ez a részfa nem replikált** címke, valamint egy **Részfa replikálása** feliratú gomb. Erre a gombra kattintva felvételre kerül az alapértelmezett csoport és albejegyzés, hogy a szerver, amelyhez a webes adminisztrációs eszköz csatlakozik, előléphessen elsődleges szerverre.
- Ha nem található az elsődleges szerverek albejegyzései, akkor az **Ehhez a részfához nincs megadva elsődleges szerver** címke jelenik meg, valamint egy **Szerver elsődlegessé előléptetése** feliratú gomb. Erre a gombra kattintva felvételre kerül a hiányzó albejegyzés, hogy a szerver, amelyhez a webes adminisztrációs eszköz csatlakozik, előléphessen elsődleges szerverre.

Részfa eltávolítása

1. Válassza ki az eltávolítani kívánt részfát.
2. Kattintson a **Részfa eltávolítása** lehetőségre.
3. A törlés jóváhagyásaként kattintson az **OK** gombra.

A részfa törlődik a **Replikált részfa** listából.

Megjegyzés: Ez a művelet csak akkor sikerül, ha az `ibm-replicaGroup=default` bejegyzés üres.

Részfa zárolása

Ez a funkció akkor hasznos, ha karbantartás vagy módosításokat akar végezni a topológián. Minimálisan csökkenti a szerveren végrehajtható frissítések számát. Egy zárolt szerver nem fogad klienskérdéseket. Kizárólag a szerver adminisztrátori konzolját használó adminisztrátor kéréseire reagál.

Ez egy logikai funkció.

1. A részfa zárolásához kattintson a **Zárolás/feloldás** gombra.
2. A művelet jóváhagyásaként kattintson az **OK** gombra.
3. A részfa zárolásának feloldásához kattintson a **Zárolás/feloldás** gombra.
4. A művelet jóváhagyásaként kattintson az **OK** gombra.

Hozzáférés-felügyeleti listák módosítása

A replikálási információk (replika albejegyzések, replikációs megállapodások, ütemezések, esetleg hitelesítési adatok is) egy **ibm-replicagroup=default** nevű speciális objektum alatt tárolódnak. Az **ibm-replicagroup** objektum közvetlenül a replikált részfa gyökérbejegyzése alatt található. Alapértelmezés szerint ez a részfa ACL-jét a replikált részfa gyökérbejegyzésétől örökli. Nem biztos, hogy ez az ACL megfelelő a replikálási információk hozzáféréseinek szabályozásához.

A szükséges jogosultságok:

- Replikáció szabályozása - Írási hozzáférés az **ibm-replicagroup=default** objektumhoz (vagy tulajdonos/adminisztrátor).
- Lépcsőzetes replikáció szabályozása - Írási hozzáférés az **ibm-replicagroup=default** objektumhoz (vagy tulajdonos/adminisztrátor).
- Sor szabályozása - Írási hozzáférés a replikációs megállapodáshoz.

További információk az ACL tulajdonságok megtekintéséről a webes adminisztrációs eszközzel, illetve az ACL-ek kezeléséről: "Hozzáférés-felügyeleti listák (ACL-ek) kezelése" oldalszám: 185.

További információk: "Hozzáférés-felügyeleti listák" oldalszám: 56.

Replikációs tulajdonságok módosítása

Bontsa ki a navigációs terület **Replikációkezelés** kategóriáját, majd kattintson a **Replikációs tulajdonságok kezelése** lehetőségre. Ahhoz, hogy a **Replikációtulajdonságok kezelése** panelekben módosíthassa a beállításokat, *ALLOBJ és *IOSYSCFG különleges jogosultságokkal rendelkező leképezett felhasználóként kell bejelentkeznie a webes adminisztrációs eszközbe.

Az ablakban az alábbi műveleteket végezheti el:

- Módosíthatja a replikációs állapot lekérdezésekben visszaadott, függőben lévő módosítások maximális számát. Az alapértelmezés szerinti érték 10.
- Felvehet, módosíthat és törölhet ellátói információkat.

Megjegyzés: Az ellátó DN-je lehet egy leképezett i5/OS felhasználói profil DN-je. A leképezett i5/OS felhasználói profilnak nem szabad LDAP adminisztrációs jogosultságokkal rendelkeznie. Nem lehet továbbá *ALLOBJ és *IOSYSCFG speciális jogosultságokkal rendelkező felhasználó, és nem kaphat adminisztrációs jogokat a címtárszerver adminisztrátori alkalmazás azonosítón keresztül sem.

További információk:

- "Ellátói információk felvétele"
- "Ellátói információk módosítása" oldalszám: 147
- "Ellátói információk eltávolítása" oldalszám: 147

Ellátói információk felvétele

1. Kattintson a **Hozzáadás** gombra.
2. Válasszon ki egy ellátót a legördülő menüből, vagy írja be annak a replikált részfának a nevét, amelyhez ellátót kíván felvenni.
3. A hitelesítési adatokhoz írja be a replikációs kapcsolódási DN-t.

Megjegyzés: A két lehetőség bármelyikét használhatja a helyzettől függően.

- Állítsa be a replikáció kapcsolódási DN-jét (és jelszavát), valamint egy alapértelmezett utalást a szerver összes replikált részfájához az "alapértelmezett hitelesítési adatok és utalás" lehetőséggel. Ezt akkor lehet használni, ha az összes részfa ugyanarról az ellátóról replikálódik.
 - Adja meg a replikáció kapcsolódási DN-jét (és jelszavát) külön minden egyes replikált részfához: vegye fel az ellátó információit minden egyes részfához. Ezt akkor kell használni, ha az egyes részfák ellátója eltér (vagyis minden részfához más elsődleges szerver tartozik).
4. A hitelesítési adatok típusától függően írja be és erősítse meg a hitelesítési adatok jelszavát. (Ez az, amit korábban felírt.)
 - **Egyszerű kapcsolódás** - Adja meg a DN-t és a jelszót
 - **Kerberos** - adjon meg egy pszeudo DN-t 'ibm-kn=LDAP-szolgáltatásnév@tartomány' formában, jelszó nélkül
 - **SSL külső csatlakozással** - Adja meg az igazolás alany DN-jét, jelszóra nincs szükség

Részletek: "Hitelesítési adatok létrehozása" oldalszám: 133.

5. Kattintson az **OK** gombra.

Az ellátó részfája felvételre kerül az Ellátó információk listára.

Ellátói információk módosítása

1. Válassza ki a módosítani kívánt ellátói részfát.
2. Kattintson a **Módosítás** gombra.
3. Ha cn=configuration alatti cn=Master Server bejegyzés létrehozásához szükséges **Alapértelmezett hitelesítési adatok és utalás** részt módosítja, akkor az Alapértelmezett ellátó LDAP URL mezőbe írja be annak a szervernek az URL-jét, amelyről a kliens replikafrissítéseket akar kapni. Ennek egy érvényes LDAP URL-nek (ldap://) kell lennie. Egyébként ugorjon a 4. lépésre.
4. A használni kívánt új hitelesítési adatokhoz adja meg a replikációs kapcsolódási DN-t.
5. Írja be és erősítse meg a hitelesítési adatok jelszavát.
6. Kattintson az **OK** gombra.

Ellátói információk eltávolítása

1. Válassza ki az eltávolítani kívánt ellátói részfát.
2. Kattintson a **Törlés** gombra.
3. A törlés jóváhagyásaként kattintson az **OK** gombra.

A részfa törlődik az Ellátó információk listából.

Replikációs ütemezések létrehozása

Nem kötelező, de megadhat replikációs ütemezéseket annak érdekében, hogy a replikáció meghatározott időben történjen vagy éppen ne történjen. Ha nem használ ütemezést, a szerver minden egyes módosítás után beütemezi a replikációt. Ez ugyanaz, mintha azonnali replikációs ütemezést állítana be minden napra, éjjel 12:00 órai kezdettel.

Bontsa ki a navigációs terület **Replikációkezelés** kategóriáját, majd kattintson az **Ütemezések kezelése** lehetőségre.

A **Heti ütemezés** lapon válassza ki a kívánt részfát, amelyhez az ütemezést készíti, majd kattintson az **Ütemezések megjelenítése** lehetőségre. Ha már létezik ütemezés, akkor megjelenik a **Heti ütemezések** mezőben. Egy új ütemezés létrehozása vagy felvétele:

1. Kattintson a **Hozzáadás** gombra.
2. Adja meg az ütemezés nevét. Lehet például **schedule1**.
3. Vasárnaptól szombatig minden egyes nap a napi ütemezés **Nincs** értéként van megadva. Ez azt jelenti, hogy nincsenek ütemezve replikációs frissítési események. A legutolsó replikációs esemény, ha van, akkor még érvényben van. Mivel ez egy új replika, nincsenek korábbi replikációs események, vagyis az ütemezés az azonnali replikáció (alapértelmezés).

4. Kiválaszthat egy napot és a **Napi ütemezés hozzáadása** gombra kattintva létrehozhat egy napi replikációs ütemezést. Ha létrehoz egy napi ütemezést, akkor az lesz az alapértelmezett ütemezés a hét minden egyes napjára. Az alábbiakat teheti:
 - Megtartja a napi ütemezést az egyes napok alapértelmezett ütemezéseként, vagy megad egy napot és visszaváltoztatja az ütemezést "Nincs" értékre. Ne feledje, hogy azokra a napokra, amelyekre nincs megadva ütemezés, továbbra is érvényes a legutolsó replikációs esemény.
 - Módosítja a napi ütemezést: kiválaszt egy napot és a **Napi ütemezés módosítása** lehetőségre kattint. Ne feledje, hogy egy napi ütemezés módosítása befolyásolja az összes olyan napot, amely az adott ütemezést használja, nemcsak a kiválasztott napot.
 - Létrehoz egy másik napi ütemezést: kiválaszt egy napot és a **Napi ütemezés hozzáadása** lehetőségre kattint. Az ütemezés létrehozása után bekerül a **Napi ütemezés** legördülő menübe. Ezután ki kell választania ezt az ütemezést a kívánt napokhoz.
- További információk a napi ütemezések beállításával kapcsolatban: "Napi ütemezés létrehozása".
5. Ha kész, kattintson az **OK** gombra.

Napi ütemezés létrehozása

Bontsa ki a navigációs terület **Replikációkezelés** kategóriáját, majd kattintson az **Ütemezések kezelése** lehetőségre.

A **Napi ütemezés** lapon válassza ki a kívánt részfát, amelyhez az ütemezést készíti, majd kattintson az **Ütemezések megjelenítése** lehetőségre. Ha már létezik ütemezés, akkor megjelenik a **Napi ütemezések** mezőben. Egy új ütemezés létrehozása vagy felvétele:

1. Kattintson a **Hozzáadás** gombra.
2. Adja meg az ütemezés nevét. Lehet például **hetfo1**.
3. Válassza ki az időzóna-beállítást (UTC vagy helyi).
4. A legördülő menüből válasszon egy replikációtípust:

Azonnali

Minden, a legutolsó replikációs esemény óta történt, függőben lévő bejegyzés-frissítést feldolgoz és folyamatosan frissíti a bejegyzéseket egészen addig, amíg el nem éri a következő ütemezett frissítési eseményt.

Egyszeri

Végrehajtja a kezdő időpont előtt függőben lévő összes frissítést. A kezdő időpont utáni frissítéseknek várniuk kell a következő ütemezett replikációs eseményre.

5. Válassza ki a replikációs esemény induló időpontját (a szerver helyi idejében).
6. Kattintson a **Hozzáadás** gombra. Megjelenik a replikációs esemény és a hozzá tartozó időpont.
7. Vegyen fel vagy töröljön eseményeket az ütemezés kialakításához. Az események listája időrendben frissül.
8. Ha kész, kattintson az **OK** gombra.

Például:

6. táblázat:

Replikáció típusa	Kezdési idő
Azonnali	12:00 AM
Egyszeri	10:00 AM
Egyszeri	2:00 PM
Azonnali	4:00 PM
Egyszeri	8:00 PM

Ebben az ütemezésben az első replikációs esemény éjjel történik, és az összes addig függőben lévő eseményt frissíti. A replikációs frissíték egészen délelőtt 10-ig folytatódnak. A délelőtt 10 óra és délután 2 közötti módosításoknak délután

2-ig kell várniuk a frissítésre. A 2 és 4 közötti frissítéseknek 4-ig kell várniuk, ekkor a replikációs frissítés folyamatossá válik a következő (8 órai) ütemezett replikációs eseményig. Az este 8 utáni frissítéseknek várniuk kell a következő ütemezett replikációs eseményre.

Megjegyzés: Ha a replikációs események túlságosan sűrűn vannak ütemezve egymás után, akkor előfordulhat, hogy egy replikációs esemény kimarad, ha az előző esemény frissítései még feldolgozás alatt vannak a bekövetkeztekor.

Sorok kezelése

Ezzel a feladattal figyelhető a szerver által használt replikációs megállapodások (sorok) replikációs állapota.

Bontsa ki a navigációs terület **Replikációkezelés** kategóriáját, majd kattintson a **Sorok kezelése** lehetőségre.

Válassza ki a replikát, amelyiknek a sorát kezelni kívánja.

- A replika állapotától függően **Felfüggesztheti/folytathatja**, illetve leállíthatja és újraindíthatja a replikációt.
- A **Replikáció kényszerítése** lehetőségre kattintva az összes változás replikációját kikényszerítheti, függetlenül attól, hogy mikorra van időzítve a következő replikáció.
- A **Sor részletei** lehetőségre kattintva részletesebb leírást kap a replika sorának állapotáról. Itt kezelhetők a sorok is.
- Kattintson a **Frissítés** gombra a sorok frissítéséhez és a szerverüzenetek törléséhez.

Sor részletei

A **Sor részletei** lehetőségre kattintva három lap jelenik meg:

- Állapot
- Legutolsó kísérlet részletei
- Függőben lévő módosítások

Az **Állapot** lapon a replika neve, részfája, állapota és a replikációs idők feljegyzett értékei láthatók. Ezen a panelen függesztheti fel és folytathatja a replikációt a **Folytatás** gombra kattintva. Kattintson a **Frissítés** gombra a sor információinak frissítéséhez.

A **Legutolsó kísérlet részletei** lapon a legutóbbi frissítési kísérlettel kapcsolatos információk láthatók. Ha egy bejegyzés nem tölthető be, nyomja meg a **Blokkoló bejegyzés átlépése** gombot a replikáció folytatásához a következő függőben lévő bejegyzéssel. Kattintson a **Frissítés** gombra a sor információinak frissítéséhez.

A **Függőben lévő módosítások** lapon a replika függőben lévő módosításai láthatók. Ha a replikáció blokkolódott, törölheti az összes függőben lévő módosítást az **Összes kihagyása** gombbal. A **Frissítés** gombra kattintva frissítheti a függőben lévő módosítások listáját a feldolgozott új frissítésekkel.

Megjegyzés: Ha úgy döntött, hogy kihagyja a blokkoló módosításokat, akkor gondoskodnia kell arról, hogy a fogyasztó szerver idővel frissítésre kerüljön. További információk: "ldapdiff" oldalszám: 217.

Replikáció beállítása biztonságos kapcsolaton keresztül

Az SSL használatával végzett replikációt érdemes lépésenként beállítani, így a művelet előrehaladása közben mindent ellenőrizhet.

A biztonságos kapcsolaton keresztül végzett replikáció beállításának megkísérlése előtt a következő feladatokat kell elvégeznie (bármilyen sorrendben):

- Állítsa be a replikációt egy nem biztonságos kapcsolaton keresztül
- Állítsa be a fogyasztó szerveret a kapcsolatok elfogadására a biztonságos porton keresztül. Ellenőrizze, hogy a kliens használni tud egy biztonságos kapcsolatot a fogyasztó szerverhez, például az ldapsearch segédprogram használatával. Ha azt szeretné, hogy az ellátó szerver tanúsítványt használjon a hitelesítéshez, mint egy SSL-en

| keresztüli külső kapcsolat esetében, akkor először be kell állítani a szerverhitelesítést, majd a kliens-szerver hitelesítést, ahol a "szerver" a fogyasztószerver és a kliens az ellátószerver.

| **Megjegyzés:** Ha a szerver be van állítva a kliens-szerver hitelesítés használatára, akkor minden SSL-t használó kliensnek rendelkeznie kell egy klienstanúsítvánnyal.

- | • Állítsa be az ellátószerveret, hogy megbízzon a fogyasztó tanúsítványát kiadó tanúsítványhatóságban.
- | 1. A webes adminisztrációs eszközben kattintson a **Replikációkezelés** kategória **Topológia kezelése** elemére.
- | 2. Válassza ki a meglévő megállapodások valamelyikét, amelyet biztonságossá kíván tenni.
- | 3. Kattintson a **Megállapodás szerkesztése...** lehetőségre és válassza az SSL használatát, hogy bizonyossá tegye a megfelelő portszám használatát. A szabványos biztonságos portszám a 636.
- | 4. Ellenőrizze, hogy a megállapodások keresztül végzett replikáció megfelelően működik.

| Ha csak egy biztonságos kapcsolaton keresztül, DN és jelszó használatával zajló hitelesítés miatt próbál beállítani egy replikációt, akkor ez az előző lépésekkel megvalósult. A klienstanúsítványokkal végzett hitelesítéshez az ellátószervernek a megállapodásban másféle hitelesítési objektumokat kell használnia, valamint be kell állítani a fogyasztó szerveret, hogy elfogadja ugyanazokat a tanúsítványokat, mint az ellátószerver.

| Biztonsági tulajdonságok kezelése

| A Directory Server számos mechanizmussal rendelkezik adatai védelmének biztosítására. Ezek közé tartozik a jelszókezelés, a titkosítás SSL és TLS használatával, a Kerberos és a DIGEST-MD5 hitelesítés. A biztonsági fogalmakkal kapcsolatban további információk: "Directory Server biztonsága" oldalszám: 46.

| További információk:

- | • "Jelszavak kezelése"
- | • "SSL és TSL engedélyezése a Directory Serveren" oldalszám: 154
- | • "Kerberos hitelesítés engedélyezése a Directory Server-hez" oldalszám: 156
- | • "DIGEST-MD5 hitelesítés beállítása a Directory Serveren" oldalszám: 157

| Jelszavak kezelése

| A jelszókezeléshez bontsa ki a **Biztonsági tulajdonságok kezelése** kategóriáját, és válassza a **Jelszó-irányelvek** oldalt.

| További információk:

- | • "Jelszótulajdonságok beállítása"
- | • "Jelszó-irányelv javaslatok" oldalszám: 152

| Jelszótulajdonságok beállítása

| A Directory Server számos jelszóhasználati lehetőséget biztosít, hogy csak a hitelesített felhasználók érhessék el a címtárat. Ezek a lehetőségek a jelszó-irányelvek, jelszókizárás és jelszóellenőrzés alatt vannak csoportosítva.

| Jelszó-irányelvek

| A jelszó-irányelv beállításának lépései:

- | 1. Bontsa ki a webes adminisztrációs eszköz navigációs területének **Biztonsági tulajdonságok kezelése** kategóriáját, és válassza az **Jelszó-irányelvek** oldalt. A panelben egy nem szerkeszthető mező, a **Jelszóattribútum** látható, amely a jelszóirányelvek által használt attribútum nevét tartalmazza.
- | 2. Válassza ki a jelszótitkosítás típusát a legördülő listából:
 - | **Nincs** Nincs titkosítás. A jelszavak nyílt szöveges formában tárolódnak.
 - | **crypt** A rendszer a jelszavakat a UNIX crypt algoritmus szerint titkosítja, mielőtt a címtárban tárolásra kerülnek.
 - | **SHA-1** A rendszer a jelszavakat az SHA-1 algoritmus szerint titkosítja, mielőtt a címtárban tárolásra kerülnek.

3. A jelszó-irányelvek engedélyezéséhez válassza ki a **Jelszó-irányelvek engedélyezve** jelölőnégyzetet.

Megjegyzés: Ha a jelszó-irányelvek nincsenek engedélyezve, akkor az ebben és a többi jelszópanelben található funkciók egyike sem lesz elérhető, amíg a jelölőnégyzetet be nem kapcsolja. A jelszó-irányelvek alapértelmezésben ki vannak kapcsolva.

4. Válassza ki a **Felhasználó módosíthatja a jelszót** jelölőnégyzetet annak megadására, hogy a felhasználók módosíthatják-e a jelszót.
5. Válassza ki a **Felhasználónak meg kell változtatnia a jelszót alaphelyzetbe állítás után** jelölőnégyzetet annak megadására, hogy a felhasználóknak meg kell-e változtatniuk a jelszót, ha egy alaphelyzetbe állított jelszóval jelentkeztek be.
6. Válassza ki a **Felhasználónak el kell küldenie a jelszót, ha változik** jelölőnégyzetet annak megadására, hogy a felhasználónak a kezdeti bejelentkezés után meg kell-e adnia újra a jelszót, mielőtt ismét képes lenne azt megváltoztatni.
7. Állítsa be a jelszólejárati korlátot. Kattintson a **Jelszó soha nem jár le** választógombra annak megadásához, hogy a jelszót nem kell adott időnként megváltoztatni, vagy kattintson a **Nap** választógombra az időköz megadásához, ahány naponta a jelszót alaphelyzetbe kell állítani.
8. Adja meg, hogy a rendszer a jelszó lejárata előtt kiadjon-e jelszólejárati figyelmeztetést.
Ha a **Soha ne figyelmeztessen** választógombra kattint, akkor a felhasználók nem kapnak figyelmeztetést az előző jelszó lejárata előtt. A felhasználók nem érhetik el a címtárat, amíg az adminisztrátor nem készít új jelszót.
Ha a **Lejárat előtt ... nappal** választógombra kattint, és megadja a napok számát (n), akkor a felhasználók a jelszó megváltoztatására figyelmeztető üzenetet fognak kapni minden bejelentkezéskor a jelszó lejárata előtti n. naptól kezdve. A felhasználók továbbra is elérhetik a címtárat, amíg a jelszó le nem jár.
9. Adja meg, hogy a jelszó lejárata után (ha egyáltalán) még hányszor léphetnek be a felhasználók. Ez a kiválasztás lehetőséget ad a felhasználóknak, hogy lejárt jelszóval is elérjék a címtárat.
10. Kattintson az **OK** gombra.

Megjegyzés: Használhatja az ldapmodify segédprogramot is (részletek: "ldapmodify és ldapadd" oldalszám: 191) a jelszó-irányelv beállításához.

További információk a jelszó-irányelvről: "Jelszó-irányelvek" oldalszám: 68.

Jelszókizárás

1. Bontsa ki a webes adminisztrációs eszköz navigációs területének **Biztonsági tulajdonságok kezelése** kategóriáját, és válassza az **Jelszókizárás** oldalt.

Megjegyzés: Ha a jelszó-irányelvek használata nincs engedélyezve a szerveren, akkor az ebben a panelben található funkciók nem lesznek érvényesek.

2. Adja meg, hogy hány másodpercnek, percnek, órának és napnak kell eltelni, mielőtt a jelszó megváltoztatható lenne.
3. Adja meg, hogy a helytelen bejelentkezések kizárják-e a jelszavakat.
 - Ha korlátlan számú bejelentkezési kísérletet szeretne engedélyezni, akkor kattintson a **Jelszó soha nem kerül kizárásra** választógombra. Ezzel kikapcsolható a jelszókizárási szolgáltatás.
 - Válassza ki a **Kísérletek** választógombot, és adja meg, hogy hány bejelentkezési kísérlet engedélyezett a jelszó kizárása előtt. Ezzel kapcsolható be a jelszókizárási szolgáltatás.
4. Adja meg a kizárás időtartamát. Válassza a **Kizárás soha nem jár le** választógombot, ha azt szeretné, hogy a rendszergazdának alaphelyzetbe kelljen állítania a jelszót, illetve a **Másodperc** választógombot, és aztán adja meg, hogy hány másodpercnek kelljen eltelnie, mielőtt a kizárás lejár és a ismét meg lehet kísérelni a bejelentkezést.
5. Adja meg a helytelen bejelentkezés lejárati idejét. Kattintson a **Helytelen bejelentkezések csak helyes jelszóval törölhetők** választógombra, ha azt szeretné, hogy a helytelen bejelentkezések csak egy sikeres bejelentkezéssel törölődjenek, vagy a **Másodperc** választógombra, és adja meg, hogy hány másodperc múlva törölődnek a sikertelen bejelentkezések a memóriából.

- | **Megjegyzés:** Ez a beállítás csak akkor működik, ha a jelszó nincs kizárva.
- | 6. Ha végzett, kattintson az **ALKalmazás** gombra, ha kilépés nélkül kívánja menteni a változásokat, illetve az **OK** gombra, ha menteni szeretne és kilépni, esetleg a **Mégse** gombra, ha változások nélkül szeretné elhagyni a panelt.

| **Jelszóellenőrzés**

- | 1. Bontsa ki a webes adminisztrációs eszköz navigációs területének **Biztonsági tulajdonságok kezelése** kategóriáját, és válassza az **Jelszóellenőrzés** oldalt.

| **Megjegyzés:** Ha a jelszó-irányelvek használata nincs engedélyezve a szerveren, akkor az ebben a panelben található funkciók nem lesznek érvényesek.

- | 2. Állítsa be, hogy hány jelszót kell használni, mielőtt egy jelszó ismét felhasználható lenne. Adjon meg egy 0 és 30 közé eső számot. Ha nullát ad meg, akkor a jelszavak korlátozás nélkül újra felhasználhatók.
- | 3. A legördülő menüben válassza ki, hogy a jelszó ellenőrzésre kerüljön-e a következő beviteli mezőkben megadott szintaxis ellenőrzésére. A következők közül választhat:

| **Ne legyen szintaxisellenőrzés**

| Nem történik szintaxisellenőrzés.

| **Legyen szintaxisellenőrzés (kivéve a titkosítottakat)**

| Szintaxisellenőrzés történik minden nem titkosított jelszó esetében.

| **Legyen szintaxisellenőrzés**

| Szintaxisellenőrzés történik minden jelszó esetében.

- | 4. Adjon meg egy számértéket a jelszó minimális hosszának meghatározásához. Ha az érték nulla, akkor nem történik szintaxisellenőrzés.
- Adjon meg egy számértéket annak meghatározásához, hogy a jelszónak minimum hány betűkaraktert kell tartalmaznia.
 - Adjon meg egy számértéket annak meghatározásához, hogy a jelszónak minimum hány számkaraktert kell tartalmaznia.

| **Megjegyzés:** A szám-, betű- és speciális karakterek összesített száma nem haladhatja meg a jelszó minimális hosszát.

- | 5. Adja meg, hogy hány karakter ismétlődhet a jelszóban. Ez a beállítás korlátozza, hogy az adott karakter hányszor jelenhet meg a jelszóban. Ha az érték nulla, akkor az ismétlődő karakterek száma nem kerül ellenőrzésre.
- | 6. Adja meg, hogy minimum hány karakternek kell különböznie az előző jelszótól, illetve a **Jelszavak minimális száma az ismételt használat előtt** mezőben megadott számú előző jelszavaktól. Ha az érték nullára van állítva, akkor az eltérő karakterek számát a rendszer nem ellenőrzi.
- | 7. Ha végzett, kattintson az **ALKalmazás** gombra, ha kilépés nélkül kívánja menteni a változásokat, illetve az **OK** gombra, ha menteni szeretne és kilépni, esetleg a **Mégse** gombra, ha változások nélkül szeretné elhagyni a panelt.

| **Jelszó-irányelv javaslatok**

| **Jelszó-irányelv lekérdezések**

| A jelszó-irányelv műveleti attribútumok a címtárbejegyzések állapotának megtekintésére vagy a megadott feltételeknek megfelelő bejegyzések lekérdezésére használhatók. A műveleti attribútumokat csak keresési kérésekre adja vissza a rendszer, amikor azt a kliens kifejezetten kéri. Ezeknek az attribútumoknak a használatához keresési műveletekben jogosultnak kell lennie a kritikus attribútumok, illetve egyes használt attribútumok elérésére.

| Egy adott bejegyzés összes jelszóirányelv-attribútumának megtekintéséhez:

```
| > ldapsearch -b "uid=user1,cn=users,o=ibm" -s base "(objectclass=*)"
|   pwdChangedTime pwdAccountLockedTime pwdExpirationWarned
|   pwdFailureTime pwdGraceUseTime pwdReset
```


| A lejárfiók jelszavú bejegyzések lekérdezéséhez használja a pwdChangedTime attribútumot. Ha például azokat a jelszavakat szeretné megtalálni, amelyek 2004. augusztus 26-án járnak le és 186 napos jelszólejárati irányelvvvel rendelkeznek, kérdezze le azokat a bejegyzéseket, amelyek jelszava 186 napja (2004. február 22. óta) változott:

```
| > ldapsearch -b "cn=users,o=ibm" -s sub  
| "!(pwdChangedTime>20040222000000Z)" 1.1
```

| -- ahol a szűrő a 2004. február 22., éjféllel kezdődő pwdChangedTime értéknek felel meg

| A kizárt fiókok lekérdezésére a pwdAccountLockedTime attribútum használható:

```
| > ldapsearch -b "cn=users,o=ibm" -s sub "(pwdAccountLockedTime=*)" 1.1
```

| -- ahol az "1.1" jelzi, hogy csak a bejegyzés DN-ek kerülnek visszaadásra.

| Azoknak a fiókoknak a lekérdezéséhez, amelyek esetében a jelszót módosítani kell, mivel alaphelyzetbe állításra került, használja a pwdReset attribútumot:

```
| > ldapsearch -b "cn=users,o=ibm" -s sub "(pwdReset=TRUE)" 1.1
```

| **Jelszó-irányelvek felülbírálása**

| A címtáradminisztrátor felülbírálhatja a jelszó-irányelvek szokásos működését azzal, hogy módosítja a jelszó-irányelv műveleti attribútumait és a szerveradminisztrációs vezérlést (az LDAP parancssoros segédprogramok -k kapcsolója) használja.

| Megelőzhető, hogy egy adott fiók jelszava lejárjon, ha a pwdChangedTime attribútumot messze a jövőbe előreállítja a userPassword attribútum beállításakor. A következő példa 2200. január 1-én éjféltre állítja ezt:

```
| > ldapmodify -D cn=root -w ? -k  
| dn: uid=wasadmin,cn=users,o=ibm  
| changetype: modify  
| replace: pwdChangedTime  
| pwdChangedTime: 22000101000000Z
```

| Egy kiterjedt bejelentkezési hibák miatt zárolt fiók zárolásának feloldásához távolítsa el a pwdAccountLockedTime és pwdFailureTime attribútumokat:

```
| > ldapmodify -D cn=root -w ? -k  
| dn: uid=user1,cn=users,o=ibm  
| changetype: modify  
| delete: pwdAccountLockedTime  
| -  
| delete: pwdFailureTime
```

| Egy lejárt fiók zárolásának megszüntetéséhez módosítsa a pwdChangedTime attribútumot és törölje a pwdExpirationWarned és pwdGraceUseTime attribútumokat:

```
| > ldapmodify -D cn=root -w ? -k  
| dn: uid=user1,cn=users,o=ibm  
| changetype: modify  
| replace: pwdChangedTime  
| pwdChangedTime: 20040826000000Z  
| -  
| delete: pwdExpirationWarned  
| -  
| delete: pwdGraceUseTime
```

| A "jelszót kötelező módosítani" állapotot törölheti vagy beállíthatja a pwdReset attribútum megadásával:

```
| > ldapmodify -D cn=root -w ? -k  
| dn: uid=user1,cn=users,o=ibm  
| changetype: modify  
| delete: pwdReset  
|  
| > ldapmodify -D cn=root -w ? -k
```

```
| dn: uid=user2,cn=users,o=ibm
| changetype: modify
| replace: pwdReset
| pwdReset: TRUE
```

| Egy fiók adminisztratív módon zárolható azzal, ha az `ibm-pwdAccountLocked` műveleti attribútumot `TRUE` értékre állítja. A fiók zárolásának megszüntetéséhez állítsa az attribútumot `FALSE` értékre. Egy fiók zárolásának ezen a módon történő feloldása nem befolyásolja a fiúk állapotát a kiterjedt jelszóhibák vagy lejárt jelszó miatti zárolás tekintetében.

| Ahhoz, hogy a felhasználó ezt az attribútumot módosíthassa, írási jogosultsággal kell rendelkeznie a `CRITICAL` elérési osztályba tartozó `ibm-pwdAccountLocked` attribútumhoz.

```
| > ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
| dn: uid=user1,cn=users,o=ibm
| changetype: modify
| replace: ibm-pwdAccountLocked
| ibm-pwdAccountLocked: TRUE
```

| A fiók zárolásának feloldásához:

```
| > ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
| dn: uid=user1,cn=users,o=ibm
| changetype: modify
| replace: ibm-pwdAccountLocked
| ibm-pwdAccountLocked: FALSE
```

| Egyéb jelszó-irányelvekkel kapcsolatos javaslatok

| Van két terület, ahol a jelszó-irányelvek megvalósítása lehet, hogy nem az elvártaknak megfelelően működik:

- | 1. Ha a `pwdReset` attribútum be volt állítva egy bejegyzéshez, a kliensek korlátlanul használhatják a bejegyzés DN-t és a visszaállítási jelszót. Ha van Jelszó-irányelv lekérdezési felügyelet, akkor ez sikertelen kapcsolódást és figyelmeztetést eredményezhet a válaszkezelésnél. Ha azonban a kliens nem határozza meg a lekérdezési felügyeletet, akkor ez a "jelszó-irányelvet nem ismerő" kliens sikeres kapcsolódást fog látni annak jelzése nélkül, hogy a jelszót meg kellene változtatni. Az ez alatt a megkülönböztetett név alatt zajló ezután következő műveletek továbbra is "nem kívánatos végrehajtás" hibával fognak megghiúsulni; csak a kezdeti kapcsolat eredménye lehet megtévesztő. Ez probléma lehet, ha a kapcsolat kizárólag a hitelesítés miatt jött létre, valamint akkor is, ha egy webalkalmazás a címtárat használja a hitelesítésre a címtárhoz.
- | 2. A `pwdSafeModify` és `pwdMustChange` irányelvek nem viselkednek az elvárt módon egy alkalmazással, amely más azonosság alatt módosítja a jelszavakat, mint annak a bejegyzésnek a megkülönböztetett neve, amelynek jelszava változik. Ebben a példahelyzetben egy adminisztrátori azonosság alatt végzett biztonságos jelszómódosítás például azt eredményezheti, hogy a `pwdReset` beállításra kerül. Egy jelszót módosító alkalmazás adminisztrátori fiókot használhat, és eltávolíthatja a `pwdReset` attribútumot a korábban leírtaknak megfelelően.

| SSL és TSL engedélyezése a Directory Serveren

| SSL

| Ha a Digitális igazolás kezelő telepítve lett a rendszerre, használhatja a védett socket réteg (Secure Sockets Layer SSL) nyújtotta biztonságot, hogy védje a Directory Server-hez hozzáférést. Mielőtt engedélyezné a címtár szolgáltatón az SSL használatát, érdemes elolvasni az alábbi részt: "Védett socket réteg (SSL) és Fordítási réteg biztonság (TLS) használata LDAP Directory Serverrel" oldalszám: 47.

| Az SSL engedélyezése az LDAP szerveren:

| 1. Tanúsítvány rendelése a Directory Server-hez

- | a. Ha a Directory Server-t egy SSL kapcsolaton keresztül kívánja felügyelni a iSeries navigátorból, akkor olvassa el az iSeries Access for Windows Felhasználói kézikönyvét (lehet, hogy telepítette a PC-re is az iSeries navigátor telepítésekor). Ha SSL és nem SSL kapcsolatokat egyaránt engedélyezni kíván a szerverre, akkor kihagyhatja ezt a lépést.

- b. Indítsa el az IBM Digitális igazoláskezelőt. További információkért tekintse meg a Digitális igazoláskezelő témakör Digitális igazoláskezelő indítása szakaszát.
- c. Ha igazolásokat kell beszereznie vagy létrehoznia vagy bármilyen egyéb módosítást vagy beállítást kell végrehajtania az igazoláskezelő rendszeren, akkor azt most tegye meg. Az igazoláskezelő rendszer beállításával kapcsolatban tekintse meg a Digitális igazoláskezelő című részt. A Directory Server-hez két szerver- és egy kliensalkalmazás tartozik. Ezek a következők:

Directory Server alkalmazás

A Directory Server alkalmazás maga a szerver.

Directory Server közzétételi alkalmazás

A Directory Server közzétételi alkalmazás azonosítja a közzététel által használt igazolást.

Directory Server kliensalkalmazás

A Directory Server kliensalkalmazás azonosítja az LDAP kliens ILE API-kat használó alkalmazások alapértelmezett igazolásait.

- d. Kattintson az **Igazolástároló kiválasztása** gombra.
- e. Válassza ki a ***SYSTEM** elemet. Kattintson a **Folytatás** gombra.
- f. Adja meg a ***SYSTEM** igazolástároló helyes jelszavát. Kattintson a **Folytatás** gombra.
- g. A baloldali navigációs menü újra betöltődése után bontsa ki az **Alkalmazások kezelése** elemet.
- h. Kattintson az **Igazolás-hozzárendelések frissítése** lehetőségre.
- i. A következő képernyőn válassza ki a **Szerver** alkalmazást. Kattintson a **Folytatás** gombra.
- j. Válassza ki a **Directory Server szerver** elemet.
- k. Az **Igazolás-hozzárendelés frissítése** gombra kattintva rendeljen egy igazolást a Directory Server-hez, amellyel azonosíthatja magát az iSeries Access for Windows kliensek felé.

Megjegyzés: Ha egy olyan CA igazolását választja, amelynek a CA igazolása még nincs benne az iSeries Access for Windows kliens kulcsadatbázisában, akkor azt fel kell vennie az SSL használatához. Mielőtt nekilátna azonban annak, fejezze előbb be ezt az eljárást.

- l. Válasszon ki a listából egy tanúsítványt, amelyet a szerverhez rendel.
 - m. Kattintson az **Új igazolás hozzárendelése** lehetőségre.
 - n. A DCM újratölti az **Igazolás-hozzárendelés frissítése** oldalt és megjelenít egy megerősítést kérő üzenetet. Ha készen van a Directory Server igazolásainak beállításával, kattintson a **Kész** gombra.
2. **Tanúsítvány rendelése a Directory Server közzétételhez** (elhagyható lépés) Ha a rendszerből a Directory Server-re közzétételt is egy SSL kapcsolaton keresztül kívánja biztosítani, akkor egy igazolást kell rendelnie a Directory Server közzétételhez is. Ez azonosítja azon LDAP ILE API-kat használó alkalmazások alapértelmezett igazolását és megbízható CA-it, amelyek nem adnak meg saját alkalmazásazonosítót, vagy egy alternatív kulcsadatbázist.
- a. Indítsa el az IBM Digitális igazolás kezelőt.
 - b. Kattintson az **Igazolástároló kiválasztása** gombra.
 - c. Válassza ki a ***SYSTEM** elemet. Kattintson a **Folytatás** gombra.
 - d. Adja meg a ***SYSTEM** igazolástároló helyes jelszavát. Kattintson a **Folytatás** gombra.
 - e. A baloldali navigációs menü újra betöltődése után bontsa ki az **Alkalmazások kezelése** elemet.
 - f. Kattintson az **Igazolás-hozzárendelések frissítése** lehetőségre.
 - g. A következő képernyőn válassza ki a **Kliens** alkalmazást. Kattintson a **Folytatás** gombra.
 - h. Válassza ki a **Directory Server közzététel** elemet.
 - i. Az **Igazolás-hozzárendelés frissítése** gombra kattintva rendeljen egy igazolást a Directory Server közzétételhez, amellyel azonosíthatja magát.
 - j. Válasszon ki a listából egy tanúsítványt, amelyet a szerverhez rendel.
 - k. Kattintson az **Új igazolás hozzárendelése** lehetőségre.
 - l. A DCM újratölti az **Igazolás-hozzárendelés frissítése** oldalt és megjelenít egy megerősítést kérő üzenetet.

Megjegyzés: Ezek a lépések feltételezik, hogy nem SSL kapcsolaton keresztül már működik az információk közzététele a Directory Server felé. További információk a közzététel beállításával kapcsolatban: “Információk publikálása a címtárszervernek” oldalszám: 92.

3. **Tanúsítvány rendelése a Directory Server klienshez** (elhagyható lépés) Ha más alkalmazások is használnak SSL kapcsolatot a Directory Server felé, akkor egy igazolást kell rendelni a Directory Server klienshez is.

- a. Indítsa el az IBM Digitális igazolás kezelőt.
- b. Kattintson az **Igazolástároló kiválasztása** gombra.
- c. Válassza ki a ***SYSTEM** elemet. Kattintson a **Folytatás** gombra.
- d. Adja meg a ***SYSTEM** igazolástároló helyes jelszavát. Kattintson a **Folytatás** gombra.
- e. A baloldali navigációs menü újra betöltődése után bontsa ki az **Alkalmazások kezelése** elemet.
- f. Kattintson az **Igazolás-hozzárendelések frissítése** lehetőségre.
- g. A következő képernyőn válassza ki a **Kliens** alkalmazást. Kattintson a **Folytatás** gombra.
- h. Válassza ki a **Directory Server kliens** elemet.
- i. Az **Igazolás-hozzárendelés frissítése** gombra kattintva rendeljen egy igazolást a Directory Server klienshez, amellyel az azonosíthatja magát.
- j. Válasszon ki a listából egy tanúsítványt, amelyet a szerverhez rendel.
- k. Kattintson az **Új igazolás hozzárendelése** lehetőségre.
- l. A DCM újratölti az **Igazolás-hozzárendelés frissítése** oldalt és megjelenít egy megerősítést kérő üzenetet.

Az SSL engedélyezése után lehetőség nyílik a Directory Server által védett kapcsolatok esetén használt portszám megváltoztatására.

TLS

Az SSL vagy TLS használatához engedélyeznie kell azt az iSeries Navigatorban.

1. az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a jobb oldali egérgombbal a **Címtár** feliratra, és válassza a **Tulajdonságok** lapot.
4. A **Hálózat** lapon jelölje ki a **Biztonságos** elem melletti jelölőnégyzetet.

Megadhatja a biztonságossá tenni kívánt portszámot is. A **Biztonságos** jelölőnégyzetre kattintva egy jelzés látható arra vonatkozólag, hogy egy alkalmazás el tud-e indulni SSL vagy TLS kapcsolaton a biztonságos porton keresztül. A rendszer azt is jelzi, hogy egy alkalmazás képes-e egy StartTLS műveletre a TSL kapcsolat engedélyezésére a nem biztonságos porton keresztül. Ennek alternatívájaként a TLS a kliens parancssoros segédprogramjából is meghívható a -Y kapcsoló használatával. Parancssor használatára esetén az ibm-slapdSecurity attribútumnak meg kell felelnie a TLS vagy SSLTLS értéknek.

Az SSL-lel és TSL-lel kapcsolatban további információk: “Védett socket réteg (SSL) és Fordítási réteg biztonság (TLS) használata LDAP Directory Serverrel” oldalszám: 47.

Kerberos hitelesítés engedélyezése a Directory Server-hez

Ha a rendszerén konfigurálta a Hálózati hitelesítés szolgáltatást (Network Authentication Service), akkor üzembe állíthatja a Directory Server-en a Kerberos hitelesítés használatát. A Kerberos hitelesítés a felhasználókra és az adminisztrátorra vonatkozik. Mielőtt engedélyezné a címtárszerveren a Kerberos használatát, érdemes megismerni a Kerberos és a Directory Server használatáról szóló áttekintést.

A Kerberos hitelesítés engedélyezéséhez végezze el az alábbiakat:

1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Properties** menüpontot.

- | 5. Kattintson a **Kerberos** lapra.
- | 6. Ellenőrizze a **Kerberos hitelesítés engedélyezését**.
- | 7. A helyzettől függően adja meg a szükséges beállításokat a **Kerberos** oldalon. Az egyes mezőkről további információkat az oldal online súgójában talál.

| **DIGEST-MD5 hitelesítés beállítása a Directory Serveren**

| A DIGEST-MD5 egy SASL hitelesítési mechanizmus. Amikor egy kliens DIGEST-MD5 hitelesítést használ, a jelszó nem kerül továbbításra nyílt szövegben, és a protokoll megakadályozza az újrarájtás típusú támadásokat is. A DIGEST-MD5 beállítására a webes adminisztrációs eszköz használható.

- | 1. A **Szerveradminisztráció** alatt bontsa ki a **Biztonsági tulajdonságok kezelése** kategóriát a navigációs területen, és válassza ki a **DIGEST-MD5** lapot.

| **Megjegyzés:** A szerver konfigurációs beállításainak módosításához a webadminisztrációs eszköz Szerveradminisztrációs kategóriájának használatával hitelesítenie kell magát a szerverhez egy i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultságokkal. Ez úgy történhet, hogy hitelesíti magát leképezett felhasználóként az adott profil jelszavával. A kapcsolódáshoz a webes adminisztrációs eszközhöz leképezett felhasználóként adjon meg egy felhasználónevet a következő formában: `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, ahol a MYUSERNAME és MYSYSTEM.COM karaktersorozatokat a saját felhasználói profiljának nevével és a beállított rendszerleképezési utótaggal helyettesíti.

- | 2. A **Szervertartomány** alatt válassza ki az előre kijelölt **Alapértelmezett** beállítást, ami a szerver teljes képzésű hosztneve, vagy kattintson a **Tartomány** lehetőségre és írja be a szerverhez beállítani kívánt tartomány nevét. Ennek a tartománynévnek a használatával dönti el a kliens, melyik felhasználónevet és jelszót fogja használni. Replikáció használata során lehet, hogy minden szervert ugyanarra a tartományra akar beállítani.
- | 3. A **Felhasználónév** attribútum alatt használja az előre kiválasztott **Alapértelmezett** beállítást, ez a felhasználói azonosító, illetve kattintson az **Attribútum** lehetőségre és adja meg annak az attribútumnak a nevét, amelyet kívánsága szerint a szerver kizárólagosan használjon az azonosításra a DIGEST-MD5 SASL kapcsolatok alatt.
- | 4. Ha címtáradminisztrátorként van bejelentkezve, akkor az **Adminisztrátor felhasználóneve** alatt adja meg az adminisztrátor felhasználónevet. Ezt a mezőt csak az adminisztrációs csoport tagjai szerkeszthetik. Ha a DIGEST-MD5 SASL kapcsolat során megadott felhasználónév egyezik ezzel a karaktersorozattal, akkor a felhasználó az adminisztrátor.

| **Megjegyzés:** Az adminisztrátor felhasználónevében a kis- és nagybetűk eltérőnek számítanak.

- | 5. Ha kész, kattintson az **OK** gombra.

Séma kezelése

További információk a sémáról: "Séma" oldalszám: 15.

A séma a webes adminisztrációs eszközzel, illetve az ldapmodify-hoz hasonló LDAP alkalmazás és LDIF fájlok együttesével kezelhető. Az új objektumosztályok és attribútumok első meghatározásakor kényelmesebb lehet a webes adminisztrációs eszköz használata. Ha át kell másolnia az új sémát más szerverekre (például egy bevezetendő termék vagy eszköz részeként), akkor az ldapmodify segédprogram hasznosabb lehet. További információk: "Séma átmásolása más szerverekre" oldalszám: 167.

További információk:

- "Objektumosztályok megjelenítése" oldalszám: 158
- "Objektumosztály hozzáadása" oldalszám: 158
- "Objektumosztály módosítása" oldalszám: 159
- "Objektumosztály másolása" oldalszám: 161
- "Objektumosztály törlése" oldalszám: 162
- "Attribútumok megjelenítése" oldalszám: 162

- “Attribútum hozzáadása” oldalszám: 163
- “Attribútum módosítása” oldalszám: 164
- “Attribútum másolása” oldalszám: 165
- “Attribútum törlése” oldalszám: 167

Objektumosztályok megjelenítése

A séma objektumosztályait a webes adminisztrációs eszközzel (ez a javasolt módszer), valamint a parancssorból tekintheti meg.

Webes adminisztráció

Bontsa ki a navigációs terület **Sémakezelés** kategóriáját, majd kattintson az **Objektumosztályok kezelése** lehetőségre. Megjelenik egy csak olvasható ablak, amelyben megtekintheti a séma objektumosztályait és azok jellemzőit. Az objektumosztályok ábécérendbe szedve jelennek meg. Az egyes oldalak között az Előző és Következő gombokkal lépkedhet. A gombok melletti mező azonosítja az éppen megjelenített oldalt. Használhatja a mező melletti legördülő menüt is egy megadott oldalra ugráshoz. Az oldalon látható első objektumosztály mellett egy oldalszám látható, amely segít a megjeleníteni kívánt objektumosztály gyorsabb kikeresésében. Ha például a **person** objektumosztályt keresi, akkor nyissa meg a legördülő menüt és görgesse le addig, amíg nem látja a **14/16. oldal, nsLiServer** és a **15/16. oldal, printerLPR** elemeket. Mivel a person szó ábécérendben az nsLiServer és a printerLPR közé esik, válassza ki a 14. oldalt, majd kattintson az **Ugrás** gombra.

Megjelenítheti típus szerint rendezve is az objektumosztályokat. Válassza ki a **Típus** lehetőséget, majd kattintson a **Rendezés** gombra. Az objektumosztályok ábécérendben jelennek meg típusaik (absztrakt, kiegészítő, strukturális) szerint. Hasonló módon, meg is fordíthatja a listázás sorrendjét, ha a **Csökkenő**, majd a **Rendezés** lehetőségekre kattint.

Megtalálva a kívánt objektumosztályt, megtekintheti annak típusát, öröklődését, valamint kötelező és elhagyható attribútumait. Az öröklődés, illetve a kötelező és elhagyható attribútumok legördülő menüinek kibontásával tekintheti meg az egyes jellemzők teljes listáját.

A végrehajtani kívánt objektumosztály-műveleteket a jobboldali eszköztárból választhatja ki, például:

- Hozzáadás
- Módosítás
- Másolás
- Törlés

Ha készen van, kattintson a **Bezárás** gombra. Visszatér az IBM Directory Server **Üdvözet** ablakába.

Parancssor

A séma objektumosztályainak megtekintéséhez adja ki az alábbi parancsot:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Objektumosztály hozzáadása

Webes adminisztráció

Ha még nem tette volna meg, bontsa ki a navigációs terület **Sémakezelés** kategóriáját, majd kattintson az **Objektumosztályok kezelése** lehetőségre. Egy új objektumosztály létrehozása:

1. Kattintson a **Hozzáadás** gombra.

Megjegyzés: Az ablakot a navigációs terület **Sémakezelés** kategóriájának kibontásával, majd az **Objektumosztály hozzáadása** lehetőségre kattintással is elérheti.

2. Az **Általános tulajdonságok** lapon:

- Írja be az **Objektumosztály nevét**. Ez egy kötelező mező és az objektumosztály funkciójára utal. Például a **tempEmployee** objektumosztály jelképezheti az ideiglenes alkalmazottakat.
 - Adja meg az objektumosztály **Leírását**, mint például **Az ideiglenes alkalmazottakhoz használt objektumosztály**.
 - Adja meg az objektumosztály **objektumazonosítóját** (OID). Ez egy kötelező mező. Részletek: “Objektumazonosító (OID)” oldalszám: 26. Ha nincs még OID, akkor használhatja az **objektumosztály nevét**, amelyhez az **-oid** betűket fűzi. Ha például az objektumosztály neve **tempEmployee**, akkor az objektumazonosító **tempEmployee-oid**. A mező értéke módosítható.
 - Válasszon ki egy **Felettes objektumosztályt** a legördülő listából. Ez határozza meg, hogy melyik objektumosztályból öröklődnek az attribútumok. A **Felettes objektumosztály** általában a **top**, de másik objektumosztály is lehet. A **tempEmployee** felettes objektumosztálya lehet például az **ePerson**.
 - Adja meg az **Objektumosztály típusát**. Az objektumosztály-típusokkal kapcsolatos további információk: “Objektumosztályok” oldalszám: 18.
 - Az Attribútumok lapra kattintva adhatja meg az objektumosztály kötelező és elhagyható attribútumait és tekintheti meg az öröklött attribútumokat. Az **OK** gombra kattintva veheti fel az új objektumosztályt, a **Mégse** gombra kattintva pedig visszatérhet az **Objektumosztály kezelése** részhez további módosítások nélkül.
3. Az **Attribútumok** lapon:
- Válasszon ki egy attribútumot a **Rendelkezésre álló attribútumok** listájából, majd kattintson a **Kötelezőkhöz hozzáadás** gombra az attribútum kötelezővé tételéhez, illetve kattintson az **Elhagyhatókhoz hozzáadás** gombra az attribútum elhagyhatóvá tételéhez az adott objektumosztályra vonatkozóan. Az attribútum a kijelölt attribútumok megfelelő listájában jelenik meg.
 - Ismételje meg az eljárást az összes kiválasztani kívánt attribútumra.
 - Az attribútumok átmozgathatók az egyik listából a másikba, illetve törölhetők az adott listából kiválasztva őket és a megfelelő **Áthelyezés** vagy **Törlés** gombra kattintva.
 - Megtekinthető a kötelező és elhagyható öröklött attribútumok listája. Az öröklött attribútumok az **Általános** lapon megadott **Felettes objektumosztálytól** függenek. Az öröklött attribútumok nem módosíthatók. Az **Általános** lap **Felettes objektumosztály** értékének módosításával azonban az öröklött képernyő egy másik halmaza jeleníthető meg.
4. Az **OK** gombra kattintva veheti fel az új objektumosztályt, a **Mégse** gombra kattintva pedig visszatérhet az **Objektumosztály kezelése** részhez további módosítások nélkül.

Megjegyzés: Ha az **Általános** lapon az **OK** gombra kattintott további attribútumok hozzáadása nélkül, akkor az új objektumosztály módosításával vehet fel további attribútumokat.

Parancssor

EGy objektumosztály a parancssorból az alábbi paranccsal vehető fel:

```
ldapmodify -D <adminDN> -w <admin_jelszó> -i
<fájlnev>
```

ahol a <fájlnev> nevű fájl az alábbiakat tartalmazza:

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: ( <myObjectClass-oid> NAME '<myObjectClass>' DESC '<Egy
objektumosztály az LDAP alkalmazáshoz>' SUP '<objectclassinheritance>'
<objectclasstype> MAY (<attribute1> $ <attribute2>))
```

Objektumosztály módosítása

Nem minden sémamódosítás megengedett. További részletek a módosítások korlátozásairól: “Nem engedélyezett sémamódosítások” oldalszám: 28.

Webes adminisztráció

Ha még nem tette volna meg, bontsa ki a navigációs terület **Sémakezelés** kategóriáját, majd kattintson az **Objektumosztályok kezelése** lehetőségre. Egy objektumosztály módosítása:

1. Kattintson a módosítani kívánt objektumosztály melletti választógombra.
2. Kattintson a **Módosítás** gombra.
3. Válasszon ki egy lapot:
 - Az **Általános** lapon az alábbiakat végezheti el:
 - A **Leírás** módosítása.
 - A **Felettes objektumosztály** módosítása. Válasszon ki egy Felettes objektumosztályt a legördülő listából. Ez határozza meg, hogy melyik objektumosztályból öröklődnek az attribútumok. A **Felettes objektumosztály** általában a **top**, de másik objektumosztály is lehet. A **tempEmployee** felettes objektumosztálya lehet például az **ePerson**.
 - Az **Objektumosztály típusának** megváltoztatása. Válasszon ki egy objektumosztály-típust. Az objektumosztály-típusokkal kapcsolatos további információk: “Objektumosztályok” oldalszám: 18.
 - Az Attribútumok lapra kattintva módosíthatja az objektumosztály kötelező és elhagyható attribútumait és tekintheti meg az öröklött attribútumokat. Az **OK** gombra érvényesítheti a módosításokat, a **Mégse** gombra kattintva pedig visszatérhet az **Objektumosztály kezelése** részhez további módosítások nélkül.
 - Az **Attribútumok** lapon:

Válasszon ki egy attribútumot a **Rendelkezésre álló attribútumok** listájából, majd kattintson a **Kötelezőkhöz hozzáadás** gombra az attribútum kötelezővé tételéhez, illetve kattintson az **Elhagyhatókhoz hozzáadás** gombra az attribútum elhagyhatóvá tételéhez az adott objektumosztályra vonatkozóan. Az attribútum a kijelölt attribútumok megfelelő listájában jelenik meg.

Ismételje meg az eljárást az összes kiválasztani kívánt attribútumra.

Az attribútumok átmozgathatók az egyik listából a másikba, illetve törölhetők az adott listákból kiválasztva őket és a megfelelő **Áthelyezés** vagy **Törlés** gombra kattintva.

Megtekinthető a kötelező és elhagyható öröklött attribútumok listája. Az öröklött attribútumok az **Általános** lapon megadott **Felettes objektumosztálytól** függenek. Az öröklött attribútumok nem módosíthatók. Az **Általános** lap **Felettes objektumosztály** értékének módosításával azonban az öröklött képernyő egy másik halmaza jeleníthető meg.
4. Az **OK** gombra kattintva érvényesítheti a módosításokat. A **Mégse** gombra kattintva pedig visszatérhet az **Objektumosztály kezelése** részhez további módosítások nélkül.

Parancssor

A séma objektumosztályainak megtekintéséhez adja ki az alábbi parancsot:

```
ldpsearch -b cn=schema -s base objectclass=* objectclasses
```

Egy objektumosztály a parancssorból az alábbi paranccsal módosítható:

```
ldpmodify -D <adminDN> -w <admin_jelszó> -i  
<fájlnev>
```

ahol a <fájlnev> nevű fájl az alábbiakat tartalmazza:

```
dn: cn=schema  
changetype: modify  
replace: objectclasses  
objectclasses: ( <myobjectClass-oid> NAME  
'<myObjectClass>' DESC  
'<Egy objektumosztály az LDAP alkalmazáshoz>'  
SUP '<új_felettes_objektumosztály>'  
          <új_objektumosztály_típus> MAY  
(attribute1) $ <attribute2>  
          $ <új_attribute3> )
```


Objektumosztály másolása

Webes adminisztráció

Ha még nem tette volna meg, bontsa ki a navigációs terület **Sémakezelés** kategóriáját, majd kattintson az **Objektumosztályok kezelése** lehetőségre. Egy objektumosztály másolása:

1. Kattintson a másolni kívánt objektumosztály melletti választógombra.
2. Kattintson a **Másolás** gombra.
3. Válasszon ki egy lapot:
 - Az **Általános** lapon az alábbiakat végezheti el:
 - Az **Objektumosztály nevének** módosítása. Az alapértelmezett név az átmásolt objektumosztály neve, kiegészítve a COPY szóval. Például a **tempPerson tempPersonCOPY** néven kerül átmásolásra.
 - A **Leírás** módosítása.
 - Módosítsa az **Objektumazonosítót**. Az alapértelmezett objektumazonosító az átmásolt objektumosztály neve, kiegészítve a COPY szóval. Például a **tempPerson-oid tempPerson-oidCOPY** néven kerül átmásolásra.
 - A **Felettes objektumosztály** módosítása. Válasszon ki egy felettes objektumosztályt a legördülő listából. Ez határozza meg, hogy melyik objektumosztályból öröklődnek az attribútumok. A **Felettes objektumosztály** általában a **top**, de másik objektumosztály is lehet. A **tempEmployeeCOPY** felettes objektumosztálya lehet például az **ePerson**.
 - Az **Objektumosztály típusának** megváltoztatása. Válasszon ki egy objektumosztály-típust. Az objektumosztály-típusokkal kapcsolatos további információk: “Objektumosztályok” oldalszám: 18.
 - Az **Attribútumok** lapra kattintva módosíthatja az objektumosztály kötelező és elhagyható attribútumait és tekintheti meg az öröklött attribútumokat. Az **OK** gombra érvényesítheti a módosításokat, a **Mégse** gombra kattintva pedig visszatérhet az **Objektumosztály kezelése** részhez további módosítások nélkül.
 - Az **Attribútumok** lapon:

Válasszon ki egy attribútumot a **Rendelkezésre álló attribútumok** listájából, majd kattintson a **Kötelezőkhöz hozzáadás** gombra az attribútum kötelezővé tételéhez, illetve kattintson az **Elhagyhatókhoz hozzáadás** gombra az attribútum elhagyhatóvá tételéhez az adott objektumosztályra vonatkozóan. Az attribútum a kijelölt attribútumok megfelelő listájában jelenik meg.

Ismételje meg az eljárást az összes kiválasztani kívánt attribútumra.

Az attribútumok átmozgathatók az egyik listából a másikba, illetve törölhetők az adott listából kiválasztva őket és a megfelelő **Áthelyezés** vagy **Törlés** gombra kattintva.

Megtekinthető a kötelező és elhagyható öröklött attribútumok listája. Az öröklött attribútumok az **Általános** lapon megadott **Felettes objektumosztálytól** függenek. Az öröklött attribútumok nem módosíthatók. Az **Általános** lap **Felettes objektumosztály** értékének módosításával azonban az öröklött képernyő egy másik halmaza jeleníthető meg.
4. Az **OK** gombra kattintva érvényesítheti a módosításokat. A **Mégse** gombra kattintva pedig visszatérhet az **Objektumosztály kezelése** részhez további módosítások nélkül.

Parancssor

A séma objektumosztályainak megtekintéséhez adja ki az alábbi parancsot:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Válassza ki a másolni kívánt objektumosztályt. Egy szerkesztővel módosítsa a kívánt információkat, majd mentse el a változásokat a <fájlnév> nevű fájlba. Adja ki a következő parancsot:

```
ldapmodify -D  
<adminDN> -w <admin_jelszó> -i <fájlnév>
```

ahol a <fájlnév> nevű fájl az alábbiakat tartalmazza:

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( <mynewobjectClass-oid> NAME
'<mynewObjectClass>'
DESC '<Egy új objektumosztály,
amelyet az LDAP alkalmazáshoz másoltam át>'
SUP '<superiorclassobject>'<objectclasstype> MAY (attribute1>
$ <attribute2> $ <attribute3> ) )
```

Objektumosztály törlése

Nem minden sémamódosítás megengedett. További részletek a módosítások korlátozásairól: “Nem engedélyezett sémamódosítások” oldalszám: 28.

Webes adminisztráció

Ha még nem tette volna meg, bontsa ki a navigációs terület **Sémakezelés** kategóriáját, majd kattintson az **Objektumosztályok kezelése** lehetőségre. Egy objektumosztály törlése:

1. Kattintson a törölni kívánt objektumosztály melletti választógombra.
2. Kattintson a **Törlés** gombra.
3. Megjelenik egy megerősítést kérő kérdés az objektumosztály törlésére vonatkozóan. Az **OK** gombra kattintva törölheti az objektumosztályt, a **Mégse** gombra kattintva pedig visszatérhet az **Objektumosztály kezelése** részhez további módosítások nélkül.

Parancssor

A séma objektumosztályainak megtekintéséhez adja ki az alábbi parancsot:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Válassza ki a törölni kívánt objektumosztályt, majd adja ki a következő parancsot:

```
ldapmodify -D <adminDN> -w <admin_jelszó> -i
<fájlnev>
```

ahol a <fájlnev> nevű fájl az alábbiakat tartalmazza:

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: (<myobjectClass-oid>)
```

Attribútumok megjelenítése

A séma attribútumait a webes adminisztrációs eszközzel (ez a javasolt módszer), valamint a parancssorból tekintheti meg.

Webes adminisztráció

Bontsa ki a navigációs terület **Sémakezelés** kategóriáját, majd kattintson az **Attribútumok kezelése** lehetőségre. Megjelenik egy csak olvasható ablak, amelyben megtekintheti a séma attribútumait és azok jellemzőit. Az attribútumok ábécérendbe szedve jelennek meg. Az egyes oldalak között az Előző és Következő gombokkal lépkedhet. A gombok melletti mező azonosítja az éppen megjelenített oldalt. Használhatja a mező melletti legördülő menüt is egy megadott oldalra ugráshoz. Az oldalon látható első objektumosztály mellett egy oldalszám látható, amely segít a megjeleníteni kívánt objektumosztály gyorsabb kikeresésében. Ha például az **authenticationUserID** objektumosztályt keresi, akkor nyissa meg a legördülő menüt és görgesse le addig, amíg nem látja a **3/62. oldal, applSystemHint** és a **4/62. oldal, authorityRevocatonList** elemeket. Mivel az authenticationUserID szó ábécérendben az applSystemHint és az authorityRevocatonList közé esik, válassza ki a 3. oldalt, majd kattintson az **Ugrás** gombra.

Megjelenítheti típus szerint rendezve is az attribútumokat. Válassza ki a **Típus** lehetőséget, majd kattintson a **Szintaxis** gombra. Az attribútumok szintaxisukon belül ábécérendbe szedve jelennek meg. Az egyes szintaktikai típusok felsorolását itt találja: "Attribútum-szintaxis" oldalszám: 25. Hasonló módon, meg is fordíthatja a listázás sorrendjét, ha a **Csökkenő**, majd a **Rendezés** lehetőségekre kattint.

Megtalálva a kívánt attribútumot, megjelenítheti annak szintaxisát, azt, hogy többértékű-e, illetve az őt tartalmazó objektumosztályokat. Bontsa ki az objektumosztályok legördülő menüjét, ha látni akarja az attribútum objektumosztályainak listáját.

Ha készen van, kattintson a **Bezárás** gombra. Visszatér az IBM Directory Server **Üdvözlő** ablakába.

Parancssor

A séma attribútumainak megtekintéséhez adja ki az alábbi parancsot:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Attribútum hozzáadása

Új attribútum az alábbi módszerek egyikével hozható létre. A javasolt módszer a webes adminisztrációs eszköz használata.

Webes adminisztráció

Ha még nem tette volna meg, bontsa ki a navigációs terület **Sémakezelés** kategóriáját, majd kattintson az **Attribútumok kezelése** lehetőségre. Egy új attribútum létrehozása:

1. Kattintson a **Hozzáadás** gombra.

Megjegyzés: Az ablakot a navigációs terület **Sémakezelés** kategóriájának kibontásával, majd az **Attribútum hozzáadása** lehetőségre kattintással is elérheti.

2. Adja meg az **Attribútum nevét**, például: **tempId**. Ez egy kötelező mező, amelynek értéke egy betű karakterrel kell, hogy kezdődjön.
3. Adja meg az attribútum **Leírását**, mint például **Az ideiglenes alkalmazottak azonosítószámaként használt attribútum**.
4. Adja meg az attribútum **objektumazonosítóját** (OID). Ez egy kötelező mező. Részletek: "Objektumazonosító (OID)" oldalszám: 26. Ha nincs még OID, akkor megadható úgy is, hogy az attribútum nevéhez az -oid betűket fűzi. Ha például az attribútum neve **tempID**, akkor az alapértelmezett objektumazonosító a **tempID-oid**. A mező értéke módosítható.
5. Válasszon ki egy **Felettes attribútumot** a legördülő listából. A felettes attribútum az az attribútum, amelyből a tulajdonságok öröklődnek.
6. Válasszon ki egy **Szintaxist** a legördülő listából. A szintaxissal kapcsolatos további információk: "Attribútum-szintaxis" oldalszám: 25.
7. Adja meg az **Attribútumhossz** értékét, vagyis az attribútum maximális hosszát. A hossz byte-ok számában van megadva.
8. Jelölje meg a **Több érték engedélyezése** négyzetet, ha többértékű is lehet az attribútum.
9. Válasszon ki egy megfeleltetési szabályt a legördülő menüből az egyenlőség, a sorrendezés és a részkarakterlánc megfeleltetési szabályokhoz. A megfeleltetési szabályok teljes listája itt található: "Megfeleltetési szabályok" oldalszám: 22.
10. Az **IBM kiterjesztések** lapra kattintva adhatja meg az attribútum speciális kiterjesztéseit. Az **OK** gombra kattintva veheti fel az új attribútumot, a **Mégse** gombra kattintva pedig visszatérhet az **Attribútum kezelése** részhez további módosítások nélkül.
11. Az **IBM kiterjesztések** lapon:
 - A **DB2 táblanév módosítása**. A szerver maga állítja elő a DB2 táblanevet, ha ez a mező üresen marad. Ha beír egy DB2 táblanevet, akkor be kell írnia egy DB2 oszlopnevet is.

- A **DB2 oszlopnév módosítása**. A szerver maga állítja elő a DB2 oszlopnevet, ha ez a mező üresen marad. Ha beír egy DB2 oszlopnevet, akkor be kell írnia egy DB2 táblanevet is.
- A **Biztonsági osztály** beállítása: válassza ki a legördülő listából a **normál**, **bizalmas** vagy **kritikus** értéket.
- Az **Indexelési szabályok** beállítása: válasszon ki egy vagy több indexelési szabályt. Az indexelési szabályokkal kapcsolatos további információk: “Indexelési szabályok” oldalszám: 24.

Megjegyzés: Célszerű legalább egyenlőségi index készítését megadni a keresési szűrőkben használt attribútumokra.

12. Az **OK** gombra kattintva veheti fel az új attribútumot, a **Mégse** gombra kattintva pedig visszatérhet az **Attribútumok kezelése** részhez további módosítások nélkül.

Megjegyzés: Ha az Általános lapon az OK gombra kattintott további kiterjesztések hozzáadása nélkül, akkor az új attribútum módosításával vehet fel további kiterjesztéseket.

Parancssor

Az alábbi példa felvesz egy attribútumtípus-meghatározást a "myAttribute" nevű attribútumhoz, Directory String szintaxissal (magyarázat: “Attribútum-szintaxis” oldalszám: 25) és Kis- és nagybetű egyezés figyelmen kívül hagyása egyeztetéssel (részletek: “Megfeleltetési szabályok” oldalszám: 22). A meghatározás IBM-specifikus része azt adja meg, hogy az attribútumadatok egy a "myAttrTable" tábla "myAttrColumn" nevű oszlopában kerüljenek tárolásra. Ha ezek a nevek nincsenek megadva, akkor az oszlop- és táblanév egyformán "myAttribute" lesz alapértelmezés szerint. Az attribútum "normál" hozzáférési osztályba kerül, és az értékei nem lehetnek 200 byte-nál hosszabbak.

```
ldapmodify -D <adminDn> -w <adminpw> -i myschema.ldif
```

ahol a **myschema.ldif** fájl tartalma:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' )
DESC 'Az LDAP alkalmazáshoz definiált attribútum'
EQUALITY 2.5.13.2 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oid DBNAME ( 'myAttrTable' 'myAttrColumn' )
ACCESS-CLASS normal LENGTH 200 )
```

A paranccsal kapcsolatos további információk: “ldapmodify és ldapadd” oldalszám: 191.

Attribútum módosítása

Nem minden sémamódosítás megengedett. További részletek a módosítások korlátozásairól: “Nem engedélyezett sémamódosítások” oldalszám: 28.

Mielőtt az adott attribútumot használó bejegyzéseket venne fel, a meghatározás bármely része módosítható. Az attribútum az alábbi módszerek egyikével módosítható. A javasolt módszer a webes adminisztrációs eszköz használata.

Webes adminisztráció

Ha még nem tette volna meg, bontsa ki a navigációs terület **Sémakezelés** kategóriáját, majd kattintson az **Attribútumok kezelése** lehetőségre. Egy attribútum módosítása:

1. Kattintson a módosítani kívánt attribútum melletti választógombra.
2. Kattintson a **Módosítás** gombra.
3. Válasszon ki egy lapot:
 - Az **Általános** lapon az alábbiakat végezheti el:
 - Válasszon ki egy lapot:

- **Általános:**
 - A **Leírás** módosítása
 - A **szintaxis** módosítása
 - Az **Attribútumhossz** beállítása
 - A **Több érték** beállítás módosítása
 - Egy **megfeleltetési szabály** megadása
 - A **Feltes attribútum** módosítása
 - Az **IBM kiterjesztések** lapra kattintva módosíthatja az attribútum speciális kiterjesztéseit. Az **OK** gombra kattintva érvényesítheti a módosításokat, a **Mégse** gombra kattintva pedig visszatérhet az **Attribútum kezelése** részhez további módosítások nélkül.
 - **IBM kiterjesztések:** ha az IBM Directory Server-t használja, az alábbiakhoz:
 - A **Biztonsági osztály** módosítása
 - Az **Indexelési szabályok** módosítása
 - Az **OK** gombra kattintva érvényesítheti a módosításokat. A **Mégse** gombra kattintva pedig visszatérhet az **Attribútumok kezelése** részhez további módosítások nélkül.
4. Az **OK** gombra kattintva érvényesítheti a módosításokat. A **Mégse** gombra kattintva pedig visszatérhet az **Attribútumok kezelése** részhez további módosítások nélkül.

Parancssor

Az alábbi példa indexeléssel bővíti az attribútumot, hogy a keresések gyorsabban történjenek. Használja az `ldapmodify` parancsot és egy LDIF fájlt a meghatározás módosításához:

```
ldapmodify -D <adminDn> -w <adminpw> -i myschemachange.ldif
```

ahol a **myschemachange.ldif** fájl tartalma:

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' ) DESC 'Az LDAP alkalmazáshoz
                 definiált attribútum' EQUALITY 2.5.13.2
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
replace: ibmattributetypes
ibmattributetypes: ( myAttribute-oid DBNAME ( 'myAttrTable' 'myAttrColumn' )
                   ACCESS-CLASS normal LENGTH 200 EQUALITY SUBSTR )
```

Megjegyzés: A meghatározás mindkét részének (**attributetypes** és **ibmattributetypes**) szerepelnie kell a csere műveletben, még akkor is, ha csak az **ibmattributetypes** szakasz módosul. Az egyetlen változás valójában az "EQUALITY SUBSTR" hozzáadása a meghatározás végéhez, amely egyenlőségi és részkarakterlánc-egyezési indexeket kér.

A parancsal kapcsolatos további információk: "ldapmodify és ldapadd" oldalszám: 191.

Attribútum másolása

Az attribútum az alábbi módszerek egyikével másolható. A javasolt módszer a webes adminisztrációs eszköz használata.

Webes adminisztráció

Ha még nem tette volna meg, bontsa ki a navigációs terület **Sémakezelés** kategóriáját, majd kattintson az **Attribútumok kezelése** lehetőségre. Egy attribútum másolása:

1. Kattintson a másolni kívánt attribútum melletti választógombra.
2. Kattintson a **Másolás** gombra.

3. Módosítsa az **Attribútum nevé**t. Az alapértelmezett név az átmásolt attribútum neve, kiegészítve a COPY szóval. Például a **tempID tempIDCOPY** néven kerül átmásolásra.
4. Módosítsa az attribútum **Leírását**, mint például **Az ideiglenes alkalmazottak azonosítószámaként használt attribútum**.
5. Change the **OID**. Az alapértelmezett objektumazonosító az átmásolt attribútum OID neve, kiegészítve a COPYOID szóval. Például a **tempID-oid tempID-oidCOPYOID** néven kerül átmásolásra.
6. Válasszon ki egy **Felettes attribútumot** a legördülő listából. A felettes attribútum az az attribútum, amelyből a tulajdonságok öröklődnek.
7. Válasszon ki egy **Szintaxist** a legördülő listából. A szintaxissal kapcsolatos további információk: "Attribútum-szintaxis" oldalszám: 25.
8. Adja meg az **Attribútumhossz** értékét, vagyis az attribútum maximális hosszát. A hossz byte-ok számában van megadva.
9. Jelölje meg a **Több érték engedélyezése** négyzetet, ha többértékű is lehet az attribútum.
10. Válasszon ki egy megfeleltetési szabályt a legördülő menüből az egyenlőség, a sorrendezés és a részkarakterlánc megfeleltetési szabályokhoz. A megfeleltetési szabályok teljes listája itt található: "Megfeleltetési szabályok" oldalszám: 22.
11. Az **IBM kiterjesztések** lapra kattintva módosíthatja az attribútum speciális kiterjesztéseit. Az **OK** gombra kattintva érvényesítheti a módosításokat, a **Mégse** gombra kattintva pedig visszatérhet az **Attribútum kezelése** részhez további módosítások nélkül.
12. Az **IBM kiterjesztések** lapon:
 - A **DB2 táblané**v módosítása. A szerver maga állítja elő a DB2 táblanevet, ha ez a mező üresen marad. Ha beír egy DB2 táblanevet, akkor be kell írnia egy DB2 oszlopnevet is.
 - A **DB2 oszlopne**v módosítása. A szerver maga állítja elő a DB2 oszlopnevet, ha ez a mező üresen marad. Ha beír egy DB2 oszlopnevet, akkor be kell írnia egy DB2 táblanevet is.
 - A **Biztonsági osztály** módosítása: válassza ki a legördülő listából a **normál**, **bizalmas** vagy **kritikus** értéket.
 - Az **Indexelési szabályok** módosítása: válasszon ki egy vagy több indexelési szabályt. Az indexelési szabályokkal kapcsolatos további információk: "Indexelési szabályok" oldalszám: 24.

Megjegyzés: Célszerű legalább egyenlőségi index készítését megadni a keresési szűrőkben használt attribútumokra.
13. Az **OK** gombra kattintva érvényesítheti a módosításokat. A **Mégse** gombra kattintva pedig visszatérhet az **Attribútumok kezelése** részhez további módosítások nélkül.

Megjegyzés: Ha az **Általános** lapon az **OK** gombra kattintott további kiterjesztések hozzáadása nélkül, akkor az új attribútum módosításával vehet fel további kiterjesztéseket.

Parancssor

A séma attribútumainak megtekintéséhez adja ki az alábbi parancsot:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes
IBMAttributeTypes
```

Válassza ki a másolni kívánt attribútumot. Egy szerkesztővel módosítsa a kívánt információkat, majd mentse el a változásokat a <fájlnév> nevű fájlba. Ezután adja ki a következő parancsot:

```
ldapmodify -D <adminDN> -w <admin_jelszó> -i
<fájlnév>
```

ahol a <fájlnév> nevű fájl az alábbiakat tartalmazza:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( <mynewAttribute-oid> NAME
'<mynewAttribute>' DESC
```

```
'<Egy új
    attribútum, az LDAP alkalmazáshoz átmásolva> EQUALITY
2.5.13.2
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications
)
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oid DBNAME ( 'myAttrTable' 'myAttrColumn' )
    ACCESS-CLASS normal LENGTH 200 )
```

Attribútum törlése

Nem minden sémamódosítás megengedett. További részletek a módosítások korlátozásairól: “Nem engedélyezett sémamódosítások” oldalszám: 28.

Az attribútum az alábbi módszerek egyikével törölhető. A javasolt módszer a webes adminisztrációs eszköz használata.

Webes adminisztráció

Ha még nem tette volna meg, bontsa ki a navigációs terület **Sémakezelés** kategóriáját, majd kattintson az **Attribútumok kezelése** lehetőségre. Egy attribútum törlése:

1. Kattintson a törölni kívánt attribútum melletti választógombra.
2. Kattintson a **Törlés** gombra.
3. Megjelenik egy megerősítést kérő kérdés az attribútum törlésére vonatkozóan. Az **OK** gombra kattintva törölheti attribútumot, a **Mégse** gombra kattintva pedig visszatérhet az **Attribútumok kezelése** részhez további módosítások nélkül.

Parancssor

```
ldapmodify -D <adminDn> -w <adminpw> -i myschemadelete.ldif
```

ahol a **myschemadelete.ldif** fájl tartalma:

```
dn: cn=schema
changetype: modify
delete: attributetypes
attributetypes: (<myAttribute-oid>)
```

A paranccsal kapcsolatos további információk: “ldapmodify és ldapadd” oldalszám: 191.

Séma átmásolása más szerverekre

A séma más szerverekre átmásolásának lépései:

1. Az ldapsearch segédprogrammal másolja ki a sémát egy fájlba:

```
ldapsearch -b cn=schema -L "(objectclass=*)" > schema.ldif
```
2. A sémafájl tartalmazza az összes objektumosztályt és attribútumot. Szerkessze át az LDIF fájlt, hogy csak a kívánt sémaelemeket tartalmazza. Másik megoldás lehet az ldapsearch program kimenetének szűrése a grep-hez hasonló eszközzel. Ne felejtse el az attribútumokat a rájuk hivatkozó objektumosztályok elé írni. Előállhat például a következő fájl (figyelje meg, hogy minden folytatott sornak van egy szóköz a végén és minden folytató sor legalább egy szóközzel kezdődik).

```
attributetypes:
( myattr1-oid NAME 'myattr1' DESC 'Némi
    információ.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
    USAGE userApplications )
IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1' 'myattr1' )
    ACCESS-CLASS normal LENGTH 500 )
attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Némi
    információ.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
    USAGE userApplications )
IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2' 'myattr2' )
```

```
ACCESS-CLASS normal LENGTH 500 )
objectclasses: ( myobject-oid NAME 'myobject' DESC 'Ide is leírás
kerül.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

3. Szűrjön be sorokat az egyes objektumosztályok és attribútumtípusok elé, hogy létrehozza a cn=schema bejegyzés alá felveendő LDIF direktívákat. Minden objektumosztályt és attribútumot külön módosításként kell felvenni.

```
dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Némi
információ.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications )
IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1' 'myattr1' )
ACCESS-CLASS normal LENGTH 500 )
```

```
dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Némi
információ.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications )
IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2' 'myattr2' )
ACCESS-CLASS normal LENGTH 500 )
```

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( myobject-oid NAME 'myobject' DESC 'Ide is leírás
kerül.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

4. Töltse be a sémát más szervereken az ldapmodify segédprogrammal:

```
ldapmodify -D cn=administrator -w <jelszó> -f schema.ldif
```

Címtárbejegyzések kezelése

A címtárbejegyzések kezeléséhez bontsa ki a webes adminisztrációs eszköz navigációs területének **Címtárkezelés** kategóriáját.

További információk:

- “Címtárfa tallózása”
- “Bejegyzés hozzáadása” oldalszám: 169
- “Nyelvi címkékkel ellátott attribútumokat tartalmazó bejegyzés hozzáadása” oldalszám: 169
- “Felhasználók másolása HTTP szerver ellenőrzési listából a Directory Serverbe” oldalszám: 94
- “Bejegyzés törlése” oldalszám: 170
- “Bejegyzés módosítása” oldalszám: 170
- “Bejegyzés másolása” oldalszám: 171
- “Hozzáférés-felügyeleti listák módosítása” oldalszám: 171
- “Kiegészítő objektumosztály hozzáadása” oldalszám: 171
- “Kiegészítő osztály törlése” oldalszám: 172
- “Csoporrtagságok módosítása” oldalszám: 172
- “Címtárbejegyzések keresése” oldalszám: 172
- “Bináris attribútumok módosítása” oldalszám: 174

Címtárfa tallózása

Ha még nem tette volna meg, bontsa ki a navigációs terület **Címtárkezelés** kategóriáját, majd kattintson a **Bejegyzések kezelése** lehetőségre. Itt bonthatja ki a különböző részfákat és választhatja ki a kezelni kívánt elemet. A végrehajtani kívánt műveletet a jobboldali eszköztárból választhatja ki.

Bejegyzés hozzáadása

Ha még nem tette volna meg, bontsa ki a navigációs terület **Címtárkezelés** kategóriáját.

1. Kattintson a **Bejegyzés hozzáadása** lehetőségre.
2. Válasszon ki egy **Strukturális objektumosztályt** a legördülő listából.
3. Kattintson a **Tovább** gombra.
4. Válassza ki a rendelkezésre álló objektumosztályok mezőjéből a kívánt **Kiegészítő objektumosztályt**, majd kattintson a **Hozzáadás** gombra. Ismételje ezt meg minden felvenni kívánt kiegészítő objektumosztályra. Törölhet is egy kiegészítő objektumosztályt a Kiválasztott mezőből: jelölje ki és kattintson a **Törlés** gombra.
5. Kattintson a **Tovább** gombra.
6. A **Relatív DN** mezőben írja be a felvenni kívánt bejegyzés viszonylagos megkülönböztető nevét (RDN), például cn=John Doe.
7. A **Szülő DN** mezőbe írja be a kiválasztott fabejegyzés nevét, például ou=Austin, o=IBM. Kattinthat a **Tallózás** gombra is, ha a Szülő DN-t listából akarja kiválasztani. Ki is terjesztheti a kijelölést, ha a részfa alacsonyabb szintjeit is meg kívánja tekinteni. Adja meg a kiválasztott elemet, majd kattintson a **Kiválasztás** gombra a kívánt Szülő DN megadásához. A **Szülő DN** alapértelmezés szerint a fában kijelölt bejegyzés.

Megjegyzés: Ha ezt a feladatot a **Bejegyzések kezelése** ablakból indította, akkor ez a mező már előre ki van töltve.

8. A **Kötelező attribútumok** lapon írja be a kötelező attribútumok értékeit. Ha egynél több értéket akar megadni egy adott attribútumnak, akkor kattintson a **Többszörös érték** gombra, és írja be egyesével az értékeket.
9. Kattintson az **Elhagyható attribútumok** lapra.
10. Az **Elhagyható attribútumok** lapon írja be az elhagyható attribútumok értékeit. A bináris értékek felvételével kapcsolatos további információk: "Bináris attribútumok módosítása" oldalszám: 174. Ha egynél több értéket akar megadni egy adott attribútumnak, akkor kattintson a **Többszörös érték** gombra, és írja be egyesével az értékeket.
11. Kattintson az OK gombra a bejegyzés létrehozásához.
12. Az **ACL** gombra kattintva módosíthatja a bejegyzés hozzáférés-felügyeleti listáját. További információk az ACL-ekről: "Hozzáférés-felügyeleti listák" oldalszám: 56.
13. Legalább a kötelező mezők kitöltése után a **Hozzáadás** gombra kattintva veheti fel az új bejegyzést. A **Mégse** gombra kattintva visszatér a **Fa tallózása** részhez a címtár módosítása nélkül.

Nyelvi címkékkel ellátott attribútumokat tartalmazó bejegyzés hozzáadása

A címtárban nyelvi címkék rendelhetők az értékekhez, hogy a kliensek kereshessenek az egyes nyelvi követelményeket kielégítő értékek között. A nyelvi címke egy attribútumleírás egyik összetevője. A nyelvi címkékkel kapcsolatban további információk: "Nyelvi címkék" oldalszám: 44.

A nyelvi címkék engedélyezéséhez (alapértelmezésben ki vannak kapcsolva) tegye a következőket:

1. Kattintson a **Szervertulajdonságok kezelése** lehetőségre a navigációs terület **Szerveradminisztráció** kategóriájában.

Megjegyzés: A szerver konfigurációs beállításainak módosításához a webadminisztrációs eszköz Szerveradminisztrációs kategóriájának használatával hitelesítenie kell magát a szerverhez egy i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultságokkal. Ez úgy történhet, hogy hitelesíti magát leképezett felhasználóként az adott profil jelszavával. A kapcsolódáshoz a webes adminisztrációs eszközhöz leképezett felhasználóként adjon meg egy felhasználónevet a következő formában: os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, ahol a MYUSERNAME és MYSYSTEM.COM karaktorsorozatokat a saját felhasználói profiljának nevével és a beállított rendszerleképezési utótaggal helyettesíti.

2. Az Általános lap előre ki van választva. Az engedélyezéshez kattintson a **Nyelvi címkék támogatásának engedélyezése** jelölőnégyzetre.

Megjegyzés: A nyelvi címke szolgáltatás engedélyezése után, ha nyelvi címkéket rendel egy bejegyzés attribútumaihoz, a szerver visszaadja a nyelvi címkékkel rendelkező bejegyzést. Ez akkor is így történik, ha később kikapcsolja a nyelvi címke szolgáltatást. Mivel a szerver működése lehet, hogy nem egyezik meg azzal, amit az alkalmazás vár, és hogy a későbbi problémák megelőzhetőek legyenek, ha egyszer bekapcsolta, akkor már ne kapcsolja ki a nyelvi címke funkciót.

Egy nyelvi címkékkel rendelkező attribútumokat tartalmazó bejegyzés készítéséhez:

1. A navigációs terület **Címtárkezelés** kategóriájában kattintson a **Bejegyzések kezelése** lehetőségre.
2. Kattintson az **Attribútumok szerkesztése** gombra.
3. Válassza ki azt az attribútumot, amelyhez nyelvi címkét szeretne létrehozni.
4. Kattintson a **Nyelve címke értéke** gombra a **Nyelvi címke értékek** panel eléréséhez.
5. A **Nyelvi címke** mezőben adja meg a létrehozni kívánt címke nevét. A címkének a lang- toldalékkal kell kezdődnie.
6. Adja meg a címke értékét az **Érték** mezőben.
7. Kattintson a **Hozzáadás** gombra. A nyelvi címke és az érték megjelenik a menülistában.
8. Hozzon létre további nyelvi címkéket vagy módosítsa az attribútumok meglévő nyelvi címkéit a 3., 4. és 5. lépés ismétlésével. A kívánt nyelvi címkék létrehozása után kattintson az **OK** gombra.
9. Bontsa ki a **Megjelenítés nyelvi címkékkel** menüt és válasszon ki egy nyelvi címkét. Kattintson a **Nézet módosítása** lehetőségre és megjelennek a nyelvi címkékhez megadott attribútumértékek. Minden ebben a nézetben megadott érték csak a kiválasztott nyelvi címkére érvényes.
10. Ha kész, kattintson az **OK** gombra.

Bejegyzés törlése

Ha még nem tette volna meg, bontsa ki a navigációs terület **Címtárkezelés** kategóriáját, majd kattintson a **Bejegyzések kezelése** lehetőségre. Itt bonthatja ki a különböző részfákat és választhatja ki a kezelni kívánt részfát, utótagot vagy elemet. Kattintson a jobb oldali eszközsor **Törlés** elemére.

- Meg kell erősítenie a törlést. Kattintson az **OK** gombra.
- A bejegyzés törlésre kerül a könyvtárból és visszatér a bejegyzések listájához.

Bejegyzés módosítása

Ha még nem tette volna meg, bontsa ki a navigációs terület **Címtárkezelés** kategóriáját, majd kattintson a **Bejegyzések kezelése** lehetőségre. Itt bonthatja ki a különböző részfákat és választhatja ki a kezelni kívánt elemet. Kattintson a jobb oldali eszközsor **Attribútumok módosítása** elemére.

1. A **Kötelező attribútumok** lapon írja be a kötelező attribútumok értékeit. A bináris értékek felvételével kapcsolatos további információk: "Bináris attribútumok módosítása" oldalszám: 174. Ha egynél több értéket akar megadni egy adott attribútumnak, akkor kattintson a **Többszörös érték** gombra, és írja be egyesével az értékeket.
2. Kattintson az **Elhagyható attribútumok** lapra.
3. Az **Elhagyható attribútumok** lapon írja be az elhagyható attribútumok értékeit. Ha egynél több értéket akar megadni egy adott attribútumnak, akkor kattintson a **Többszörös érték** gombra, és írja be egyesével az értékeket.
4. Kattintson a **Tagságok** lapra.
5. Ha létrehozott már csoportokat, akkor a **Tagságok** lapon:
 - Válasszon ki egy csoportot a **Rendelkezésre álló csoportok** listájából, majd kattintson a **Hozzáadás** gombra, hogy a bejegyzés a kiválasztott **statikus csoport** tagja legyen.
 - A **Statikus csoporttagság** egyik csoportját kiválasztva és a **Törlés** gombra kattintva távolíthatja el a bejegyzést a kijelölt csoportból.
6. Ha a bejegyzés csoportbejegyzés, akkor a **Tagok** lap látható. A **Tagok** lapon láthatók a kiválasztott csoport tagjai. Szabadon vehet fel és törölhet csoporttagokat.
 - Egy tag felvétele a csoportba:
 - a. Vagy kattintson a **Tagok** lap **Többszörös érték** elemére, vagy a **Tagok** lapon kattintson a **Tagok** mezőre.

- b. A Tagok mezőbe írja be a felvenni kívánt bejegyzés DN-jét.
 - c. Kattintson a **Hozzáadás** gombra.
 - d. Kattintson az **OK** gombra.
- Egy tag törlése a csoportból:
 - a. Vagy kattintson a **Tagok** lap **Többszörös érték** elemére, vagy a **Tagok** lapon kattintson a **Tagok** mezőre.
 - b. Válassza ki a törölni kívánt bejegyzést.
 - c. Kattintson a **Törlés** gombra.
 - d. Kattintson az **OK** gombra.
 - A taglista frissítéséhez kattintson a **Frissítés** elemre.
7. Kattintson az **OK** gombra a bejegyzés módosításához.

Bejegyzés másolása

Ez a funkció akkor hasznos, ha hasonló bejegyzéseket hoz létre. A másolat az eredeti összes attribútumát megőröklí. Az új bejegyzés elnevezéséhez némi módosításokat végre kell hajtania.

Ha még nem tette volna meg, bontsa ki a navigációs terület **Címtárkezelés** kategóriáját, majd kattintson a **Bejegyzések kezelése** lehetőségre. Itt bonthatja ki a különböző részfákat és választhatja ki a kezelni kívánt elemet (például John Doe bejegyzését). Kattintson a jobb oldali eszközsor **Másolás** elemére.

- Módosítsa a DN mező RDN bejegyzését. Például írja át a cn=John Doe elemet cn=Jim Smith értékre.
- A kötelező attribútumok lapon módosítsa a cn bejegyzést az új RDN-re. Ez a jelen példában Jim Smith.
- Szükség szerint módosítsa a többi kötelező attribútumot. A jelen példában írja át az sn (vezetéknevez) attribútum értékét Doe-ról Smith-re.
- Ha kész a szükséges módosításokkal, akkor kattintson az **OK** gombra az új bejegyzés létrehozásához.
- Az új bejegyzés (Jim Smith) bekerül a bejegyzéslista legaljára.

Megjegyzés: Ez az eljárás csak a bejegyzés attribútumait másolja át. Az eredeti bejegyzés csoporttagságai nem másolódnak át az új bejegyzésbe. A tagságok felviteléhez használja az Attribútumok módosítása funkciót.

Hozzáférés-felügyeleti listák módosítása

További információk az ACL tulajdonságok megtekintéséről a webes adminisztrációs eszközzel, illetve az ACL-ek kezeléséről: “Hozzáférés-felügyeleti listák (ACL-ek) kezelése” oldalszám: 185.

További információk: “Hozzáférés-felügyeleti listák” oldalszám: 56.

Kiegészítő objektumosztály hozzáadása

A címtárfa egy már meglévő bejegyzéséhez az eszközsor **Kiegészítő osztály hozzáadása** gombjával vehet fel kiegészítő objektumosztályt. A kiegészítő objektumosztályok további attribútumok használatát teszik lehetővé.

Ha még nem tette volna meg, bontsa ki a navigációs terület **Címtárkezelés** kategóriáját, majd kattintson a **Bejegyzések kezelése** lehetőségre. Itt bonthatja ki a különböző részfákat és választhatja ki a kezelni kívánt elemet (például John Doe bejegyzését). Kattintson a jobb oldali eszközsor **Kiegészítő osztály hozzáadása** elemére.

1. Válassza ki a rendelkezésre álló objektumosztályok mezőjéből a kívánt **Kiegészítő objektumosztályt**, majd kattintson a **Hozzáadás** gombra. Ismételje ezt meg minden felvenni kívánt kiegészítő objektumosztályra. Törölhet is egy kiegészítő objektumosztályt a Kiválasztott mezőből: jelölje ki és kattintson a **Törlés** gombra.
2. A **Kötelező attribútumok** lapon írja be a kötelező attribútumok értékeit. Ha egynél több értéket akar megadni egy adott attribútumnak, akkor kattintson a **Többszörös érték** gombra, és írja be egyesével az értékeket.
3. Kattintson az **Elhagyható attribútumok** lapra.
4. Az **Elhagyható attribútumok** lapon írja be az elhagyható attribútumok értékeit. Ha egynél több értéket akar megadni egy adott attribútumnak, akkor kattintson a **Többszörös érték** gombra, és írja be egyesével az értékeket.

5. Kattintson a **Tagságok** lapra.
6. Ha létrehozott már csoportokat, akkor a **Tagságok** lapon:
 - Válasszon ki egy csoportot a **Rendelkezésre álló csoportok** listájából, majd kattintson a **Hozzáadás** gombra, hogy a bejegyzés a kiválasztott **statikus csoport** tagja legyen.
 - A **Statikus csoporttagság** egyik csoportját kiválasztva és a **Törlés** gombra kattintva távolíthatja el a bejegyzést a kijelölt csoportból.
7. Kattintson az **OK** gombra a bejegyzés módosításához.

Kiegészítő osztály törlése

Bár egy kiegészítő osztály törölhető a Kiegészítő osztály hozzáadása eljárás során is, egyszerűbb a Kiegészítő osztály törlése funkciót használni, ha csak egyetlen kiegészítő osztályt akar törölni egy bejegyzésből. Ha több kiegészítő osztályt akar törölni a bejegyzésből, akkor kényelmesebb lehet a Kiegészítő osztály hozzáadása funkció használata.

1. Ha még nem tette volna meg, bontsa ki a navigációs terület **Címtárkezelés** kategóriáját, majd kattintson a **Bejegyzések kezelése** lehetőségre. Itt bonthatja ki a különböző részfákat és választhatja ki a kezelni kívánt elemet (például John Doe bejegyzését). Kattintson a jobb oldali eszközsor **Kiegészítő osztály törlése** elemére.
2. A kiegészítő osztályok listájából válassza ki a törölni kívántat, majd kattintson az **OK** gombra.
3. A törlés jóváhagyásaként kattintson az **OK** gombra.
4. A kiegészítő osztály törlésre kerül és visszatér a bejegyzések listájához.

Ismételje meg az eljárást minden törölni kívánt kiegészítő osztályra.

Csoporttagságok módosítása

Ha még nem tette volna meg, bontsa ki a navigációs terület **Címtárkezelés** kategóriáját.

1. Kattintson a **Bejegyzések kezelése** lehetőségre.
2. Válassza ki a címtárfa egy felhasználóját, majd kattintson az eszköztár **Attribútumok módosítása** ikonjára.
3. Kattintson a **Tagságok** lapra.
4. A felhasználó tagságának módosítása: A **Tagság módosítása** ablakban látható a **Rendelkezésre álló csoportok** listája, amelybe a felhasználó felvehető, illetve a bejegyzés **Statikus csoporttagságai**.
 - Válasszon ki egy csoportot a **Rendelkezésre álló csoportok** listájából, majd kattintson a **Hozzáadás** gombra, hogy a bejegyzés a kiválasztott csoport tagja legyen.
 - A **Statikus csoporttagság** egyik csoportját kiválasztva és a **Törlés** gombra kattintva távolíthatja el a bejegyzést a kijelölt csoportból.
5. Az **OK** gombra kattintva elmentheti a változtatásokat. A **Mégse** gombra kattintva pedig visszatérhet az előző ablakba a módosítások elmentése nélkül.

Címtárbejegyzések keresése

Háromféle módon lehet keresni a címtárfaiban:

- Egyszerű kereséssel, előre meghatározott keresési feltételek szerint
- Összetett kereséssel, a felhasználó által megadott keresési feltételek szerint
- Kézi kereséssel

A keresési funkciók a navigációs terület **Címtárkezelés** kategóriájának kibontásával, majd a **Bejegyzések keresése** elemre kattintással érhetők el. Válassza ki vagy a **Keresési szűrők**, vagy a **Beállítások** lapot.

Megjegyzés: A bináris bejegyzésekre (például a jelszavakra) nem lehet keresni.

Keresési szűrők

Az alábbi keresési típusok közül választhat:

Egyszerű keresés

Az egyszerű keresés előre meghatározott keresési feltételeket használ:

- Az alap DN az **Összes utótag**
- A keresés hatóköre a **Részfa**
- A keresés mérete **Korlátlan**
- Az időkorlát **Korlátlan**
- Álnév-hivatkozás feloldása: **soha**
- Kapcsolatkövetések kikapcsolva (ki)

Egy egyszerű keresés végrehajtása:

1. A **Keresési szűrő** lapon kattintson az **Egyszerű keresés** lehetőségre.
2. Válasszon ki egy felettes objektumosztályt a legördülő listából.
3. Adjon meg egy attribútumot a kiválasztott bejegyzéstípushoz. Ha egy meghatározott attribútum alapján keres, akkor válassza ki az attribútumot a legördülő listából és írja be az attribútum értékét az **egyenlő** mezőbe. Ha nem ad meg attribútumot, akkor a keresés az adott bejegyzéstípusú összes címtárbejegyzést visszaadja.

Összetett keresés

Az összetett keresés során keresési megszorításokat adhat meg és használhat keresési szűrőket. Az alapértelmezett keresési feltételek alapján kereséshez használja az Egyszerű keresés funkciót.

- Egy összetett keresés végrehajtása:
 1. A **Keresési szűrő** lapon kattintson az **Összetett keresés** lehetőségre.
 2. Válasszon ki egy **attribútumot** a legördülő listából.
 3. Válasszon ki egy **Összehasonlítási** operátort
 - = Az attribútum egyenlő az értékkel.
 - ! Az attribútum nem egyenlő az értékkel.
 - < Az attribútum nem nagyobb az értéknél.
 - > Az attribútum nem kisebb az értéknél.
 - ~ Az attribútum megközelítőleg egyenlő az értékkel.
 4. Írja be az összehasonlításhoz tartozó **értéket**.
 5. Összetett lekérdezésekhez használja a keresési operátor gombokat.
 - Ha már legalább egy keresési szűrőt megadott, megadhat egy újabb feltételt, majd kattintson az **ÉS** lehetőségre. Az **ÉS** parancs hatására a mindkét keresési feltételnek eleget tevő bejegyzések kerülnek visszaadásra.
 - Ha már legalább egy keresési szűrőt megadott, megadhat egy újabb feltételt, majd kattintson a **VAGY** lehetőségre. Az **VAGY** parancs hatására a legalább az egyik keresési feltételnek eleget tevő bejegyzések kerülnek visszaadásra.
 6.
 - A **Hozzáadás** gombra kattintva veheti fel a keresési szűrő feltételt az összetett keresésbe.
 - A **Törlés** gombra kattintva törölheti a keresési szűrő feltételt az összetett keresésből.
 - A **Visszaállítás** gombra kattintva törölheti az összes keresési szűrőt.

Kézi keresés

Ezzel a módszerrel hozhat létre keresési szűrőket. Ha például a vezetéknevekre akar keresni, akkor írja be a mezőbe, hogy `sn=*`. Ha több attribútumra akar keresni, akkor a keresési szűrők szintaktikáját kell használnia. Ha például egy adott osztály vezetékneveire keres:

```
(&(sn=*)(dept=<osztály_neve>))
```

Beállítások

A **Beállítások** lapon:

- **Alap DN keresése** - Válassza ki a legördülő listából, hogy mely utótagon belül kíván keresni.

Megjegyzés: Ha ezt a feladatot a **Bejegyzések kezelése** ablakból indította, akkor ez a mező már előre ki van töltve. A **Szülő DN**-t már kiválasztotta, mielőtt a **Hozzáadás** gombbal elindította volna a bejegyzés felvételi folyamatát.

Az **Összes utótag** lehetőség kiválasztása esetén a teljes címtárfában keres.

Megjegyzés: Egy kiválasztott **Minden utótag** lehetőséggel együtt végzett részfa-keresés nem fog sémainformációkat és változásnapló-információkat visszaadni, illetve semmit sem ad vissza a rendszer által leképezett háttérből.

- **Keresés hatásköre**
 - Az **Objektum** lehetőség kiválasztása esetén a keresés csak a kijelölt objektumon belül történik.
 - Az **Egy szint** lehetőség kiválasztása esetén a keresés csak a kijelölt objektum közvetlen leszármazottain belül történik.
 - A **Részfa** kiválasztása esetén a keresés az összes leszármazott bejegyzésére kiterjed.
- **Keresési méret korlátozása** - Adja meg a keresés során visszakapott bejegyzések maximális számát, vagy legyen a keresés mérete **Korlátlan**.
- **Keresési időkorlát** - Adja meg a keresésre fordítható másodpercek maximális számát, vagy legyen a keresés ideje **Korlátlan**.
- Válassza ki a **Álnév-hivatkozás feloldás** típusát a legördülő listából.
 - **Soha** - Ha a kiválasztott bejegyzés álnév, akkor nem kerül feloldásra a keresés során, vagyis a keresés figyelmen kívül hagyja az álnév-hivatkozást.
 - **Találat** - Ha a kiválasztott bejegyzés álnév, akkor a keresés során feloldásra kerül és a keresés figyelmen kívül hagyja az álnév-hivatkozást.
 - **Keresés** - A kijelölt bejegyzés nem kerül feloldásra, de a keresés során talált bejegyzések igen.
 - **Mindig** - A keresés során talált minden álnév-hivatkozás feloldásra kerül.
- Jelölje meg az **Utalások követése** négyzetet az utalások követéséhez egy másik szerverre, ha a keresés során utalást is talál a rendszer. Ha egy hivatkozás a keresést egy másik szerverre utalja, akkor a szerverkapcsolat az aktuális hitelesítési adatokat használja. Ha névtelenül van bejelentkezve, akkor lehet, hogy egy hitelesített DN-nel kell bejelentkeznie a szerverre.

A keresésekkel kapcsolatos további információk: “Keresési beállítások módosítása” oldalszám: 127.

Bináris attribútumok módosítása

Ha egy attribútum bináris adatokat igényel, akkor az attribútummező mellett megjelenik egy **Bináris adatok** gomb. Ha az attribútumban nincsenek adatok, a mező üres. Mivel a bináris adatok nem jeleníthetők meg, a mezőben **Bináris adat - 1** felirat látható. Ha az attribútum egynél több értéket tartalmaz, a mező legördülő listaként jelenik meg.

A bináris attribútumok kezeléséhez kattintson a **Bináris adatok** gombra.

Bináris adatok importálhatók, exportálhatók és törölhetők.

Bináris adat hozzáadása egy attribútumhoz:

1. Kattintson a **Bináris adatok** gombra.
2. Kattintson az **Importálás** lapra.
3. Beírhatja a kívánt fájl elérési útját, vagy kattinthat a **Tallózás** gombra a bináris fájl kikereséséhez.
4. Kattintson a **Fájl elküldése** gombra. Megjelenik egy Fájl feltöltve üzenet.
5. Kattintson a **Bezárás** gombra. A **Bináris adat bejegyzések** alatt megjelenik a **Bináris adatok - 1** felirat.
6. Ismétlje meg az importálási eljárást a kívánt bináris fájlok felvételéhez. A bejegyzések sorra **Bináris adatok - 2**, **Bináris adatok - 3** néven jelennek meg.

7. Ha kész a bináris adatok felvételével, kattintson az **OK** gombra.

Bináris adatok exportálása:

1. Kattintson a **Bináris adatok** gombra.
2. Kattintson az **Exportálás** lapra.
3. Kattintson a **Letölthető bináris adatok** gombra.
4. Kövesse a varázsló utasításait a bináris fájl megjelenítéséhez vagy egy új helyre elmentéséhez.
5. Kattintson a **Bezárás** gombra.
6. Ismételje meg az exportálási eljárást az exportálni kívánt bináris fájlokhoz.
7. Ha kész a bináris adatok exportálásával, kattintson az **OK** gombra.

Bináris adatok törlése:

1. Kattintson a **Bináris adatok** gombra.
2. Jelölje meg a törölni kívánt bináris adatfájlokat. Több fájl is kiválasztható.
3. Kattintson a **Törlés** gombra.
4. A törlés jóváhagyásaként kattintson az **OK** gombra. A törlésre megjelölt bináris adatok törlésre kerülnek a listából.
5. Ha kész a bináris adatok törlésével, kattintson az **OK** gombra.

Megjegyzés: A bináris attribútumoknak csak a létezése kereshető.

Felhasználók és csoportok kezelése

A felhasználók és csoportok kezeléséhez bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

További információk:

- “Felhasználók kezelése”
- “Csoportok kezelése” oldalszám: 176

Felhasználók kezelése

A tartományok és sablonok beállítása után feltöltheti őket felhasználókkal. További információk:

- “Felhasználók felvétele”
- “Felhasználók keresése a tartományon belül”
- “Felhasználó információinak módosítása” oldalszám: 176
- “Felhasználó másolása” oldalszám: 176
- “Felhasználó eltávolítása” oldalszám: 176

Felhasználók felvétele

Bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

1. Kattintson a **Felhasználó felvétele** lehetőségre, vagy a **Felhasználók kezelése** lehetőségre és a **Hozzáadás** gombra.
2. Válassza ki a tartományt a legördülő menüből, amelybe fel akarja venni a felhasználót.
3. Kattintson a **Tovább** gombra. Megjelenik a tartományhoz rendelt sablon. Töltse ki a csillaggal (*) jelölt kötelező mezőket és a lapok többi mezőjét. Ha már létrehozott csoportokat a tartományon belül, akkor a felhasználót fel is veheti egy vagy több csoportba.
4. Ha kész, kattintson a **Bezárás** gombra.

Felhasználók keresése a tartományon belül

Bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

1. Kattintson a **Felhasználó keresése** vagy a **Felhasználók kezelése** lehetőségre, majd kattintson a **Keresés** gombra.

2. A **Tartomány kiválasztása** mezőből válassza ki a tartományt, amelyben keresni kíván.
3. Az **Elnevezési tulajdonság** mezőbe írja be a keresési karaktersorozatot. Helyettesítő karakterek is használhatók, például a ***smith** karaktersorozat beírására az eredmény minden olyan bejegyzés, amelynek a névattribútuma smith-re végződik.
4. A kiválasztott felhasználóval az alábbi műveleteket végezheti:
 - **Módosítás** - Részletek: "Felhasználó információinak módosítása".
 - **Másolás** - Részletek: "Felhasználó másolása".
 - **Törlés** - Részletek: "Felhasználó eltávolítása".
5. Ha kész, kattintson az **OK** gombra.

Felhasználó információinak módosítása

Bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

1. Kattintson a **Felhasználók kezelése** lehetőségre.
2. A legördülő menüből válasszon ki egy tartományt. Ha a felhasználók még nem láthatók a **Felhasználók** mezőben, akkor kattintson a **Felhasználók megjelenítése** lehetőségre.
3. Válassza ki a módosítani kívánt felhasználót, majd kattintson a **Módosítás** gombra.
4. Módosítsa a lapokon található információkat és a csoporttagságot.
5. Ha kész, kattintson az **OK** gombra.

Felhasználó másolása

Ha majdnem megegyező tulajdonságokkal bíró felhasználókat kell létrehoznia, akkor a többi felhasználót létrehozhatja az első felhasználó átmásolásával és a szükséges információk módosításával is.

Bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

1. Kattintson a **Felhasználók kezelése** lehetőségre.
2. A legördülő menüből válasszon ki egy tartományt. Ha a felhasználók még nem láthatók a **Felhasználók** mezőben, akkor kattintson a **Felhasználók megjelenítése** lehetőségre.
3. Válassza ki az átmásolni kívánt felhasználót, majd kattintson a **Másolás** gombra.
4. Módosítsa az új felhasználó szükséges információit - például az adott felhasználót azonosító adatokat (sn és cn). A felhasználók egyforma adatain nem kell módosítani.
5. Ha kész, kattintson az **OK** gombra.

Felhasználó eltávolítása

Bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

1. Kattintson a **Felhasználók kezelése** lehetőségre.
2. A legördülő menüből válasszon ki egy tartományt. Ha a felhasználók még nem láthatók a **Felhasználók** mezőben, akkor kattintson a **Felhasználók megjelenítése** lehetőségre.
3. Válassza ki az eltávolítani kívánt felhasználót, majd kattintson a **Törlés** gombra.
4. A törlés jóváhagyásaként kattintson az **OK** gombra.
5. A felhasználó eltávolításra kerül a felhasználók listájából.

Csoportok kezelése

A tartományok és sablonok beállítása után létrehozhat csoportokat. További információk:

- "Csoportok felvétele" oldalszám: 177
- "Csoportok keresése a tartományon belül" oldalszám: 177
- "Csoport információinak módosítása" oldalszám: 177
- "Csoport másolása" oldalszám: 177
- "Csoport eltávolítása" oldalszám: 178

Csoportok felvétele

Bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

1. Kattintson a **Csoport felvétele** lehetőségre, vagy a **Csoportok kezelése** lehetőségre és a **Hozzáadás** gombra.
2. Adja meg a létrehozni kívánt csoport nevét.
3. Válassza ki a tartományt a legördülő menüből, amelybe fel akarja venni a csoportot.
4. A csoport létrehozásához kattintson a **Befejezés** lehetőségre. Ha már vannak felhasználók a tartományban, akkor a **Tovább** gombra kattintva és felhasználókat kiválasztva felveheti őket a csoportba. Ezután kattintson a **Befejezés** lehetőségre.

További információk: "Csoportok és szerepek" oldalszám: 48.

Csoportok keresése a tartományon belül

Bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

1. Kattintson a **Csoport keresése** vagy a **Csoportok kezelése** lehetőségre, majd kattintson a **Keresés** gombra.
2. A **Tartomány kiválasztása** mezőből válassza ki a tartományt, amelyben keresni kíván.
3. Az **Elnevezési tulajdonság** mezőbe írja be a keresési karaktersorozatot. Helyettesítő karakterek is használhatók, például a ***club** karaktersorozat beírására az eredmény minden olyan csoport, amelynek a névattribútuma club-ra végződik.
4. A kiválasztott csoporttal az alábbi műveleteket végezheti:
 - **Módosítás** - Részletek: "Csoport információinak módosítása".
 - **Másolás** - Részletek: "Csoport másolása".
 - **Törlés** - Részletek: "Csoport eltávolítása" oldalszám: 178.
5. Ha kész, kattintson a **Bezárás** gombra.

Csoport információinak módosítása

Bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

1. Kattintson a **Csoportok kezelése** lehetőségre.
2. A legördülő menüből válasszon ki egy tartományt. Ha a csoportok még nem láthatók a **Csoportok** mezőben, akkor kattintson a **Csoportok megjelenítése** lehetőségre.
3. Válassza ki a módosítani kívánt csoportot, majd kattintson a **Módosítás** gombra.
4. A **Szűrő** gombra kattintva korlátozhatja a **Rendelkezésre álló felhasználók** számát. Ha például beírja a **Vezetéknév** mezőbe, hogy **"*smith"**, akkor a rendelkezésre álló felhasználók listája csak azokból fog állni, akiknek a neve a **"smith"** karakterekre végződik (vagyis Ann Smith, Bob Smith, Joe Goldsmith stb.)
5. Szabadon vehet fel és törölhet felhasználókat a csoportba.
6. Ha kész, kattintson az **OK** gombra.

Csoport másolása

Ha majdnem megegyező tagokkal rendelkező csoportokat kell létrehoznia, akkor a többi csoportot létrehozhatja az első csoport átmásolásával és a szükséges információk módosításával is.

Bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

1. Kattintson a **Csoportok kezelése** lehetőségre.
2. A legördülő menüből válasszon ki egy tartományt. Ha a csoportok még nem láthatók a **Csoportok** mezőben, akkor kattintson a **Csoportok megjelenítése** lehetőségre.
3. Válassza ki az átmásolni kívánt csoportot, majd kattintson a **Másolás** gombra.
4. Módosítsa a csoport nevét a **Csoport neve** mezőben. Az új csoportnak ugyanazok a tagjai, mint az eredeti csoportnak.
5. Módosíthatja a csoport tagságát.
6. Ha kész, kattintson az **OK** gombra. Létrejön az új csoport és ugyanazokat a tagokat tartalmazza, mint az eredeti csoport, a másolási eljárás végrehajtott módosításokkal.

Csoport eltávolítása

Bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

1. Kattintson a **Csoportok kezelése** lehetőségre.
2. A legördülő menüből válasszon ki egy tartományt. Ha a csoportok még nem láthatók a **Csoportok** mezőben, akkor kattintson a **Csoportok megjelenítése** lehetőségre.
3. Válassza ki az eltávolítani kívánt csoportot, majd kattintson a **Törlés** gombra.
4. A törlés jóváhagyásaként kattintson az **OK** gombra.
5. A csoport eltávolításra kerül a csoportok listájából.

Tartományok és felhasználói sablonok kezelése

A tartományok és felhasználói sablonok kezeléséhez bontsa ki a webes adminisztrációs eszköz navigációs területének **Tartományok és sablonok** kategóriáját. Tartományok és felhasználói sablonok használatával egyszerűbb másoknak adatokat bevinni a címárba. A tartományokkal és felhasználói sablonokkal kapcsolatos alapfogalmakról itt olvashat: “Tartományok és felhasználói sablonok” oldalszám: 42.

További információk:

- “Tartomány létrehozása”
- “Tartományadminisztrátor létrehozása”
- “Sablon létrehozása” oldalszám: 179
- “Sablon felvétele egy tartományba” oldalszám: 181
- “Csoportok létrehozása” oldalszám: 181
- “Felhasználó felvétele a tartományba” oldalszám: 181
- “Tartományok kezelése” oldalszám: 182
- “Sablonok kezelése” oldalszám: 183

Tartomány létrehozása

A tartományokkal és felhasználói sablonokkal kapcsolatos alapfogalmakról itt olvashat: “Tartományok és felhasználói sablonok” oldalszám: 42.

Egy tartomány létrehozása:

1. Bontsa ki a webes adminisztrációs eszköz navigációs területének **tartományok és sablonok** kategóriáját.
2. Kattintson a **Tartomány hozzáadása** lehetőségre.
 - Adja meg a tartomány nevét. Lehet például **realm1**.
 - Adja meg a tartományt azonosító Szülő DN-t. Ez a bejegyzés utótag formátumú (például **o=ibm,c=us**). A bejegyzés lehet utótag, de a címár más bejegyzése is. Kattinthat a **Tallózás** gombra is a hely kiválasztásához a részfából.
3. Ha kész, kattintson a **Tovább** vagy a **Befejezés** gombra.
4. Ha a **Tovább** gombra kattintott, tekintse át az információkat. E ponton még ténylegesen nincsen létrehozva a tartomány, úgyhogy a **Felhasználói sablon** és a **Felhasználói keresési szűrő** figyelmen kívül hagyható.
5. A tartomány létrehozásához kattintson a **Befejezés** lehetőségre.

Tartományadminisztrátor létrehozása

Egy tartományadminisztrátor létrehozásához először készítenie kell egy adminisztrációs csoportot a tartományhoz:

1. Hozza létre a tartományadminisztrációs csoportot.
 - a. Bontsa ki a webes adminisztrációs eszköz navigációs területének **Címtárkezelés** kategóriáját.
 - b. Kattintson a **Bejegyzések kezelése** lehetőségre.
 - c. Bontsa ki a címárfát és válassza ki az imént létrehozott **cn=realm1,o=ibm,c=us** tartományt.

- d. Kattintson az **ACL módosítása** gombra.
 - e. Kattintson a **Tulajdonosok** lapra.
 - f. Győződjön meg róla, hogy a **Tulajdonos továbbadása** négyzet be van jelölve.
 - g. Adja meg a tartomány DN-jét (**cn=realm1,o=ibm,c=us**).
 - h. Módosítsa a **Típust** csoportra.
 - i. Kattintson a **Hozzáadás** gombra.
2. Hozza létre az adminisztrátor bejegyzését. Ha még nem készített felhasználói bejegyzést az adminisztrátornak, akkor most tegye meg.
- a. Bontsa ki a webes adminisztrációs eszköz navigációs területének **Címtárkezelés** kategóriáját.
 - b. Kattintson a **Bejegyzések kezelése** lehetőségre.
 - c. Bontsa ki a címtárfa azon részét, ahol létre kívánja hozni az adminisztrátor bejegyzését.

Megjegyzés: Kívül helyezve az adminisztrátort saját tartományán megakadályozható, hogy véletlenül kitorölje saját magát. A jelen példában az **o=ibm,c=us** helyen hozzuk létre.

- d. Kattintson a **Hozzáadás** gombra.
 - e. Válassza ki a **Strukturális objektumosztályt**, például **inetOrgPerson**.
 - f. Kattintson a **Tovább** gombra.
 - g. Válassza ki a felvenni kívánt kiegészítő objektumosztályokat.
 - h. Kattintson a **Tovább** gombra.
 - i. Adja meg a bejegyzés kötelező attribútumait. Például:
 - **RDN** cn=JohnDoe
 - **DN** o=ibm,c=us
 - **cn** John Doe
 - **sn** Doe
 - j. Az **Egyéb attribútumok** lapon győződjön meg róla, hogy jelszót is rendelt a bejegyzéshez.
 - k. Ha kész, kattintson a **Bezárás** gombra.
3. Vegye fel az adminisztrátort az adminisztrátori csoportba.
- a. Bontsa ki a webes adminisztrációs eszköz navigációs területének **Címtárkezelés** kategóriáját.
 - b. Kattintson a **Bejegyzések kezelése** lehetőségre.
 - c. Bontsa ki a címtárfát és válassza ki az imént létrehozott **cn=realm1,o=ibm,c=us** tartományt.
 - d. Kattintson az **Attribútumok módosítása** lehetőségre.
 - e. Kattintson a **Tagok** lapra.
 - f. Kattintson a **Tagok** mezőre.
 - g. A **Tagok** mezőbe írja be az adminisztrátor DN-jét, ami példánkban **cn=John Doe,o=ibm,c=us**.
 - h. Kattintson a **Hozzáadás** gombra. A DN megjelenik a **Tagok** listában.
 - i. Kattintson az **OK** gombra.
 - j. Kattintson a **Frissítés** gombra. A DN megjelenik az **Aktuális tagok** listában.
 - k. Kattintson az **OK** gombra.
4. Ezzel létrehozta a tartomány bejegyzéseit felügyelni képes adminisztrátort.

Sablon létrehozása

A tartomány létrehozása utáni következő lépés egy felhasználói sablon létrehozása. A sablonokkal könnyebb a beírandó információk rendszerezése. Bontsa ki a webes adminisztrációs eszköz navigációs területének **tartományok és sablonok** kategóriáját.

1. Kattintson a **Felhasználói sablon hozzáadása** lehetőségre.
 - Írja be a sablon nevét, például **template1**.

- Adja meg a helyet, ahová a sablon kerül. Replikációs okokból a sablon kerüljön a tartomány azon részéjébe, amely használni fogja a sablont. Ilyen például az előző műveletben létrehozott **cn=realm1,o=ibm,c=us**. A **Tallózás** gombra kattintva kiválaszthat egy másik részét is a sablonnak.
2. Kattintson a **Tovább** gombra. A **Befejezés** gombra kattintva létrejön az üres sablon. Később is vehet fel információkat a sablonba (“Sablon módosítása” oldalszám: 184).
 3. Ha a **Tovább** gombra kattintott, akkor válassza ki a sablon strukturális objektumosztályát (például **inetOrgPerson**). Tetszés szerinti számú kiegészítő objektumosztályt is felvehet.
 4. Kattintson a **Tovább** gombra.
 5. A sablonban létrejön a **Kötelező** lap. A lapon található információkat módosíthatja.
 - a. Válassza ki a lapmenü **Kötelező** elemét, majd kattintson a **Módosítás** gombra. Megjelenik a **Lap módosítása** ablak. Megjelenik a **Kötelező** lap neve, valamint az **inetOrgPerson** objektumosztály által megkövetelt kötelező attribútumok:
 - *sn - vezetéknev
 - *cn - általános név

Megjegyzés: A * a kötelező információkat jelzi.

- b. Ha további információkat akar felvenni a lapra, akkor válassza ki a kívánt attribútumot az **Attribútumok** menüből. Például válassza ki a **departmentNumber** elemet, majd kattintson a **Hozzáadás** gombra. Válassza ki az **employeeNumber** elemet, majd kattintson a **Hozzáadás** gombra. Válassza ki a **title** elemet, majd kattintson a **Hozzáadás** gombra. A **Kiválasztott attribútumok** menü immár így néz ki:
 - title
 - employeeNumber
 - departmentNumber
 - *sn
 - *cn
 - c. A mezők sorrendjét módosíthatja a sablonon belül: jelölje ki a kívánt attribútumot és kattintson a **Fel** vagy **Le** gombokra. Így egy hellyel arrébb lép az attribútum a listában. Ismétlje ezt addig, amíg az attribútumok a kívánt sorrendben nem találhatók. Például:
 - *sn
 - *cn
 - title
 - employeeNumber
 - departmentNumber
 - d. Módosíthatja is az egyes kiválasztott attribútumokat.
 - 1) Jelölje meg az attribútumot a **Kiválasztott attribútumok** mezőben, majd kattintson a **Módosítás** gombra.
 - 2) Módosíthatja a mező megjelenítési nevét is a sablonban. Például megteheti, hogy a **departmentNumber** mezőhöz az **Osztály száma** felirat jelenjen meg. Írja be a kívánt szöveget a **Megjelenítési név** mezőbe.
 - 3) Megadhat egy alapértelmezett értéket is a sablon attribútummezejének előre kitöltéséhez. Ha például a beírt felhasználók többsége a 789-es osztályhoz fog tartozni, akkor beírhatja a 789-et alapértelmezett értékként. A sablon mezejébe előre be fog íródni a 789 érték. Az érték módosítható a tényleges felhasználói információk beírásakor.
 - 4) Kattintson az **OK** gombra.
 - e. Kattintson az **OK** gombra.
6. Ha újabb lapkategoriót akar létrehozni további információkhoz, akkor kattintson a **Hozzáadás** gombra.
 - Adja meg az új lap nevét. Például: Címadatok.
 - Az új lap attribútumait válogassa ki az **Attribútumok** menüből. Például válassza ki a **homePostalAddress** elemet, majd kattintson a **Hozzáadás** gombra. Válassza ki a **postOfficeBox** elemet, majd kattintson a **Hozzáadás** gombra. Válassza ki a **telephoneNumber** elemet, majd kattintson a **Hozzáadás** gombra. Válassza ki

a **homePhone** elemet, majd kattintson a **Hozzáadás** gombra. Válassza ki a **facsimileTelephoneNumber** elemet, majd kattintson a **Hozzáadás** gombra. A **Kiválasztott attribútumok** menü így néz ki:

- homePostalAddress
- postOfficeBox
- telephoneNumber
- homePhone
- facsimileTelephoneNumber

- A mezők sorrendjét módosíthatja a sablonon belül: jelölje ki a kívánt attribútumot és kattintson a **Fel** vagy **Le** gombokra. Így egy hellyel arrébb lép az attribútum a listában. Ismételje ezt addig, amíg az attribútumok a kívánt sorrendben nem találhatók. Például:

- homePostalAddress
- postOfficeBox
- telephoneNumber
- facsimileTelephoneNumber
- homePhone

- Kattintson az **OK** gombra.

7. Ismételje meg a fenti eljárást, amíg létre nem hozta az összes kívánt lapot. Ha kész, kattintson a **Befejezés** gombra a sablon létrehozásához.

Sablon felvétele egy tartományba

A tartomány és sablon létrehozása után fel kell vennie a sablont a tartományba. Bontsa ki a webes adminisztrációs eszköz navigációs területének **tartományok és sablonok** kategóriáját.

1. Kattintson a **Tartományok kezelése** lehetőségre.
2. Válassza ki a tartományt, amelybe fel kívánja venni a sablont (példánkban a **cn=realm1,o=ibm,c=us**), majd kattintson a **Módosítás** gombra.
3. Görgesse le a menüt a **Felhasználói sablon** elemig, majd bontsa ki a legördülő menüt.
4. válassza ki a sablont (példánkban **cn=template1,cn=realm1,o=ibm,c=us**).
5. Kattintson az **OK** gombra.
6. Kattintson a **Bezárás** gombra.

Csoportok létrehozása

Bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

1. Kattintson a **Csoportok hozzáadása** gombra.
2. Adja meg a létrehozni kívánt csoport nevét. Lehet például **group1**.
3. Válassza ki a tartományt a legördülő menüből, amelybe fel akarja venni a felhasználót. A jelen esetben ez a **realm1**.
4. A csoport létrehozásához kattintson a **Befejezés** lehetőségre. Ha már vannak felhasználók a tartományban, akkor a **Tovább** gombra kattintva és felhasználókat kiválasztva felveheti őket a group1 csoportba. Ezután kattintson a **Befejezés** lehetőségre.

További információk: "Csoportok és szerepek" oldalszám: 48.

Felhasználó felvétele a tartományba

Bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

1. Kattintson a **Felhasználó hozzáadása** lehetőségre.
2. Válassza ki a tartományt a legördülő menüből, amelybe fel akarja venni a felhasználót. A jelen esetben ez a **realm1**.

3. Kattintson a **Tovább** gombra. Megjelenik az imént létrehozott template1 sablon. Töltse ki a csillaggal (*) jelölt kötelező mezőket és a lapok többi mezőjét. Ha már létrehozott csoportokat a tartományon belül, akkor a felhasználót fel is veheti egy vagy több csoportba.
4. Ha kész, kattintson a **Bezárás** gombra.

Tartományok kezelése

Miután beállította és feltöltötte az első tartományt, létrehozhat további tartományokat is, illetve módosíthatja a meglévőket.

Bontsa ki a navigációs terület **Tartományok és sablonok** kategóriáját, majd kattintson a **Tartományok kezelése** lehetőségre. Megjelenik a meglévő tartományok listája. Ebben az ablakban vehet fel, módosíthat és törölhet tartományokat, illetve módosíthatja a tartomány hozzáférés-felügyelet listáját (ACL). További információk:

- “Tartomány hozzáadása”
- “Tartomány módosítása”
- “Tartomány eltávolítása”
- “Tartomány ACL-jeinek módosítása” oldalszám: 183

Tartomány hozzáadása

Bontsa ki a webes adminisztrációs eszköz navigációs területének **tartományok és sablonok** kategóriáját.

1. Kattintson a **Tartomány hozzáadása** lehetőségre.
 - Adja meg a tartomány nevét. Lehet például **realm2**.
 - Ha már léteznek más tartományok is (például a **realm1**), akkor kiválaszthat egy már meglévő tartományt, hogy annak beállításai átmásolódnak az éppen létrehozottba.
 - Adja meg a tartományt azonosító Szülő DN-t. Ez a bejegyzés utótag formátumú (például **o=ibm,c=us**). Kattinthat a **Tallózás** gombra is a hely kiválasztásához a részfából.
2. Ha kész, kattintson a **Tovább** vagy a **Befejezés** gombra.
3. Ha a **Tovább** gombra kattintott, tekintse át az információkat.
4. Válasszon ki egy **Felhasználói sablont** a legördülő listából. Ha a beállításokat egy már létező tartományból veszi, akkor a sablon előre kitölti ezt a mezőt.
5. Adjon meg egy **Felhasználó keresési szűrőt**.
6. A tartomány létrehozásához kattintson a **Befejezés** lehetőségre.

Tartomány módosítása

Bontsa ki a webes adminisztrációs eszköz navigációs területének **tartományok és sablonok** kategóriáját.

- Kattintson a **Tartományok kezelése** lehetőségre.
- Válassza ki a módosítani kívánt tartományt a legördülő menüből.
- Kattintson a **Módosítás** gombra.
 - A **Tallózás** gombokkal módosíthatja a tartomány:
 - Adminisztrátori csoportját
 - Csoporttárolóját
 - Felhasználói tárolóját
 - Másik sablont is választhat a legördülő menüből.
 - A **Felhasználó keresési szűrő** módosításához kattintson a **Módosítás** gombra.
- Ha kész, kattintson az **OK** gombra.

Tartomány eltávolítása

Bontsa ki a webes adminisztrációs eszköz navigációs területének **tartományok és sablonok** kategóriáját.

1. Kattintson a **Tartományok kezelése** lehetőségre.
2. Válassza ki a törölni kívánt tartományt.

3. Kattintson a **Törlés** gombra.
4. A törlés jóváhagyásaként kattintson az **OK** gombra.
5. A tartomány eltávolításra kerül a tartományok listájából.

Tartomány ACL-jeinek módosítása

További információk az ACL tulajdonságok megtekintéséről a webes adminisztrációs eszközzel, illetve az ACL-ek kezeléséről: “Hozzáférés-felügyeleti listák (ACL-ek) kezelése” oldalszám: 185.

További információk: “Hozzáférés-felügyeleti listák” oldalszám: 56.

Sablonok kezelése

Az első sablon létrehozása után további sablonokat vehet fel vagy módosíthatja a meglévő sablonokat.

Bontsa ki a navigációs terület **Tartományok és sablonok** kategóriáját, majd kattintson a **Felhasználói sablonok kezelése** lehetőségre. Megjelenik a meglévő sablonok listája. Ebben az ablakban vehet fel, módosíthat és törölhet sablonokat, illetve módosíthatja a sablon hozzáférés-felügyeleti listáját (ACL). További információk:

- “Felhasználói sablon létrehozása”
- “Sablon módosítása” oldalszám: 184
- “Sablon eltávolítása” oldalszám: 185
- “Sablon ACL-jeinek módosítása” oldalszám: 185

Felhasználói sablon létrehozása

Bontsa ki a webes adminisztrációs eszköz navigációs területének **tartományok és sablonok** kategóriáját.

1. Kattintson a **Felhasználói sablon hozzáadása** lehetőségre, vagy a **Felhasználói sablonok kezelése** lehetőségre és a **Hozzáadás** gombra.
 - Adja meg az új sablon nevét. Lehet például **template2**.
 - Ha már léteznek más sablonok is (például a **template1**), akkor kiválaszthat egy már meglévő sablont, hogy annak beállításai átmásolódnak az éppen létrehozottba.
 - Adja meg a sablont azonosító Szülő DN-t. Ez a bejegyzés DN formátumú (például **cn=realm1,o=ibm,c=us** .) Kattinthat a **Tallózás** gombra is a hely kiválasztásához a részfából.
2. Kattintson a **Tovább** gombra. A **Befejezés** gombra kattintva létrejön az üres sablon. Később is vehet fel információkat a sablonba (“Sablon módosítása” oldalszám: 184).
3. Ha a **Tovább** gombra kattintott, akkor válassza ki a sablon strukturális objektumosztályát (például **inetOrgPerson**). Tetszés szerinti számú kiegészítő objektumosztályt is felvehet.
4. Kattintson a **Tovább** gombra.
5. A sablonban létrejön a **Kötelező** lap. A lapon található információkat módosíthatja.
 - a. Válassza ki a lapmenü **Kötelező** elemét, majd kattintson a **Módosítás** gombra. Megjelenik a **Lap módosítása** ablak. Megjelenik a **Kötelező** lap neve, valamint az **inetOrgPerson** objektumosztály által megkövetelt kötelező attribútumok:
 - *sn - vezetéknév
 - *cn - általános név
 - Megjegyzés:** A * a kötelező információkat jelzi.
 - b. Ha további információkat akar felvenni a lapra, akkor válassza ki a kívánt attribútumot az **Attribútumok** menüből. Például válassza ki a **departmentNumber** elemet, majd kattintson a **Hozzáadás** gombra. Válassza ki az **employeeNumber** elemet, majd kattintson a **Hozzáadás** gombra. Válassza ki a **title** elemet, majd kattintson a **Hozzáadás** gombra. A **Kiválasztott attribútumok** menü immár így néz ki:
 - title
 - employeeNumber
 - departmentNumber

- *sn
 - *cn
- c. A mezők sorrendjét módosíthatja a sablonon belül: jelölje ki a kívánt attribútumot és kattintson a **Fel** vagy **Le** gombokra. Így egy hellyel arrébb lép az attribútum a listában. Ismétlje ezt addig, amíg az attribútumok a kívánt sorrendben nem találhatók. Például:
- *sn
 - *cn
 - title
 - employeeNumber
 - departmentNumber
- d. Módosíthatja is az egyes kiválasztott attribútumokat.
- 1) Jelölje meg az attribútumot a **Kiválasztott attribútumok** mezőben, majd kattintson a **Módosítás** gombra.
 - 2) Módosíthatja a mező megjelenítési nevét is a sablonban. Például megteheti, hogy a **departmentNumber** mezőhöz az **Osztály száma** felirat jelenjen meg. Írja be a kívánt szöveget a **Megjelenítési név** mezőbe.
 - 3) Megadhat egy alapértelmezett értéket is a sablon attribútummezejének előre kitöltéséhez. Ha például a beírt felhasználók többsége a 789-es osztályhoz fog tartozni, akkor beírhatja a 789-et alapértelmezett értéként. A sablon mezejébe előre be fog íródni a 789 érték. Az érték módosítható a tényleges felhasználói információk beírásakor.
 - 4) Kattintson az **OK** gombra.
- e. Kattintson az **OK** gombra.
6. Ha újabb lapkategóriát akar létrehozni további információkhoz, akkor kattintson a **Hozzáadás** gombra.
- Adja meg az új lap nevét. Például: Címadatok.
 - Az új lap attribútumait válogassa ki az **Attribútumok** menüből. Például válassza ki a **homePostalAddress** elemet, majd kattintson a **Hozzáadás** gombra. Válassza ki a **postOfficeBox** elemet, majd kattintson a **Hozzáadás** gombra. Válassza ki a **telephoneNumber** elemet, majd kattintson a **Hozzáadás** gombra. Válassza ki a **homePhone** elemet, majd kattintson a **Hozzáadás** gombra. Válassza ki a **facsimileTelephoneNumber** elemet, majd kattintson a **Hozzáadás** gombra. A **Kiválasztott attribútumok** menü így néz ki:
 - homePostalAddress
 - postOfficeBox
 - telephoneNumber
 - homePhone
 - facsimileTelephoneNumber
 - A mezők sorrendjét módosíthatja a sablonon belül: jelölje ki a kívánt attribútumot és kattintson a **Fel** vagy **Le** gombokra. Így egy hellyel arrébb lép az attribútum a listában. Ismétlje ezt addig, amíg az attribútumok a kívánt sorrendben nem találhatók. Például:
 - homePostalAddress
 - postOfficeBox
 - telephoneNumber
 - facsimileTelephoneNumber
 - homePhone
 - Kattintson az **OK** gombra.
7. Ismétlje meg a fenti eljárást, amíg létre nem hozta az összes kívánt lapot. Ha kész, kattintson a **Befejezés** gombra a sablon létrehozásához.

Sablon módosítása

Bontsa ki a webes adminisztrációs eszköz navigációs területének **tartományok és sablonok** kategóriáját.

- Kattintson a **Felhasználói sablonok kezelése** lehetőségre.
- Válassza ki a módosítani kívánt tartományt a legördülő menüből.

- Kattintson a **Módosítás** gombra.
- Ha már léteznek más sablonok is (például a template1), akkor kiválaszthat egy már meglévő sablont, hogy annak beállításai átmásolódjanak az éppen módosítottba.
- Kattintson a **Tovább** gombra.
 - A legördülő menüt is használhatja a sablon strukturális objektumosztályának módosításához.
 - Szabadon vehet fel és törölhet kiegészítő objektumosztályokat.
- Kattintson a **Tovább** gombra.
- A sablon lapjai és attribútumai módosíthatók. A lapok módosításával kapcsolatos további információk: 5 oldalszám: 183.
- Ha kész, kattintson a **Bezárás** gombra.

Sablon eltávolítása

Bontsa ki a webes adminisztrációs eszköz navigációs területének **tartományok és sablonok** kategóriáját.

1. Kattintson a **Felhasználói sablonok kezelése** lehetőségre.
2. Válassza ki a törölni kívánt sablont.
3. Kattintson a **Törlés** gombra.
4. A törlés jóváhagyásaként kattintson az **OK** gombra.
5. A sablon eltávolításra kerül a sablonok listájából.

Sablon ACL-jeinek módosítása

Bontsa ki a webes adminisztrációs eszköz navigációs területének **tartományok és sablonok** kategóriáját.

1. Kattintson a **Felhasználói sablonok kezelése** lehetőségre.
2. Válassza ki a sablont, amelynek az ACL-jét módosítani kívánja.
3. Kattintson az **ACL módosítása** gombra.

További információk az ACL tulajdonságok megtekintéséről a webes adminisztrációs eszközzel, illetve az ACL-ek kezeléséről: “Hozzáférés-felügyeleti listák (ACL-ek) kezelése”.

További információk: “Hozzáférés-felügyeleti listák” oldalszám: 56.

Hozzáférés-felügyeleti listák (ACL-ek) kezelése

További információk a hozzáférés-felügyeleti listákról: “Hozzáférés-felügyeleti listák” oldalszám: 56.

Az ACL tulajdonságok megtekintése a webes adminisztrációs eszközzel és az ACL-ek kezelésének lépései:

1. Válasszon ki egy címtárbejegyzést. Legyen ez például a cn=John Doe,ou=Advertising,o=ibm,c=US bejegyzés.
2. Kattintson az **ACL módosítása** gombra. Megjelenik az ACL módosítása ablak és annak **Hatályos ACL-ek** lapja.

Az ablak öt lapból áll:

- “Hatályos ACL-ek” oldalszám: 186
- “Hatályos tulajdonosok” oldalszám: 186
- “Nem szűrt ACL-ek” oldalszám: 186
- “Szűrt ACL-ek” oldalszám: 188
- “Tulajdonosok” oldalszám: 189

A **Hatályos ACL-ek** és a **Hatályos tulajdonosok** lapokon csak olvasható információk láthatók az ACL-ekkel kapcsolatban.

Hatályos ACL-ek

A hatályos ACL-ek az adott bejegyzés közvetlenül megadott és öröklött ACL-jeinek együttese. Egy adott hatályos ACL hozzáférési jogainak megtekintéséhez válassza ki, majd kattintson a **Megjelenítés** gombra. Megjelenik a **Hozzáférési jogok megjelenítése** ablak.

Hozzáférési jogok megtekintése

- A **Jogok** szakaszban láthatók az alanyok hozzáadási és törlési jogai.
 - A **Leszármazott felvétele** jog engedélyezi vagy tiltja az alany számára, hogy címtárbejegyzést hozzon létre a kiválasztott bejegyzés alatt.
 - A **Bejegyzés törlése** jog engedélyezi vagy tiltja az alany számára, hogy törölje a kiválasztott bejegyzést.
- A **Biztonsági osztály** szakasz a biztonsági osztályokkal kapcsolatos jogosultságokat adja meg. Az attribútumok biztonsági osztályokba vannak csoportosítva:
 - **Normál** - A normál attribútumosztályok igénylik a legkisebb biztonságot, ilyen például a `commonName` attribútum.
 - **Bizalmas** - A bizalmas attribútumosztály közepes biztonsági szintet követel meg, ilyen például a `homePhone` attribútum.
 - **Kritikus** - A kritikus attribútumosztályok a legmagasabb szintű biztonságot követelik meg, ilyen például az `userpassword` attribútum.
 - **Rendszer** - A rendszerattribútumok írásvédett attribútumok, amelyeket a szerver tart karban.
 - **Korlátozott** - A korlátozott attribútumok a hozzáférés-felügyelet megadására szolgálnak-

Mindegyik biztonsági osztályhoz külön engedélyek tartoznak.

- **Olvadás** - az alany kiolvashatja az attribútumokat.
- **Írás** - az alany írhatja az attribútumokat.
- **Keresés** - az alany kereshet az attribútumok alapján.
- **Összehasonlítás** - az alany összehasonlíthatja az attribútumokat.

Kattintson az **OK** gombra a Hatályos ACL-ek lapra visszatéréshez.

Kattintson a **Mégse** gombra az ACL módosítása ablakba visszatéréshez.

Hatályos tulajdonosok

A hatályos tulajdonosok az adott bejegyzés közvetlenül megadott és öröklött tulajdonosainak együttese.

Nem szűrt ACL-ek

Felvehet nem szűrt ACL-eket egy bejegyzéshez, vagy módosíthatja a nem szűrt ACL-eket.

A nem szűrt ACL-ek továbbadhatók. Ez azt jelenti, hogy az egyik bejegyzéshez megadott hozzáférés-felügyeleti információk alkalmazhatók annak összes alárendelt bejegyzésére is. Az ACL forrása a kiválasztott bejegyzés aktuális ACL-jének a forrása. Ha a bejegyzésnek nincsen ACL-je, akkor megörökli az ACL-t a szülőobjektumtól, a szülőobjektumok ACL-beállításainak megfelelően.

Írja be az alábbi információkat a **Nem szűrt ACL-ek** lapon:

- ACL-ek továbbadása - A **Továbbadás** négyzet megjelölése esetén a közvetlen ACL-lel nem rendelkező leszármazott bejegyzések megöröklik e bejegyzés ACL-jét. Ha a négyzet meg van jelölve, akkor a leszármazott megörökli e bejegyzés ACL-jét. Ha a leszármazott bejegyzéshez van közvetlenül megadva ACL, akkor az felülbírálja a szülőtől megöröklött ACL. Ha a négyzet nincs megjelölve, akkor a közvetlenül megadott ACL-lel nem rendelkező leszármazottak e bejegyzés azon ősétől öröklik meg ACL-jüket, amelyiknél be van állítva ez a lehetőség.
- DN (megkülönböztetett név) - Adja meg annak az entitásnak a **(DN) megkülönböztetett nevét**, amely kérni fogja műveletek végrehajtását az adott bejegyzésen. Például: `cn=Marketing Group`.
- Típus - Adja meg a DN **Típusát**. Ha például a DN egy felhasználó, akkor válassza ki az `access-id` lehetőséget.

Hozzáférési jogok felvétele és módosítása

Egy meglévő DN ACL-jének módosításához kattintson az ACL lista DN (megkülönböztetett név) mezőjében a **Hozzáadás** gombra, vagy a **Módosítás** gombra.

A **Hozzáférési jogok felvétele** és a **Hozzáférési jogok módosítása** ablakokban beállíthatja az új vagy meglévő hozzáférés-felügyeleti listák (ACL-ek) hozzáférési jogait. A **Típus** mező alapértelmezése az **ACL módosítása** ablakban megadott típus. Ha újonnan veszi fel az ACL-t, akkor az összes többi mező alapértelmezetten üres. Ha módosítja az ACL-t, akkor a mezőkben az ACL legutolsó módosításakor megadott értékek láthatók.

Az alábbiakat teheti:

- Az ACL típusának megváltoztatása
- Hozzáadási és törlési jogok beállítása
- Jogosultságok beállítása a biztonsági osztályokhoz

A hozzáférési jogok beállítása:

1. Válassza ki az ACL bejegyzésének **típusát**. Ha például a DN egy felhasználó, akkor válassza ki az access-id lehetőséget.
2. A **Jogok** szakaszban láthatók az alanyok hozzáadási és törlési jogai.
 - A **Leszármazott felvétele** jog engedélyezi vagy tiltja az alany számára, hogy címtárbejegyzést hozzon létre a kiválasztott bejegyzés alatt.
 - A **Bejegyzés törlése** jog engedélyezi vagy tiltja az alany számára, hogy törölje a kiválasztott bejegyzést.
3. A **Biztonsági osztály** szakasz a biztonsági osztályokkal kapcsolatos jogosultságokat adja meg. Az attribútumok biztonsági osztályokba vannak csoportosítva:
 - **Normál** - A normál attribútumosztályok igénylik a legkisebb biztonságot, ilyen például a commonName attribútum.
 - **Bizalmas** - A bizalmas attribútumosztály közepes biztonsági szintet követel meg, ilyen például a homePhone attribútum.
 - **Kritikus** - A kritikus attribútumosztályok a legmagasabb szintű biztonságot követelik meg, ilyen például az userpassword attribútum.
 - **Rendszer** - A rendszerattribútumok írásvédett attribútumok, amelyeket a szerver tart karban.
 - **Korlátozott** - A korlátozott attribútumok a hozzáférés-felügyelet megadására szolgálnak-

Mindegyik biztonsági osztályhoz külön engedélyek tartoznak.

- Olvasás - az alany kiolvashatja az attribútumokat.
- Írás - az alany írhatja az attribútumokat.
- Keresés - az alany kereshet az attribútumok alapján.
- Összehasonlítás - az alany összehasonlíthatja az attribútumokat.

Ezenfelül megadhat jogosultságokat az attribútum alapján is, nemcsak a biztonsági osztály alapján, amelyhez az attribútum tartozik. Az attribútum szakasz alább, a **Kritikus biztonsági osztály** részben van felsorolva.

- Válasszon ki egy attribútumot az **Attribútum megadása** legördülő listából.
- Kattintson a **Megadás** mezőre. Az attribútum megjelenik egy jogosultságtáblázattal együtt.
- Döntse el, hogy az attribútumhoz tartozó négy biztonsági osztály engedélyből melyeket adja meg vagy tagadja meg.
- Ezt az eljárást más attribútumokra is megismételheti.
- Egy attribútum eltávolításához egyszerűen csak válassza ki az attribútumot, majd kattintson a **Törlés** gombra.
- Ha kész, kattintson az **OK** gombra.

ACL-ek eltávolítása

Az ACL-ek eltávolítása kétféle módon történhet:

- Kattintson a törölni kívánt ACL melletti választógombra. Kattintson a **Törlés** gombra.
- Az **Összes törlése** gombbal törölheti a lista összes DN-jét.

Szűrt ACL-ek

Felvehet szűrt ACL-eket egy bejegyzéshez, vagy módosíthatja a szűrt ACL-eket.

A szűrő alapú ACL-ek szűrő alapú összehasonlítást használnak egy meghatározott objektumszűrő segítségével, hogy azonosítsák a célobjektumokat a tényleges rájuk vonatkozó hozzáférési jogosultságokkal.

Egy szűrő alapú ACL alapértelmezett viselkedése az, hogy összegyűlik a legalacsonyabb tartalmazó bejegyzéstől felfelé az öröklődési láncon, a DIT legmagasabb tartalmazó bejegyzéséig. A tényleges hozzáférési jogok az ő bejegyzésekhez megadott és elvett összes jog uniójaként kerülnek kiszámításra. Egy kivétel van erre a viselkedésre. A részfa-replikációs funkció használata és a jobb adminisztrációs irányítás érdekében létezik egy "plafon" (ceiling) attribútum, amelynek a szerepe, hogy megállítsa a jogok gyűjtését annál a bejegyzésnél, amely őt tartalmazza.

Írja be az alábbi információkat a Szűrt ACL-ek lapon:

- Szűrt ACL-ek gyűjtése -
 - A **Nincs megadva** választógombbal törölheti az `ibm-filterACLInherit` attribútumot a kiválasztott bejegyzésből.
 - Az **Igaz** választógomb kiválasztásával engedélyezheti a kiválasztott bejegyzés ACL-jének, hogy összegyűljön a legalacsonyabb tartalmazó bejegyzéstől felfelé az öröklődési láncon, a DIT legmagasabb tartalmazó bejegyzéséig.
 - A **Hamis** választógombbal megállíthatja a szűrő ACL-ek összegyűjtését a kiválasztott bejegyzésnél.
- DN (megkülönböztetett név) - Adja meg annak az entitásnak a **(DN) megkülönböztetett nevét**, amely kérni fogja műveletek végrehajtását az adott bejegyzésen. Például: `cn=Marketing Group`.
- Típus - Adja meg a DN **Típusát**. Ha például a DN egy felhasználó, akkor válassza ki az `access-id` lehetőséget.

Hozzáférési jogok felvétele és módosítása

Egy meglévő DN ACL-jének módosításához kattintson az ACL lista DN (megkülönböztetett név) mezőjében a **Hozzáadás** gombra, vagy a **Módosítás** gombra.

A **Hozzáférési jogok felvétele** és a **Hozzáférési jogok módosítása** ablakokban beállíthatja az új vagy meglévő hozzáférés-felügyeleti listák (ACL-ek) hozzáférési jogait. A Típus mező alapértelmezése az ACL módosítása ablakban megadott típus. Ha újonnan veszi fel az ACL-t, akkor az összes többi mező alapértelmezetten üres. Ha módosítja az ACL-t, akkor a mezőkben az ACL legutolsó módosításakor megadott értékek láthatók.

Az alábbiakat teheti:

- Az ACL típusának megváltoztatása
- Hozzáadási és törlési jogok beállítása
- Objektumszűrő beállítása a szűrt ACL-ekhez
- Jogosultságok beállítása a biztonsági osztályokhoz

A hozzáférési jogok beállítása:

1. Válassza ki az ACL bejegyzésének **típusát**. Ha például a DN egy felhasználó, akkor válassza ki az `access-id` lehetőséget.
2. A **Jogok** szakaszban láthatók az alanyok hozzáadási és törlési jogai.
 - A **Leszármazott felvétele** jog engedélyezi vagy tiltja az alany számára, hogy címtárbejegyzést hozzon létre a kiválasztott bejegyzés alatt.
 - A **Bejegyzés törlése** jog engedélyezi vagy tiltja az alany számára, hogy törölje a kiválasztott bejegyzést.

3. Objektumszűrő beállítása szűrő alapú összehasonlításhoz. Az **Objektumszűrő** mezőbe írja be a kiválasztott ACL kívánt szűrőjét. Ha segítségre van szüksége a keresési szűrő karaktersorozat kialakítása során, kattintson a **Szűrő módosítása** gombra. Az aktuális szűrt ACL a hozzá rendelt részfa leszármazott azon objektumaira terjed tova, amelyek megfelelnek a mezőben megadott szűrőnek.
4. A **Biztonsági osztály** szakasz a biztonsági osztályokkal kapcsolatos jogosultságokat adja meg. Az attribútumok biztonsági osztályokba vannak csoportosítva:
 - **Normál** - A normál attribútumosztályok igénylik a legkisebb biztonságot, ilyen például a commonName attribútum.
 - **Bizalmas** - A bizalmas attribútumosztály közepes biztonsági szintet követel meg, ilyen például a homePhone attribútum.
 - **Kritikus** - A kritikus attribútumosztályok a legmagasabb szintű biztonságot követelik meg, ilyen például az userpassword attribútum.
 - **Rendszer** - A rendszerattribútumok írásvédett attribútumok, amelyeket a szerver tart karban.
 - **Korlátozott** - A korlátozott attribútumok a hozzáférés-felügyelet megadására szolgálnak-

Mindegyik biztonsági osztályhoz külön engedélyek tartoznak.

- Olvasás - az alany kiolvashatja az attribútumokat.
- Írás - az alany írhatja az attribútumokat.
- Keresés - az alany kereshet az attribútumok alapján.
- Összehasonlítás - az alany összehasonlíthatja az attribútumokat.

Ezenfelül megadhat jogosultságokat az attribútum alapján is, nemcsak a biztonsági osztály alapján, amelyhez az attribútum tartozik. Az attribútum szakasz alább, a **Kritikus biztonsági osztály** részben van felsorolva.

- Válasszon ki egy attribútumot az **Attribútum megadása** legördülő listából.
- Kattintson a **Megadás** mezőre. Az attribútum megjelenik egy jogosultságtáblázzal együtt.
- Döntse el, hogy az attribútumhoz tartozó négy biztonsági osztály engedélyből melyeket adja meg vagy tagadja meg.
- Ezt az eljárást más attribútumokra is megismételheti.
- Egy attribútum eltávolításához egyszerűen csak válassza ki az attribútumot, majd kattintson a **Törlés** gombra.
- Ha kész, kattintson az **OK** gombra.

ACL-ek eltávolítása

Az ACL-ek eltávolítása kétféle módon történhet:

- Kattintson a törölni kívánt ACL melletti választógombra. Kattintson a **Törlés** gombra.
- Az **Összes törlése** gombbal törölheti a lista összes DN-jét.

Tulajdonosok

A bejegyzések tulajdonosai teljeskörű jogosultsággal rendelkeznek: minden műveletet végrehajthatnak az objektumon. A bejegyzések tulajdonosai lehetnek közvetlenül megadva, de öröklődhetnek is.

Írja be az alábbi információkat a **Tulajdonosok** lapon:

- A **Továbbadás** négyzet megjelölése esetén a közvetlen tulajdonossal nem rendelkező leszármazott bejegyzések megöröklik e bejegyzés tulajdonosát. Ha a négyzet nincs megjelölve, akkor a közvetlenül megadott tulajdonossal nem rendelkező leszármazottak e bejegyzés azon őstől öröklik meg tulajdonosukat, amelyiknél be van állítva ez a lehetőség.
- DN (megkülönböztetett név) - Adja meg annak az entitásnak a **(DN) megkülönböztetett nevét**, amely kérni fogja műveletek végrehajtását az adott bejegyzésen. Például: cn=Marketing Group
A cn=this értéket használva azon objektumok esetén, amelyek saját tulajdonosait továbbadják másoknak, egyszerűen létre lehet hozni egy olyan címtár részfat, amelyben minden objektum saját magának tulajdonosa.
- Típus - Adja meg a DN **Típusát**. Ha például a DN egy felhasználó, akkor válassza ki az access-id lehetőséget.

Tulajdonos hozzáadása

A DN hozzáadásához kattintson a **DN (megkülönböztetett név)** mezőben a **Hozzáadás** gombra.

Tulajdonos eltávolítása

A tulajdonosok eltávolítása kétféle módon történhet:

- Kattintson a törölni kívánt tulajdonos melletti választógombra. Kattintson a **Törlés** gombra.
- Az **Összes törlése** gombbal törölheti a lista összes tulajdonos DN-jét.

8. fejezet Referencia

Az alábbiakat használja referenciainformációkként.

- “Parancssori segédprogramok”
- “LDAP adatcsere formátum (LDIF)” oldalszám: 220
- “Directory Server konfigurációs séma” oldalszám: 223
- “Objektumazonosítók (OID)” oldalszám: 261

Parancssori segédprogramok

Ez a rész írja le az i5/OS Qshell parancskörnyezetében futtatható segédprogramokat. További információkat az alábbi parancsok leírásánál talál:

- “ldapmodify és ldapadd”
- “ldapdelete” oldalszám: 195
- “ldapexop” oldalszám: 198
- “ldapmodrdn” oldalszám: 203
- “ldapsearch” oldalszám: 206
- “ldapchangepwd” oldalszám: 215
- “ldapdiff” oldalszám: 217
- “Az SSL védelem LDAP parancssori segédprogramok használata” oldalszám: 220

Ügyeljen rá, hogy a Qshell parancskörnyezetben egyes karaktersorozatokat idézőjelek között kell megadni a helyes feldolgozás érdekében. Ez általában az olyan karaktersorozatokra vonatkozik, mint a DN-ek, keresési szűrők, valamint az ldapsearch által visszaadott attribútumlista. Az alábbi listában bemutatunk néhány példát.

- Szóközöket tartalmazó karaktersorozatok: "cn=John Smith,cn=users"
- Helyettesítő karaktereket tartalmazó karaktersorozat: "*"
- Zárójeleket tartalmazó karaktersorozatok: "(objectclass=person)"

További információkat a Qshell parancskörnyezetről a “Qshell” témakörben talál.

ldapmodify és ldapadd

Az LDAP modify-entry (bejegyzésmódosító) és LDAP add-entry (bejegyzés-feltevő) eszközök

Összegzés

```
ldapmodify [-a] [-b] [-c] [-C karakterkészlet] [-d  
nyomkövetési_szint] [-D binddn] [-g]  
[-f fájl] [-F] [-g] [-G tartomány] [-h ldaphoszt] [-i fájl] [-k] [-K kulcsfájl]  
[-m mechanizmus] [-M] [-n] [-N igazolásnév] [-O max_szakasz] [-p ldapport]  
[-P kulcsfájl-jelszó] [-r] [-R] [-U felhasználónév] [-v] [-V] [-w jelszó | ?] [-y proxydn]  
[-Y] [-Z]
```

```
ldapadd [-a] [-b] [-c] [-C karakterkészlet] [-d nyomkövetési_szint] [-D binddn] [-g]  
[-f fájl] [-F] [-g] [-G tartomány] [-h ldaphoszt] [-i fájl] [-k] [-K kulcsfájl]  
[-m mechanizmus] [-M] [-n] [-N igazolásnév] [-O max_szakasz] [-p ldapport]  
[-P kulcsfájl-jelszó] [-r] [-R] [-U felhasználónév] [-v] [-V] [-w jelszó | ?] [-y proxydn]  
[-Y] [-Z]
```

Leírás

Az **ldapmodify** egy parancssori felület az `ldap_modify`, `ldap_add`, `ldap_delete` és `ldap_modrdn` alkalmazásprogram illesztőkhöz (API-khoz). Az **ldapadd** az `ldapmodify` átnevezett változataként került megvalósításra. `ldapadd` néven meghívva, a **-a** (új bejegyzés hozzáadása) jelző automatikusan bekapcsolásra kerül.

Az **ldapmodify** megnyit egy kapcsolatot egy LDAP szerver felé, majd kapcsolódik hozzá. Az **ldapmodify** programmal módosíthatók és felvehetők bejegyzések. A bejegyzések információit a program a szabványos bemenetről olvassa, vagy az **-i** kapcsoló megadása esetén egy fájlból.

Az **ldapmodify** vagy **ldapadd** parancs szintaxisának megjelenítéséhez írja be az alábbi parancsot:

```
ldapmodify -?
```

vagy

```
ldapadd -?
```

Beállítások

- a** Új bejegyzések felvétele. Az **ldapmodify** alapértelmezett tevékenysége a létező bejegyzések módosítása. **ldapadd** néven meghívva a programot, ez a kapcsoló automatikusan beállításra kerül.
- b** Feltételezi, hogy minden érték, amely a ``/`` karakterrel kezdődik, bináris érték, és a tényleges érték egy fájlban található, amelynek elérési útvonala az érték helyén van megadva.
- c** Folyamatos működési üzemmód. A hibákat jelenti a program, de az **ldapmodify** tovább végzi a módosításokat. Egyébként az alapértelmezés a hiba jelzése után kilépés.
- C karakterkészlet**
Azt jelzi, hogy az **ldapmodify** és **ldapadd** segédprogram bemenetén a karakterláncok a "karakterkészlet" paraméter által jelzett helyi karakterkészlet kódolásúak, és ezeket UTF-8 karakterkészletre kell konvertálni. Akkor használja a **-C karakterkészlet** paramétert, ha a bemeneti karakterlánc kódlapja eltér a job kódlapjától. Az `ldap_set_iconv_local_charset()` dokumentációjában megtalálhatja a támogatott "karakterkészlet" értékeket.
- d nyomkövetési_szint**
Az LDAP nyomkövetési szintet a "nyomkövetési_szint" paraméter értékére állítja be.
- D binddn**
A **binddn** paraméter által megadott kapcsolódási DN-t használja az LDAP címtárhoz kapcsolódáshoz. A **binddn** egy karakterláncal képviselt DN. Az **-m DIGEST-MD5** kapcsolóval használva a hitelesítési azonosító megadására szolgál. Lehet egy DN, vagy egy "u:" vagy "dn:" jellel kezdődő authZid karaktersorozat.
- f fájl** A bejegyzés módosítási információinak beolvasása a megadott LDIF fájlból történik, nem a szabványos bemenetről. Ha nincs külön LDIF fájl megadva, akkor a szabványos bemenetet kell használni az LDIF formátumú frissítési rekordok kijelölésére.
- F** Kikényszeríti az összes változás alkalmazását, függetlenül a replica: karaktersorozattal kezdődő bemeneti sorok tartalmától (alapértelmezésben a replica: kezdetű sorok az LDAP szerverhoszttal és -porttal kerülnek összehasonlításra annak eldöntésére, hogy egy replikációs naplóbejegyzést aktuálisan alkalmazni kell-e).
- g** Ne válassza le az attribútumértékeket követő szóközőket.
- G** Megadja a tartományt. Ez a paraméter nem kötelező. Az **-m DIGEST-MD5** kapcsolóval használva az érték a kapcsolódás során átadásra kerül a szervernek.
- hdaphoszt**
Egy alternatív hoszt megadása, amelyiken az LDAP szerver fut.
- i fájl** A bejegyzés módosítási információinak beolvasása a megadott LDIF fájlból történik, nem a szabványos bemenetről. Ha nincs külön LDIF fájl megadva, akkor a szabványos bemenetet kell használni az LDIF formátumú frissítési rekordok kijelölésére.
- k** A szerver adminisztrációs vezérlés használatát írja elő.
- K kulcsfájl**
Megadja a **kdb** alapértelmezett kiterjesztésű SSL kulcsadatbázis-fájl nevét. Ha a kulcsadatbázis-fájl nem az

aktuális könyvtárban található, megadja az adatbázisfájl teljes nevét. Ha a kulcsadatbázis-fájl neve nincs megadva, akkor ez a program az SSL_KEYRING környezeti változóban keres hozzá tartozó fájlnevet. Ha az SSL_KEYRING környezeti változó nincs megadva, akkor - feltéve, hogy az létezik -, a program a rendszer kulcsesemő fájlját használja.

Ez a paraméter engedélyezi a **-Z** kapcsolót. Az i5/OS alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

-m *mechanizmus*

A **mechanizmus** a szerverhez kapcsolódáshoz használt SASL eljárás. A rendszer az ldap_sasl_bind_s() API-t használja. Az **-m** paraméter figyelmen kívül marad, ha a **-V 2** kapcsoló be van állítva. Ha a **-m** kapcsoló nincs megadva, akkor egyszerű hitelesítés történik. Az érvényes mechanizmusok:

- CRAM-MD5 - védi a szervernek elküldött jelszót.
- EXTERNAL - az SSL igazolást használja. Szükséges a **-Z** kapcsoló megadása is.
- GSSAPI - a felhasználó Kerberos hitelesítési adatait használja
- DIGEST-MD5 - azt igényli, hogy a kliens küldjön egy felhasználónév-értéket a szerverre. Szükséges a **-U** kapcsoló megadása is. A hitelesítési azonosító megadására a **-D** paraméter (általában a kapcsolati DN) használható. Lehet egy DN, vagy egy u: vagy dn: jellel kezdődő authzId karaktersorozat.
- OS400_PRFTKN - hitelesíti magát a helyi LDAP szerverhez az aktuális i5/OS felhasználóként a felhasználó megkülönböztetett nevét használva a rendszer leképezett háttérben. Nem kell megadni a **-D** (kapcsolati DN) és a **-w** (jelszó) paramétereket.

-M Az utalási objektumok normál bejegyzésként kezelése.

-n Megmutatja, mi történne, de valójában nem változtatja meg a bejegyzéseket. Hibakereséskor hasznos a **-v** paraméterrel együtt.

-N *igazolásnév*

A kulcsadatbázis-fájlban található kliensigazoláshoz tartozó azonosítót adja meg. Amennyiben az LDAP szerver csak szerver hitelesítésre lett beállítva, a kliensigazolásra nincs szükség. Ha az LDAP szerver kliens- és szerverhitelesítésre lett beállítva, a kliensigazolásra szükség van. A **igazolásnév** nem szükséges, ha egy alapértelmezés szerinti igazolás/privát kulcspár alapértelmezés szerintinek lett kijelölve. Hasonlóképpen akkor sem szükséges az **igazolásnév**, ha van egy egyedi igazolás/privát kulcspár a megjelölt adatbázisfájlban. Ez a paraméter figyelmen kívül marad, ha sem a **-Z**, sem a **-K** kapcsoló nincs megadva. Az i5/OS alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

-O *max_szakasz*

A **max_szakasz** beállítja azoknak a szakaszoknak a maximális számát, amelyeket a klienskönyvtár az utalások kereséskor számba vesz. Az alapértelmezett szakaszszám érték 10.

-p *ldapport*

Egy alternatív TCP port megadása, amelyiken az LDAP szerver figyel. Az alapértelmezés szerinti LDAP port a 389. Ha a **-p** kapcsoló nincs megadva, de a **-Z** kapcsoló igen, akkor a rendszer az alapértelmezés szerinti 636-os LDAP SSL portot használja.

-P *kulcsfájl_jelszó*

A kulcsadatbázis jelszavát adja meg. A jelszó a kulcsadatbázis-fájl rejtjelezett tartalmának (amely egy vagy több privát kulcsot is tartalmazhat) eléréséhez szükséges. Ha rendelve lett jelszótároló fájl a kulcsadatbázis-fájlhoz, akkor a jelszó a jelszótároló fájlból kérdezhető le, ezért a **-P** paraméterre nincs szükség. Ez a paraméter figyelmen kívül marad, ha sem a **-Z**, sem a **-K** nincs megadva.

-r A meglévő értékek lecserélése alapértelmezés szerinti értékekre.

-R Azt határozza meg, hogy az utalásokat nem kell automatikusan követni.

-U Megadja a felhasználónevet. Az **-m** DIGEST-MD5 használata esetén szükséges, minden más mechanizmussal figyelmen kívül marad.

-v Bővebb diagnosztikai információt nyújt, amelyet a szabványos kimenetre ír.

-V változat

Megadja, hogy az **ldapmodify** parancs melyik LDAP változatot használja a szervertel való kapcsolódáskor. Alapértelmezés szerint LDAP V3 összeköttetést létesít. Ahhoz, hogy kifejezetten az LDAP V3 legyen kiválasztva, **-V 3** kapcsolót kell megadni. Adja meg a **-V 2** kapcsolót, ha LDAP V2 alkalmazásként kívánja futtatni.

-w jelszó | ?

A **jelszó** használata hitelesítési jelszóként. A ? karakter megadása esetén a program bekéri a jelszót.

| -y proxydn

Megadja a proxy azonosítót a proxy hitelesítési beállításokhoz.

| -Y Biztonságos LDAP kapcsolatot (TLS) használ.

-Z Védett SSL kapcsolat használata az LDAP szervertel folyó kommunikáció során. Az i5/OS alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

Bemenet formátuma

A fájl (vagy ha nincs **-i** kapcsoló megadva a parancssorban, akkor a szabványos bemenet) formátumának meg kell felelnie az LDIF formátumnak. Az LDIF formátummal kapcsolatos további információk: "LDAP adatcsere formátum (LDIF)" oldalszám: 220.

Példák

Tételezzük fel, hogy a /tmp/entrymods nevű fájl már 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: /tmp/modme.jpeg
-
delete: description
-
```

akkor a következő parancs:

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

lecseréli a Modify Me bejegyzés mail attribútumát a modme@student.of.life.edu értékre, felveszi a title attribútum értékeként a Grand Poobah szöveget, hozzáadja a /tmp/modme.jpeg fájl tartalmát a jpegPhoto attribútumhoz, és törli a description attribútumot. Ugyanezek a módosítások végrehajthatók a régebbi ldapmodify bemeneti formátummal is:

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

és a következő paranccsal:

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

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: a világ leghíresebb ismeretlen személye
mail: johndoe@student.of.life.edu
uid: jdoe
```

akkor a következő parancs:

```
ldapadd -i /tmp/entrymods
```

felvesz egy új bejegyzést John Doe számára, amely értékeit a /tmp/newentry fájlból veszi.

Megjegyzés

Ha nem adja meg a bejegyzés információit egy fájlban, a **-i** kapcsoló segítségével, akkor az **ldapmodify** parancs várakozik, hogy a bejegyzéseket a szabványos bemenetről olvassa be.

Diagnosztika

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

Ldapdelete

Az LDAP delete-entry (bejegyzéstörölő) eszköz

Összegzés

```
ldapdelete [-c] [-C karakterkészlet] [-d nyomkövetési_szint] [-D
binddn] [-f fájl]
[-G tartomány] [-h ldaphoszt] [-i fájl] [-k] [-K kulcsfájl] [-m mechanizmus]
[-M] [-n] [-N igazolásnév] [-O max szakasz] [-p ldapport]
[-P kulcsfájljelszó] [-R] [-s] [-U felhasználónév] [-v] [-V verzió]
[-w fejlészó] [-y proxydn] [-Y] [-Z] [dn].....
```

Leírás

Az **ldapdelete** egy parancssori illesztő az ldap_delete alkalmazási programcsatolóhoz (API).

Az **ldapdelete** megnyit egy kapcsolatot egy LDAP szerver felé, majd kapcsolódik hozzá. Ha egy vagy több megkülönböztetett név (DN) argumentumot megad a parancshoz, akkor az adott DN-ű bejegyzések törlésre kerülnek. Az összes DN karakterlánccal képviselt DN. Ha nincs DN paraméter megadva, akkor a DN-ek listáját a program a szabványos bemenetről olvassa, illetve a **-i** kapcsoló használata esetén egy fájlból.

Az **ldapdelete** parancs szintaxisának megjelenítéséhez írja be az alábbi parancsot:

```
ldapdelete -?
```

Beállítások

-c Folyamatos működési üzemmód. A hibákat jelenti a program, de az **ldapdelete** tovább végzi a törléseket. Egyébként az alapértelmezés a hiba jelzése után kilépés.

-C karakterkészlet

Azt jelzi, hogy az **ldapdelete** segédprogram bemeneteként megadott DN-ek ábrázolása a "karakterkészlet" paraméterben megadott helyi karakterkészlet szerint történik. Akkor használja a **-C karakterkészlet** paramétert, ha a bemeneti karakterlánc kódlapja eltér a job kódlapjától. Az ldap_set_iconv_local_charset() dokumentációjában megtalálhatja a támogatott "karakterkészlet" értékeket.

-d nyomkövetési_szint

Az LDAP nyomkövetési szintet a "nyomkövetési_szint" paraméter értékére állítja be.

-D binddn

A **binddn** paraméter által megadott kapcsolódási DN-t használja az LDAP címtárhoz kapcsolódáshoz. A **binddn** egy karakterláncsal képviselt DN. Az -m DIGEST-MD5 kapcsolóval használva a hitelesítési azonosító megadására szolgál. Lehet egy DN, vagy egy "u:" vagy "dn:" jellel kezdődő authzId karaktersorozat.

-f file Egy fájlból olvas be sorokat, minden sorra végrehajt egy LDAP törlést. Mindegyik sor egyetlen megkülönböztetett nevet (DN) tartalmazhat.

-G realm

Megadja a tartományt. Ez a paraméter nem kötelező. Az -m DIGEST-MD5 kapcsolóval használva az érték a kapcsolódás során átadásra kerül a szervernek.

-hldaphoszt

Alternatív hoszt megadása, amelyiken az LDAP szerver fut.

-i fájl Egy fájlból olvas be sorokat, minden sorra végrehajt egy LDAP törlést. Mindegyik sor egyetlen megkülönböztetett nevet (DN) tartalmazhat.

-k A szerver adminisztrációs vezérlés használatát írja elő.

-K kulcsfájl

Az SSL kulcsadatbázis-fájl nevét adja meg. Ha a kulcsadatbázis-fájl nem az aktuális könyvtárban található, megadja az adatbázisfájl teljes nevét.

Ha a segédprogram nem találja meg a kulcsadatbázist, akkor az alapértelmezés szerinti megbízható jogosultság gyökerek hardver-kódolt készletét fogja használni. A kulcsadatbázis-fájl általában egy vagy több, a kliens által megbízhatónak tartott CA-któl származó igazolást tartalmaz. Ezeket az X.509 típusú igazolásokat megbízható gyökereknek is hívják.

Ez a paraméter engedélyezi a -Z kapcsolót. Az i5/OS alatt futó Directory Server esetében, ha a -Z kapcsolót használja, de a -K vagy -N kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

-m mechanizmus

A **mechanizmus** a szerverhez kapcsolódáshoz használt SASL eljárás. A rendszer az ldap_sasl_bind_s() API-t használja. Az -m paraméter figyelmen kívül marad, ha a -V 2 kapcsoló be van állítva. Ha a -m kapcsoló nincs megadva, akkor egyszerű hitelesítés történik. Az érvényes mechanizmusok:

- CRAM-MD5 - védi a szervernek elküldött jelszót.
- EXTERNAL - az SSL igazolást használja. Szükséges a -Z kapcsoló megadása is.
- GSSAPI - a felhasználó Kerberos hitelesítési adatait használja
- DIGEST-MD5 - azt igényli, hogy a kliens küldjön egy felhasználónév-értéket a szerverre. Szükséges a -U kapcsoló megadása is. A hitelesítési azonosító megadására a -D paraméter (általában a kapcsolati DN) használható. Lehet egy DN, vagy egy u: vagy dn: jellel kezdődő authzId karaktersorozat.
- OS400_PRFTKN - hitelesíti magát a helyi LDAP szerverhez az aktuális i5/OS felhasználóként a felhasználó megkülönböztetett nevét használva a rendszer leképezett háttérben. Nem kell megadni a -D (kapcsolati DN) és a -w (jelszó) paramétereket.

-M Az utalási objektumok normál bejegyzésként kezelése.

-n Megmutatja, mi történne, de valójában nem változtatja meg a bejegyzéseket. Hibakereséskor hasznos a -v paraméterrel együtt.

-N igazolásnév

A kulcsadatbázis-fájlban található kliensigazoláshoz tartozó azonosítót adja meg. Amennyiben az LDAP szerver csak szerver hitelesítésre lett beállítva, a kliensigazolásra nincs szükség. Ha az LDAP szerver kliens- és szerverhitelesítésre lett beállítva, a kliensigazolásra szükség van. Az **igazolásnév** nem szükséges, ha egy alapértelmezett igazolás/privát kulcspár alapértelmezettként ki lett jelölve. Hasonlóképpen akkor sem szükséges az **igazolásnév**, ha van egy egyedi igazolás/privát kulcspár a megjelölt adatbázisfájlban. Ez a paraméter figyelmen kívül marad, ha sem a -Z, sem a -K kapcsoló nincs megadva. Az i5/OS alatt futó Directory Server esetében, ha a -Z kapcsolót használja, de a -K vagy -N kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

-O *max_szakasz*

A **max_szakasz** beállítja azoknak a szakaszoknak a maximális számát, amelyeket a klienskönyvtár az utalások keresésekor számba vesz. Az alapértelmezett szakaszszám érték 10.

-p *ldapport*

Egy alternatív TCP port megadása, amelyiken az LDAP szerver figyel. Az alapértelmezés szerinti LDAP port a 389. Ha a **-p** kapcsoló nincs megadva, de a **-Z** kapcsoló igen, akkor a rendszer az alapértelmezés szerinti 636-os LDAP SSL portot használja.

-P *kulcsfajl_jelszo*

A kulcsadatbázis jelszavát adja meg. A jelszó a kulcsadatbázis-fájl rejtjelezett tartalmának (amely egy vagy több privát kulcsot is tartalmazhat) eléréséhez szükséges. Ha rendelve lett jelszótároló fájl a kulcsadatbázis-fájlhoz, akkor a jelszó a jelszótároló fájlból kérdezhető le, ezért a **-P** paraméterre nincs szükség. Ez a paraméter figyelmen kívül marad, ha sem a **-Z**, sem a **-K** nincs megadva.

-R Azt határozza meg, hogy az utalásokat nem kell automatikusan követni.

-s Ezzel a kapcsolóval törölheti a megadott bejegyzésnél kezdődő teljes részét.

-U *felhasználónév*

Adja meg a felhasználónevet. Az **-m** DIGEST-MD5 használata esetén szükséges, minden más mechanizmussal figyelmen kívül marad.

-v Bővebb diagnosztikai információt nyújt, amelyet a szabványos kimenetre ír.

-V *változat*

Megadja, hogy az **ldapdelete** parancs melyik LDAP változatot használja a szerverhez kapcsolódáskor. Alapértelmezés szerint LDAP V3 összeköttetést létesít. Ahhoz, hogy kifejezetten az LDAP V3 legyen kiválasztva, **-V 3** kapcsolót kell megadni. Adja meg a **-V 2** kapcsolót, ha LDAP V2 alkalmazásként kívánja futtatni.

-w *jelszo | ?*

A **jelszo** használata hitelesítési jelszóként. A ? karakter megadása esetén a program bekéri a jelszót.

-y *proxydn*

Megadja a proxy azonosítót a proxy hitelesítési művelethez.

-Y Biztonságos LDAP kapcsolatot (TLS) használ.

-Z Védett SSL kapcsolat használata az LDAP szerverrel folyó kommunikáció során. Az i5/OS alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

dn Egy vagy több DN argumentumot ad meg. Minden egyes DN egy karakterlánccal képviselt DN.

Példák

A következő parancs:

```
ldapdelete -D cn=administrator -w secret "cn=Delete Me, o=University of Life, c=US"
```

megkísérli törölni a "Delete Me" commonName attribútumú bejegyzést közvetlenül a University of Life szervezeti bejegyzés alól:

Megjegyzés

Ha nem ad meg DN argumentumokat, akkor az **ldapdelete** parancs a szabványos bemenetről várja a DN-ek listáját.

Diagnosztika

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

ldapexop

Az LDAP kibővített művelet eszköz

Összegzés

```
ldapexop [-C karakterkészlet] [-d nyomkövetési_szint] [-D binddn] [-e] [-G tartomány]
[-h ldaphoszt] [-help] [-K kulcsfájl] [-m mechanizmus] [-N igazolásnév]
[-p ldapport] [-P kulcsfájl_jelszó] [-?] [-v] [-w jelszó | ?] [-Z]
-op {cascrepl | controlqueue | controlrepl | getAttributes |
getusertype | quiesce | readconfig | uniqueattr}
```

Leírás

Az **ldapexop** segédprogram egy parancssori felület, amelynek használatával a szerverhez csatlakozva kiadható egy kiterjesztett művelet adatokkal együtt, amelyek a kiterjesztett művelet értékét adják.

Az **ldapexop** segédprogram támogatja a többi LDAP segédprogram által is használt szabványos hoszt, port, SSL és hitelesítési beállításokat. Ezenfelül további kapcsolókkal adható meg a végrehajtani kívánt művelet, illetve az egyes kiterjesztett műveletek paraméterei

Az **ldapexop** parancs szintaxisának megjelenítéséhez írja be az alábbi parancsot:

```
ldapexop -?
```

vagy

```
ldapexop -help
```

Beállítások

Az **ldapexop** parancs beállításai két kategóriára oszthatók:

1. Általános beállítások, amelyek a címtárszerverhez kapcsolódást szabályozzák. Ezeket a beállításokat a műveletspecifikus beállítások előtt meg kell adni.
2. Kiterjesztett műveleti beállítások, amelyek a végrehajtandó kiterjesztett műveletet azonosítják.

Általános beállítások

Ezek a beállítások szabályozzák a szerverhez kapcsolódás módját és még az **-op** kapcsoló előtt kell szerepelniük.

-C karakterkészlet

Azt jelzi, hogy az **ldapexop** segédprogram bemeneteként megadott DN-ek ábrázolása a "karakterkészlet" paraméterben megadott helyi karakterkészlet szerint történik. Akkor használja a **-C karakterkészlet** paramétert, ha a bemeneti karakterlánc kódlapja eltér a job kódlapjától. Az `ldap_set_iconv_local_charset()` dokumentációjában megtalálhatja a támogatott "karakterkészlet" értékeket.

-d nyomkövetési_szint

Az LDAP nyomkövetési szintet a "nyomkövetési_szint" paraméter értékére állítja be.

-D binddn

A **binddn** paraméter által megadott kapcsolódási DN-t használja az LDAP címtárhoz kapcsolódáshoz. A **binddn** egy karakterláncal képviselt DN. Az **-m** DIGEST-MD5 kapcsolóval használva a hitelesítési azonosító megadására szolgál. Lehet egy DN, vagy egy "u:" vagy "dn:" jellel kezdődő authzId karaktersorozat.

-e Kijelöl az LDAP könyvtár verziószámát, majd kilép.

-G Megadja a tartományt. Ez a paraméter nem kötelező. Az **-m** DIGEST-MD5 kapcsolóval használva az érték a kapcsolódás során átadásra kerül a szervernek.

-hldaphoszt

Alternatív hoszt megadása, amelyiken az LDAP szerver fut.

-help A parancs szintaxisával és használatával kapcsolatos információkat jelenít meg.

-K kulcsfájl

Az SSL kulcsadatbázis-fájl nevét adja meg. Ha a kulcsadatbázis-fájl nem az aktuális könyvtárban található, megadja az adatbázisfájl teljes nevét.

Ha a segédprogram nem találja meg a kulcsadatbázist, akkor a rendszer kulcsadatbázisát fogja használni. A kulcsadatbázis-fájl általában egy vagy több, a kliens által megbízhatónak tartott CA-któl származó igazolást tartalmaz. Ezeket az X.509 típusú igazolásokat megbízható gyökereknek is hívják.

Ez a paraméter engedélyezi a **-Z** kapcsolót. Az i5/OS alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

-m mechanizmus

A **mechanizmus** a szerverhez kapcsolódáshoz használt SASL eljárás. A rendszer az `ldap_sasl_bind_s()` API-t használja. Az **-m** paraméter figyelmen kívül marad, ha a **-V 2** kapcsoló be van állítva. Ha a **-m** kapcsoló nincs megadva, akkor egyszerű hitelesítés történik. Az érvényes mechanizmusok:

- CRAM-MD5 - védi a szervernek elküldött jelszót.
- EXTERNAL - az SSL igazolást használja. Szükséges a **-Z** kapcsoló megadása is.
- GSSAPI - a felhasználó Kerberos hitelesítési adatait használja
- DIGEST-MD5 - azt igényli, hogy a kliens küldjön egy felhasználónév-értéket a szerverre. Szükséges a **-U** kapcsoló megadása is. A hitelesítési azonosító megadására a **-D** paraméter (általában a kapcsolati DN) használható. Lehet egy DN, vagy egy `u:` vagy `dn:` jellel kezdődő `authzId` karaktersorozat.
- OS400_PRFTKN - hitelesíti magát a helyi LDAP szerverhez az aktuális i5/OS felhasználóként a felhasználó megkülönböztetett nevét használva a rendszer leképezett hátterében. Nem kell megadni a **-D** (kapcsolati DN) és a **-w** (jelszó) paramétereket.

-N igazolásnév

A kulcsadatbázis-fájlban található kliensigazoláshoz tartozó azonosítót adja meg. Amennyiben az LDAP szerver csak szerver hitelesítésre lett beállítva, a kliensigazolásra nincs szükség. Ha az LDAP szerver kliens- és szerverhitelesítésre lett beállítva, a kliensigazolásra szükség van. Az **igazolásnév** nem szükséges, ha egy alapértelmezett igazolás/privát kulcspár alapértelmezettként ki lett jelölve. Hasonlóképpen akkor sem szükséges az **igazolásnév**, ha van egy egyedi igazolás/privát kulcspár a megjelölt adatbázisfájlban. Ez a paraméter figyelmen kívül marad, ha sem a **-Z**, sem a **-K** kapcsoló nincs megadva. Az i5/OS alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

-p ldapport

Egy alternatív TCP port megadása, amelyiken az LDAP szerver figyel. Az alapértelmezés szerinti LDAP port a 389. Ha a **-p** kapcsoló nincs megadva, de a **-Z** kapcsoló igen, akkor a rendszer az alapértelmezés szerinti 636-os LDAP SSL portot használja.

-P kulcsfájl_jelszó

A kulcsadatbázis jelszavát adja meg. A jelszó a kulcsadatbázis-fájl rejtjelezett tartalmának (amely egy vagy több privát kulcsot is tartalmazhat) eléréséhez szükséges. Ha rendelve lett jelszótároló fájl a kulcsadatbázis-fájlhoz, akkor a jelszó a jelszótároló fájlból kérdezhető le, ezért a **-P** paraméterre nincs szükség. Ez a paraméter figyelmen kívül marad, ha sem a **-Z**, sem a **-K** nincs megadva.

-? A parancs szintaxisával és használatával kapcsolatos információkat jelenít meg.

-U Adja meg a felhasználónevet. Az **-m** DIGEST-MD5 használata esetén szükséges, minden más mechanizmussal figyelmen kívül marad.

-v Bővebb diagnosztikai információt nyújt, amelyet a szabványos kimenetre ír.

-w jelszó | ?

A **jelszó** használata hitelesítési jelszóként. A **?** karakter megadása esetén a program bekéri a jelszót.

-Y Biztonságos LDAP kapcsolatot (TLS) használ.

-Z Védett SSL kapcsolat használata az LDAP szerverrel folyó kommunikáció során. Az i5/OS alatt futó

Directory Server esetében, ha a -Z kapcsolót használja, de a -K vagy -N kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

Kiterjesztett műveleti beállítások

A **-op** kapcsoló után kell megadni a végrehajtandó kiterjesztett műveletet. A kiterjesztett művelet az alábbiak egyike lehet:

- **cascrepl**: lépcsőzetes vezérlésű replikáció kiterjesztett művelet. A kért művelet a megadott szerverre alkalmazása után a rendszer továbbadja az adott részfa összes további replikájának is. Ha ezek bármelyike továbbító replika, akkor azok a kiterjesztett műveletet továbbadják saját replikáiknak. A művelet lépcsőzetesen végighalad a teljes replikációs topológián.

-action quiesce | unquiesce | replnow | wait

Ez egy kötelező attribútum, amely azt jelzi, hogy pontosan milyen műveletet is kell végrehajtani.

quiesce

További frissítések letiltása (kivéve a replikációból származó frissítéseket).

unquiesce

Normális működés visszaállítása, a szerver újra fogadja a klienskéréseket.

replnow

Az összes sorbaállított módosítás replikálása az összes replikaszerverre a lehető leghamarabb, ütemezéstől függetlenül.

wait A frissítések replikációjának várakoztatása.

-rc contextDn

Ez egy kötelező attribútum, amely a részfa gyökerét adja meg.

-timeout secs

Ez egy elhagyható attribútum; ha jelen van, egy időkorlátot ad meg, másodpercben. Ha nincs jelen, a program 0-nak tekinti az értékét (nincs időkorlát).

Példa:

```
ldapexop -op cascrepl -action -quiesce -rc "o=acme,c=us" -timeout 60
```

- **controlqueue**: vezérlési sor replikáció kiterjesztett művelet. Ezzel a művelettel törölhetők a függőben lévő módosítások a replikációs hibák miatt felgyűlt és nem lefutott replikációs módosítások listájából. Ez a művelet akkor hasznos, ha kézzel javítja a replika adatait. Ekkor ezzel a művelettel lehet átugrani a felgyűlt hibák egy részét.

-skip all | change-id

Ez egy kötelező attribútum.

- A **-skip all** a megállapodás összes függőben lévő módosításának átugrását jelenti.
- A **change-id** paraméter egy kihagyandó módosítást azonosít. Ha a szerver pillanatnyilag nem replikálja ezt a módosítást, akkor a kérés meghiúsul.

-ra agreementDn

Ez egy kötelező attribútum, amely a replikációs megállapodás DN-jét adja meg.

Példák:

```
ldapexop -op controlqueue -skip all -ra "cn=server3,  
ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,  
o=acme,c=us"
```

```
ldapexop -op controlqueue -skip 2185 -ra "cn=server3,  
ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,  
o=acme,c=us"
```

- **controlrepl**: replikáció vezérlése kiterjesztett művelet

-action suspend | resume | replnow

Ez egy kötelező attribútum, amely azt jelzi, hogy pontosan milyen műveletet is kell végrehajtani.

-rc contextDn | -ra agreementDn

Az **-rc contextDn** a replikációs kontextus DN-je. A művelet a kontextus összes megállapodásán végrehajtásra kerül. Az **-ra agreementDn** a replikációs kontextus DN-je. A művelet csak az adott replikációs megállapodáson kerül végrehajtásra.

Példa:

```
ldapexop -op controlrepl -action suspend -ra "cn=server3,  
ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,  
o=acme,c=us"
```

- **getattributes -attrType<típus> -matches bool<érték>**

-attrType {operational | language_tag | attribute_cache | unique | configuration}

Ez egy kötelező attribútum, amely a lekérdezendő attribútum típusát adja meg.

-matches bool {true | false}

Megadja, hogy a visszaadott attribútumok listája megfelel-e az **-attrType<** beállításban megadott attribútumtípusnak.

Példa:

```
ldapexop -op getattributes -attrType unique -matches bool true
```

Visszaadja az összes attribútum listáját, amely egyedi attribútumként került megjelölésre.

```
ldapexop -op getattributes -attrType unique -matches bool false
```

Visszaadja az összes attribútum listáját, amely nem került egyedi attribútumként megjelölésre.

- **getusertype:** kért felhasználó típusú kiterjesztett művelet

Ez a kiterjesztett művelet visszaadja a felhasználótípust a kapcsolati DN alapján.

Példa:

```
ldapexop - D <AdminDN> -w <Adminpw> -op getusertype
```

Visszaadott érték:

User : root_administrator

Szerep(ek) : server_config_administrator directory_administrator

- **quiesce:** részfa zárolása (zárolás feloldása) kiterjesztett művelet

-rc contextDn

Ez egy kötelező attribútum, amely a zárolandó (vagy feloldandó) replikációs megállapodás (részfa) DN-jét adja meg.

-end Ez egy elhagyható attribútum; ha jelen van, a részfa zárolásának feloldását adja meg. Ha nincs megadva, akkor az alapértelmezett művelet a részfa zárolása.

Példák:

```
ldapexop -op quiesce -rc "o=acme,c=us"
```

```
ldapexop -op quiesce -end -rc "o=ibm,c=us"
```

- **readconfig:** konfigurációs fájl újraolvasása kiterjesztett művelet

-scope entire | single<bejegyzés DN><attribútum>

Ez egy kötelező attribútum.

– Az **entire** paraméter megadása a teljes konfigurációs fájl újraolvasását eredményezi.

– A **single** paraméter megadása a megadott bejegyzés és attribútum újraolvasását eredményezi.

Példák:

```
ldapexop -op readconfig -scope entire
```

```
ldapexop -op readconfig -scope single "cn=configuration" ibm-slappAdminPW
```

Megjegyzés: Az alábbi lista bejegyzéseire vonatkozó megjegyzések:

- ¹ readconfig után azonnal érvénybe lép
- ² új műveletek esetén lép életbe
- ³ a jelszó módosítása esetén azonnal életbe lép (nincs szükség a konfiguráció kiolvasására)
- ⁴ a parancssori segédprogram támogatja i5/OS rendszer alatt, de az i5/OS rendszeren futó Directory Server nem

```
cn=Configuration
ibm-slapdadmin2
ibm-slapdadminpw2, 3
ibm-slapderrorlog1, 4
ibm-slapdpwencryption1
ibm-slapdsizelimit1
ibm-slapdsysloglevel1, 4
ibm-slapdtimelimit1
```

```
cn=Front End, cn=Configuration
ibm-slapdaclcache1
ibm-slapdaclcachesize1
ibm-slapdentrycachesize1
ibm-slapdfiltercachebypasslimit1
ibm-slapdfiltercachesize1
ibm-slapdidletimeout1
```

```
cn=Event Notification, cn=Configuration
ibm-slapdmaxeventsperconnection2
ibm-slapdmaxeventstotal2
```

```
cn=Transaction, cn=Configuration
ibm-slapdmaxnumoftransactions2
ibm-slapdmaxoppertransaction2
ibm-slapdmaxtimelimitoftransactions2
```

```
cn=ConfigDB, cn=Config Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdreadonly2
```

```
cn=Directory, cn=RDBM Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdbulkloaderrors1, 4
ibm-slapdclierrors1, 4
ibm-slapdpagedresallownonadmin2
ibm-slapdpagedreslmt2
ibm-slapdpagesizelmt2
ibm-slapdreadonly2
ibm-slapdsortkeylimit2
ibm-slapdsortsrchallownonadmin2
ibm-slapdsuffix2
```

- **unbind** {-dn<specificDN>| -ip<sourceIP> | -dn<specificDN> -ip<sourceIP> | all}:

megszünteti a kapcsolatokat DN, IP, DN/IP alapján vagy minden kapcsolatot megszüntet. A műveletek nélküli és a feladat várakozási sorban álló műveletekkel rendelkező kapcsolatok azonnal megszakadnak. Ha egy dolgozó jelenleg használ egy kapcsolatot, akkor az lezárásra kerül, amint a dolgozó a műveletet befejezi.

-dn<specificDN>

Kiad egy kapcsolatlezárási kérést csak egy DN alapján. Ez a kérés a megadott DN összes kapcsolatának kiürítését eredményezi.

-ip<sourceIP>

Kiad egy kapcsolatlezárási kérést csak egy IP-cím alapján. Ez a kérés a megadott IP-forrás összes kapcsolatának kiürítését eredményezi.

-dn<specificDN> **-ip**<sourceIP>

Kiad egy kérést egy DN/IP-cím által meghatározott kapcsolat lezárására. Ez a kérés a megadott DN és a meghatározott IP-forrás összes kapcsolatának kiürítését eredményezi.

-all Kiad egy kérést az összes kapcsolat lezárására. Ez a kérés az összes kapcsolat kiürítését eredményezi, kivéve azét, ahonnan a kérés érkezett. Az attribútum nem használható a -D vagy -IP attribútumokkal.

Példák:

```
ldapexop -op unbind -dn cn=john
ldapexop -op unbind -ip 9.182.173.43
ldapexop -op unbind -dn cn=john -ip 9.182.173.43
ldapexop -op unbind -all
```

- **uniqueattr -a <attributeType>**: azonosítja egy adott attribútum összes nem egyedi attribútumát.

-a <attribute>

Megad egy attribútumot, amelynek minden ütköző értéke felsorolásra kerül.

Megjegyzés: Nem jelennek meg a bináris, műveleti és konfigurációs attribútumok többször szereplő értékei, valamint az objectclass attribútum. Ezeket az attribútumokat az egyedi attribútumok kiterjesztett műveletei nem támogatják.

Példa:

```
ldapexop -op uniqueattr -a "uid"
```

A következő sor ennél a kiterjesztett műveletnélhozzáadásra kerül a konfigurációs fájlhoz a "cn=Directory,cn=RDBM Backends,cn=IBM Directory,cn=schema,cn=Configuration" bejegyzés alatt:

```
ibm-slapdPlugin:extendedop /bin/libback-rdbm.dll initUniqueAttr
```

Diagnosztika

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

ldapmodrdn

Az LDAP modify-entry RDN eszköz

Összegzés

```
ldapmodrdn [-C karakterkészlet] [-d nyomkövetési_szint][ -D binddn]
[-f fájl] [-G tartomány] [-h ldaphoszt] [-i fájl] [-k] [-K kulcsfájl]
[-m mechanizmus] [-M] [-n] [-N igazolásnév] [-O max_szakas]
[-p ldapport] [-P kulcsfájl_jelszó] [-r] [-R] [-U felhasználónév] [-v] [-V változat]
[-w jelszó] [-y proxydn] [-Y] [-Z] [dn új_rdn | [-i file]]
```

Leírás

Az **ldapmodrdn** egy parancssori illesztő az **ldap_modrdn** alkalmazási programcsatlóhoz (API).

Az **ldapmodrdn** megnyit egy kapcsolatot egy LDAP szerver felé, majd kapcsolódik hozzá. A bejegyzések információit a program a szabványos bemenetről olvassa, az -f kapcsoló megadása esetén egy fájlból, vagy a parancssori dn és rdn párból.

A relatív megkülönböztetett nevekkkel (RDN) és a megkülönböztetett nevekkkel (DN) kapcsolatos további információ: "Megkülönböztetett nevek (DN)" oldalszám: 11.

Az **ldapmodrdn** parancs szintaxisának megjelenítéséhez írja be az alábbi parancsot:

```
ldapmodrdn -?
```

Beállítások

-c Folyamatos működési üzemmód. A hibákat jelenti, de az **ldapmodrdn** tovább végzi a módosításokat. Egyébként az alapértelmezés a hiba jelzése után kilépés.

-C karakterkészlet

Azt jelzi, hogy az **ldapmodr**dn segédprogram bemeneteként megadott karaktersorozatok ábrázolása a "karakterkészlet" paraméterben megadott helyi karakterkészlet szerint történik. Akkor használja a **-C karakterkészlet** paramétert, ha a bemeneti karakterlánc kódlapja eltér a job kódlapjától. A támogatott "karakterkészlet" értékeket az `ldap_set_iconv_local_charset()` dokumentációjában találja meg. A "karakterkészlet" paraméter támogatott értékei ugyanazok, mint a `charset` címke támogatott értékei, amelyek nem kötelező módon a Version 1 LDIF fájlokban vannak megadva.

-d nyomkövetési_szint

Az LDAP nyomkövetési szintet a "nyomkövetési_szint" paraméter értékére állítja be.

-D binddn

A **binddn** paraméter által megadott kapcsolódási DN-t használja az LDAP címtárhoz kapcsolódáshoz. A **binddn** egy karakterláncal képviselt DN kell, hogy legyen. Az **-m DIGEST-MD5** kapcsolóval használva a hitelesítési azonosító megadására szolgál. Lehet egy DN, vagy egy "u:" vagy "dn:" jellel kezdődő `authzId` karaktersorozat.

-f fájl

A bejegyzés módosítási információinak beolvasása a megadott LDIF fájlból történik, nem a szabványos bemenetről vagy a parancssorból (a `dn` és az új `rdn` megadásával). A szabványos bemenet fájlból is biztosítható (< file).

-G tartomány

Megadja a tartományt. Ez a paraméter nem kötelező. Az **-m DIGEST-MD5** kapcsolóval használva az érték a kapcsolódás során átadásra kerül a szervernek.

-hldaphoszt

Egy alternatív hoszt megadása, amelyiken az LDAP szerver fut.

-i fájl

A bejegyzés módosítási információinak beolvasása a megadott fájlból történik, nem a szabványos bemenetről vagy a parancssorból (a `dn` és az új `rdn` megadásával). A szabványos bemenet fájlal is helyettesíthető ("< fájl").

-k

A szerver adminisztrációs vezérlés használatát írja elő.

-K kulcsfájl

Az SSL kulcsadatbázis-fájl nevét adja meg. Ha a kulcsadatbázis-fájl nem az aktuális könyvtárban található, megadja az adatbázisfájl teljes nevét.

Ha a segédprogram nem találja meg a kulcsadatbázist, akkor az alapértelmezés szerinti megbízható jogosultság gyökerek hardver-kódolt készletét fogja használni. A kulcsadatbázis-fájl általában egy vagy több, a kliens által megbízhatónak tartott CA-któl származó igazolást tartalmaz. Ezeket az X.509 típusú igazolásokat megbízható gyökereknek is hívják.

Ez a paraméter engedélyezi a **-Z** kapcsolót. Az `i5/OS` alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

-m mechanizmus

A **mechanizmus** a szerverhez kapcsolódáshoz használt SASL eljárás. A rendszer az `ldap_sasl_bind_s()` API-t használja. Az **-m** paraméter figyelmen kívül marad, ha a **-V 2** kapcsoló be van állítva. Ha a **-m** kapcsoló nincs megadva, akkor egyszerű hitelesítés történik. Az érvényes mechanizmusok:

- CRAM-MD5 - védi a szervernek elküldött jelszót.
- EXTERNAL - az SSL igazolást használja. Szükséges a **-Z** kapcsoló megadása is.
- GSSAPI - a felhasználó Kerberos hitelesítési adatait használja
- DIGEST-MD5 - azt igényli, hogy a kliens küldjön egy felhasználónév-értéket a szerverre. Szükséges a **-U** kapcsoló megadása is. A hitelesítési azonosító megadására a **-D** paraméter (általában a kapcsolati DN) használható. Lehet egy DN, vagy egy `u:` vagy `dn:` jellel kezdődő `authzId` karaktersorozat.
- OS400_PRFTKN - hitelesíti magát a helyi LDAP szerverhez az aktuális `i5/OS` felhasználóként a felhasználó megkülönböztetett nevét használva a rendszer leképezett háttérben. Nem kell megadni a **-D** (kapcsolati DN) és a **-w** (jelszó) paramétereiket.

- M Az utalási objektumok normál bejegyzésként kezelése.
- n Megmutatja, mi történne, de valójában nem változtatja meg a bejegyzéseket. Hibakereséskor hasznos a -v paraméterrel együtt.
- N *igazolásnév*
A kulcsadatbázis-fájlban található kliensigazoláshoz tartozó azonosítót adja meg. Amennyiben az LDAP szerver csak szerver hitelesítésre lett beállítva, a kliensigazolásra nincs szükség. Ha az LDAP szerver kliens- és szerverhitelesítésre lett beállítva, a kliensigazolásra szükség van. Az *igazolásnév* nem szükséges, ha egy alapértelmezett igazolás/privát kulcspár alapértelmezettként ki lett jelölve. Hasonlóképpen akkor sem szükséges az *igazolásnév*, ha van egy egyedi igazolás/privát kulcspár a megjelölt adatbázisfájlban. Ez a paraméter figyelmen kívül marad, ha sem a -Z, sem a -K kapcsoló nincs megadva. Az i5/OS alatt futó Directory Server esetében, ha a -Z kapcsolót használja, de a -K vagy -N kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.
- O *szakaszszám*
A *szakaszszám* beállítja azoknak a szakaszoknak a maximális számát, amelyeket a klienskönyvtár az utalások kereséskor számba vesz. Az alapértelmezett szakaszszám érték 10.
- 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 paraméter szerepel, az alapértelmezés szerinti 636-os LDAP SSL port kerül beállításra.
- P *kulcsfájl_jelszó*
A kulcsadatbázis jelszavát adja meg. A jelszó a kulcsadatbázis-fájl rejtjelezett tartalmának (amely egy vagy több privát kulcsot is tartalmazhat) eléréséhez szükséges. Ha rendelve lett jelszótároló fájl a kulcsadatbázis-fájlhoz, akkor a jelszó a jelszótároló fájlból kérdezhető le, ezért a -P paraméterre nincs szükség. Ez a paraméter figyelmen kívül marad, ha sem a -Z, sem a -K nincs megadva.
- r Régi RDN értékek törlése a bejegyzésből. Alapértelmezés: a régi értékek megtartása.
- R Azt határozza meg, hogy az utalásokat nem kell automatikusan követni.
- U *felhasználónév*
Adja meg a felhasználónevet. Az -m DIGEST-MD5 használata esetén szükséges, minden más mechanizmussal figyelmen kívül marad.
- v Bővebb diagnosztikai információt nyújt, amelyet a szabványos kimenetre ír.
- V *változat*
Megadja, hogy az **ldapmodrtn** parancs melyik LDAP változatot használja a szerverhez kapcsolódáskor. Alapértelmezés szerint LDAP V3 összeköttetést létesít. Ahhoz, hogy kifejezetten az LDAP V3 legyen kiválasztva, -V 3 kapcsolót kell megadni. Adja meg a -V 2 kapcsolót, ha LDAP V2 alkalmazásként kívánja futtatni. Az **ldapmodrtn** segédprogramhoz hasonló alkalmazások úgy választják az LDAP V3-at előnyben részesített protokollként, hogy az ldap_init funkciót használják az ldap_open helyett.
- w *jelszó | ?*
A *jelszó* használata hitelesítési jelszóként. A ? karakter megadása esetén a program bekéri a jelszót.
- y **proxydn**
Megadja a proxy azonosítót a proxy hitelesítési művelethez.
- Y Biztonságos LDAP kapcsolatot (TLS) használ.
- Z Védett SSL kapcsolat használata az LDAP szerverrel folyó kommunikáció során. Az i5/OS alatt futó Directory Server esetében, ha a -Z kapcsolót használja, de a -K vagy -N kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

dn újrdn

További információkért tekintse meg a következő részt (“dn újrdn beviteli formátuma”).

dn újrdn beviteli formátuma

Ha a *dn* és *újr*dn parancssori argumentumok meg vannak adva, akkor az *újr*dn paraméter felváltja a bejegyzésnek a *dn* paraméter által meghatározott DN-jét. Másikülönben a fájl tartalma (vagy a szabványos bemenet, ha nem adja meg a **-i** kapcsolót) egy vagy több bejegyzésből áll:

Megkülönböztetett név (Distinguished Name, DN)

Relatív megkülönböztetett név (Relative Distinguished Name, RDN)

A DN és RDN párokat egy vagy több üres sor választhatja el egymástól.

Példák

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

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

akkor a következő parancs:

```
ldapmodrdrn -r -i /tmp/entrymods
```

a *Modify Me* bejegyzés RDN-jét *Modify Me*-ről *The New Me*-re változtatja, a *Modify Me* régi DN pedig törlésre kerül.

Megjegyzés

Ha nem ad meg bejegyzés információkat fájlban az **-i** kapcsoló használatával (vagy a *dn* és *rdn* parancssori paraméterpárral), akkor az **ldapmodrdrn** parancs a szabványos bemeneten várja a bejegyzéseket.

Diagnosztika

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

ldapsearch

Az LDAP keresési eszköz és példaprogram

Összegzés

```
ldapsearch [-a deref] [-A] [-b keresési_alap] [-B] [-C karakterkészlet] [-d nyomkövetési_szint]
[-D kapcsolati_dn] [-e] [-f fájl] [-F sep] [-G tartomány] [-h ldaphoszt] [-i fájl] [-K kulcsfájl]
[-l időkorlát] [-L] [-m mechanizmus] [-M] [-n] [-N tanúsítványnév]
[-o attribútumtípus] [-O max szakasz] [-p ldapport] [-P kulcsfájl_jelszó] [-q oldalméret]
[-R] [-s hatókör] [-t] [-T másodperc] [-U felhasználónév] [-v] [-V változat]
[-w jelszó ?] [-z méretkorlát] [-y proxydn] [-Y] [-Z]
szűrő [-9 p] [-9 s] [attrs...]
```

Leírás

Az **ldapsearch** egy parancssori illesztő az *ldap_search* alkalmazási programcsatlóhoz (API).

Az **ldapsearch** megnyit egy kapcsolatot egy LDAP szerver felé, majd kapcsolódik hozzá. A szűrőnek meg kell felelnie az LDAP szűrők karakteres reprezentációjára vonatkozó előírásoknak (a szűrőkkel kapcsolatos további információkért tekintse meg a Directory Server API-k témakör *ldap_search* szakaszát).

Ha az **ldapsearch** egy vagy több bejegyzést talál, akkor az *attrs* paraméter által megadott attribútumok lekérésre kerülnek, majd a bejegyzések és értékeik a szabványos kimenetre íródnak. Ha nincs megadva az *attrs* paraméter, akkor minden attribútum visszaadásra kerül.

Az **ldapsearch** parancs szintaxisának megjelenítéséhez írja be az alábbi parancsot: `ldapsearch -?`.

Beállítások

-a deref

Az álnév-hivatkozások feloldási módját határozza meg. A deref paraméter lehetséges értékei: never (soha), always (mindig), search (keres) vagy find (találat). Rendre azt adja meg, hogy milyen módon történik az álnevek használata, ami lehet soha, mindig, kereséskor vagy a keresés bázisobjektumának megtalálásakor. Az alapértelmezés szerint álnevek nincsenek használva (never).

-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 keresési_alap

Az alapértelmezés helyett a megadott alap DN szolgál a keresés kezdőpontjául. Ha nem adja meg a **-b** kapcsolót, akkor a segédprogram az LDAP_BASEDN környezeti változóban keresi a keresési_alap definícióját. Ha egyik sincs beállítva, akkor az alapértelmezett alap az "".

-B Nem nyomja el a nem ASCII értékek megjelenítést. Ez hasznos lehet olyan értékek esetében, melyek alternatív karakterkészletekben jelennek meg, amilyen pl. az ISO-8859.1 karakterkészlet. Az **-L** kapcsoló ezt magában foglalja.

-C karakterkészlet

Azt jelzi, hogy az ldapsearch segédprogram bemeneteként megadott karaktersorozatok ábrázolása a "karakterkészlet" paraméterben megadott helyi karakterkészlet szerint történik. A bemeneti karakterlánc magában foglalja a szűrőt, a kapcsolódási DN-t és az alap DN-t. Ugyanúgy, mint az adatok megjelenítésekor, az **ldapsearch** segédprogram speciális karakterekre konvertálja az LDAP szervertől kapott adatokat. Akkor használja a **-C karakterkészlet** paramétert, ha a bemeneti karakterlánc kódlapja eltér a job kódlapjától. Az ldap_set_iconv_local_charset() dokumentációjában megtalálhatja a támogatott "karakterkészlet" értékeket. Ha a **-C** és az **-L** kapcsoló 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 őrződnek 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. A "karakterkészlet" paraméter támogatott értékei ugyanazok, mint a charset címke támogatott értékei, amelyek nem kötelező módon a Version 1 LDIF fájlokban vannak megadva.

-d nyomkövetési_szint

Az LDAP nyomkövetési szintet a "nyomkövetési_szint" paraméter értékére állítja be.

-D binddn

A binddn paraméter által megadott kapcsolódási DN-t használja az LDAP címtárhoz kapcsolódáshoz. **kapcsolati_dn** egy karakterlánc jelölt DN-nek kell lennie (lásd: LDAP megkülönböztetett nevek). Az -m DIGEST-MD5 kapcsolóval használva a hitelesítési azonosító megadására szolgál. Lehet egy DN, vagy egy "u:" vagy "dn:" jellel kezdődő authzId karaktersorozat.

-e Kiírja az LDAP könyvtár verziószámát, majd kilép.

-F sep A sep mező elválasztóként szerepel az attribútumnevek és -értékek között. Az alapértelmezett elválasztó az '=', kivéve, ha megadja a **-L** kapcsolót, amely esetben ez a beállítás figyelmen kívül marad.

-G tartomány

Megadja a tartományt. Ez a paraméter nem kötelező. Az -m DIGEST-MD5 kapcsolóval használva az érték a kapcsolódás során átadásra kerül a szervernek.

-h ldaphoszt

Egy alternatív hoszt megadása, amelyiken az LDAP szerver fut.

-i fájl Egy fájlból olvas be sorokat, minden sorra végrehajt egy LDAP keresést. Ebben az esetben a parancssorban megadott szűrőt mintának tekinti a program, amelyben a % jelek első előfordulását lecseréli a fájl egy sorára. Ha a fájl egyetlen "-" karakterből áll, akkor a sorokat a szabványos bemenetről olvassa a program.

-K kulcsfájl

Az SSL kulcsadatbázis-fájl nevét adja meg. Ha a kulcsadatbázis-fájl nem az aktuális könyvtárban található, megadja az adatbázisfájl teljes nevét.

Ha a segédprogram nem találja meg a kulcsadatbázist, akkor az alapértelmezés szerinti megbízható jogosultság gyökerek hardver-kódolt készletét fogja használni. A kulcsadatbázis-fájl általában egy vagy több, a kliens által megbízhatónak tartott CA-któl származó igazolást tartalmaz. Ezeket az X.509 típusú igazolásokat megbízható gyökereknek is hívják.

Ez a paraméter engedélyezi a **-Z** kapcsolót. Az i5/OS alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

-l időkorlát

Maximum "időkorlát" másodpercet vár a keresés befejezéséig.

-L A keresési eredményeket LDIF formátumban jeleníti meg. Ez a kapcsoló bekapcsolja a **-B** kapcsolót, és figyelmen kívül hagyja az **-F** kapcsolót.

-m mechanizmus

A **mechanizmus** a szerverhez kapcsolódáshoz használt SASL eljárás. A rendszer az `ldap_sasl_bind_s()` API-t használja. Az **-m** paraméter figyelmen kívül marad, ha a **-V 2** kapcsoló be van állítva. Ha a **-m** kapcsoló nincs megadva, akkor egyszerű hitelesítés történik. Az érvényes mechanizmusok:

- CRAM-MD5 - védi a szervernek elküldött jelszót.
- EXTERNAL - az SSL igazolást használja. Szükséges a **-Z** kapcsoló megadása is.
- GSSAPI - a felhasználó Kerberos hitelesítési adatait használja
- DIGEST-MD5 - azt igényli, hogy a kliens küldjön egy felhasználónév-értéket a szerverre. Szükséges a **-U** kapcsoló megadása is. A hitelesítési azonosító megadására a **-D** paraméter (általában a kapcsolati DN) használható. Lehet egy DN, vagy egy `u:` vagy `dn:` jellel kezdődő `authzId` karaktersorozat.
- OS400_PRFTKN - hitelesíti magát a helyi LDAP szerverhez az aktuális i5/OS felhasználóként a felhasználó megkülönböztetett nevét használva a rendszer leképezett háttérben. Nem kell megadni a **-D** (kapcsolati DN) és a **-w** (jelszó) paramétereket.

-M Az utalási objektumok normál bejegyzésként kezelése.

-n Megmutatja, mi történne, de valójában nem változtatja meg a bejegyzéseket. Hibakereséskor hasznos a **-v** paraméterrel együtt.

-N igazolásnév

A kulcsadatbázis-fájlban található kliensigazoláshoz tartozó azonosítót adja meg.

Megjegyzés: Amennyiben az LDAP szerver csak szerver hitelesítésre lett beállítva, a kliensigazolásra nincs szükség. Ha az LDAP szerver kliens- és szerverhitelesítésre lett beállítva, a kliensigazolásra szükség van. Az *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 adatbázisfájlban. Ez a paraméter figyelmen kívül marad, ha sem a **-Z**, sem a **-K** kapcsoló nincs megadva.

Az i5/OS alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

-o attr_típus

Ha egy attribútumot rendezési feltételként kíván használni a keresési eredmények rendezéséhez, akkor használja a **-o** paramétert. A rendezés finomítása érdekében több **-o** paramétert is megadhat. Az alábbi példában a keresési eredmények először vezetéknev (sn), majd keresztnév (givenname) szerint kerülnek rendezésre, úgy, hogy a keresztnév szerinti rendezés fordított (csökkenő) sorrendben történik, a megadott mínusz (-) jel miatt:

```
-o sn -o -givenname
```

A rendezési paraméter szintaxisa tehát:

```
[-]<attribútumnév>[:<megfeleltetési szabály OID>]
```

ahol

- attribútumnév a rendezés alapjául használni kívánt attribútum neve.
- megfeleltetési szabály OID pedig a rendezéshez esetleg használni kívánt megfeleltetési szabály objektumazonosítója. A Directory Server nem támogatja a megfeleltetési szabály OID paraméter használatát, de előfordulhat, hogy más LDAP szerverek igen.
- A mínusz (-) jel azt jelzi, hogy az eredményeket fordított sorrendben kell rendezni.
- A fontosság mértéke mindig kritikus.

Az alapértelmezett ldapsearch művelet nem rendezi a visszaadott eredményeket.

-O max_szakasz

A max_szakasz beállítja azoknak a szakaszoknak a maximális számát, amelyeket a klienskönyvtár az utalások keresésekor számba vesz. Az alapértelmezett szakaszszám érték 10.

-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 paraméter szerepel, az alapértelmezés szerinti 636-os LDAP SSL port kerül beállításra.

-P kulcsfájl_jelszó

A kulcsadatbázis jelszavát adja meg. A jelszó a kulcsadatbázis-fájl rejtjelezett tartalmának (amely egy vagy több privát kulcsot is tartalmazhat) eléréséhez szükséges. Ha rendelve lett jelszótároló fájl a kulcsadatbázis-fájlhoz, akkor a jelszó a jelszótároló fájlból kérdezhető le, ezért a -P paraméterre nincs szükség. Ez a paraméter figyelmen kívül marad, ha sem a -Z, sem a -K nincs megadva.

-q oldalméret

A keresési eredmények oldalakra bontása esetén két paramétert lehet használni: a -q (lekérdezési oldal mérete) és a -T (idő másodpercben két keresés között). A következő példában a keresés egyszerre egy oldalt (25 bejegyzést) ad vissza, 15 másodpercenként, addig, amíg az összes eredmény visszaadásra nem került. Az ldapsearch kliens a keresési művelet ideje alatt intézi a kapcsolatok fenntartását az egyes eredményoldalak megjelenítése utáni folytatás érdekében.

Ezek a paraméterek akkor lehetnek hasznosak, ha a kliens erőforrásai korlátozottak, vagy ha egy alacsony sávszélességű kapcsolaton keresztül csatlakozik. Általánosságban szabályozható a keresési kérésből visszakapott adatok érkezési sebessége. Ahelyett, hogy az összes eredmény egyszerre érkezne meg, darabonként kérhetők le. Ezenfelül szabályozható a késleltetés két oldalkérés között, vagyis a kliensnek jut ideje feldolgozni az eredményeket.

-q 25 -T 15

A -v (részletes) paraméter megadása esetén az ldapsearch az egyes bejegyzésoldalak végén kiírja, hány bejegyzést adott eddig vissza a szerverről. Az alábbihoz hasonló üzenet jelenik meg: **Összesen 30 bejegyzés került visszaadásra.**

Több -q paraméter is megadható, így szabályozhatók a különböző oldalméretek egyetlen keresési műveleten belül is. A következő példában az első oldal 15 bejegyzést tartalmaz, a második oldal 20-at, a harmadik pedig lezárja az oldalakra bontott eredményeket/keresési műveletet:

-q 15 -q 20 -q 0

A következő példában az első oldal 15 bejegyzést tartalmaz, az összes többi 20-at, a legutoljára megadott -q értéket használva a keresési művelet befejezéséig:

-q 15 -q 20

Az ldapsearch segédprogram alapértelmezett működése, hogy minden bejegyzést visszaad egy kérdésben. Az alapértelmezett ldapsearch művelet nem bontja oldalakra a műveletet.

-R Azt határozza meg, hogy az utalásokat nem kell automatikusan követni.

-s hatókör

A keresés érvényességi tartományát határozza meg. A hatókör paraméter lehetséges értékei base, one vagy sub, amelyek rendre bázisobjektum szintű, egyszintű vagy alárendelt fa szintű keresést határoz meg. Az alapértelmezés szerinti érték a sub.

-t A beolvasott értékeket ideiglenes fájlokba írja. Ez hasznos lehet nem ASCII értékek esetében, mint amilyenek a jpegPhoto vagy audio.

-T másodpercek

Két keresés között eltelt idő (másodpercben). A **-T** kapcsoló csak akkor használható, ha a **-q** kapcsoló is meg van adva.

-U felhasználónév

Adja meg a felhasználónevet. Az **-m DIGEST-MD5** használata esetén szükséges, minden más mechanizmussal figyelmen kívül marad.

-v Bővebb diagnosztikai információt nyújt, amelyet a szabványos kimenetre ír.

-V Megadja, hogy az ldapmodify parancs melyik LDAP változatot használja a szerverhez kapcsolódáskor. Alapértelmezés szerint LDAP V3 összeköttetést létesít. Ahhoz, hogy kifejezetten az LDAP V3 legyen kiválasztva, **-V 3** kapcsolót kell megadni. Adjon meg **-V 2** kapcsolót, ha LDAP V2 alkalmazásként kívánja futtatni. Az ldapmodify segédprogramhoz hasonló alkalmazások úgy választják az LDAP V3-at előnyben részesített protokollként, hogy az ldap_init funkciót használják az ldap_open helyett.

-w jelszó | ?

A **jelszó** használata hitelesítési jelszóként. A ? karakter megadása esetén a program bekéri a jelszót. .

-y proxydn

Megadja a proxy azonosítót a proxy hitelesítési művelethez.

-Y Biztonságos LDAP kapcsolatot (TLS) használ.

-z méretkorlát


A keresést korlátozza maximum méretkorlát bejegyzésre. Ezzel megadható a keresési művelet által visszaadott bejegyzések maximális száma.

-Z Védett SSL kapcsolat használata az LDAP szerverrel folyó kommunikáció során. Az i5/OS alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

szűrő A keresésben alkalmazandó szűrő karaktersorozattal képviselt formában. Az egyszerű szűrők attribútumtípus=attribútumérték formában adhatók meg. Az összetettebb szűrők előtag jelölésmóddal, az alábbi Backus Naur Form (BNF) definícióknak megfelelő formában adhatók meg:

```
<filter> ::= '(' <filtercomp> ')'  
<filtercomp> ::= <and> | <or> | <not> | <simple>  
<and> ::= '&' <filterlist>  
<or> ::= '|' <filterlist>  
<not> ::= '!' <filter>  
<filterlist> ::= <filter> | <filter> <filterlist>  
<simple> ::= <attributetype> <filtertype>  
<attributevalue>  
<filtertype> ::= '=' | '~=' | '<=' | '>='
```


A '~=' szerkezettel közelítő egyezés adható meg. Az <attributetype> (attribútumtípus) és <attributevalue >

(attribútumérték) ábrázolása az "RFC 2252, LDAP V3 attribútum szintaxis meghatározások"  dokumentumban található. Ezenfelül, ha a szűrőtípus '=', akkor az <attributevalue> lehet egyetlen * karakter az attribútum meglétének ellenőrzéséhez, illetve állhat szövegből és csillag (*) karakterekből vegyesen részkarakterlánc-egyezés vizsgálatához.

A "mail=" például megtalálja az összes olyan bejegyzést, amely rendelkezik mail attribútummal. A "mail=*@student.of.life.edu" azokat a bejegyzéseket találja meg, amelyeknek nemcsak, hogy van mail

attribútumuk, de annak értéke a megadott karaktersorozatra végződik. Ha zárójeleket akar használni egy szűrőben, akkor egy balra döntött törtvonal (\) karaktert kell eléjük írnia.

Megjegyzés: A "cn=Bob*" szűrőfeltétel hatására, vagyis ahol van egy szóköz a Bob név és a csillag (*) karakter között, az IBM Directory Server megtalálja "Bob Carter"-t, de "Bobby Carter"-t már nem. A "Bob" és a helyettesítő karakter (*) közötti szóköz befolyásolja a szűrőt használó keresést.

A használható szűrők részletesebb leírásával kapcsolatban tekintse meg az "RFC 2254, LDAP keresési szűrők karaktersorozat alakban megjelenítése"  dokumentumot.

Kimeneti formátum

Ha egynél több bejegyzést talál a rendszer, akkor mindegyik megtalált bejegyzés az alábbi formában íródik ki a szabványos kimenetre:

Megkülönböztetett név (Distinguished Name, DN)

attribútumnév=érték

attribútumnév=érték

attribútumnév=érték

...

Az egyes bejegyzéseket egy üres sor választja el egymástól. Ha a **-F** kapcsolót használja elválasztó karakter megadására, akkor a program azt a karaktert használja az '=' helyett. Ha a **-t** kapcsolót használja, az ideiglenes fájl neve lecseréli a tényleges értéket. Ha megadja az **-A** kapcsolót is, akkor csak az "attribútumnév" rész íródik ki.

Példák

A következő parancs:

```
ldapsearch "cn=john doe" cn telephoneNumber
```

keresést hajt végre egy részfán (az alapértelmezett keresési kiindulópontot használva) az olyan bejegyzések után, amelyek általános neve (commonName) "john doe". A commonName és telephoneNumber attribútumok értékét lekéri a program és kiírja a szabványos kimenetre. A kimenet az alábbihoz hasonló lehet, ha a program két bejegyzést talál:

```
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
```

A következő parancs:

```
ldapsearch -t "uid=jed" jpegPhoto audio
```

keresést hajt végre egy részfán (az alapértelmezett keresési kiindulópontot használva) az olyan bejegyzések után, amelyek felhasználói azonosítója (user id) "jed". A jpegPhoto és audio attribútumok értékét lekéri a program és ideiglenes fájlba írja őket. Ha a keresés egy bejegyzést talál egyetlen értékkel mindkét lekérdezett attribútumhoz, akkor a kimenet az alábbihoz 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
```

A következő parancs:

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

egyszintű keresést hajt végre az olyan szervezetek után, amelyek szervezeti neve (organizationName) a "university" szóval kezdődik. A keresési eredményeket LDIF formátumban jeleníti meg a program (tekintse meg az LDAP Adatcsere formátum (LDIF) részt). A program lekéri az organizationName és description attribútumértékeket és kinyomtatja őket a szabványos kimenetre. Az eredmény az alábbihoz lesz hasonló:

```
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: UF1
description: Shaper of young minds
...
```

A következő parancs:

```
ldapsearch -b "c=US" -o ibm-slapdDN "objectclass=person" ibm-slapdDN
```

egy részfa szintű keresést hajt végre a c=US szinten és kikeres minden személyt. A speciális attribútum (ibm-slapdDN) a rendezett keresésekben a keresési eredményeket a megkülönböztetett név (DN) karakterlánc formátumú ábrázolása szerint szedi sorba. A kimenet az alábbihoz hasonló lehet:

```
cn=Al Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US
cn=Al Garcia,ou=Home Entertainment,ou=Austin,o=IBM,c=US
cn=Amy Nguyen,ou=In Flight Systems,ou=Austin,o=IBM,c=US
cn=Arthur Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US
cn=Becky Garcia,ou=In Flight Systems,ou=Austin,o=IBM,c=US
cn=Ben Catu,ou=In Flight Systems,ou=Austin,o=IBM,c=US
cn=Ben Garcia Jr,ou=Home Entertainment,ou=Austin,o=IBM,c=US
cn=Bill Keller Jr.,ou=In Flight Systems,ou=Austin,o=IBM,c=US
cn=Bob Campbell,ou=In Flight Systems,ou=Austin,o=IBM,c=US
```

A következő parancs:

```
ldapsearch -h hosztnév -o sn -b "o=ibm,c=us" "title=engineer"
```

visszaadja az összes olyan bejegyzését egy IBM alkalmazotti címtárnak, amelynek beosztása (title) "engineer", és az eredményeket vezetéknev szerint rendezi sorba.

A következő parancs:

```
ldapsearch -h hosztnév -o -sn -o cn -b "o=ibm,c=us" "title=engineer"
```

visszaadja az összes olyan bejegyzését egy IBM alkalmazotti címtárnak, amelynek beosztása (title) "engineer", és az eredményeket vezetéknev szerint rendezi sorba (csökkenő sorrendbe), majd általános név szerint (növekvő sorrendbe).

A következő parancs:

```
ldapsearch -h hosztnév -q 5 -T 3 -b o=ibm,c=us "title=engineer"
```

öt olyan bejegyzést ad vissza egy IBM alkalmazotti címtárból, amelynek beosztása (title) "engineer".

A következő példa olyan keresést illusztrál, amelyben utalási objektum is szerepel. Amint a "LDAP címtárutalások" oldalszám: 46 alatt tárgyaltuk, a Directory Server LDAP címtárak utalási objektumokat is tartalmazhatnak, feltéve, ha csak a következőket tartalmazzák:

- Egy megkülönböztetett nevet (dn).

- Egy objektumosztályt (**objectClass**).
- Egy utalási (**ref**) attribútumot.

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 egy kliens kérést küld 'System_A' felé, akkor a System_A rendszeren futó LDAP szerver 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 (kivéve, ha megadta a **-R** kapcsolót, jelezvén, hogy ne kövesse a program az utalásokat).

Amikor a kliens egy utalási választ kap a szervertől, újra kiadja a kérést, ezúttal azon szerver felé, amelyre a visszaküldött URL utal. Az új kérés hatóköre ugyanaz, mint az eredeti kérésé. A keresés eredménye függ a keresés hatásköréként megadott értéktől (**-b**).

Ha **-s base** paramétert ad meg, mint itt:

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

akkor a keresés az összes olyan bejegyzésre vonatkozó összes attribútumot beolvassa, ahol 'sn=Jensen', és amelyek az 'ou=Rochester, o=Big Company, c=US' helyen található a System_A-n és System_B-n egyaránt.

Ha **-s sub** paramétert ad meg, mint itt:

```
ldapsearch -s sub "cn=John"
```

a szerver minden utótagot megtalál és minden "cn=John" karaktersorozatot tartalmazó bejegyzést visszaad. Ezt null alapon végzett részfa-keresésként szokás ismerni. A teljes címtár keresésre kerül egy keresési művelettel ahelyett, hogy több keresés futna keresési alapként az egyes utótagokkal. Ez a fajta keresési művelet tovább tart és több rendszererőforrást fogyaszt, mivel a teljes címtárat (minden utótagot) végigkeresi.

Megjegyzés: Egy null alapon végzett részfa. keresés nem ad vissza séma- és változásnapló-információkat, sem semmit a rendszer által leképezett háttérből.

Ha **-s sub** paramétert ad meg, mint itt:

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

akkor a keresés az 'ou=Rochester, o=Big Company, c=US' helyen és alatta található összes olyan bejegyzésre vonatkozó összes attribútumot beolvassa, amelyre igaz az 'sn=Jensen', a System_A-n és System_B-n egyaránt.

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
```

Erre a kliens a következő kérést nyújtja be:

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

Ez sem ad semmilyen eredményt, mivel az alábbi bejegyzés:

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
```

ezen a címen található:

```
ou=Rochester, o=Big Company, c=US
```

Az **-s one** kapcsolóval kiadott keresés a bejegyzéseket közvetlenül egy szinttel az

```
ou=Rochester,
o=Big Company, c=US
```

alatt keresi.

Diagnosztika

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

ldapchangepwd

Az LDAP jelszómódosító eszköz.

Összegzés

```
ldapchangepwd -D binddn -w jelszó | ? -n új_jelszó | ?
[-C karakterkészlet] [-d nyomkövetési_szint] [-G tartomány] [-h ldaphoszt]
[-K kulcsfájl] [-m mechanizmus] [-M] [-N igazolásnév]
[-O max_szakasz] [-p ldapport] [-P kulcsfájl_jelszó] [-R]
[-U felhasználónév] [-v] [-V változat] [-y proxydn] [-Y] [-Z] [-?]
```

Leírás

Jelszómódosítási kérelmet küld az LDAP szervernek. Lehetővé teszi egy címtárbejegyzés jelszavának megváltoztatását.

Beállítások

-C karakterkészlet

Azt jelzi, hogy az **ldapdelete** segédprogram bemeneteként megadott DN-ek ábrázolása a "karakterkészlet" paraméterben megadott helyi karakterkészlet szerint történik. Akkor használja a **-C karakterkészlet** paramétert, ha a bemeneti karakterlánc kódlapja eltér a job kódlapjától. Az `ldap_set_iconv_local_charset()` dokumentációjában megtalálhatja a támogatott "karakterkészlet" értékeket.

-d nyomkövetési_szint

Az LDAP nyomkövetési szintet a "nyomkövetési_szint" paraméter értékére állítja be.

-D binddn

A **binddn** paraméter által megadott kapcsolódási DN-t használja az LDAP címtárhoz kapcsolódáshoz. A

binddn egy karakterlánccal képviselt DN. Az **-m** DIGEST-MD5 kapcsolóval használva a hitelesítési azonosító megadására szolgál. Lehet egy DN, vagy egy "u:" vagy "dn:" jellel kezdődő authzId karaktersorozat.

-G *tartomány*

Megadja a tartományt. Ez a paraméter nem kötelező. Az **-m** DIGEST-MD5 kapcsolóval használva az érték a kapcsolódás során átadásra kerül a szervernek.

-h*ldaphoszt*

Egy alternatív hoszt megadása, amelyiken az LDAP szerver fut.

-K *kulcsfájl*

Az SSL kulcsadatbázis-fájl nevét adja meg. Ha a kulcsadatbázis-fájl nem az aktuális könyvtárban található, megadja az adatbázisfájl teljes nevét.

Ha a segédprogram nem találja meg a kulcsadatbázist, akkor az alapértelmezés szerinti megbízható jogosultság gyökerek hardver-kódolt készletét fogja használni. A kulcsadatbázis-fájl általában egy vagy több, a kliens által megbízhatónak tartott CA-któl származó igazolást tartalmaz. Ezeket az X.509 típusú igazolásokat megbízható gyökereknek is hívják.

Ez a paraméter engedélyezi a **-Z** kapcsolót. Az i5/OS alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

-m *mechanizmus*

A **mechanizmus** a szerverhez kapcsolódáshoz használt SASL eljárás. A rendszer az `ldap_sasl_bind_s()` API-t használja. Az **-m** paraméter figyelmen kívül marad, ha a **-V 2** kapcsoló be van állítva. Ha a **-m** kapcsoló nincs megadva, akkor egyszerű hitelesítés történik. Az érvényes mechanizmusok:

- CRAM-MD5 - védi a szervernek elküldött jelszót.
- EXTERNAL - az SSL igazolást használja. Szükséges a **-Z** kapcsoló megadása is.
- GSSAPI - a felhasználó Kerberos hitelesítési adatait használja
- DIGEST-MD5 - azt igényli, hogy a kliens küldjön egy felhasználónév-értéket a szerverre. Szükséges a **-U** kapcsoló megadása is. A hitelesítési azonosító megadására a **-D** paraméter (általában a kapcsolati DN) használható. Lehet egy DN, vagy egy u: vagy dn: jellel kezdődő authzId karaktersorozat.

-M Az utalási objektumok normál bejegyzésként kezelése.

-n *új_jelszó* | ?

Az új jelszót adja meg. A ? karakter megadása esetén a program bekéri a jelszót.

-N *igazolásnév*

A kulcsadatbázis-fájlban található kliensigazoláshoz tartozó azonosítót adja meg. Amennyiben az LDAP szerver csak szerver hitelesítésre lett beállítva, a kliensigazolásra nincs szükség. Ha az LDAP szerver kliens- és szerverhitelesítésre lett beállítva, a kliensigazolásra szükség van. Az **igazolásnév** nem szükséges, ha egy alapértelmezett igazolás/privát kulcspár alapértelmezettként ki lett jelölve. Hasonlóképpen akkor sem szükséges az **igazolásnév**, ha van egy egyedi igazolás/privát kulcspár a megjelölt adatbázisfájlban. Ez a paraméter figyelmen kívül marad, ha sem a **-Z**, sem a **-K** kapcsoló nincs megadva. Az i5/OS alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

-O *max_szakas*

A **max_szakas** beállítja azoknak a szakaszoknak a maximális számát, amelyeket a klienskönyvtár az utalások kereséskor számba vesz. Az alapértelmezett szakaszszám érték 10.

-p *ldapport*

Egy alternatív TCP port megadása, amelyiken az LDAP szerver figyel. Az alapértelmezés szerinti LDAP port a 389. Ha a **-p** kapcsoló nincs megadva, de a **-Z** kapcsoló igen, akkor a rendszer az alapértelmezés szerinti 636-os LDAP SSL portot használja.

-P *kulcsfájl_jelszó*

A kulcsadatbázis jelszavát adja meg. A jelszó a kulcsadatbázis-fájl rejtjelezett tartalmának (amely egy vagy több privát kulcsot is tartalmazhat) eléréséhez szükséges. Ha rendelve lett jelszótároló fájl a

kulcsadatbázis-fájlhoz, akkor a jelszó a jelszótároló fájlból kérdezhető le, ezért a **-P** paraméterre nincs szükség. Ez a paraméter figyelmen kívül marad, ha sem a **-Z**, sem a **-K** nincs megadva.

-R Azt határozza meg, hogy az utalásokat nem kell automatikusan követni.

-U felhasználónév

Adja meg a felhasználónevet. Az **-m** DIGEST-MD5 használata esetén szükséges, minden más mechanizmussal figyelmen kívül marad.

-v Bővebb diagnosztikai információt nyújt, amelyet a szabványos kimenetre ír.

-V változat

Megadja, hogy az **ldapdchangepwd** parancs melyik LDAP változatot használja a szervertel való kapcsolódáskor. Alapértelmezés szerint LDAP V3 összeköttetést létesít. Ahhoz, hogy kifejezetten az LDAP V3 legyen kiválasztva, **-V 3** kapcsolót kell megadni. Adja meg a **-V 2** kapcsolót, ha LDAP V2 alkalmazásként kívánja futtatni. Az **ldapmodrtn** segédprogramhoz hasonló alkalmazások úgy választják az LDAP V3-at előnyben részesített protokollként, hogy az `ldap_init` funkciót használják az `ldap_open` helyett.

-w jelszó | ?

A **jelszó** használata hitelesítési jelszóként. A **?** karakter megadása esetén a program bekéri a jelszót.

-y proxydn

Megadja a proxy azonosítót a proxy hitelesítési művelethez.

-Y Biztonságos LDAP kapcsolatot (TLS) használ.

-Z Védett SSL kapcsolat használata az LDAP szervertel folyó kommunikáció során. Az i5/OS alatt futó Directory Server esetében, ha a **-Z** kapcsolót használja, de a **-K** vagy **-N** kapcsolót nem, akkor a Directory Services kliensalkalmazás azonosítóhoz rendelt igazolás kerül használatra.

-? Megjeleníti az `ldapdchangepwd` parancs szintaxis-súgóját.

Példák

A következő parancs:

```
ldapdchangepwd -D cn=John Doe -w a1b2c3d4 -n wxyz9876
```

megváltoztatja a "John Doe" `commonName` attribútumú bejegyzés jelszavát a `a1b2c3d4`-ről a `wxyz9876` értékre

Diagnosztika

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

ldapdiff

Az LDAP replikasinkronizációs eszköz.

Megjegyzés: Ez a parancs meglehetősen hosszú ideig is futhat, a replikált bejegyzések (és azok attribútumainak) számától függően.

Összegzés

(Összehasonlítja és szinkronizálja egy replikációs környezet két szervere közötti adatbejegyzéseket.)

```
ldapdiff -b baseDN -sh hoszt -ch hoszt [-a] [-C számláló]
[-cd dn] [-ck keyStore] [-cw jelszó] [-cN kulcsazonosító]
[-cp port] [-cP kulcs tároló_jelszó] [-cZ] [-F] [-L fájl név] [-sD dn] [-sK kulcs tároló]
[-sw jelszó] [-sN kulcsazonosító] [-sp port] [-sP kulcs tároló_jelszó]
[-sZ] [-v]
```

vagy

(Összehasonlítja két szerver sémáját.)

```
ldapdiff -S -sh hoszt -ch hoszt [-a] [-C számláló][-cD dn]
[-cK keyStore] [-cw jelszó] [-cN kulcsazonosító] [-cp port]
[-cP kulcstároló_jelszó] [-cZ] [-L fájlnev] [-sD dn]
[-sK kulcstároló] [-sw jelszó] [-sN kulcsazonosító] [-sp port]
[-sP kulcstároló_jelszó] [-sZ] [-v]
```

Leírás

Ez az eszköz szinkronizál egy replikaszervert az elsődleges szerverrel. Az **ldapdiff** parancs szintaxisának megjelenítéséhez írja be az alábbi parancsot:

```
ldapdiff -?
```

Beállítások

Az alábbi beállítások az **ldapdiff** parancsra vonatkoznak. Két alcsoport van, amelyek az ellátó és a fogyasztó kiszolgálókra vonatkoznak.

- a** A szerver adminisztrációs vezérlés használatát írja elő egy csak olvasható replika számára.
- b baseDN**
Az alapértelmezés helyett a megadott alap DN szolgál a keresés kezdőpontjául. Ha nem adja meg a **-b** kapcsolót, akkor a segédprogram az LDAP_BASEDN környezeti változóban keresi a keresési_alap definícióját.
- C számláló**
Megszámlálja a javítandó bejegyzéseket. Ha a megadott számnál több eltérést talál, az eszköz kilép.
- F** Ez a javítási paraméter. Ha meg van adva, a fogyasztó replika tartalma módosításra kerül az ellátó szerver tartalmának megfelelően. Ez a kapcsoló nem használható együtt a **-S** kapcsolóval.
- L** Ha a **-F** kapcsoló nincs megadva, használja ezt a kapcsolót egy LDIF formátumú kimenet előállításához. Az LDIF fájl azután használható a fogyasztón a különbségek megszüntetésére.
- S** A két szerver sémájának összehasonlítását írja elő.
- v** Bővebb diagnosztikai információt nyújt, amelyet a szabványos kimenetre ír.

Replikációs ellátó beállításai

Az alábbi paraméterek az ellátó (supplier) szerverre vonatkoznak, ezt egy kezdő 's' betű jelzi a paraméterek nevében.

- sD dn** A **dn** paraméter által megadott kapcsolódási DN-t használja az LDAP címtárhoz kapcsolódáshoz. A **dn** egy karakterlánccal képviselt DN.
- sh hoszt**
A hoszt nevét adja meg.
- sK kulcstároló**
Megadja a **kdb** alapértelmezett kiterjesztésű SSL kulcsadatbázis-fájl nevét. Ha ez a paraméter nincs megadva, vagy az értéke üres karaktorsorozat (**-sK""**), akkor a program a rendszer kulcstárolóját használja. Ha a kulcsadatbázis-fájl nem az aktuális könyvtárban található, megadja az adatbázisfájl teljes nevét.
- sN kulcsazonosító**
A kulcsadatbázis-fájlban található kliensigazolásához tartozó azonosítót adja meg. Ha kulcstároló nélkül ad meg azonosítót, akkor az azonosító a Digitális igazoláskezelő (DCM) egy alkalmazásazonosítója. Az alapértelmezett azonosító (alkalmazásazonosító) a QIBM_GLD_DIRSrv_CLIENT. Amennyiben az LDAP szerver csak szerver hitelesítésre lett beállítva, a kliensigazolásra nincs szükség. Ha az LDAP szerver kliens- és szerverhitelesítésre lett beállítva, a kliensigazolásra szükség van. A **kulcsazonosító** paraméter nem szükséges, ha egy alapértelmezett igazolás/privát kulcspár ki lett jelölve. Hasonlóképpen akkor sem szükséges a **kulcsazonosító**, ha van egy egyedi igazolás/privát kulcspár a megjelölt adatbázisfájlban. Ez a paraméter figyelmen kívül marad, ha sem a **-sZ**, sem a **-sK** kapcsoló nincs megadva.

-sp *ldapport*

Egy alternatív TCP port megadása, amelyiken az LDAP szerver figyel. Az alapértelmezés szerinti LDAP port a 389. Ha a **-sp** kapcsoló nincs megadva, de a **-sZ** kapcsoló igen, akkor a rendszer az alapértelmezés szerinti 636-os LDAP SSL portot használja.

-sP *kulcstároló_jelszó*

A kulcsadatbázis jelszavát adja meg. A jelszó a kulcsadatbázis-fájl rejtjelezett tartalmának (amely egy vagy több privát kulcsot is tartalmazhat) eléréséhez szükséges. Ha rendelve lett jelszótároló fájl a kulcsadatbázis-fájlhoz, akkor a jelszó a jelszótároló fájlból kérdezhető le, ezért a **-sP** paraméterre nincs szükség. Ez a paraméter figyelmen kívül marad, ha sem a **-sZ**, sem a **-sK** kapcsoló nincs megadva. A paramétert nem használja a program, ha a kulcstárolóhoz jelszótároló fájlt használ.

-st *trustStoreType*

A bizalmi adatbázis-fájlban található kliensigazolóhoz tartozó azonosítót adja meg. Amennyiben az LDAP szerver csak szerver hitelesítésre lett beállítva, a kliensigazolásra nincs szükség. Ha az LDAP szerver kliens- és szerverhitelesítésre lett beállítva, a kliensigazolásra szükség van. A **trustStoreType** paraméter nem szükséges, ha egy alapértelmezett igazolás/privát kulcspár alapértelmezettként ki lett jelölve. Hasonlóképpen akkor sem szükséges a **trustStoreType** paraméter, ha van egy egyedi igazolás/privát kulcspár a megjelölt adatbázisfájlban. Ez a paraméter figyelmen kívül marad, ha sem a **-sZ**, sem a **-sT** kapcsoló nincs megadva.

-sZ Védett SSL kapcsolat használata az LDAP szerverrel folyó kommunikáció során.

Replikációs fogyasztó beállításai

Az alábbi paraméterek a fogyasztó (consumer) szerverre vonatkoznak, ezt egy kezdő 'c' betű jelzi a paraméterek nevében. A kényelem érdekében, ha a **-cZ** kapcsoló ki lett adva úgy, hogy a **-cK**, **-cN** vagy **-cP** paraméterek nem kaptak értéket, akkor ez utóbbiakhoz a program ugyanazokat az értékeket használja, mint amelyek az ellátó SSL paramétereiként meg lettek adva. Ha nem az ellátó beállításait akarja használni, hanem az alapértelmezéseket, akkor **-cK ""**, **-cN ""** és **-cP ""** formában adja meg a paramétereket.

-cD dn A **dn** paraméter által megadott kapcsolódási DN-t használja az LDAP címtárhoz kapcsolódáshoz. A **dn** egy karakterlánccal képviselt DN.

-ch *hoszt*

A hoszt nevét adja meg.

-cK *kulcstároló*

Megadja a kdb alapértelmezett kiterjesztésű SSL kulcsadatbázis-fájl nevét. Ha a paraméter értéke üres karaktorsorozat (**-sK ""**), akkor a program a rendszer kulcstárolóját használja. Ha a kulcsadatbázis-fájl nem az aktuális könyvtárban található, megadja az adatbázisfájl teljes nevét.

-cN *kulcsazonosító*

A kulcsadatbázis-fájlban található kliensigazolóhoz tartozó azonosítót adja meg. Amennyiben az LDAP szerver csak szerver hitelesítésre lett beállítva, a kliensigazolásra nincs szükség. Ha kulcstároló nélkül ad meg azonosítót, akkor az azonosító a Digitális igazoláskézelő (DCM) egy alkalmazásazonosítója. Az alapértelmezett azonosító (alkalmazásazonosító) a QIBM_GLD_DIRSrv_CLIENT. Ha az LDAP szerver kliens- és szerverhitelesítésre lett beállítva, a kliensigazolásra szükség van. A **kulcsazonosító** paraméter nem szükséges, ha egy alapértelmezett igazolás/privát kulcspár ki lett jelölve. Hasonlóképpen akkor sem szükséges a **kulcsazonosító**, ha van egy egyedi igazolás/privát kulcspár a megjelölt adatbázisfájlban. Ez a paraméter figyelmen kívül marad, ha sem a **-cZ**, sem a **-cK** nincs megadva.

-cp *ldapport*

Egy alternatív TCP port megadása, amelyiken az LDAP szerver figyel. Az alapértelmezés szerinti LDAP port a 389. Ha a **-cp** kapcsoló nincs megadva, de a **-cZ** kapcsoló igen, akkor a rendszer az alapértelmezés szerinti 636-os LDAP SSL portot használja.

-cP *kulcstároló_jelszó*

A kulcsadatbázis jelszavát adja meg. A jelszó a kulcsadatbázis-fájl rejtjelezett tartalmának (amely egy vagy több privát kulcsot is tartalmazhat) eléréséhez szükséges. Ha rendelve lett jelszótároló fájl a

kulcsadatbázis-fájlhoz, akkor a jelszó a jelszótároló fájlból kérdezhető le, ezért a **-cP** paraméterre nincs szükség. Ez a paraméter figyelmen kívül marad, ha sem a **-cZ**, sem a **-cK** nincs megadva.

-cw jelszó | ?

A **jelszó** paraméter használata hitelesítési jelszoként. A ? karakter megadása esetén a program bekéri a jelszót.

-cZ Védett SSL kapcsolat használata az LDAP szerverrel folyó kommunikáció során.

Példák

```
ldapdiff -b <baseDN> -sh <ellátóhosztnév> -ch <fogyasztóhosztnév> [beállítások]
```

vagy

```
ldapdiff -S -sh <supplierhostname> -ch  
<fogyasztóhosztnév> [ beállítások]
```

Diagnosztika

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

Az SSL védelem LDAP parancssori segédprogramok használata

A "Védett socket réteg (SSL) és Fordítási réteg biztonság (TLS) használata LDAP Directory Serverrel" oldalszám: 47 tárgyalja az SSL használatát a Directory Server LDAP szerverrel. Ebbe beleértendő a megbízható CA-k (Certificate Authorities) digitális igazoláskezelővel (Digital Certificate Manager) 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 lesznek többek között az alkalmazásprogram csatolók (API-k) által szolgáltatott LDAP igazoló levelek is, amelyek a címtárszerverhez 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 szerverigazolást használ, a szerver adminisztrátorától kell kérni egy szerverigazolást 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 gyökérigazolást 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 címtárszerverhez 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.

LDAP adatcsere formátum (LDIF)

Az alábbiakban leírjuk az LDAP Adatcsere formátumot (LDIF), amint azt az ldapmodify, ldapsearch és ldapadd segédprogramok használják. Az itt megadott LDIF formátumot támogatják az IBM Directory Server egyéb segédprogramjai is.

Az LDIF feladata, hogy az LDAP bejegyzéseket szöveges formátumban jelenítse meg. Egy LDIF bejegyzés alapvető formája:

```
dn: <megkülönböztetett név>
<attribútumtípus> : <attribútumérték>
<attribútumtípus> : <attribútumérték>
...
```

Egy sor folytatódhat a következő sorban, ha az egy szóköz vagy tabulátor karakterrel kezdődik, például:

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

A többszörös attribútumértékek külön sorokban adhatók meg, például:

```
cn: John E Doe
cn: John Doe
```

Ha egy <attribútumérték> nem US-ASCII karaktert tartalmaz, illetve szóköz vagy kettőspont (':') karakterrel kezdődik, akkor az <attribútumtípust> egy dupla kettőspont követi és az értéket base-64 jelöléssel kell megadni. A " begins with a space" (" szóközzel kezdődik") angol karaktersorozat kódolása például így néz ki:

```
cn:: IGJlZ2lucyB3aXRoIGEgc3BhY2U=
```

Ugyanazon LDIF fájlban belül a bejegyzéseket üres sorok választják el. Több üres sor logikai "fájl vége" jelnek számít.

További információk:

- "Példa: LDIF"
- "Version 1 LDIF támogatás" oldalszám: 222
- "Példák: 1. változat LDIF" oldalszám: 222

Példa: LDIF

Alább bemutatunk egy LDIF példafájlt, amely három bejegyzést tartalmaz.

```
dn: cn=John E Doe, o=University of High
    er Learning, c=US
cn: John E Doe
cn: John Doe
objectclass: person
sn: Doe

dn: cn=Bjorn L Doe, o=University of High
    er Learning, c=US
cn: Bjorn L Doe
cn: Bjorn Doe
objectclass: person
sn: Doe

dn: cn=Jennifer K. Doe, o=University of High
    er Learning, c=US
cn: Jennifer K. Doe
cn: Jennifer Doe
objectclass: person
sn: Doe
jpegPhoto:: /9j/4AAQSkZJRgABAAAAQABAAD/2wBDABALD
    A4MChAODQ4SERATGCGaGBYWGDEjJR0o0jM9PDkzODdASFxOQ
    ERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARESEhgVG
    ...
```

Jennifer Jensen bejegyzésének jpegPhoto attribútuma base-64 kódolású értéket tartalmaz. A szöveges attribútumértékek megadhatók base-64 formátumban is. Ebben az esetben azonban a base-64 kódolásnak a protokoll vezetékes formátumának kódlapjában kell lennie (LDAP V2 esetén IA5 karakterkészlet, LDAP V3 esetén UTF-8 kódolás).

Version 1 LDIF támogatás

A kliens segédprogramok (ldapmodify és ldapadd) továbbfejlesztésre kerültek, hogy felismerjék az LDIF legfrissebb változatát, amelyet a fájl fejlécében található "version: 1" címke jelöl. Szemben az LDIF eredeti változatával, az új LDIF változat UTF-8 kódolású attribútumértékeket is kezel (szemben a rendkívül korlátozott US-ASCII kódolással).

Egy UTF-8 kódolású értékeket tartalmazó LDIF fájl készítése azonban nehézkes lehet. A feladat leegyszerűsítése érdekében a programok támogatják az LDIF formátum egy karakterkészlet-bővítését. E bővítés lehetővé teszi egy IANA karakterkészlet nevének megadását az LDIF fájl fejlécében (a verziószám mellett). Az IANA karakterkészleteknek csak egy korlátozott halmaza támogatott.

Az 1-es változatú LDIF formátum fájl URL-ek használatát is lehetővé teszi. Ez rugalmasabb megoldást tesz lehetővé a fájlok megadásában. A fájl URL-ek az alábbi formátumúak:

```
attribútum:< file:///elérési_út          (az elérési_út
szintaxisa platformként eltérő)
```

A következő webcímek például érvényesek:

```
jpegphoto:< file:///d:\temp\photos\myphoto.jpg (DOS/Windows stílusú elérési utak)
jpegphoto:< file:///etc/temp/photos/myphoto.jpg (UNIX-stílusú elérési utak)
```

Megjegyzés: Az IBM Directory Server segédprogramjai támogatják mind az újfajta fájl URL meghatározásokat, mind a régebbi stílusúakat ("jpegphoto: /etc/temp/myphoto"), függetlenül a megadott verziószámtól. Más szavakkal, az új fájl URL formátum akkor is használható, ha nem veszi bele a verziószám címkét az LDIF fájllokba.

Példák: 1. változat LDIF

Az elhagyható charset (karakterkészlet) címkét használva a segédprogramok automatikusan átalakítják a megadott karakterkészletet UTF-8 karakterkészletre, az alábbi példához hasonlóan:

```
version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, o=University of New Mexico, c=US
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd
title: Associate Dean
title: [beosztás spanyolul]
jpegPhoto:> file:///usr/local/photos/jgriego.jpg
```

Ebben a példában minden attribútumnév és egyszeres kettőspont utáni érték átfordításra kerül az ISO-8859-1 karakterkészletről UTF-8-ra. Az attribútumnév és dupla kettőspont utáni értékek (például a description:: V2hhdCBhIGNhcm...) base-64 kódolásúak, és vagy bináris, vagy UTF-8 kódolású karaktorsorozatok. A fájlokból olvasott értékek, mint például az előző példában a webcímmel megadott jpegPhoto attribútum szintén vagy bináris, vagy UTF-8 kódolásúak kell, hogy legyenek. Ezen értékek esetén semmilyen átalakítás nem történik a megadott "charset" (karakterkészlet) és az UTF-8 kódolás között.

Az alábbi példában, ahol az LDIF fájlban nincs megadva a charset címke, a tartalomnak UTF-8 kódolásúnak, illetve base-64 kódolású UTF-8 vagy base-64 kódolású bináris adatnak kell lennie:

```
# IBM Directory Server minta LDIF fájl
#
# Az "o=IBM, c=US" utótagot még azelőtt kell definiálni, hogy
# megpróbálná betölteni ezeket az adatokat.

version: 1

dn: o=IBM, c=US
objectclass: top
objectclass: organization
o: IBM
```

```
dn: ou=Austin, o=IBM, c=US
ou: Austin
objectclass: organizationalUnit
seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

Ugyanez a fájl használható a version: 1 fejlécinformációk nélkül is, az IBM Directory Server korábbi kiadásaihoz hasonlóan:

```
# IBM Directory Server minta LDIF fájl
#
# Az "o=IBM, c=US" utótagot még azelőtt kell definiálni, hogy
# megpróbálná betölteni ezeket az adatokat.
```

```
dn: o=IBM, c=US
objectclass: top
objectclass: organization
o: IBM
```

```
dn: ou=Austin, o=IBM, c=US
ou: Austin
objectclass: organizationalUnit
seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

Megjegyzés: A szöveges attribútumértékek megadhatók base-64 formátumban is.

Directory Server konfigurációs séma

Az alábbi rész a címtár-információs fát (Directory Information Tree, DIT) és az `ibmslapd.conf` fájl beállításához használt attribútumokat írja le. A korábbi kiadásokban a címtár konfigurációs beállításai egyedi formátumban tárolódtak a konfigurációs fájlban. A címtár beállításai most már LDIF formátumban kerülnek tárolásra a konfigurációs fájlban.

A konfigurációs fájl neve `ibmslapd.conf`. Most már rendelkezésre áll a konfigurációs fájl által használt séma is. Az attribútumtípusok a `v3.config.at`, az objektumosztályok pedig a `v3.config.oc` fájlban találhatóak. Az attribútumok az `ldapmodify` paranccsal módosíthatók. További információk az `ldapmodify` parancsról: “`ldapmodify` és `ldapadd`” oldalszám: 191.

- “Címtár-információs fa”
- “Attribútumok” oldalszám: 232

Címtár-információs fa

`cn=Configuration`

- `cn=Admin`
- `cn=Event Notification`
- `cn=Front End`
- `cn=Kerberos`
- `cn=Master Server`
- `cn=Referral`
- `cn=Schema`
 - `cn=IBM Directory`
 - `cn=Config Backends`
 - `cn=ConfigDB`
 - `cn=RDBM Backends`
 - `cn=Directory`
 - `cn=ChangeLog`

- cn=LDCF Backends
 - cn=SchemaDB
- cn=SSL
 - cn=CRL
- cn=Transaction

cn=Configuration

DN cn=Configuration

Leírás Ez a konfigurációs DIT legfelső szintje. Ez elsősorban a szerver globális hatókörű beállításait tartalmazza, bár a gyakorlatban sok egyéb dolog is ide kerül. E bejegyzés minden attribútuma az ibmslapd.conf fájl első szakaszából (globális szakasz) származik.

Szám 1 (kötelező)

Objektumosztály
ibm-slapdTop

Kötelező attribútumok

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

Elhagyható attribútumok

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (Deprecated)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion

cn=Admin

DN cn=Admin, cn=Configuration

Leírás Az IBM Admin démon globális konfigurációs beállításai

Szám 1 (kötelező)

Objektumosztály
ibm-slapdAdmin

Kötelező attribútumok

- cn
- ibm-slapdErrorLog
- ibm-slapdPort

Elhagyható attribútumok

- ibm-slapdSecurePort

cn=Event Notification

DN cn=Event Notification, cn=Configuration

Leírás A Directory Server globális eseményértesítési beállításai

Szám 0 vagy 1 (elhagyható; csak akkor van rá szükség, ha engedélyezni akarja az eseményértesítést)

Objektumosztály

ibm-slapdEventNotification

Kötelező attribútumok

- cn
- ibm-slapdEnableEventNotification
- objectClass

Elhagyható attribútumok

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

cn=Front End

DN cn=Front End, cn=Configuration

Leírás A szerver által induláskor alkalmazott globális környezeti beállítások.

Szám 0 vagy 1 (elhagyható)

Objektumosztály

ibm-slapdFrontEnd

Kötelező attribútumok

- cn
- objectClass

Elhagyható attribútumok

- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdDB2CP
- ibm-slapdEntryCacheSize
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdPlugin
- ibm-slapdSetenv
- ibm-slapdIdleTimeOut

cn=Kerberos

DN cn=Kerberos, cn=Configuration

Leírás A Directory Server globális Kerberos hitelesítési beállításai.

Szám 0 vagy 1 (elhagyható)

Objektumosztály

ibm-slapdKerberos

Kötelező attribútumok

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

Elhagyható attribútumok

- Nincs

cn=Master Server

DN cn=Master Server, cn=Configuration

Leírás Egy replika beállításakor ez a bejegyzés tartalmazza az elsődleges szerver kapcsolódási hitelesítési adatait és utalási URL-jét.

Szám 0 vagy 1 (elhagyható)

Objektumosztály

ibm-slapdReplication

Kötelező attribútumok

- cn
- ibm-slapdMasterPW (Kötelező, ha nem Kerberos hitelesítést használ.)

Elhagyható attribútumok

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Kerberos hitelesítés használata esetén elhagyható.)
- ibm-slapdMasterReferral
- objectClass

cn=Referral

DN cn=Referral, cn=Configuration

Leírás Ez a bejegyzés tartalmazza az ibmslapd.conf fájl első szakaszának (globális szakasz) összes utalási bejegyzését. Ha nincsenek utalások (alapértelmezés szerint nincsenek), akkor ez a bejegyzés elhagyható.

Szám 0 vagy 1 (elhagyható)

Objektumosztály

ibm-slapdReferral

Kötelező attribútumok

- cn
- ibm-slapdReferral
- objectClass

Elhagyható attribútumok

- Nincs

cn=Schemas

DN cn=Schemas, cn=Configuration

Leírás Ez a bejegyzés szolgál a sémák tárolójául. Ez a bejegyzés valójában nem igazán szükséges, mivel a sémák megkülönböztethetők az ibm-slapdSchema objektumosztály segítségével. A DIT olvashatósága érdekében került be.

Jelenleg csak egy sémabejegyzés engedélyezett: cn=IBM Directory.

Szám 1 (kötelező)

Objektumosztály

Tároló

Kötelező attribútumok

- cn
- objectClass

Elhagyható attribútumok

- Nincs

cn=IBM Directory

DN cn=IBM Directory, cn=Schemas, cn=Configuration

Leírás Ez a bejegyzés tartalmazza az ibmslapd.conf fájl első szakaszának (globális szakasz) összes sémakonfigurációs adatát. Ezenfelül tárolóként szolgál a sémát használó összes célterület számára. Jelenleg nem támogatott több séma használata, de amennyiben lenne, úgy sémánként egy ibm-slapdSchema bejegyzés létezne. Ne feledje, hogy több séma feltételezhetően inkompatibilis. Éppen ezért egy célterület csak egyetlen sémához rendelhető.

Szám 1 (kötelező)

Objektumosztály

ibm-slapdSchema

Kötelező attribútumok

- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

Elhagyható attribútumok

- ibm-slapdSchemaAdditions

cn=Config Backends

DN cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Leírás Ez a bejegyzés szolgál a Konfigurációs célterületek tárolójául.

Szám 1 (kötelező)

Objektumosztály

Tároló

Kötelező attribútumok

- cn
- objectClass

Elhagyható attribútumok

Nincs

cn=ConfigDB

DN cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Leírás Konfigurációs célterület az IBM Directory Server konfigurációjához

Szám 0 - n (elhagyható)

Objektumosztály

ibm-slapdConfigBackend

Kötelező attribútumok

- ibm-slapdSuffix
- ibm-slapdPlugin

Elhagyható attribútumok

- ibm-slapdReadOnly

cn=RDBM Backends

DN cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Leírás Ez a bejegyzés szolgál az RDBM célterületek tárolójául. Lényegében felváltja az ibmslapd.conf adatbázis rdbm sorát és az összes albejegyzést DB2 célterületként azonosítja. Ez a bejegyzés valójában nem igazán szükséges, mivel az RDBM célterületek megkülönböztethetők az ibm-slapdRdbmBackend objektumosztály segítségével. A DIT olvashatósága érdekében került be.

Szám 0 vagy 1 (elhagyható)

Objektumosztály

Tároló

Kötelező attribútumok

- cn
- objectClass

Elhagyható attribútumok

- Nincs

cn=Directory

DN cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Leírás Ez a bejegyzés tartalmazza az alapértelmezett RDBM adatbázis célterület összes adatbázis-konfigurációs beállítását.

Bár több célterület is létrehozható tetszőleges nevekkel, a szerveradminisztráció feltételezi, hogy a "cn=Directory" a fő címtár célterület és a "cn=ChangeLog" az opcionális változtatási napló célterület. A szerveradminisztráció segítségével csak a "cn=Directory" alatt megjelenő utótagok konfigurálhatók (kivéve a changelog utótagot amely átlátszó módon állítható a változtatási napló engedélyezésével).

Szám 0 - n (elhagyható)

Objektumosztály

ibm-slapdRdbmBackend

Kötelező attribútumok

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Elhagyható attribútumok

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Megjegyzés: Ha használja az **ibm-slapdUseProcessIdPw** attribútumot, akkor módosítania kell a sémát, hogy az **ibm-slapdDbUserPW** attribútum elhagyható legyen.

cn=Change Log

DN cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Leírás Ez a bejegyzés tartalmazza a változtatási napló célterület összes adatbázis-konfigurációs beállítását.

Szám 0 - n (elhagyható)

Objektumosztály

ibm-slapdRdbmBackend

Kötelező attribútumok

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Elhagyható attribútumok

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin

- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Megjegyzés: Ha használja az **ibm-slapdUseProcessIdPw** attribútumot, akkor módosítania kell a sémát, hogy az **ibm-slapdDbUserPW** attribútum elhagyható legyen.

cn=LDCF Backends

DN cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Leírás Ez a bejegyzés szolgál az LDCF célterületek tárolójául. Lényegében felváltja az ibmslapd.conf adatbázis ldcf sorát és az összes albejegyzést LDCF célterületként azonosítja. Ez a bejegyzés valójában nem igazán szükséges, mivel az LDCF célterületek megkülönböztethetők az ibm-slapdLdcfBackend objektumosztály segítségével. A DIT olvashatósága érdekében került be.

Szám 1 (kötelező)

Objektumosztály
Tároló

Kötelező attribútumok

- cn
- objectClass

Elhagyható attribútumok

- ibm-slapdPlugin

cn=SchemaDB

DN cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Leírás Ez a bejegyzés tartalmazza az ibmslapd.conf fájl adatbázis szakaszának összes adatbázis-konfigurációs adatát.

Szám 1 (kötelező)

Objektumosztály
ibm-slapdLdcfBackend

Kötelező attribútumok

- cn
- objectClass

Elhagyható attribútumok

- ibm-slapdPlugin
- ibm-slapdSuffix

cn=SSL

DN cn=SSL, cn=Configuration

Leírás A Directory Server globális SSL kapcsolati beállításai.

Szám 0 vagy 1 (elhagyható)

Objektumosztály
ibm-slapdSSL

Kötelező attribútumok

- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

Elhagyható attribútumok

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

Megjegyzés: Az **ibm-slapdSslCipherSpecs** attribútum most már elavult. Használja helyette az **ibm-slapdSslCipherSpec** attribútumot. Ha az **ibm-slapdSslCipherSpecs** attribútumot használja, akkor a szerver átalakítja a támogatott attribútumra.

- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW

cn=CRL

DN cn=CRL, cn=SSL, cn=Configuration

Leírás Ez a bejegyzés tartalmazza az ibmslapd.conf fájl első szakaszának (globális szakasz) igazolás visszavonási lista adatait. Csak akkor van rá szükség, ha a cn=SSL bejegyzés "ibm-slapdSslAuth = serverclientauth" attribútuma és a kliensigazolások ki lettek adva CRL ellenőrzésre.

Szám 0 vagy 1 (elhagyható)

Objektumosztály

ibm-slapdCRL

Kötelező attribútumok

- cn
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPort
- objectClass

Elhagyható attribútumok

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword

cn=Transaction

DN cn = Transaction, cn = Configuration

Leírás Globális tranzakciótámogatási beállítások. A tranzakciók támogatását a következő bedolgozó biztosítja:
extendedop /QSYS.LIB/QGLDTRANEX.SRVPGM tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6

A szerver (**slapd**) automatikusan betölti ezt a bedolgozót induláskor, ha **ibm-slapdTransactionEnable = TRUE**. A bedolgozót nem kell külön kifejezetten felvenni az **ibmslapd.conf** fájlba.

Szám 0 vagy 1 (elhagyható; csak akkor kötelező, ha tranzakciókat akar használni)

Objektumosztály

ibm-slapdTransaction

Kötelező attribútumok

- cn

- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

Elhagyható attribútumok

- Nincs

Attribútumok

- cn
- ibm-slapdACIMechanism
- ibm-slapdACLAccess
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN
- | • ibm-slapdAdminGroupEnabled
- ibm-slapdAdminPW
- | • ibm-slapdAllowAnon
- | • ibm-slapdAllReapingThreshold
- | • ibm-slapdAnonReapingThreshold
- | • ibm-slapdBoundReapingThreshold
- ibm-slapdBulkloadErrors
- | • ibm-slapdCachedAttribute
- | • ibm-slapdCachedAttributeAutoAdjust
- | • ibm-slapdCachedAttributeAutoAdjustTime
- | • ibm-slapdCachedAttributeAutoAdjustTimeInterval
- | • ibm-slapdCachedAttributeSize
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConcurrentRW
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- | • ibm-slapdDerefAliases
- | • ibm-slapdDigestAdminUser
- | • ibm-slapdDigestAttr
- | • ibm-slapdDigestRealm
- ibm-slapdEnableEventNotification
- ibm-slapdEntryCacheSize
- ibm-slapdErrorLog

- | • ibm-slapdESizeThreshold
- | • ibm-slapdEThreadActivate
- | • ibm-slapdEThreadEnable
- | • ibm-slapdETimeThreshold
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- | • ibm-slapdLanguageTagsEnabled
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword
- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdMasterDN
- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplDbConns
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit

- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSuffix
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTransactionEnable
- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- ibm-slapdWriteTimeout
- objectClass

cn

Leírás Ez az X.500 általános név (common name) attribútum, amely az objektum nevét tartalmazza.

Szintaxis

Directory string

Maximális hossz

256

Érték

Többértékű

ibm-slapdACIMechanism

Leírás Azt határozza meg, hogy a szerver milyen ACL modellt használ. (Csak i5/OS és OS/400 rendszeren, a 3.2-es változat óta támogatott, minden más platformon figyelmen kívül marad.)

- 1.3.18.0.2.26.1 = IBM SecureWay v3.1 ACL modell
- 1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL modell

Alapértelmezett érték

1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL modell

Szintaxis

Directory string

Maximális hossz

256

Érték

Többértékű

ibm-slapdACLAccess

Leírás Azt szabályozza, hogy az ACL-ek engedélyezve vannak-e. TRUE értékre állítva az ACL-ek engedélyezve vannak. FALSE értékre állítva az ACL-ek le vannak tiltva.

Alapértelmezett érték

TRUE

Szintaxis

Logikai

Maximális hossz

5

Érték Egyértékű

ibm-slapdACLCache

Leírás Azt szabályozza, hogy a szerver ideiglenesen tárolja-e az ACL információkat.

- TRUE értékre állítva a szerver ideiglenesen tárolja az ACL információkat.
- FALSE értékre állítva a szerver nem tárolja ideiglenesen az ACL információkat.

Alapértelmezett érték

TRUE

Szintaxis

Logikai

Maximális hossz

5

Érték Egyértékű

ibm-slapdACLCacheSize

Leírás Az ACL gyorsítótárban tárolt bejegyzések maximális száma.

Alapértelmezett érték

25000

Szintaxis

Egész

Maximális hossz

11

Érték Egyértékű

ibm-slapdAdminDN

Leírás A Directory Server adminisztrátori kapcsolódási DN-je.

Alapértelmezett érték

cn=root

Szintaxis

DN

Maximális hossz

Korlátlan

Érték Egyértékű

ibm-slapdAdminGroupEnabled

Leírás Megadja, hogy az adminisztrációs csoport jelenleg engedélyezve van-e. Ha az értéke TRUE, akkor a szerver engedélyezni fogja az adminisztrációs csoport tagjainak a bejelentkezést.

Alapértelmezett érték

FALSE

Szintaxis

Logikai

Maximális hossz

128

| **Érték** Egyértékű

ibm-slapdAdminPW

Leírás A Directory Server adminisztrátori kapcsolódási jelszava.

Alapértelmezett érték
secret

Szintaxis
Bináris

Maximális hossz
128

Érték Egyértékű

| **ibm-slapdAllowAnon**

| **Leírás** Megadja, hogy engedélyezettek-e a névtelen kapcsolatok.

| **Alapértelmezett érték**
True

| **Szintaxis**
Logikai

| **Maximális hossz**
128

| **Érték** Egyértékű

| **ibm-slapdAllReapingThreshold**

Leírás Megadja, hogy hány kapcsolatot kell fenntartai a szerveren, mielőtt a kapcsolatkezelés aktiválásra kerülne.

Alapértelmezett érték
1200

Szintaxis
Directory string pontos egyezéssel

Maximális hossz
1024

Érték Egyértékű

| **ibm-slapdAnonReapingThreshold**

Leírás Megadja, hogy hány kapcsolatot kell fenntartai a szerveren, mielőtt a névtelen kapcsolatok kezelése aktiválásra kerülne.

Alapértelmezett érték
0

Szintaxis
Directory string pontos egyezéssel

Maximális hossz
1024

Érték Egyértékű

| **ibm-slapdBoundReapingThreshold**

| **Leírás** Megadja, hogy hány kapcsolatot kell fenntartani a szerveren, mielőtt a névtelen és kötött kapcsolatok kezelése aktiválásra kerülne.

| **Alapértelmezett érték**
| 1100

| **Szintaxis**
| Directory string pontos egyezéssel

| **Maximális hossz**
| 1024

| **Érték** Egyértékű

ibm-slapdBulkloadErrors

Leírás Fájl elérési út vagy eszköz az ibmslapd hosztgépen, amelybe az ömlesztett betöltés hibaüzenetei kiíródnak.

Alapértelmezett érték
/var/bulkload.log

Szintaxis
Directory string pontos egyezéssel

Maximális hossz
1024

Érték Egyértékű

ibm-slapdCachedAttribute

| **Leírás** Az attribútum-gyorsítótárban elhelyezendő attribútumok nevét tartalmazza, értékenként egy nevet.

| **Alapértelmezett érték**
| Nincs

| **Szintaxis**
| Directory string

| **Maximális hossz**
| 256

| **Érték** Többértékű

ibm-slapdCachedAttributeAutoAdjust

| **Leírás** Felügyeli, hogy a szerver automatikusan beállítja-e az attribútum-gyorsítótárat az ibm-slapdCachedAttributeAutoAdjustTime és ibm-slapdCachedAttributeAutoAdjustTimeInterval elemekben beállított időközönként.

| **Alapértelmezett érték**
| FALSE

| **Szintaxis**
| Logikai

| **Maximális hossz**
| 5

| **Érték** Egyértékű

ibm-slapdCachedAttributeAutoAdjustTime

| **Leírás** Ha az ibm-slapdCachedAttributeAutoAdjust értéke TRUE, felügyeli azt az időpontot, amikor a szerver automatikusan elkezd beállítani az attribútum-gyorsítótárat.

| Minimum = T000000
| Maximum = T235959

| **Alapértelmezett érték**

| T000000

| **Szintaxis**

| Katonai idő

| **Maximális hossz**

| 7

| **Érték** Egyértékű

| **ibm-slapdCachedAttributeAutoAdjustTimeInterval**

| **Leírás** Ha az ibm-slapdCachedAttributeAutoAdjust értéke TRUE, felügyeli az attribútum-gyorsítótár automatikus beállításai közötti időközt.

| Minimum = 1
| Maximum = 24

| **Alapértelmezett érték**

| 2

| **Szintaxis**

| Egész

| **Maximális hossz**

| 2

| **Érték** Egyértékű

| **ibm-slapdCachedAttributeSize**

| **Leírás** Az attribútum-gyorsítótárhoz felhasználható memória mennyisége byte-okban. 0 érték jelzi, ha az attribútum-gyorsítótár nincs használatban.

| **Alapértelmezett érték**

| 0

| **Szintaxis**

| Egész

| **Maximális hossz**

| 11

| **Érték** Egyértékű

| **ibm-slapdChangeLogMaxEntries**

| **Leírás** Ezt az attribútumot használja a változtatási napló bedolgozó arra, hogy megadja az RDBM adatbázisban tárolt változtatási napló bejegyzések maximális számát. Minden egyes változtatási naplóhoz saját changeLogMaxEntries attribútum tartozik.

| Minimális érték = 0 (korlátlan)
| Maximális érték = 2 147 483 647 (32 bites, előjeles egész)

| **Alapértelmezett érték**

| 0

| **Szintaxis**

| Egész

| **Maximális hossz**

| 11

| **Érték** Egyértékű

ibm-slapdCLIErrors

Leírás Fájl elérési út vagy eszköz az ibmslapd hosztgépen, amelybe a CLI hibaüzenetek kiíródnak.

Alapértelmezett érték
/var/db2cli.log

Szintaxis
Directory string pontos egyezéssel

Maximális hossz
1024

Érték Egyértékű

ibm-slapdConcurrentRW

Leírás TRUE értékre állítva lehetővé teszi a keresések és frissítések egyidejű végrehajtását. Engedélyezi a "piszkos olvasásokat", vagyis olyan eredményeket, amelyek nem feltétlenül egyeznek meg az adatbázis véglegesített állapotával.

FIGYELEM: Ez az attribútum elavult.

Alapértelmezett érték
FALSE

Szintaxis
Logikai

Maximális hossz
5

Érték Egyértékű

ibm-slapdDB2CP

Leírás A címtár-adatbázis kódlapját adja meg. Az UTF-8 adatbázisok kódlapja a 1208-as.

Szintaxis
Directory string pontos egyezéssel

Maximális hossz
11

Érték Egyértékű

ibm-slapdDBAlias

Leírás A DB2 adatbázis álnév.

Szintaxis
Directory string pontos egyezéssel

Maximális hossz
8

Érték Egyértékű

ibm-slapdDbConnections

Leírás A szerver által a DB2 célterületnek fenntartott DB2 kapcsolatok számát adja meg. Az érték 5 & 50 közé kell, hogy essen (a határokat is beleértve).

Megjegyzés: Az ODBCCONS környezeti változó felülbírálja ennek a beállításnak az értékét. Ha az ibm-slapdDbConnections (vagy a ODBCCONS változó) értéke kisebb mint 5 vagy nagyobb mint

50, akkor a szerver az 5, illetve 50 értéket használja. 1 további kapcsolat kerül létrehozásra a replikációhoz (még akkor is, ha nincs megadva replikáció). 2 további kapcsolat kerül létrehozásra a változtatási naplóhoz (amennyiben engedélyezve van).

Alapértelmezett érték

15

Szintaxis

Egész

Maximális hossz

50

Érték Egyértékű

ibm-slapdDbInstance

Leírás A célterület DB2 adatbázispéldányát adja meg.

Alapértelmezett érték

ldapdb2

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

8

Érték Egyértékű

Megjegyzés: Az összes ibm-slapdRdbmBackend objektumnak ugyanazokat az ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW és DB2 karakterkészlet beállításokat kell használnia.

ibm-slapdDbLocation

Leírás A fájlrendszer elérési út, ahol a háttéradatbázis található.

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

1024

Érték Egyértékű

ibm-slapdDbName

Leírás A célterület DB2 adatbázisának nevét adja meg.

Alapértelmezett érték

ldapdb2

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

8

Érték Egyértékű

ibm-slapdDbUserID

Leírás A jelen célterület által az DB2 adatbázishoz kapcsolódáshoz használt felhasználónevet adja meg.

Alapértelmezett érték

ldapdb2

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

8

Érték Egyértékű

Megjegyzés: Az összes ibm-slapdRdbmBackend objektumnak ugyanazokat az ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW és DB2 karakterkészlet beállításokat kell használnia.

| ibm-slapdDerefAliases

| Leírás A keresési kérések maximális hivatkozásfeloldási szintje, függetlenül a klienskérésben megadott minden derefAliases elemtől. Az engedélyezett értékek: **soha**, **találat**, **keresés** és **mindig**.

| Alapértelmezett érték**| mindig****| Szintaxis****| Címtár karaktersorozat****| Maximális hossz****| 6****| Érték** Egyértékű**ibm-slapdDbUserPW**

Leírás A jelen célterület által az DB2 adatbázishoz kapcsolódáshoz használt jelszót adja meg. A jelszó lehet sima szöveg vagy imask kódolású.

Alapértelmezett érték

ldapdb2

Szintaxis

Bináris

Maximális hossz

128

Érték Egyértékű

Megjegyzés: Az összes ibm-slapdRdbmBackend objektumnak ugyanazokat az ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW és DB2 karakterkészlet beállításokat kell használnia.

| ibm-slapdDigestAdminUser

| Leírás Megadja az LDAP adminisztrátor vagy az adminisztrációs csoporttag Digest MD5 felhasználónevét. Akkor kell, ha az adminisztrátor hitelesítésére MD5 Digest eljárást használnak.

| Alapértelmezett érték**| Nincs****| Szintaxis****| Directory string****| Maximális hossz****| 512**

| **Érték** Egyértékű

| **ibm-slapdDigestAttr**

| **Leírás** Felülbírálja az alapértelmezett DIGEST-MD5 felhasználónév-attribútumot. A DIGEST-MD5 SASL kapcsolat felhasználónév kikereséshez használt attribútum neve. Ha az érték nincs megadva, akkor a szerver az uid-t használja.

| **Alapértelmezett érték**

| Ha nincs megadva, akkor a szerver az uid-t használja.

| **Szintaxis**

| Címtár karaktersorozat.

| **Maximális hossz**

| 64

| **Érték** Egyértékű

| **ibm-slapdDigestRealm**

| **Leírás** Felülbírálja az alapértelmezett DIGEST-MD5 tartományt. Egy karaktersorozat, amely engedélyezheti a felhasználók számára annak megismerését, hogy melyik felhasználónevet és jelszót kell használni, abban az esetben, ha a különféle szervereken különbözőeket használnak. Fogalmilag ez egy fiókgyűjtemény neve, ami tartalmazhatja a felhasználói fiókot. Ennek a karaktersorozatnak legalább a hitelesítést végrehajtó hoszt nevét tartalmaznia kell, de emellett jelezheti a hozzáférést igénylő felhasználók gyűjteményét is. Példa lehet a `registered_users@gotham.news.example.com`. Ha az attribútum nincs megadva, akkor a szerver a szerver teljes képzésű hosztnevét használja.

| **Alapértelmezett érték**

| A szerver teljes képzésű hosztneve

| **Szintaxis**

| Címtár karaktersorozat.

| **Maximális hossz**

| 1024

| **Érték** Egyértékű

ibm-slapdEnableEventNotification

Leírás Az eseményértesítés engedélyezését határozza meg. Értéke TRUE vagy FALSE lehet.

FALSE értékre állítja a szerver LDAP_UNWILLING_TO_PERFORM kiterjesztett eredménnyel visszautasít minden eseményértesítés bejegyzésére vonatkozó klienskérést.

Alapértelmezett érték

TRUE

Szintaxis

Logikai

Maximális hossz

5

Érték Egyértékű

ibm-slapdEntryCacheSize

Leírás A bejegyzés gyorsítótárban tárolt bejegyzések maximális száma.

Alapértelmezett érték

25000

Szintaxis

Egész

Maximális hossz

11

Érték Egyértékű**ibm-slapdErrorLog****Leírás** Azt a fájl elérési utat vagy eszközt adja meg a Directory Server gépen, amelybe a hibaüzenetek íródnak.**Alapértelmezett érték**

/var/ibmslapd.log

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

1024

Érték Egyértékű**| ibm-slapdESizeThreshold****| Leírás** Megadja, hogy hány feladatelem lehet a feladat várakozási sorban, mielőtt a vészszál aktiválásra kerülne**| Alapértelmezett érték****|** 50**| Szintaxis****|** Egész**| Maximális hossz****|** 1024**| Érték** Egyértékű**| ibm-slapdEThreadActivate****| Leírás** Megadja, hogy mely feltételek aktiválják a vészszálatAz alábbi értékek egyike kell, hogy legyen:**|** **S** Csak méret**|** **T** Csak idő**|** **SOT** Méret vagy idő**|** **SAT** Méret és idő**| Alapértelmezett érték****|** SAT**| Szintaxis****|** Karaktorsorozat**| Maximális hossz****|** 1024**| Érték** Egyértékű**| ibm-slapdEThreadEnable****| Leírás** Megadja, hogy aktív-e a vészszál**| Alapértelmezett érték****|** True

| **Szintaxis**
| Logikai
| **Maximális hossz**
| 1024
| **Érték** Egyértékű

ibm-slapdETimeThreshold

| **Leírás** Megadja, hogy hány percenként kerülnek eltávolításra elemek a feladatsorból, mielőtt a vészsál aktiválásra kerül.

| **Alapértelmezett érték**
| 5

| **Szintaxis**
| Egész

| **Maximális hossz**
| 1024

| **Érték** Egyértékű

ibm-slapdFilterCacheBypassLimit

Leírás Ennél több bejegyzésnek megfelelő keresési szűrő nem kerül be a Keresési szűrő gyorsítótárba. Mivel a szűrőnek megfelelő bejegyzésazonosítók bekerülnek a gyorsítótárba, ez a beállítás segít a memóriahasználat korlátozásában. A 0 érték a korlátozás hiányát jelzi.

Alapértelmezett érték
100

Szintaxis
Egész

Maximális hossz
11

Érték Egyértékű

ibm-slapdFilterCacheSize

Leírás A Keresési szűrő gyorsítótárban tárolt bejegyzések maximális számát adja meg.

Alapértelmezett érték
25000

Szintaxis
Egész

Maximális hossz
11

Érték Egyértékű

ibm-slapdIdleTimeOut

Leírás Egy LDAP kapcsolat maximális nyitvatartási ideje, ha a kapcsolaton nem zajlik tevékenység. Az LDAP kapcsolat tétlenségi ideje (másodpercben) a kapcsolat legutolsó művelete és a pillanatnyi idő között. Ha a kapcsolat - az attribútum értéke alapján - lejárt, akkor az LDAP szerver kitakarítja és lezárja az LDAP kapcsolatot és elérhetővé teszi más kérések számára.

Alapértelmezett érték
300

Szintaxis

Egész

Hossz 11**Számosság**

Egyszeres

Használat

Címtárművelet

Felhasználó által módosítható

Igen

Hozzáférési osztály

Kritikus

Kötelező

Nem

ibm-slapdIncludeSchema

Leírás Egy sémameghatározásokat tartalmazó fájl elérési útját adja meg a Directory Server szervergépen.

Alapértelmezett érték

/etc/V3.system.at
/etc/V3.system.oc
/etc/V3.config.at
/etc/V3.config.oc
/etc/V3.ibm.at
/etc/V3.ibm.oc
/etc/V3.user.at
/etc/V3.user.oc
/etc/V3.ldapsyntaxes
/etc/V3.matchingrules

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

1024

Érték Többértékű**ibm-slapdKrbAdminDN**

Leírás Az LDAP adminisztrátor Kerberos azonosítóját adja meg (például `ibm-kn=admin1@realm1`). Kerberos hitelesítés használata esetén szolgál az adminisztrátor hitelesítésére, amikor az bejelentkezik a szerveradminisztrátori felületre. Ez az érték az `adminDN` és `adminPW` attribútumokkal együtt vagy helyettük adható meg.

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

128

Érték Egyértékű

ibm-slapdKrbEnable

Leírás Azt határozza meg, hogy a szerver kezel-e Kerberos hitelesítést. Értéke TRUE vagy FALSE lehet.

Alapértelmezett érték

TRUE

Szintaxis

Logikai

Maximális hossz

5

Érték Egyértékű

ibm-slapdKrbIdentityMap

Leírás A Kerberos azonosság-leképezés használatát szabályozza. Értéke TRUE vagy FALSE lehet. TRUE értékre állítva, ha egy kliens Kerberos azonosítóval hitelesíti magát, akkor a szerver kikeresi az egyező Kerberos hitelesítési adatokkal rendelkező összes helyi felhasználót, és felveszi ezeket a felhasználói DN-eket az összeköttetés kapcsolódási hitelesítési adatai közé. Így az ACL-ek LDAP felhasználói DN-ek alapján adhatók meg, ugyanakkor mégis használhatók Kerberossal együtt.

Alapértelmezett érték

FALSE

Szintaxis

Logikai

Maximális hossz

5

Érték Egyértékű

ibm-slapdKrbKeyTab

Leírás Az LDAP szerver Kerberos keytab fájlját adja meg. Ez a fájl tartalmazza az LDAP szervernek a Kerberos fiókjához rendelt magánkulcsát. Ezt a fájlt védeni kell (ugyanúgy, mint a szerver SSSL kulcsadatbázis-fájlt).

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

1024

Érték Egyértékű

ibm-slapdKrbRealm

Leírás Az LDAP szerver Kerberos tartományát adja meg. Használatával kerül az ldapservicename attribútum közzétételre a gyökér DSE-ben. Ügyeljen rá, hogy bár az LDAP szerver több KDC (és tartomány) fiókinformációit is képes tárolni, addig az LDAP szerver maga, mint Kerberos-vezérlésű szerver, csak egy tartományba tartozhat.

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

256

Érték Egyértékű**| ibm-slapdLanguageTagsEnabled**

| Leírás Engedélyezi-e a szerver a nyelvi címkék használatát. Az attribútum `ibmslapd.conf` fájlból kiolvasott értéke FALSE, de TRUE-ra állítható.

| Alapértelmezett érték

| FALSE

| Szintaxis

| Logikai

| Maximális hossz

| 5

| Érték Egyértékű

ibm-slapdLdapCrlHost

Leírás Az x.509v3 igazolások ellenőrzéséhez használt Igazolás visszavonási listákat (CRL-eket) tároló LDAP szerver hosztnevét adja meg. Erre a paraméterre akkor van szükség, ha az `ibm-slapdSslAuth` attribútum értéke "serverclientauth" és a kliensigazolások kiadásra kerültek CRL ellenőrzésre.

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

256

Érték Egyértékű

ibm-slapdLdapCrlPassword

Leírás Azt a jelszót adja meg, amellyel a szerveroldali SSL kapcsolódik az x.509v3 igazolások ellenőrzéséhez használt Igazolás visszavonási listákat (CRL-eket) tároló LDAP szerverhez. Erre a paraméterre szükség lehet, ha az `ibm-slapdSslAuth` attribútum értéke "serverclientauth" és a kliensigazolások kiadásra kerültek CRL ellenőrzésre.

Megjegyzés: Ha a CRL-eket tároló LDAP szerver engedi a nem hitelesített (vagyis anonim) hozzáférést a CRL-ekhez, akkor nincs szükség az `ibm-slapdLdapCrlPassword` attribútum használatára.

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

Bináris

Maximális hossz

128

Érték Egyértékű

ibm-slapdLdapCrlPort

Leírás Az x.509v3 igazolások ellenőrzéséhez használt Igazolás visszavonási listákat (CRL-eket) tároló LDAP szerverhez csatlakozáshoz használt portot adja meg. Erre a paraméterre akkor van szükség, ha az

ibm-slapdSslAuth attribútum értéke "serverclientauth" és a kliensigazolások kiadásra kerültek CRL ellenőrzésre. (Az IP portok előjel nélküli, 16 bites egészek az 1 - 65535 tartományban)

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

Egész

Maximális hossz

11

Érték Egyértékű

ibm-slapdLdapCrlUser

Leírás Azt a bindDN-t adja meg, amellyel a szerveroldali SSL kapcsolódik az x.509v3 igazolások ellenőrzéséhez használt igazolás visszavonási listákat (CRL-eket) tároló LDAP szerverhez. Erre a paraméterre szükség lehet, ha az ibm-slapdSslAuth attribútum értéke "serverclientauth" és a kliensigazolások kiadásra kerültek CRL ellenőrzésre.

Megjegyzés: Ha a CRL-eket tároló LDAP szerver engedi a nem hitelesített (vagyis anonim) hozzáférést a CRL-ekhez, akkor nincs szükség az ibm-slapdLdapCrlUser attribútum használatára.

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

DN

Maximális hossz

1000

Érték Egyértékű

ibm-slapdMasterDN

Leírás Az elsődleges szerver kapcsolódási DN-je. Ennek az értéknek meg kell egyeznie az elsődleges szerverhez megadott replicaObject objektum replicaBindDN attribútumának értékével. Ha a replikához hitelesítésre Kerberost használ, akkor az ibm-slapdMasterDN attribútumnak a Kerberos azonosító DN ábrázolását kell tartalmaznia (például ibm-kn=freddy@realm1). Kerberos használata esetén a MasterServerPW attribútum figyelmen kívül marad.

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

DN

Maximális hossz

1000

Érték Egyértékű

ibm-slapdMasterPW

Leírás Az elsődleges replikaszerver kapcsolódási jelszava. Ennek az értéknek meg kell egyeznie az elsődleges szerverhez megadott replicaObject objektum replicaBindDN attribútumának értékével. Ha a replikához hitelesítésre Kerberost használ, akkor az ibm-slapdMasterDN attribútumnak a Kerberos azonosító DN ábrázolását kell tartalmaznia (például ibm-kn=freddy@realm1). Kerberos használata esetén a MasterServerPW attribútum figyelmen kívül marad.

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

Bináris

Maximális hossz

128

Érték Egyértékű**ibm-slapdMasterReferral****Leírás** Az elsődleges replikaszerver URL-jét adja meg. Például:

ldap://master.us.ibm.com

Csak SSL használatára beállított biztonság esetén:

ldaps://master.us.ibm.com:636

"Nincs" értékre állított biztonság és nem szabványos port használata esetén:

ldap://master.us.ibm.com:1389

Alapértelmezett érték

none

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

256

Érték Egyértékű**ibm-slapdMaxEventsPerConnection****Leírás** A kapcsolatonként bejegyezhető eseményértesítések maximális számát adja meg.

Minimális érték = 0 (korlátlan)

Maximális érték = 2 147 483 647

Alapértelmezett érték

100

Szintaxis

Egész

Maximális hossz

11

Érték Egyértékű**ibm-slapdMaxEventsTotal****Leírás** Az összesen bejegyezhető eseményértesítések maximális összesített számát adja meg.

Minimális érték = 0 (korlátlan)

Maximális érték = 2 147 483 647

Alapértelmezett érték

0

Szintaxis

Egész

Maximális hossz

11

Érték Egyértékű

ibm-slapdMaxNumOfTransactions

Leírás A szerverenkénti tranzakciók maximális számát adja meg.

Minimális érték = 0 (korlátlan)

Maximális érték = 2 147 483 647

Alapértelmezett érték

20

Szintaxis

Egész

Maximális hossz

11

Érték Egyértékű

ibm-slapdMaxOpPerTransaction

Leírás A tranzakciónkénti műveletek maximális számát adja meg.

Minimális érték = 0 (korlátlan)

Maximális érték = 2 147 483 647

Alapértelmezett érték

5

Szintaxis

Egész

Maximális hossz

11

Érték Egyértékű

ibm-slapdMaxPendingChangesDisplayed

Leírás A megjelenítendő, függőben lévő módosítások maximális száma.

Alapértelmezett érték

200

Szintaxis

Egész

Maximális hossz

11

Érték Egyértékű

ibm-slapdMaxTimeLimitOfTransactions

Leírás Egy függőben lévő tranzakció maximális időkorlátja másodpercekben.

Minimális érték = 0 (korlátlan)

Maximális érték = 2 147 483 647

Alapértelmezett érték

300

Szintaxis

Egész

Maximális hossz

11

Érték Egyértékű

ibm-slapdPagedResAllowNonAdmin

Leírás Azt határozza meg, hogy a szerver engedi-e a nem adminisztrátori kapcsolódást, ha a keresési kérés oldalakra bontott eredménymegjelenítést kér. Ha az ibmslapd.conf fájlból olvasott érték FALSE, akkor a szerver csak az adminisztrátori jogosultsággal elküldött klienskéréseket dolgozza fel. Ha egy kliens oldalakra bontott eredménymegjelenítést kér egy keresési műveletben, nem rendelkezik adminisztrátori jogosultsággal, és az attribútumnak az ibmslapd.conf fájlból olvasott értéke FALSE, akkor a szerver a kliensnek insufficientAccessRights visszatérési kódot ad vissza és semmilyen keresés vagy oldalra bontás nem történik.

Alapértelmezett érték

FALSE

Szintaxis

Logikai

Hossz

5

Számosság

Egyszeres

Használat

directoryOperation

Felhasználó által módosítható

Igen

Hozzáférési osztály

kritikus

Objektumosztály

ibm-slapdRdbmBackend

Kötelező

Nem

ibm-slapdPagedResLmt

Leírás Az egyidejűleg aktív, kinnlévő, oldalakra bontott eredménymegjelenítést kérő keresési kérések maximális száma. Tartomány=0... Ha egy kliens oldalakra bontott eredménymegjelenítést kér és már az itt megadott számú kinnlévő, oldalakra bontott eredménymegjelenítést kérő keresési kérés aktív, akkor a szerver a kliensnek "busy" visszatérési kódot ad vissza és semmilyen keresés vagy oldalra bontás nem történik.

Alapértelmezett érték

3

Szintaxis

Egész

Hossz

11

Számosság

Egyszeres

Használat

directoryOperation

Felhasználó által módosítható

Igen

Hozzáférési osztály

kritikus

Kötelező

Nem

Objektumosztály

ibm-slapdRdbmBackend

ibm-slapdPageSizeLmt

Leírás Oldalakra bontott eredménymegjelenítés esetén az egyszerre maximálisan visszaadott bejegyzések száma, függetlenül attól, hogy a kliens keresési kérésében milyen oldalméret lett megadva. Tartomány = 0... Ha a kliens megadta az oldalméretet, akkor a kliens által megadott érték és az ibmslapd.conf fájlból olvasott érték közül a kisebbiket használja a rendszer.

Alapértelmezett érték

50

Szintaxis

Egész

Hossz 11**Számosság**

Egyszeres

Használat

directoryOperation

Felhasználó által módosítható

Igen

Hozzáférési osztály

kritikus

Kötelező

Nem

Objektumosztály

ibm-slapdRdbmBackend

ibm-slapdPlugin

Leírás A bedolgozók dinamikusan betöltött könyvtárak, amelyek kiterjesztik a szerver képességeit. Az ibm-slapdPlugin attribútum adja meg a szerver számára, hogyan töltsön be és inicializáljon egy bedolgozó könyvtárat. A szintaxis:

```
keyword filename init_function [args...]
```

A szintaxis platformonként kicsit eltér a könyvtár elnevezési megállapodásai miatt.

A legtöbb bedolgozó elhagyható, de az RDBM célterület bedolgozóra szükség van minden RDBM célterület esetén.

Alapértelmezett érték

```
database /bin/libback-rdbm.dll rdbm_backend_init
```

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

2000

Érték Többértékű**ibm-slapdPort**

Leírás A nem SSL kapcsolatokhoz használt TCP/IP portot adja meg. Nem egyezhet meg az értéke az ibm-slapdSecurePort attribútuméval. (Az IP portok előjel nélküli, 16 bites egészek az 1 - 65535 tartományban.)

Alapértelmezett érték

389

Szintaxis

Egész

Maximális hossz

5

Érték Egyértékű

ibm-slapdPWEncryption

Leírás A felhasználói jelszavaknak a címtárban tárolás előtt használt kódolási mechanizmusát adja meg. A lehetséges értékek: none (nincs), imask, crypt vagy sha (az **sha** kulcsszó használata kötelező, ha SHA-1 kódolást akar használni). Ahhoz, hogy az SASL cram-md5 kapcsolódási típus sikeres legyen, az attribútumot "none" értékre kell állítani.

Alapértelmezett érték

none

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

5

Érték Egyértékű

ibm-slapdReadOnly

Leírás Ez az attribútum általában a Címtár célterületre vonatkozik. Azt adja meg, hogy a célterület írható-e. Értéke TRUE vagy FALSE lehet. Ha nincs megadva, alapértelmezett értéke FALSE. TRUE értékre állítva a szerver LDAP_UNWILLING_TO_PERFORM (0x35) kódot ad vissza minden olyan klienskérésre, amely módosítani kívánja egy readOnly adatbázis adatait.

Alapértelmezett érték

FALSE

Szintaxis

Logikai

Maximális hossz

5

Érték Egyértékű

ibm-slapdReferral

Leírás Az utalási LDAP URL-t adja meg, amelyet akkor ad vissza a rendszer, ha a helyi utótagok nem felelnek meg a kérésnek. Használható felettes utalásra is (vagyis ha az utótag egyáltalán nincs meg a szerver névkontextusában).

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

32700

Érték Többértékű

ibm-slapdReplDbConns

Leírás A replikáció által használt adatbázis-összeköttetések maximális száma.

Alapértelmezett érték

4

Szintaxis

Egész

Maximális hossz

11

Érték Egyértékű

ibm-slapdReplicaSubtree

Leírás A replikált részfa DN-je.

Szintaxis

DN

Maximális hossz

1000

Érték Egyértékű

ibm-slapdSchemaAdditions

Leírás Az ibm-slapdSchemaAdditions attribútum szolgál annak pontos megadására, melyik fájl is tartalmazza az új sémabejegyzéseket. Ez a fájl alapértelmezés szerint a /etc/V3.modifiedschema. Ha az attribútum nincsen megadva, akkor a szerver a legutóljára használt last ibm-slapdIncludeSchema fájlt használja, csakúgy, mint a korábbi kiadásokban.

A 3.2-es változat előtt az **slapd.conf** fájl legutolsó includeSchema bejegyzése adta meg azt a fájlt, amelybe a szerver az új sémabejegyzéseket írta, ha hozzáadási kérést kapott egy klienstől. Szokásos esetben az utolsó includeSchema a V3.modifiedschema fájl, amely egy üres fájl pontosan e célra.

Megjegyzés: A "modified" név félrevezető, ugyanis a fájl kizárólag új bejegyzéseket tartalmaz. A meglévő sémabejegyzések módosításai az eredeti fájlba íródnak.

Alapértelmezett érték

/etc/V3.modifiedschema

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

1024

Érték Egyértékű

ibm-slapdSchemaCheck

Leírás A hozzáadás/módosítás/törlés műveletek sémaellenőrzési mechanizmusát adja meg. Az értéke V2, V3 vagy V3_lenient lehet.

- V2 - v2 és v2.1 ellenőrzés megtartása. Áttérés során célszerű a használata.
- V3 - v3 ellenőrzés.
- V3_lenient - Nem minden szülő objektumosztály szükséges. Csak a közvetlen objektumosztályra van szükség a bejegyzés felvételéhez.

Alapértelmezett érték

V3_lenient

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

10

Érték Egyértékű**ibm-slapdSecurePort**

Leírás Az SSL kapcsolatokhoz használt TCP/IP portot adja meg. Nem egyezhet meg az értéke az ibm-slapdPort attribútuméval. (Az IP portok előjel nélküli, 16 bites egészek az 1 - 65535 tartományban.)

Alapértelmezett érték

636

Szintaxis

Egész

Maximális hossz

5

Érték Egyértékű**ibm-slapdSecurity**

Leírás SSL és TLS összeköttetések engedélyezése. None, SSL, SSLOnly, TLS vagy SSLTLS lehet.

- none - a szerver csak a nem biztonságos porton figyel.
- SSL - a szerver az SSL és a nem SSL porton egyaránt figyel. A biztonságos port a biztonságos kapcsolat használatának egyetlen eszköze.
- SSLOnly - A szerver csak az SSL porton figyel.
- TLS - A szerver csak a nem biztonságos porton figyel. A StartTSL kiterjesztett művelet a biztonságos kapcsolat használatának egyetlen eszköze.
- SSLTLS - A szerver mind az alapértelmezett, mind a biztonságos porton figyel. A StartTLS kiterjesztett művelet biztonságos kapcsolat elérésére szolgál az alapértelmezett porton, vagy arra, hogy a kliens közvetlenül használhassa a biztonságos portot. Egy StartTLS parancs elküldése a biztonságos porton a következő üzenetet eredményezi: LDAP_OPERATIONS_ERROR.

Alapértelmezett érték

none

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

7

Érték Egyértékű**ibm-slapdServerId**

Leírás A szervert megjelöli, mint replikációban részt vevő szervert.

Szintaxis

IA5 String szintaxis

Maximális hossz

240

Érték Egyértékű

ibm-slapdSetenv

Leírás A szerver induláskor lefuttatja a **putenv()** függvényt az **ibm-slapdSetenv** minden értékére a szerver futási környezetének módosítása érdekében. A parancsértelmező változói (például %PATH% vagy \$LANG) nem kerülnek feloldásra.

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

2000

Érték Többértékű

ibm-slapdSizeLimit

Leírás Az egyszerre maximálisan visszaadott bejegyzések száma, függetlenül attól, hogy a kliens keresési kérésében milyen oldalméret lett megadva. Tartomány = 0.... Ha a kliens megadott korlátot, akkor a rendszer a kliens által megadott érték és az **ibmslapd.conf** fájlból olvasott érték közül a kisebbiket használja. Ha a kliens nem adott meg korlátot és admin DN-nel kapcsolódott, akkor nincs korlátozás. Ha a kliens nem adott meg korlátot és nem admin DN-nel kapcsolódott, akkor a korlát az **ibmslapd.conf** fájlból olvasott érték. 0 = nincs korlát.

Alapértelmezett érték

500

Szintaxis

Egész

Maximális hossz

12

Érték Egyértékű

ibm-slapdSortKeyLimit

Leírás Egyetlen keresési kérésben megadható rendezési feltételek (kulcsok) maximális száma. Tartomány = 0.... Ha egy kliens a korlát által engedélyezettnél több rendezési kulcsot tartalmazó kérést adott ki és a rendezett keresés vezérlés kritikusság értéke FALSE, akkor a szerver az **ibmslapd.conf** fájlból kiolvasott értéket fogja használni és figyelmen kívül hagy minden olyan rendezési kulcsot, amelyet a korlát elérése után észlelt. A keresés és a rendezés végrehajtása megtörténik. Ha egy kliens a korlát által engedélyezettnél több rendezési kulcsot tartalmazó kérést adott ki és a rendezett keresés vezérlés kritikusság értéke TRUE, akkor a szerver **adminLimitExceeded** kódot ad vissza a kliensnek és sem keresés, sem rendezés nem kerül végrehajtásra.

Alapértelmezett érték

3

Szintaxis

cis

Hossz 11

Számosság

Egyszeres

Használat

directoryOperation

Felhasználó által módosítható

Igen

Hozzáférési osztály

kritikus

Objektumosztály

ibm-slapdRdbmBackend

Kötelező

Nem

ibm-slapdSortSrchAllowNonAdmin

Leírás Azt határozza meg, hogy a szerver engedi-e a nem adminisztrátori kapcsolódást, ha a keresési kérés rendezést ír elő. Ha az ibmslapd.conf fájlból olvasott érték FALSE, akkor a szerver csak az adminisztrátori jogosultsággal elküldött klienskéresekkel dolgozza fel. Ha egy kliens rendezett eredménymegjelenítést kér egy keresési műveletben, nem rendelkezik adminisztrátori jogosultsággal, és az attribútumnak az ibmslapd.conf fájlból olvasott értéke FALSE, akkor a szerver a kliensnek insufficientAccessRights visszatérési kódot ad vissza és semmilyen keresés vagy rendezés nem történik.

Alapértelmezett érték

FALSE

Szintaxis

Logikai

Hossz 5**Számosság**

Egyszeres

Használat

directoryOperation

Felhasználó által módosítható

Igen

Hozzáférési osztály

kritikus

Objektumosztály

ibm-slapdRdbmBackend

Kötelező

Nem

ibm-slapdSslAuth

Leírás Az SSL kapcsolat hitelesítési típusát adja meg (serverauth vagy serverclientauth).

- serverauth - szerver hitelesítés támogatása a kliensen. Ez az alapértelmezés.
- serverclientauth - szerver és kliens hitelesítés támogatása.

Alapértelmezett érték

serverauth

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

16

Érték Egyértékű**ibm-slapdSslCertificate**

Leírás Azt az azonosítót adja meg, amely azonosítja a szerver saját igazolását a kulcsadatbázis-fájlban. Az

azonosító akkor kerül megadásra, amikor a szerver magánkulcsát és igazolását létrehozza a **gsk4ikm** alkalmazással. Ha az `ibm-slapdSslCertificate` attribútum nincs megadva, akkor az LDAP szerver az SSL kapcsolatokhoz a kulcsadatbázisban megadott alapértelmezett magánkulcsot fogja használni.

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

128

Érték Egyértékű

ibm-slapdSslCipherSpec

A szerverhez hozzáférni kívánó kliensek SSL titkosítási módszerét adja meg. Az alábbi értékek egyike kell, hogy legyen:

7. táblázat: SSL titkosítási módszerek

Attribútum	Titkosítási szint
TripleDES-168	Triple DES titkosítás 168 bites kulccsal és SHA-1 MAC
DES-56	DES titkosítás 56 bites kulccsal és SHA-1 MAC
RC4-128-SHA	RC4 titkosítás 128 bites kulccsal és SHA-1 MAC
RC4-128-MD5	RC4 titkosítás 128 bites kulccsal és MD5 MAC
RC2-40-MD5	RC4 titkosítás 40 bites kulccsal és MD5 MAC
RC4-40-MD5	RC4 titkosítás 40 bites kulccsal és MD5 MAC
AES	AES titkosítás

Szintaxis

IA5 String

Maximális hossz

30

ibm-slapdSslKeyDatabase

Leírás Az LDAP szerver SSL kulcsadatbázis-fájljának elérési útja. Ezt a kulcsadatbázis fájlt használja a rendszer az LDAP kliensek SSL kapcsolatainak kezeléséhez, valamint biztonságos SSL kapcsolatok létrehozásához a replika LDAP szerverekkel.

Alapértelmezett érték

/etc/key.kdb

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

1024

Érték Egyértékű

ibm-slapdSslKeyDatabasePW

Leírás Az LDAP szerver SSL kulcsadatbázis-fájljához (`ibm-slapdSslKeyDatabase` attribútum) tartozó jelszót adja meg. Ha az LDAP szerver kulcsadatbázis-fájljához tartozik egy hozzárendelt jelszótároló fájl, akkor az `ibm-slapdSslKeyDatabasePW` paraméter elhagyható, vagy "none" értékre állítható.

Megjegyzés: A jelszótároló fájlnak ugyanabban a könyvtárban kell lennie, mint a kulcsadatbázis-fájlnak és a neve is meg kell, hogy egyezzen vele, csak a kiterjesztése .kdb helyett .sth.

Alapértelmezett érték

none

Szintaxis

Bináris

Maximális hossz

128

Érték Egyértékű

ibm-slapdSslKeyRingFile

Leírás Az LDAP szerver SSL kulcsadatbázis-fájljának elérési útja. Ezt a kulcsadatbázis fájlt használja a rendszer az LDAP kliensek SSL kapcsolatainak kezeléséhez, valamint biztonságos SSL kapcsolatok létrehozásához a replika LDAP szerverekkel.

Alapértelmezett érték

key.kdb

Szintaxis

IA5 String szintaxis

Maximális hossz

1024

Érték Egyértékű

ibm-slapdSuffix

Leírás A célterületen tárolandó névkontextus.

Megjegyzés: Ugyanaz a neve, mint az objektumosztálynak.

Alapértelmezett érték

Nincs előre beállított alapértelmezett érték.

Szintaxis

DN

Maximális hossz

1000

Érték Többértékű

ibm-slapdSupportedWebAdmVersion

Leírás Ez az attribútum adja meg a webes adminisztrációs eszköz legkorábbi változatát, amely képes kezelni ezt a cn=configuration szerveret.

Alapértelmezett érték

Szintaxis

Directory String

Maximális hossz

Érték Egyértékű

ibm-slapdSysLogLevel

Leírás Megadja, hogy a hibakeresési és működési statisztikák milyen részletességgel kerüljenek naplózásra az slapd.errors fájlban. Az értéke l, m vagy h lehet.

- h - magas (a legtöbb információ)
- m - közepes (ez az alapértelmezés)
- l - alacsony (a legkevesebb információ)

Alapértelmezett érték

m

Szintaxis

Directory string pontos egyezéssel

Maximális hossz

1

Érték Egyértékű

ibm-slapdTimeLimit

Leírás Az egy keresésen tölthető másodpercek maximális száma, függetlenül attól, hogy a kliens keresési kérésében milyen időkorlát lett megadva. Ha a kliens megadott korlátot, akkor a rendszer a kliens által megadott érték és az **ibmslapd.conf** fájlból olvasott érték közül a kisebbiket használja. Ha a kliens nem adott meg korlátot és admin DN-nel kapcsolódott, akkor nincs korlátozás. Ha a kliens nem adott meg korlátot és nem admin DN-nel kapcsolódott, akkor a korlát az **ibmslapd.conf** fájlból olvasott érték. 0 = nincs korlát.

Alapértelmezett érték

900

Szintaxis

Egész

Maximális hossz

Érték Egyértékű

ibm-slapdTransactionEnable

Leírás Ha a tranzakciós bedolgozó be van töltve, de az ibm-slapdTransactionEnable attribútum értéke FALSE, akkor a szerver visszautasít minden StartTransaction kérést LDAP_UNWILLING_TO_PERFORM visszatérési kóddal.

Alapértelmezett érték

TRUE

Szintaxis

Logikai

Maximális hossz

5

Érték Egyértékű

ibm-slapdUseProcessIdPw

Leírás Ha az attribútum értéke TRUE, akkor a szerver figyelmen kívül hagyja az ibm-slapdDbUserID és az ibm-slapdDbUserPW attribútumok értékét és a saját hitelesítési adatait használja a DB2 adatbázishoz hitelesítésre.

Alapértelmezett érték

FALSE

Szintaxis

Logikai

Maximális hossz

5

Érték Egyértékű**ibm-slapdVersion****Leírás** Az IBM Slapd verziószáma.**Alapértelmezett érték****Szintaxis**

IA5 String szintaxis

Maximális hossz**Érték** Egyértékű**ibm-slapdWriteTimeout****Leírás** Megadja a blokkolt írások időkorlát-értékét másodpercben. Ha az időkorlát meghaladásra kerül, akkor a kapcsolat törlődik.**Alapértelmezett érték**

120

Szintaxis

Egész

Maximális hossz

1024

Érték Egyértékű**objectClass****Leírás** Az objectClass (objektumosztály) attribútum értéke adja meg, hogy a bejegyzés milyen típusú objektum.**Szintaxis**

Directory string

Maximális hossz

128

Érték Többértékű

Objektumazonosítók (OID)

A Directory Server az alábbi táblázatokban látható objektumazonosítókat használja. Ezek az OID-k a root DSE-ben találhatóak. A root DSE bejegyzés információkat tartalmaz magáról a szerverről.

Vezérlőelemek*8. táblázat: Támogatott Directory Server vezérlőelemek*

Név	OID	Legkorábbi, i5/OS vagy OS/400 kiadás	Legkorábbi IBM Directory Server verzió	Leírás
DSA IT kezelése	2.16.840.1.1137.30.3.4.2	V4R5	V3.2	A hivatkozott bejegyzések normál bejegyzéseként kezelése.

8. táblázat: Támogatott Directory Server vezérlőelemek (Folytatás)

Név	OID	Legkorábbi, i5/OS vagy OS/400 kiadás	Legkorábbi IBM Directory Server verzió	Leírás
“Tranzakciók” oldalszám: 46	1.3.18.0.2.10.5	V4R5	V3.2	Egy művelet egy tranzakció részeként megjelölése.
os400-dltusrprf-ownobjopt	1.3.18.0.2.10.8	V5R2		Felhasználói profil törlése lehetőség az objektum tulajdonosa számára. További részletek: “Operációs rendszer leképzett háttér objektumai” oldalszám: 75.
os400-dltusrprf-pgpopt	1.3.18.0.2.10.9	V5R2		Felhasználói profil beállítások törlése az elsődleges csoportból. További részletek: “Operációs rendszer leképzett háttér objektumai” oldalszám: 75.
Rendezett keresés	1.2.840.113556.1.4.473 (kérés) és 1.2.840.113556.1.4.474 (válasz)	V5R2 PTF-fel	V4.1	A keresési eredmények rendezése a kliensnek visszaadás előtt. Részletek: “Keresési paraméterek” oldalszám: 43.
Oldalakra bontott keresés	1.2.840.113556.1.4.319	V5R2 PTF-fel	V4.1	A keresési eredmények oldalakra bontva visszaadása (nem egyben). Részletek: “Keresési paraméterek” oldalszám: 43.
Fa törlése vezérlőelem	1.2.840.113556.1.4.805	V5R3	V5.1	Ez a vezérlőelem egy Törlés kéréshez csatolható és azt jelzi, hogy a megadott bejegyzéssel annak összes leszármazott bejegyzése is törlésre kerüljön. A felhasználó csak a címtáradminisztrátor lehet. A törlendő bejegyzés nem lehet replikációs kontextus.
“Jelszó-irányelvek” oldalszám: 68	1.3.6.1.4.1.42.2.27.8.5.1	V5R3	V5.1	Extra jelszó irányelv információk visszaadása a kliens számára.

8. táblázat: Támogatott Directory Server vezérlőelemek (Folytatás)

Név	OID	Legkorábbi, i5/OS vagy OS/400 kiadás	Legkorábbi IBM Directory Server verzió	Leírás
Szerveradminisztráció	1.3.18.0.2.10.15	V5R3	V5.1	Lehetővé teszi az adminisztrátor számára normális esetben visszautasított javítási műveletek végrehajtását (például: csak olvasható replika frissítése, egy zárolt szerver frissítése, vagy bizonyos műveleti attribútumok beállítása).
“Proxy hitelesítés” oldalszám: 55	2.16.840.1.113730.3.4.18	V5R4	V5.2	A klienskalkalmazás egy másik címtárhoz kapcsolódhat saját azonosságának felhasználásával, de lehetősége van arra, hogy egy másik felhasználó nevében műveleteket hajtson végre.
Replikációellátó kapcsolat vezérlőelem	1.3.18.0.2.10.18	V5R3	V5.2	Ezt a vezérlőelemet az ellátó adhatja hozzá, ha az ellátó átjárószerver.

Kiterjesztett műveletek

9. táblázat: Objektumazonosítók kiterjesztett műveletekhez

Név	OID	Legkorábbi i5/OS vagy OS/400 kiadás	Legkorábbi IBM Directory Server verzió	Leírás
Események regisztrálása	1.3.18.0.2.12.1	V4R5	V3.2	Kérésbejegyzés a SecureWay V3.2 Event Support eseményeire vonatkozólag
Események regisztrálásának megszüntetése	1.3.18.0.2.12.3	V4R5	V3.2	Megszünteti az eseményregisztrációs kérések használatával bejegyzett kérések regisztrációját.
Tranzakció kezdete	1.3.18.0.2.12.5	V4R5	V3.2	Elindít egy tranzakciós kontextust a SecureWay V3.2 termékhez
Tranzakció befejezése	1.3.18.0.2.12.6	V4R5	V3.2	Befejez egy tranzakciós kontextust (véglegesítés/visszagörgetés) a SecureWay V3.2 termékhez
DN normalizálási kérés	1.3.18.0.2.12.30	V5R3	V5.1	Kéri egy DN vagy DN-ek egy sorozatának normalizálását.
StartTLS	1.3.6.1.4.1.1466.20037	V5R4	V5.2	Kéri a TLS elindítását.

További kiterjesztett műveletek is léteznek, amelyeket nem kliensekről lehet kezdeményezni. Ezeket a műveleteket az ldapexop segédprogram használja, illetve a webes adminisztrációs eszköz különféle műveletei. A műveletek és az indításukhoz szükséges jogosultságokat az alábbiakban felsoroljuk:

10. táblázat: További kiterjesztett műveletek

Név	OID	Legkorábbi i5/OS kiadás	Legkorábbi IBM Directory Server verzió	Leírás
Replikáció vezérlése	1.3.18.0.2.12.16	V5R3	V5.1	Ez a művelet elvégzi a kért tevékenységet a megadott szerveren, majd a hívást továbbítja az összes, a replikációs topológiában alatta található fogyasztó felé. A kliens vagy a címtáradminisztrátor kell, hogy legyen, vagy legalább írási joggal kell, hogy rendelkezzen a megadott replikációs kontextus <code>ibm-replicagroup=default</code> objektumához.
Replikációs sor vezérlése	1.3.18.0.2.12.17	V5R3	V5.1	Ez a művelet egy adott megállapodásra vonatkozóan már replikált állapotúnak jelzi a megadott elemeket. Ez a művelet csak akkor használható, ha a kliens írási jogosultsággal rendelkezik a replikációs megállapodáshoz.
Zárolás és feloldása	1.3.18.0.2.12.19	V5R3	V5.1	Ez a művelet a részfat egy olyan állapotba hozza, amelyben nem fogad további klienskéréseket (illetve megszünteti ezt az állapotot); pontosabban csak olyan kéréseket, amelyek a címtáradminisztrátorként bejelentkezett kientől származnak és a szerveradminisztráció vezérlőelem megtalálható benne. A kliens vagy a címtáradminisztrátor kell, hogy legyen, vagy legalább írási joggal kell, hogy rendelkezzen a megadott replikációs kontextus <code>ibm-replicagroup=default</code> objektumához.
Lépcsőzetes vezérlőelem-replikáció	1.3.18.0.2.12.15	V5R3	V5.1	Ez a művelet elvégzi a kért tevékenységet a megadott szerveren, majd a hívást továbbítja az összes, a replikációs topológiában alatta található fogyasztó felé. A kliens vagy a címtáradminisztrátor kell, hogy legyen, vagy legalább írási joggal kell, hogy rendelkezzen a megadott replikációs kontextus <code>ibm-replicagroup=default</code> objektumához.
Konfiguráció frissítése	1.3.18.0.2.12.28	V5R3	V5.1	E művelet hatására a szerver újraolvassa a megadott beállításokat a konfigurációs állományból. A műveletet csak a címtáradminisztrátorként bejelentkezett kliens hajthatja végre.
Kapcsolatfelbontási kérés	1.3.18.0.2.12.35	V5R4	V5.2	Kéri a kapcsolatok felbontását a szerveren.
Egyedi attribútumkérés	1.3.18.0.2.12.44	V5R4	V5.2	Kéri a szervertől, hogy adja vissza az összes nem egyedi érték listáját egy adott attribútumnévhez. Lásd: "Idapexop" oldalszám: 198 -op uniqueattr.

10. táblázat: További kiterjesztett műveletek (Folytatás)

Név	OID	Legkorábbi i5/OS kiadás	Legkorábbi IBM Directory Server verzió	Leírás
Attribútumtípus-kérés	1.3.18.0.2.12.46	V5R4	V5.2	Kéri a szervertől, hogy adja vissza az adott jellemzőkkel rendelkező attribútumok listáját. Lásd: "ldapexop" oldalszám: 198 -op getattributes
Szervernyomkövetés felügyelete	1.3.18.0.2.12.40	V5R3	V5.2	Aktiválja vagy deaktiválja a nyomkövetést az IBM Directory Serverben.
Felhasználótípus-kérés	1.3.18.0.2.12.37	V5R3	V5.2	Kérés a kapcsolat felhasználó felhasználótípusának bekérésére

Támogatott és engedélyezett funkciók

A következő tábla a támogatott és engedélyezett funkciók objektumazonosítóját mutatja. Ezek használatával ellenőrizheti, hogy egy adott szerver támogatja-e ezeket a funkciókat.

11. táblázat: A támogatott és engedélyezett funkciók objektumazonosítója

Név	OID	Leírás
Kibővített replikációs modell	1.3.18.0.2.32.1	Azonosítja az IBM Directory Server v5.1-ben bemutatott replikációs modellt, beleértve a részfák és a lépcsőzetes replikáció használatát is.
Bejegyzés ellenőrző összeg	1.3.18.0.2.32.2	Jelzi, hogy a szerver támogatja az ibm-entrychecksum és ibm-entrychecksumop funkciókat.
Bejegyzés UUID	1.3.18.0.2.32.3	Jelzi, hogy a szerver támogatja az ibm-entryuuid műveleti attribútum használatát.
Szűrő ACL-elk	1.3.18.0.2.32.4	Jelzi, hogy a szerver támogatja az IBM Filter ACL modellt
Jelszó-irányelv	1.3.18.0.2.32.5	Jelzi, hogy a szerver támogatja a jelszó-irányelvek használatát.
Rendezés DN szerint	1.3.18.0.2.32.6	Jelzi, hogy a szerver támogatja az ibm-slapdDn használatát a DN szerinti rendezés érdekében.
Adminisztrációs csoport delegáció	1.3.18.0.2.32.8	A szerver támogatja a szerveradminisztráció delegálását egy adminisztrátori csoportnak, amely a konfigurációs háttérben került megadásra.
Szolgáltatásbénítási támadások kivédése	1.3.18.0.2.32.9	A szerver támogatja a szolgáltatásbénítási támadások ellen védő funkciót, beleértve az írás/olvasási időkorlátokat és a vészszállak használatát.
Bejegyzések és részfák dinamikus frissítése	1.3.18.0.2.32.15	A szerver támogatja a bejegyzések és részfák dinamikus konfigurációs frissítését.
Álnév hivatkozás-feloldási beállítás	1.3.18.0.2.32.10	A szerver támogat egy beállítást, hogy az álnevek nem kerüljenek alapértelmezésben feloldásra.
Csoportspecifikus keresési korlátok	1.3.18.0.2.32.17	A csoportspecifikus keresési korlátok támogatják az embercsoportok kibővített keresési korlátait
Dinamikus nyomkövetés	1.3.18.0.2.32.14	A szerver támogatja a szerver aktív nyomkövetését egy kiterjesztett LDAP művelet használatával.
TLS funkciók	1.3.18.0.2.32.28	Megadja, hogy a szerver jelenleg képes a TSL használatára
Admin démon felülvizsgálat	1.3.18.0.2.32.11	A szerver támogatja az admin démon felülvizsgálatát.

11. táblázat: A támogatott és engedélyezett funkciók objektumazonosítója (Folytatás)

Név	OID	Leírás
Kerberos funkciók	1.3.18.0.2.32.30	Megadja, hogy a szerver jelenleg képes a Kerberos használatára
Nem blokkoló replikáció	1.3.18.0.2.32.29	Az ellátó nem próbálja állandóan újraküldeni a frissítéseket, ha a fogyasztó hibát ad vissza.
ibm-allMembers és ibm-allGroups műveleti attribútumok	1.3.18.0.2.32.31	A háttér támogatja a statikus, dinamikus és beágyazott csoportkeresést az ibm-allMembers és ibm-allGroups műveleti attribútumok használatával. A statikus, dinamikus és/vagy beágyazott csoport tagjai lekérdezhetőek az ibm-allMembers műveleti attribútumon végrehajtott kereséssel. A statikus, dinamikus és/vagy beágyazott csoportok, amelyekhez a tag DN tartozik, lekérdezhetőek egy keresés végrehajtásával az ibm-allGroups műveleti attribútumon végrehajtott kereséssel.
Globálisan egyedi attribútumok	1.3.18.0.2.32.16	A szerver rendelkezik a globálisan egyedi attribútumok kikényszerítésének képességével.
Képernyő műveletszámlálók	1.3.18.0.2.32.24	A szerver képernyő műveletszámlálókat kínál az elkezdett és befejezett művelettípusokhoz.
Képernyő naplózási számláló	1.3.18.0.2.32.20	A szerver képernyő naplózási számlálókat kínál a szerver-, CLI- és felülvizsgálati naplófájlokhoz hozzáadott üzenetekhez.
Képernyő kapcsolattípus-számláló	1.3.18.0.2.32.22	A szerver képernyő kapcsolattípus-számlálókat kínál az SSL és TLS kapcsolatokhoz.
Képernyő aktív dolgozók információ	1.3.18.0.2.32.21	A szerver képernyő-információkat kínál az aktív dolgozókról (cn=workers,cn=monitor).
Képernyő kapcsolati információk	1.3.18.0.2.32.23	A szerver képernyő-információkat kínál a kapcsolatokról IP-cím szerint, nem pedig kapcsolatazonosító szerint ID (cn=connections, cn=monitor).
Képernyő nyomkövetési információk	1.3.18.0.2.32.25	A szerver képernyő-információkat kínál a jelenleg használt nyomkövetési beállításokról.
Attribútum-gyorsítótár keresési szűrő feloldás	1.3.18.0.2.32.13	A szerver támogatja az attribútum-gyorsítótár használatát a keresési szűrők feloldásához.
Proxy hitelesítés	1.3.18.0.2.32.27	A szerver támogatja a proxy hitelesítést a felhasználói csoportokhoz.
Nyelvi címke lehetőség támogatása	1.3.6.1.4.1.4203.1.5.4	Jelzi, hogy a szerver támogatja a nyelvi címkék használatát az RFC 2596 szabványban meghatározottak szerint.
Változásnapló bejegyzések maximális kora	1.3.18.0.2.32.19	Megadja, hogy a szerver képes a változásnapló bejegyzések megtartására a koruk alapján.
IBMpoliciés replikációs részfa	1.3.18.0.2.32.18	A szerver támogatja a cn=IBMpoliciés részfa replikációját.
NULL alapú részfa keresés	1.3.18.0.2.32.26	A szerver megengedi a null alapú részfa-keresést, amely a szerveren megadott teljes DIT-ben keres.
Önálló attribútum-gyorsítótárazás	1.3.18.0.2.32.50	A szerver támogatja az önálló attribútum-gyorsítótárazást.
ibm-entrychecksumop	1.3.18.0.2.32.56	6.0 IDS ibm-entrychecksumop funkcionalitás

ACL mechanizmusok objektumazonosítói

| A következő táblában az ACL mechanizmusok objektumazonosítói láthatók.

| *12. táblázat: ACL mechanizmusok objektumazonosítói*

Név	OID	Leírás
IBM SecureWay V3.2 ACL modell	1.3.18.0.2.26.2	Jelzi, hogy az LDAP szerver támogatja az IBM SecureWay V3.2 ACL modell használatát
IBM Filter Based ACL mechanizmus	1.3.18.0.2.26.3	Jelzi, hogy az LDAP szerver támogatja az IBM Directory Server v5.1 szűrő alapú ACL-ek használatát
Rendszer és korlátozott ACL-támogatás	1.3.18.0.2.26.4	Jelzi, hogy a szerver támogatja a rendszer és a korlátozott hozzáférési osztályt az ACL bejegyzésekben

9. fejezet A Directory Server hibaelhárítása

Sajnos, még az olyan megbízható szerverekkel, mint amilyen a Directory Server, alkalmanként problémák adódhatnak. Ha problémák vannak a Directory Server-rel, az alábbi információk segíthetnek a hiba okának kiderítésében és a hiba kiküszöbölésében.

Az LDAP hibák visszaadott hibakódjai az ldap.h fájlban található, amely a rendszer QSYSINC/H.LDAP könyvtárban helyezkedik el.

“Hibafigyelés és hozzáférés követés a Directory Server feladatnapló segítségével” oldalszám: 270

Ha a Directory Server-en hiba fordul elő, és részletesebb tájékoztatást akar, egy másik lehetőség a QDIRSRV feladatnapló megtekintése.

“Hibakeresés TRCTCPAPP segítségével” oldalszám: 270

Reprodukálható hibák esetén a Trace TCP/IP Application (TRCTCPAPP APP(*DIRSRV)) parancs segítségével futtathatja a hibák nyomkövetését.

“Hibák nyomkövetése az LDAP_OPT_DEBUG kapcsolóval” oldalszám: 271

Az LDAP C API-kat használó kliensek problémáinak keresése.

“Általános LDAP klienshibák” oldalszám: 274


Az általános LDAP kliens hibák ismerete segít a szerverrel kapcsolatos problémák megoldásában.

“Jelszóirányelvekkel kapcsolatos hibák” oldalszám: 276

Egy jelszó-irányelv engedélyezése néha váratlan hibákhoz vezethet.

“A QGLDCPYVL API hibaelhárítása” oldalszám: 276

A Felhasználói nyomkövetés szolgáltatás használata megmagyarázhatja a hibát, illetve eldöntheti, ha segítségre van szükség.

Az általános Directory Server problémákról további információkat kaphat a Directory Server honlapon  (www.iseries.ibm.com/ldap).

A Directory Server több SQL (Structured Query Language, strukturált lekérdezési nyelvi) szervert használ, amelyek iSeries QSQRVR jobok. 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 mely SQL szerverjebeket indítja el a szerver, tudni, hogy mely QSQRVR munkanaplókban kell keresni a további hibákat.

Amikor a Directory Server szabályosan indul el, az alábbihoz hasonló üzenetet generál.

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

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

Az üzenetek a szerver számára elindított QSQRVR jobokra vonatkoznak. Az üzenetek száma eltérhet a szerver konfigurációjától és a szerver indításához szükséges QSQRVR jobok számától.

Az iSeries navigátorban a címtárszerver **Adatbázis/utótagok** tulajdonságlapján megadhatja az SQL szerverek maximális számát, amelyeket a Directory Server a címtárműveletekhez használ a szerver elindítása után. A replikációhoz további SQL szerverek indulnak el.

Hibafigyelés és hozzáférés követés a Directory Server feladatnapló segítségével

A Directory Server munkanaplójának megtekintése hibákra hívhatja fel a figyelmet, és segít nyomon követni a szerver elérését. A munkanapló tartalma:

- A szerver működésével és a szerver problémáival (például az SQL szerverjobokkal vagy replikációs hibákkal) kapcsolatos üzenetek.
- A biztonsággal kapcsolatos, a kliensek működésére (például helytelen jelszavakra) vonatkozó üzenetek.
- Üzenetek a klienshibák (például hiányzó attribútumok) részleteiről.

Nem biztos, hogy szükség van a klienshibák naplózására, csak akkor, ha kliensproblémákat próbál megoldani. A klienshibák naplózása az iSeries navigátorban, a Directory Server **Általános** oldalán szabályozható.

Ha a szerver már elindult, az alábbi lépéseket követve tekintheti meg a QDIRSRV munkanaplót:

1. Az iSeries navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** pontra.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Szerver feladatok** menüpontot.
5. A **Fájl** menüből válassza a **Munkanapló** elemet.

Ha a szerver még nem indult el, kövesse az alábbi lépéseket a QDIRSRV feladatnapló megtekintéséhez:

1. Az iSeries navigátorban nyissa meg az **Alapműveletek** kategóriát.
2. Kattintson a **Nyomtatókimenet** lehetőségre.
3. A QDIRSRV a **Felhasználó** oszlopban jelenik meg az iSeries navigátor jobboldali keretén belül. A munkanapló megtekintéséhez kattintson duplán a **Qpjoblog** elemre ugyanabban a sorban, a QDIRSRV-től balra.

Megjegyzés: Lehetséges, hogy az iSeries navigátor pillanatnyi beállítása csak a spoolfájlokat mutatja meg. Ha a QDIRSRV nem jelenik meg a listán, kattintson a **nyomtatókimenet** elemre, majd válassza ki a **Beállítások** menü **Tartalmaz** elemét. Válassza ki az **Összes** értéket az **Felhasználó** mezőben, majd kattintson az **OK** gombra.

Megjegyzés: A Directory Server egyes feladatok végrehajtásához más rendszererőforrásokat is igénybe vesz. Ha ezen erőforrásokkal kapcsolatban fordul elő hiba, a munkanapló jelzi, hova lehet információért fordulni. Néhány esetben a Directory Server nem képes meghatározni a hiba forrását. Ilyenkor tekintse meg az SQL (Structured Query Language) szerver munkanaplóját, 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) csatolója. Az átlagos felhasználó nem feltétlenül érti meg a nyomkövetési adatok teljes tartalmát. A nyomkövetési bejegyzések segítségével azonban meghatározható, hogy az adatsere két pont között valóban megtörtént-e.

A Directory Server használhatja a Trace TCP/IP Application (TRCTCPAPP) parancsot *DIRSRV paraméterrel a kliensekkel vagy az alkalmazásokkal kapcsolatos problémák megtalálásához.

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

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

Hibák nyomkövetése az LDAP_OPT_DEBUG kapcsolóval

Az `ldap_set_option()` API program LDAP_OPT_DEBUG paramétere segítségével nyomon követheti az LDAP C API-kat használó kliensekkel kapcsolatos problémákat. A hibakeresési beállítás 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 kliensalkalmazást 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 kliensjob száma.

Az információ párbeszédés megjelenítéséhez írja be az iSeries parancssorba:

```
DSPPFM QAP0ZDMP QP0Znnnnnn
```

ahol `QAP0ZDMP` egy nullát tartalmaz és `nnnnnn` a job száma.

Az információk elmentése és elküldése a szerviznek:

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

```
SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
```

ahol `QAP0ZDMP` egy nullát tartalmaz és `xxx` az SAVF fájl megadott neve.

GLEnnnn üzenetazonosítók

| Az üzenetazonosítók a GLEnnnn formát használják, ahol az nnnn a decimális hibaszám. Az 50-es (0x32) visszatérési kód részletes leírása például a következő parancs kiadásával érhető el:

| DSPMSGD MSGID(GLE0050) MSGF(QGLDMSG)

| Ez megadja az LDAP_INSUFFICIENT_ACCESS leírását.

A következő tábla a GLE üzenetazonosítókat és leírásukat tartalmazza:

Üzenetazonosító	Leírás
GLE0000	A kérés sikeres volt (LDAP_SUCCESS)
GLE0001	Műveleti hiba (LDAP_OPERATIONS_ERROR)
GLE0002	Protokollhiba (LDAP_PROTOCOL_ERROR)
GLE0003	Időkorlát túllépése (LDAP_TIMELIMIT_EXCEEDED)
GLE0004	Méretkorlát túllépése (LDAP_SIZELIMIT_EXCEEDED)
GLE0005	Az összehasonlított típus és érték nem létezik a bejegyzésben (LDAP_COMPARE_FALSE)
GLE0006	Az összehasonlított típus és érték létezik a bejegyzésben (LDAP_COMPARE_TRUE)
GLE0007	Nem támogatott hitelesítési eljárás (LDAP_AUTH_METHOD_NOT_SUPPORTED)
GLE0008	Erős hitelesítésre van szükség (LDAP_STRONG_AUTH_REQUIRED)
GLE0009	Részleges eredmények és utalás érkezett (LDAP_PARTIAL_RESULTS)
GLE0010	Visszaadott utalás (LDAP_REFERRAL)
GLE0011	Adminisztrációs korlát meghaladva (LDAP_ADMIN_LIMIT_EXCEEDED)
GLE0012	Kritikus kiterjesztés nem támogatott (LDAP_UNAVAILABLE_CRITICAL_EXTENSION)
GLE0013	Bizalmasság kötelező (LDAP_CONFIDENTIALITY_REQUIRED)
GLE0014	SASL kapcsolat folyamatban (LDAP_SASL_BIND_IN_PROGRESS)
GLE0016	Nincs ilyen attribútum (LDAP_NO_SUCH_ATTRIBUTE)
GLE0017	Nem definiált attribútumtípus (LDAP_UNDEFINED_TYPE)
GLE0018	Nem megfelelő egyezés (LDAP_INAPPROPRIATE_MATCHING)
GLE0019	Korlátsértés (LDAP_CONSTRAINT_VIOLATION)
GLE0020	Típus vagy érték létezik (LDAP_TYPE_OR_VALUE_EXISTS)
GLE0021	Érvénytelen szintaxis (LDAP_INVALID_SYNTAX)
GLE0032	Nincs ilyen objektum (LDAP_NO_SUCH_OBJECT)
GLE0033	Álnévprobléma (LDAP_ALIAS_PROBLEM)
GLE0034	Érvénytelen DN szintaxis (LDAP_INVALID_DN_SYNTAX)
GLE0035	Az objektum levélobjektum (LDAP_IS_LEAF)
GLE0036	Álnév hivatkozás-feloldási probléma (LDAP_ALIAS_DEREF_PROBLEM)
GLE0048	Nem megfelelő hitelesítés (LDAP_INAPPROPRIATE_AUTH)
GLE0049	Érvénytelen hitelesítési adatok (LDAP_INVALID_CREDENTIALS)
GLE0050	Érvénytelen hozzáférés (LDAP_INSUFFICIENT_ACCESS)
GLE0051	A cím társzerver túlterhelt (LDAP_BUSY)
GLE0052	Cím társzolgáltatási ügynök nem elérhető (LDAP_UNAVAILABLE)

Üzenetazonosító	Leírás
GLE0053	A címtárszerver képtelen a kért művelet végrehajtására (LDAP_UNWILLING_TO_PERFORM)
GLE0054	A rendszer hurkot észlelt (LDAP_LOOP_DETECT)
LE0064	Elnevezésmegsértés (LDAP_NAMING_VIOLATION)
LE0065	Objektumosztálysértés (LDAP_OBJECT_CLASS_VIOLATION)
GLE0066	A művelet nem engedélyezett nem levél objektumon (LDAP_NOT_ALLOWED_ON_NONLEAF)
GLE0067	A művelet nem engedélyezett relatív megkülönböztetett név objektumon (LDAP_NOT_ALLOWED_ON_RDN)
GLE0068	Már létezik (LDAP_ALREADY_EXISTS)
GLE0069	Nem módosíthatja az objektumosztályt (LDAP_NO_OBJECT_CLASS_MODS)
GLE0070	Az eredmény túl nagy (LDAP_RESULTS_TOO_LARGE)
GLE0071	Több szervert is érint. (LDAP_AFFECTS_MULTIPLE_DSAS)
GLE0080	Ismeretlen hiba (LDAP_OTHER)
GLE0081	Nem lehetséges a kapcsolódás az LDAP szerverhez (LDAP_SERVER_DOWN)
GLE0082	Helyi hiba (LDAP_LOCAL_ERROR)
GLE0083	Kódolási hiba (LDAP_ENCODING_ERROR)
GLE0084	Visszafejtési hiba (LDAP_DECODING_ERROR)
GLE0085	A kérés túllépte az időkorlátot (LDAP_TIMEOUT)
GLE0086	Ismeretlen hitelesítési metódus (LDAP_AUTH_UNKNOWN)
GLE0087	Rossz keresési szűrő (LDAP_FILTER_ERROR)
GLE0088	A felhasználó félbeszakította a műveletet (LDAP_USER_CANCELLED)
GLE0089	Rossz paraméter egy LDAP rutin számára (LDAP_PARAM_ERROR)
GLE0090	Elfogyott a memória (LDAP_NO_MEMORY)
GLE0091	Kapcsolati hiba (LDAP_CONNECT_ERROR)
GLE0092	A funkció nem támogatott (LDAP_NOT_SUPPORTED)
GLE0093	A vezérlőelem nem található (LDAP_CONTROL_NOT_FOUND)
GLE0094	Nincs visszaadott eredmény (LDAP_NO_RESULTS_RETURNED)
GLE0095	Több eredmény került visszaadásra (LDAP_MORE_RESULTS_TO_RETURN)
GLE0096	Nem LDAP URL (LDAP_URL_ERR_NOTLDAP)
GLE0097	Az URL-cím nem rendelkezik megkülönböztetett névvel (LDAP_URL_ERR_NODN)
GLE0098	Az URL-cím hatókör értéke érvénytelen (LDAP_URL_ERR_BADSCOPE)
GLE0099	Memórialefoglalási hiba (LDAP_URL_ERR_MEM)
GLE0100	Kliens hurok (LDAP_CLIENT_LOOP)

Üzenetazonosító	Leírás
GLE0101	Utalási limit meghaladva (LDAP_REFERRAL_LIMIT_EXCEEDED)
GLE0112	Az SSL környezet már inicializálva van (LDAP_SSL_ALREADY_INITIALIZED)
GLE0113	Az inicializálási hívás sikertelen volt (LDAP_SSL_INITIALIZE_FAILED)
GLE0114	Az SSL környezet nincs inicializálva (LDAP_SSL_CLIENT_INIT_NOT_CALLED)
GLE0115	Illegális SSL paraméterértékek kerültek meghatározásra (LDAP_SSL_PARAM_ERROR)
GLE0116	Nem sikerült a biztonságos kapcsolat egyeztetése (LDAP_SSL_HANDSHAKE_FAILED)
GLE0118	Az SSL könyvtár nem található meg (LDAP_SSL_NOT_AVAILABLE)
GLE0128	Nem található explicit tulajdonos (LDAP_NO_EXPLICIT_OWNER)
GLE0129	A kívánt erőforrás nem zárolható (LDAP_NO_LOCK)
GLE0133	Nincsenek LDAP szerverek a DNS-ben (LDAP_DNS_NO_SERVERS)
GLE0134	Csonkolt DNS eredmények (LDAP_DNS_TRUNCATED)
GLE0135	A DNS adatok nem értelmezhetők (LDAP_DNS_INVALID_DATA)
GLE0136	A rendszertartomány vagy a névszerver nem oldható fel (LDAP_DNS_RESOLVE_ERROR)
GLE0137	DNS konfigurációs fájl hiba (LDAP_DNS_CONF_FILE_ERROR)
GLE0160	Kimeneti puffer túlsordulás (LDAP_XLATE_E2BIG)
GLE0161	Bemeneti puffer csonkolt (LDAP_XLATE_EINVAL)
GLE0162	Használhatatlan bemeneti karakter (LDAP_XLATE_EILSEQ)
GLE0163	A karakter nem képezhető le egy kódkészlet pontra (LDAP_XLATE_NO_ENTRY)

Általános LDAP klienshibák

Az általános LDAP kliens hibák ismerete segít a szerverrel kapcsolatos problémák megoldásában. Az LDAP kliens hibaállapotairól teljes listát az iSeries Információs központ Programozás című fejezetének “Directory Server API-k” témakörében talál.

A kliens hibaüzenetek az alábbi formátumban jelennek meg:

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

Megjegyzés: A hibák magyarázata feltételezi, hogy a kliens i5/OS 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)” oldalszám: 275
- “[Hibás LDAP művelet]: Operations error (Műveleti hiba)” oldalszám: 275

- “ldap_bind: No such object (Nem létező objektum)”
- “ldap_bind: Inappropriate authentication (Nem megfelelő hitelesítés)”
- “[Hibás LDAP művelet]: Insufficient access (Nem elegendő elérés)”
- “[Hibás LDAP művelet]: Nem lehet az LDAP szerverhez kapcsolódni”
- “[Hibás LDAP művelet]: Meghiúsult az SSL szerverhez a kapcsolat” oldalszám: 276

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 a Directory Server keresési idejét. Ezzel kapcsolatos további információk: “Teljesítménnyel kapcsolatos beállítások módosítása” oldalszám: 128.
- Csökkentse a rendszer tevékenységét. Az éppen futó aktív LDAP kliensjombok számát is csökkentheti.

[Hibás LDAP művelet]: Operations error (Műveleti hiba)

Több körülmény is okozhatja ezt a hibát. Adott feltételek mellett a hiba okáról információt kaphat, ha megtekinti az QDIRSRV munkanaplóját (részletek: “Hibafigyelés és hozzáférés követés a Directory Server feladatnapló segítségével” oldalszám: 270) és az SQL (strukturált lekérdezési nyelv) szerver feladatnaplóját (részletek: 9. fejezet, “A Directory Server hibaelhárítása”, oldalszám: 269).

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 kísérel meg összekapcsolódni. Ez gyakran előfordul, amikor a felhasználó tévesen azt gondolja, hogy ő DN adminisztrátor. Például a felhasználó megadhatja a QSECOFR vagy Administrator értéket, pedig az adminisztrátor tényleges DN-je cn=Administrator vagy hasonló érték.

A hibáról további részleteket a QDIRSRV feladatnaplóban talál. Részletek: “Hibafigyelés és hozzáférés követés a Directory Server feladatnapló segítségével” oldalszám: 270.

ldap_bind: Inappropriate authentication (Nem megfelelő hitelesítés)

A szerver Érvénytelen hitelesítési adatok üzenetet adott vissza, mert a jelszó vagy a kapcsolódási DN helytelen. A szerver Nem megfelelő hitelesítés üzenetet küld vissza, ha a kliens a következő módokon kísérel meg kapcsolódni:

- A bejegyzés nem rendelkezik userpassword attribútummal
- Az i5/OS felhasználót képviselő bejegyzés rendelkezik UID attribútummal, de nem rendelkezik userpassword attribútummal. Ez összehasonlítást eredményez a megadott jelszó és az i5/OS felhasználói jelszó között, amelyek nem egyeznek meg.
- Olyan bejegyzésre van szükség, ami egy leképzett felhasználót képvisel, és a kapcsolódási mód nem az Egyszerű kapcsolódás.

Ez a hiba általában akkor lép fel, ha a kliens érvénytelen jelszóval kísérel meg összekapcsolódni. A hiba részleteivel kapcsolatban tekintse meg a QDIRSRV feladatnaplót (részletes leírás: “Hibafigyelés és hozzáférés követés a Directory Server feladatnapló segítségével” oldalszám: 270).

[Hibás LDAP művelet]: Insufficient access (Nem elegendő elérés)

Ezt a hibát általában egy kapcsolódó 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 munkanaplóját (részletes leírás: “Hibafigyelés és hozzáférés követés a Directory Server feladatnapló segítségével” oldalszám: 270).

[Hibás LDAP művelet]: 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 munkanaplóját (részletes leírás: “Hibafigyelés és hozzáférés követés a Directory Server feladatnapló segítségével” oldalszám: 270). Ha a Directory Server sikeresen elindult, akkor a QDIRSRV feladatnaplójában a Directory Server started successfully (A Directory Server sikeresen elindult) szövegű üzenet található.

[Hibás LDAP művelet]: 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 szerverre irányuló kapcsolatfelvételi kísérletét. A Digitális igazoláskezelővel győződjön meg róla, hogy igazolásai megfelelően vannak összeállítva, majd indítsa újra a szervert, és kísérelje meg újból a kapcsolatfelvételt.
- A felhasználó nem rendelkezik a *SYSTEM igazolástárhoz (ez alapértelmezés szerint /QIBM/userdata/ICSS/Cert/Server/default.kdb) olvasási hozzáférési joggal.

i5/OS C alkalmazások esetében további SSL hibainformációk állnak rendelkezésre. További részleteket a Programozás témakör “Directory Server API-k” részében talál.

Jelszóirányelvekkel kapcsolatos hibák

| Ha bizonyos jelszó-irányelvek engedélyezve vannak, akkor nem nyilvánvaló hibákat okozhatnak. Tekintse át a következőket segítségül a jelszó-irányelvekkel összefüggő hibák elhárításához.

| **A helyes jelszóval létrehozott kapcsolat "érvénytelen hitelesítési adatok" üzenettel meghiúsul:** A jelszó lehet, hogy lejárt, vagy a fiók zárolva van. Vizsgálja meg a bejegyzés pwdchangedtime és pwdaccountlockedtime attribútumát a(z) “Jelszó-irányelv javaslatok” oldalszám: 152 részben leírtaknak megfelelően.

| **A kérések "nem kívánatos végrehajtás" üzenettel meghiúsulnak a sikeres kapcsolódás után:** Lehet, hogy a jelszót alaphelyzetbe kell állítani; Ebben az esetben a kapcsolódás sikeres lesz, de a szerver a felhasználó számára csak a jelszó megváltoztatását engedélyezi. A többi kérés "nem kívánatos végrehajtás" üzenettel meg fog hiúsulni, amíg a jelszó megváltoztatása meg nem történik.

| **Az alaphelyzetbe állított jelszóval történő hitelesítés váratlan módon viselkedik:** Ha a jelszó alaphelyzetbe állításra került, akkor a kapcsolati kérések sikeresek lesznek a fentiekben leírt módon. Ez azt jelenti, hogy a felhasználó lehet, hogy képes lesz korlátlanul használni egy alaphelyzetbe állítási jelszót.

A QGLDCPYVL API hibaelhárítása

| Ez az API a Felhasználó nyomkövetési szolgáltatást használja műveletei feljegyzésére. Ha hiba történik vagy akár csak a gyanúja felmerül, akkor a nyomkövetés megmagyarázhatja a látszólagos hibát vagy nyilvánvalóvá teheti, ha szervizre van szükség. A nyomkövetés a következőképpen érhető el:

```
| STTRC SSNID(COPYVLDL) JOBTRCTYPE(*TRCTYPE) TRCTYPE((*DIRSRV *INFO))
| CALL QGLDCPYVL PARM(...)
| ENDTRC SSNID(COPYVLDL) DTALIB(QTEMP) PRTRC(*YES)
```

| Az információk elmentése és elküldése a szerviznek:

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




```
| SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
```

I ahol QAP0ZDMP egy nullát tartalmaz és xxx az SAVF fájl megadott neve.



10. fejezet Kapcsolódó információk

Az alábbiakban felsoroltuk az alábbiakban felsoroljuk a Directory Server témakörrel kapcsolatos IBM Redbook kiadványokat (PDF formátumban), webhelyeket és Információs központ témaköröket. A PDF-ek bármelyikét megtekintheti és kinyomtathatja.

Redbook kiadványok (www.redbooks.ibm.com)

- Understanding LDAP, SG24-4986  .
- Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino , SG24-6163  .
- Implementation and Practical Use of LDAP on the iSeries Server, SG24-6193  .

Webhelyek

- IBM Directory Server for iSeries Web site 
(www.ibm.com/servers/eserver/series/ldap)
- The Java Naming and Directory Interface (JNDI) Tutorial Web site 
(java.sun.com/products/jndi/tutorial/)

Egyéb információk

A Programozás fejezet alatt, a “Directory Server API-k” kategóriában.

Nyilatkozatok

Ezek az információk az Egyesült Államokban forgalmazott termékekre és szolgáltatásokra vonatkoznak.

Elképzelhető, hogy a dokumentumban szereplő termékeket, szolgáltatásokat vagy lehetőségeket az IBM más országokban nem forgalmazza. Az adott országokban rendelkezésre álló termékekről és szolgáltatásokról a helyi IBM képviselőknek szolgálnak felvilágosítással. Az IBM termékekre, programokra vagy szolgáltatásokra vonatkozó hivatkozások sem állítani, sem sugallni nem kívánják, hogy az adott helyzetben csak az IBM termékeit, programjait vagy szolgáltatásait lehet alkalmazni. Minden olyan működésében azonos termék, program vagy szolgáltatás alkalmazható, amely nem sérti az IBM szellemi tulajdonjogát. A nem IBM termékek, programok és szolgáltatások működésének megítélése és ellenőrzése természetesen a felhasználó felelőssége.

A dokumentum tartalmával kapcsolatban az IBM-nek bejegyzett vagy bejegyzés alatt álló szabadalmi lehetnek. Ezen dokumentum nem ad semmiféle licenct ezen szabadalmakhoz. A licenckérelmeket írásban a következő címre küldheti:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Ha duplabyte-os (DBCS) információkkal kapcsolatban van szüksége licencre, akkor lépjen kapcsolatba saját országában az IBM szellemi tulajdon osztályával, vagy írjon a következő címre:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

A következő bekezdés nem vonatkozik az Egyesült Királyságra, valamint azokra az országokra, amelyeknek jogi szabályozása ellentétes a bekezdés tartalmával: AZ INTERNATIONAL BUSINESS MACHINES CORPORATION JELEN KIADVÁNYT "JELENLEGI FORMÁJÁBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA NÉLKÜL ADJA KÖZRE, IDEÉRTVE, DE NEM KIZÁRÓLAG A JOGSÉRTÉS KIZÁRÁSÁRA, A KERESKEDELMI ÉRTÉKESÍTHETŐSÉGRE ÉS BIZONYOS CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁT. Bizonyos államok nem engedélyezik egyes tranzakciók kifejezett vagy vélelmezett garanciáinak kizárását, így elképzelhető, hogy az előző bekezdés Önre nem vonatkozik.

Jelen dokumentum tartalmazhat technikai, illetve szerkesztési hibákat. Az itt található információk bizonyos időnként módosításra kerülnek; a módosításokat a kiadvány új kiadásai tartalmazzák. Az IBM mindennemű értesítés nélkül fejlesztheti és/vagy módosíthatja a kiadványban tárgyalt termékeket és/vagy programokat.

A kiadványban a nem IBM webhelyek megjelenése csak kényelmi célokat szolgál, és semmilyen módon nem jelenti ezen webhelyek előnyben részesítését másokhoz képest. Az ilyen webhelyeken található anyagok nem képezik az adott IBM termék dokumentációjának részét, így ezek használata csak saját felelősségre történhet.

Az IBM belátása szerint bármilyen formában felhasználhatja és továbbadhatja a felhasználóktól származó információkat anélkül, hogy a felhasználó felé ebből bármilyen kötelezettsége származna.

A programlicenc azon birtokosainak, akik információkat kívánnak szerezni a programról (i) a függetlenül létrehozott programok vagy más programok (beleértve ezt a programot is) közti információcseréhez, illetve (ii) a kicserélt információk kölcsönös használatához, fel kell venniük a kapcsolatot az alábbi címmel:

IBM Corporation
Software Interoperability Coordinator, Department YBWA

3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Az ilyen információk bizonyos feltételek és kikötések mellett állnak rendelkezésre, ideértve azokat az eseteket is, amikor ez díjfizetéssel jár.

- | A dokumentumban tárgyalt licencprogramokat és a hozzájuk tartozó licenc anyagokat az IBM az IBM Vásárlói
- | megállapodás, az IBM Nemzetközi programlicenc szerződés, az IBM Gépi kódra vonatkozó licencszerződés vagy a
- | felek azonos tartalmú megállapodása alapján biztosítja.

A dokumentumban található teljesítményadatok ellenőrzött környezetben kerültek meghatározásra. Ennek következtében a más működési körülmények között kapott adatok jelentősen különbözhetnek a dokumentumban megadottaktól. Egyes mérések fejlesztői szintű rendszereken kerültek végrehajtásra, így nincs garancia arra, hogy ezek a mérések azonosak az általánosan hozzáférhető rendszerek esetében is. Továbbá bizonyos mérések következtetés útján kerültek becslésre. A tényleges értékek eltérhetnek. A dokumentum felhasználóinak ellenőrizni kell az adatok alkalmazhatóságát az adott környezetben.

A nem IBM termékekre vonatkozó információkat az IBM a termékek szállítóitól, az általuk közzétett bejelentésekből, illetve egyéb nyilvánosan elérhető forrásokból szerezte be. Az IBM nem tesztelte ezeket a termékeket, így a nem IBM termékek esetében nem tudja megerősíteni a teljesítményre és kompatibilitásra vonatkozó, valamint az egyéb állítások pontosságát. A nem IBM termékekkel kapcsolatos kérdéseivel forduljon az adott termék szállítóhoz.

Az IBM jövőbeli tevékenységére vagy szándékaira vonatkozó állításokat az IBM mindennemű értesítés nélkül módosíthatja, azok csak célokat jelentenek.

A közzétett árak az IBM által javasolt aktuális kiskereskedelmi árak, amelyek előzetes bejelentés nélkül bármikor változhatnak. Az egyes forgalmazók árai eltérhetnek ezektől.

A leírtak csak tervezési célokat szolgálnak. Az információk a tárgyalt termékek elérhetővé válása előtt megváltozhatnak.

Az információk között példaként napi üzleti tevékenységekhez kapcsolódó jelentések és adatok lehetnek. A valóságot a lehető legjobban megközelítő illusztráláshoz a példákban egyének, vállalatok, márkák és termékek nevei szerepelnek. Minden ilyen név a képzelet szüleménye, és valódi üzleti vállalkozások neveivel és címeivel való bármilyen hasonlóságuk teljes egészében a véletlen műve.

Szerzői jogi licenc:

A kiadvány forrásnyelvi alkalmazásokat tartalmaz, amelyek a programozási technikák bemutatására szolgálnak a különböző működési környezetekben. A példaprogramokat tetszőleges formában, az IBM-nek való díjfizetés nélkül másolhatja, módosíthatja és terjesztheti fejlesztési, használati, marketing célból, illetve olyan alkalmazási programok terjesztése céljából, amelyek megfelelnek azon operációs rendszer alkalmazásprogram illesztőjének, ahol a példaprogramot írta. Ezek a példák nem kerültek minden körülmények között tesztelésre. Az IBM így nem tudja garantálni a megbízhatóságukat, szervizelhetőségüket, de még a programok funkcióit sem.

Ha az információkat elektronikus formában tekinti meg, akkor elképzelhető, hogy a fotók és a színes ábrák nem jelennek meg.

Védjegyek

A következő kifejezések az International Business Machines Corporation védjegyei az Egyesült Államokban és/vagy más országokban:

Application System/400
AS/400

DB2
e(logo)server
eServer
i5/OS
IBM
iSeries
Lotus
Lotus Notes
Operating System/400
OS/400
Redbooks
SecureWay
WebSphere
400

A Microsoft, a Windows, a Windows NT és a Windows logó a Microsoft Corporation védjegye az Egyesült Államokban és/vagy más országokban.

A Java, valamint minden Java alapú kifejezés a Sun Microsystems, Inc. védjegye az Egyesült Államokban és/vagy más országokban.

A UNIX a The Open Group bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

Más cégek, termékek és szolgáltatások nevei mások védjegyei vagy szolgáltatás védjegyei lehetnek.

Feltételek és kikötések

- | A kiadványok használata az alábbi feltételek és kikötések alapján lehetséges.
- | **Személyes használat:** A kiadványok másolhatók személyes, nem kereskedelmi célú használatra, de valamennyi tulajdonosi feljegyzést meg kell tartani. Az IBM kifejezett engedélye nélkül nem szabad a kiadványokat vagy azok részeit terjeszteni, megjeleníteni, illetve belőlük származó munkát készíteni.
- | **Kereskedelmi használat:** A kiadványok másolhatók, terjeszthetők és megjeleníthetők, de kizárólag a vállalaton belül, és csak az összes tulajdonosi feljegyzés megtartásával. Az IBM kifejezett hozzájárulása nélkül nem készíthetők olyan munkák, amelyek a kiadványokból származnak, továbbá nem másolhatók, nem terjeszthetők és nem jeleníthetők meg, még részben sem, a vállalaton kívül.
- | A jelen engedélyben foglalt, kifejezetten megadott hozzájáruláson túlmenően a kiadványokra, illetve a bennük található információkra, adatokra, szoftverekre vagy egyéb szellemi tulajdonra semmilyen más kifejezett vagy vélelmezett engedély nem vonatkozik.
- | Az IBM fenntartja magának a jogot, hogy jelen engedélyeket saját belátása szerint bármikor visszavonja, ha úgy ítéli meg, hogy a kiadványokat az IBM érdekeit sértő módon használják fel, vagy a fenti útmutatásokat nem megfelelően követik.
- | Jelen információk kizárólag valamennyi vonatkozó törvény és előírás betartásával tölthetők le, exportálhatók és reexportálhatók, beleértve az Egyesült Államok exportra vonatkozó törvényeit és előírásait is.
- | AZ IBM A KIADVÁNYOK TARTALMÁRA VONATKOZÓAN SEMMIFÉLE GARANCIÁT NEM NYÚJT. A KIADVÁNYOK "ÖNMAGUKBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA VÁLLALÁSA NÉLKÜL KERÜLNEK KÖZREADÁSRA, IDEÉRTVE, DE NEM KIZÁRÓLAG A KERESKEDELMI ÉRTÉKESÍTHETŐSÉGRE, A SZABÁLYOSSÁGRA ÉS AZ ADOTT CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁKAT IS.



Nyomtatva Dániában