System i

Directory Server
IBM Tivoli Directory Server for i5/OS (LDAP)

6. változat 1. kiadás

System i

Directory Server
IBM Tivoli Directory Server for i5/OS (LDAP)

6. változat 1. kiadás

Megjegyzés

Jelen leírás és a tárgyalt termék használatba vétele előtt feltétlenül olvassa el a “Nyilatkozatok”, oldalszám: 315 részben leírtakat.

Ez a kiadás az IBM i5/OS (termékszám: 5722-SS1) V6R1M0 változatára, és minden ezt követő kiadásra és módosításra vonatkozik mindaddig, amíg az újabb kiadások ezt másként nem jelzik. Ez a változat nem fut minden csökkentett utasításkészletű (RISC) rendszeren illetve a CISC modelleken.

Tartalom

IBM Tivoli Directory Server for i5/OS (LDAP)

IBM Tivoli Directory Server for i5/OS (a továbbiakban: Directory Server) az i5/OS Egyszerűsített címtárhozzáférési protokoll (LDAP) szervert biztosító szolgáltatása. 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 segítséget nyújtanak a Directory Server megismerése során.

V6R1 újdonságok

Olvassa el az új, illetve jelentősen módosított IBM Tivoli Directory Server for i5/OS (LDAP) témakörgyűjteményben található információkat.

Replikációs ütközések feloldása

Több elsődleges szerverrel rendelkező hálózatban az IBM Tivoli® Directory Server képes az ütköző módosítások felismerésére, illetve feloldására, hogy ezáltal az összes szerveren található címtár konzisztens maradjon. Ha a rendszer replikációs ütközést észlel, akkor az ütköző módosítást a rendszer a szerver naplóban jelzi, illetve a módosítás a ″talált tárgyak″ naplófájlban is rögzítésre kerül, hogy ezáltal az adminisztrátorok az esetlegesen elveszett adatokat helyreállíthassák.

- Replikáció áttekintés
- Talált tárgyak napló beállításainak módosítása
- Talált tárgyak naplófájl megjelenítése

ldapmodify parancs

Az ldapmodify -e hibafájl paraméterrel bővült, amelynek köszönhetően megadható az a fájl, amelyben a visszautasított bejegyzések rögzítésre kerülnek. Az új -n paraméternek köszönhetően pedig az esetleges módosításokat a szabványos kimeneten felkiáltójel előzi meg.

- ldapmodify és ldapadd
- LDAP adatcsere formátum (LDIF)

Több szálon futó replikáció

A replikáció - a replikáció átfogó teljesítményének javításához - használhat több szálat.

- Több szálon futó replikáció
- Replikációs megállapodások

Jelszótitkosítás

Az IBM Tivoli Directory Server konfigurációs paraméterének segítségével a felhasználói jelszó adatok a címtárban történő eltárolásuk előtt titkosíthatók. A titkosítási paraméternek köszönhetően megelőzhető, hogy az egyszerű szöveges jelszó adatokhoz a normál címtár felhasználók, illetve az adminisztrátori címtár felhasználók hozzáférjenek.

- Jelszótitkosítás
- Jelszó házirend tulajdonságok beállítása

Az IBMAttributeTypes attribútum

Az IBM Tivoli Directory Server 6.0 lehetővé teszi, hogy az attribútumok első 128 karakterének segítségével a tábla nevét létrehozza.

- Az IBMAttributeTypes attribútum

Nem engedélyezett sémamódosítások

Az oszlopméret a séma módosításával növelhető. Ennek köszönhetően az attribútumok maximális hossza a séma módosítás használatával a webes adminisztrációs, illetve az ldapmodify segédprogram segítségével egyaránt növelhető.

- Nem engedélyezett sémamódosítások

Elosztott könyvtár

Az IBM Tivoli Directory Server a jelen változattól kezdődően elosztott címtár. Ha az elosztott címtár szolgáltatást proxy szerverrel együttesen használja, akkor a címtárfürtök egyetlen címtárként jeleníthetők meg. Az elosztott címtár és a proxy szerver szolgáltatások együttes használatával lehetővé válik, hogy a címtár telepítések több millió bejegyzést tartalmazzanak.

- Elosztott címtárak

ldapmodrdn

Az IBM Tivoli Directory Server támogatja a modifyDN használatát a newsuperior attribútummal a levél csomópontokon.

- ldapmodrdn

Hibakeresés TRCTCPAPP segítségével

A TRCTCPAPP parancs segítségével az aktív szerver példányok nyomon követhetők.

- Hibakeresés TRCTCPAPP segítségével

Olvasási hozzáférés leképezett felhasználóknak

A felhasználói leképezett háttér objektumokra irányuló összes kereső művelet letiltható.

- LDAP műveletek
- Olvasási hozzáférés leképezett felhasználók számára

Több szerver példány

i5/OS® rendszeren több címtárszerver is futhat. Az egyes szerverek az ún. példányok. Ha a címtárszervert az i5/OS egy korábbi kiadása alatt használta, akkor a címtárszerver QUSRDIR példány néven átállításra kerül. Az alkalmazások kiszolgálásához több címtárszerver példány is létrehozható.

- Példányok kezelése
- Directory Server beállítása

Átállítási tényezők

Az IBM Tivoli Directory Server a szerver első indításakor frissítésre kerül az újabb változatra.

- Átállítás V5R4 vagy V5R3 változatról V6R1 változatra

Jelszóirányelv

Az adminisztrátori fiókok a nagy mennyiségű hitelesítési hibák miatt zárolhatók. A szolgáltatás csak a távoli kliens kapcsolatokra vonatkozik. A szerver indításakor a fiók alaphelyzetbe áll. A meghatározott új attribútum lehetővé teszi a fiókok adminisztrátori zárolását.

- Adminisztrátori jelszó és kizárási házirend beállítása
- Jelszó házirend tulajdonságok beállítása

A kiterjesztett műveletek közé tartozó fiók állapot kérésnek köszönhetően egy adott fiók állapota (nyitott (engedélyezett), zárolt, illetve lejárt) lekérhető.

- ldapexop

Egyéb

IBM® Tivoli® Directory Server megfelelőség: A V6R1 változatú Directory Server megfelel az IBM Tivoli Directory Server 6.0 változatának.

- Tivoli szoftver információs központ

Újdonságok és módosítások megtekintésének módjai

A technikai változások gyors áttekintését a következő ábrák segítik:

- Az új vagy módosított információk kezdetét a  kép jelöli.
- Az új vagy módosított információk végét a  kép jelöli.

A PDF fájlok esetében az új vagy módosított információkat a bal margón található módosítás jel (|) jelöli.

A kiadás további újdonságairól és változásairól a Jegyzék a felhasználóknak című dokumentumból tájékozódhat.

IBM Tivoli Directory Server for i5/OS (LDAP) PDF fájl

Az IBM Tivoli Directory Server for i5/OS (LDAP) PDF fájl formátumban megjeleníthető, illetve kinyomtatható.

A dokumentum PDF változatának megjelenítéséhez válassza ki az IBM Tivoli Directory Server for i5/OS (LDAP) lehetőséget (kb. 2700 KB).

Egyéb információk

A kapcsolódó PDF fájlok és IBM Redbooks kiadványok megjelenítésével és nyomtatásával kapcsolatosan további információkat a “Kapcsolódó információk” oldalszám: 313 alatt talál.

PDF fájlok mentése

A PDF fájl mentése a munkaállomáson megjelenítés vagy nyomtatás céljából:

1. Kattintson a jobb egérgombbal a böngészőben a PDF hivatkozásra.
2. Válassza az előugró menü PDF helyi mentésére vonatkozó menüpontját.
3. Válassza ki azt a könyvtárat, amelybe a PDF fájlt menteni kívánja.
4. Kattintson a **Mentés** gombra.

Adobe Reader letöltése

A PDF fájlok megtekintéséhez vagy kinyomtatásához telepítenie kell az Adobe Reader alkalmazást. A program ingyenesen letölthető az Adobe weboldaláról (www.adobe.com/products/acrobat/readstep.html) .

Directory Server - Alapfogalmak

Információk a Directory Server alapfogalmairól.

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 LDAP műveletek tranzakciós integritása, a nagy teljesítményű működés, valamint az üzem közbeni mentési és visszaállítási lehetőségek érdekében háttértárként az IBM DB2 Universal Database for iSeries adatbázis-kezelőjét használja. Együttműködik az IETF LDAP V3 szabványnak megfelelő kliensekkel.

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 részhalmazát 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 karaktersorozatokkal vannak megadva: a cn jelenti a közönséges nevet (common name), a mail pedig az e-mail címet.

A példacímtárban (1. ábra: oldalszám: 5) 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.

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 engedelmeskedni tartozik.

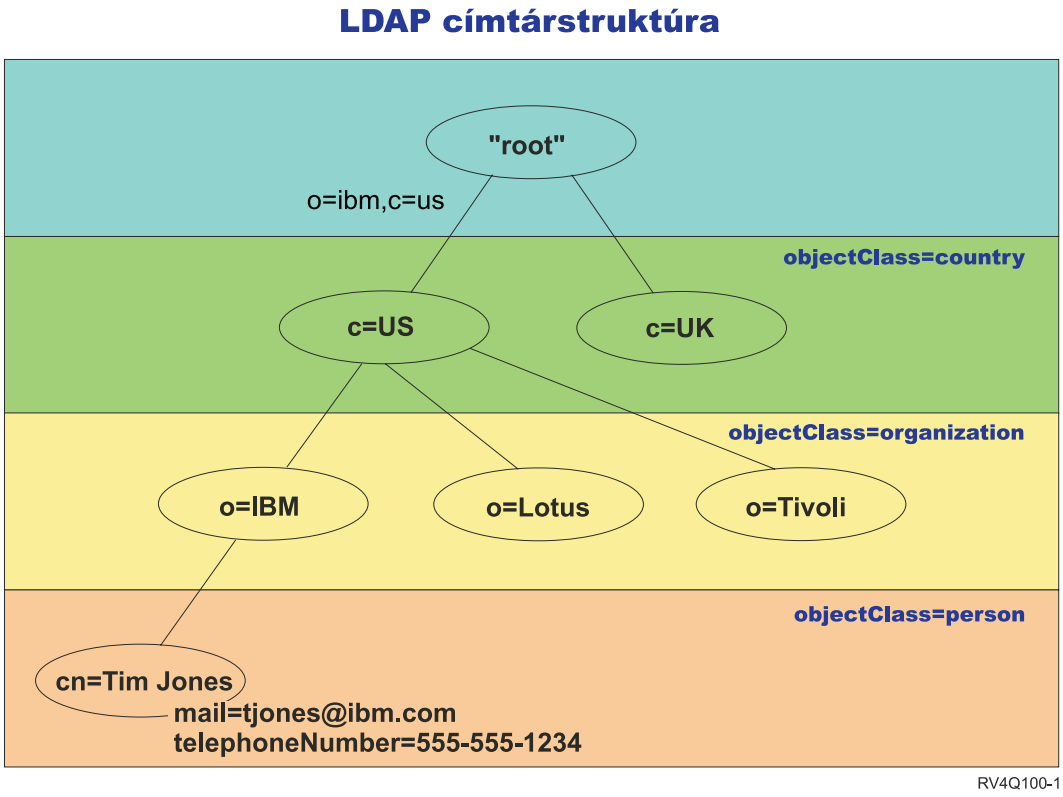
A séma által megadott attribútumok mellett vannak a szerver által kezelt attribútumok is. Ezek közt az úgynevezett működési attribútumok közt olyan dolgok találhatók, mint például mikor lett létrehozva a bejegyzés, hozzáférés-felügyeleti információk és hasonlók.

Hagyományosan, az LDAP címtárbejegyzések hierarchikus struktúrába rendeződnek, amely politikai, földrajzi, vagy szervezeti határokat tükröz (1. ábra: oldalszám: 5). 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 nevekkel (Distinguished Names, DN-ek) hivatkozik. Egy megkülönböztetett név tartalmazza magának a bejegyzésnek a nevét, csakúgy, mint a címtárban felette álló objektumok nevét lentről felfelé. Például, az 1. ábra: bal alsó sarkában található bejegyzés teljes DN-je cn=Tim Jones, o=IBM, c=US. Minden egyes bejegyzés rendelkezik legalább egy attribútummal a bejegyzés nevéhez. 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.

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: 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.



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 részeiből állnak. Például a dc=ibm,dc=com név előnyösebb lehet az o=ibm,c=us névnél.

Tegyük fel, hogy létre akar hozni egy címtárat 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 ugyanazokon 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.

Kapcsolódó fogalmak

“Séma” oldalszám: 14
A séma az a szabályhalmaz, amelyik szabályozza, milyen adatok tárolhatók a címtárban. A séma határozza meg az engedélyezett bejegyzések típusát, attribútumaik szerkezetét és szintaxisát.

“Műveleti attribútumok” oldalszám: 92
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.

“Megkülönböztetett nevek (DN)” oldalszám: 9
A címtár minden bejegyzésének vagy egy megkülönböztetett neve (DN). A DN az a név, amelyik egyedi módon azonosítja a címtárbejegyzést. A DN első elemét szokás relatív megkülönböztetett névként (Relative Distinguished Name, RDN) emlegetni.

Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek
A Directory Server alkalmazás programozási felületekkel kapcsolatosan további információkat az Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek témakör tartalmaz.

“Directory Server biztonság” oldalszám: 52
Ismerje meg azokat a funkciókat, amelyeknek köszönhetően a Directory Server biztonságosabbá tehető.

Kapcsolódó tájékoztatás

Java Naming and Directory Interface (JNDI) ismertető webhely

Elosztott címtárak

Az elosztott címtár olyan címtár környezet, amelyben az adatok több címtárszerver között particionáltak. Ahhoz, hogy az elosztott címtárak a kliens alkalmazások felé egy könyvtárként jelenjenek meg, a rendszer néhány proxy szervert biztosít, amelyek ismerik az összes szervert, illetve az egyes szervereken tárolt adatokat.

A proxy szerverek a bejövő kéréseket továbbítják a megfelelő szerverek felé, majd a válaszok összegyűjtését követően a kliens felé egységesített választ adnak vissza. Az elosztott címtár egyes részeit több háttér szerver tartalmazza. Ezek a háttér szerverek valójában általános, kiegészítő proxy szerver támogatással rendelkező LDAP szerverek, amelynek köszönhetően képesek egy másik szerveren található, illetve másik szerveren meghatározott csoporthoz tartozó felhasználó nevében kéréseket kiadni.

Az IBM Tivoli Directory Server 6.0 és újabb változatai (elosztott operációs rendszerek) ilyen elosztott címtárat biztosítanak, proxy és háttér szerverekkel, illetve az ilyen címtárak beállításához szükséges eszközökkel. Az ilyen címtárak képesek sok millió bejegyzés kezelésére is.

IBM Directory Server for i5/OS elosztott címtár támogatás

Az IBM Directory Server for i5/OS képes az IBM Tivoli Directory Server elosztott címtárakban háttér szerverként működni. Az i5/OS címtárszerver nem lehet proxy szerver, illetve az elosztott címtár beállításához szükséges eszközöket nem tartalmazza. A proxy szerver futhat más platformon, miközben a tényleges adatok egy vagy több i5/OS címtárszerveren, illetve i5/OS és Tivoli platformon futó címtárszerverek keverékén találhatók.

Ahhoz, hogy a meglévő, i5/OS címtárszerverről származó adatok az elosztott címtár topológiában felhasználhatók legyenek, az adatokat az i5/OS címtárból LDIF fájlba kell exportálni, Tivoli platformok esetében a Tivoli által biztosított elosztott címtár telepítő eszközt az LDIF fájl felhasználásával futtatni kell, majd az adatokat vissza kell tölteni az elosztott címtárban háttér szerverként részt vevő i5/OS és Tivoli címtárszerverekre. A feldolgozás hasonló módon történik az i5/OS szerverek és Tivoli platformmal rendelkező szerverek esetében is, illetve a felhasználók már rendelkeznek az elosztott címtár telepítő eszközzel, mivel rendelkeznek Tivoli platformon futó proxy szerverrel.

Elosztott címtárakat támogató vezérlőelemek és kiterjesztett műveletek

Mivel a felhasználók, illetve azok a csoportok, amelyekhez tartoznak, több szerver között lehetnek elosztva, az IBM Tivoli Directory Server számos vezérlőelemet és kiterjesztett műveletet határoz meg, amelyek támogatják az elosztott címtárak csoporttagság és hozzáférés felügyeletét. Ezen kívül a rendszer ″nyomkövetési napló″ mechanizmust is tartalmaz, amely a műveleteket a kezdeményező kliensig visszavezeti.

Megjegyzés: A címtárbejegyzések egy szerveren, illetve a szerver replikáin kerülnek tárolásra. Elosztott címtárak esetében azonban a felhasználók az egyik szerveren más csoportokhoz tartozhatnak, mint a másikon. Hasonlóképpen előfordulhat, hogy maga a felhasználó az adott kérést feldolgozó háttér szerveren nincs meghatározva.

Felülvizsgálat vezérlés

A felülvizsgálat vezérlés olyan mechanizmus, amelynek segítségével a proxy szerver a proxy szerver által kezdeményezett kliens kérések egyedi azonosítóját a háttér szerverek felé továbbítja. A felülvizsgálat vezérlés keretein belül az egyedi azonosítón kívül a kezdeményező kliens IP is továbbításra kerül. A proxy és a háttér szerveren található felülvizsgálati bejegyzések egymásnak az egyedi azonosító segítségével kerülnek megfeleltetésre. Ha egy kérés több szerveren halad át, akkor az egyes szerverek IP információja hozzáfűzésre kerül, amelynek következtében a nyom visszavezet egészen az eredeti kliensig.

Csoporttagság-kiértékelése kiterjesztett művelet

A kiterjesztett művelet segítségével egy jogosult kliens (a proxy szerver) egy felhasználó információit egy háttér szervernek továbbíthatja, majd lekérheti azoknak a (statikus, beágyazott, illetve dinamikus) csoportoknak a listáját, amelyeknek a felhasználó a háttér szerveren tagja.

Csoporttagság vezérlőelem

A vezérlőelem segítségével egy jogosult kliens (a proxy szerver) egy, a hozzáférés felügyelet során felhasználandó csoportlistát továbbíthat. A hozzáférés felügyelet kiértékelése során a szerver által egyébként használt, a helyileg tárolt csoportinformációk alapján összeállított lista helyett a rendszer ezt a listát használja. Jellemzően a csoportlista

| megegyezik azzal a listával, amelyet a proxy szerver az egyes szerverektől csoporttagság kiértékelése kiterjesztett
| művelet segítségével összegyűjt.

Elosztott címtárak felülvizsgálati támogatása

| Az i5/OS biztonsági felülvizsgálat az elosztott címtárak támogatásával bővült.

- **Felülvizsgálat vezérlés**: A kérés visszakövetése a kezdeményező kliensig számos esetben hasznos lehet. Az I5/OS a ″felülvizsgálat vezérlést″ olyan módon vizsgálja felül, hogy a meglévő DI biztonsági felülvizsgálati naplóbejegyzést egy ″útválasztási″ mezővel egészíti ki. Ugyan a tartalom nem ellenőrizhető, azonban a proxy hitelesítés használatára jogosult klienstől származik, tehát megbízható kliensnek számít.
- **Csoporttagság vezérlőelem**: A csoport vezérlőelem jelenléte két részben kerül felülvizsgálatra: a DI biztonsági felülvizsgálati naplóbejegyzés egy karakteres “csoporttagság-érvényesítő” mezővel bővült. A szerver választhatóan beállítható a kliens által biztosított csoportlista felülvizsgálatára is. Ha a beállítás meg van adva, akkor a DI naplóbejegyzésben a szerver egy ″XD kereszthivatkozás″ mezőt is felülvizsgál, illetve néhány XD biztonsági felülvizsgálati naplóbejegyzést is létrehoz a megfelelő ″XD kereszthivatkozás″ mezővel, illetve a csoportlistával (egy bejegyzéshez legfeljebb 5 csoportot)

| Az i5/OS biztonsági felülvizsgálattal kapcsolatosan további részleteket az alábbi kapcsolódó hivatkozások Biztonsági
| referencia témaköre tartalmaz. Ezen kívül érdemes megtekinteni a The Internet Engineering Task Force webhelyet is,
| ahol az *rfc4648* kifejezésre keresve többet is megtudhat a címtárszerver felülvizsgálatának beállításáról.

| Az elosztott címtárakkal, illetve az elosztott címtárak beállításával kapcsolatosan további információkat a Tivoli
| szoftver információs központ Elosztott címtárak témaköre tartalmaz.

| **Kapcsolódó fogalmak**

| “Felülvizsgálat” oldalszám: 52
| A felülvizsgálat segítségével nyomon követhetők bizonyos Directory Server tranzakciók részletei.

| **Kapcsolódó tájékoztatás**

| Biztonsági felülvizsgálatok
| A felülvizsgálattal kapcsolatosan további információkat a Biztonsági felülvizsgálatok témakör tartalmaz.

| Kiterjesztett műveletek és vezérlők objektumazonosítói (OID)

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 első elemét szokás relatív megkülönböztetett névként (Relative Distinguished Name, RDN) emlegetni.

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 kapcsolatosan.

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
Névtelen	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
Névtelen	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 aclentry 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 szerverséma alapján normalizálja. Ez a kiterjesztett művelet hasznos lehet a DN-eket használó alkalmazások esetén.

Megkülönböztetett nevek szintaxisa

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

```
<név> ::= <név-összetevő> ( <szóközzel-elválasztott-elválasztó> )
          | <név-összetevő> <szóköz-elválasztó> <név>

   <szóköz-elválasztó> ::= <elhagyható-szóköz>
                           <elválasztó>
                           <elhagyható-szóköz>

   <elválasztó> ::=  "," | ";"

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

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

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

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

   <oid> ::= <számkaraktersorozat> | <számkaraktersorozat> "." <oid>
   <számkaraktersorozat> ::= 1*<szám>
   <szám> ::= 0-9 szám

   <karaktersorozat> ::= *( <karaktersorozatkarakter> | <pár> )
            | '"' *( <karaktersorozatkarakter> | <speciális> | <pár> ) '"'
            | "#" <hex>


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

   <pár> ::= "\" ( <speciális> | "\" | '"')
   <karaktersorozatkarakter> ::= tetszőleges karakter, kivéve a <speciális> vagy "\" és '"' karaktereket


   <hex> ::= 2*<hexkarakter>
   <hexkarakter> ::= 0-9, a-f, A-F
```

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

Szóközszerű karakterek (szóközök) szerepelhetnek a vessző vagy pontosvessző bármelyik oldalán. A szóközszerű 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 azonosítson egy adott bejegyzést olyan esetben, amikor egyetlen sima CN érték kétértelmű lenne:

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

Kapcsolódó fogalmak

“Címtárak” oldalszám: 4
A Directory Server (címtárszerver) segítségével egy olyan adatbázistípus érhető el, amely az információkat az i5/OS integrált fájlrendszerének felépítéséhez hasonló, hierarchikus struktúrába szervezve tárolja.

“Directory Server biztonság” oldalszám: 52
Ismerje meg azokat a funkciókat, amelyeknek köszönhetően a Directory Server biztonságosabbá tehető.

“Vezérlőelemek és kiterjesztett műveletek” oldalszám: 94
A vezérlőelemek és kiterjesztett műveletek segítségével az LDAP protokoll a protokoll módosítása nélkül kiterjeszthető.

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.

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=sajatceg,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=rendszer-nev.sajattartomany.com″ utótag az i5/OS objektumok LDAP címtáron keresztül történő elérését biztosítja (egyelőre csak felhasználói profilok és csoportok esetében)

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 sajatceg.com, akkor választható például a dc=sajatceg,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=sajatceg,dc=com
objectclass: domain
dc: sajatceg
```

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.

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.

Kapcsolódó fogalmak

“Címtárbejegyzésekkel kapcsolatos feladatok” oldalszám: 194
Az alábbi információk segítséget nyújtanak a címtárbejegyzések kezelése során.

“Sémafeladatok” oldalszám: 183
Az alábbi információk segítséget nyújtanak a séma kezelése során.

Kapcsolódó feladatok

“Directory Server utótagok felvétele és eltávolítása” oldalszám: 124
Az alábbi információk segítséget nyújtanak a Directory Server utótagok felvétele és eltávolítása során.

Kapcsolódó hivatkozás

“ldapmodify és ldapadd” oldalszám: 216
Az LDAP modify-entry (bejegyzésmódosító) és LDAP add-entry (bejegyzés-felvevő) parancssori segédprogram.

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 sémákkal kapcsolatos további információk:

Kapcsolódó fogalmak

“Címtárak” oldalszám: 4
A Directory Server (címtárszerver) segítségével egy olyan adatbázistípus érhető el, amely az információkat az i5/OS integrált fájlrendszerének felépítéséhez hasonló, hierarchikus struktúrába szervezve tárolja.

“Címtárbejegyzésekkel kapcsolatos feladatok” oldalszám: 194
Az alábbi információk segítséget nyújtanak a címtárbejegyzések kezelése során.

“Sémafeladatok” oldalszám: 183
Az alábbi információk segítséget nyújtanak a séma kezelése során.

Directory Server séma

A Directory Server sémája előre meghatározott, azonban az igényeknek megfelelően a séma módosítható.

A Directory Server képes dinamikus sémakezelésre. A séma a címtáradatok 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.

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:

- objectClasses
- attributeTypes
- IBMAttributeTypes
- megfeleltetési szabályok
- ldap szintaxisok

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. A ″cn=schema″ DN használatával felvehet, törölhet és lecserélhet attribútumtípusokat és objektumosztályokat. Teljes leírást is megadhat. A sémabejegyzést felveheti vagy lecserélheti LDAP V3 meghatározás, IBM attribútum-kiterjesztés meghatározás használatával, vagy mindkettővel.

Kapcsolódó fogalmak

“Sémafeladatok” oldalszám: 183
Az alábbi információk segítséget nyújtanak a séma kezelése során.

Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek
A Directory Server alkalmazás programozási felületekkel kapcsolatosan további információkat az Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek témakör tartalmaz.

“Objektumosztályok” oldalszám: 17
Az objektumosztályok határozzák meg, hogy egy adott objektumtípust milyen attribútumok írnak le.

“Attribútumok” oldalszám: 18
Minden címtárbejegyzéshez tartozik egy sor attribútum, az objektumosztály meghatározása alapján.

Kapcsolódó hivatkozás

“Az IBMAttributeTypes attribútum” oldalszám: 20
Az IBMAttributeTypes attribútum használható az LDAP Version 3 szabvány által nem szabályozott attribútumok sémainformációinak megadásához.

“Megfeleltetési szabályok” oldalszám: 21
A megfeleltetési szabályok határozzák meg, hogyan történjen a karaktersorozatok összehasonlítása a keresési műveletek közben.

“Attribútum-szintaxis” oldalszám: 24
Az attribútum-szintaxis határozza meg egy attribútum lehetséges értékeit.

“Dinamikus séma” oldalszám: 27
A séma dinamikus módosítására szintén lehetőség van.

Általános séma támogatása

Az IBM Directory támogatja a szabványos címtársémát.

Az IBM Directory támogatja az alábbiak szerinti szabványos címtárséma használatát:

- Az Internet Engineering Task Force (IETF) LDAP Version 3 RFC-k, például az RFC 2252 és 2256 dokumentumok.
- 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 akkor, amikor az LDAP címtárhoz fordulnak. Ide tartoznak például a következők:

- 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 alrendszerekhez, például fiókok, szolgáltatások és hozzáférési pontok, felhatalmazás, hitelesítés, biztonsági irányelvek és még sokminden más.

Kapcsolódó tájékoztatás

Internet Engineering Task Force (IETF)

Desktop Management Task Force (DMTF)

Network Application Consortium

Objektumosztályok

Az objektumosztályok határozzák meg, hogy egy adott objektumtípust milyen attribútumok írnak 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 közösek strukturális objektumosztályok egy adott részhalmazára. 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 örökölhetnek. Az objektumosztály-struktúra határozza megy egy adott bejegyzés kötelező és lehetséges attribútumainak listáját. Az objektumosztály-öröklődés függ az objektumosztály-meghatározások sorrendjétől. Egy objektumosztály csak az őt megelőző objektumosztályoktól örökölhet. 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 örököl, 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=sajatceg, 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 információkért tekintse meg az alábbi hivatkozásokat:

Szokásos alséma-elemek:

Az alséma attribútumértékeinek nyelvtana az elemek segítségével határozható meg.

Az alséma attribútumértékeinek megadására az alábbi elemek használatosak:

- alpha = ’a’ - ’z’, ’A’ - ’Z’
- number = ’0’ - ’9’
- anh = alpha / number / ’-’ / ’;’
- anhstring = 1 * anh
- keystring = alpha [anhstring]
- numericstring = 1 * number
- oid = descr / numericoid
- descr = keystring
- 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 ″(″ qdescrlist ″)″ whsp)
- qdescrlist = [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

Kapcsolódó fogalmak

“Sémafeladatok” oldalszám: 183
Az alábbi információk segítséget nyújtanak a séma kezelése során.

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: 21
- “Attribútum-szintaxis” oldalszám: 24

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 caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch 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)

Kapcsolódó fogalmak

“Sémafeladatok” oldalszám: 183
Az alábbi információk segítséget nyújtanak a séma kezelése során.

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-karaktersorozathoz
      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 128 karaktere alapján kerül kialakításra egy név (amelynek egyedinek kell lennie). Az adatbázis-táblanevek 128 karakterre vannak csonkítva. Az oszlopnevek pedig 30 karakterre.

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 megfeleltetési szabályok három kategóriába esnek:

- Egyenlőség

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

Az IBM Directory Serverben a rész-karaktersorozat és a rendezésillesztés viselkedését az illesztési szabály határozza meg implicite: a rész-karaktersorozat illesztést támogató szintaxisokban van egy beleértett rész-karaktersorozat illesztési szabály is, a rendezésillesztést támogató szintaxisokban pedig egy beleértett rendezésillesztési szabály. A kis- és nagybetűk különbségét figyelmen kívül hagyó illesztési szabállyal megadott attribútumok esetén a beleértett rész-karaktersorozat 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 karaktersorozat.
objectIdentifierMatch	2.5.13.0	OID-ket tartalmazó String. Az OID egy számokból (0-9) és pontokból (.) álló karaktersorozat
octetStringMatch	2.5.13.17	Directory String szintaxis
telephoneNumberMatch	2.5.13.20	Telephone Number szintaxis
uTCTimeMatch	2.5.13.25	UTC Time szintaxis

Sorrendezést 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-karaktersorozatok 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.

Kapcsolódó hivatkozás

“Generalized time és UTC time” oldalszám: 33
A Directory Server a generalized time és a universal (UTC) time szintaxist egyaránt támogatja.

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
- Rendezés
- Közelítés
- Rész-karaktersorozat
- 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 válaszidejét.

Az indexelési szabályok ötféle lehetséges típusa a keresési szűrőn végzett műveletekkel kapcsolatosak.

Egyenlőség

A következő keresési műveletekre vonatkozik:

- equalityMatch ’=’

Például:

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

Rendezés

A következő keresési műveletekre vonatkozik:

- greaterOrEqual ’>=’
- lessOrEqual ’<=’

Például:

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

Közelítés

A következő keresési műveletekre vonatkozik:

- approxMatch '~='

Például:

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

Rész-karaktersorozat

A substring (rész-karaktersorozat) 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 érkeznének vissza. Ha rendezett értékhalmazra 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-karaktersorozat) attribútumok UTF-8 kódú karaktereket tartalmazó szöveges karaktersorozatokat 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 IA5 String attribútumok IA5 kódolású (7 bites US ASCII) karaktersorozatokat 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-karaktersorozatok 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.

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 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 számokból (0-9) és pontokból (.) álló karaktersorozat.	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

Szintaxis	OID
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.	1.3.6.1.4.1.1466.115.121.1.53

Kapcsolódó fogalmak

“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.

Kapcsolódó hivatkozás

“Generalized time és UTC time” oldalszám: 33
A Directory Server a generalized time és a universal (UTC) time szintaxist egyaránt támogatja.

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) találhatók. 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 a nemzeti szabványügyi hivatal saját OID nyilvántartással rendelkezik. 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) találhatók.

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 (képzeletbeli) 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.

Kapcsolódó tájékoztatás

ANSI webhely

ISO webhely

IANA webhely

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

IBMsubschema objektumosztály specifikus objektumosztály, amely egy adott címtárszerver összes attribútumát és objektumosztályát tárolja.'

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.

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.

Kapcsolódó fogalmak

Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek
A Directory Server alkalmazás programozási felületekkel kapcsolatosan további információkat az Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek témakör tartalmaz.

Dinamikus séma

A séma dinamikus módosítására szintén lehetőség van.

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, zárójelekben. Például az <attr-oid> OID-jű 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 típussor 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)
```

Hozzáférés-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 szülőtípusa, nem törölhető. Egy objektumosztály ″MAY″ vagy ″MUST″ attribútumtípusa szintén nem törölhető.
- Egy olyan objektumosztály, amelyik egy másik osztály szülője, nem törölhető.
- Nem létező elemekre (például szintaxisokra vagy objektumosztályokra) hivatkozó attribútumtípusok és objektumosztályok nem vehetők fel.
- Nem módosíthatók úgy attribútumtípusok és objektumosztályok, hogy nem létező elemekre (például szintaxisokra vagy objektumosztályokra) hivatkozzanak.
- Az új attribútumok IBMattributestype 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.

Az oszlopméret a séma módosításával növelhető. Ennek köszönhetően az attribútumok maximális hossza a séma módosítás használatával a webes adminisztrációs, illetve az ldapmodify segédprogram segítségével egyaránt növelhető.

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
- leírás
- dn, distinguishedName
- entryOwner
- hasSubordinates
- ibm-entryChecksum
- ibm-entryChecksumOp
- ibm-entryUuid
- member
- modifiersName
- modifyTimestamp
- név
- 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-supgrpprf

- os400-sys os400-text
- os400-uid
- os400-usrcls
- os400-usropt
- ou, organizationalUnit, organizationalUnitName
- tulajdonos
- 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 meghiúsul és a szerver hibaüzenetet 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 meghiúsul. 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 letiltható a sémaellenőrzés egy része a sémaellenőrzési szint módosításával. Ehhez a System i navigátorban módosítania kell a Directory Server tulajdonságok **Adatbázis/utótagok** oldalán lévő **Sémaellenőrzés** mező értékét.

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.

Kapcsolódó fogalmak

“Directory Server konfigurációs séma” oldalszám: 255
Az alábbi rész a címtár-információs fát (Directory Information Tree, DIT) és az ibmslapd.conf fájl beállításához használt attribútumokat írja le.

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’ karaktersorozatok (illetve a csak kis- és nagybetűkben eltérő megfelelőik) szabadon felcserélve használhatók a sémán, illetve a címtárba felvett bejegyzéseken belül.

Generalized time és UTC time

A Directory Server a generalized time és a universal (UTC) time szintaxist egyaránt támogatja.

Többféle módon is jelölhetők a dátumokkal és idővel kapcsolatos információk. 1999. február negyedike 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:

  `ÉÉÉÉHHNNŐŐPPMM[.|,tört][(+|-ŐŐPP)|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 '-' jelnek az óra-perc érték előtt kell állnia.

- Az Universal time szintaxis, amely a következő formátumú:

  `ÉÉHHNNŐŐPP[MM][(+ | -)ŐŐPP)|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-karaktersorozatok 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
```

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.

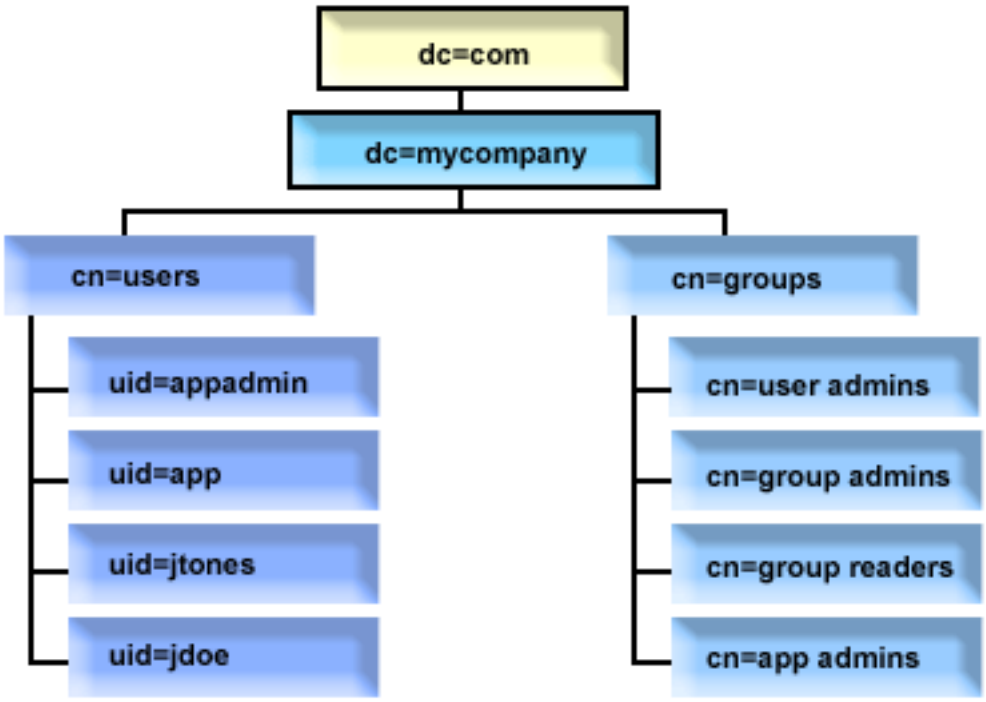
Ugyanígy, a csoportok általában egy külön tárolóban (például ″cn=groups″) találhatók.

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:



2. ábra: Példa címtárstruktúra

- A c=sajatceg, 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 hozzáférésének 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.

Megjegyzések:

- 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=sajatceg,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.

Közzététel

A Directory Server 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 információk LDAP szerveren való közzétételéhez rendelkezik beépített támogatással:

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 alkalmazás programozási felületen (API) keresztül teszi. Így az LDAP címtárat összehangolja a rendszer terjesztési címtárának változásaival.

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

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 kíván használni, és azt kívánja, hogy a meglévő operációs rendszer felhasználói képesek legyenek hitelesíteni magukat az operációs rendszeren használt jelszavukkal, a nem i5/OS felhasználókat pedig a címtárba saját kezűleg kívánja felvenni, akkor érdemes megfontolni a funkció használatát.

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 bejegyzéseihez 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.

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 NetServer nyomtatómegosztások adatai közzétételre kerülnek a beállított Active Directory szerveren. A nyomtatómegosztások Active Directory címtáron keresztüli közzétételének köszönhetően a felhasználók a System i nyomtatókat a Windows 2000 Nyomtató hozzáadása varázslójával felvehetik Windows 2000 asztali

gépeikre. Ahhoz, hogy a Nyomtató hozzáadása varázsló használható legyen, a nyomtatót a Windows 2000 Active Directory címtárában meg kell adni. A nyomtatómegosztásokat egy olyan címtárszerveren kell közzétenni, amely támogatja a Microsoft Active Directory sémáját.

TCP/IP Szolgáltatási minőség (QoS)
A TCP/IP szolgáltatási minőség (QoS) szerver beállítható úgy, hogy 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.

Kapcsolódó fogalmak

Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek
A Directory Server alkalmazás programozási felületekkel kapcsolatosan további információkat az Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek témakör tartalmaz.

Kapcsolódó feladatok

“Információk publikálása a címtárszervernek” oldalszám: 129
Az alábbi információk segítséget nyújtanak az információk Directory Server szerveren történő közzététele során.

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 replikációról:

Kapcsolódó fogalmak

“Replikációs feladatok” oldalszám: 146
Az alábbi információk segítséget nyújtanak a replikáció kezelése során.

“Replikált szerverek hálózatának átállítása” oldalszám: 98
Az alábbi információk segítséget nyújtanak akkor, ha replikált szerverekből álló hálózattal rendelkezik.

Replikáció áttekintés

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.

A replikáció két fő előnyt biztosít:

- Redundánsan tárolt információk - a másolatok a fő szerver biztonsági tartalékául 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 objektumosztállyal. Minden egyes részfa replikálása függetlenül történik. A részfa lefelé folytatódik a címtár-információs fán (DIT), egészen le a levél bejegyzésekig vagy más replikált részfákig. A replikált részfa gyökere alatti bejegyzések tárolják a replikációs topológia adatait. Ez egy vagy több replikacsoport bejegyzés, amelyek alatt a másolatok albejegyzései találhatók. Az egyes replika részbejegyzésekhez replikációs megállapodások vannak rendelve, amelyek azonosítják az ellátó (replikált) szervereket, valamint meghatározzák a hitelesítési adatokat és az ütemezés jellemzőit.

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) részfánkénti megadása

- Több elsődleges szerver, egyenrangú replikációhoz
- Átjáróreplikáció hálózatok között

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

1. táblázat: Szerverszerepek

Címtár	Leírás
Elsődleges/ egyenrangú	Az elsődleges/társszerver 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. 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. **Megjegyzések:** 1. Az elsődleges szerver replikálják a kliensektől érkező összes frissítést, de nem replikálják a más elsődleges szerverektől kapott frissítéseket. 2. Ha ugyanazon bejegyzés több szerveren is módosításra kerül, akkor inkonzisztenssé válhatnak a címtáradatok, mivel nincs mechanizmus az ütközések feloldására.
Lépcsőzetes felépítés (továbbítás)	Lépcsőzetesnek az olyan replikaszervert nevezzük, amely továbbreplikálja a neki küldött változásokat. Ez ellentétben áll az elsődleges/társszerverre épülő rendszerrel, ahol csak az elsődleges/társszerver replikálja a szerverhez csatlakozó kliensek módosításait. Egy lépcsőzetes szerver csökkentheti az elsődleges szerverek replikációs terhelését egy olyan hálózatban, amely sok, nagymértékben elosztott replikát tartalmaz.
Átjáró	Az átjáróreplikáció az átjárószervereket használja a replikációs információk hatékony összegyűjtésére és szétosztására a replikációs hálózatban. Az átráróreplikáció elsődleges előnye a hálózati forgalom mérséklése.
Replika (csak olvasható)	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 tartalékát is képezi.

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.

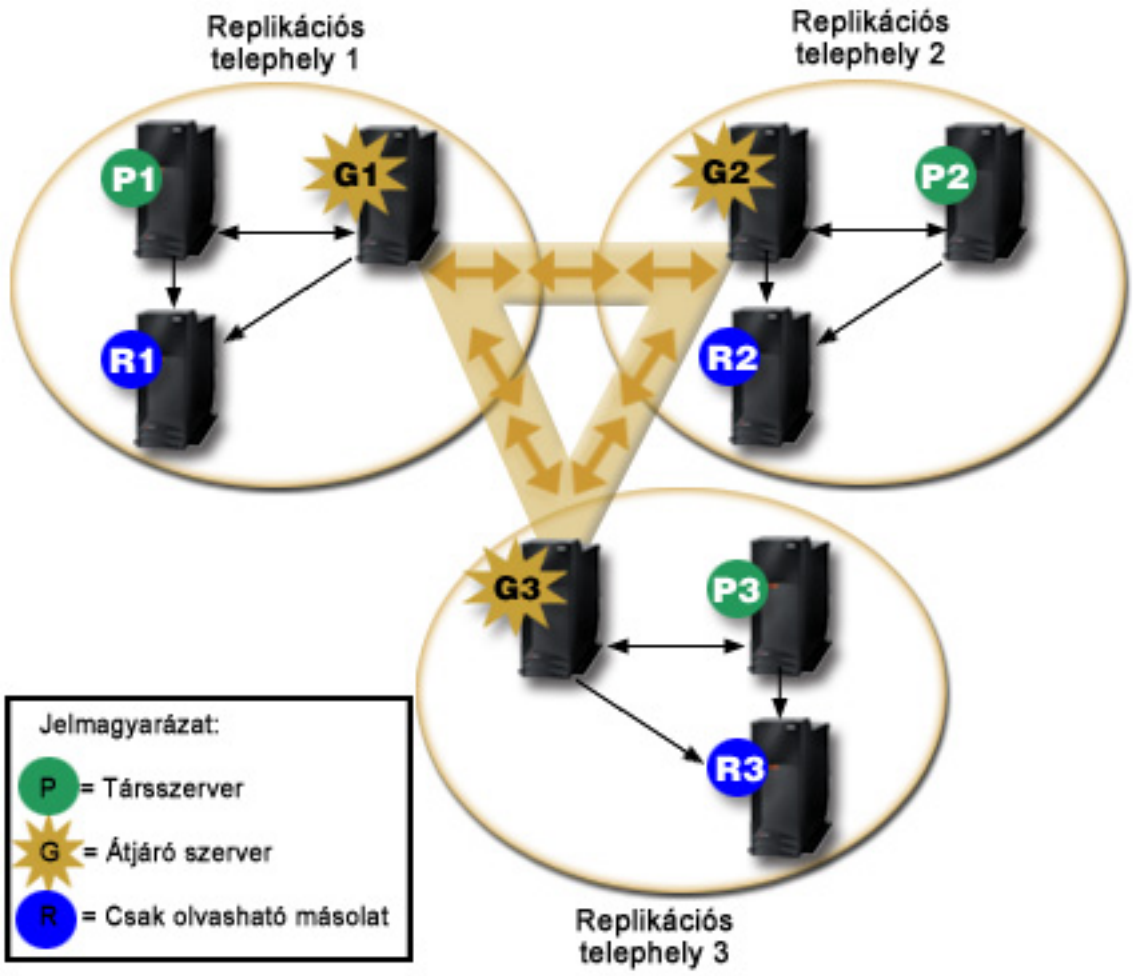
A replikaszerveren frissítések is kérhetők, de a frissítés ténylegesen az elsődleges szerverhez kerül továbbításra, visszaadva egy utalást a kliensre. Ha a frissítés sikeres, akkor az elsődleges szerver továbbküldi a frissített adatokat a replikáknak. A változások addig nem jelennek meg a kérést eredetileg 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 próbálkozni 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 átráróreplikáció elsődleges előnye a hálózati forgalom mérséklése. Az átjárószervereknek elsődleges (írható) szervereknek kell lenniük.

A következő ábrán az átjáróreplikáció működése látható:



3. 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. Egyúttal 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 átjárószervert. 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-objektumosztályt (ibm-replicaGateway), amely nem elsődleges, hibaüzenetet fog kapni.

Átjárószerver kétféleképpen hozható létre. Az alábbiakat teheti:

- Létrehozhat egy új átjárószervert
- Egy meglévő társszervert átjárószerverré alakíthat

Megjegyzés: Nagyon fontos, hogy replikációs helyenként csak egy átjárószervert rendeljen hozzá.

Replikációs ütközések feloldása

Több elsődleges szerverrel rendelkező hálózatokban előfordulhat, hogy egy bejegyzés ütköző módosítások következtében a szerver a módosítások replikálása után a bejegyzésre vonatkozóan eltérő adatokkal rendelkezik. Ütköző módosítások ritkán fordulnak elő, mivel a helyzet csak akkor állhat elő, ha eltérő elsődleges szervereken a módosítások megközelítőleg egyidejűleg mennek végbe. Ütköző módosítások például:

- Ha ugyanazt a bejegyzést két szerveren eltérő attribútumokkal veszi fel.
- Ha egy bejegyzés jelszavát két szerveren eltérő jelszó segítségével állítja vissza.
- Ha az egyik szerveren egy bejegyzést átnevez, miközben a bejegyzést egy másik szerveren módosítja.

Az IBM Tivoli Directory Server képes az ütköző módosításokat automatikusan felismerni, illetve feloldani, hogy ezáltal a szervereken található címtárak továbbra is konzisztensek maradjanak. Ha a rendszer replikációs ütközést észlel, akkor az ütköző módosítást a rendszer a szerver naplóban jelzi, illetve a módosítás a ″talált tárgyak″ naplófájlban is rögzítésre kerül, hogy ezáltal az adminisztrátorok az esetlegesen elveszett adatokat helyreállíthassák.

Egyenrangú replikáció esetében a hozzáadás és módosítás műveletek ütközésének feloldása a beviteli és módosítási időpecsét alapján történik. A több elsődleges szervert tartalmazó replikációs környezetekben az összes szerver között a legújabb időpecséttel rendelkező frissítés élvez elsőbbséget. Ha replikációs ütközés fordul elő, akkor a felülírt bejegyzés helyreállítási célból archiválásra kerül a talált tárgyak naplóban.

A replikált törlési és átnevezési kéréseket a szerver érkezési sorrendben fogadja el, az ütközések feloldása nélkül. Ha a replikációs ütközés törlés vagy modifyDN (átnevezés vagy áthelyezés) műveletet érint, akkor lehetséges, hogy felhasználói beavatkozást igénylő hiba áll elő. Ha például egy bejegyzés az egyik szerveren átnevezésre kerül, miközben egy másik szerveren módosítják, akkor lehetséges, hogy a modifyDN művelet a replikára a módosítási művelet előtt érkezik meg. Ezt követően a módosítási művelet - amikor a szerverre megérkezik - meghiúsul. Ebben az esetben az adminisztrátornak válaszolnia kell a hibára, vagyis az új DN felhasználásával a bejegyzést érintő módosításokat végre kell hajtania. A módosítások - a megfelelő névvel történő - ismételt végrehajtásához szükséges minden információ a replikációs és hibanaplóban kerül megtartásra. Az ilyen és ehhez hasonló replikációs hibák a megfelelően beállított replikációs topológiákban ritkán fordulnak elő, azonban nem tanácsos feltételezni, hogy sosem fordulnak elő.

Ha ugyanazt a bejegyzést több szerver is frissíti, akkor ez a címtáradatok inkonzisztenciájához vezethet, mivel az ütközés feloldás a bejegyzések időpecsétje alapján történik. Elsőbbséget a legújabb időpecsét élvez. Ha a szervereken található adatok inkonzisztenssé válnak, akkor a szerverek újraszinkronizálásával kapcsolatos további információkért tekintse meg a kapcsolódó hivatkozások alatt található ldapdiff témakört.

A replikációs ütközések feloldása megköveteli, hogy az ellátó megadja azt az időpecsétet, mielőtt a bejegyzés az ellátón frissítésre került. Az IBM Tivoli Directory Server for i5/OS V5R4 és ezt megelőző változatai nem képesek ezt az információt biztosítani. Ennek következtében a replikációs ütközés feloldása nem alkalmazható olyan esetekben, amikor az ellátó alacsonyabb szintű szerver. A V6R1 változatban az IBM Tivoli Directory Server for i5/OS fogyasztó szerver - ebben az esetben - elfogadja a replikált időpecsétet, majd az időpecsétet az ütközések ellenőrzése nélkül frissíti, illetve alkalmazza.

Megjegyzés: Az IBM Tivoli Directory Server for i5/OS korábbi változatai az időpecsét-alapú ütközés feloldást nem támogatják. Ha a topológia az IBM Tivoli Directory Server for i5/OS korábbi változatait tartalmazza, akkor a hálózaton az adatok konzisztenciája nem biztosított.

Az ütköző módosítások elkerülhetők terheléskiegyenlítő, virtuális IP cím átvétel, illetve egyéb olyan módszerek alkalmazásával, amelyek biztosítják, hogy a címtárat érintő módosítások egy szerveren kerülnek végrehajtásra, miközben automatikus átállást biztosítanak egyéb szerverekre akkor, ha az előnyben részesített szerver nem elérhető.

A terheléskiegyenlítő (például IBM WebSphere Edge Server) olyan virtuális hosztnévvel rendelkezik, amelyet az alkalmazások a címtár-frissítések továbbítására használnak. A terheléskiegyenlítő úgy kerül beállításra, hogy a frissítéseket csak egyetlen szerver felé továbbítsa. Ha a szerver offline állapotú vagy hálózati meghibásodás nem elérhető, akkor a terheléskiegyenlítő a frissítéseket a soron következő elsődleges szervernek küldi el mindaddig, amíg az első szerver ismét online és elérhető nem lesz. A terheléskiegyenlítő szerver telepítésével és beállításával kapcsolatosan információkat a terheléskiegyenlítő termék dokumentációja tartalmaz.

Kapcsolódó feladatok

"Talált tárgyak napló beállításai" oldalszám: 164
A talált tárgyak napló (LostAndFound.log az alapértelemzett fájlnév) a replikációs ütközések eredményeként fellépő hibákat rögzíti. A talált tárgyak napló szabályozásához rendelkezésre állnak beállítások, a fájl helyének és maximális méretének megadását, valamint a régi naplófájlok archiválásának lehetőségét is beleértve.

"Egyszerű topológia létrehozása egyenrangú replikációval" oldalszám: 153
Az egyenrangú replikáció egy olyan replikációs topológia, amelyben több szerver is elsődleges. Az egyenrangú replikációt csak olyan környezetekben használja, amelyben a frissítési vektorok jól ismertek.

Kapcsolódó hivatkozás

"ldapdiff" oldalszám: 245
Az LDAP replikaszinkronizálási parancssori segédprogram.

Replikációs szakkifejezések

A replikáció leírása során használt bizonyos szakkifejezések definíciója.

Lépcsőzetes replikáció
Szerverek több rétegéből 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 társszerver által küldött összes változást. A kliensek frissítési kérései esetén utalás történik az elsődleges vagy társszerverre.

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 objektumosztállyal,

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 replikaszerver, amely egymás replikálására van beállítva.

Ütemezés
A replikáció ütemezhető, hogy csak meghatározott időközönként történjen, és az ellátón addig felgyűlt 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.

Több szálon futó replikáció

Több szálon futó (aszinkron) replikáció esetén a replikáció - a replikáció átfogó teljesítményének javítása érdekében - használhat több szálat.

Egy szálon futó (szinkron) replikáció használata esetén elképzelhető, hogy a kliensek következetesen gyorsabban végeznek frissítéseket, mint hogy a replikáció el tudná küldeni a változtatásokat a szerver számára. Ennek oka, hogy a szabványos replikációs modell egy szálat használ az összes változás beérkezési sorrendben történő replikálásához.

A szabványos replikációs modell bizonyos típusú hibák esetén is leáll, ha például egy replikált módosítás kérés meghiúsul, mert a célbejegyzés nem létezik a fogyasztó szerveren. Ez a viselkedés felhívja a figyelmet a szerverek közötti ellentmondásokra, amelyeket ki kell javítani, azonban a függőben lévő változások lemaradásának növekedéséhez vezethet. Bizonyos alkalmazások esetén szükség lehet a nem replikált változások lemaradásának kiküszöbölésére.

Ennek megoldása érdekében a több szálon futó replikáció lehetővé teszi a meghiúsult változásokkal kapcsolatos információk naplózását egy hibanaplóba, majd a fennmaradó változások elvégésének folytatását. A napló elegendő információt biztosít a kihagyott változásokat, valamint annak meghatározásához, hogy mely bejegyzések ellentmondásosak, valamint biztosítja a hibák kijavítása után a változások újbóli megkísérlésére szolgáló eszközöket.

Annak megakadályozása érdekében, hogy nagy ellentmondások miatt nagy számú változtatás kihagyására kerüljön, egy beállítható hibaküszöb biztosított. Ennek elérése esetén a replikáció leáll, amíg a hibák kijavításra, a replikációs hibanapló pedig kiürítésre nem kerül.

- A több szálon futó (aszinkron) replikáció felügyelete bonyolult lehet, ha a szerverek és hálózatok nem megbízhatók, ezáltal számos replikált változás kihagyásra kerülhet.

A hibák fellépés estén naplózásra kerülnek és az adminisztrátor újraküldheti azokat, de a hibanaplókat gondosan meg kell figyelni. A következő keresés bemutatja az egy szerver által biztosított összes megállapodás replikációs lemaradását:

```
ldapsearch -h supplier-host -D cn=admin -w ? -s sub
   objectclass=ibm-replicationagreement
   ibm-replicationpendingchangecount ibm-replicationstate
```

Ha a replikációs állapot aktív és a függőben lévő szám növekszik, akkor a lemaradás nem csökken, hacsak nem csökken a frissítési sebesség vagy a replikációs mód meg nem változik szinkronról aszinkronra (több szálon futó).

A replikáció az elsődleges szerverre is terhelést ró, amelyen a frissítések elsőként alkalmazásra kerülnek. A címtáradatok másolatának frissítésén felül az elsődleges szervernek el kell küldenie a változásokat az összes replikaszerver számára. Ha az alkalmazás vagy a felhasználók nem függenek az azonnali replikációtól, akkor replikáció csúcsidőt elkerülő, körültekintő ütemezésével minimalizálható az elsődleges szerver teljesítményére gyakorolt hatás.

Több szálon futó replikáció esetén replikációs hiba fellépésekor a következő történik:

- ibm-slapdReplMaxErrors: A 0 azt jelenti, hogy nem kell hibát naplózni a replikációs hibanaplóban, de a hibák bekerülnek a szervernaplóba és a replikáció felfüggesztésre kerül, amíg az összes hiba törlésre nem kerül.
- Ha egy megállapodás hibáinak száma meghaladja a korlátot, akkor a replikáció felfüggesztésre kerül, amíg legalább egy hiba törlésre nem kerül, vagy a megállapodás hibaszámának korlátját meg nem növelik.
- A replikációs megállapodás állapota:

```
ibm-replicationStatus: hibanaplõ tele
```

Replikációs hibatábla

A replikációs hibatábla a meghiúsult frissítéseket rögzíti a későbbi helyreállítás céljából. A replikáció kezdetekor a rendszer összeszámolja az összes replikációs megállapodással kapcsolatos meghibásodás számát. Ez a szám akkor növekszik, ha egy frissítés meghiúsul, és ezáltal a tábla új bejegyzéssel bővül.

A replikációs hibatábla bejegyzései az alábbi információkat tartalmazzák:

- A replikációs megállapodás azonosítója.
- A replikációs módosítás azonosítója.
- A frissítésre tett kísérlet időpontjának időpecsétje.
- A kísérletek száma (alapértelmezésben értéke 1, de minden újabb kísérlet esetén 1-gyel nő).
- A fogyasztótól származó eredménykód.
- A frissítéssel kapcsolatos, a replikációs műveletből származó valamennyi információ (például a DN, a tényleges adatok, vezérlőelemek, kapcsolók stb.).

Ha a szerverkonfiguráció ibm-slapdReplMaxErrors attribútumának értéke 0, akkor a replikáció a frissítések feldolgozását nem állítja le. Az ibm-slapdReplMaxErrors attribútum a replikáció konfigurációs bejegyzésének dinamikusan módosítható attribútuma.

Ha az ibm-slapdReplMaxErrors attribútum által megadott érték 0-nál nagyobb, akkor ha a replikációs megállapodás hibaszáma az adott értéket meghaladja, akkor a replikáció végrehajtja az alábbiak valamelyikét:

- **Egy szálon futó**: A replikáció belép egy ciklusba, és megkísérli a meghiúsult frissítés replikációját.
- **Több szálon futó**: A replikációt a rendszer felfüggeszti.

Ha a szervert egy kapcsolat használatára állította be, akkor egy 60 másodperces várakozást követően a replikáció ugyanazt a frissítést megpróbálja ismét elküldeni, majd mindaddig újra próbálkozik, ameddig a frissítés nem sikerül, illetve az adminisztrátor a frissítés kihagyása mellett nem dönt.

A több kapcsolat használatára beállított szerverek esetében a megállapodásra vonatkozó replikáció felfüggesztésre kerül. A fogadó szálak továbbra is lekérdezik az esetlegesen elküldött frissítések állapotát, de további frissítések nem kerülnek replikálásra. A replikáció folytatásához a címtár-adminisztrátornak a megállapodásra vonatkozó hibák közül legalább egyet törölnie kell, vagy a szerverkonfiguráció dinamikus módosításával a korlátot növelnie kell.

További információkat az alábbi kapcsolódó témakörök Replikációs sorok kezelése témaköre tartalmaz. Ezen kívül tekintse meg az ldapexop témakörben található -op controlreplerr paraméter témakört is az alábbi kapcsolódó hivatkozások között.

Kapcsolódó feladatok

"Replikációs sorok kezelése" oldalszám: 163
Az alábbi információk segítséget nyújtanak a szerver által használt replikációs megállapodások (sorok) állapotának megfigyelése során.

Kapcsolódó hivatkozás

"ldapexop" oldalszám: 223
Az LDAP kiterjesztett művelet parancssori segédprogram.

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 névattribútuma.
- 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″ lekérhetők 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.

Az egy szálon futó replikációs módszert használó replikációs megállapodások esetében a fogyasztókapcsolatok száma mindig egy, és az attribútumérték figyelmen kívül marad. A több szálon futó replikációt használó megállapodások esetében a kapcsolatok száma 1 és 32 között állítható be. Ha a megállapodásnak értéket nem ad meg, akkor a fogyasztói kapcsolatok számát a rendszer 1-re állítja be.

Megjegyzés: A cn=ibmpolicies részfa esetében az összes replikációs megállapodás az egy szálon futó replikációs módszert használja, egy fogyasztó kapcsolattal, és az attribútumérték figyelmen kívül marad.

Hogyan tárolódnak a replikációs információk a szerveren?

A replikációs információk a címtárban több helyen kerülnek tárolásra.

- 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=sajat ceg″ egy replikált részfa teteje, akkor egy ″ibm-replicagroup=default″ nevű objektum kerül közvetlenül alatta létrehozásra (ibm-replicagroup=default,o=sajat ceg). 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.
- Egy ″cn=replication,cn=IBMpolicies″ nevű objektum tartalmazza a többi szerverre replikált információkat.

Biztonsági megfontolások a replikációs információkkal kapcsolatban

Tekintse át a bizonyos objektumokkal kapcsolatos biztonsági tényezőket.

- 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 érhessék 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 replikáció használatával a Directory Server magasszintű rendelkezésre állást biztosítóvá tehető, mégpedig kétféleképpen: az IBM Load Balancer használatával, illetve az IP cím átvétellel. A témával kapcsolatosan további információkat az *IBM WebSphere V5.1 Performance, Scalability, and High Availability* IBM Redbooks kiadvány 13.2-es fejezete tartalmaz.

Kapcsolódó tájékoztatás

IBM WebSphere 5.1 teljesítmény, méretezhetőség és magas szintű rendelkezésre állás

Tartományok és felhasználói sablonok

A webes adminisztrációs eszköz tartomány és felhasználói sablon objektumainak célja, hogy megkönnyítse a felhasználók dolgát azáltal, hogy nem kell az LDAP rendszer alapvető kérdéseivel részletesen foglalkozniuk.

Egy tartomány felhasználók és csoportok gyűjteménye. Egy lapos címtárstruktúrában megadja, hol találhatók 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.

Kapcsolódó fogalmak

“Tartomány- és felhasználói sablon feladatok” oldalszám: 204
Az alábbi információk segítséget nyújtanak a tartományok és felhasználói sablonok kezelése során.

Kapcsolódó feladatok

“Tartomány létrehozása” oldalszám: 204
Az alábbi információk segítséget nyújtanak a tartományok létrehozása során.

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
- Álnévhivatkozás-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 részhalmaza (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 szolgálva. A rendszergazda korlátozhatja ennek használatát azzal, hogy csak az adminisztrátorok számára teszi elérhetővé.

Rendezett keresés

A rendezett keresés eredményeit a kliens egy feltétellista 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.

Álnévhivatkozás-feloldás letiltása

Egy alias vagy aliasObject objektumosztállyal rendelkező címtárbejegyzés tartalmazza az aliasedObjectName attribútumot, amellyel a címtár másik bejegyzésére lehet hivatkozni. Hogy az álnevek feloldásra kerüljenek-e, az csak keresési kérésekben adható meg. A *feloldás* az álnév visszakövetését jelenti az eredeti bejegyzésig. A **mindig** vagy **kereséskor** álnévhivatkozás-feloldási beállításokkal rendelkező IBM Directory Server keresési válaszideje jelentősen hosszabb lehet, mint a **soha** beállítással rendelkezőé, még akkor is, ha a címtárban nincsenek álnévbejegyzések. Két beállítás határozza meg a szerver álnévhivatkozás-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 álnévhivatkozás-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 álnévhivatkozás-feloldás kivonatos működését:

2. táblázat: Tényleges álnévhivatkozás-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 felhasználókénál 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 kéréséi, 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-csoporthoz 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 alat 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 bejegszéseknek prioritásuk van az IBMpolicies alattiakkal szemben.

Kapcsolódó fogalmak

“Keresésikorlát-csoport feladatok” oldalszám: 135
Az alábbi információk segítséget nyújtanak a keresésikorlát-csoportok kezelése során.

Kapcsolódó feladatok

“Keresési beállítások módosítása” oldalszám: 128
Az alábbi információk segítséget nyújtanak a felhasználó keresési képességeinek vezérlése során.

“Címtárbejegyzések keresése” oldalszám: 198
Az alábbi információk segítséget nyújtanak a címtárbejegyzések keresése során.

Nemzeti nyelvek támogatása (NLS)

Az NLS tényezők adatformátumokat, karaktereket, leképezési módszereket és a karaktersorozat kis- és nagybetűs formájának meghatározását foglalják magukban.

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).

Kapcsolódó tájékoztatás

i5/OS globalizáció
Az NLS szempontjából fontos tényezőkkel kapcsolatosan további információkat az i5/OS globalizáció témakör tartalmaz.

Nyelvi címkék

A *nyelvi címkék* meghatározzák azt a mechanizmust, amelynek segítségével a Directory Server a természetes nyelvek kódjait a címtárban tárolt értékekhez rendelheti és a kliensek lekérdezhetik a bizonyos természetes nyelvi feltételeknek megfelelő értékeket.

A nyelvi címke egy attribútumleírás egyik összetevője. A nyelvi címke 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 nyelvi címkékben a kis- és a nagybetűk nem számítanak eltérőknek; 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

Kapcsolódó feladatok

“Nyelvi címkékkel ellátott attribútumokat tartalmazó bejegyzés hozzáadása” oldalszám: 195
Az alábbi információk segítséget nyújtanak a nyelvi címkékkel ellátott attribútumokat tartalmazó bejegyzések hozzáadása során.

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 utalás használható. 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 objektumai csak egy megkülönböztető nevet (dn), egy objektumosztályt (objectClass), illetve egy utalás (ref) attribútumot tartalmazhatnak. A korlátozást az ldapsearch parancsnál bemutatott példa szemlélteti.

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.

Kapcsolódó feladatok

“Szerver kijelölése címtári utalások részére” oldalszám: 123
Az alábbi információk segítséget nyújtanak az utalási szerverek meghatározása során.

Kapcsolódó hivatkozás

“ldapsearch” oldalszám: 234
Az LDAP keresés parancssori segédprogram.

Tranzakciók

A Directory Server beállítható úgy, hogy megengedje a klienseknek tranzakciók használatát. 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 szervezetten 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 részelemei:

- hozzáadás
- 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.

Kapcsolódó feladatok

“Tranzakciós beállítások megadása” oldalszám: 122
Az alábbi információk segítséget nyújtanak a Directory Server tranzakciós beállításainak megadása során.

Directory Server biztonság

Ismerje meg azokat a funkciókat, amelyeknek köszönhetően a Directory Server biztonságosabbá tehető.

A Directory Server biztonságával az alábbi témakörök foglalkoznak:

Kapcsolódó fogalmak

“Címtárak” oldalszám: 4
A Directory Server (címtárszerver) segítségével egy olyan adatbázistípus érhető el, amely az információkat az i5/OS integrált fájlrendszerének felépítéséhez hasonló, hierarchikus struktúrába szervezve tárolja.

“Megkülönböztetett nevek (DN)” oldalszám: 9
A címtár minden bejegyzésének vagy egy megkülönböztetett neve (DN). A DN az a név, amelyik egyedi módon azonosítja a címtárbejegyzést. A DN első elemét szokás relatív megkülönböztetett névként (Relative Distinguished Name, RDN) emlegetni.

“Biztonsági tulajdonság feladatok” oldalszám: 174
Az alábbi információk segítséget nyújtanak a biztonsági tulajdonság feladatok kezelése során.

Kapcsolódó feladatok

“Directory Server objektumfelügyelet engedélyezése” oldalszám: 127
Az alábbi információk segítséget nyújtanak a Directory Server objektumfelügyelet engedélyezése során.

Felülvizsgálat

A felülvizsgálat segítségével nyomon követhetők bizonyos Directory Server tranzakciók részletei.

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

- 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, illetve a megkülönböztető nevek (DN) 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 értékben *OBJAUD került beállításra, akkor az objektumok naplózása a System i navigátor segítségével engedélyezhető.

A felülvizsgálathoz csoport nevek adhatók meg. A jogosult kliensek kérhetik, hogy egy művelet a szerver által a kliens azonossághoz rendelt csoportok jogosultsága helyett a kliens által meghatározott csoportok jogosultságát használja. A beállítás meghatározza, hogy a kérések felülvizsgálata csak jelzi azt, hogy a kliens meghatározta a használandó csoportokat, vagy pedig ténylegesen tartalmazza a meghatározott csoportok listáját. A csoportlista felülvizsgálata további felülvizsgálati bejegyzéseket hoz létre, amelyek az egyes kérésekhez tartalmazzák a csoportok listáját is.

Annak meghatározásához, hogy a csoportnevek felülvizsgálatra kerüljenek-e, tegye a következőket:

1. A System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Tulajdonságok** menüpontot.
5. A **Felülvizsgálat** lapon jelölje be a **Hívó által meghatározott csoportok felülvizsgálatakor tartalmazza a csoportok nevét is** jelölőnégyzetet.

Kapcsolódó fogalmak

“Elosztott címtárak” oldalszám: 7
Az elosztott címtár olyan címtár környezet, amelyben az adatok több címtárszerver között particionáltak. Ahhoz, hogy az elosztott címtárak a kliens alkalmazások felé egy könyvtárként jelenjenek meg, a rendszer néhány proxy szervert biztosít, amelyek ismerik az összes szervert, illetve az egyes szervereken tárolt adatokat.

Kapcsolódó feladatok

“Directory Server objektumfelügyelet engedélyezése” oldalszám: 127
Az alábbi információk segítséget nyújtanak a Directory Server objektumfelügyelet engedélyezése során.

Kapcsolódó tájékoztatás

Biztonsági kézikönyv

Biztonsági felülvizsgálatok
A felülvizsgálattal kapcsolatosan további információkat a Biztonsági felülvizsgálatok témakör tartalmaz.

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) biztonsági eljárást.

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.

Az SSL használatához a rendszeren telepíteni kell a Digitális igazolás kezelőt (az i5/OS 34-es lehetősége). A DCM program lehetővé teszi, hogy digitális igazolásokat állítson elő, kezeljen és tároljon.

A TLS az SSL utódául készült, és ugyanazt a kriptográfiai eljárást használja, de több kriptográfiai algoritmust támogat. 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 TSL-t:

1. A Directory Servernek beállítva kell lennie a TLS vagy SSLTLS használatára.
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.

Kapcsolódó feladatok

"SSL és TSL engedélyezése a Directory Serveren" oldalszám: 180
Az alábbi információk segítséget nyújtanak SSL és TSL Directory Server szerveren történő engedélyezése során.

"SSL és TSL engedélyezése a Directory Serveren" oldalszám: 180
Az alábbi információk segítséget nyújtanak SSL és TSL Directory Server szerveren történő engedélyezése során.

"Az SSL védelem LDAP parancssori segédprogramok használata" oldalszám: 248
Az alábbi információk segítséget nyújtanak az SSL és LDAP parancssori segédprogramokok együttes használatának megértésében.

Kapcsolódó tájékoztatás

Digitális igazolás kezelő

Védett socket réteg (SSL)

Támogatott SSL és Szállítási réteg biztonság (TLS) protokollok

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 és szerver alkalmazások számára.

Kerberos hitelesítés engedélyezéséhez konfigurálni kell a hálózati hitelesítési szolgáltatást.

A Directory Server Kerberos szolgáltatása támogatja a GSSAPI SASL eljárást. 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 hosztnév 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 címtáradatok 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.

Kapcsolódó tájékoztatás

Hálózati hitelesítési szolgáltatás
A Kerberos hitelesítéssel kapcsolatosan további információkat a Hálózati hitelesítési szolgáltatás témakör tartalmaz.

Hálózati hitelesítési szolgáltatás beállítása
Információkat azzal kapcsolatosan, hogy a kulcscímke (keytab) fájlokhoz információk milyen módon adhatók hozzá, a Hálózati hitelesítési szolgáltatás beállítása témakör tartalmaz.

Jelszótitkosítás

Az IBM Tivoli Directory Server segítségével megakadályozható, hogy a felhasználói jelszavakhoz jogosulatlan személyek hozzáférhessenek. Az adminisztrátor beállíthatja a szervert úgy, hogy a userPassword attribútum értékeit egy- vagy kétirányú titkosítási formátumban titkosítsa. A titkosított jelszavakat a rendszer megjelöli a titkosítási algoritmus nevével, tehát a különböző formátumban titkosított jelszavak a címtárban egymás mellett tárolhatók. A titkosítási konfiguráció módosításakor a meglévő titkosított jelszavak változatlanok maradnak, és továbbra is használhatók.

Az egyirányú titkosítási formátumok használata esetében a felhasználói jelszavak titkosíthatók, majd a címtárban tárolhatók, amelynek köszönhetően megakadályozható, hogy a titkosítatlan jelszavakhoz a felhasználók (az adminisztrátorokat is beleértve) hozzáférjenek. A kétirányú titkosítási formátumok használata esetében a jelszavak az adatbázisban tárolás során kerülnek titkosításra, illetve a jogosult kliens felé továbbításkor kerülnek visszafejtésre. A kétirányú titkosítás védi az adatbázisban tárolt jelszót, miközben támogatja a különféle (például DIGEST-MD5) hitelesítési módszereket, amelyek megkövetelik, hogy a szerver a titkosítatlan jelszóhoz hozzáférjen, illetve támogatja az olyan alkalmazásokat, amelyeknek a titkosítatlan jelszóhoz hozzá kell férniük.

Az egyirányú titkosított jelszavak jelszóegyeztetésre ugyan használhatók, azonban nem fejthetők vissza. A felhasználó bejelentkezése során a bejelentkezési jelszó titkosításra kerül, majd a rendszer a titkosított jelszót ellenőrzés céljából összehasonlítja a tárolt változattal.

Még akkor is, ha a szervert úgy állították be, hogy az új jelszavakat egy adott formátumban tárolja, a szerver elfogadja a korábban eltérő módszerrel titkosított jelszavakat. A szerver például beállítható az AES256 jelszótitkosítás használatára, de közben lehetővé teheti, hogy az adminisztrátor egy másik, SHA-1 módszerrel titkosított jelszavakat tartalmazó szerverről származó adatokat betöltsön. Az egyszerű jelszó-hitelesítésnek köszönhetően a szerver felé hitelesítésre mindkét jelszókészlet használható, azonban az SHA-1 jelszavak titkosított karaktersorozatként kerülnek visszaadásra és a DIGEST-MD5 hitelesítéssel nem használhatók.

Egyirányú titkosítási formátumok:
- SHA-1
- MD5
- crypt

A szerver beállítását követően az (új felhasználók) új jelszavai, illetve a (meglévő felhasználók) módosított jelszavai még azt megelőzően titkosításra kerülnek, hogy a rendszer azokat a címtár-adatbázisban eltárolná. A további LDAP keresések megjelölt és titkosított értéket adnak vissza.

A titkosítatlan jelszavak lekérését igénylő alkalmazások (például középrétegbeli hitelesítő ügynökök) esetében a címtár adminisztrátorának a szervert úgy kell beállítania, hogy a felhasználói jelszavakon kétirányú titkosítást hajtson végre. Ebben az esetben a szerver által visszaadott titkosítatlan jelszavakat a címtár ACL mechanizmusa védi.

Kétirányú titkosítási formátumok:
- Nincs
- AES

A rendszer által biztosított AES kétirányú titkosítási lehetőségnek köszönhetően a userPassword attribútum értékei a címtárban titkosíthatók, majd az eredeti titkosítatlan formátumú bejegyzés részeként kérhetők le. Az AES beállítható 128, 192, illetve 256 bites kulcshossz használatára. Bizonyos alkalmazások (például középrétegbeli hitelesítési szerverek) megkövetelhetik, hogy a jelszavak titkosítatlan szövegként kerüljenek visszaadásra, azonban előfordulhat,

hogy a vállalati biztonsági irányelvek nem teszik lehetővé a titkosítatlan jelszavak tárolását másodlagos állandó tárolókban. Ez a lehetőség mindkét követelménynek eleget tesz.

Továbbá az AES jelszótitkosítás replikált hálózatban történő felhasználása esetén ha az összes szerver azonos AES jelmondat és módosító érték használatára van beállítva, akkor a jelszóadatok titkosított formájukban kerülnek replikálásra, amely a jelszóadatoknak nagyobb védelmet biztosít. Ha az egyik szerver az AES titkosítást nem támogatja, vagy a többitől eltérő AES információkat használ, akkor a jelszavak - visszafejtés után - titkosítatlan szövegként kerülnek replikálásra.

Megjegyzés:

1. Az AES a V6R1 változatnál korábbi LDAP szervereken nem támogatott. Pontosabban az AES módszerrel titkosított adatok használata a V6R1 változatnál korábbi LDAP szervereken nem támogatott.
2. Ha egyéb platformok esetében a ″Nincs″ lehetőséget választja ki, akkor az adatbázisban a titkosítatlan jelszavak kerülnek tárolásra. Ha a szerver olyan hálózat részét képezi, amely egyéb platformokon futó IBM Tivoli Directory Server szervereket tartalmaz, akkor tanácsos az AES titkosítási lehetőségek használatát megfontolni.

Az egyszerű csatlakozás akkor lesz sikeres, ha a csatlakozási kérésben megadott jelszó megegyezik a userPassword attribútum értékeinek egyikével.

Ha a szervert a webes adminisztráció segítségével állítja be, akkor az alábbi titkosítási lehetőségek közül választhat:

Nincs A jelszavak kétirányú módszerrel titkosítva kerülnek tárolásra egy ellenőrzési listában, illetve lekérésre az eredeti, titkosítatlan formátumú bejegyzés részeként kerülnek. A beállítás használatához a QRETSVRSEC rendszerváltozót 1 értékre kell állítani.

crypt A rendszer a jelszavakat - mielőtt a címtárban eltárolásra kerülnének - a UNIX crypt titkosítási algoritmus segítségével titkosítja. A crypt használata esetében csak a jelszó első 8 karaktere kerül felhasználásra. A 8 karakternél hosszabb jelszavakat a rendszer csonkolja.

MD5 A rendszer a jelszavakat - mielőtt a címtárban eltárolásra kerülnének - az MD5 kivonatoló titkosítási algoritmus segítségével titkosítja.

SHA-1 A rendszer a jelszavakat - mielőtt a címtárban eltárolásra kerülnének - az SHA-1 titkosítási algoritmus segítségével titkosítja.

AES128
A rendszer a jelszavakat - mielőtt a címtárban eltárolásra kerülnének - az AES128 algoritmus segítségével titkosítja. A jelszavak lekérésre az eredeti, titkosítatlan formátumú bejegyzés részeként kerülnek.

AES192
A rendszer a jelszavakat - mielőtt a címtárban eltárolásra kerülnének - az AES192 algoritmus segítségével titkosítja. A jelszavak lekérésre az eredeti, titkosítatlan formátumú bejegyzés részeként kerülnek.

AES256
A rendszer a jelszavakat - mielőtt a címtárban eltárolásra kerülnének - az AES256 algoritmus segítségével titkosítja. A jelszavak lekérésre az eredeti, titkosítatlan formátumú bejegyzés részeként kerülnek.

Megjegyzés: A korábbi kiadásokban rendelkezésre álló imask formátum a titkosítás esetében már nem elérhető. Azonban az imask által titkosított értékek továbbra is működnek.

A Tivoli Directory Server for i5/OS alapértelmezett lehetősége az SHA-1, amely kompatibilis a korábbi kiadásokkal, és nem követeli meg AES jelmondat és módosító érték beállítását.

A userPassword mellett a secretKey attribútum értékei AES256 felhasználásával mindig titkosításra kerülnek a címtárban. A userPassword attribútummal szemben a rendszer a secretKey esetében a titkosítási módszert kikényszeríti, vagyis más lehetőséget nem biztosít. A secretKey attribútum egy IBM által meghatározott séma. Az

| alkalmazások az attribútum segítségével olyan érzékeny adatokat tárolhatnak, amelyeket a címtárban folyamatosan titkosítva kell tárolni, illetve az adatokat - a címtár hozzáférés felügyeletének köszönhetően - titkosítatlan formátumban lekérhetik.

| Ha a titkosítás típusát a parancssor segítségével kívánja módosítani (például **crypt** titkosításra kívánja állítani), akkor adja ki a következő parancsot:

```
ldapmodify -D <adminDN> -w <adminPW> -i <fájlnév>
```

| ahol a <fájlnév> a következőt tartalmazza:

```
dn: cn=configuration
changetype: modify
replace: ibm-slapdPWEncryption
ibm-slapdPWEncryption: crypt
```

| Ha a frissített beállításokat dinamikusan kívánja hatályba léptetni, akkor adja ki a következő ldapexop parancsot:

```
ldapexop -D <adminDN> -w <adminPW> -op readconfig -scope single
"cn=configuration" ibm-slapdPWEncryption
```

| **Megjegyzés:** A konfiguráció módosításához egy *ALLOBJ és *IOSYSCFG különleges jogosultsággal rendelkező i5/OS felhasználói profilhoz tartozó leképezett felhasználói DN és jelszó segítségével kell magát hitelesítenie. A szerverkonfiguráció módosításához az egyéb felületek esetében is ilyen jogosultság szükséges.

| **Kapcsolódó feladatok**

| “Jelszó-irányelv tulajdonságok beállítása” oldalszám: 175
| Az alábbi információk segítséget nyújtanak a jelszó-irányelvek tulajdonságainak beállítása során.

Csoportok és szerepek

A csoportok és szerepek segítségével a tagok hozzáférését és jogosultságait rendszerezheti.

A csoportok lényegében listák, nevek gyűjteménye. A csoportok az **aclentry**, **ibm-filterAclEntry** és **entryowner** attribútumokban használhatók a hozzáférés vezérlésére, vagy alkalmazásspecifikus feladatokra, mint például a levelezőlisták. A csoportok lehetnek statikusak, dinamikusak és egymásba ágyazottak.

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

További információk:

Kapcsolódó fogalmak

“Hozzáférés-felügyeleti listák” oldalszám: 65
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.

“Felhasználói és csoportfeladatok” oldalszám: 200
Az alábbi információk segítséget nyújtanak a felhasználók és csoportok kezelése során.

Kapcsolódó feladatok

“Csoportok hozzáadása” oldalszám: 202
Az alábbi információk segítséget nyújtanak a csoportok hozzáadása során.

“Csoportok létrehozása” oldalszám: 207
Az alábbi információk segítséget nyújtanak a csoportok létrehozása során.

Statikus csoportok:

A statikus csoportok tagjaikat az egyedi tagok felsorolásával határozzák meg.

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 tagjaikat LDAP keresés segítségével határozzák 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**. 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 searchfilter szintaxisával kapcsolatosan további információkat az ldapsearch szűrő beállításai témakör tartalmaz. 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 hosztnevet 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 találhatók 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 csoportbejegyzésben. 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:

A hibrid csoporttagság a statikus, dinamikus és beágyazott tagtípusok kombinációjával írható le.

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
```

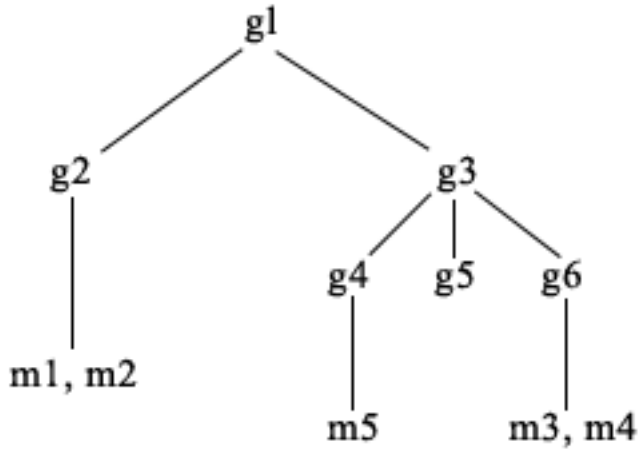
Csoporttagság meghatározása:

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 ős 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.

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:

A beágyazott és dinamikus csoportok objektumosztályainak felsorolása.

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** attribútumnak legalább 1 tagot meg kell adnia.

Csoport attribútum típusok:

A csoportattribútum-típusok felsorolása.

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=sajat ceg″ tagja-e a ″cn=system administrators, o=sajat ceg″ csoportnak:

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

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=sajat ceg″ tagja-e a ″cn=system administrators, o=sajat ceg″ csoportnak:

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

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 szerepalapú hitelesítés a csoportalapú hitelesítés konceptuális kiegészítése.

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 elsőre, 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.

Adminisztrátori hozzáférés

Az adminisztrátori hozzáférés segítségével vezérelhető az adott adminisztrációs feladatok elérhetősége.

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 jogosultsággal módosíthatja a címtárbeállításokat az LDAP csatolók (a cn=configuration subtree vagy a webes adminisztrációs eszköz ″Szerveradminisztráció″ feladatai) segítségével, valamint LDAP adminisztrátorként működik az egyéb címtárbejegyzések (a DB2 valamelyik utótagjában vagy sémájában tárolt bejegyzések) tekintetében. A szerverbeállításokat csak a leképezett i5/OS adminisztrátorok módosíthatják.
- **LDAP adminisztrátor:** A Directory Server megengedi egyetlen felhasználói azonosító (DN) használatát elsődleges LDAP szerveradminisztrátorként. A Directory Server szintén módot ad arra, hogy leképezett operációsrendszeri felhasználói profilok LDAP adminisztrátorok legyenek. Az LDAP szerveradminisztrátorok sokféle adminisztrációs feladatot hajhatnak végre, például kezelhetik a replikációs, séma- és címtárbejegyzéseket.
- **Adminisztrátori felhasználók csoportja:** Egy leképezett i5/OS adminisztrátor kijelölhet egyes felhasználókat, hogy azok tagjai legyenek az adminisztrátori csoportnak. A csoport tagjai bármilyen feladatot végrehajthatnak, mivel ugyanolyan adminisztrációs hozzáféréssel rendelkeznek, mint az LDAP szerveradminisztrátor.

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

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

- Módosíthatják saját jelszavukat.
- Kapcsolatokat zárhatnak le.
- Engedélyezhetik és módosíthatják a jelszó-házirendeket, kivéve a jelszótitkosítást, amelyet csak a leképezett i5/OS adminisztrátorok módosíthatnak.
- Egyedi attribútumokat kezelhetnek.
- 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 el.

Kapcsolódó fogalmak

“Adminisztrációs csoport feladatok” oldalszám: 134
Az alábbi információk segítséget nyújtanak az adminisztrátori csoportok felügyelete során.

“Adminisztrátori és replika kötés DN” oldalszám: 90
A leképzett felhasználói profilt megadhatja konfigurált adminisztrátori vagy replika csatlakozási DN-nek. A felhasználói profil jelszavát használja a rendszer.

Kapcsolódó feladatok

“Adminisztrátori hozzáférés biztosítása leképezett felhasználók számára” oldalszám: 125
Az alábbi információk segítséget nyújtanak a felhasználói profiloknak adminisztrátori hozzáférés megadása során.

Proxy felhatalmazás

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 tagjaiét.

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 alkalmazásszerver 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. Máskülönben érvénytelen DN szintaxis üzenet érkezik. Csoport DN nem lehet tag proxy hitelesítési csoportban.

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

Kapcsolódó fogalmak

“Proxy hitelesítési csoport feladatok” oldalszám: 138
Az alábbi információk segítséget nyújtanak a proxy hitelesítési csoportok felügyelete során.

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 szűrt ACL-ek közül. A nem szűrt 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. Ezek az attribútumok:

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

További információk:

Kapcsolódó fogalmak

“Csoportok és szerepek” oldalszám: 57
A csoportok és szerepek segítségével a tagok hozzáférését és jogosultságait rendszerezheti.

“Hozzáférés felügyeleti lista (ACL) feladatok” oldalszám: 211
Az alábbi információk segítséget nyújtanak a hozzáférés felügyeleti listák (ACL) kezelésében.

“Műveleti attribútumok” oldalszám: 92
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.

“Hozzáférés felügyeleti listák módosítása” oldalszám: 197
Az alábbi információk segítséget nyújtanak a hozzáférés felügyeleti listák (ACL) kezelésében.

“Tartomány hozzáférés felügyeleti listáinak módosítása” oldalszám: 209
Az alábbi információk segítséget nyújtanak a tartományok hozzáférés felügyeleti listáinak módosítása során.

Kapcsolódó feladatok

“Sablon ACL listáinak módosítása” oldalszám: 211
Az alábbi információk segítséget nyújtanak a sablonok hozzáférés felügyeleti listáinak módosítása során.

Szűrt hozzáférés felügyeleti listák:

A szűrő alapú hozzáférés felügyeleti listák (ACL) szűrő alapú összehasonlítást használnak egy meghatározott objektumszűrő segítségével, hogy a célobjektumokat és a ténylegesen rájuk vonatkozó hozzáférési jogosultságokat egymásnak megfeleltessék.

A szűrő alapú ACL-ek jellegüknél fogva tovaterjednek minden összehasonlítással megfeleltetett objektumra a társított részfában. 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 ős 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.

Kapcsolódó fogalmak

“Továbbadás” oldalszám: 70
Amikor egy bejegyzés aclEntry vagy entryOwner eleme nincs explicit módon meghatározva, akkor azt a bejegyzés az őstől örökli, illetve a fán lefelé kerül terjesztésre.

Hozzáférés-felügyeleti attribútumok szintaxisa:

A hozzáférés felügyeleti lista (ACL) attribútumai az LDAP adatcsere formátum (LDIF) jelölésmód segítségével kezelhetők. Az új, szűrő alapú ACL attribútumok a meglévő, nem szűrő alapú ACL attribútumok módosított változatai.

Az alábbiakban megadjuk a hozzáférés felügyeleti információk (ACI) és az entryOwner attribútumok definícióját BNF formátumban:

```
<aclEntry> ::=  <tárgy> [ ":"  <jogok> ]

<aclPropagate> ::=  "true" | "false"
<ibm-filterAclEntry> ::=  <tárgy>  ":" <objektumszűrő>  [ ":"  <jogok> ]

<ibm-filterAclInherit> ::=  "true" | "false"
<entryOwner> ::=  <tárgy>

<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> ::= karaktersorozat kereső szűrő az RFC 2254, 4. rész szerint
                               (a bővíthető illesztés nem támogatott).
<rights> ::= <accessList> [":" <jogok> ]

<accessList> ::=  <objectAccess> | <attributeAccess> |
                          <attributeClassAccess>

<objectAccess> ::= "object:" [<művelet> ":"]  <objectPermissions>

<action> ::= "grant" | "deny"

<objectPermisssions> ::=  <objectPermission> [ <objectPermissions> ]

<objectPermission> ::= "a" | "d" |  ""

<attributeAccess> ::= "at." <attributeName> ":" [<művelet> ":"]
                              <attributePermissions>

<attributeName> ::= attributeType név az RFC 2251, 4.1.4 rész szerint
                       (OID vagy alfanumerikus karaktersorozat vezető
                        betűvel, "-" és ";" karakterek engedélyezettek)

<attributePermissions> ::=  <attributePermission>
                                   [<attributePermissions>]

<attributePermission> ::=  "r" | "w" | "s" | "c" |  ""
```

```
<attributeClassAccess> ::= <osztály> ":" [<művelet> ":"]
                                    <attributePermissions>

<class> ::= "normal" | "sensitive" | "critical" | "system" | "restricted"
```

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 hasonlók, elvben különböznek. Amikor egy felhasználó hozzárendelődik 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.

Pszeudo DN

Az LDAP címtár számos pszeudo 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 pszeudo 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, amelyiken 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 értékhalmaz 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)
ldapmodify	írás (a módosított attribútumokhoz)
ldapsearch	• keresés, olvasás (az RDN attribútumaihoz) • keresés (a keresési szűrőben megadott attribútumokhoz) • keresés (a csak nevekkel visszaadott attribútumokhoz) • keresés, olvasás (az értékekkel visszaadott attribútumokhoz)
ldapmodrdn	írás (az RDN attribútumokhoz)
ldapcompare	összehasonlítás (az összehasonlított attribútumokhoz)

Megjegyzés: Keresési műveletek esetén az alanynak keresési jogokkal kell rendelkeznie a keresési szűrő összes attribútumához, vagy különben egy bejegyzés sem kerül visszaadásra. A keresésből visszaadott bejegyzésekre az alanynak 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 diszkrétek: 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 **aclSource** leírását a Terjesztés témakör tartalmazza.

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.

Kapcsolódó fogalmak

"Továbbadás"
Amikor egy bejegyzés aclEntry vagy entryOwner eleme nincs explicit módon meghatározva, akkor azt a bejegyzés az őstől örökli, illetve a fán lefelé kerül terjesztésre.

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 egyénekkel, 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:

Amikor egy bejegyzés aclEntry vagy entryOwner eleme nincs explicit módon meghatározva, akkor azt a bejegyzés az őstől örökli, illetve a fán lefelé kerül terjesztésre.

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 örökli 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. Jellegüknél fogva tovaterjednek minden összehasonlítással megfeleltetett objektumra a társított részfában.

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.

Kapcsolódó fogalmak

“Szűrt hozzáférés felügyeleti listák” oldalszám: 66
A szűrő alapú hozzáférés felügyeleti listák (ACL) szűrő alapú összehasonlítást használnak egy meghatározott objektumszűrő segítéségével, hogy a célobjektumokat és a ténylegesen rájuk vonatkozó hozzáférési jogosultságokat egymásnak megfeleltessék.

Hozzáférés kiértékelése:

Egy adott művelet hozzáférésének 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 a társszerver (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 legegyedibb 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 alanynak 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.attributel:grant:rsc:sensitive:deny:rsc
2. aclEntry: group: cn=group1,o=IBM:critical:deny:rwsc
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).

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.

ACI-k és bejegyzéstulajdonosok megadása: Példa:

A következő két példa bemutatja egy adminisztrációs altartomány kialakítását a parancssori segédprogramok segítségével.

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
```

Példa az ACI és bejegyzéstulajdonos értékek módosítására:

Számos példa az ACI és bejegyzéstulajdonos értékek módosítására a parancssori segédprogramok segítségével.

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 minősítők. 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 nullértéket, a művelet pedig **grant** (megadás) értéket kap.

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.

ACI és bejegyzéstulajdonos értékek törlése: Példa:

Példa az ACI és bejegyzéstulajdonos értékek törlésére a parancssori segédprogramok segítségével.

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.

ACI és bejegyzéstulajdonos értékek lekérése: Példa:

Példa az ACI és bejegyzéstulajdonos értékek lekérésére a parancssori segédprogramok segítségével.

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 hozzáférésének 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 ős forrásból származhatnak, az aclSource attribútum a társított források listáját adja vissza.

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.

Tulajdonjog a következő módon rendelhető hozzá:

- 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.

Kapcsolódó fogalmak

"Címtárbejegyzésekkel kapcsolatos feladatok" oldalszám: 194
Az alábbi információk segítséget nyújtanak a címtárbejegyzések kezelése során.

Jelszó-irányelv

LDAP szervereket használva hitelesítéshez, fontos, hogy az LDAP szerver támogasson a jelszavak lejáratára, a meghiúsult bejelentkezési kísérletekre, valamint a jelszószabályokra vonatkozó irányelveket. A Directory Server konfigurálható támogatást nyújt mindhárom fajta irányelvhez.

A jelszó-irányelv minden userPassword attribútummal rendelkező címtárbejegyzésre alkalmazható. 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 attribútumit, amelyek alapján az adminisztrátor keresni tud például olyan dolgokat, mint a lejárt jelszavú felhasználók vagy a letiltott fiókok.

Konfiguráció

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 módosíthatják saját jelszavukat. 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 kéréssel 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 lejárta előtt. Ahhoz, hogy figyelmeztetést kapjon a jelszó lejártáról, az alkalmazásnak képesnek kell lennie az irányelvek kezelésére.
  - Meghatározott számú ″grátisz″ bejelentkezés engedélyezése a felhasználó jelszavának lejárta 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.
  - Jelszószintaxis-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 meghiúsult bejelentkezésekkel kapcsolatban:
  - Minimális időköz két jelszóváltás között. Ez megakadályozza a felhasználókat abban, hogy gyorsan végigpörgessenek néhány jelszót és újra a régit állítsák be.
  - A meghiúsult 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 meghiúsult bejelentkezési kísérleteket. Ha ennyi időn belül megtörténik a maximális számú meghiúsult kísérlet, akkor a fiók letiltásra kerül. Ennyi idő után a szerver eldobja a fiók meghiúsult 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 felkészített alkalmazások

A Directory Server jelszó-irányelv támogatásának része egy sor LDAP vezérlőelem, amelyek használatával a jelszó-irányelvek kezelésére felkészített alkalmazás értesítéseket kaphat a jelszó-irányelvekkel kapcsolatos további 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 értesíthető a szerver értesítésére arról, 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. A Java Naming and Directory Interface (JNDI) például beépített támogatást tartalmaz több elterjedt vezérlőelemhez, illetve keretrendszert biztosít a JNDI által fel nem ismert vezérlőelemek támogatásához.

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-irányelv 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-irányelvek replikációja

A jelszó-irányelvek 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-irányelv 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-irányelv változásai azonban nem replikálódnak más szerverekre.

Kapcsolódó fogalmak

“Jelszófeladatok” oldalszám: 175
Az alábbi információk segítséget nyújtanak a jelszófeladatok kezelése során.

“Műveleti attribútumok” oldalszám: 92
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.

Jelszó-irányelv javaslatok

Lehetséges, hogy a jelszó-irányelvek nem mindig a várt módon viselkednek.

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 meghiúsulni; 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.

Hitelesítés

A Directory Server hozzáférése hitelesítési módszer segítségével felügyelhető.

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:

- Névtelen
- a címtáradminisztrátor (alapértelmezés szerint cn=administrator)
- Leképezett i5/OS felhasználói profil

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

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

- Egyszerű csatlakozás, amikor is az alkalmazás megad egy megkülönböztetett nevet, illetve hozzá sima szövegben a megkülönböztetett névhez 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: Beke Antal
        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 keresésekkor 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 kivonatolt 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 sima szövegű jelszóhoz (a jelszóvédelem szintje nincs kell, hogy legyen), és a QRETSVRSEC rendszerértéknek 1-nek kell lennie. A megkülönböztetett név a szerverre elküldése helyett a DIGEST-MD5 azt igényli, hogy a kliens a szerverre felhasználónév-értéket küldjön. 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. A Directory Server lehetőséget ad a felhasználó leképezett vagy közzétett felhasználókénti kapcsolódására, amely esetben a szerver ellenőrzi a megadott jelszót a rendszeren megadott felhasználói profil jelszavához képest. Mivel a felhasználói profilok nyílt szöveges jelszava nem elérhető a szerver számára, a DIGEST-MD5 nem használható leképezett vagy közzétett felhasználókhoz.

Csatlakozás közzétett felhasználóként

A Directory Server lehetőséget ad olyan LDAP bejegyzések használatára, amelyek jelszava megegyezik ugyanazon rendszer egy operációs rendszer felhasználói profiljáéval. 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 sajat-rendszer.acme.com JSMITH nevű felhasználójának DN-je például a következő:

```
os400-profile=JSMITH,cn=accounts,os400-sys=sajat-rendszer.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 megkülönböztetett nevet generál.
- Kikeresi azt a bejegyzést, amelynek létezik ibm-securityidentities kiegészítő osztálya és KERBEROS:<azonosító>@<tartomány> formátumú altsecurityidenties értéke.

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

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

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=sajat-as400.sajatceg.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 alkalmazás programozási felület szükséges. Adjon meg egy üres megkülönböztetett nevet, 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 alkalmazás programozási felületek i5/OS rendszeren kerülnek felhasználásra, vagy a helyi címtárszerver elérése QSH parancs segédprogramok (például ldapsearch) használatával történik, akkor a jelszó kihagyható, és a kliens alkalmazás programozási felületek a fa 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=sajatprofil,cn=accounts,os400-sys=sajatrendszer -w sajatjelszo -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 protokollszintű lehallgatás elleni védekezésképpen 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.

Kapcsolódó fogalmak

"Operációs rendszer leképzett háttérobjektumok"
A rendszer leképezett háttér objektumai funkció az i5/OS objektumokat leképezi az LDAP által elérhető címtárfán belüli bejegyzésekre. A leképzett objektumok az operációs rendszer objektumok LDAP reprezentánsai, amelyeket az LDAP szerver adatbázisában tárolt tényleges bejegyzés helyett használunk.

"Felhasználói feladatok" oldalszám: 201
Az alábbi információk segítséget nyújtanak a felhasználók kezelése során.

Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek
A Directory Server alkalmazás programozási felületekkel kapcsolatosan további információkat az Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek témakör tartalmaz.

Kapcsolódó feladatok

"DIGEST-MD5 hitelesítés beállítása a Directory Serveren" oldalszám: 183
Az alábbi információk segítséget nyújtanak DIGEST-MD5 hitelesítés Directory Server szerveren történő beállítása során.

"Kerberos hitelesítés engedélyezése a Directory Server szerverhez" oldalszám: 182
Az alábbi információk segítséget nyújtanak a Kerberos hitelesítés Directory Server szerveren való engedélyezése során.

Szolgáltatás megbénítása

A szolgáltatás megbénítása támadások ellen a szolgáltatás megbénítása konfigurációs beállítás segítségével védekezhet.

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 szolgáltatásbénításos 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 szervert, hogy ne engedélyezzen névtelen hozzáférést. Más konfigurációs beállítások is üzembe helyezhetők, amelyekkel a szerver aktívan megelőzheti a szolgáltatásbénításos támadásokat.

Kapcsolódó feladatok

"Szerverkapcsolatok kezelése" oldalszám: 118
Az alábbi információk segítséget nyújtanak a szerverrel fennálló kapcsolatok és a kapcsolatokon végrehajtott műveletek megjelenítése során.

"Kapcsolat tulajdonságainak kezelése" oldalszám: 119
Az alábbi információk segítséget nyújtanak a kapcsolat tulajdonságainak beállítása során, például azon tulajdonságokénál, amelyek megakadályozzák, hogy a kliensek zároljanak egy szervert.

Operációs rendszer leképzett háttérobjektumok

A rendszer leképezett háttér objektumai funkció az i5/OS objektumokat leképezi az LDAP által elérhető címtárfán 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:

Kapcsolódó feladatok

“Adminisztrátori hozzáférés biztosítása leképezett felhasználók számára” oldalszám: 125
Az alábbi információk segítséget nyújtanak a felhasználói profiloknak adminisztrátori hozzáférés megadása során.

Kapcsolódó hivatkozás

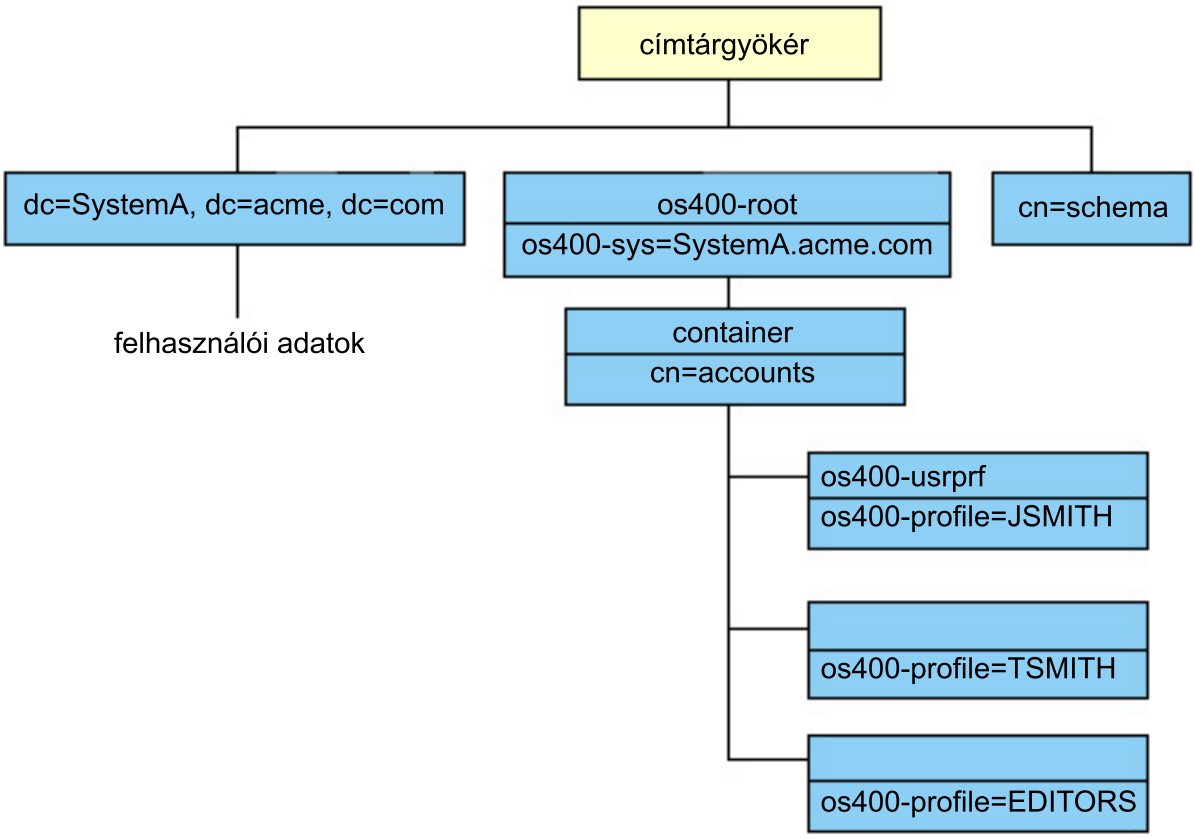
“Hitelesítés” oldalszám: 82
A Directory Server hozzáférése hitelesítési módszer segítségével felügyelhető.

Felhasználói leképezett címtár-információs fa

Ismerje meg, hogy az utótag és felhasználói profilok a felhasználói leképezett címtár-információs fán milyen módon kerülnek ábrázolásra.

Az alábbi ábra egy minta katalógus információs fát (DIT) mutat be a felhasználói leképezett 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

Leképezett háttér objektumokon végrehajtható LDAP műveletek ismertetése.

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 értékként 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 leképezett 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 hátterének elérésére.
- 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

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.

| Az LDAP adminisztrátor a felhasználói leképzett háttér objektumokra irányuló összes kereső műveletet letilthatja.
| További információkért tekintse meg az alábbi kapcsolódó hivatkozás Leképezett felhasználók olvasási hozzáférése
| témakörét.

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 értékeik visszaadása a megadott hatáskör és szűrő alapján. A hardverkódolt attribútumokat és értékeiket a rendszer objektumok utótagjára és az alatta lévő tárolóra vonatkozóan kapja vissza.
Az összes felhasználói profil visszaadása.	cn=accounts, os400-sys= SystemA.acme.com	one vagy sub	os400-gid=0	Csak a megkülönböztetett név (DN), az objectclass és az os400-profile értékeket kapja vissza a leképzett felhasználói profilokra. Ha más szűrő van megadva, akkor a rendszer LDAP_UNWILLING_TO_PERFORM értéket ad vissza.
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 más szűrő van megadva, akkor a rendszer LDAP_UNWILLING_TO_PERFORM értéket ad 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 más szűrő van megadva, akkor a rendszer LDAP_UNWILLING_TO_PERFORM értéket ad 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=* os400-profile=JSMITH	Más visszaadandó attribútumok megadhatók. Noha egyszintű hatáskör megadható, a keresési eredmények nem adnak vissza értéket, mivel a DIT-ben lévő JSMITH felhasználói profil alatt semmi sincs.
Az összes A-val kezdődő felhasználói és 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 más szűrő van megadva, akkor a rendszer LDAP_UNWILLING_TO_PERFORM értéket ad 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 más szűrő van megadva, akkor a rendszer LDAP_UNWILLING_TO_PERFORM értéket ad vissza.
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 más szűrő van megadva, akkor a rendszer LDAP_UNWILLING_TO_PERFORM értéket ad vissza.

Összehasonlítás

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

Az LDAP adminisztrátor a felhasználói leképzett háttér objektumokra irányuló összes összehasonlító műveletet letilthatja. További információkért tekintse meg az alábbi kapcsolódó hivatkozás Leképezett felhasználók olvasási hozzáférése témakörét.

Hozzáadás és módosítás (Add and modify)

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

Törlés

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

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

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

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

Kapcsolódó fogalmak

Vállalati azonosság leképezés (EIM)

"Olvasási hozzáférés leképezett felhasználók számára"
Alapértelmezésben a rendszer a leképzett háttér objektum olvasási hozzáférést a felhasználói profil információkhoz az erre jogosult felhasználóknak az LDAP kereső és összehasonlító műveleteken keresztül biztosítja. A leképezett felhasználók számára az olvasási hozzáférés a System i navigátor, illetve a /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf fájl (az alapértelmezett szerverpéldány esetében /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf fájl) konfigurációs paraméterének segítségével engedélyezhető, illetve tiltható le.

Adminisztrátori és replika kötés 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.

Kapcsolódó fogalmak

"Adminisztrátori hozzáférés" oldalszám: 64
Az adminisztrátori hozzáférés segítségével vezérelhető az adott adminisztrációs feladatok elérhetősége.

Felhasználói leképezett séma

A leképzett háttér objektumok objektum osztályai és attribútumai egy, az egész szerverre kiterjedő sémában találhatók.

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.

Olvasási hozzáférés leképezett felhasználók számára

Alapértelmezésben a rendszer a leképzett háttér objektum olvasási hozzáférést a felhasználói profil információkhoz az erre jogosult felhasználóknak az LDAP kereső és összehasonlító műveleteken keresztül biztosítja. A leképezett felhasználók számára az olvasási hozzáférés a System i navigátor, illetve a /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf fájl (az alapértelmezett szerverpéldány esetében /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf fájl) konfigurációs paraméterének segítségével engedélyezhető, illetve tiltható le.

A felhasználói profil információk olvasási hozzáférésének letiltásához tegye a következőket:

1. A System i navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek>TCP/IP** elemet.
3. Kattintson a jobb egérgombbal az **IBM Tivoli Directory Server** elemre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
4. Válassza ki az **Adatbázis/utótagok** lapot.
5. Szüntesse meg az **Olvasási hozzáférés engedélyezése a felhasználói információkhoz** jelölőnégyzet kijelölését.

A felhasználói leképezési háttér kereső és összehasonlító műveleteinek letiltásához a konfigurációs fájl cn=Front End, cn=Configuration szakaszában az alábbi sor módosítható:

ibm-slapdOs400UsrprjRead: TRUE

Az olvasási hozzáférés letiltásához a TRUE értéket módosítsa FALSE értékre. Ha az érték TRUE vagy a konfigurációs fájl a beállítást nem tartalmazza, akkor a leképezett felhasználói információkra vonatkozóan az olvasási hozzáférés engedélyezett.

Kapcsolódó feladatok

"Leképezett felhasználók olvasási hozzáférésének engedélyezése vagy letiltása" oldalszám: 129
Az alábbi információk segítséget nyújtanak a felhasználói leképzett háttér objektumokat érintő kereső és összehasonlító műveletek letiltása során.

Kapcsolódó hivatkozás

"LDAP műveletek" oldalszám: 87
Leképezett háttér objektumokon végrehajtható LDAP műveletek ismertetése.

Directory Server és i5/OS naplózási támogatás

A Directory Server i5/OS adatbázis támogatást használ a címtárinformációk tárolásához. A Directory Server a véglegesítés vezérlés alapján tárolja a címtárbejegyzéseket az adatbázisban. Ehhez i5/OS naplózási támogatás szükséges.

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

- Egy napló
- Egy naplófogadó
- A kezdetben szükséges adatbázis tábla

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

Az aktuális környezet: a címtár mérete és szerkezete, valamint a mentési és visszaállítási stratégia megkövetelhet az alapértelmezéstől bizonyos eltéréseket, beleértve ezeknek az objektumoknak a kezelését és a használt méretküszöbüket is. Ha szükséges, megváltoztathatja a naplózási parancs paramétereit. Az LDAP naplózás alapértelmezés szerinti beállítása törli a régi fogadókat. Ha 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)
```

Kapcsolódó tájékoztatás

Napló módosítása (CHGJRN)

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=IBMpolicies. 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

Kapcsolódó fogalmak

"Egyedi attribútum feladatok" oldalszám: 140
Az alábbi információk segítséget nyújtanak az egyedi attribútumok kezelése során.

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 attribútumuk 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.
- 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.
- 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.

Kapcsolódó fogalmak

“Címtárak” oldalszám: 4
A Directory Server (címtárszerver) segítségével egy olyan adatbázistípus érhető el, amely az információkat az i5/OS integrált fájlrendszerének felépítéséhez hasonló, hierarchikus struktúrába szervezve tárolja.

“Hozzáférés-felügyeleti listák” oldalszám: 65
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.

“Jelszó-irányelv” oldalszám: 78
LDAP szervereket használva hitelesítéshez, fontos, hogy az LDAP szerver támogasson a jelszavak lejáratára, a meghiúsult bejelentkezési kísérletekre, valamint a jelszószabályokra vonatkozó irányelveket. A Directory Server konfigurálható támogatást nyújt mindhárom fajta irányelvhez.

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 az olyan kereséseknél, amelyek DB2 kapcsolatot igényelnek, még akkor is, ha az információk a DB2 gyorsítótárban találhatók. 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.

Kapcsolódó fogalmak

"Teljesítmény feladatok" oldalszám: 142
Az alábbi információk segítséget nyújtanak a teljesítmény beállítások megadása során.

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 lennük.

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

A vezérlőelemek és kiterjesztett műveletek segítségével az LDAP protokoll a protokoll módosítása nélkül kiterjeszthető.

Vezérlőelemek

A vezérlőelemek további információkat biztosítanak a szerver számá Például a delete subtree (részfa 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 válaszértéket ASN.1 jelölésmóddal kell megadni. Az érték maga a válasz adat BER kódolással.

Kapcsolódó fogalmak

"Megkülönböztetett nevek (DN)" oldalszám: 9
A címtár minden bejegyzésének vagy egy megkülönböztetett neve (DN). A DN az a név, amelyik egyedi módon azonosítja a címtárbejegyzést. A DN első elemét szokás relatív megkülönböztetett névként (Relative Distinguished Name, RDN) emlegetni.

Kapcsolódó hivatkozás

"Objektumazonosítók (OID)" oldalszám: 293
Az alábbi információk a Directory Server termékben használt objektumazonosítók (OID) leírását tartalmazzák.

Mentési és visszaállítási szempontok

A Directory Server az adatokat és a konfigurációs információkat számos helyen tárolja.

A Directory Server az információkat az alábbi helyeken tárolja:

- Adatbáziskönyvtár (alapértelmezés szerint a QUSRDIRDB), amely tartalmazza a címtárszerver tartalmát.

  Megjegyzés: Azt, hogy melyik adatbázis-könyvtárat használja, az IBM Directory Server **Adatbázis/utótag** lapjának használatával nézheti meg a System i navigátorban.
- 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.

Kapcsolódó tájékoztatás

Rendszermentés és helyreállítás

Directory Server használatának megkezdése

Kezdje meg a Directory Server telepítését, átállítását, tervezését, személyre szabását, illetve felügyeletét.

A Directory Server az i5/OS rendszerrel együtt automatikusan telepítésre kerül. A Directory Server része egy alapértelmezés szerinti konfiguráció. A Directory Server használatának megkezdéséhez tekintse meg az alábbi témaköröket:

Áttérési megfontolások

Ha V5R4 kiadást telepít, és a Directory Server-t használta már egy korábbi kiadáson, akkor tekintse át az áttéréssel kapcsolatos megfontolásokat.

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.

Áttérés V5R4 vagy V5R3 változatról V6R1 változatra

Az alábbi információk segítséget nyújtanak, ha V5R4 V5R3 változaton futó Directory Serverrel rendelkezik.

Az i5/OS V6R1 új Directory Server funkciókat és képességet vezet be. Ezek a változtatások érintik az LDAP címtárszervert és az System i navigátor grafikus felhasználói kezelőfelületét (GUI-t). Ahhoz, hogy kihasználhassa az új GUI funkciók előnyeit, telepítenie kell az System i navigátor programot egy olyan PC-re, ami TCP/IP-n keresztül kommunikál az iSeries szerverrel. Az System i navigátor az System i Access for Windows egyik részeleme. Ha telepítve van az System i navigátor egy korábbi verziója, akkor azt V6R1 változatra kell frissíteni.

V5R4 és V5R3 változatról közvetlen frissíthet i5/OS V6R1 változatra. A Directory Server a szerver első indításakor frissítésre kerül V6R1 változatra. Az LDAP címtáradatok és a címtársémafájlok automatikusan átállításra kerülnek, hogy megfeleljenek a V6R1 formátumnak.

Az i5/OS V6R1 verzióra frissítéskor figyelembe kell venni néhány átállítási problémát:

- Ha V6R1 változatra frissít és elindítja a címtárszervert, a Directory Server automatikusan átállítja a sémafájlokat V6R1 változatra és törli a régi sémafájlokat. Ha már törölte vagy átnevezte a sémafájlokat, akkor a Directory Server nem fogja tudni átállítani azokat. Lehet, hogy hibaüzenetet kap, vagy a Directory Server feltételezheti, hogy a fájlok már átállításra kerültek.
- A V6R1 változatra frissítés után indítsa el legalább egyszer a szervert, 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 V6R1 formátumra állítja át a címtáradatokat a szerver első indításakor vagy egy LDIF fájl importálásakor. Szánjon némi időt az áttelepítés elvégzésére.
- A V6R1 a i5/OS rendszeren több címtárszerver-példányt tesz lehetővé. Ha a címtárszervert V6R1 változatra frissítés előtt használta, akkor a címtárszerver átállításra kerül egy példányra. Ez magában foglalja a konfigurációs és sémafájlok áthelyezését a /QIBM/UserData/OS400/DirSrv címtárból a /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR címtárba. Ez lesz az alapértelmezett címárszerver-példány, és QUSRDIR példánynak fogják hívni. A QUSRSYS könyvtár két objektuma áthelyezésre kerül a USRDIRCF nevű új könyvtárba. Ez az áttérés a címtárszerver V6R1 változatra való frissítése utáni első indításakor kerül végrehajtásra.
- 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 System i navigátorral.

Adatok átállítása V4R4 ,V4R5, V5R1 vagy V5R2 változatról V6R1 változatra

Az alábbi információk segítséget nyújtanak, ha V4R4, V4R5 vagy V5R1 változaton futó Directory Serverrel rendelkezik.

V4R4, V4R5 és V5R1 változatról nem lehet közvetlenül i5/OS V5R4 változatra frissíteni.

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

- A Directory Server V4R4 és korábbi verziói nem vették figyelembe az időzónákat az időbélyeg-bejegyzések létrehozásakor. A V4R5 változattól kezdve a rendszer figyelembe veszi az időzónákat a címtár minden módosításánál és bővítésénél. Ezért ha V4R4 vagy korábbi verzióról frissíti az adatokat, akkor a Directory Server beállítja a meglévő createtimestamp és modifytimestamp attribútumot, hogy azok a helyes időzónát tükrözzék. Ezt úgy valósítja meg, hogy kivonja a rendszeren jelenleg definiált időzónát a címtárban tárolt időbélyegekből. 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 karakterkészletet. 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.

Ha ezeket a kiadásokat kívánja frissíteni a V5R4 kiadásra, akkor az alábbi eljárások szerint kell eljárnia.

Frissítés V4R4, V4R5 vagy V5R1 kiadásokról köztes kiadásra:

A Directory Server szervert állíthatja először egy köztes kiadásra (V5R2 vagy V5R3 változatra), majd ezt követően a V6R1 változatra.

Ugyan a V4R4, V4R5, V5R1 és V5R2 változatokról a V6R1 változatra történő frissítés nem támogatott, az alábbi frissítések támogatottak:

- V4R4 és V4R5 frissíthető V5R1-re
- V4R5 és V5R1 frissíthető V5R2-re
- V5R1 és V5R2 frissíthető V5R3-ra
- V5R2 és V5R3 frissíthető V5R4-re
- V5R3 és V5R4 frissítése V6R1 változatra

Az i5/OS telepítési eljárásával kapcsolatosan részletes információkat az i5/OS és kapcsolódó szoftver telepítése, frissítése és törlése témakör tartalmaz. Az átállás 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 V5R1 változatra telepít, akkor ezt követően a V5R3 változatra is telepítenie kell. Ha V5R2 változatra telepít, akkor ezt követően a V5R3 vagy V5R4 változatra is telepítenie kell.
3. V5R1 esetén végezze el a V5R3 telepítését.
4. V5R2 esetében végezze le a V5R3 vagy V5R4 telepítését.
5. Ha a V5R3 vagy V5R4 szintet elérte, akkor végezze el a V6R1 változat telepítését.
6. Ha még nem indított el eddig, akkor indítsa el a Directory Servert.

Adatbáziskönyvtár mentése és a V6R1 telepítése:

A Directory Server átállítható úgy is, hogy elmenti a Directory Server által használt adatbáziskönyvtárat a V4R4 vagy V4R5 kiadásban, majd a V6R1 telepítése után visszaállítja.

Ezzel a módszerrel megtakarítható a közbenső kiadás telepítési fázisa. Ilyenkor azonban a szerver beállításai nem helyeződnek át, így a szervert újra kell konfigurálni. Az i5/OS telepítési eljárásával kapcsolatosan részletes információkat az i5/OS és kapcsolódó szoftver telepítése, frissítése és törlése témakör tartalmaz. 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 szever elindult az új kiadással, használhassa őket. Az egyedi attribútumtípus és objektumoszály-definíciók a címtárkezelő eszköz vagy a webes adminisztrációs eszköz (más V6R1 rendszeren futtatva) segítségével jeleníthetők meg. Ha a módosítások csak új attribútumtípusok és objektumosztályok hozzáadására terjednek ki, készítsen egy másolatot a /qibm/userdata/os400/dirsrv/v3.modifiedschema fájlról. Ennek a fájlnak a felhasználásával hozhatók létre a sémafrissítéseket tartalmazó LDIF fájlok. További információkért forduljon a “Séma” oldalszám: 14 részhez.
2. Jegyezze fel a Directory Server különböző konfigurációs beállításait (például az adatbáziskönyvtár nevét).
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 konfiguráció (a jelszó-információk kivételével) a System i navigátor segítségével jeleníthető meg. A konfiguráció megjelenítéséhez válassza ki a rendszerre vonatkozó **Tulajdonságok** elemet, majd kattintson a **Címtár szolgáltatások** lapra.
5. Telepítse az i5/OS V6R1 változatát a rendszerre.
6. A Directory Server a System i navigátorban található varázsló segítségével állítható be.
7. Állítsa vissza az 3. lépésben elmentett adatbáziskönyvtárat. Ha a 3. lépésben elmentette a QUSRDIRCL könyvtárat, akkor állítsa azt is vissza.
8. Az System i navigátorral konfigurálja újra a Directory Server-t. Adja meg a korábban beállított adatbázis-könyvtárat, amelyet az előző lépésekben elmentett és visszaállított.
9. Az System i 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 alábbi információk segítséget nyújtanak akkor, ha replikált szerverekből álló hálózattal rendelkezik.

Az elsődleges szerver első elindításakor átmozgatja a replikációt vezérlő címtár információit. A cn=localhost alatti, replicaObject objektumosztályú bejegyzéseket felváltják az új replikációs modell által használt bejegyzések. 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 parancssori eszközt “ldapsearch” oldalszám: 234 és mentse el a kimenetet egy fájlba. A keresési parancs az alábbihoz hasonló lesz:

```
ldapsearch -h elsodleges-szerver-hoszt-nev -p elsodleges-szerver-port \
 -D elsődleges_szerver_admin_DN -w
elsődleges_szerver_admin_jelszó \
 -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 adjon meg, hogy ezáltal a további keresések során az adatok ne felülírják a kimeneti fájlt, hanem ahhoz 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 a System i navigátor **Indítás** parancsát.

A szerver leállításához használja a System i navigátor **Leállítás** parancsát.

Amikor felveszi a fájlt a replikaszerverre, ügyeljen rá, hogy a replikaszerver ne működjön. Az adatok felvételéhez használja a System i 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_hosztnév -p elsődleges_szerver_port \
   -D elsődleges_szerver_admin_DN -w
  elsődleges_szerver_admin_jelszó \
   -op controlrepl -action resume -ra replica-agreement-DN
  ```

  Ez a parancs újra elindítja a megadott DN-ű bejegyzésben meghatározott szerver replikációját.

Az, hogy megyik 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_hosztnév -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 címtáradatok szinkronizálására. Ez garantálja, hogy a nem replikált bejegyzések vagy attribútumok is frissítésre kerüljenek a replikán.

Kapcsolódó fogalmak

“Replikáció” oldalszám: 38
A címtárszerverek a replikáció nevű technikát használják a teljesítmény és a megbízhatóság javítására. A replikációs folyamat feladata, hogy szinkronban tartsa több címtár adatait.

Kapcsolódó feladatok

“Directory Server elindítása” oldalszám: 116
Az alábbi információk segítséget nyújtanak a Directory Server elindítása során.

Kerberos szolgáltatás megváltozott neve

Akkor használja ezeket az információkat, ha V5R3 változatnál korábbi Kerberost használ.

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-hosztnév@Kerberos-tartomány formátumú szolgáltatásnevet használtak, ha a hitelesítés a GSSAPI mechanizmussal (Kerberosszal) 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 igaza akkor, ha a Kerberos kulcsterjesztő központ (KDC) érzékeny a kis- és nagybetűk különbségére az azonosítókban. 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. Alapértelmezésben a címtárszerver a /QIBM/UserData/OS/400/NetworkAuthentication/keytab/krb5.keytab fájlt használja. A V5R3M0 System i navigátor 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

A Directory Server beállításának megkezdése előtt, illetve az LDAP címtár szerkezetének létrehozása előtt tanácsos egy pár percet a tervezésre szánni.

A Directory Server beállításának megkezdése előtt, illetve az LDAP címtár szerkezetének létrehozása előtt gondolja át a következőket:

- **A címtár kialakítása**. Tervezze meg a címtár szerkezetét és döntse el, milyen utótagok és attribútumok szükségesek a címtárszerver működéséhez. További információkat a Címtárszerkezet: Ajánlott gyakorlat, a Címtárak, az Utótagok, illetve az Attribútumok témakör tartalmaz.
- **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.

  Ha például egy üres címtár a Directory Server alapértelmezett sémáját használja, akkor körülbelül 10 MB tárolóterületet igényel. 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, illetve a kommunikáció biztonsága érdekében a Fordítási réteg biztonság (TLS) használatát. A Kerberos hitelesítés ugyancsak támogatott.

  A Directory Server lehetővé teszi, hogy a címtár objektumaihoz való hozzáférést hozzáférés felügyeleti listák (ACL) segítségével szabályozza. 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=administrator. 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 eszközének használatához az alábbi termékeknek kell telepítve lenniük.
  - IBM HTTP Server for i5/OS (5761-DG1)
  - IBM WebSphere Application Server 6.0 (5733-W60 Base vagy Express lehetőség)
- **Rendszermentési és helyreállítási stratégia tervezése**. Tervezze meg az adatok, illetve konfigurációs információk mentésének módját.

Kapcsolódó fogalmak

“Javasolt példák a címtár felépítésére” oldalszám: 35
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.

“Címtárak” oldalszám: 4
A Directory Server (címtárszerver) segítségével egy olyan adatbázistípus érhető el, amely az információkat az i5/OS integrált fájlrendszerének felépítéséhez hasonló, hierarchikus struktúrába szervezve tárolja.

“Utótag (névkontextus)” oldalszám: 13
Az utótag (más néven névkontextus) egy olyan DN, amely egy helyileg tárolt címtárhierarchia legfelső bejegyzését azonosítja.

“Attribútumok” oldalszám: 18
Minden címtárbejegyzéshez tartozik egy sor attribútum, az objektumosztály meghatározása alapján.

“Mentési és visszaállítási szempontok” oldalszám: 95
A Directory Server az adatokat és a konfigurációs információkat számos helyen tárolja.

Kapcsolódó tájékoztatás

IBM HTTP Server
Az IBM HTTP Server és az IBM WebSphere Application Server termékekkel kapcsolatosan további információkat az IBM HTTP Server témakör tartalmaz.

Directory Server beállítása

A Directory Server beállításainak személyre szabásához futtassa a Directory Server konfigurációs varázslót.

1. Ha rendszere nem úgy lett konfigurálva, hogy képes legyen információkat egy másik LDAP szervernek továbbítani, és a TCP/IP DNS szerver nem ismer LDAP szervereket, akkor a Directory Server automatikusan egy korlátozott alapértelmezés szerinti konfigurációt telepít. A Directory Server egy varázslót biztosít a Directory Server egyedi igények szerinti konfigurálásának támogatására. A varázsló a későbbiek folyamán a System i navigátorból futtatható. 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 ″tiszta lappal″ indul. Az eredeti konfiguráció törlésre kerül a módosítás helyett. Azonban a címtáradatok nem törlődnek, 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** feliratra, 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 módon indítható:
   a. A System i navigátorban bontsa ki a **Hálózat** részt.
   b. Bontsa ki a **Szerverek** kategóriát.
   c. Kattintson a **TCP/IP** lehetőségre.
   d. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, 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: Érdemes 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 témakör Domino LDAP és Directory Server működtetése ugyanazon a rendszeren részében talál.
   - Megváltoztatja a Directory Server által használt portot. További információkat a “Port vagy IP cím módosítása” oldalszám: 123 témakör tartalmaz.

- Megadott IP címeket használ. További információkat a “Port vagy IP cím módosítása” oldalszám: 123 témakör tartalmaz.

5. A beállított utótagoknak megfelelő bejegyzéseket készít. További információk: “Directory Server utótagok felvétele és eltávolítása” oldalszám: 124.
6. A folytatás előtt azonban célszerű az alábbiakban felsorolt dolgok közül néhányat vagy az összeset elvégezni:
   - SSL (Védett socket réteg) biztonság engedélyezése. Részletek: “SSL és TSL engedélyezése a Directory Serveren” oldalszám: 180.
   - Kerberos hitelesítés engedélyezése. Részletek: “Kerberos hitelesítés engedélyezése a Directory Server szerverhez” oldalszám: 182.
   - Utalás beállítása. Részletek: “Szerver kijelölése címtári utalások részére” oldalszám: 123.
7. Indítsa el a Directory Server szervert. További információkért tekintse meg az “Directory Server elindítása” oldalszám: 116 témakört.
8. A meglévő címtárszerverpéldányra a rendszer QUSRDIR példányként hivatkozik. A példányhoz tartozó séma és konfigurációs fájlok a /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR könyvtárban találhatók. A szerverpéldány automatikusan létrehozható akkor, ha megpróbálja az alapértelmezett példányt elindítani. Egyéb példányok automatikusan nem kerülnek létrehozásra.

Kapcsolódó fogalmak

“Directory Server alapértelmezett konfigurációja” oldalszám: 303
A Directory Server az i5/OS rendszerrel együtt automatikusan telepítésre kerül. Ez a telepítés tartalmaz egy alapértelmezés szerinti konfigurációt.

A címtár feltöltése

A címtárat töltse fel adatokkal.

A címtárat többféleképp feltöltheti adatokkal:

- Az információkat közzéteheti a Directory Server szerver számára.
- Az adatokat importálhatja LDIF fájlból.
- A felhasználókat egy HTTP szerver ellenőrzési listájából a Directory Server szerverre másolhatja.

Kapcsolódó feladatok

“Információk publikálása a címtárszervernek” oldalszám: 129
Az alábbi információk segítséget nyújtanak az információk Directory Server szerveren történő közzététele során.

“LDIF fájl importálása” oldalszám: 131
Ezen információk segítségével importálhat LDAP adatcsere formátum (LDIF) fájlt.

“Felhasználók másolása HTTP szerver ellenőrzési listából a Directory Server szerverre” oldalszám: 132
Az alábbi információk segítséget nyújtanak a felhasználók HTTP szerver ellenőrzési listából Directory Server szerverre történő másolása során.

Webes adminisztráció

A Directory Server szerverek felügyeletéhez állítsa be és használja a webes adminisztrációs konzolt.

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: 104), majd ezután folytassa a következő lépéssel.

2. Jelentkezzen be a Directory Server webes adminisztrációs rendszerében az alábbi módok valamelyikével:
   - A System i navigátorban válassza ki a szervert, majd kattintson a **Hálózat → Szerverek → TCP/IP** lehetőségre, kattintson a jobb egérgombbal az **IBM Directory Server** lehetőségre, majd válassza az előugró menü **Szerveradminisztráció** menüpontját.
   - Az iSeries Feladatok oldalán (http://*saját_szerver*:2001) kattintson az **IBM Directory Server** lehetőségre.
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** gombra. Megjelenik az IBM Directory Server webes adminisztrációs eszközének oldala. Az IBM Directory Server webes adminisztrációs eszköz oldallal kapcsolatos további információk: “Webes adminisztrációs eszköz” oldalszám: 106.
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** gombra. Megjelenik az IBM Directory Server webes adminisztrációs eszközének oldala. Az IBM Directory Server webes adminisztrációs eszköz oldallal kapcsolatos további információk: “Webes adminisztrációs eszköz” oldalszám: 106.
   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

Az alábbi témakör útmutatást nyújt arra vonatkozóan, hogy a Directory Server webes adminisztrációja első alkalommal milyen módon állítható be.

1. Ha még nincsenek telepítve, akkor telepítse az IBM WebSphere Application Server 6.0 (5733-W60 alapszintű vagy Express lehetőség) terméket és a hozzá tartozó előfeltétel-szoftvereket.
2. Kapcsolja be a rendszer alkalmazásszerver példányt a HTTP ADMIN szerverben. További információkat az IBM HTTP Server témakör tartalmaz.
   a. A HTTP ADMIN szerver az alábbi módokon indítható:
      - A System i navigátorban kattintson a **Hálózat → Szerverek → TCP/IP** elemre, kattintson a jobb egérgombbal a **HTTP adminisztráció** elemre, majd válassza az előugró menü **Indítás** menüpontját.
      - 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), majd kattintson az **IBM Web Administration for iSeries** elemre.
   c. A HTTP szerver adminisztráció *saját_szerver* lapon kattintson a **Kezelés**, majd a **HTTP szerverek** lapra. Győződjön meg róla, hogy az **ADMIN – Apache** ki van választva a **Szerver** legördülő listában, és hogy a **/QIBM/UserData/HTTPA/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 kattintással (a második gomb a **HTTP szerverek** lap alatt). A HTTP ADMIN szerverpéldányt a System i navigátorból vagy a parancssorból is leállíthatja, illetve elindíthatja.

Az alábbi módszerek valamelyikével ugyancsak leállíthatja a HTTP ADMIN szerverpéldányt.

- A System i navigátorban kattintson a **Hálózat → Szerverek → TCP/IP** kategóriára, kattintson a jobb egérgombbal a **HTTP adminisztráció** elemre, majd válassza az előugró menü **Leállítás** menüpontját.
- Egy parancssorba írja be az ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN) parancsot.

Az alábbi módszerek valamelyikével ugyancsak elindíthatja a HTTP ADMIN szerverpéldányt.

- A System i navigátorban kattintson a **Hálózat → Szerverek → TCP/IP** elemre, kattintson a jobb egérgombbal a **HTTP adminisztráció** elemre, majd válassza az előugró menü **Indítás** menüpontját.
- Egy parancssorba írja be az STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN) parancsot.

További információkat az IBM HTTP Server témakör tartalmaz.

3. Jelentkezzen be a Directory Server webes adminisztrációs eszközre.
   a. A **Bejelentkezési lap** az alábbi módszerek valamelyikével jöhet elő.
      - A System i navigátorban válassza ki a szervert, kattintson a **Hálózat → Szerverek → TCP/IP** elemre, kattintson a jobb egérgombbal az **IBM Directory Server** lehetőségre, majd válassza az előugró menü **Szerveradminisztráció** menüpontját.
      - Az iSeries Feladatok oldalon (http://*saját_szerver*:2001) kattintson az **IBM Directory Server for iSeries** elemre.
   b. Válassza ki az **LDAP hosztnév** mezőben a **Konzol adminisztráció** lehetőséget.
   c. A **Felhasználónév** mezőbe írja be, hogy superadmin.
   d. A **Jelszó** mezőbe írja be, hogy secret.
   e. Kattintson a **Bejelentkezés** gombra. 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** gombra. A Sikeres kijelentkezés képernyő megjelente 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

A webes adminisztrációs eszközre bejelentkezve megjelenik egy öt részből álló alkalmazásablak.

Csíkterület
A csíkterület 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.

Többszörözés kezelése
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.

Directory Server példahelyzetek

Az alábbi információk segítséget nyújtanak a jellemző Directory Server feladatokat bemutató példahelyzetek áttekintése során.

Példahelyzet: Directory Server beállítása

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

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 címtár-adatbázist az alkalmazottak adataival (név, e-mail cím, telefonszám és hasonlók).

A példahelyzet céljai az alábbiak:

- 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 címtár-adatbázisban, ugyanakkor a nem vezetők ezt ne tehessék meg.
- A rendszer képes legyen az alkalmazottak adatainak közzétételére a címtár-adatbázisban.

Részletek

A Directory Server a mySystem nevű rendszeren fut.

Az alábbi példa bemutatja, hogy a MyCo Rt. milyen adatokat kíván tárolni az egyes alkalmazottakról a címtár-adatbázisban.

```
Név: Jose Alvirez
Osztály: DEPTA
Telefonszám: 999 999 9999
Email-cím: jalvirez@my_co.com
```

A példahelyzethez alkalmazható címtár 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
         mySystem.my_co.com
.
.
.
```

Minden alkalmazott (vezetők és nem vezetők egyaránt) az employees címtárfában található. A vezetők a managers csoport tagjai. A managers csoport tagjai jogosultak az alkalmazottak adatainak módosítására.

A rendszernek (mySystem) az alkalmazottak adatainak módosítására is jogosultnak kell lennie. Ebben a példahelyzetben a rendszer bekerül az employees címtárfába és a managers csoport tagja lesz.

Ha az alkalmazottak bejegyzéseit külön akarja választani a rendszer bejegyzésétől, akkor létrehozhat egy másik címtárfát (például ″computers″ néven) és felveheti abba a rendszert. A rendszernek mindazonáltal ugyanazokat a jogokat kell adni, mint a vezetőknek.

Előfeltételek és feltételezések

A webes adminisztrációs eszköz megfelelően be van állítva és fut. További információkat a “Webes adminisztráció” oldalszám: 103 témakör tartalmaz.

Beállítási lépések

Tegye a következőket:

Példahelyzet részletek: A Directory Server telepítése

1. lépés: A Directory Server beállítása:

Megjegyzés: A szerver konfigurálásához *ALLOBJ és *IOSYSCFG különleges jogosultságokkal kell rendelkeznie.

1. A System i navigátorban kattintson a **Hálózat → Servers → TCP/IP** lehetőségre.
2. Kattintson a System i navigátor jobb alsó részében, a **Szerverkonfigurációs feladatok** ablak **Rendszer címtárszerverként konfigurálása** lehetőségére.
3. Megjelenik a **Directory Server beállítási varázsló**.
4. Kattintson az **IBM Directory Server beállítási varázsló - üdvözlet** ablak **Helyi LDAP címtárszerver beállítása** lehetőségére.
5. Kattintson az **IBM Directory Server beállítási varázsló - üdvözlet** ablak **Tovább** lehetőségére.
6. Az **IBM Directory Server beállítási varázsló - Beállítások megadása** ablakban válassza ki a **Nem** lehetőséget. Így konfigurálhatja az LDAP szervert 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	titok
Jelszó megerősítése	titok

Megjegyzés: A jelen példahelyzet összes jelszava kizárólag példa. A rendszer és a hálózat biztonsága érdekében soha ne használja ténylegesen ezeket a jelszavakat a saját konfigurációban.

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** mezejébe írja be, hogy dc=sajat_ceg,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://*sajatRendszer.sajat_ceg.com*:9080/IDSWebApp/IDSjsp/Login.jsp oldalra, ahol a *sajatRendszer.sajat_ceg.com* a saját rendszer.
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 titok. Kattintson a **Bejelentkezés** menüpontra.
3. Állítsa be a webes adminisztrációs eszközt úgy, hogy csatlakozzon a rendszeren található LDAP szerverhez. A bal oldali navigációs területen válassza ki a **Konzoladminisztráció → Konzolszerverek kezelése** elemet.
4. Kattintson a **Hozzáadás** gombra.
5. A **Szerver hozzáadása** mezőben adja meg a sajatRendszer.sajat_ceg.com karaktersorozatot.
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 (**sajatRendszer.sajat_ceg.com**).
9. A **Felhasználónév** mezőben adja meg a cn=administrator, a **Jelszó** mezőben pedig a titok karaktersorozatot. Kattintson a **Bejelentkezés** gombra. 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** lehetőségére. 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...** lehetőségre. 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** mezőben adja meg a dc=sajat_ceg értéket. A **Szülő DN** mezőben adja meg a dc=com értéket. A **dc** mezőben adja meg a sajat_ceg értéket.
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** lehetőségre.
2. A **Felhasználói sablon neve** mezőbe írja be, hogy Alkalmazott.
3. Kattintson a **Szülő DN** mező melletti **Tallóz...** gombra. Kattintson a korábbi részben létrehozott alap DN-re (**dc=sajat_ceg,dc=com**), majd kattintson az ablak jobb oldalán látható **Kiválasztás** lehetőségre.
4. Kattintson a **Tovább** gombra.
5. Válassza ki a **Strukturális objektumosztály** legördülő lista **inetOrgPerson** elemét, majd kattintson a **Tovább** gombra.
6. Az **Elnevezési tulajdonság** legördülő listából válassza ki a **cn** elemet.
7. A **Lapok** listából válassza ki a **Kötelező** elemet és kattintson a **Módosítás** lehetőségre.

8. A **Lap módosítása** ablakban adhatja meg, hogy a felhasználói sablon milyen mezőket tartalmazzon. Az **sn** és **cn** mezők kötelezők.
9. Az **Attribútumok** listából válassza ki a **departmentNumber** elemet, majd kattintson a **Hozzáadás >>>** elemre.
10. Válassza ki a **telephoneNumber** elemet, majd kattintson a **Hozzáadás>>>** gombra.
11. Válassza ki a **mail** elemet, majd kattintson a **Hozzáadás>>>** gombra.
12. Válassza ki a **userPassword** elemet, majd kattintson a **Hozzáadás>>>** gombra.
13. 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** lehetőségre.
2. A **Tartomány neve** mezőbe írja be az employees karaktersorozatot.
3. Kattintson a **Szülő DN** mező melletti **Tallózás...** gombra.
4. Válassza ki a létrehozott szülő DN-t (**dc=sajat_ceg,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=sajat_ceg,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** lehetőségre.
   b. A **Csoport neve** mezőbe írja be a managers karaktersorozatot.
   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** lehetőségre.
   b. Válassza ki a létrehozott tartományt (**cn=employees,dc=sajat_ceg,dc=com**), majd kattintson a **Módosítás** lehetőségre.
   c. Az **Adminisztrátor csoport** mező jobb oldalán kattintson a **Tallózás...** lehetőségre.
   d. Válassza ki a **dc=sajat_ceg,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=sajat_ceg,dc=com** utótaghoz.
   a. Kattintson a **Címtárkezelés → Bejegyzések kezelése** menüpontra.
   b. Válassza ki a **dc=sajat_ceg,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=sajat_ceg,dc=com** adatfa tulajdonosa is lesz.
   e. A **Típus** legördülő listából válassza ki a **Csoport** lehetőséget.
   f. A **DN (megkülönböztetett név)** mezőben adja meg a cn=managers,cn=employees,dc=sajat_ceg,dc=com karaktersorozatot.
   g. Kattintson a **Hozzáadás** gombra.
   h. Kattintson az **OK** gombra.

5. lépés: Vezető felhasználó felvétele:

1. A webes adminisztrációs eszközben kattintson a **Felhasználók és csoportok → Felhasználók hozzáadása** lehetőségre.
2. A **Tartomány** legördülő menüből válassza ki a létrehozott tartományt (**employees**), majd kattintson a **Tovább** gombra.
3. A **cn** mezőbe írja be a Jose Alvirez karaktersorozatot.
4. Az ***sn** (vezetéknév) mezőben adja meg az Alvirez karaktersorozatot.
5. A ***cn** (teljes név) mezőben adja meg a Jose Alvirez karaktersorozatot. A cn szükséges a bejegyzés DN-jének létrehozásához. A *cn az objektum egyik attribútuma.
6. A **telephoneNumber** mezőben adja meg a 999 555 1234 számsort.
7. A **departmentNumber** mezőben adja meg a DEPTA karaktersorozatot.
8. A **mail** mezőben adja meg a jalvirez@sajat_ceg.com karaktersorozatot.
9. A **userPassword** mezőben adja meg a titok karaktersorozatot.
10. Kattintson a **Felhasználói csoportok** lapra.
11. A **Rendelkezésre álló csoportok** listából válassza ki a **managers** csoportot, 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: A System i5 adatok közzététele a címtár-adatbázisban

A közzététel beállítása lehetővé teszi, hogy a rendszer a felhasználói adatokat az LDAP címtárba automatikusan beírja. A rendszer terjesztési címtárának felhasználói információi közzétételre kerülnek az LDAP címtárban.

Megjegyzés: A System i navigátorban létrehozott felhasználókhoz a rendszer felhasználói profilt, illetve a rendszer terjesztési címtárában bejegyzést rendel. 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: A rendszer felvétele Directory Server felhasználóként:

1. Jelentkezzen be a webes adminisztrációs eszközre (http://**sajatRendszer.sajat_ceg.com**:9080/IDSWebApp/IDSjsp/Login.jsp) adminisztrátorként.
   a. Válassza ki az **LDAP hosztnév** lista **sajatRendszer.sajat_ceg.com** elemét.
   b. A **Felhasználónév** mezőben adja meg a cn=administrator karaktersorozatot.
   c. A **Jelszó** mezőben adja meg a secret karaktersorozatot.
   d. Kattintson a **Bejelentkezés** gombra.
2. Válassza ki a **Felhasználók és csoportok → Felhasználó hozzáadása** lehetőséget.
3. Válassza ki a **Tartomány** lista **employees** elemét.
4. Kattintson a **Tovább** gombra.
5. A **cn** mezőben adja meg a sajatRendszer.sajat_ceg.com karaktersorozatot.
6. Az ***sn** mezőben adja meg a sajatRendszer.sajat_ceg.com karaktersorozatot.
7. A ***cn** mezőben adja meg a sajatRendszer.sajat_ceg.com karaktersorozatot.
8. A **userPassword** mezőbe írja be, hogy titok.
9. Kattintson a **Felhasználói csoportok** lapra.
10. Válassza ki a **managers** csoportot.
11. Kattintson a **Hozzáadás →** gombra.
12. Kattintson a **Befejezés** gombra.

2. lépés: A rendszer beállítása adatok közzétételére:

1. A System i navigátorban kattintson a jobb egérgombbal a bal oldali navigációs területen található iSeries rendszerre, 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. Adja meg a sajatRendszer.sajat_ceg.com karaktersorozatot.
7. A **Mely DN alatt** mezőben adja meg a cn=employees,dc=sajat_ceg,dc=com karaktersorozatot.
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 a cn=sajatRendszer,cn=employees,dc=sajat_ceg,dc=com karaktersorozatot.
9. Kattintson a **Jelszó** elemre.
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, illetve hogy a rendszer tud-e az LDAP címtárhoz csatlakozni.
14. Kattintson az **OK** gombra.
15. Kattintson az **OK** gombra.

Példahelyzet részletek: Információk beírása a címtár-adatbázisba

Vezetőként Jose Alvirez most beírja és frissíti a saját osztályán dolgozók adatait. Jane Doe-ról további információkra is szüksége van. Jane Doe a rendszer egyik olyan felhasználója, amelynek információi közzétételre kerültek. Jose Alvirez John Smithről is be akar írni adatokat. John Smith nem a rendszer felhasználója. Jose Alvirez a következőket teszi:

1. lépés: Bejelentkezés a webes adminisztrációs eszközre:
Jelentkezzen be a webes adminisztrációs eszközre. (http://**sajatRendszer.sajat_ceg.com**:9080/IDSWebApp/IDSjsp/Login.) az alábbi módon:

1. Válassza ki az **LDAP hosztnév** lista **sajatRendszer.sajat_ceg.com** elemét.
2. A Felhasználónév mezőbe írja be, hogy cn=Jose Alvirez,cn=sajatceg employees,dc=sajat_ceg,dc=com.
3. A Jelszó mezőbe írja be, hogy titok.
4. Kattintson a **Bejelentkezés** menüpontra.

2. lépés: Az alkalmazott adatainak módosítása:

1. Kattintson a **Felhasználók és csoportok → Felhasználók kezelése** lehetőségre.
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** mezőben adja meg a DEPTA karaktersorozatot.
5. Kattintson az **OK** gombra.
6. Kattintson a **Bezárás** elemre.

3. lépés: Alkalmazottak adatainak felvitele:

1. Kattintson a **Felhasználók és csoportok → Felhasználó hozzáadása** lehetőségre.
2. Válassza ki a **Tartomány** legördülő menü **employees** elemét, majd kattintson a **Tovább** gombra.
3. A **cn** mezőben adja meg a John Smith karaktersorozatot.
4. Az ***sn** mezőben adja meg a Smith karaktersorozatot.

5. A ***cn** mezőben adja meg a John Smith karaktersorozatot.
6. A **telephoneNumber** mezőben adja meg a 999 555 1235 számsort.
7. A **departmentNumber** mezőben adja meg a DEPTA karaktersorozatot.
8. A **mail** mezőben adja meg a jsmith@sajat_ceg.com karaktersorozatot.
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:

Címtáradatbázis keresése az e-mail cím címjegyzék segítségével:
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, hogy a Lotus Notes 6 és a Microsoft Outlook Express 6 levelezőprogramot milyen módon lehet beállítani. Az eljárás más e-mail kliensek esetén is hasonló.

Lotus Notes:

1. Nyissa meg a címjegyzéket.
2. Kattintson a **Tevékenységek → Új → Fiók** menüpontra.
3. A **Fióknév** mezőben adja meg a sajatRendszer karaktersorozatot.
4. A **Fiókszerver neve** mezőben adja meg sajatRendszer.sajat_ceg.com karaktersorozatot.
5. Válassza ki a **Protokoll** mező **LDAP** elemét.
6. Kattintson a **Protokoll konfiguráció** lapra.
7. A **Keresés alapja** mező értéke dc=sajat_ceg,dc=com legyen.
8. Kattintson a **Mentés és bezárás** elemre.
9. Kattintson a **Létrehozás → Levél → Emlékeztető** menüpontra.
10. Kattintson a **Cím...** lehetőségre.
11. A **Címjegyzék kiválasztása** mezőben adja meg a sajatRendszer karaktersorozatot.
12. A **Keresett érték** mezőben adja meg az Alvirez karaktersorozatot.
13. Kattintson a **Keresés** gombra. Megjelennek Jose Alvirez adatai.

Microsoft Outlook Express:

1. Kattintson az **Eszközök → Fiókok** lehetőségre.
2. Kattintson a **Hozzáadás → Címtár szolgáltatás** lehetőségre.
3. Az **Internetes címtár (LDAP) szerver** mezőben adja meg a rendszer webcímét (sajatRendszer.sajat_ceg.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 sajatRendszer.sajat_ceg.com elemet (az imént beállított címtárszolgáltatást), majd kattintson a **Tulajdonságok** gombra.
9. Kattintson a **Speciális** lapra.
10. A **Keresés alapja** mező értéke dc=sajat_ceg,dc=com legyen.
11. Kattintson az **OK** gombra.
12. Kattintson a **Bezárás** elemre.
13. A Ctrl+E billentyűk lenyomásával hívja meg a **Személy keresése** ablakot.
14. Válassza ki a **Keresett adatok** lista sajatRendszer.sajat_ceg.com elemét.

15. A **Név** mezőben adja meg az Alvirez karaktersorozatot.
16. Kattintson a **Azonnali keresés** gombra. Megjelennek Jose Alvirez adatai.

Keresés a címtáradatbázisban 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 sajatRendszer.sajat_ceg.com –b
dc=sajat_ceg,dc=com objectclass=*
```

Ahol:

–h az LDAP szervert 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=sajat_ceg,dc=com
 dc=sajat_ceg
 objectclass=domain
 objectclass=top

 cn=MyCo employee,dc=sajat_ceg,dc=com

.
.
.

cn=Jose Alvirez,cn=MyCo Employees,dc=sajat_ceg,dc=com

sn=Alvirez
departmentNumber=DEPTA
mail=jalvirez@sajat_ceg.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 fájlnévhez 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=sajat_ceg,dc=com**.

Példahelyzet: Felhasználók másolása HTTP szerver ellenőrzési listából a Directory Server szerverre

Az alábbi példa bemutatja, hogy milyen módon másolhatók felhasználók a HTTP szerver ellenőrzési listából a Directory Server szerverre.

Körülmények és áttekintés

Van egy jelenleg (Apache) HTTP szerveren futó alkalmazása, amely a MYLIB/HTTPVLDL ellenőrzőlistában található internetes felhasználókkal dolgozik. Ugyanezeket az internetes felhasználókat kívánja használni a WebSphere Application Server (WAS) termékben, 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 címtárszerverre.
2. Állítsa be a WAS szervert az LDAP hitelesítés használatára.
3. Állítsa át a HTTP szervert, hogy az LDAP hitelesítést használja az ellenőrzőlista helyett.

1. lépés: A meglévő ellenőrzőlista-felhasználók átmásolása a helyi címtárszerverre

Ez a lépés feltételezi, hogy a címtárszerver előzőleg az ″o=sajat ceg″ utótaggal volt beállítva, és fut. Az LDAP felhasználóknak a ″cn=users,o=sajat ceg″ részfában kell lenniük. A címtárszerver adminisztrátorának megkülönböztetett neve ″cn=administrator″ és az adminisztrátori jelszó ″titok″.

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=sajat ceg' X'00000000' '' X'00000000'
X'00000000')
```

Ha kész, a címtárszerver inetorgperson bejegyzéseket fog tartalmazni az ellenőrzőlista bejegyzései alapján. A következő ellenőrzőlista-felhasználó esetében például:

```
Felhasználónév: jsmith
Leírás: John Smith
Jelszó: ******
```

a következő címtárbejegyzés keletkezik:

```
dn: uid=jsmith,cn=users,o=sajat ceg
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 címtárszerverhez. Az alábbi QSH ldapsearch parancs például ki fogja olvasni a kiszolgáló root DSE bejegyzését:

```
> ldapsearch -D "uid=jsmith,cn=users,o=sajat ceg" -w ****** -s base "(objectclass=*)"
```

Ha a címtárbejegyzések létrejöttek, akkor módosíthatók, hogy további információkat is tartalmazzanak. Lehet például, hogy módosítani kívánja a cn és sn értékeket a felhasználó teljes nevére és vezetéknevére, vagy fel szeretne venni egy telefonszámot és egy e-mail címet.

2. lépés: A WAS szerver beállítása az LDAP hitelesítés használatára

A WAS LDAP biztonsági szolgáltatást be kell állítani, hogy megkeresse a dn ″cn=users,o=sajat ceg″ 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 információkat a Websphere Application Server for iSeries információs központ LDAP keresőszűrők beállítása témaköre tartalmaz.

Állítsa át a HTTP szervert úgy, hogy az ellenőrzőlista helyett az LDAP hitelesítést használja

Megjegyzés: Az alábbiakban leírt eljárás a példahelyzetben leírt példák illusztrálását szolgálja azáltal, hogy magas szintű áttekintést nyújt a HTTP szever beállításáról az LDAP hitelesítés használatára. Ezzel kapcsolatosan szükség lehet az Implementation and Practical Use of LDAP on the IBM eServer iSeries Server, SG24-6193  IBM Redbooks kiadvány 6.3.2-es, ″Setting up LDAP authentication for the

powered by Apache server″ című szakaszában, illetve a Jelszavak védelem beállítása a HTTP Server szerveren (Apache) témakörben található információkra.

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. Végezze el a beállítást a fent hivatkozott Redbooks kiadványban leírtaknak megfelelően, majd 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=sajat ceg.
   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. Végezze el az LDAP szerver kapcsolatot a fent hivatkozott Redbooks kiadványban leírtaknak megfelelően.

Directory Server felügyelete

Az alábbi információk segítséget nyújtanak a Directory Server felügyelete során.

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 háttérobjektumok” oldalszám: 85), aki jogosultsággal bír a Directory Server adminisztrátori funkció azonosítójához. A legtöbb adminisztrációs feladatot az adminisztrátori csoportban található felhasználók is elvégezhetik (lásd: “Adminisztrátori hozzáférés” oldalszám: 64).

Általános adminisztrációs feladatok

Az alábbi információk segítséget nyújtanak a Directory Server általános felügyelete során.

Directory Server elindítása

Az alábbi információk segítséget nyújtanak a Directory Server elindítása során.

1. Az System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
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 a címtár szolgáltatót a Directory Server korábbi változatáról történő frissítést követően első alkalommal indítja el, az indulás a megszokottnál néhány perccel hosszabb időt

vehet igénybe, mivel a szervernek a fájlokat át kell állítania. Időről-időre ellenőrizheti a szerver állapotát (részletek: “Directory Server állapotának ellenőrzése”), hogy megállapítsa, leállt-e már.

A Directory Server a STRTCPSVR *DIRSRV parancs segítségével a karakteres felületről is elindítható. Amennyiben a címtárszervert úgy állította be, hogy a TCP/IP-vel egyidőben induljon, a STRTCP paranccsal is indíthatja azt.

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.

Kapcsolódó feladatok

“Directory Server leállítása”
Az alábbi információk segítséget nyújtanak a Directory Server leállítása során.

“Directory Server állapotának ellenőrzése”
Az alábbi információk segítséget nyújtanak a Directory Server állapotának ellenőrzése során.

Directory Server leállítása

Az alábbi információk segítséget nyújtanak a Directory Server leállítása során.

Megjegyzés: A Directory Server leállítása hatással van az összes olyan alkalmazásra, amely a szervert a leállítás pillanatában használja. 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.

1. Az System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
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: “Directory Server állapotának ellenőrzése”), hogy megállapítsa, leállt-e már.

A Directory Server a karakteralapú felületről is leállítható. A leállításhoz adja meg az ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL vagy ENDTCP parancsot. Az ENDTCPSVR *ALL és az ENDTCP parancs hatással van a rendszerben működő összes TCP/IP szerverre. Az ENDTCP parancs leállítja magát a TCP/IP-t is.

Kapcsolódó feladatok

“Directory Server elindítása” oldalszám: 116
Az alábbi információk segítséget nyújtanak a Directory Server elindítása során.

Directory Server állapotának ellenőrzése

Az alábbi információk segítséget nyújtanak a Directory Server állapotának ellenőrzése során.

Az alapszintű állapotinformációkat a System i navigátor tartalmazza. Ennél bővebb információk is találhatók a webes adminisztrációs eszköz használatával.

A System i navigátor a jobb keret **Állapot** oszlopában megjeleníti a Directory Server állapotát.

Ha a Directory Server állapotát a System i navigátorban ellenőrizni kívánja, akkor tegye a következőket:

1. Bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** kategóriát.

3. Kattintson a **TCP/IP** lehetőségre. A System i 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** feliratra, 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 is frissítheti a Directory Server állapotát, hogy a többi TCP/IP szerver állapotfrissítését is ki kellene várnia.

A címtárszerver állapotának ellenőrzéséhez a webes adminisztrációs eszközben tegye a következőket:

1. Bontsa ki a **Szerveradminisztráció** kategóriát a navigációs területen.

   Megjegyzés: A szerver konfigurációs beállításainak módosításához a webes adminisztrációs eszköz Szerveradminisztráció kategóriájának használatával hitelesítenie kell magát a szerveren egy olyan 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. Kattintson a **Szerverállapot megjelenítése** menüpontra.
3. A **Szerverállapot megjelenítése** panelben válassza ki a különféle lapokat az állapotinformációk megjelenítésére.

Jobok ellenőrzése a Directory Server szerveren

Az alábbi információk segítséget nyújtanak a Directory Server szerveren futó adott jobok megfigyelése során.

Ha a szerverjobokat a System i navigátorban kívánja megfigyelni, akkor tegye a következőket:

1. Az System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Szerver feladatok** menüpontot.

Szerverkapcsolatok kezelése

Az alábbi információk segítséget nyújtanak a szerverrel fennálló kapcsolatok és a kapcsolatokon végrehajtott műveletek megjelenítése során.

Az adminisztrátor ezután a kapcsolatok alapján döntéseket tud hozni a hozzáférés felügyeletével és a szolgáltatás megbénításos (DOS) támadások megelőzésével kapcsolatban. Erre a webes adminisztrációs eszköz ad lehetőséget.

Megjegyzés: A szerver konfigurációs beállításainak módosításához a webes adminisztrációs eszköz Szerveradminisztráció kategóriájának használatával hitelesítenie kell magát a szerveren egy olyan i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultsággal. 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.

1. Bontsa ki a **Szerveradminisztráció** kategóriát a navigációs területen.
2. Kattintson a **Szerverkapcsolatok kezelése** lehetőségre.

   Megjelenik egy táblázat, amely a következő információkat tartalmazza az egyes kapcsolatokról:

   DN Megadja a szerverre csatlakozó kliens megkülönböztetett nevét.

IP cím 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 aktívnak, 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, hgoy a táblázat elemei csökkenő vagy növekvő sorrendben legyenek-e rendezve.

3. Az aktuális kapcsolati információk frissítéséhez kattintson a **Frissítés** gombra.
4. 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 szolgáltatásmegbénításos (DOS) támadásokat és kézben 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 szolgáltatás megbénításos támadások elleni védekezéssel kapcsolatos további információkért tekintse meg a Kapcsolattulajdonságok kezelése részt.

Kapcsolódó fogalmak

“Szolgáltatás megbénítása” oldalszám: 85
A szolgáltatás megbénítása támadások ellen a szolgáltatás megbénítása konfigurációs beállítás segítségével védekezhet.

Kapcsolódó feladatok

“Kapcsolat tulajdonságainak kezelése”
Az alábbi információk segítséget nyújtanak a kapcsolat tulajdonságainak beállítása során, például azon tulajdonságokénál, amelyek megakadályozzák, hogy a kliensek zároljanak egy szervert.

Kapcsolat tulajdonságainak kezelése

Az alábbi információk segítséget nyújtanak a kapcsolat tulajdonságainak beállítása során, például azon tulajdonságokénál, amelyek megakadályozzák, hogy a kliensek zároljanak egy szervert.

A kapcsolati tulajdonságok felügyeletének lehetősége módot ad annak megakadályozására, hogy a kliensek zárolják a szervert. Ez biztosítja azt is, hogy az adminisztrátor mindig elérheti a szervert 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 webes adminisztrációs eszköz Szerveradminisztráció kategóriájának használatával hitelesítenie kell magát a szerveren egy olyan i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultsággal. 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. Kattintson az **Általános** lapra.
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 meghibásodhatnak 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 **Üresjárati 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 **Üresjárati 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 **Üresjárati időkorlát** mezőben megadott határérték alapján törlésre kerülnek.
7. Az **Üresjárati időkorlát** mezőben állítsa be, hogy egy kapcsolat hány másodpercig lehet tétlen, mielőtt azt egy törlési műveled 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 lapcsolatokat az operációs rendszer automatikusan eldobja. Ennek következtében ezt az **Eredmény időkorlátot** az operációs rendszer 30 másodperc után hatályon kívül helyezi.

9. Kattintson a **Sürgősségi szál** lapra.
10. Adja meg a vészszál beállításait. A **Vészszál engedélyezése** jelölőnégyzet már ki van választva, vagyis a vészszál engedélyezett. Ez az alapértelmezett beállítás. A jelölőnégyzetre kattintva megszüntetheti a **Vészszál engedélyezése** lehetőség kiválasztását. Ezzel a művelettel megelőzhető a vészszál aktiválása.
11. A **Függőben lévő kérések küszöbértéke** mezőben állítsa be a vészszálat aktiváló kérések számának korlátját. Adjon meg egy 0 és 65535 közötti számot, amellyel beállítja, hogy hány feladatkérés lehet a várakozási sorban, mielőtt a vészszál aktiválásra kerül. Az alapértelmezett beállítás az 50. Ha a megadott korlát meghaladásra kerül, a vészszál 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 vészszál aktiválásra kerül. 0 és 240 közötti szám adható meg. Az alapértelmezett beállítás 5.
13. Válassza ki a legördülő menüből a vészszál aktiválására használt feltételeket. A következők közöl választhat:
    - **Csak méret:** A vészszál csak akkor kerül aktiválásra, ha a várakozási sorban a függőben lévő munkák meghaladják a megadott mennyiséget.
    - **Csak idő:** A vészszál csak akkor kerül aktiválásra, ha az eltávolított feladatok időkorlátja meghaladja a megadott mennyiséget.
    - **Méret vagy idő:** A vészszál akkor kerül aktiválásra, ha vagy a sorméret, vagy az időkorlát meghaladja a megadott mennyiséget.
    - **Méret és idő:** A vészszál 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.

Kapcsolódó fogalmak

“Szolgáltatás megbénítása” oldalszám: 85
A szolgáltatás megbénítása támadások ellen a szolgáltatás megbénítása konfigurációs beállítás segítségével védekezhet.

Kapcsolódó feladatok

“Szerverkapcsolatok kezelése” oldalszám: 118
Az alábbi információk segítséget nyújtanak a szerverrel fennálló kapcsolatok és a kapcsolatokon végrehajtott műveletek megjelenítése során.

Eseményértesítés engedélyezése

Az információk segítséget nyújtanak a Directory Server eseményértesítés engedélyezése során.

Az eseményértesítésnek köszönhetően a kliensek bejegyezhetik magukat a Directory Server szerverre, hogy egy megadott eseményről (például arról, ha a címtárhoz valami hozzáadásra kerül) értesítést kapjanak.

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 eseményértesítéssel kapcsolatosan további információkat az IBM Tivoli Directory Server 6.0 programozási kézikönyv Eseményértesítés szakasza tartalmaz.

Kapcsolódó tájékoztatás

IBM Tivoli szoftver információs központ
Az IBM Tivoli Directory Server termékkel kapcsolatosan további információkat az IBM Tivoli szoftver információs központ tartalmaz.

Tranzakciós beállítások megadása

Az alábbi információk segítséget nyújtanak a Directory Server tranzakciós beállításainak megadása során.

A Directory Server tranzakciók lehetővé teszik, hogy az LDAP címtárműveletek egy csoportját a rendszer egy egységként kezelje.

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.

Kapcsolódó fogalmak

“Tranzakciók” oldalszám: 51
A Directory Server beállítható úgy, hogy megengedje a klienseknek tranzakciók használatát. Egy tranzakció LDAP címtárműveletek csoportja, amit a címtár egyetlen egységként kezel.

Port vagy IP cím módosítása

Az alábbi eljárás segítségével módosíthatók a Directory Server által használt portok, illetve azok az IP címek, amelyeken a Directory Server kapcsolatokat elfogad.

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 szerverhez, vagy különböző IP címeket használ a két szerverre, ha az alkalmazások támogatják az adott IP címhez rendelést.

Ha módosítani kívánja a Directory Server által használt portokat, illetve azok az IP címeket, amelyeken a Directory Server kapcsolatokat elfogad, akkor tegye a következőket:

1. A System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Tulajdonságok** menüpontot.
5. Kattintson a **Hálózat** lapra.
6. Ha a portszámot módosítani kívánja, akkor írja be a kívánt portszámokat, majd kattintson az **OK** gombra.
7. Ha az IP címet módosítani kívánja, akkor kattintson az **IP címek...** gombra. Ezután folytassa a következő lépésnél.
8. Válassza ki a **Megjelölt IP címek használata** lehetőséget, majd válassza ki a szerver számára a kapcsolatok elfogadásakor használandó IP címeket.

Kapcsolódó tájékoztatás

Host Domino LDAP és Directory Server ugyanazon a rendszeren

Szerver kijelölése címtári utalások részére

Az alábbi információk segítséget nyújtanak az utalási szerverek meghatározása során.

Ha utalási szervereket kíván hozzárendelni a Directory Server szerverhez, akkor tegye a következőket:

1. Az System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Properties** menüpontot.
5. Válassza ki az **Általános** adatlapot.
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.

Kapcsolódó fogalmak

"LDAP címtárutalások" oldalszám: 51
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.

Directory Server utótagok felvétele és eltávolítása

Az alábbi információk segítséget nyújtanak a Directory Server utótagok felvétele és eltávolítása során.

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. A System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb egérgombbal az **IBM Directory Server** elemre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
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. A System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb egérgombbal az **IBM Directory Server** elemre, majd válassza az előugró menü **Tulajdonságok** menüpontját
5. Kattintson az **Adatbázis/utótagok** lapra.
6. Kattintással válassza ki azt az utótagot, amelyet törölni kíván.
7. Kattintson az **Eltávolítás** gombra.

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

Kapcsolódó fogalmak

"Utótag (névkontextus)" oldalszám: 13
Az utótag (más néven névkontextus) egy olyan DN, amely egy helyileg tárolt címtárhierarchia legfelső bejegyzését azonosítja.

Utótag hozzáadása a címtárszerverhez:

Ha utótagot kíván felvenni a címtárszerverbe, kövesse az alábbi lépéseket:

1. A System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Tulajdonságok** 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.

Utótag eltávolítása a címtárszerverről:
A Directory Server egy utótagjának eltávolítása:

1. A System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Tulajdonságok** menüpontot.
5. Kattintson az **Adatbázis/utótagok** lapra.
6. Kattintással válassza ki azt az utótagot, amelyet törölni kíván.
7. Kattintson az **Eltávolítás** gombra.

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

Adminisztrátori hozzáférés biztosítása leképezett felhasználók számára

Az alábbi információk segítséget nyújtanak a felhasználói profiloknak adminisztrátori hozzáférés megadása során.

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.

Az Adminisztrátori hozzáférés biztosítása a jogosult felhasználóknak lehetőség, illetve a Directory Server adminisztrátori funkció azonosító kiválasztásához tegye a következőket:

1. A System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a jobb egérgombbal a **Címtár** elemre, és válassza ki a **Tulajdonságokat**.
4. Az **Adminisztrátor információk** alatti **Általános** lapon válassza ki az **Adminisztrátori hozzáférés megadása a hitelesített felhasználók számára** lehetőséget.
5. A System i navigátorban kattintson a jobb egérgombbal a rendszernévre, majd válassza az előugró menü **Alkalmazások adminisztrációja** menüpontját.

6. Kattintson a **Hosztalkalmazások** lapra.
7. Bontsa ki az **Operating System/400** elemet.
8. Kattintson a **Directory Server Administrator** elemre, melynek hatására az megjelölődik.
9. Kattintson a **Személyre szabás** gombra.
10. Bontsa ki a **Felhasználók**, **Csoportok** vagy a **Nem csoporttag felhasználók** részt, amelyik megfelelő a felhasználó esetében.
11. Válassza ki a **Hozzáférés engedélyezett** listához hozzáadandó felhasználót vagy csoportot.
12. Kattintson a **Hozzáadás** gombra.
13. A módosítások mentéséhez kattintson az **OK** gombra.
14. Kattintson az **OK** gombra az **Alkalmazás-adminisztráció** párbeszédablakban.

Kapcsolódó fogalmak

"Adminisztrátori hozzáférés" oldalszám: 64
Az adminisztrátori hozzáférés segítségével vezérelhető az adott adminisztrációs feladatok elérhetősége.

"Operációs rendszer leképzett háttérobjektumok" oldalszám: 85
A rendszer leképezett háttér objektumai funkció az i5/OS objektumokat leképezi az LDAP által elérhető címtárfán belüli bejegyzésekre. A leképzett objektumok az operációs rendszer objektumok LDAP reprezentánsai, amelyeket az LDAP szerver adatbázisában tárolt tényleges bejegyzés helyett használunk.

Nyelvi címkék engedélyezése

Az alábbi információk segítséget nyújtanak a nyelvi címkék engedélyezése során.

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 webes adminisztrációs eszköz Szerveradminisztráció kategóriájának használatával hitelesítenie kell magát a szerveren egy olyan i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultsággal. 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 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 megelőzhetők legyenek, ha egyszer bekapcsolta, akkor már ne kapcsolja ki a nyelvi címke funkciót.

LDAP címtár eléréseinek és változásainak nyomon követése

Az alábbi információk segítséget nyújtanak az LDAP címtár eléréseinek és változásainak nyomon követése során.

Az LDAP címtárak változásait tartalmazó napló segítségével nyomon követheti a címtár 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. A System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.

4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Tulajdonságok** menüpontot.
5. Kattintson a **Napló módosítása** lapra.
6. Válassza ki a **Címtárváltozások naplózása** elemet.
7. Választható: A **Bejegyzések maximális száma** 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 címtárszerverre 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=adminisztrátor -w jelszó
-b cn=changelog  (changetype=*)
```

Directory Server objektumfelügyelet engedélyezése

Az alábbi információk segítséget nyújtanak a Directory Server objektumfelügyelet engedélyezése során.

A Directory Server támogatja az i5/OS biztonsági felügyeletet. Ha a QAUDCTL rendszer értékben *OBJAUD került beállításra, akkor a System i navigátor segítségével engedélyezhető az objektumok naplózása.

A Directory Server szerverhez az objektumfelügyelet az alábbi lépésekkel engedélyezhető:

1. A System i navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Tulajdonságok** menüpontot.
5. Kattintson a **Felügyelet** 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.

Kapcsolódó fogalmak

“Felülvizsgálat” oldalszám: 52
A felülvizsgálat segítségével nyomon követhetők bizonyos Directory Server tranzakciók részletei.

“Directory Server biztonság” oldalszám: 52
Ismerje meg azokat a funkciókat, amelyeknek köszönhetően a Directory Server biztonságosabbá tehető.

Keresési beállítások módosítása

Az alábbi információk segítséget nyújtanak a felhasználó keresési képességeinek vezérlése során.

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 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 szolgálva.

A rendezett keresés eredményeit a kliens egy feltétellista szerint rendezett formában kapja vissza, ahol az egyes feltételek rendezési kulcsokat reprezentálnak. A rendezés feladata ily 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 webes adminisztrációs eszköz Szerveradminisztráció kategóriájának használatával hitelesítenie kell magát a szerveren egy olyan i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultsággal. 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 keresésikorlát-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 keresésikorlát-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 **Álnévhivatkozás-feloldás** menüpontot és válassza ki a következők valamelyikét. Az alapértelmezett beállítás a **Mindig**.

   Soha Az álnevek soha nem kerülnek feloldásra.

   Keresés
   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.

Kapcsolódó feladatok

“Címtárbejegyzések keresése” oldalszám: 198
Az alábbi információk segítséget nyújtanak a címtárbejegyzések keresése során.

Kapcsolódó hivatkozás

“Keresési paraméterek” oldalszám: 48
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.

Leképezett felhasználók olvasási hozzáférésének engedélyezése vagy letiltása

Az alábbi információk segítséget nyújtanak a felhasználói leképzett háttér objektumokat érintő kereső és összehasonlító műveletek letiltása során.

A felhasználói leképezett háttér objektumokat érintő kereső és összehasonlító műveletek letiltásához tegye a következőket:

1. Állítsa le a címtárszervert. Írja be a következő parancsot: ENDTCPSVR *DIRSRV.
2. Módosítsa a /QIBM/UserData/OS400/DirSrv/ibmslapd.conf fájlt. Például írja be a következőt: EDTF '/QIBM/UserData/OS400/DirSrv/ibmslapd.conf'.
3. Keressen rá a következő szövegre: cn=Front End.
4. A cn=Front End tartalmazó sor után közvetlenül szúrjon be egy új, ibm-slapdSetEnv: IBMSLAPDOS400USRPRJREAD=FALSE szöveget tartalmazó sort. Az alábbi példában a második sor került beszúrásra:

   ```
   dn: cn=Front End, cn=Configuration
   ibm-slapdSetEnv: IBMSLAPDOS400USRPRJREAD=FALSE
   cn: Front End
   ```

5. Mentse el a fájlt, majd lépjen ki a szövegszerkesztőből. EDTF használata esetén például az F2 segítségével mentse el a fájlt, majd az F3 segítségével lépjen ki a szövegszerkesztőből.
6. Indítsa újra a címtárszervert. Írja be a következő parancsot: STRTCPSVR *DIRSRV.

Kapcsolódó fogalmak

“Olvasási hozzáférés leképezett felhasználók számára” oldalszám: 90
Alapértelmezésben a rendszer a leképzett háttér objektum olvasási hozzáférést a felhasználói profil információkhoz az erre jogosult felhasználóknak az LDAP kereső és összehasonlító műveleteken keresztül biztosítja. A leképezett felhasználók számára az olvasási hozzáférés a System i navigátor, illetve a /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf fájl (az alapértelmezett szerverpéldány esetében /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf fájl) konfigurációs paraméterének segítségével engedélyezhető, illetve tiltható le.

Információk publikálása a címtárszervernek

Az alábbi információk segítséget nyújtanak az információk Directory Server szerveren történő közzététele során.

Rendszerét úgy konfigurálhatja, hogy az bizonyos információkat, , valamint a felhasználó által megadott információkat közzétegyen ugyanazon a rendszeren vagy egy másik rendszeren található Directory Server számára. Ezeket az információkat az operációs rendszer automatikusan közzéteszi a Directory Server szervernek akkor, amikor a System i navigátor segítségével az i5/OS rendszerben ezeket az információkat módosítja. A közzétehető információk lehetnek rendszer (több rendszerre és nyomtatóra vonatkozó) információk, nyomtatásmegosztási és felhasználói információk, illetve TCP/IP QoS szabályok.

Ha az a szülő DN, amely számára az adatok közzétételre kerülnek, nem létezik, akkor azt a Directory Server automatikusan létrehozza. Más olyan i5/OS alkalmazásokat is telepíthet, amelyek egy LDAP címtárban információkat tesznek közzé. Továbbá alkalmazásprogram csatolókat (API-kat) is meghívhat a saját programjából, hogy más típusú adatokat tegyen közzé az LDAP címtárban.

Megjegyzés: i5/OS információkat nem i5/OS felügyelete alatt működő címtárszerver számára is közzétehet, amennyiben ez a szerver az IBM séma használatára beállított.

Ha rendszerét úgy kívánja beállítani, hogy egy címtárszerver számára i5/OS információkat tegyen közzé, akkor tegye a következőket:

1. Az System i navigátorban a jobb oldali egérgombbal kattintson rendszerére, és válassza a **Tulajdonságok** lapot.
2. Kattintson a **Directory Server** lapra.
3. Válassza ki a közzétenni kívánt információtípusokra. Válassza ki a közzétenni kívánt információtípusokra.

   Tipp: Ha egynél többféle információtípust kíván küldeni ugyanarra a helyre, időt takaríthat meg, ha egyszerre több információtípust választ ki beállítás céljából. A Műveletek navigátor az első információtípushoz beadott értéket alapértelmezett értéknek fogja tekinteni a többi információtípus beállításánál.
4. Kattintson a **Részletek** pontra.
5. Kattintson a **Rendszerinformációk közzététele** jelölőnégyzetre.
6. Adja meg a szerveren használni kívánt **hitelesítési módszert**, továbbá a megfelelő hitelesítési információkat.
7. Kattintson az **(aktív) címtárszerver** mező melletti **Módosítás** gombra. A megjelenő kiugró párbeszédablakban adja meg annak a címtárszervernek a nevét, amelyen az i5/OS információt közzé kívánja tenni, majd kattintson az **OK** gombra.
8. Az **Under DN** mezőben adja meg annak a szülőnek az egyedi nevét (DN), ahonnan információt kíván a címtárszervernek átadni.
9. Töltse ki a **Szerverkapcsolat** keretben azokat a mezőket, melyek megfelelnek konfigurációjának.

   Megjegyzés: Ha a címtárszerver felé i5/OS információkat SSL vagy Kerberos segítségével kíván közzé tenni, akkor először állítsa be címtárszerverét a megfelelő protokoll használatára. További információk az SSL és Kerberos használatával kapcsolatban: “Kerberos hitelesítés használata Directory Server-rel” oldalszám: 54.
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: i5/OS információk egy másik platformon működő címtárszerver számára is közzétehetők. Felhasználói és rendszer információk egy címtárszerveren csak akkor tehetők közzé, ha a címtárszerver az IBM Directory Server sémával kompatibilis sémát használ. Az IBM címtár sémájával kapcsolatos további információk: “Directory Server séma” oldalszám: 15.

Az LDAP szerverkonfiguráció és a közzétételi alkalmazás programozási felületek segítségével a saját fejlesztésű i5/OS programoknak is lehetővé tehető az egyéb típusú információk közzététele. Ezután ezek az információtípusok 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 CSVR0500 formátumot használja a kezdeti ügynöknév hozzáadásához, amely a letiltott tételek között szerepel. Az alkalmazás felhasználóinak szóló leírásokban utasítsa őket, hogy az System i 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.

Kapcsolódó fogalmak

“Közzététel” oldalszám: 36
A Directory Server 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.

Directory Server alkalmazás programozási felületek

LDIF fájl importálása

Ezen információk segítségével importálhat LDAP adatcsere formátum (LDIF) fájlt.

Különböző Directory Server-ek között az információcsere LDAP Data Interchange Format (LDIF) formátumú fájlokkal lehetséges. Az importáló eszköz (és a megfelelő QgldImportLdif API) új bejegyzéseket ad a címtárhoz. Az importáló eszközzel nem módosíthatók és törölhetők bejegyzések, illetve az LDIF fájlnak a címtártartalom-stílust kell használnia a módosítási rekord stílusú LDIF rekordok helyett. Ha a bemeneti LDIF fájl tartalmazza a módosítási rekord stílusú LDIF rekordokban használt changetype direktívákat, akkor a changetype sor más attribútumhoz hasonlóan kerül értelmezésre, és a bejegyzés nem kerül hozzáadásra a címtárhoz.

Jellemző használat esetén a teljes címtár, vagy a címtár részfája exportálásra kerül egy szerverről az exportáló eszköz (vagy a QgldExportLdif API) segítségével, majd importálásra kerül másik szerverre.

Az exportáló és importáló eszköz nem egyenértékű az ldapsearch és ldapadd parancssori segédprogramok használatával. Az exportáló eszköz számos működési attribútumot (mint például a hozzáférés-felügyeleti információk, és a bejegyzéslétrehozásai időbélyegek) tartalmaz, amelyet normális esetben az ldapsearch nem ad vissza, miközben az importáló eszköz be tud állítani olyan attribútumokat, amelyeket a kliensalkalmazás - mint például az ldapadd - normális esetben nem tud beállítani. Az ldapadd segédprogram használható a -k paraméterrel (kiszolgálóadminisztráció-felügyelet) ezen fájlok betöltéséhez.

Mielőtt elindítaná ezt a műveletet, vigye át adatfolyam fájlként az LDIF fájlt a rendszerre.

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 elindítása” oldalszám: 116.
2. Az System i navigátorban bontsa ki a **Hálózat** részt.
3. Bontsa ki a **Szerverek** elemet.
4. Kattintson a **TCP/IP** lehetőségre.
5. Kattintson a jobb oldali egérgombbal az **IBM Directory Server** lehetőségre, és válassza az előugró menü **Eszközök**, majd **Fájl importálása** menüpontját.

   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) szervert, 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.

Kapcsolódó hivatkozás

“LDAP adatcsere formátum (LDIF)” oldalszám: 248
Az LDAP adatcsere formátum az LDAP objektumok és frissítések (hozzáadás, módosítás, törlés, DN módosítás) szöveges ábrázolásához. Az LDIF rekordokat tartalmazó fájlok segítségével adatok vihetők át a címtárszerverek között, vagy az LDAP eszközök - mint például az **ldapadd** és **ldapmodify** - bemenetként használhatják.

“ldapmodify és ldapadd” oldalszám: 216
Az LDAP modify-entry (bejegyzésmódosító) és LDAP add-entry (bejegyzés-felvevő) parancssori segédprogram.

LDIF fájl exportálása

Az alábbi információk segítséget nyújtanak az LDAP adatcsere formátum (LDIF) fájl exportálása során.

Különböző LDIF fájlok között információk vihetők át. LDIF fájlba menthető az LDAP címtár egésze vagy csak egy része.

Egy LDIF fájl exportálása a címtárszerverből:

1. A System i navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb oldali egérgombbal az **IBM Directory Server** lehetőségre, majd válassza az előugró menü **Eszközök**, majd **Fájl exportálása** menüpontját.

   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. Használja az -L kapcsolót és irányítsa fájlba a kimenetet.
3. Ne felejtsen el az LDIF fájlra megfelelő jogosultságot beállítani, hogy megakadályozza a jogosulatlan hozzáférést a címtárhoz. Ehhez a System i navigátorban kattintson a jobb egérgombbal a fájlra, majd válassza az előugró menü **Jogosultságok** menüpontját.

Kapcsolódó hivatkozás

“LDAP adatcsere formátum (LDIF)” oldalszám: 248
Az LDAP adatcsere formátum az LDAP objektumok és frissítések (hozzáadás, módosítás, törlés, DN módosítás) szöveges ábrázolásához. Az LDIF rekordokat tartalmazó fájlok segítségével adatok vihetők át a címtárszerverek között, vagy az LDAP eszközök - mint például az **ldapadd** és **ldapmodify** - bemenetként használhatják.

“ldapsearch” oldalszám: 234
Az LDAP keresés parancssori segédprogram.

Felhasználók másolása HTTP szerver ellenőrzési listából a Directory Server szerverre

Az alábbi információk segítséget nyújtanak a felhasználók HTTP szerver ellenőrzési listából Directory Server szerverre történő másolása során.

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 beolvassa az ellenőrzőlista bejegyzéseit, majd létrehozza a megfelelő LDAP objektumokat a helyi címtárszerverből. Az objektumok userPassword attribútummal rendelkező váz inetOrgPerson bejegyzések, 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.

Például:

```
CALL PGM(QSYS/QGLDCPYVL) PARM('HTTPVLDL  MYLIB     ' 'cn=administrator'
X'00000000' 'secret' X'00000000' 'cn=users,o=sajat ceg' X'00000000' '' X'00000000'
X'00000000')
```

Kapcsolódó fogalmak

Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek
A Directory Server alkalmazás programozási felületekkel kapcsolatosan további információkat az Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek témakör tartalmaz.

Kapcsolódó feladatok

“Példahelyzet: Felhasználók másolása HTTP szerver ellenőrzési listából a Directory Server szerverre” oldalszám: 114
Az alábbi példa bemutatja, hogy milyen módon másolhatók felhasználók a HTTP szerver ellenőrzési listából a Directory Server szerverre.

Példányok kezelése

Az i5/OS rendszeren több címtárszerver is futhat. Az egyes szerverek az ún. példányok. Ha a címtárszervert az i5/OS egy korábbi kiadása alatt használta, akkor a címtárszerver QUSRDIR példány néven átállításra kerül. Az alkalmazások kiszolgálásához több címtárszerver-példány is létrehozható.

A címtárszerver-példányok egyedisége az adja meg, hogy a példány mely IP címen és/vagy porton figyel. Minden futó címtárszerver-példánynak egyedi adatbázissal, változásnaplóval és konfigurációs fájllal kell rendelkeznie. Létrehozhat és beállíthat ütköző szerverpéldányokat, azonban ha megpróbál elindítani egy másik példánnyal ütköző szerverpéldányt, akkor a második példány nem indul el és hibaüzenet kerül kiadásra.

A címtárszerver-példány tartalmazza a címtárszerver számítógépen való futtatásához szükséges összes fájlt.

A címtárszerver-példány fájlok a következőket tartalmazzák:

- Az ibmslapd.conf fájl (a konfigurációs fájl)
- Sémafájlok
- Naplófájlok
- Ideiglenes állapotfájlok

A címtárszerver-példány fájljait az idsslapd-*példánynév* nevű címár tárolja, ahol a *példánynév* a címtárszerver-példány neve. Az idsslapd-*példánynév* címtár a /QIBM/UserData/OS400/DirSrv címtárban található.

A címtárszerver-példányok létrehozáskor bejegyeznek egy új alkalmazást a Digitális igazolás kezelőben (DCM). Az új címtárszerver-példányok neve QIBM_DIRECTORY_SERVER_ <példánynév>. A DCM segítségével digitális igazolást kell rendelni a címtárszerver-példányhoz, ha SSL-t kíván használni. Az egyes címtárszerver-példányok induláskor a System i navigátorban szerverként bejegyzésre kerülnek, ezáltal a System i navigátor segítségével nyomon követhetők.

A címtárszerver-példány jobjának neve a megegyezik a példánynévvel. A QUSRDIR példány teljes képzésű jobneve például xxxxxx/QDIRSRV/QUSRDIR. Az ’xxxxxx’ a jobszám, amely a job indulásakor kerül meghatározásra. A címtárszerver használó felhasználók esetén ez eltérő, mivel ebben az esetben a jobnév az xxxxxx/QDIRSRV/QDIRSRV.

A példányok kezeléséhez tegye a következőket:

1. A System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** elemet.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb egérgombbal az **IBM Tivoli Directory Server** elemre, majd válassza az előugró menü **Példányok kezelése** menüpontját.

Ha rendszeres időközönként elmenti a példányokat, akkor a <*példánynév*>CF címtárat az adatbáziscímtárral együtt kell elmenteni.

Adminisztrációs csoport feladatok

Az alábbi információk segítséget nyújtanak az adminisztrátori csoportok felügyelete során.

A adminisztrátori csoport lehetőséget ad az adminisztrációs szolgáltatások ellátására anélkül, hogy az adminisztrátoroknak egyetlen azonosítón és jelszón kellene osztozniuk. Az adminisztrátori csoport tagjainak saját azonosítójuk és jelszavuk van. Az adminisztrátori 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 adminisztrátori csoporttag megkülönböztetett nevével sem.

Ez a szabály az IBM Directory Server adminisztrátorok és az adminisztrátori csoporttagok Kerberos vagy Digest-MD5 azonosítóira is vonatkozik. Ezeknek a megkülönböztetett neveknek nem szabad megegyezniük az IBM Directory Server replikációszolgáltató DN-jeivel. Ez azt is jelenti, hogy az IBM Directory Server replikációszolgáltató DN-jeinek nem szabad egyezniük egyetlen adminisztrátori csoporttag vagy az IBM Directory Server adminisztrátor DN-jével sem.

Megjegyzés: Az IBM Directory Server replikációszolgáltató DN-jei megegyezhetnek egymással.

Kapcsolódó fogalmak

“Adminisztrátori hozzáférés” oldalszám: 64
Az adminisztrátori hozzáférés segítségével vezérelhető az adott adminisztrációs feladatok elérhetősége.

Adminisztrációs csoport engedélyezése

Az alábbi információk segítséget nyújtanak az adminisztrátori csoport engedélyezése során.

Ennek a műveletnek az elvégzéséhez IBM Directory Server adminisztrátornak kell lennie.

1. Bontsa ki a **Szerveradminisztráció** kategóriát a webes adminisztrációs eszköz navigációs területén, és kattintson az **Adminisztrációs csoportok kezelése** lehetőségre.

   Megjegyzés: A szerver konfigurációs beállításainak módosításához a webes adminisztrációs eszköz Szerveradminisztráció kategóriájának használatával hitelesítenie kell magát a szerveren egy olyan i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultsággal. 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 adminisztrátori csoport engedélyezéséhez vagy letiltásához kattintson az **Adminisztrációs csoport engedélyezése** melletti jelölőnégyzetre. Ha a jelölőnégyzet ki van jelölve, akkor az adminisztrátori csoport engedélyezett.
3. Kattintson az **OK** gombra.

   Megjegyzés: Ha letiltja az adminisztrátori 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

Az alábbi információk segítséget nyújtanak az adminisztrátori csoport tagjainak hozzáadása, módosítása, illetve eltávolítása során.

Előfeltétel: Ennek a műveletnek az elvégzéséhez IBM Directory Server adminisztrátornak kell lennie.

1. Bontsa ki a **Szerveradminisztráció** kategóriát a webes adminisztrációs eszköz navigációs területén, és kattintson az **Adminisztrációs csoportok kezelése** lehetőségre.

   Megjegyzés: A szerver konfigurációs beállításainak módosításához a webes adminisztrációs eszköz Szerveradminisztráció kategóriájának használatával hitelesítenie kell magát a szerveren egy olyan i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultsággal. 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. Választható: Írja be 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. Választható: Adja meg a tag **Digest-MD5 felhasználói nevét**.

   Megjegyzés: A Digest-MD5 felhasználónévben a kis- és nagybetűk különbözőnek számítanak.
5. Kattintson az **OK** gombra.
6. Ismételje meg az eljárást minden, az adminisztrátori 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 adminisztrátori csoport tagjainak módosításához vagy eltávolításához is a fent leírtakat kell tennie, de az **Adminisztrációs csoport** panelben használja a **Szerkesztés** és **Törlés** gombokat.

Az adminisztrátori csoport tagjának jelszava módosítható a Change Directory Server Attr (CHGDIRSVRA) parancs segítségével is. Ha a cn=adminuser1 csatlakozási megkülönböztetett névvel rendelkező adminisztrátori csoport tag jelszavát ujjelszo értékre kívánja módosítani, akkor azt a következő parancs segítségével teheti meg:

```
CHGDIRSVRA
INSTANCE(QUSRDIR) DN('cn=adminuser1' 'ujjelszo')
```

Keresésikorlát-csoport feladatok

Az alábbi információk segítséget nyújtanak a keresésikorlát-csoportok kezelése során.

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 felhasználókénál sokkal rugalmasabb keresési korlátokkal rendelkező keresésikorlát-csoportokat hozhatnak létre. Ezen a módon az adminisztrátor speciális keresési jogosultságokat adhat felhasználói csoportoknak.

A keresésikorlát-csoportok felügyeletére a webes adminisztrációs eszköz használható.

Kapcsolódó hivatkozás

“Keresési paraméterek” oldalszám: 48
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.

Keresésikorlát-csoport létrehozása

Az alábbi információk segítséget nyújtanak keresésikorlát-csoport létrehozása során.

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. A szám 0 és 2 147 483 647 közé eshet. A 0 érték megadása ugyanaz, mint a **Korlátlan**.
   - Az **ibm-searchTimeLimit** mezőben adja meg a másodpercek számát, amelyek szerint a keresés időtartamát korlátozni kell. A szám 0 és 2 147 483 647 közé eshet. 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 leíróinak hozzáadásához vagy eltávolításához.
11. Kattintson az **Egyéb attribútumok** menüpontra.

12. Az **Egyéb attribútumok** lapon írja be az attribútumokhoz megfelelő értékeket. További információkat a “Bináris attribútumok módosítása” oldalszám: 200 témakör tartalmaz.
13. A bejegyzés létrehozásához kattintson a **Befejezés** lehetőségre.

Keresésikorlát-csoport módosítása

Az alábbi információk segítséget nyújtanak keresésikorlát-csoport módosítása során.

Módosíthatja a keresésikorlát-csoportok méret- vagy időkorlát-attribútumait. Csoporttagokat is felvehet és törölhet. A webes adminisztrációs eszközzel módosíthat egy keresésikorlát-csoportot.

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. Kattintson a jobb oldali eszközsor **Attribútumok módosítása** elemére.
2. A **Kötelező attribútumok** lapon írja be a kötelező attribútumok értékeit. A bináris értékek felvételével kapcsolatos további információk: “Bináris attribútumok módosítása” oldalszám: 200. 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** gombra.
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. 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 az **Eltávolítás** gombra.
     d. Kattintson az **OK** gombra.
   - A taglista frissítéséhez kattintson a **Frissítés** elemre.
8. A bejegyzés módosításához kattintson az **OK** gombra.

Keresésikorlát-csoport másolása

Az alábbi információk segítséget nyújtanak keresésikorlát-csoport másolása során.

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.

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 **Másolás** elemére.
2. Módosítsa a DN mező RDN bejegyzését. Például írja át a cn=John Doe elemet cn=Jim Smith értékre.
3. A kötelező attribútumok lapon módosítsa a cn bejegyzést az új RDN-re. Ez a jelen példában Jim Smith.

4. Szükség szerint módosítsa a többi kötelező attribútumot. A jelen példában írja át az sn (vezetéknéz) attribútum értékét Doe-ról Smith-re.
5. Ha kész a szükséges módosításokkal, akkor kattintson az **OK** gombra az új bejegyzés létrehozásához. Az új bejegyzés (Jim Smith) bekerül a bejegyzéslista legaljára.

Keresésikorlát-csoport eltávolítása

Az alábbi információk segítséget nyújtanak keresésikorlát-csoport eltávolítása során.

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 részfát, utótagot vagy elemet. Kattintson a jobb oldali eszközsor **Törlés** elemére.
2. Meg kell erősítenie a törlést. Kattintson az **OK** gombra. A bejegyzés törlésre kerül a könyvtárból és visszatér a bejegyzések listájához.

Proxy hitelesítési csoport feladatok

Az alábbi információk segítséget nyújtanak a proxy hitelesítési csoportok felügyelete során.

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 tagjaiét.

A proxy hitelesítés felügyeletére a webes adminisztrációs eszköz használható.

Kapcsolódó fogalmak

"Proxy felhatalmazás" oldalszám: 64
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.

Proxy hitelesítési csoport létrehozása

Az alábbi információk segítséget nyújtanak a proxy hitelesítési csoport létrehozása során.

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. Ismételje 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. A kívánt szülő DN megadásához adja meg a kiválasztott elemet, majd kattintson a **Kiválasztás** gombra. 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: 200.

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: 200.
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

Az alábbi információk segítséget nyújtanak a proxy csoport módosítása során.

A proxy hitelesítési csoport módosításához (például tagok hozzáadásához vagy törléséhez) a webes adminisztrációs eszköz használható.

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. Kattintson a jobb oldali eszközsor **Attribútumok módosítása** elemére.
2. A **Kötelező attribútumok** lapon írja be a kötelező attribútumok értékeit. A bináris értékek felvételével kapcsolatos további információk: “Bináris attribútumok módosítása” oldalszám: 200. 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** gombra.
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. 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 az **Eltávolítás** gombra.

d. Kattintson az **OK** gombra.

- A taglista frissítéséhez kattintson a **Frissítés** elemre.

8. A bejegyzés módosításához kattintson az **OK** gombra.

Proxy hitelesítési csoport másolása

Az alábbi információk segítséget nyújtanak a proxy hitelesítési csoport másolása során.

Hasznos a proxy hitelesítési csoportok lemásolása, ha ugyanazt a localhost és az IBMpolicies alatt is tárolni szeretné.

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 **Másolás** elemére.
2. Módosítsa a DN mező RDN bejegyzését. Például írja át a cn=John Doe elemet cn=Jim Smith értékre.
3. A kötelező attribútumok lapon módosítsa a cn bejegyzést az új RDN-re. Ez a jelen példában Jim Smith.
4. Szükség szerint módosítsa a többi kötelező attribútumot. A jelen példában írja át az sn (vezetéknéz) attribútum értékét Doe-ról Smith-re.
5. Ha kész a szükséges módosításokkal, akkor kattintson az **OK** gombra az új bejegyzés létrehozásához. Az új bejegyzés (Jim Smith) bekerül a bejegyzéslista legaljára.

Proxy hitelesítési csoport eltávolítása

Az alábbi információk segítséget nyújtanak a proxy hitelesítési csoport eltávolítása során.

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 részfát, utótagot vagy elemet. Kattintson a jobb oldali eszközsor **Törlés** elemére.
2. Meg kell erősítenie a törlést. Kattintson az **OK** gombra. A bejegyzés törlésre kerül a könyvtárból és visszatér a bejegyzések listájához.

Egyedi attribútum feladatok

Az alábbi információk segítséget nyújtanak az egyedi attribútumok kezelése során.

Az egyedi attribútumok kezelése a webes adminisztrációs eszköz **Szerveradminisztráció** kategóriajának használatával történik.

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 webes adminisztrációs eszköz Szerveradminisztráció kategóriájának használatával hitelesítenie kell magát a szerveren egy olyan i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultsággal. 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.

Kapcsolódó fogalmak

“Egyedi attribútumok” oldalszám: 91
Egyedi attribútumok: Az egyedi attribútumok funkció biztosítja, hogy a megadott attribútum értéke egyedi maradjon a címtáron belül.

Kapcsolódó feladatok

“Egyedi attribútumlista létrehozása” oldalszám: 141
Az alábbi információk segítséget nyújtanak az egyedi attribútumlista létrehozása során.

“Bejegyzés eltávolítása az egyedi attribútumlistából” oldalszám: 142
Az információk segítséget nyújtanak a bejegyzések egyedi attribútumlistából való törlése során.

Annak meghatározása, hogy egy attribútum megadható-e egyedi attribútumként

Az alábbi információk segítséget nyújtanak annak meghatározása során, hogy egy attribútum megadható-e egyedi attribútumként.

Nem minden attribútum adható meg egyediként. Azon helyzetek leírása, amelyben egy attribútum egyediként nem adható meg, az alábbiakban található:

- A bináris, műveleti, konfigurációs és objektumosztály attribútumok nem lehetnek egyedi jelölésűek.
- A jelenleg ütköző értékkel rendelkező attribútumok nem tehetők egyedivé.
- Attribútumonként a nyelvi címkék közösen kizárják egymást az egyedi attribútumokkal. Ha egy adott attribútum egyedi attribútumként van megjelölve, akkor nem lehet hozzárendelve nyelvi címke.

A webes adminisztrációs eszköz Egyedi attribútumok kezelése feladata csak azokat az attribútumokat tartalmazza, amelyek az első feltételnek megfelelnek. Ugyanez az attribútumlista lekérhető az ldapexop parancs végrehajtásával is, miután adminisztrátorként csatlakozott. Az egyedivé tehető attribútumok listájának megjelenítéséhez adja meg a következőt:

```
ldapexop -op getattributes
-attrType unique -matches true
```

Az egyedivé nem tehető attribútumok listájának megjelenítéséhez adja meg a következőt:

```
ldapexop -op getattributes -attrType unique -matches false
```

Létezhetnek olyan attribútumok, amelyek a listában egyedi attribútumként megengedettként szerepelnek, azonban ütköző értékkel rendelkeznek és ezért nem tehetők egyedivé. Annak eldöntésére, hogy egy adott attribútum megadható-e egyedi attribútumként, az ldapexop parancs használható. Az

```
ldapexop
-op uniqueattr -a uid
```

parancs például azt jelöli, hogy az uid attribútum egyedivé tehető-e. Ezen kívül felsorolja az attribútum esetleges ütköző értékeit is.

Ha az ldapexop parancs ütköző értékeket jelez, akkor az ütköző értékkel rendelkező bejegyzések megtalálásához az ldapsearch parancs használható. Az alábbi parancs például az uid=jsmith értékkel rendelkező bejegyzést jeleníti meg:

```
ldapsearch -b "" -s sub "(uid=jsmith)"
```

Egyedi attribútumlista létrehozása

Az alábbi információk segítséget nyújtanak az egyedi attribútumlista létrehozása során.

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=IBMploicies objektumban, a szerver a cn, employeeNumber és telephoneNumber attribútumokat kezeli egyediekként.
4. Ismételje 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 címtárhoz egy olyan attribútumértékkel, amely megkettőzi a meglévő címtárbejegyzést, 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 hibanaplóba (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
```

Kapcsolódó fogalmak

“Egyedi attribútum feladatok” oldalszám: 140
Az alábbi információk segítséget nyújtanak az egyedi attribútumok kezelése során.

Bejegyzés eltávolítása az egyedi attribútumlistából

Az információk segítséget nyújtanak a bejegyzések egyedi attribútumlistából való törlése során.

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 az **Eltávolítás** gombra.
4. Ismételje 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 cn=uniqueattribute,cn=IBMpolicies lista tárolóbejegyzése automatikusan törlésre kerül.

Kapcsolódó fogalmak

“Egyedi attribútum feladatok” oldalszám: 140
Az alábbi információk segítséget nyújtanak az egyedi attribútumok kezelése során.

Teljesítmény feladatok

Az alábbi információk segítséget nyújtanak a teljesítmény beállítások megadása során.

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

Kapcsolódó fogalmak

“Szerver gyorsítótárak” oldalszám: 93
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.

Adatbázis-kapcsolatok és gyorsítótár-beállítások megadása

Az alábbi információk segítséget nyújtanak az adatbázis-kapcsolatok és a gyorsítótár beállítása során.

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 **Adatbáziskapcsolatok számát**. Ezzel állítható be a szerveren használt DB2 kapcsolatok száma. A minimális megadandó érték 4, az alapértelmezett beállítás 15. Ha az LDAP szerver nagymennyiségű klienskérést 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.
3. 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.
4. A következő ACl gyorsítótári beállítások használatához válassza ki az **ACL információk gyorsítótárazása** lehetőséget.
5. Adja meg az **ACL gyorsítótárban található elemek maximális száma** értékét. Az alapértelmezés a 25 000.
6. Adja meg a **Bejegyzés-gyorsítótárban található elemek maximális száma** értékét. Az alapértelmezés a 25 000.
7. Adja meg az **Keresési szűrő gyorsítótárban található elemek maximális száma** értékét. Az alapértelmezés a 25 000. A keresési szűrő gyorsítótár a kért attribútumszűrők aktuális lekérdezéseit, valamint az eredményül kapott megfelelő azonosítókat tartalmazzák. Egy frissítési műveletnél minden szűrő gyorsítótári bejegyzés érvénytelenítésre kerül.
8. 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.
9. Ha kész, kattintson az **OK** gombra.
10. 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 alábbi információk segítséget nyújtanak az attribútum-gyorsítótár beállítása során.

Az attribútum-gyorsítótár beállításai a webes adminisztrációs eszközben és a System i navigátorban is megadhatók.

Ha az attribútum-gyorsítótárat saját kezűleg, a webes adminisztrációs eszközből kívánja beállítani, akkor tegye a következőket:

1. 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 webes adminisztrációs eszköz Szerveradminisztráció kategóriájának használatával hitelesítenie kell magát a szerveren egy olyan

i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultsággal. 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. Módosítsa, hogy hány kilobyte memória álljon a címtár gyorsítótár rendelkezésére. Az alapértelmezés 16 384 KB (16 MB).
3. Módosítsa, hogy hány kilobyte memória álljon a változásnapló gyorsítótár rendelkezésére. Az alapértelmezés 16 384 KB (16 MB).

   Megjegyzés: Ez a választási lehetőség le van tiltva, ha a változásnapló nincs beállítva. A változásnaplók esetében az attribútum-gyorsítárazást 0 értékre érdemes állítani és semmilyen attribútumot nem kell beállítani, hacsak nem keres sűrűn a változásnaplókban és ezeknek a kereséseknek nem kritikus a sebessége.
4. 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.
5. 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-gyorsítárazást 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. Ismételje meg ezt a műveletet minden attribútumnál, amelyet hozzá kíván adni az attribútum-gyorsítótárhoz.
7. Ha kész, kattintson az **OK** gombra.

Ha az automatikus attribútum-gyorsítótárazást a System i navigátorban engedélyezni kívánja, akkor tegye a következőket:

1. A System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Tulajdonságok** 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 határásra az időközt, akkor a gyorsítótár automatikusan beállításra fog kerülni reggel hatkor, délben, délután hatkor és éjfélkor, 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.
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 leteltekor érvénybe lépnek. Ha az automatikus gyorsítótárazás le van tiltva, akkor a beállítások tárolásra kerülnek és az automatikus gyorsítótárazás engedélyezésekor lépnek hatályba.

Tranzakció-beállítások megadása

Az alábbi információk segítséget nyújtanak a tranzakció-beállítások megadása során.

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.

Replikációs feladatok

Az alábbi információk segítséget nyújtanak a replikáció kezelése során.

A replikáció kezeléséhez bontsa ki a webes adminisztrációs eszköz **Replikáció kezelése** kategóriáját.

Kapcsolódó fogalmak

“Replikáció” oldalszám: 38
A címtárszerverek a replikáció nevű technikát használják a teljesítmény és a megbízhatóság javítására. A replikációs folyamat feladata, hogy szinkronban tartsa több címtár adatait.

Elsődleges és replikaszerverekből álló topológia létrehozása

Az alábbi információk segítséget nyújtanak az elsődleges és replikaszerverekből álló topológia létrehozása során.

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. Lásd: “Elsődleges szerver (replikált részfa) létrehozása” oldalszám: 147.
2. Hozza létre az ellátó által használt hitelesítési adatokat. Lásd: “Replikációs hitelesítési adatok létrehozása” oldalszám: 149.
3. Hozzon létre egy replikaszervert. Lásd: “Replikaszerver létrehozása” oldalszám: 150.
4. Exportálja a topológiát az elsődleges szerverről a replikára. Lásd: “Adatok másolása a replikába” oldalszám: 152.
5. Módosítsa a replika konfigurációját és adja meg, ki jogosult replikálni a változásait. Adjon meg továbbá egy utalást az elsődleges szerverre. Lásd: “Ellátói információk hozzáadása az új replikához” oldalszám: 152.

Megjegyzés:

Ha a replikálni kívánt részfa gyökérobjektuma nem a szerver egyik utótagja, akkor a **Részfa hozzáadása** funkció használatához előbb biztosítania kell, hogy annak ACL-jei is meg legyenek adva:

Nem szűrt ACL-ek esetén:

```
ownersource: <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 információkat az “Hozzáférés felügyeleti lista (ACL) feladatok” oldalszám: 211 című témakörben talál.

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 és továbbító replikaszerverekből álló topológia létrehozása

Az alábbi információk segítséget nyújtanak az elsődleges és továbbító replikaszerverekből álló topológia létrehozása során.

Egy elsődleges és továbbító szerverekből álló topológia létrehozása az alábbi lépésekből áll:

1. Egy elsődleges és egy replikaszerver létrehozása. Lásd: “Elsődleges és replikaszerverekből álló topológia létrehozása” oldalszám: 146.
2. Hozzon létre egy új replikaszervert az eredeti replikához. Lásd: “Új replikaszerver létrehozása”.
3. Másolja át az adatokat a replikákba. Lásd: “Adatok másolása a replikába” oldalszám: 152.

Elsődleges szerver (replikált részfa) létrehozása

Az alábbi információk segítséget nyújtanak az elsődleges szerver replikált részfák létrehozása során.

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://<sajatszervernev>.<sajathely>.<sajatceg>.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.

Új replikaszerver létrehozása

Az alábbi információk segítséget nyújtanak az új replikaszerverek létrehozása során.

Ha már beállított egy replikációs topológiát (lásd: Elsődleges szerver létrehozása (replikált részfa)) egy elsődleges (szerver1) és egy replikaszerverrel (szerver2), akkor a szerver2 szerepét módosíthatja úgy, hogy továbbító szerver legyen. Ehhez azonban egy újabb replikát kell (szerver3) létrehozni szerver2 alatt.

1. Kapcsolódjon a webes adminisztrációs eszközzel az elsődleges szerverhez (szerver1)
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 **szerver1** kijelölés melletti nyílra a szerverek listájának kibontásához.
6. Válassza ki a szerver2 szervert, majd kattintson a **Replika hozzáadása** lehetőségre.
7. A **Replika hozzáadása** ablak **Szerver** lapján:

- Írja be a létrehozandó replika (szerver3) 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 társ vagy továbbító szerver lesz. Célszerű minden szerveren ugyanazt a kiadást futtatni.
- Adja meg a replikaszerver leírását.

A **Kiegészítések** lapon:

- 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.
- Kattintson a **Kiválasztás** gombra.
  - Válassza ki a hitelesítési adatok helyét. Célszerűen ez a cn=replication,cn=localhost legyen.
  - Kattintson a **Hitelesítési adatok megjelenítése** lehetőségre.
  - Bontsa ki a hitelesítési adatok listáját és válassza ki a használni kívántakat.
  - Kattintson az **OK** gombra.

    A megállapodás hitelesítési adataival kapcsolatosan további információkat a Replikációs hitelesítési adatok létrehozása témakör tartalmaz.
- Válasszon ki egy replikációs ütemezést legördülő listából, vagy hozzon létre egyet a **Hozzáadás** gomb megnyomásával. Információkat a Replikáció ütemezések létrehozása témakör tartalmaz.
- 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 jelszóirányelvek 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.
- Válassza ki a replikáció módját: a replikáció lehet egy, illetve több szálon futó. Ha több szálon futó replikációt választ, akkor adja meg a replikációhoz használt kapcsolatok számát (2-32 között) is. Az alapértelmezett kapcsolatszám a 2.
- Kattintson az **OK** gombra a replika létrehozásához.

8. Másolja át az adatokat a szerver2 szerverről az új replikára (szerver3). Ennek leírását az Adatok replikára másolása témakör tartalmazza.
9. Vegyen fel egy ellátó megállapodást a szerver3 szerverre, amelynek értelmében szerver2 a szerver3 szerver ellátója, szerver3 pedig szerver2 fogyasztója. Ennek leírását az Ellátói információk hozzáadása az új replikához témakör tartalmazza.

A szerverek szerepeit ikonok jelzik a webes adminisztrációs eszközben. A topológia most így néz ki:

- szerver1 (elsődleges)

– szerver2 (továbbító)
  - szerver3 (replika)

Replikációs hitelesítési adatok létrehozása

Az alábbi információk segítséget nyújtanak replikációs hitelesítési adatok létrehozása során.

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 szerverA) és egy másik szerverre (szerverB) 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 szerverA semmilyen **cn=localhost** alatti adata a szerverB 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: 147 rész tartalmazza a replikálni kívánt részfa létrehozásával kapcsolatos utasításokat.
2. Kattintson a **Hozzáadás** gombra.
3. Írja be a létrehozni kívánt hitelesítési adatok nevét, például **sajathitelesitesiAdatok**. 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 információkat a “Kerberos hitelesítés engedélyezése a Directory Server szerverhez” oldalszám: 182 témakör tartalmaz.
     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) kulcscímke 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 kulcscímke fájl, akkor a szerver ezt használja a hitelesítési adatok lekérdezésére a megadott azonosítónévhez. Ha nincs megadott kulcscímke fájl, akkor a szerver a Kerberos konfigurációjában megadott kulcscímke 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=sajatazonosito@VALAMELY.TARTOMANY**).
g. Írja be a **replicaCredentials** attribútum értékét. Ez a **sajatazonosito** azonosítóhoz használt kulcscímke fájlnév.

Megjegyzés: Ez az azonosító és jelszó meg kell, hogy egyezzen azokkal, amelyek segítségével a **kinit** programot futtatta a parancssorból.

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 **Szerkesztés** gombra.
d. Adja meg a replikációs bindDN-t. Ez a jelen példában **ibm-kn=sajatazonosito@VALAMELY.TARTOMANY**).
e. Írja be és erősítse meg a **Replikációs kapcsolódási jelszót**. Ez a **sajatazonosito** azonosítóhoz használt KDC jelszó.

- Ha SSL használatát választotta igazolásos 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 információkat az “SSL és TSL engedélyezése a Directory Serveren” oldalszám: 180 témakör tartalmaz.

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

Az alábbi információk segítséget nyújtanak a replikaszerverek létrehozása során.

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 szervert, majd kattintson a **Replika hozzáadása** lehetőségre.
4. A **Replika hozzáadása** ablak **Szerver** lapján:
   a. Írja be a létrehozandó replika hosztnevét és portszámát. Az alapértelmezett port a 389 nem SSL és 636 SSL kapcsolatok esetén. Ezek kötelező mezők.
   b. Állítsa be, hogy engedélyezi-e az SSL alapú kommunikációt.
   c. Írja be a replika nevét, vagy hagyja üresen (ekkor a hosztnevet használja a rendszer).
   d. 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 társ vagy továbbító szerver lesz. Célszerű minden szerveren ugyanazt a kiadást futtatni.
   e. Adja meg a replikaszerver leírását.
5. A **Kiegészítések** lapon
   - 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 replikált részfában tárolt hitelesítési adatok az adott részfa ibm-replicagroup=default bejegyzése alatt kerülnek létrehozásra.
   - Kattintson a **Kiválasztás** gombra.
     - Válassza ki a hitelesítési adatok helyét. Célszerűen ez a cn=replication,cn=localhost legyen.
     - Kattintson a **Hitelesítési adatok megjelenítése** lehetőségre.
     - Bontsa ki a hitelesítési adatok listáját és válassza ki a használni kívántakat.
     - Kattintson az **OK** gombra.

       A megállapodás hitelesítési adataival kapcsolatosan további információkat a Replikációs hitelesítési adatok létrehozása témakör tartalmaz.
   - Válasszon ki egy replikációs ütemezést legördülő listából, vagy hozzon létre egyet a **Hozzáadás** gomb megnyomásával. Információkat a Replikáció ütemezések létrehozása témakör tartalmaz.
   - 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 jelszóirányelvek 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.
   - Válassza ki a replikáció módját: a replikáció lehet egy, illetve több szálon futó. Ha több szálon futó replikációt választ, akkor adja meg a replikációhoz használt kapcsolatok számát (2-32 között) is. Az alapértelmezett kapcsolatszám a 2.
   - A replika létrehozásához kattintson az **OK** gombra.
6. Megjelenik egy üzenet, hogy további teendőkre is szükség van még. Kattintson az **OK** gombra.

Megjegyzés: Ha további replikaként több szervert vesz fel, illetve összetett topológiát hoz létre, akkor ne lépjen tovább az Adatok replikára másolása, illetve Ellátói információk hozzáadása a replikához lépésekre mindaddig, amíg az elsődleges szerveren a topológia meghatározását be nem fejezte. 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

Az alábbi információk segítséget nyújtanak az adatok replikába másolása során.

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. A System i navigátor menüjében bontsa ki a **Hálózat** elemet.
   b. Bontsa ki a **Szerverek** kategóriát.
   c. Kattintson a **TCP/IP** lehetőségre.
   d. Kattintson a jobb oldali egérgombbal az **IBM Directory Server** lehetőségre, majd válassza az előugró menü **Eszközök**, majd **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, hajtsa 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) A System i navigátor menüjében bontsa ki a **Hálózat** elemet.
      2) Bontsa ki a **Szerverek** kategóriát.
      3) Kattintson a **TCP/IP** lehetőségre.
      4) Kattintson a jobb oldali egérgombbal az **IBM Directory Server** lehetőségre, majd válassza az előugró menü **Eszközök**, majd **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 részfában tárolódnak) betöltésre kerülnek a replikaszerveren.
   d. Indítsa el a szervert.

Ellátói információk hozzáadása az új replikához

Az alábbi információk segítséget nyújtanak az ellátói információk replikákhoz adása során.

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 beállításokat a **Replikációtulajdonságok kezelése** panelekben módosíthassa, a webes adminisztrációs eszközre *ALLOBJ és *IOSYSCFG különleges jogosultsággal rendelkező leképezett OS/400 felhasználóként kell bejelentkeznie.
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/<*sajátszervernév@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

   Lásd: “Replikációs hitelesítési adatok létrehozása” oldalszám: 149.
6. Kattintson az **OK** gombra.
7. A replikaszervert újra kell indítani a változtatások érvénybe léptetéséhez.

További információkat a “Replikációs tulajdonságok módosítása” oldalszám: 160 témakör tartalmaz.

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 információkat az “Replikációs sorok kezelése” oldalszám: 163 című témakörben talál. A replika most már fogadja a frissítéseket az elsődleges szervertől.

Egyszerű topológia létrehozása egyenrangú replikációval

Az egyenrangú replikáció egy olyan replikációs topológia, amelyben több szerver is elsődleges. Az egyenrangú replikációt csak olyan környezetekben használja, amelyben a frissítési vektorok jól ismertek.

A címtáron belül az egyes objektumok frissítése csak egy szerveren történjen. Ennek célja az olyan helyzetek megelőzése, amelyben az egyik szerver kitöröl egy objektumot, majd ezt követően az objektumot egy másik szerver módosítja. Ilyenkor ugyanis előfordulhat, hogy egy társszerver előbb egy törlési, majd közvetlenül ezt követően egy módosítási parancsot kap, amely ütközést okoz. A replikált törlési és átnevezési kéréseket a szerver érkezési sorrendben fogadja el, az ütközések feloldása nélkül. A replikációs ütközések feloldásával kapcsolatosan további információkat az alábbi kapcsolódó hivatkozások tartalmaznak.

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. Ha a meglévő topológia megjelenítéséhez az ellátó szerverek listáját ki kívánja bontani, akkor kattintson a meglévő szerverek mellett található jelölőnégyzetre.
3. Kattintson az **Elsődleges hozzáadása** lehetőségre.

Az **Elsődleges hozzáadása** ablak **Szerver** lapján:

- Írja be a létrehozandó szerver 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.

- Válassza ki, hogy a szervert átjáró szerverként kívánja-e létrehozni.
- Írja be a szerver nevét, vagy a mezőt hagyja üresen (ekkor a rendszer a hosztnevet használja).
- Írja be a szerver azonosítóját. Ha a szerver, amelyen az elsődleges társ szervert éppen létrehozza, már fut, akkor kattintson a **Szerver azonosító lekérése** lehetőségre a mező automatikus kitöltéséhez. Ha nem ismeri a szerver azonosítót, akkor adja meg az **unknown** értéket.
- Adja meg a szerver leírását.
- Adja meg azokat a hitelesítési adatokat, amelyek segítségével a szerver az elsődleges szerverrel kommunikál. Kattintson a **Kiválasztás** elemre.

  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 hitelesítési adatok a cn=replication,cn=localhost alatti elhelyezése biztonságosabb megoldás.

  – **cn=replication,cn=IBMpolicies**, amely akkor is rendelkezésre áll, ha az a szerver, amely alá a replikát fel kívánja venni, nem egyezik meg azzal szerverrel, amelyhez a webes adminisztrációs eszköz segítségével csatlakozik. A hely alatt elhelyezkedő hitelesítési adatok a szerverekre replikálásra kerülnek.

    Megjegyzés: A cn=replication,cn=IBMpolicies hely csak akkor áll rendelkezésre, ha az IBMpolicies támogatási OID, 1.3.18.0.2.32.18, a root DSE ibm-supportedcapabilities eleme alatt létezik.

  – 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.

  1. Válassza ki a hitelesítési adatok helyét. Célszerűen ez a cn=replication,cn=localhost legyen.
  2. Ha már létrehozott hitelesítési adatokat, akkor kattintson a Hitelesítési adatok megjelenítése lehetőségre.
  3. Bontsa ki a hitelesítési adatok listáját és válassza ki a használni kívántakat.
  4. Kattintson az OK gombra.
  5. Ha nem rendelkezik már létező hitelesítési adatokkal, akkor a hitelesítési adatok létrehozásához kattintson a Hitelesítési adatok létrehozása lehetőségre.

A **Kiegészítések** lapon:

1. Válasszon ki egy replikációs ütemezést legördülő listából, vagy hozzon létre egyet a **Hozzáadás** gomb megnyomásával. Információkat a Replikáció ütemezések létrehozása témakör tartalmaz.
2. 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 jelszóirányelvek más változások miatt replikált műveleti attribútumokat használnak. A legtöbb esetben az a legjobb, ha a használt funkciókat minden szerver támogatja. 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.
3. Ha az ellátó hitelesítési adatainak dinamikus frissítését engedélyezni kívánja, akkor jelölje be a **Fogyasztó hitelesítési adatokkal kapcsolatos információinak hozzáadása** jelölőnégyzetet. A kiválasztás automatikusan frissíti a fogyasztó szerver konfigurációs fájljában található ellátói hitelesítési adatokat. Ennek köszönhetően a topológia információk a szerveren replikálhatók.
   - Írja be a fogyasztó szerver adminisztrátori megkülönböztetett nevét. Például cn=root.

     Megjegyzés: Ha a szerver konfigurációs folyamata során létrehozott adminisztrátori DN cn=root, akkor adja meg a teljes adminisztrátori megkülönböztetett nevet. Ne egyszerűen root értéket adjon meg.

- Írja be a fogyasztó szerver adminisztrátori jelszavát. Például secret.

4. Kattintson az **OK** gombra.
5. Az új elsődleges szerver és a meglévő szerverek közötti ellátói és fogyasztói megállapodások megjelennek a listában. Szüntesse meg az összes olyan megállapodás kijelölését, amelyet nem kíván létrehozni. Ez különösen fontos akkor, ha átjáró szervert hoz létre.
6. Kattintson a **Folytatás** gombra.
7. Megjelenhetnek olyan üzenetek, hogy további teendőkre is szükség van még. Hajtsa végre vagy jegyezze fel a megfelelő műveleteket. Ha kész, kattintson az **OK** gombra.
8. Vegye fel a megfelelő hitelesítési adatokat.

   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.
9. Kattintson az **OK** gombra az elsődleges társ szerver létrehozásához.
10. Megjelenhetnek olyan üzenetek, hogy további teendőkre is szükség van még. Hajtsa végre vagy jegyezze fel a megfelelő műveleteket. Ha kész, kattintson az **OK** gombra.

Kapcsolódó hivatkozás

“Replikáció áttekintés” oldalszám: 38
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.

Összetett replikációs topológia létrehozása

Összetett replikációs topológia kialakításához használja az alábbi áttekintést.

1. Indítson el minden társszervert 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, töltse be a ″első″ elsődleges szerverről replikált részfa adatait.
4. Válassza ki a replikálandó részfát.
5. Vegye fel az összes leendő társszervert az ″első″ elsődleges szerver replikájaként.
6. Vegye fel a többi replikát is.
7. Léptesse elő a többi elsődleges társszervert.
8. Vegye fel a többi elsődleges társszerverre 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 társszerverek replikációja sikertelen, ha nincsenek létrehozva a hitelesítési objektumok.
9. Vegye fel a többi elsődleges társszerverre az egyes elsődleges társszerverekre 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 replikaszervereket és importálja mindegyik replikán és elsődleges társszerveren a replikált részfa adatait. Ezután indítsa újra a szervereket.
15. Állítsa be a replikáció tulajdonságait mindegyik replikán és elsődleges társszerveren: adja meg az ellátók által használt hitelesítési adatokat.

Összetett topológia létrehozása egyenrangú replikációval

Az alábbi információk segítséget nyújtanak egyenrangú replikációval rendelkező összetett topológia létrehozása során.

Az egyenrangú replikáció egy olyan replikációs topológia, amelyben több szerver is elsődleges. Szemben a ″multimaster″ környezetekkel, a társszerverek között nem történik ütközésfeloldás. Az LDAP szerverek elfogadják a társszerverek 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: 150), inicializálni kell a címtáradatokat, majd elő kell léptetni a szervereket elsődlegessé (részletek: “Szerver áthelyezése vagy előléptetése” oldalszám: 172).

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.

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 : <*tetszőleges 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: 174).

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 információkat az “Replikációs sorok kezelése” oldalszám: 163 című témakörben talál. 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 társszerver egy törlési parancsot kap, majd közvetlenül utána egy módosítását; ez pedig ütközést okoz.

Egy két egyenrangú-elsődleges és négy replikaszerverből álló egyenrangú-továbbító-replika topológia kialakítása az alábbi lépésekből áll:

1. Egy elsődleges és egy replikaszerver létrehozása. Lásd: “Elsődleges és replikaszerverekből álló topológia létrehozása” oldalszám: 146.
2. Két további replikaszerver létrehozása az elsődleges szerverhez. Lásd: “Replikaszerver létrehozása” oldalszám: 150.
3. Két replika létrehozása az újonnan létrehozott replikaszerverek alatt.
4. Az eredeti replikák előléptetése elsődlegessé. Lásd: “Szerver előléptetése társszerverré” oldalszám: 157.

   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 replikaszerverekre. Lásd: “Adatok másolása a replikába” oldalszám: 152.

Kapcsolódó feladatok

“Szerver áthelyezése vagy előléptetése” oldalszám: 172
Az alábbi információk segítséget nyújtanak a szerverek áthelyezése, illetve előléptetése során.

Szerver előléptetése társszerverré

Az alábbi információk segítséget nyújtanak a szerver társszerverré történő előléptetése során.

Az “Elsődleges és továbbító replikaszerverekből álló topológia létrehozása” oldalszám: 147 részben létrehozott továbbítási topológia használatával egy szerver előléptethető társszerverré. 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 részfát, 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. Lásd: “Replikaszerver létrehozása” oldalszám: 150. 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** lehetőségre.
12. Megjelenik a **További ellátói megállapodások** párbeszédablak. 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. Lásd: “Replikációs hitelesítési adatok létrehozása” oldalszám: 149.

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: 152.

Átjárótopológia beállítása

Az alábbi információk segítséget nyújtanak egy átjárótopológia beállítása során.

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.

Ha egy átjárót a Szerver előléptetése társsá részben leírt társreplikációval rendelkező összetett topológia használatával kíván átjárót beállítani, akkor tegye a következőket:

- Alakítson át egy meglévő társszervert (peer 1) átjárószerverré az 1. replikációs hely létrehozásához.
- Hozzon létre egy új replikációs szervert a 2. replikációs helyhez és egyeztesse a peer 1 szerverrel.
- Hozza létre a 2. replikációs hely topológiáját (ebben a példában nincs szemléltetve).
- Másolja át az adatokat az elsődleges szerverről a topológia összes többi gépére.

1. A webes adminisztrációs eszköz használatával lépjen be az elsődleges szerverre (szerver1).
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. Egy meglévő szerver átjárószerverré alakításához válassza ki az **Átjárószerverek kezelése** elemet. Válassza ki a **szerver1** szervert, vagy társát, a **szerver5** szervert. Ehhez a példához válassza ki a **szerver1** szervert, majd kattintson az **Átjáró létrehozása** elemre.
5. Kattintson az **OK** gombra.

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.

6. 6. Új átjárószerver létrehozásához kattintson a **Szerver hozzáadása** elemre.
7. Az új szervert (**szerver9**) hozza létre átjárószerverként. Ezzel kapcsolatosan információkat a “Elsődleges társ vagy átjáró szerver hozzáadása” oldalszám: 168 témakör tartalmaz.
8. Megjelenik a **További ellátói megállapodások** ablak. Ebben az ablakban, gondoskodjék róla, hogy az alábbi ellátói megállapodás négyzetek meg legyenek jelölve: Szüntesse meg a többi megállapodás kijelölését.

	Ellátó	Fogyasztó
✓	szerver1	szerver9
✓	szerver9	szerver1
	szerver2	szerver9
	szerver9	szerver2
	szerver4	szerver9
	szerver9	szerver4
	szerver9	szerver5
	szerver5	szerver9

9. Kattintson a **Folytatás** gombra.
10. Kattintson az **OK** gombra.
11. Vegye fel a megfelelő hitelesítési adatokat és fogyasztói információkat.

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. Információkat a Replikáció hitelesítési adatainak létrehozása témakör tartalmaz.

12. Kattintson az **OK** gombra. A szerverek szerepeit ikonok jelzik a webes adminisztrációs eszközben. A topológia most így néz ki:
    - szerver1 (elsődleges átjáró a site1 számára)
      - szerver2 (továbbító)
        - szerver3 (replika)
        - szerver6 (replika)
      - szerver4 (továbbító)
        - szerver7 (replika)
        - szerver8 (replika)
      - szerver5 (elsődleges)
      - szerver9 (elsődleges átjáró a 2. replikációs hely számára)
    - szerver5 (elsődleges)
      - szerver1 (elsődleges)
      - szerver2 (továbbító)
        - szerver3 (replika)
        - szerver6 (replika)
      - szerver4 (továbbító)
        - szerver7 (replika)
        - szerver8 (replika)

- szerver9 (elsődleges átjáró)
  - szerver1 (elsődleges átjáró)

13. Adjon hozzá szervereket a **szerver9** szerverhez a 2. replikációs hely topológiájának kialakítása érdekében. Ne felejtse el megszüntetni az új szerverek 2. replikációs helyen kívüli szerverekre vonatkozó megállapodásainak kijelölését.
14. Ismételje meg ezt a folyamatot további replikációs helyek létrehozására. Ne felejtse el, hogy replikációs helyenként csak egy átjárószervert készíthet. Azonban az egyes átjárószervereknek a topológiákban az egyéb átjárószerverekre vonatkozó megállapodásokkal együtt kell szerepelniük.
15. Ha végzett a topológia kialakításával, másolja át a szerver1-ről az adatokat az összes replikációs hely összes gépére és adja hozzá az ellátó információkat az összes új szerverhez. Ezzel kapcsolatosan információkat az Adatok replikára másolása és az Ellátói információk hozzáadása az új replikához témakör tartalmaz.

Kapcsolódó feladatok

“Replika hozzáadása” oldalszám: 166
Az alábbi információk segítséget nyújtanak a replikák létrehozása során.

“Elsődleges társ vagy átjáró szerver hozzáadása” oldalszám: 168
Az alábbi témakör az új elsődleges társ, illetve az átjáró szerverek létrehozási módjának leírását tartalmazza.

“Átjárószerverek kezelése” oldalszám: 170
A témakör az átjárószerverekkel kapcsolatos információkat biztosít. Kijelölheti, hogy az elsődleges szerver rendelkezzen-e átjárószerver-szereppel a replikációs helyen.

Replikációs tulajdonságok módosítása

Az alábbi információk segítséget nyújtanak a replikációs tulajdonságok módosítása során.

Ahhoz, hogy a **Replikációtulajdonságok kezelése** panelekben módosíthassa a beállításokat, *ALLOBJ és *IOSYSCFG különleges jogosultságokkal rendelkező leképezett felhasználóként kell bejelentkeznie a webes adminisztrációs eszközbe.

1. Bontsa ki a navigációs terület **Replikációkezelés** kategóriáját, majd kattintson a **Replikációs tulajdonságok kezelése** lehetőségre
2. Az ablakban az alábbi műveleteket végezheti el:
   a. Módosíthatja a replikációs állapot lekérdezésekben visszaadott, függőben lévő módosítások maximális számát. Az alapértelmezés szerinti érték 10.
   b. Állítsa be a szerver által naplózandó replikációs hibák maximális számát, a frissítések ügyfél felé való replikációja során. Ha a szerver egy szálon futó replikációt használ és a túllépi a maximális számot, akkor a rendszer rendszeres időközönként újra megkísérli a frissítést, amíg az sikeres nem lesz, vagy ameddig az adminisztrátor ki nem üríti a naplót, és ezáltal a hiba hozzáadható lesz. Ha a szerver több szálon futó replikációt használ és túllépi a maximális számot, akkor folyamatban lévő frissítések replikációs hibái naplózásra kerülnek és a replikáció arra vár, hogy az adminisztrátor kiürítse a naplót. A napló a sikeretlen frissítések újbóli megkísérlésével vagy eltávolításával üríthető ki. Minden fogyasztó számára külön napló van fenntartva. Az alapértelmezett érték a nulla, ami azt jelenti, hogy nem történik naplózás.

      Megjegyzés: A naplózás engedélyezett, ha nullánál nagyobb érték van megadva.
   c. Módosítsa a replikációs kontextus gyorsítótár byte-ban megadott méretét. Az alapértelmezett érték a 100 000 byte.
   d. Adja meg a replikációs ütközik maximális bejegyzésméretét byte-ban. Ha a bejegyzés teljes mérete meghaladja a mezőben lévő értéket, akkor a bejegyzést az ellátó nem küldi el újra a fogyasztó replikációs ütközésének feloldása érdekében. Az alapértelmezett érték a 0, ami korlátlan méretet jelent.
   e. Felvehet, módosíthat és törölhet ellátói információkat.

      Megjegyzés: Az ellátó DN-je lehet egy leképzett i5/OS felhasználói profil DN-je. A leképzett i5/OS felhasználói profil nem rendelkezhet LDAP adminisztrációs jogosultsággal. Nem lehet továbbá *ALLOBJ és *IOSYSCFG speciális jogosultságokkal rendelkező felhasználó, és nem kaphat adminisztrációs jogokat a címtárszerver adminisztrátori alkalmazás azonosítón keresztül sem.

További információkért tekintse meg az alábbi hivatkozásokat:

- “Ellátói információk megadása”
- “Ellátói információk módosítása”
- “Ellátói információk eltávolítása”

Ellátói információk megadása

Az alábbi információk segítséget nyújtanak az ellátói információk megadása során.

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

   Lásd: “Replikációs hitelesítési adatok létrehozása” oldalszám: 149.
5. Kattintson az **OK** gombra.

Az ellátó részfája felvételre kerül az Ellátó információk listára.

Ellátói információk módosítása

Az alábbi információk segítséget nyújtanak az ellátói információk módosítása során.

1. Válassza ki a módosítani kívánt ellátói részfát.
2. Kattintson a **Szerkesztés** 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. különben ugorjon a következő lépésre: 4.
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.

A replikáció ellátó DN jelszava módosítható a Change Directory Server Attr (CHGDIRSVRA) parancs segítségével is. Ha a cn=master replikáció csatlakozás DN jelszavát ujjelszo értékre kívánja módosítani, akkor azt a következő parancs segítségével teheti meg:

```
CHGDIRSVRA INSTANCE(QUSRDIR) DN('cn=master' 'ujjelszo')
```

Ellátói információk eltávolítása

Az alábbi információk segítséget nyújtanak az ellátói információk eltávolítása során.

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

Az alábbi információk segítséget nyújtanak replikációs ütemtervek létrehozása során.

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** értékként 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 replikációs ütemezés létrehozása”.
5. Ha kész, kattintson az **OK** gombra.

Kapcsolódó feladatok

“Replikációs ütemezés megjelenítése” oldalszám: 171
Ha a replikációs ütemezést a webes adminisztrációs eszköz segítségével kívánja megjeleníteni, akkor tegye a következőket.

Napi replikációs ütemezés létrehozása

Az alábbi információk segítséget nyújtanak a napi replikációs ütemezés létrehozása során.

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:

Replikáció típusa	Indítás időpontja
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 frissítek 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.

Replikációs sorok kezelése

Az alábbi információk segítséget nyújtanak a szerver által használt replikációs megállapodások (sorok) állapotának megfigyelése során.

1. Bontsa ki a navigációs terület **Replikációkezelés** kategóriáját, majd kattintson a **Sorok kezelése** lehetőségre.
2. Válassza ki a replikát, amelyiknek a sorát kezelni kívánja.
3. A replika állapotától függően **Felfüggeszthető/folytatható**, illetve leállíthatja és újraindíthatja a replikációt.
4. A **Replikáció kényszerítése** lehetőségre kattintva az összes változás replikációját kikényszerítheti, függetlenül attól, hogy mikorra van időzítve a következő replikáció.
5. a **Sor részletei** lehetőségre kattintva részletesebb leírást kap a replika sorának állapotáról. Itt kezelhetők a sorok is.
6. A replikációs hibakezelő párbeszédablak megjelenítéséhez kattintson a **Hibák megjelenítése** elemre. A párbeszédablakban megjeleníthető a replikációs hibanapló, a meghiúsult módosítások újrapróbálhatók, illetve a naplóból bejegyzések eltávolíthatók.
7. Kattintson a **Frissítés** gombra a sorok frissítéséhez és a szerverüzenetek törléséhez.

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.

Kapcsolódó fogalmak

"Replikációs hibatábla" oldalszám: 44
A replikációs hibatábla a meghiúsult frissítéseket rögzíti a későbbi helyreállítás céljából. A replikáció kezdetekor a rendszer összeszámolja az összes replikációs megállapodással kapcsolatos meghibásodás számát. Ez a szám akkor növekszik, ha egy frissítés meghiúsul, és ezáltal a tábla új bejegyzéssel bővül.

Kapcsolódó hivatkozás

"ldapdiff" oldalszám: 245
Az LDAP replikaszinkronizálási parancssori segédprogram.

Talált tárgyak napló beállításai

A talált tárgyak napló (LostAndFound.log az alapértelemzett fájlnév) a replikációs ütközések eredményeként fellépő hibákat rögzíti. A talált tárgyak napló szabályozásához rendelkezésre állnak beállítások, a fájl helyének és maximális méretének megadását, valamint a régi naplófájlok archiválásának lehetőségét is beleértve.

A talált tárgyak napló beállításainak módosításához tegye a következőket:

1. Az IBM Tivoli Directory Server webes adminisztrációs eszközben bontsa ki a **Szerver adminisztráció** lehetőséget, majd a navigációs területen lévő **Naplók** elemet és kattintson a **Naplóbeállítások módosítása** lehetőségre.
2. 2. Kattintson a **Talált tárgyak napló** lehetőségre.
3. 3. Adja meg a hibanapló elérési útját és fájlnevét. Győződjön meg róla, hogy a fájl létezik az ldap szerveren, és hogy az elérési út érvényes. Az alapértelmezett napló elérési út a *<meghajtó>\idsslapd-<példánynév>\logs*, ahol a *meghajtó* a címtárszerver-példány létrehozásakor megadott meghajtó, a *példánynév* pedig a címtárszerver-példány neve. Ha nem elfogadható fájlnevet ad meg (például a szintaxis érvénytelen vagy a szerver nem jogosult a fájl létrehozására és/vagy módosítására), akkor a kísérlet a következő hibával meghiúsul: Az LDAP szerver nem hajtja végre a műveletet.
4. Válassza ki a **Naplóméret küszöbértéke (MB)** első választógombját és adja meg a maximális naplóméretet megabyte-ban. Ha nem kívánja korlátozni a naplóméretet, akkor válassza ki a **Korlátlan** választógombot.
5. Válassza ki a **Naplóarchívumok maximális száma** lehetőségei közül a következők egyikét:
   - Ha meg kívánja adni az archivált naplók maximális számát, akkor válassza ki azt a választógombot, amelyhez egy szerkesztőablak tartozik. Adja meg a menteni kívánt archívumok maximális számát. Az archivált napló egy korábbi napló, amely elérte a méretének küszöbértékét.
   - Ha a naplókat nem kívánja archiválni, akkor válassza a Nincs archiválás lehetőséget.
   - Ha nem kívánja korlátozni az archivált naplók számát, akkor válassza a korlátlan lehetőséget.
6. A **Naplóarchívum elérési útja** lehetőség alatt hajtsa végre a következők egyikét:
   - Ha meg kívánja adni az archívumok helyét, akkor válassza ki azt a választógombot, amelyhez egy szerkesztőablak tartozik, és adja meg a kívánt elérési utat.

- Ha az archívumokat ugyanabban a címtárban kívánja tárolni, mint a naplófájlt, akkor válassza ki a **Naplófájlével megegyező címtár** választógombot.

7. Kattintson az **Alkalmaz** gombra a változások alkalmazásához és a naplók kezelésének folytatásához, vagy az **OK** gombra a módosítások mentéséhez és az IBM Tivoli Directory Server webes adminisztrációs bevezető panelhez való visszatéréshez. Kattintson a **Mégse** gombra, ha a módosítások mentése nélkül kíván visszatérni az IBM Tivoli Directory Server webes adminisztrációs bevezető paneléhez.

Kapcsolódó hivatkozás

"Replikáció áttekintés" oldalszám: 38
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.

Talált tárgyak naplófájl megjelenítése

A replikáció talált tárgyak naplófájl megjeleníthető az IBM Tivoli Directory Server webes adminisztrációs eszköz, illetve az ldapexop segédprogram naplófájl paramétereinek segítségével. A fájl továbbá közvetlenül is megjeleníthető.

Ha a talált tárgyak naplófájlt a webes adminisztrációs eszköz segítségével kívánja megjeleníteni, akkor bontsa ki a webes adminisztráció navigációs területén található **Szerveradminisztráció** kategóriát, majd válassza ki a kibontott lista **Naplók** elemét.

1. Kattintson a **Napló megjelenítése** lehetőségre.
2. A **Naplók megjelenítése** párbeszédablakban válassza ki a **Talált tárgyak napló** lehetőséget, majd kattintson a **Megjelenítés** gombra.

Megjegyzés: A párbeszédablakhoz csak a címtár-adminisztrátor és az adminisztrátori csoport tagjai férnek hozzá.

Ha a talált tárgyak naplót az ldapexop segédprogram segítségével kívánja megjeleníteni, akkor a Qshell parancsértelmezőben adja meg a következőt:

```
ldapexop -D  -w  -op readlog -log LostAndFound -lines all
```

A talált tárgyak napló kiürítéséhez adja meg a következő parancsot:

```
ldapexop -D  -w  -op clearlog -log LostAndFound
```

Megjegyzés: Ha az i5/OS rendszerre *ALLOBJ és *IOSYSCFG különleges jogosultsággal rendelkező felhasználóként jelentkezett be, vagy a címtárszerverhez adminisztrátori hozzáféréssel rendelkezik, akkor az ldapexop segédprogramot az adminisztrátor DN és jelszó megadása helyett használhatja a -m OS400-PRFTKN paraméterrel. Például:

```
ldapexop -m OS400-PRFTKN -op readlog -log LostAndFound -lines all
```

Kapcsolódó hivatkozás

"ldapexop" oldalszám: 223
Az LDAP kiterjesztett művelet parancssori segédprogram.

Replikáció beállítása biztonságos kapcsolaton keresztül

Az alábbi információk segítséget nyújtanak a replikáció biztonságos kapcsolaton keresztüli beállítása során.

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 szervert 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 ellátószervert, 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 szervert, hogy elfogadja ugyanazokat a tanúsítványokat, mint az ellátószerver.

Replikációs topológia feladatok

Az alábbi információk segítséget nyújtanak a replikált részfák topológiáinak kezelése során.

A topológiák az egyes replikált részfákra vonatkoznak.

Topológia megjelenítése

Az alábbi információk segítséget nyújtanak a részfa topológiák megjelenítése során.

Megjegyzés: E feladat végrehajtásához a szervernek futnia kell.

Bontsa ki a navigációs terület **Replikációkezelés** kategóriáját, majd kattintson a **Topológia kezelése** lehetőségre.

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 előléptetése elsődleges szerverré.
- Replika törlése.
- Replikációs ütemezés megjelenítése

Replika hozzáadása

Az alábbi információk segítséget nyújtanak a replikák létrehozása során.

Megjegyzés: Az itt leírt lépések azt mutatják be, hogy replikák a webes adminisztrációs feladat segítségével milyen módon vehetők fel. Ezek a lépések az új szerver inicializálásához szükséges átfogó folyamat részét képezik, több egyéb lépéssel együtt. További információkért tekintse meg a kapcsolódó hivatkozások alatt található témakört.

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 szervert, majd kattintson a **Replika hozzáadása** lehetőségre.
4. A **Replika hozzáadása** ablak **Szerver** lapján:
   a. Írja be a létrehozandó replika hosztnevét és portszámát. Az alapértelmezett port a 389 nem SSL és 636 SSL kapcsolatok esetén. Ezek kötelező mezők.
   b. Állítsa be, hogy engedélyezi-e az SSL alapú kommunikációt.
   c. Írja be a replika nevét, vagy hagyja üresen (ekkor a hosztnevet használja a rendszer).
   d. 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 társ vagy továbbító szerver lesz. Célszerű minden szerveren ugyanazt a kiadást futtatni.
   e. Adja meg a replikaszerver leírását.
5. A **Kiegészítések** lapon
   - 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 replikált részfában tárolt hitelesítési adatok az adott részfa ibm-replicagroup=default bejegyzése alatt kerülnek létrehozásra.
   - Kattintson a **Kiválasztás** gombra.
     - Válassza ki a hitelesítési adatok helyét. Célszerűen ez a cn=replication,cn=localhost legyen.
     - Kattintson a **Hitelesítési adatok megjelenítése** lehetőségre.
     - Bontsa ki a hitelesítési adatok listáját és válassza ki a használni kívántakat.
     - Kattintson az **OK** gombra.

       A megállapodás hitelesítési adataival kapcsolatosan további információkat a Replikációs hitelesítési adatok létrehozása témakör tartalmaz.
   - Válasszon ki egy replikációs ütemezést legördülő listából, vagy hozzon létre egyet a **Hozzáadás** gomb megnyomásával. Információkat a Replikáció ütemezések létrehozása témakör tartalmaz.
   - 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 jelszóirányelvek 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.
   - Válassza ki a replikáció módját: a replikáció lehet egy, illetve több szálon futó. Ha több szálon futó replikációt választ, akkor adja meg a replikációhoz használt kapcsolatok számát (2-32 között) is. Az alapértelmezett kapcsolatszám a 2.
   - A replika létrehozásához kattintson az **OK** gombra.
6. Megjelenik egy üzenet, hogy további teendőkre is szükség van még. Kattintson az **OK** gombra.

   Megjegyzés: Ha további replikaként több szervert vesz fel, illetve összetett topológiát hoz létre, akkor ne lépjen tovább az Adatok replikára másolása, illetve Ellátói információk hozzáadása a replikához lépésekre mindaddig, amíg az elsődleges szerveren a topológia meghatározását be nem fejezte. 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.

Kapcsolódó feladatok

"Átjárótopológia beállítása" oldalszám: 158
Az alábbi információk segítséget nyújtanak egy átjárótopológia beállítása során.

Elsődleges társ vagy átjáró szerver hozzáadása

Az alábbi témakör az új elsődleges társ, illetve az átjáró szerverek létrehozási módjának leírását tartalmazza.

Megjegyzés: Az itt leírt lépések azt mutatják be, hogy elsődleges társ vagy átjáró szerverek a webes adminisztrációs feladat segítségével milyen módon vehetők fel. Ezek a lépések az új szerver inicializálásához szükséges átfogó folyamat részét képezik, több egyéb lépéssel együtt. További információkért tekintse meg a kapcsolódó hivatkozások alatt található témakört.

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. Ha a meglévő topológia megjelenítéséhez az ellátó szerverek listáját ki kívánja bontani, akkor kattintson a **Replikáció topológia** mellett található jelölőnégyzetre.
3. Kattintson az **Elsődleges hozzáadása** lehetőségre.

Az **Elsődleges hozzáadása** ablak **Szerver** lapján:

- Írja be a létrehozandó szerver 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.
- Válassza ki, hogy a szervert átjáró szerverként kívánja-e létrehozni.
- Írja be a szerver nevét, vagy a mezőt hagyja üresen (ekkor a rendszer a hosztnevet használja).
- Írja be a **szerverazonosító** értékét. Ha a szerver, amelyen az elsődleges társ szervert éppen létrehozza, már fut, akkor kattintson a Szerver azonosító lekérése lehetőségre a mező automatikus kitöltéséhez.
- Adja meg a szerver leírását.
- Adja meg azokat a hitelesítési adatokat, amelyek segítségével a szerver a másik elsődleges szerverrel kommunikál. Kattintson a **Kiválasztás** gombra.

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 hitelesítési adatok a cn=replication,cn=localhost alatti elhelyezése biztonságosabb megoldás.
- **cn=replication,cn=IBMpolicies**, amely akkor is rendelkezésre áll, ha az a szerver, amely alá a replikát fel kívánja venni, nem egyezik meg azzal szerverrel, amelyhez a webes adminisztrációs eszköz segítségével csatlakozik. A hely alatt elhelyezkedő hitelesítési adatok a szerverekre replikálásra kerülnek.

  Megjegyzés: A cn=replication,cn=IBMpolicies hely csak akkor áll rendelkezésre, ha az IBMpolicies támogatási OID, 1.3.18.0.2.32.18, a root DSE ibm-supportedcapabilities eleme alatt létezik.
- 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.

1. Válassza ki a hitelesítési adatok helyét. Célszerűen ez a cn=replication,cn=localhost legyen.
2. Ha már létrehozott hitelesítési adatokat, akkor kattintson a Hitelesítési adatok megjelenítése lehetőségre.
3. Bontsa ki a hitelesítési adatok listáját és válassza ki a használni kívántakat.

4. Kattintson az OK gombra.
5. Ha nem rendelkezik már létező hitelesítési adatokkal, akkor a hitelesítési adatok létrehozásához kattintson a Hitelesítési adatok létrehozása lehetőségre.

A **Kiegészítések** lapon:

1. Válasszon ki egy replikációs ütemezést legördülő listából, vagy hozzon létre egyet a **Hozzáadás** gomb megnyomásával. Információkat a Replikáció ütemezések létrehozása témakör tartalmaz.
2. 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 (Szűrt hozzáférés felügyeleti listák) és a jelszó házirendek (Jelszó házirend tulajdonságok beállítása) más változások miatt replikált műveleti attribútumokat használnak. A legtöbb esetben az a legjobb, ha a használt funkciókat minden szerver támogatja. 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.
3. Ha a forrás hitelesítési adatainak dinamikus frissítését engedélyezni kívánja, akkor jelölje be a **Fogyasztó hitelesítési adatokkal kapcsolatos információinak hozzáadása** jelölőnégyzetet. A kiválasztás automatikusan frissíti a létrehozás alatt álló szerver konfigurációs fájljában található ellátói információkat. Ennek köszönhetően a topológia információk a szerveren replikálhatók.
   - Írja be a (jelen) fogyasztó szerver adminisztrátori megkülönböztetett nevét. Például cn=root.

     Megjegyzés: Ha a szerver konfigurációs folyamata során létrehozott adminisztrátori DN cn=root, akkor adja meg a teljes adminisztrátori megkülönböztetett nevet. Ne egyszerűen root értéket adjon meg.
   - Írja be a (jelen) fogyasztó szerver adminisztrátori jelszavát. Például secret.
4. Kattintson az **OK** gombra.
5. Az új elsődleges szerver és a meglévő szerverek közötti ellátói és fogyasztói megállapodások megjelennek a listában. Szüntesse meg az összes olyan megállapodás kijelölését, amelyet nem kíván létrehozni. Ez különösen fontos akkor, ha átjáró szervert hoz létre.
6. Kattintson a **Folytatás** gombra.
7. Megjelenhetnek olyan üzenetek, hogy további teendőkre is szükség van még. Hajtsa végre vagy jegyezze fel a megfelelő műveleteket. Ha kész, kattintson az **OK** gombra.
8. Vegye fel a megfelelő hitelesítési adatokat.

   Megjegyzés: Egyes esetekben megjelenhet a Hitelesítési adatok kiválasztása ablak, amely 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.
9. Ha a forrás hitelesítési adatainak dinamikus frissítését engedélyezni kívánja, akkor jelölje be a **Fogyasztó hitelesítési adatokkal kapcsolatos információinak hozzáadása** jelölőnégyzetet. A kiválasztás automatikusan frissíti a létrehozás alatt álló szerver konfigurációs fájljában található ellátói információkat. Ennek köszönhetően a topológia információk a szerveren replikálhatók.
   - Írja be a (jelen) fogyasztó szerver adminisztrátori megkülönböztetett nevét. Például cn=root.

     Megjegyzés: Ha a szerver konfigurációs folyamata során létrehozott adminisztrátori DN cn=root, akkor adja meg a teljes adminisztrátori megkülönböztetett nevet. Ne egyszerűen root értéket adjon meg.
   - Írja be a (jelen) fogyasztó szerver adminisztrátori jelszavát. Például secret.
10. Kattintson az **OK** gombra az elsődleges társ szerver létrehozásához.
11. Megjelenhetnek olyan üzenetek, hogy további teendőkre is szükség van még. Hajtsa végre vagy jegyezze fel a megfelelő műveleteket. Ha kész, kattintson az **OK** gombra.

Megjegyzés: Ha a webes adminisztrációs eszköz segítségével végzett Elsődleges szerver felvétele művelet során a fogyasztókhoz hitelesítési adatokat ad hozzá, és eközben egy külső hitelesítési adat objektum kiválasztott, akkor az IBM WebSphere Application Server alkalmazást futtató számítógépen az alábbi beállításokat kell megadni:

- A WAS_ALAP\java\jre\lib\ext\ az alábbi jar fájlokat tartalmazza:
  - ibmjceprovider.jar
  - ibmpkcs.jar
  - ibmjcefw.jar
  - local_policy.jar
  - US_export_policy.jar
  - ibmjlog.jar
  - gsk7cls.jar
- A WAS_ALAP\java\jre\lib\security\java.security fájlnak a CMS és JCE szolgáltatók bejegyzéséhez a következő két sort kell tartalmaznia:

  ```
  security.provider.2=com.ibm.spi.IBMCMSProvider
  security.provider.3=com.ibm.crypto.provider.IBMJCE
  ```

- Indítsa újra az IBM WebSphere Application Server szervert.
- A Gskit eszközkészletnek telepítve kell lennie, illetve a rendszer elérési útjának tartalmaznia kell a gsk7\lib helyet.
- Ahhoz, hogy a webes adminisztrációs eszköz az elsődleges szerver által a replikához csatlakozás során használt hitelesítési adatokat tartalmazó kulcsfájlt olvasni tudja, illetve a replikán a hitelesítési adatokat létrehozhassa, a kulcsfájlnak Windows platformok esetében a C:\temp, UNIX esetében pedig a /tmp könyvtárban kell lennie.

Kapcsolódó feladatok

"Átjárótopológia beállítása" oldalszám: 158
Az alábbi információk segítséget nyújtanak egy átjárótopológia beállítása során.

Átjárószerverek kezelése

A témakör az átjárószerverekkel kapcsolatos információkat biztosít. Kijelölheti, hogy az elsődleges szerver rendelkezzen-e átjárószerver-szereppel a replikációs helyen.

Átjárószerver elsődlegesként való kijelöléséhez 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.
2. Kattintson az **Átjárószerverek kezelése** lehetőségre.
3. Az **Elsődleges szerverek** mezőben válassza ki az átjárószerverként kijelölni kívánt szervert.
4. Kattintson a **Kijelölés átjáróként** lehetőségre. A szerver áthelyezésre kerül az **Elsődleges szerverek** mezőből az **Átjárószerverek** mezőbe.
5. Kattintson az **OK** gombra.

Átjárószerver-szerep megvonása egy elsődleges szervertől.

1. Kattintson az **Átjárószerverek kezelése** lehetőségre.
2. Az **Átjárószerverek** mezőben válassza ki az elsődleges szerverként kijelölni kívánt szervert.
3. Kattintson a **Kijelölés elsődlegesként** lehetőségre. A szerver áthelyezésre kerül az **Átjárószerverek** mezőből az **Elsődleges szerverek** mezőbe.
4. Kattintson az **OK** gombra.

Megjegyzés: Ne feledje el, hogy replikációs helyenként csak egy átjárószerver lehet. Ha további átjárószerverket hoz létre a topológiában, akkor a Webes adminisztrációs eszköz az átjárót partnerszerverként kezeli és

megállapodásokat hoz létre a topológia összes szerveréhez. Győződjön meg róla, hogy megszüntette az összes olyan megállapodást, amely nem más átjárószerverhez van meghatározva és nem a replikációs helyet birtokló átjárón belül van.

További információkért tekintse meg az alábbi kapcsolódó hivatkozások Átjárótopológia beállítása témakörét.

Kapcsolódó feladatok

"Átjárótopológia beállítása" oldalszám: 158
Az alábbi információk segítséget nyújtanak egy átjárótopológia beállítása során.

Szerverinformációk megjelenítése

A Szerver megjelenítése párbeszédablakban megjeleníthető a szervernév, a hosztnév, a port, a szerverazonosító, a konfigurációs mód, a példánynév, illetve megjeleníthetők a biztonsági beállítások.

Bontsa ki a webes adminisztrációs eszköz navigációs területén található **Replikációkezelés** kategóriát, majd kattintson a **Topológia kezelése** lehetőségre.

1. Válassza ki a megjeleníteni kívánt részfát, majd kattintson a **Topológia megjelenítése** lehetőségre.
2. Válassza ki a megjeleníteni kívánt szervert.
3. A szerver megjelenítése párbeszédablak megjelenítéséhez kattintson a **Szerver megjelenítése** lehetőségre.

A Szerver megjelenítése párbeszédablak az alábbi információkat tartalmazza:

Szerver neve
A mező megjeleníti annak a szervernek a nevét, amelyen a címtárpéldány fut. Az információk hosztnév:port formátumban jelennek meg.

Hosztnév
A mező megjeleníti annak a számítógépnek a hosztnevét, amelyen a címtárpéldány fut.

Port A mező megjeleníti azt a nem biztonságos portot, amelyen a szerver figyel.

Szerverazonosító
A mező megjeleníti a szerverhez a szerver első indításakor hozzárendelt egyedi azonosítót. Az azonosítót a rendszer a replikációs topológiában a szerver szerepének meghatározása során használja.

Szerepkör
A mező megjeleníti, hogy a szerver a replikációs topológiában milyen szerepre került beállításra.

Konfigurációs mód
A mező megjeleníti, hogy a szerver konfigurációs módban fut-e. Ha értéke IGAZ, akkor a szerver konfigurációs módban fut. HAMIS érték esetén a szerver nem fut konfigurációs módban.

Példány neve
A mező megjeleníti a szerveren futó címtárszerver-példány nevét.

Biztonság
A mező megjeleníti azt a védett SSL port számot, amelyen a szerver figyel.

Továbbá megjelenik a szerver neve, azonosítója és szerepe, illetve megjelenítésre kerülnek a fogyasztói információk.

Replikációs ütemezés megjelenítése

Ha a replikációs ütemezést a webes adminisztrációs eszköz segítségével kívánja megjeleníteni, akkor tegye a következőket.

Bontsa ki a webes adminisztrációs eszköz navigációs területén található **Replikációkezelés** kategóriát, majd kattintson a **Topológia kezelése** lehetőségre.

1. Válassza ki a megjeleníteni kívánt részfát, majd kattintson a **Topológia megjelenítése** lehetőségre.
2. Válassza ki a megjeleníteni kívánt elsődleges vagy átjáró szervert.
3. Kattintson az **Ütemezés megjelenítése** lehetőségre.

Ha a kiválasztott szerver és fogyasztói között létezik replikációs ütemezés, akkor az megjelenítésre kerül. Az ütemezések módosíthatók, illetve törölhetők. Ha ütemezés nem létezik vagy újat kíván létrehozni, akkor használja a webes adminisztrációs eszköz navigációs területén található **Ütemezések kezelése** funkciót. Az ütemezések kezelésével kapcsolatosan információkat az alábbi kapcsolódó hivatkozások Replikációs ütemezések létrehozása témaköre tartalmaz.

Kapcsolódó feladatok

"Replikációs ütemezések létrehozása" oldalszám: 162
Az alábbi információk segítséget nyújtanak replikációs ütemtervek létrehozása során.

Megállapodás módosítása

Az alábbi információk segítséget nyújtanak a replikációs megállapodás módosítása során.

A replika alábbi információi módosíthatók:

1. A **Szerver** lapon csak az alábbiak módosíthatók:
   - Hosztnév
   - Port
   - SSL engedélyezése
   - Leírás
2. A **Kiegészítések** lapon az alábbiak módosíthatók:
   - Hitelesítési adatok - lásd: "Replikációs hitelesítési adatok létrehozása" oldalszám: 149.
   - Replikáció ütemezések - lásd: "Replikációs ütemezések létrehozása" oldalszám: 162.
   - A fogyasztó replikához replikált funkciók módosítása. Az ellátó funkcióinak listájában kikapcsolhat bármilyen olyan funkciót, amelyet nem kíván replikálni a fogyasztó felé.
3. Ha kész, kattintson az **OK** gombra.

Szerver áthelyezése vagy előléptetése

Az alábbi információk segítséget nyújtanak a szerverek áthelyezése, illetve előléptetése során.

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 szerverré előléptetéséhez kattintson a **Replikációs topológia** lehetőségre. Kattintson az **Áthelyezés** lehetőségre.
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. Lásd: "Replikációs hitelesítési adatok létrehozása" oldalszám: 149.
4. Megjelenik a **További ellátói megállapodások** párbeszédablak. Válassza ki a szerver szerepének megfelelő ellátói megállapodásokat. Ha például egy replikaszervert társszerverré 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.

Kapcsolódó feladatok

"Összetett topológia létrehozása egyenrangú replikációval" oldalszám: 155
Az alábbi információk segítséget nyújtanak egyenrangú replikációval rendelkező összetett topológia létrehozása során.

Elsődleges szerver lejjebb sorolása

Az alábbi információk segítséget nyújtanak egy szerver szerepének elsődlegesről replikára módosítása során.

Egy szerver elsődlegesből replikaszerverré 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. Lásd: “Replikaszerver létrehozása” oldalszám: 150.

Részfa replikálása

Az alábbi információk segítséget nyújtanak a részfa replikálása során.

Megjegyzés: E feladat végrehajtásához a szervernek futnia kell.

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 DN-jét, vagy kattintson a **Tallózás** lehetőségre a részfa gyökereként megjelölt bejegyzés kiválasztásához.
3. Írja be az elsődleges szerver utalási URL-jét. Ezt LDAP URL-ként kell megadni, például:
   `ldap://<sajatszervernev>.<sajathely>.<sajatceg>.com`
4. Kattintson az **OK** gombra.

Az új szerver megjelenik a Topológia kezelése ablakban, a **Replikált részfák** címsor alatt

Részfa módosítása

Az alábbi információk segítséget nyújtanak azon elsődleges kiszolgáló URL címének módosítása során, amelynek a részfa, illetve replikái frissítéseket küldenek. 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 szerkesztése** gombra.
3. Írja be az elsődleges szerver utalási URL-jét. Ezt LDAP URL-ként kell megadni, például:
   `ldap://<sajatujszervernev>.<sajathely>.<sajatceg>.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 szerverré.
- 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 szerverré.
- Ha nem találhatók 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 szerverré.

Részfa eltávolítása

Az alábbi információk segítséget nyújtanak a részfa eltávolítása során.

1. Válassza ki a törölni kívánt részfát.

2. Kattintson a **Részfa törlése** gombra.
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

Az alábbi információk segítséget nyújtanak a részfák zárolása során.

Ez a funkció akkor hasznos, ha karbantartás vagy módosításokat akar végezni a topológián. Minimálisra csökkenti a szerveren végrehajtható frissítések számát. Egy zárolt szerver nem fogad klienskéréseket. 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

Az alábbi témakör a hozzáférés felügyeleti listák (ACL) módosításához szükséges jogosultságok leírását tartalmazza, illetve a hozzáférés felügyeleti listák kezelésével kapcsolatos információkat tartalmaz.

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 hozzáférésének 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 lista (ACL) feladatok” oldalszám: 211.

További információk: “Hozzáférés-felügyeleti listák” oldalszám: 65.

Biztonsági tulajdonság feladatok

Az alábbi információk segítséget nyújtanak a biztonsági tulajdonság feladatok kezelése során.

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 biztonság” oldalszám: 52.

Kapcsolódó fogalmak

“Directory Server biztonság” oldalszám: 52
Ismerje meg azokat a funkciókat, amelyeknek köszönhetően a Directory Server biztonságosabbá tehető.

Jelszófeladatok

Az alábbi információk segítséget nyújtanak a jelszófeladatok kezelése során.

A jelszókezeléshez bontsa ki a **Biztonsági tulajdonságok kezelése** kategóriáját, és válassza a **Jelszó-irányelvek** oldalt.

Kapcsolódó fogalmak

"Jelszó-irányelv" oldalszám: 78
LDAP szervereket használva hitelesítéshez, fontos, hogy az LDAP szerver támogasson a jelszavak lejáratára, a meghiúsult bejelentkezési kísérletekre, valamint a jelszószabályokra vonatkozó irányelveket. A Directory Server konfigurálható támogatást nyújt mindhárom fajta irányelvhez.

Jelszó-irányelv tulajdonságok beállítása:

Az alábbi információk segítséget nyújtanak a jelszó-irányelvek tulajdonságainak beállítása során.

A jelszó-irányelv beállításának lépései:

| **Megjegyzés:** Az alábbi lépések bemutatják a felhasználói jelszó-irányelvek beállításának módját. Az adminisztrátori csoport tagjaira vonatkozó adminisztrátori jelszó-irányelvvel kapcsolatosan információkat a kapcsolódó hivatkozások alatt található Adminisztrátori jelszó és kizárási irányelv beállítása témakör tartalmaz.

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 jelszó-irányelvek által használt attribútum nevét tartalmazza.
2. Válassza ki a jelszótitkosítás típusát a legördülő listából:

   | **Nincs** A jelszavak kétirányú módszerrel titkosítva kerülnek tárolásra egy ellenőrzési listában, illetve lekérésre az eredeti, titkosítatlan formátumú bejegyzés részeként kerülnek. A beállítás használatához a QRETSVRSEC rendszerváltozót 1 értékre kell állítani.

   crypt A rendszer a jelszavakat - mielőtt a címtárban eltárolásra kerülnének - a UNIX crypt titkosítási algoritmus segítségével titkosítja.

   SHA-1 A rendszer a jelszavakat az SHA-1 algoritmus szerint titkosítja, mielőtt a címtárban tárolásra kerülnek.

   | **MD5** A rendszer a jelszavakat az MD5 titkosítási algoritmus segítségével titkosítja, mielőtt a címtárban eltárolásra kerülnek.

   | **AES128**
   A rendszer a jelszavakat az AES128 algoritmus segítségével titkosítja, mielőtt a címtárban eltárolásra kerülnek. A jelszavak lekérésre az eredeti, titkosítatlan formátumú bejegyzés részeként kerülnek.

   | **AES192**
   A rendszer a jelszavakat az AES192 algoritmus segítségével titkosítja, mielőtt a címtárban eltárolásra kerülnek. A jelszavak lekérésre az eredeti, titkosítatlan formátumú bejegyzés részeként kerülnek.

   | **AES256**
   A rendszer a jelszavakat az AES256 algoritmus segítségével titkosítja, mielőtt a címtárban eltárolásra kerülnek. A jelszavak lekérésre az eredeti, titkosítatlan formátumú bejegyzés részeként kerülnek.

   | **Megjegyzés:** Az AES a V6R1 változatnál korábbi LDAP szervereken nem támogatott. Ha az AES által titkosított jelszavakat exportálja, majd egy V6R1 változatnál korábbi szerverre importálja, akkor a jelszavak használhatatlanok lesznek.

   | Ha több szervert használ és az AES titkosítás mellett dönt, akkor az összes szervernek ugyanazt az AES jelmondatot és módosító értéket kell használnia. A jelmondatot az adminisztrátornak kell nyilvántartania, a rendelkezésre álló módosító értékeket a szerverkonfiguráció megjeleníti. Amikor az AES használatára az adminisztrátor további szervereket beállít, akkor meg kell adnia a megfelelő AES jelmondatot, illetve módosító értéket.

   | További információkat az alábbi kapcsolódó témakörök Jelsztitkosítás témaköre tartalmaz.
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 alapértemezésben 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: 216) a jelszó-irányelv beállításához.

További információk a jelszó-irányelvről: “Jelszó-irányelv” oldalszám: 78.

Kapcsolódó fogalmak

“Jelszótitkosítás” oldalszám: 55
Az IBM Tivoli Directory Server segítségével megakadályozható, hogy a felhasználói jelszavakhoz jogosulatlan személyek hozzáférhessenek. Az adminisztrátor beállíthatja a szervert úgy, hogy a userPassword attribútum értékeit egy- vagy kétirányú titkosítási formátumban titkosítsa. A titkosított jelszavakat a rendszer megjelöli a titkosítási algoritmus nevével, tehát a különböző formátumban titkosított jelszavak a címtárban egymás mellett tárolhatók. A titkosítási konfiguráció módosításakor a meglévő titkosított jelszavak változatlanok maradnak, és továbbra is használhatók.

Kapcsolódó feladatok

“Adminisztrátori jelszó és kizárási irányelv beállítása”
Az adminisztrátori jelszó-irányelv csak a parancssor segítségével állítható be. A jelszó-irányelvek használatát a webes adminisztrációs eszköz nem támogatja.

Adminisztrátori jelszó és kizárási irányelv beállítása:

Az adminisztrátori jelszó-irányelv csak a parancssor segítségével állítható be. A jelszó-irányelvek használatát a webes adminisztrációs eszköz nem támogatja.

Megjegyzés: *ALLOBJ és *IOSYSCFG különleges jogosultsággal rendelkező i5/OS felhasználóként kell magát hitelesítenie.

Ha EAL4 biztonságos konfiguráció esetén az adminisztrátori jelszó-irányelvet be kívánja kapcsolni, akkor adja ki a következő parancsot:

```
ldapmodify -D <adminDN>
-w <adminPW> -i <fájlnév>
```

ahol a <fájlnév> a következőt tartalmazza:

```
dn: cn=pwdPolicy Admin,cn=Configuration
changetype: modify
replace: ibm-slapdConfigPwdPolicyOn
ibm-slapdConfigPwdPolicyOn: true
```

Az adminisztrátori jelszó-irányelv engedélyezéséhez és az alapértelmezett beállítások módosításához adja ki a következő parancsot:

```
ldapmodify -D
<adminDN> -w <adminPW> -i <fájlnév>
```

ahol a <fájlnév> a következőt tartalmazza:

```
dn: cn=pwdPolicyAdmin,cn=Configuration
changetype: modify
replace: ibm-slapdConfigPwdPolicyOn
ibm-slapdConfigPwdPolicyOn: TRUE
-
replace: pwdlockout
pwdlockout: TRUE
#engedélyezéshez válassza a TRUE, letiltáshoz a FALSE értéket
-
replace:pwdmaxfailure
pwdmaxfailure: 10
-
replace:pwdlockoutduration
pwdlockoutduration: 300
-
replace:pwdfailurecountinterval
pwdfailurecountinterval: 0
-
replace:pwdminlength
pwdminlength: 8
-
replace:passwordminalphachars
passwordminalphachars: 2
-
replace:passwordminotherchars
passwordminotherchars: 2
-
replace:passwordmaxrepeatedchars
passwordmaxrepeatedchars: 2
-
replace:passwordmindiffchars
passwordmindiffchars: 2
```

Megjegyzés: Az adminisztrátori fiókok a nagy mennyiségű hitelesítési hibák miatt zárolhatók. Ez azonban csak a távoli kliens kapcsolatokra vonatkozik. A szerver indításakor a fiók alaphelyzetbe áll.

Kapcsolódó feladatok

“Jelszó-irányelv tulajdonságok beállítása” oldalszám: 175

Az alábbi információk segítséget nyújtanak a jelszó-irányelvek tulajdonságainak beállítása során.

Jelszókizárási tulajdonságok beállítása:

Az alábbi információk segítséget nyújtanak a jelszókizárási tulajdonságok beállítása során.

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 törlődjenek, vagy a **Másodperc** választógombra, és adja meg, hogy hány másodperc múlva törlődnek 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.

Jelszó-ellenőrzési tulajdonságok beállítása:

Az alábbi információk segítséget nyújtanak a jelszó-ellenőrzési tulajdonságok beállítása során.

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 közöl 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 attribútumok megjelenítése:

Az alábbi információk segítséget nyújtanak a jelszó-irányelv attribútumok megjelenítése során.

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.

1. Egy adott bejegyzés összes jelszó-irányelv attribútumának megtekintéséhez:

   ```
   > ldapsearch -b "uid=user1,cn=users,o=ibm" -s base "(objectclass=*)"
    pwdChangedTime pwdAccountLockedTime pwdExpirationWarned
    pwdFailureTime pwdGraceUseTime pwdReset
   ```

2. A lejárni készülő 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 irányelvvel 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., éjféli pwdChangedTime értéknek felel meg

3. 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.

4. 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-irányelv attribútumok felülbírálása:

Az alábbi információk segítséget nyújtanak a jelszó-irányelv attribútumok felülbírálása során.

Először ezt kell tennie.

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.

1. 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 éjfélre állítja ezt:

   ```
   > ldapmodify -D cn=root -w ? -k
   dn: uid=wasadmin,cn=users,o=ibm
   changetype: modify
   replace: pwdChangedTime
   pwdChangedTime: 220001010000000Z
   ```

2. 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
   ```

3. 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
```

4. 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
```

5. Egy fiók adminisztratív módon zárolható azzal, ha az ibm-pwdAccountLocked műveleti attribútumot TRUE értékre állítja.

   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
```

6. 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: FALSE
```

SSL és TSL engedélyezése a Directory Serveren

Az alábbi információk segítséget nyújtanak SSL és TSL Directory Server szerveren történő engedélyezése során.

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 a címtárszerveren az SSL réteget engedélyezné, hasznos lehet elolvasni a Védett socket réteg (SSL) és Szállítási réteg biztonság (TLS) engedélyezése a Directory Server szerveren témakört.

Az SSL engedélyezése az LDAP szerveren:

1. **Tanúsítvány rendelése a Directory Server-hez**
   a. Ha a Directory Servert SSL kapcsolaton keresztül kívánja felügyelni a System i navigátorból, akkor olvassa el a *System i Access for Windows felhasználói kézikönyv* kiadványt (lehet, hogy telepítette a PC-re is a System i 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, illetve 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** igazolástárolót. Kattintson a **Folytatás** gombra.

f. Adja meg a *SYSTEM igazolástároló helyes jelszavát. Kattintson a **Folytatás** gombra.

g. A bal oldali navigációs menü újratöltése után bontsa ki az **Alkalmazások kezelése** kategóriát.

h. Kattintson az **Igazolás hozzárendelés frissítése** hivatkozásra.

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 System i Access for Windows kliensek felé.

   Megjegyzés: Ha egy olyan CA igazolását választja, amelynek a CA igazolása még nincs benne az System i 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** elemre.

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. Választható: **Tanúsítvány rendelése a Directory Server közzétételhez** Ha a rendszerből a Directory Serverre közzétételt is SSL kapcsolaton keresztül kívánja biztosítani, akkor 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** igazolástárolót. Kattintson a **Folytatás** gombra.

   d. Adja meg a *SYSTEM igazolástároló helyes jelszavát. Kattintson a **Folytatás** gombra.

   e. A bal oldali navigációs menü újratöltése után bontsa ki az **Alkalmazások kezelése** kategóriát.

   f. Kattintson az **Igazolás hozzárendelés frissítése** hivatkozásra.

   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 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.

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: 129.

3. Választható: **Tanúsítvány rendelése a Directory Server klienshez** Ha más alkalmazások is használnak SSL kapcsolatot a Directory Server felé, akkor 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** igazolástárolót. Kattintson a **Folytatás** gombra.
   d. Adja meg a *SYSTEM igazolástároló helyes jelszavát. Kattintson a **Folytatás** gombra.
   e. A bal oldali navigációs menü újratöltése után bontsa ki az **Alkalmazások kezelése** kategóriát.
   f. Kattintson az **Igazolás hozzárendelés frissítése** hivatkozásra.
   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** elemre.
   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.

Az SSL vagy TLS használatához engedélyeznie kell azt a System i navigátorban.

1. A System i navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a jobb egérgombbal a **Címtár** elemre, és válassza ki a **Tulajdonságokat**.
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 használata esetén az ibm-slapdSecurity attribútumnak meg kell felelnie a TLS vagy SSLTLS értéknek.

   Kapcsolódó fogalmak

   “Védett socket réteg (SSL) és Fordítási réteg biztonság (TLS) használata LDAP Directory Serverrel” oldalszám: 53
   A Directory Server kapcsolatainak biztonságosabbá tételéhez a Directory Server alkalmazhatja az SSL (Secure Sockets Layer, védett socket réteg) és a Transport Layer Security (TLS) biztonsági eljárást.

Kerberos hitelesítés engedélyezése a Directory Server szerverhez

Az alábbi információk segítséget nyújtanak a Kerberos hitelesítés Directory Server szerveren való engedélyezése során.

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 a címtárszerveren a Kerberos hitelesítést engedélyezné, hasznos lehet elolvasni a Kerberos használatának bemutatása Directory Server szerverrel témakört.

A Kerberos hitelesítés engedélyezéséhez végezze el az alábbiakat:

1. A System i navigátor menüjében bontsa ki a **Hálózat** elemet.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.

4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Tulajdonságok** 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.

Kapcsolódó hivatkozás

"Hitelesítés" oldalszám: 82
A Directory Server hozzáférése hitelesítési módszer segítségével felügyelhető.

DIGEST-MD5 hitelesítés beállítása a Directory Serveren

Az alábbi információk segítséget nyújtanak DIGEST-MD5 hitelesítés Directory Server szerveren történő beállítása során.

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 újrajátszás 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 webes adminisztrációs eszköz Szerveradminisztráció kategóriájának használatával hitelesítenie kell magát a szerveren egy olyan i5/OS felhasználói profillal, amely rendelkezik a speciális *ALLOBJ és IOSYSCFG jogosultsággal. 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 felhasználónevét. Ezt a mezőt csak az adminisztrátori 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.

Kapcsolódó hivatkozás

"Hitelesítés" oldalszám: 82
A Directory Server hozzáférése hitelesítési módszer segítségével felügyelhető.

Sémafeladatok

Az alábbi információk segítséget nyújtanak a séma kezelése során.

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: 193.

Kapcsolódó fogalmak

“Utótag (névkontextus)” oldalszám: 13
Az utótag (más néven névkontextus) egy olyan DN, amely egy helyileg tárolt címtárhierarchia legfelső bejegyzését azonosítja.

“Séma” oldalszám: 14
A séma az a szabályhalmaz, amelyik szabályozza, milyen adatok tárolhatók a címtárban. A séma határozza meg az engedélyezett bejegyzések típusát, attribútumaik szerkezetét és szintaxisát.

Objektumosztályok megjelenítése

Az alábbi információk segítséget nyújtanak az objektumosztályok megjelenítése során.

A séma objektumosztályait a webes adminisztrációs eszközzel, illetve a parancssorból tekintheti meg.

1. 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.
2. 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
   - Szerkesztés
   - Másolás
   - Törlés
3. Ha készen van, kattintson a **Bezárás** gombra. Visszatér az IBM Directory Server **Üdvözlet** ablakába.

A séma objektumosztályainak megtekintéséhez adja meg a következőt:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Objektumosztály hozzáadása

Az alábbi információk segítséget nyújtanak az objektumosztályok hozzáadása során.

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. Lásd: “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 kapcsolatosan további információkat az “Objektumosztályok” oldalszám: 17 témakör tartalmaz.
- 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 listákból. Ehhez válassza ki az attribútumokat, majd kattintson a megfelelő **Áthelyezés** vagy **Törlés** gombra.
   - 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.

EGy objektumosztály a parancssorból az alábbi paranccsal vehető fel:

```
ldapmodify -D <adminDN> -w <adminPW> -i
<fájlnév>
```

ahol a <*fájlnév*> a következőt tartalmazza:

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: ( <myobjectClass-oid> NAME
'<myobjectClass>' DESC '<LDAP alkalmazáshoz meghatározott
objektumosztály>' SUP '<objectclassinheritance>'
                 <objectclasstype> MAY (<attribútum1> $ <attribútum2>))
```

Objektumosztály módosítása

Az alábbi információk segítséget nyújtanak az objektumosztályok módosítása során.

Nem minden sémamódosítás megengedett. További részletek a módosítások korlátozásairól: “Nem engedélyezett sémamódosítások” oldalszám: 28.

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 **Szerkesztés** 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 kapcsolatosan további információkat az “Objektumosztályok” oldalszám: 17 témakör tartalmaz.
     - 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 az adott listákból törölhetők. Ehhez válassza ki az attribútumokat, majd kattintson a megfelelő **Áthelyezés** vagy **Törlés** gombra.

     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.

A séma objektumosztályainak megtekintéséhez adja ki az alábbi parancsot:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Egy objektumosztály a parancssorból az alábbi paranccsal módosítható:

```
ldapmodify -D <adminDN> -w <adminPW> -i
<fájlnév>
```

ahol a <*fájlnév*> a következőt tartalmazza:

```
dn: cn=schema
changetype: modify
replace: objectclasses
objectclasses: ( <sajatobjektumOsztaly-oid> NAME '<sajatobjektumOsztaly>' DESC '<Egy objektumosztály az LDAP
alkalmazásomhoz>' SUP '<újsuperiorosztályobjektum>'
                 <újobjektumosztálytípus> MAY
(attribútum1> $ <attribútum2>
                  $ <újattribútum3>) )
```

Objektumosztály másolása

Az alábbi információk segítséget nyújtanak az objektumosztályok másolása során.

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. A **tempPerson** másolatának neve például **tempPersonCOPY** lesz.
     - A **Leírás** módosítása.
     - Módosítsa az **Objektumazonosító** értékét. Az alapértelmezett objektumazonosító az átmásolt objektumosztály neve, kiegészítve a COPY szóval. A **tempPerson-oid** másolatának neve például **tempPerson-oidCOPY** lesz.
     - 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 kapcsolatosan további információkat az “Objektumosztályok” oldalszám: 17 témakör tartalmaz.
     - 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 az adott listákból törölhetők. Ehhez válassza ki az attribútumokat, majd kattintson a megfelelő **Áthelyezés** vagy **Törlés** gombra.

     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.

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
<adminPW> -i <fájlnév>
```

ahol a <*fájlnév*> a következőt tartalmazza:

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( <sajatujobjektumOsztaly-oid> NAME '<sajatujobjektumOsztaly>'
                DESC '<Egy új objektumosztály,
```

```
                amelyet az LDAP alkalmazáshoz másoltam át>'
              SUP
'<superiorosztályobjektum>>'<objektumosztálytípus> MAY (attribútum1>
              $ <attribútum2> $ < attribútum3>) )
```

Objektumosztály törlése

Az alábbi információk segítséget nyújtanak az objektumosztályok törlése során.

Nem minden sémamódosítás megengedett. További részletek a módosítások korlátozásairól: “Nem engedélyezett sémamódosítások” oldalszám: 28.

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.

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
<adminPW> -i <fájlnév>
```

ahol a <*fájlnév*> a következőt tartalmazza:

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: (<sajatobjektumOsztaly-oid>)
```

Attribútumok megjelenítése

Az alábbi információk segítséget nyújtanak az attribútumok megjelenítése során.

A séma attribútumait a webes adminisztrációs eszközzel (ez a javasolt módszer), valamint a parancssorból tekintheti meg.

1. 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: 24. 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.
2. Ha készen van, kattintson a **Bezárás** gombra. Visszatér az IBM Directory Server **Üdvözlet** ablakába.

A séma attribútumainak megtekintéséhez adja ki az alábbi parancsot:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes
IBMAttributeTypes
```

Attribútum hozzáadása

Az alábbi információk segítséget nyújtanak az attribútumok hozzáadása során.

Új attribútum az alábbi módszerek egyikével hozható létre. A javasolt módszer a webes adminisztrációs eszköz használata.

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. Lásd: “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: 24.
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 menükből az egyenlőség, a sorrendezés és a részkarakterlánc megfeleltetési szabályokhoz. A megfeleltetési szabályok teljes listája itt található: “Megfeleltetési szabályok” oldalszám: 21.
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: 23.

      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.

Ha attribútumot a parancssor segítségével kíván hozzáadni, akkor adja ki a következő parancsot. Az alábbi példa felvesz egy attribútumtípus-meghatározást a ″sajatAttributum″ nevű attribútumhoz, Directory String szintaxissal (magyarázat: “Attribútum-szintaxis” oldalszám: 24) és Kis- és nagybetű egyezés figyelmen kívül hagyása egyeztetéssel (részletek: “Megfeleltetési szabályok” oldalszám: 21). A meghatározás IBM-specifikus része azt adja meg, hogy az attribútumadatok egy a ″sajatAttrTabla″ tábla ″sajatAttrOszlop″ nevű oszlopában kerüljenek tárolásra. Ha ezek a nevek nincsenek megadva, akkor az oszlop- és táblanév egyformán ″sajatAttributum″ lesz alapértelmezés szerint. Az attribútum ″normál″ hozzáférési osztályba kerül, és az értékei nem lehetnek 200 byte-nál hosszabbak.

```
ldapmodify -D <admindn> -w <adminPW> -i sajatsema.ldif
```

ahol a **sajatsema.ldif** fájl tartalma:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( sajatAttributum-oid NAME ( 'sajatAttributum' )
                 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: ( sajatAttributum-oid  DBNAME ( 'sajatAttrTabla' 'sajatAttrOszlop' )
                    ACCESS-CLASS normal LENGTH 200 )
```

Attribútum módosítása

Az alábbi információk segítséget nyújtanak az attribútumok módosítása során.

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.

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 **Szerkesztés** 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
         - **Megfeleltetési szabály** megadása
         - A **Felettes 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.

Ha attribútumot a parancssor segítségével kíván módosítani, akkor adja ki a következő parancsot. 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 sajatsemamodositas.ldif
```

ahol a **sajatsemamodositas.ldif** fájl tartalma:

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: ( sajatAttributum-oid NAME ( 'sajatAttributum' ) 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: ( sajatAttributum-oid  DBNAME ( 'sajatAttrTabla' 'sajatAttrOszlop' )
                  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.

Attribútum másolása

Az alábbi információk segítséget nyújtanak az attribútumok másolása során.

Az attribútum az alábbi módszerek egyikével másolható. A javasolt módszer a webes adminisztrációs eszköz használata.

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 nevét**. Az alapértelmezett név az átmásolt attribútum neve, kiegészítve a COPY szóval. A **tempID** másolatának neve például **tempIDCOPY** lesz.
4. Módosítsa az attribútum **Leírását**, mint például **Az ideiglenes alkalmazottak azonosítószámaként használt attribútum**.
5. Módosítsa az **Objektumazonosító** értékét. Az alapértelmezett objektumazonosító az átmásolt attribútum OID neve, kiegészítve a COPYOID szóval. A **tempID-oid** másolatának neve például **tempID-oidCOPYOID** lesz.
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: 24.
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 menükből az egyenlőség, a sorrendezés és a részkarakterlánc megfeleltetési szabályokhoz. A megfeleltetési szabályok teljes listája itt található: “Megfeleltetési szabályok” oldalszám: 21.
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 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** 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: 23.

      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.

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
<adminPW> -i <fájlnév>
```

ahol a <*fájlnév*> a következőt tartalmazza:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( <sajatújAttributum-oid> NAME '<sajatujAttributum>' DESC '<Az LDAP alkalmazásomhoz
                 másolt új attribútum> EQUALITY 2.5.13.2
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( sajatAttributum-oid  DBNAME ( 'sajatAttrTabla' 'sajatAttrOszlop' )
                   ACCESS-CLASS normal LENGTH 200 )
```

Attribútum törlése

Az információk segítséget nyújtanak az attribútumok könyvtárfából való törlése során.

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.

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.

Ha a parancssor segítségével kíván attribútumot törölni, akkor adja ki a következő parancsot:

```
ldapmodify -D <admindn>
-w <adminjelszó> -i sajatsematorles.ldif
```

ahol a **sajatsematorles.ldif** fájl tartalma:

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

Séma átmásolása más szerverekre

Az alábbi információk segítséget nyújtanak a sémák más szerverekre másolása során.

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: ( sajatattr1-oid NAME 'sajatattr1' DESC 'Információk.'
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( sajatattr1-oid DBNAME( 'sajatattr1'  'sajatattr1' )
     ACCESS-CLASS normal LENGTH 500 )
   attributetypes: ( sajatattr2-oid NAME 'sajatattr2' DESC 'Információk.' SYNTAX
   1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( sajatattr2-oid DBNAME( 'sajatattr2'  'sajatattr2' )
     ACCESS-CLASS normal LENGTH 500 )
   objectclasses: ( sajatobjektum-oid NAME 'sajatobjektum' DESC 'Ide is leírás
      kerül.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( sajatattr1 $ sajatattr2 ) )
   ```

3. Szúrjon 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: ( sajatattr1-oid NAME 'sajatattr1' DESC 'Információk.' SYNTAX
   1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( sajatattr1-oid DBNAME( 'sajatattr1'  'sajatattr1' )
     ACCESS-CLASS normal LENGTH 500 )

   dn: cn=schema
   changetype: modify
   add: attributetypes ibmattributetypes
   attributetypes: ( sajatattr2-oid NAME 'sajatattr2' DESC 'Információk.' SYNTAX
   1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( sajatattr2-oid DBNAME( 'sajatattr2'  'sajatattr2' )
     ACCESS-CLASS normal LENGTH 500 )

   dn: cn=schema
   changetype: modify
   ```

```
add: objectclasses
objectclasses: ( sajatobjektum-oid NAME 'sajatobjektum' DESC 'Ide is leírás
   kerül.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( sajatattr1 $ sajatattr2 ) )
```

4. Töltse be a sémát más szervereken az ldapmodify segédprogrammal:

```
ldapmodify -D cn=administrator -w <jelszó> -f schema.ldif
```

Címtárbejegyzésekkel kapcsolatos feladatok

Az alábbi információk segítséget nyújtanak a címtárbejegyzések kezelése során.

A címtárbejegyzések kezeléséhez bontsa ki a webes adminisztrációs eszköz navigációs területének **Címtárkezelés** kategóriáját.

Kapcsolódó fogalmak

“Utótag (névkontextus)” oldalszám: 13
Az utótag (más néven névkontextus) egy olyan DN, amely egy helyileg tárolt címtárhierarchia legfelső bejegyzését azonosítja.

“Séma” oldalszám: 14
A séma az a szabályhalmaz, amelyik szabályozza, milyen adatok tárolhatók a címtárban. A séma határozza meg az engedélyezett bejegyzések típusát, attribútumaik szerkezetét és szintaxisát.

“LDAP címtárobjektumok tulajdonjoga” oldalszám: 77
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.

Címtárfa tallózása

Az alábbi információk segítséget nyújtanak a címtárfa tallózása során.

Először ezt kell tennie.

A szakaszt éppen így kell beállítani.

1. Ha még nem tette volna meg, bontsa ki a navigációs terület **Címtárkezelés** kategóriáját.
2. 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

Az információk segítséget nyújtanak a bejegyzések címtárfához adása során.

1. Ha még nem tette volna meg, bontsa ki a navigációs terület **Címtárkezelés** kategóriáját.
2. Kattintson a **Bejegyzés hozzáadása** lehetőségre.
3. Válasszon ki egy **Strukturális objektumosztályt** a legördülő listából.
4. Kattintson a **Tovább** gombra.
5. 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.
6. Kattintson a **Tovább** gombra.
7. A **Relatív DN** mezőben írja be a felvenni kívánt bejegyzés viszonylagos megkülönböztető nevét (RDN), például cn=John Doe.
8. 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.

9. 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.
10. Kattintson az **Elhagyható attribútumok** lapra.
11. Az **Elhagyható attribútumok** lapon írja be az elhagyható attribútumok értékeit. A bináris értékek felvételével kapcsolatos további információk: “Bináris attribútumok módosítása” oldalszám: 200. Ha egynél több értéket akar megadni egy adott attribútumnak, akkor kattintson a **Többszörös érték** gombra, és írja be egyesével az értékeket.
12. Kattintson az OK gombra a bejegyzés létrehozásához.
13. Az **ACL** gombra kattintva módosíthatja a bejegyzés hozzáférés-felügyeleti listáját. További információk az ACL-ekről: “Hozzáférés-felügyeleti listák” oldalszám: 65.
14. 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

Az alábbi információk segítséget nyújtanak a nyelvi címkékkel ellátott attribútumokat tartalmazó bejegyzések hozzáadása során.

Egy nyelvi címkékkel rendelkező attribútumokat tartalmazó bejegyzés készítéséhez:

1. Engedélyezze a nyelvi címkéket. Lásd: “Nyelvi címkék engedélyezése” oldalszám: 126.
2. A navigációs terület **Címtárkezelés** kategóriájában kattintson a **Bejegyzések kezelése** lehetőségre.
3. Kattintson az **Attribútumok szerkesztése** gombra.
4. Válassza ki azt az attribútumot, amelyhez nyelvi címkét szeretne létrehozni.
5. Kattintson a **Nyelve címke értéke** gombra a **Nyelvi címke értékek** panel eléréséhez.
6. A **Nyelvi címke** mezőben adja meg a létrehozni kívánt címke nevét. A címkének a lang- toldalékkal kell kezdődnie.
7. Adja meg a címke értékét az **Érték** mezőben.
8. Kattintson a **Hozzáadás** gombra. A nyelvi címke és az érték megjelenik a menülistában.
9. Hozzon létre további nyelvi címkéket vagy módosítsa az attribútumok meglévő nyelvi címkéit a 4., 5. és 6. lépés megismétlésével. A kívánt nyelvi címkék létrehozása után kattintson az **OK** gombra.
10. Bontsa ki a **Megjelenítés nyelvi címkékkel** menüt és válasszon ki egy nyelvi címkét. Kattintson a **Nézet módosítása** alehetőségre és megjelennek a nyelvi címkékhez megadott attribútumértékek. Minden ebben a nézetben megadott érték csak a kiválasztott nyelvi címkére érvényes.
11. Ha befejezte, akkor kattintson az **OK** gombra.

Kapcsolódó hivatkozás

“Nyelvi címkék” oldalszám: 50
A *nyelvi címkék* meghatározzák azt a mechanizmust, amelynek segítségével a Directory Server a természetes nyelvek kódjait a címtárban tárolt értékekhez rendelheti és a kliensek lekérdezhetik a bizonyos természetes nyelvi feltételeknek megfelelő értékeket.

Bejegyzés törlése

Az információk segítséget nyújtanak a bejegyzések könyvtárfából való törlése során.

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 részfát, utótagot vagy elemet. Kattintson a jobb oldali eszközsor **Törlés** elemére.
2. Meg kell erősítenie a törlést. Kattintson az **OK** gombra. A bejegyzés törlésre kerül a könyvtárból és visszatér a bejegyzések listájához.

Bejegyzés módosítása

Az alábbi információk segítséget nyújtanak a címtárfa bejegyzéseinek módosítása során.

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. Kattintson a jobb oldali eszközsor **Attribútumok módosítása** elemére.
2. A **Kötelező attribútumok** lapon írja be a kötelező attribútumok értékeit. A bináris értékek felvételével kapcsolatos további információk: “Bináris attribútumok módosítása” oldalszám: 200. 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** gombra.
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. 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 az **Eltávolítás** gombra.
     d. Kattintson az **OK** gombra.
   - A taglista frissítéséhez kattintson a **Frissítés** elemre.
8. A bejegyzés módosításához kattintson az **OK** gombra.

Bejegyzés másolása

Az alábbi információk segítséget nyújtanak a címtárfa bejegyzéseinek másolása során.

Ez a funkció akkor hasznos, ha hasonló bejegyzéseket hoz létre. A másolat az eredeti összes attribútumát megörökli. Az új bejegyzés elnevezéséhez némi módosításokat végre kell hajtania.

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 **Másolás** elemére.
2. Módosítsa a DN mező RDN bejegyzését. Például írja át a cn=John Doe elemet cn=Jim Smith értékre.
3. A kötelező attribútumok lapon módosítsa a cn bejegyzést az új RDN-re. Ez a jelen példában Jim Smith.
4. Szükség szerint módosítsa a többi kötelező attribútumot. A jelen példában írja át az sn (vezetéknéz) attribútum értékét Doe-ról Smith-re.
5. 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

Az alábbi információk segítséget nyújtanak a hozzáférés felügyeleti listák (ACL) kezelésében.

További információk az ACL tulajdonságok megtekintéséről a webes adminisztrációs eszközzel, illetve az ACL-ek kezeléséről: “Hozzáférés felügyeleti lista (ACL) feladatok” oldalszám: 211.

Kapcsolódó fogalmak

“Hozzáférés-felügyeleti listák” oldalszám: 65
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.

Kiegészítő objektumosztály hozzáadása

Az alábbi információk segítséget nyújtanak a kiegészítő objektumosztályok hozzáadása során.

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** gombra.
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. A bejegyzés módosításához kattintson az **OK** gombra.

Kiegészítő osztály törlése

Az alábbi információk segítséget nyújtanak a kiegészítő osztályok törlése során.

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.

Csoporttagság módosítása

Az alábbi információk segítséget nyújtanak a csoporttagság módosítása során.

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

Az alábbi információk segítséget nyújtanak a címtárbejegyzések keresése során.

Háromféle módon lehet keresni a címtárfában:

- 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.

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)

Az összetett keresés során keresési megszorításokat adhat meg és használhat keresési szűrőket. Az alapértelmezett keresési feltételek alapján kereséshez használja az Egyszerű keresés funkciót.

1. Egy egyszerű keresés végrehajtása:
   a. A **Keresési szűrő** lapon kattintson az **Egyszerű keresés** lehetőségre.
   b. Válasszon ki egy felettes objektumosztályt a legördülő listából.
   c. 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.
2. Egy összetett keresés végrehajtása:
   a. A **Keresési szűrő** lapon kattintson az **Összetett keresés** lehetőségre.
   b. Válasszon ki egy **attribútumot** a legördülő listából.
   c. Válasszon ki egy **Összehasonlító** operátort.
   d. Írja be az összehasonlításhoz tartozó **értéket**.

e. 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.
   - 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.

3. Kézi keresés végrehajtásához hozzon létre egy kereső szűrőt.

   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=<részlegnév>))`

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.

Kapcsolódó feladatok

“Keresési beállítások módosítása” oldalszám: 128
Az alábbi információk segítséget nyújtanak a felhasználó keresési képességeinek vezérlése során.

Kapcsolódó hivatkozás

"Keresési paraméterek" oldalszám: 48
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.

Bináris attribútumok módosítása

Az alábbi információk segítséget nyújtanak a bináris adatok importálása, exportálása, illetve törlése során.

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.

1. Bináris adat hozzáadása egy attribútumhoz:
   a. Kattintson a **Bináris adatok** gombra.
   b. Kattintson az **Importálás** gombra.
   c. Beírhatja a kívánt fájl elérési útját, vagy kattinthat a **Tallózás** gombra a bináris fájl kikereséséhez.
   d. Kattintson a **Fájl elküldése** gombra. Megjelenik egy Fájl feltöltve üzenet.
   e. Kattintson a **Bezárás** elemre. A **Bináris adat bejegyzések** alatt megjelenik a **Bináris adatok - 1** felirat.
   f. Ismételje meg az importálási eljárást a kívánt bináris fájlok felvételéhez. A bejegyzések sorra **Bináris adatok - 2**, **Bináris adatok - 3** néven jelennek meg.
   g. Ha kész a bináris adatok felvételével, kattintson az **OK** gombra.
2. Bináris adatok exportálása:
   a. Kattintson a **Bináris adatok** gombra.
   b. Kattintson az **Exportálás** gombra.
   c. Kattintson a **Letölthető bináris adatok** gombra.
   d. Kövesse a varázsló utasításait a bináris fájl megjelenítéséhez vagy egy új helyre elmentéséhez.
   e. Kattintson a **Bezárás** elemre.
   f. Ismételje meg az exportálási eljárást az exportálni kívánt bináris fájlokhoz.
   g. Ha kész a bináris adatok exportálásával, kattintson az **OK** gombra.
3. Bináris adatok törlése:
   a. Kattintson a **Bináris adatok** gombra.
   b. Jelölje meg a törölni kívánt bináris adatfájlokat. Több fájl is kiválasztható.
   c. Kattintson a **Törlés** gombra.
   d. A törlés jóváhagyásaként kattintson az **OK** gombra. A törlésre megjelölt bináris adatok törlésre kerülnek a listából.
   e. Ha kész a bináris adatok törlésével, kattintson az **OK** gombra.

Megjegyzés: A bináris attribútumoknak csak a létezése kereshető.

Felhasználói és csoportfeladatok

Az alábbi információk segítséget nyújtanak a felhasználók és csoportok kezelése során.

A felhasználók és csoportok kezeléséhez bontsa ki a webes adminisztrációs eszköz navigációs területének **Felhasználók és csoportok** kategóriáját.

Kapcsolódó fogalmak

"Csoportok és szerepek" oldalszám: 57
A csoportok és szerepek segítségével a tagok hozzáférését és jogosultságait rendszerezheti.

Felhasználói feladatok

Az alábbi információk segítséget nyújtanak a felhasználók kezelése során.

A tartományok és sablonok beállítása után feltöltheti őket felhasználókkal.

Kapcsolódó hivatkozás

“Hitelesítés” oldalszám: 82
A Directory Server hozzáférése hitelesítési módszer segítségével felügyelhető.

Felhasználók hozzáadása:

Az alábbi információk segítséget nyújtanak a felhasználók hozzáadása során.

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:

Az alábbi információk segítséget nyújtanak a felhasználók tartományon belüli keresése során.

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 azt 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:
   - **Szerkesztés** - Lásd: “Felhasználó információinak módosítása”.
   - **Másolás** - Lásd: “Felhasználó másolása”.
   - **Törlés** - Lásd: “Felhasználó eltávolítása” oldalszám: 202.
5. Ha kész, kattintson az **OK** gombra.

Felhasználó információinak módosítása:

Az alábbi információk segítséget nyújtanak a felhasználó információinak módosítása során.

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:

Az alábbi információk segítséget nyújtanak a felhasználók másolása során.

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:

Az alábbi információk segítséget nyújtanak a felhasználók eltávolítása során.

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.

Csoportfeladatok

Az alábbi információk segítséget nyújtanak a csoportok kezelésében.

A tartományok és sablonok beállítása után létrehozhat csoportokat.

Csoportok hozzáadása:

Az alábbi információk segítséget nyújtanak a csoportok hozzáadása során.

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. Ezt követően kattintson a **Befejezés** gombra.

   Kapcsolódó fogalmak

   “Csoportok és szerepek” oldalszám: 57
   A csoportok és szerepek segítségével a tagok hozzáférését és jogosultságait rendszerezheti.

Csoportok keresése a tartományon belül:

Az alábbi információk segítséget nyújtanak a csoportok tartományon belüli keresése során.

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”.
5. Ha kész, kattintson a **Bezárás** gombra.

Csoport információinak módosítása:

Az alábbi információk segítséget nyújtanak a csoport információinak módosítása során.

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:

Az alábbi információk segítséget nyújtanak a csoportok másolása során.

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:

Az alábbi információk segítséget nyújtanak a csoportok eltávolítása során.

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.

Tartomány- és felhasználói sablon feladatok

Az alábbi információk segítséget nyújtanak a tartományok és felhasználói sablonok kezelése során.

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 címtárba.

Kapcsolódó fogalmak

"Tartományok és felhasználói sablonok" oldalszám: 47
A webes adminisztrációs eszköz tartomány és felhasználói sablon objektumainak célja, hogy megkönnyítse a felhasználók dolgát azáltal, hogy nem kell az LDAP rendszer alapvető kérdéseivel részletesen foglalkozniuk.

Tartomány létrehozása

Az alábbi információk segítséget nyújtanak a tartományok létrehozása során.

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 címtár 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.

Kapcsolódó fogalmak

"Tartományok és felhasználói sablonok" oldalszám: 47
A webes adminisztrációs eszköz tartomány és felhasználói sablon objektumainak célja, hogy megkönnyítse a felhasználók dolgát azáltal, hogy nem kell az LDAP rendszer alapvető kérdéseivel részletesen foglalkozniuk.

Tartományadminisztrátor létrehozása

Az alábbi információk segítséget nyújtanak a tartományadminisztrátorok létrehozása során.

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 címtárfát és válassza ki az imént létrehozott **cn=realm1,o=ibm,c=us** tartományt.
   d. Kattintson az **ACL szerkesztése** elemre.
   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 kitörölje 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 szerkesztése** gombra.
   e. Kattintson a **Tagok** lapra.
   f. Kattintson a **Tagok** lapra.
   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** lehetőségre. A DN megjelenik az **Aktuális tagok** listában.
   k. Kattintson az **OK** gombra.
4. Ezzel létrehozta a tartomány bejegyzéseit felügyelni képes adminisztrátort.

Sablon létrehozása

Az alábbi információk segítséget nyújtanak a sablonok létrehozása során.

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 részfájába, amely használni fogja a sablont. Ilyen például az előző műveletben létrehozott **cn=realm1,o=ibm,c=us**. A **Tallózás** gombra kattintva kiválaszthat egy másik részfát 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: 210).
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. Ismételje 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 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. 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 hozzáadása egy tartományhoz

Az alábbi információk segítséget nyújtanak a sablonok tartományokhoz adása során.

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** elemre.

Csoportok létrehozása

Az alábbi információk segítséget nyújtanak a csoportok létrehozása során.

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. Ezt követően kattintson a **Befejezés** gombra.

Kapcsolódó fogalmak

“Csoportok és szerepek” oldalszám: 57
A csoportok és szerepek segítségével a tagok hozzáférését és jogosultságait rendszerezheti.

Felhasználó hozzáadása a tartományhoz

Az alábbi információk segítséget nyújtanak a felhasználó tartományhoz adása során.

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.

Tartományfeladatok

Az alábbi információk segítséget nyújtanak a tartományok kezelése során.

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).

Tartomány hozzáadása:

Az alábbi információk segítséget nyújtanak a tartományok hozzáadása során.

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 átmásolódjanak 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:

Az alábbi információk segítséget nyújtanak a tartományok módosítása során.

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 **Szerkesztés** 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 befejezte, akkor kattintson az **OK** gombra.

Tartomány eltávolítása:

Az alábbi információk segítséget nyújtanak a tartományok eltávolítása során.

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 hozzáférés felügyeleti listáinak módosítása:

Az alábbi információk segítséget nyújtanak a tartományok hozzáférés felügyeleti listáinak módosítása során.

További információk az ACL tulajdonságok megtekintéséről a webes adminisztrációs eszközzel, illetve az ACL-ek kezeléséről: “Hozzáférés felügyeleti lista (ACL) feladatok” oldalszám: 211.

Kapcsolódó fogalmak

“Hozzáférés-felügyeleti listák” oldalszám: 65
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.

Sablonfeladatok

Az alábbi információk segítséget nyújtanak a sablonok kezelése során.

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).

Felhasználói sablon felvétele:

Az alábbi információk segítséget nyújtanak a felhasználói sablon felvétele során.

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 átmásolódjanak 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: 210).
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. Ismételje 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 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 sorrendje a sablonon belül módosítható. Ehhez jelölje ki a kívánt attribútumot, majd kattintson a **Fel** vagy **Le** gombra. 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 módosítása:

Az alábbi információk segítséget nyújtanak a sablonok módosítása során.

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 **Szerkesztés** 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: 209.
- Ha kész, kattintson a **Bezárás** gombra.

Sablon eltávolítása:

Az alábbi információk segítséget nyújtanak a sablonok eltávolítása során.

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 listáinak módosítása:

Az alábbi információk segítséget nyújtanak a sablonok hozzáférés felügyeleti listáinak módosítása során.

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 szerkesztése** elemre.

További információk az ACL tulajdonságok megtekintéséről a webes adminisztrációs eszközzel, illetve az ACL-ek kezeléséről: “Hozzáférés felügyeleti lista (ACL) feladatok”.

Kapcsolódó fogalmak

“Hozzáférés-felügyeleti listák” oldalszám: 65
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.

Hozzáférés felügyeleti lista (ACL) feladatok

Az alábbi információk segítséget nyújtanak a hozzáférés felügyeleti listák (ACL) kezelésében.

Kapcsolódó fogalmak

“Hozzáférés-felügyeleti listák” oldalszám: 65
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.

Adott hatályos ACL hozzáférési jogainak megtekintése

Az alábbi információk segítséget nyújtanak egy adott hatályos hozzáférés felügyeleti lista (ACL) hozzáférési jogainak megjelenítéséhez.

A hatályos ACL-ek az adott bejegyzés közvetlenül megadott és öröklött ACL-jeinek együttese.

1. Válasszon ki egy címtárbejegyzést. Legyen ez például a cn=John Doe,ou=Advertising,o=ibm,c=US bejegyzés.
2. Kattintson az **ACL szerkesztése** elemre. Megjelenik az ACL módosítása ablak és annak **Hatályos hozzáférés felügyeleti listák** lapja. A **Hatályos hozzáférés felügyeleti listák** lap a hozzáférés felügyeleti listákra vonatkozó, csak olvasható információkat tartalmaz.
3. Válassza ki a megfelelő hatályos ACL listát, majd kattintson a **Megjelenítés** gombra. Megjelenik a **Hozzáférési jogok megjelenítése** ablak.
4. Kattintson az **OK** gombra a Hatályos ACL-ek lapra visszatéréshez.
5. Kattintson a **Mégse** gombra az ACL módosítása ablakba visszatéréshez.

Tényleges tulajdonosok megjelenítése

Az alábbi információk segítséget nyújtanak a tényleges tulajdonosok megjelenítése során.

A hatályos tulajdonosok az adott bejegyzés közvetlenül megadott és öröklött tulajdonosainak együttese.

1. Válasszon ki egy címtárbejegyzést. Legyen ez például a cn=John Doe,ou=Advertising,o=ibm,c=US bejegyzés.
2. Kattintson az **ACL szerkesztése** elemre.
3. Kattintson a **Tényleges tulajdonosok** lapra. A **Tényleges tulajdonosok** lap a hozzáférés felügyeleti listákra vonatkozó, csak olvasható információkat tartalmaz.
4. Kattintson a **Mégse** gombra az ACL módosítása ablakba visszatéréshez.

Nem szűrt ACL listák hozzáadása, módosítása és eltávolítása

Az alábbi információk segítséget nyújtanak a nem szűrt hozzáférés felügyeleti listák (ACL) kezelésében.

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 szülőobjektumoktól, 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 megörökölt 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.

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 **Meghatározás** lehetőségre. 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.

Az ACL-ek eltávolítása kétféle módon történhet:

- Kattintson a törölni kívánt ACL melletti választógombra. Kattintson az **Eltávolítás** gombra.
- Az **Összes törlése** gombbal törölheti a lista összes DN-jét.

Szűrt ACL listák hozzáadása, módosítása és eltávolítása

Az alábbi információk segítséget nyújtanak egy szűrt hozzáférés felügyeleti lista (ACL) hozzáférési jogainak megjelenítéséhez.

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 ős 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.

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 **Meghatározás** lehetőségre. 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.

Az ACL-ek eltávolítása kétféle módon történhet:

- Kattintson a törölni kívánt ACL melletti választógombra. Kattintson az **Eltávolítás** gombra.
- Az **Összes törlése** gombbal törölheti a lista összes DN-jét.

Tulajdonosok felvétele és eltávolítása

Az alábbi információk segítséget nyújtanak a tulajdonosok felvétele és eltávolítása során.

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:

1. 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 ősétől öröklik meg tulajdonosukat, amelyiknél be van állítva ez a lehetőség.
2. 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 részfát, amelyben minden objektum saját magának tulajdonosa.
3. Típus - Adja meg a DN **Típusát**. Ha például a DN egy felhasználó, akkor válassza ki az access-id lehetőséget.

Tulajdonos felvétele esetén a DN hozzáadásához kattintson a **DN (megkülönböztetett név)** mezőben a **Hozzáadás** gombra.

A tulajdonosok eltávolítása kétféle módon történhet:

- Kattintson a törölni kívánt tulajdonos melletti választógombra. Kattintson az **Eltávolítás** gombra.
- Az **Összes törlése** gombbal törölheti a lista összes tulajdonos DN-jét.

Referencia

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

Az alábbiakat használja referenciainformációkként.

Directory Server parancssori segédprogramok

Az alábbi rész a Qshell parancskörnyezetből futtatható Directory Server segédprogramok leírását tartalmazza.

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 karaktersorozatok: "*"
- Zárójeleket tartalmazó karaktersorozatok: "(objectclass=person)"

További információkata a Qshell parancskörnyezetről a “Qshell” témakörben talál.

További információkat az alábbi parancsok leírásánál talál:

ldapmodify és ldapadd

Az LDAP modify-entry (bejegyzésmódosító) és LDAP add-entry (bejegyzés-felvevő) parancssori segédprogram.

Összegezés

```
| ldapmodify [-a] [-b] [-c] [-C karakterkészlet] [-d nyomkövetési_szint][-D binddn] [-e hibafájl]
  [-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] [-e hibafájl]
  [-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_rename alkalmazás
| programozási felülethez (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 -?
```

Kapcsolók

-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* kapcsolót, 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.

-e *hibafájl*
Megadja a fájlt, amelyhez a visszautasított bejegyzések megírásra kerülnek. Ehhez a kapcsolóhoz a -c folyamatos működés kapcsoló szükséges. Ha a bejegyzés feldolgozása meghiúsul, akkor a bejegyzés beírásra kerül a visszautasítás fájlba és a visszautasított bejegyzések száma nő. Ha az ldapmodify vagy ldapadd parancs bemenete fájlból származik, akkor a fájl feldolgozásakor a visszautasítás fájlba írt bejegyzések teljes száma kerül megadásra.

-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. A -i vagy -f kapcsolóval megadható egy bemeneti fájl. A viselkedés azonos.

-F Kikényszeríti az összes változás alkalmazását, függetlenül a replica: karaktesorozattal 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 szóközöket.

–G Megadja a tartományt. A paraméter elhagyható. 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* 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. A -i vagy -f kapcsolóval megadható egy bemeneti fájl. A viselkedés azonos.

-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 kulcscsomó 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.

-l Ne kerüljön replikálásra a változás. A Ne történjen replikálás vezérlőelem kéri, hogy a változás ne legyen

replikálva. Ezt a Replikáció topológia használja annak megakadályozásához, hogy a célszerver replikálja az elvégzett módosításokat a replikáció topológia szinkronizálása érdekében, azaz hogy ne okozza más szerverek módosítását. Ezt a vezérlőelemet az adminisztrációs kliens használhatja.

-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 kapcsoló (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) paramétert.

-M Az utalási objektumok normál bejegyzésként kezelése.

-n Adja meg a nincs művelet kapcsolót a kiadott parancs eredményének előzetes megjelenítésének engedélyezéséhez anélkül, hogy a tevékenység ténylegesen végrehajtásra kerüljön a címtáron. Az esetleges módosításokat a szabványos kimeneten felkiáltójel előzi meg. A címtár változtatását végző függvények meghívása előtt, a bemeneti fájl feldolgozása során észlelt szintaktikai hibák megjelenítésre kerülnek a szabványos kimeneten. Ez a kapcsoló különösen a -v kapcsolóval együtt hasznos a műveletek nyomkövetéséhez, hibák észlelése esetén.

-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 az ***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** 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 kliens könyvtár 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 *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 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 **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. 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 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.

Bemenet formátuma

A fájl (vagy ha nincs **-i** kapcsoló megadva a parancssorban, akkor a szabványos bemenet) formátumának meg kell felelnie az LDIF formátumnak.

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, hozzáaadja 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.

Megjegyzések

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.

Kapcsolódó fogalmak

“Utótag (névkontextus)” oldalszám: 13
Az utótag (más néven névkontextus) egy olyan DN, amely egy helyileg tárolt címtárhierarchia legfelső bejegyzését azonosítja.

Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek
A Directory Server alkalmazás programozási felületekkel kapcsolatosan további információkat az Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek témakör tartalmaz.

“Directory Server konfigurációs séma” oldalszám: 255
Az alábbi rész a címtár-információs fát (Directory Information Tree, DIT) és az ibmslapd.conf fájl beállításához használt attribútumokat írja le.

Kapcsolódó hivatkozás

“LDAP adatcsere formátum (LDIF)” oldalszám: 248
Az LDAP adatcsere formátum az LDAP objektumok és frissítések (hozzáadás, módosítás, törlés, DN módosítás) szöveges ábrázolásához. Az LDIF rekordokat tartalmazó fájlok segítségével adatok vihetők át a címtárszerverek között, vagy az LDAP eszközök - mint például az **ldapadd** és **ldapmodify** - bemenetként használhatják.

ldapdelete

LDAP delete-entry (bejegyzéstörlő) parancssori segédprogram.

Összegezés

```
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 fejlszó| ?] [-y proxydn][-Y] [-Z] [dn]......
```

Leírás

Az **ldapdelete** egy parancssori illesztő az ldap_delete alkalmazás programozási felülethez (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 -?
```

Kapcsolók

-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 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.

-f *fájl* Egy fájlból olvas be sorokat, minden sorra végrehajt egy LDAP törlést. Mindegyik sor egyetlen megkülönböztetett nevet (DN) tartalmazhat.

-G *tartomány*
Megadja a tartományt. A paraméter elhagyható. Az -m DIGEST-MD5 kapcsolóval használva az érték a kapcsolódás során átadásra kerül a szervernek.

-h *ldaphoszt*
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 kapcsoló (általában a kapcsolati DN) használható. Lehet egy DN, illetve 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) paramétert.

-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 az ***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** 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 kliens könyvtár 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 *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.

-s Ezzel a kapcsolóval törölheti a megadott bejegyzésnél kezdődő teljes részfát.

–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 *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 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:

Megjegyzések

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.

Kapcsolódó fogalmak

Directory Server alkalmazás programozási felületek

ldapexop

Az LDAP kiterjesztett művelet parancssori segédprogram.

Összegezés

```
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. Ezen felül 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
```

Kapcsolók

Az ldapexop parancs kapcsolói 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 kapcsolók

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* kapcsolót, 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.

-e Kiírja az LDAP könyvtár verziószámát, majd kilép.

-G Megadja a tartományt. A paraméter elhagyható. Az -m DIGEST-MD5 kapcsolóval használva az érték a kapcsolódás során átadásra kerül a szervernek.

-h *ldaphoszt*

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 kapcsoló (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) paramétert.

-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 az ***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** 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 mechanizmusnál 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:

- **acctstatus**: Fiókállapot kiterjesztett művelet. Megjeleníti a megadott fiók állapotát.

```
ldapexop –op acctstatus –d <DN>
```

-d DN

Azonosítja a bejegyzés megkülönböztetett nevét, amelyhez a fiókállapot lekérésre kerül.

A fiókállapot lehet nyitott, zárolt vagy lejárt.

- **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 kliens kéréseket.

  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
```

- **clearlog | getlogsize | readlog -log ...**

Ez a három művelet támogat egy új naplófájlt:

LostAndFound

Ezek a műveletek használhatók az i5/OS címtárszerverrel (V6R1 és újabb), de csak bizonyos naplófájlok támogatottak:

LostAndFound – a replika ütközik a naplófájllal

- **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"
```

- **controlreplerr**

A controlreplerr kiterjesztett művelet lehetővé teszi a replikálási hibatábla kezelését i5/OS V6R1 (vagy IBM Tivoli Directory Server v6.0) vagy újabb szerveren. A beállítási lehetőségek a következők:

```
ldapexop -op controlreplerr –show <hibaazonosító> -ra <agreementDN>
```

Ez lehetővé teszi a replikálási hibatáblában lévő bejegyzések megjelenítését

<hibaazonosító>

A hiba azonosítója. Az összes bejegyzés megjelenítéséhez adja meg a 0 értéket.

<agreementDN>

A replikációs megállapodás, amelyhez a bejegyzés hozzá van rendelve.

```
ldapexop -op controlreplerr –delete <hibaazonosító> -ra <agreementDN>
```

Ez lehetővé teszi a bejegyzések törlését a replikálási hibatáblából

<hibaazonosító>
A hiba azonosítója. Az összes bejegyzés megjelenítéséhez adja meg a 0 értéket.

<agreementDN>
A replikációs megállapodás, amelyhez a bejegyzés hozzá van rendelve.

```
ldapexop -op controlreplerr –retry <hibaazonosító> -ra <agreementDN>
```

Ez lehetővé teszi egy bejegyzés újbóli megkísérlését a replikálási hibatáblában

<hibaazonosító>
A hiba azonosítója. Az összes bejegyzés megjelenítéséhez adja meg a 0 értéket.

<agreementDN>
A replikációs megállapodás, amelyhez a bejegyzés hozzá van rendelve.

- **evaluateGroups**

  Az ldapexop segédprogram egy új evaluateGroups műveletet támogat:

  ```
  ldapexop –op evaluateGroups –d userDN –a <attribútum és érték párok
  szóközzel elválasztott listája>
  ```

  Megjeleníti a csoportok listáját, amelyhez a megadott userDN tartozik.

  A ″–a″ kapcsoló megadja a bejegyzés attribútumértékeit és lekéri a bejegyzésnek megfelelő dinamikus csoportokat. Ha a ″–a″ kapcsoló nincs megadva, akkor a kérés a kiszolgálóhoz csak statikus csoporthoz kerül elküldésre. Ez a kiterjesztett művelet csoporttagsági információkat kér le a userDN elemhez, amely nem létezik a kiszolgálón (például a userDN távoli csoporttagot ábrázol). Az ibm-allGroups működési attribútumot a userDN-t tartalmazó kiszolgáló csoporttagságait listázza.

  Példa:

  Az uid=sample,cn=users,o=ibm bejegyzés csoporttagságának kiértékelése a bejegyzés *departmentnumber* és *objectclass* attribútumának értéke alapján:

  ```
  ldapexop -op evaluateGroups -d uid=sample,cn=users,o=ibm -a objectclass=person
  departmentnumber=abc
  ```

  Megjegyzés: Ez a kiterjesztett művelet jellemzően a kérdéses bejegyzéshez az összes attribútumértéket megadja.

- **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 <Adminjelszó> -op getusertype
  ```

  Visszaadott érték:

  ```
  User : root_administrator
  Role(s) : server_config_administrator directory_administrator
  User : global_admin_group_member
  Role(s) : 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-slapdAdminPW
  ```

  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-slapdadmindn[2]
  ibm-slapdadminpw[2, 3]
  ibm-slapderrorlog[1, 4]
  ibm-slapdpwencryption[1]
  ibm-slapdsizelimit[1]
  ibm-slapdsysloglevel[1, 4]
  ibm-slapdtimelimit[1]

  cn=Front End, cn=Configuration
  ibm-slapdaclcache[1]
  ibm-slapdaclcachesize[1]
  ibm-slapdentrycachesize[1]
  ibm-slapdfiltercachebypasslimit[1]
  ibm-slapdfiltercachesize[1]
  ibm-slapdidletimeout[1]

  cn=Event Notification, cn=Configuration
  ibm-slapdmaxeventsperconnection[2]
  ibm-slapdmaxeventstotal[2]

  cn=Transaction, cn=Configuration
  ibm-slapdmaxnumoftransactions[2]
  ibm-slapdmaxoppertransaction[2]
  ibm-slapdmaxtimelimitoftransactions[2]


  cn=ConfigDB, cn=Config Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
  ibm-slapdreadonly[2]

  cn=Directory, cn=RDBM Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
  ibm-slapdbulkloaderrors[1, 4]
  ```

ibm-slapdclierrors[1, 4]
ibm-slapdpagedresallownonadmin[2]
ibm-slapdpagedreslmt[2]
ibm-slapdpagesizelmt[2]
ibm-slapdreadonly[2]
ibm-slapdsortkeylimit[2]
ibm-slapdsortsrchallownonadmin[2]
ibm-slapdsuffix[2]

- **repltopology -rc [kapcsolók]**:

  A repltopology kiterjesztett művelet a fogyasztó szerveren lévő replikáció topológia információkat egyezteti az ellátó szerveren lévő topológiával.

  ```
  ldapexop –op repltopology –rc  [-timeout secs] [-ra agreementDn]
  ```

  ahol

  -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).

  -ra agreementDn
  Az **-ra** agreementDn a replikációs megállapodás DN-je. A művelet csak az adott replikációs megállapodáson kerül végrehajtásra. Ha az -ra kapcsoló nincs megadva, akkor a művelet a kontextus alatt megadott összes replikációs megállapodáshoz végrehajtásra kerül.

  Példa:

  ```
  ldapexop -op repltopology -rc "o=acme,c=us" -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"-timeout 60
  ```

  Az ellátó szerver a fogyasztó szerverhez van kötve a beállított replikációs hitelesítési adatokkal. Az ellátó megkülönböztetett nevek jogosultak utótagok hozzáadására a fogyasztó (replika) szerver konfigurációs ellátójához. Ezt az ellátó szerver használja a replikáció topológia kiterjesztett művelet részeként, a hiányzó utótagok fogyasztó szerverhez adásához. Azon utótagok esetén, amelyekhez a contextDN bejegyzés még nem létezik, az ellátó megkülönböztetett nevek jogosultak új replikált részfa létrehozására. Ha a contextDN bejegyzés már létezik, akkor már korábban meg kellett adni a replikált részfa gyökereként, azaz rendelkeznie kell ibm-replicationcontext objektumosztállyal.

- **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 állú műveletekkel rendelkező kapcsolatok azonnal megszakadnak. Ha egy dolgozó jelenleg haszál 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 <*attribútum*>
  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 kiterjeszett műveletnélhozzáadásra kerül a konfigurációs fájlhoz a ″cn=Directory,cn=RDBM Backends,cn=IBM Directory,cn=schema,cn=Configuration″ bejegyzés alatt:

  ```
  ibm-slapdPlugin: extendedop /QSYS.LIB/QGLDRDBM.SRVPGM 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.

Kapcsolódó fogalmak

Directory Server alkalmazás programozási felületek

“Replikációs hibatábla” oldalszám: 44
A replikációs hibatábla a meghiúsult frissítéseket rögzíti a későbbi helyreállítás céljából. A replikáció kezdetekor a rendszer összeszámolja az összes replikációs megállapodással kapcsolatos meghibásodás számát. Ez a szám akkor növekszik, ha egy frissítés meghiúsul, és ezáltal a tábla új bejegyzéssel bővül.

Kapcsolódó feladatok

“Talált tárgyak naplófájl megjelenítése” oldalszám: 165
A replikáció talált tárgyak naplófájl megjeleníthető az IBM Tivoli Directory Server webes adminisztrációs eszköz, illetve az ldapexop segédprogram naplófájl paramétereinek segítségével. A fájl továbbá közvetlenül is megjeleníthető.

ldapmodrdn

Az LDAP (modify-entry) bejegyzésmódosító RDN parancssori segédprogram.

Összegezés

```
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_szakasz]
[-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 felület az ldap_rename alkalmazás programozási felülethez (API).

| Az **ldapmodrdn** megnyit egy kapcsolatot egy LDAP szerver felé, kapcsolódik hozzá, illetve bejegyzéseket helyez
| vagy nevez át. A bejegyzések információit a program a szabványos bemenetről olvassa, az **- f** kapcsoló megadása
| esetén egy fájlból, vagy a parancssori dn és rdn párból. Ha a -s kapcsolót használja bejegyzések áthelyezéséhez, akkor a
| -s kapcsoló a parancs által érintett összes bejegyzésre vonatkozik.

Az **ldapmodrdn** parancs szintaxisának megjelenítéséhez írja be az alábbi parancsot:

```
ldapmodrdn -?
```

Kapcsolók

-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 **ldapmodrdn** 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 karakterlánccal 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. A paraméter elhagyható. 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* 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 fájllal 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 kapcsoló (általában a kapcsolati DN) használható. Lehet egy DN, illetve 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) paramétert.

-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 az ***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** 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 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.

-r Régi RDN értékek törlése a bejegyzésből. Alapértelmezés: a régi értékek megtartása.

-R Azt határozza meg, hogy az utalásokat nem kell automatikusan követni.

-s newSuperior
Megadja az új superior bejegyzés megkülönböztetett nevét, amellyel az átnevezett bejegyzés áthelyezésre kerül. Az newSuperior argumentum lehet nulla hosszúságú karaktersorozat (-s ″″).

Megjegyzés: Az új superior lehetőség V6R1 (ITDS v6.0) változatnál korábbi kiadású szerverhez való csatlakozás esetén nem támogatott. A lehetőség csak levél bejegyzés esetén megengedett.

–U *felhasználónév*
Adja meg a felhasználónevet. Az -m DIGEST-MD5 használata esetén szükséges, minden más mechanizmusnál figyelmen kívül marad.

-v Bővebb diagnosztikai információt nyújt, amelyet a szabványos kimenetre ír.

-V *változat*
Megadja, hogy az **ldapmodrdn** 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 **ldapmodrdn** 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 *újrdn* parancssori argumentum meg van adva, akkor az *újrdn* paraméter felváltja a bejegyzés *dn* paraméter által meghatározott RDN-jét. Máskülönben 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:

```
ldapmodrdn -r -i /tmp/entrymods
```

a Modify Me bejegyzés RDN-jét Modify Me-ről The New Me értékre változtatja, a Modify Me régi DN pedig törlésre kerül.

Megjegyzések

Ha nem ad meg bejegyzés információkat fájlban az **-i** kapcsoló használatával (vagy a *dn* és *rdn* parancssori paraméterpárral), akkor az **ldapmodrdn** 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.

Kapcsolódó fogalmak

Directory Server alkalmazás programozási felületek

“Megkülönböztetett nevek (DN)” oldalszám: 9
A címtár minden bejegyzésének vagy egy megkülönböztetett neve (DN). A DN az a név, amelyik egyedi módon azonosítja a címtárbejegyzést. A DN első elemét szokás relatív megkülönböztetett névként (Relative Distinguished Name, RDN) emlegetni.

ldapsearch

Az LDAP keresés parancssori segédprogram.

Összegezés

```
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 alkalmazás programozási felülethez (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 értékeit 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 -?.

Kapcsolók

-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** kapcsolót, 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 karakterlánccal 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. A paraméter elhagyható. 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 %s 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 kapcsoló (általában a kapcsolati DN) használható. Lehet egy DN, illetve 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) paramétert.

-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 az *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** 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 vezetéknév (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>[:<megfelelési szabályazonosító>]
```

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 kliens könyvtár 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 kérésben. 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 *másodperc*
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 mechanizmusnál 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:

```
<szűrő> ::='('<szűrőkomp>')'
<szűrőkomp> ::= <and>|<or>|<not>|<egyszerű>
<and> ::= '&' <szűrőlista>
<or> ::= '|' <szűrőlista>
<not> ::= '!' <szűrő>
<szűrőlista> ::= <szűrő>|<szűrő><szűrőlista>
<egyszerű> ::= <attribútumtípus><szűrőtípus>
<atribútumérték>
<szűrőtípus> ::= '='|'~='|'<='|'>='
```

A '~=' szerkezettel közelítő egyezés adható meg. Az <*attribútumtípus*> és <*attribútumérték*> leírását az RFC 2252, 'LDAP V3 attribútum szintaxis meghatározások' tartalmazza. Ezen felül, ha a szűrőtípus '=', akkor az <*attribútumérték*> lehet egyetlen * karakter az attribútum meglétének ellenőrzéséhez, illetve állhat szövegből és csillag (*) karakterekből vegyesen részkarakterlánc-egyezés vizsgálata érdekében.

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 fájlokba 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: UFl

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 hostname –o sn –b "o=ibm,c=us" "title=engineer"
```

visszaadja az összes olyan bejegyzését egy IBM alkalmazotti címtárban, amelynek beosztása (title) ″engineer″, és az eredményeket vezetéknév 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 címtárban, amelynek beosztása (title) ″engineer″, és az eredményeket vezetéknév szerint (csökkenő sorrendbe), majd általános név szerint (növekvő sorrendbe) rendezi sorba.

A következő parancs:

```
ldapsearch –h hostname –q 5 –T 3 –b o=ibm,c=us "title=engineer"
```

öt bejegyzést ad vissza oldalanként, az oldalak között 3 másodpercces késleltetéssel egy IBM alkalmazotti címtárból, amelynek beosztása (title) ″engineer″.

A következő példa olyan keresést illusztrál, amelyben utalási objektum is szerepel. A Directory Server LDAP címtárak utalási objektumokat is tartalmazhatnak, feltéve, hogy 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 hatásköreként 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 találhatók 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 a következő alatt keresi:

```
ou=Rochester, o=Big Company, c=US
```

Diagnosztika

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

Kapcsolódó fogalmak

Directory Server alkalmazás programozási felületek

"LDAP címtárutalások" oldalszám: 51
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.

Kapcsolódó hivatkozás

"LDAP adatcsere formátum (LDIF)" oldalszám: 248
Az LDAP adatcsere formátum az LDAP objektumok és frissítések (hozzáadás, módosítás, törlés, DN módosítás) szöveges ábrázolásához. Az LDIF rekordokat tartalmazó fájlok segítségével adatok vihetők át a címtárszerverek között, vagy az LDAP eszközök - mint például az **ldapadd** és **ldapmodify** - bemenetként használhatják.

Kapcsolódó tájékoztatás

RFC 2252, LDAP attribútumszintaxis-definíciók

RFC 2254, LDAP keresési szűrők megjelenítése karaktersorozat alakban

ldapchangepwd

Az LDAP jelszómódosító parancssori segédprogram.

Összegezés

```
ldapchangepwd -D binddn -w passwd | ? -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.

Kapcsolók

-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 kapcsolót, ha a bemeneti karakterlánc kódlapja eltér a job kódlapértékétől. 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. A paraméter elhagyható. 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, illetve egy u: vagy dn: jellel kezdődő authzId karaktersorozat.

-M Az utalási objektumok normál bejegyzésként kezelése.

-n *újjelszó* **| ?**
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 az ***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** 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 *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 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 **ldapmodrdn** 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.

-? Megjeleníti az ldapchangepwd parancs szintaxis-súgóját.

Példák

A következő parancs:

```
ldapchangepwd -D cn=John Doe -w a1b2c3d4 -n wxyz9876
```

megváltoztatja a ″John Doe″ commonName attribútumú bejegyzés jelszavát 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.

Kapcsolódó fogalmak

Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek
A Directory Server alkalmazás programozási felületekkel kapcsolatosan további információkat az Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek témakör tartalmaz.

ldapdiff

Az LDAP replikaszinkronizálási parancssori segédprogram.

Megjegyzés: Ez a parancs meglehetősen hosszú ideig is futhat, a replikált bejegyzések (és azok attribútumainak) számától függően.

Összegezés

(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 kulcstároló_jelszó]  [-cZ] [-F] [-L fájlnév] [-sD dn] [-sK kulcstároló]
 [-sw jelszó] -[sN kulcsazonosító] [-sp port] [-sP kulcstároló_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 fájlnév] [-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 -?
```

Kapcsolók

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 paraméterek

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 *keyStore*
Megadja a **kdb** alapértelmezett kiterjesztésű SSL kulcsadatbázis-fájl nevét. Ha ez a paraméter nincs megadva, vagy az értéke üres karaktersorozat (-sK″″), akkor a program a rendszer kulcstárolóját használja. Ha a kulcsadatbázis-fájl nem az aktuális könyvtárban található, megadja az adatbázisfájl teljes nevét.

-sN *keyLabel*
A kulcsadatbázis-fájlban található kliensigazoláshoz 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 *keyStorePwd*
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 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 ***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 *keyStore*
Megadja a kdb alapértelmezett kiterjesztésű SSL kulcsadatbázis-fájl nevét. Ha a paraméter értéke üres karaktersorozat (-sK″″), akkor a program a rendszer kulcstárolóját használja. Ha a kulcsadatbázis-fájl nem az aktuális könyvtárban található, megadja az adatbázisfájl teljes nevét.

-cN *keyLabel*
A kulcsadatbázis-fájlban található kliensigazoláshoz 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 igazoláskezelő (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 *keyStorePwd*
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 jelszóként. 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 <ellátó_hosztneve> -ch <fogyasztó_hosztneve> [paraméterek]
```

vagy

```
ldapdiff -S  -sh <ellátó_hosztneve> -ch
<fogyasztóhosztnév>> [ paraméterek]
```

Diagnosztika

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

Kapcsolódó feladatok

“Replikációs sorok kezelése” oldalszám: 163
Az alábbi információk segítséget nyújtanak a szerver által használt replikációs megállapodások (sorok) állapotának megfigyelése során.

Kapcsolódó hivatkozás

“Replikáció áttekintés” oldalszám: 38
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 SSL védelem LDAP parancssori segédprogramok használata

Az alábbi információk segítséget nyújtanak az SSL és LDAP parancssori segédprogramokok együttes használatának megértésében.

A “Védett socket réteg (SSL) és Fordítási réteg biztonság (TLS) használata LDAP Directory Serverrel” oldalszám: 53 rész az SSL és a Directory Server LDAP szerver együttes használatát mutatja be. 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.

Kapcsolódó fogalmak

“Védett socket réteg (SSL) és Fordítási réteg biztonság (TLS) használata LDAP Directory Serverrel” oldalszám: 53
A Directory Server kapcsolatainak biztonságosabbá tételéhez a Directory Server alkalmazhatja az SSL (Secure Sockets Layer, védett socket réteg) és a Transport Layer Security (TLS) biztonsági eljárást.

LDAP adatcsere formátum (LDIF)

Az LDAP adatcsere formátum az LDAP objektumok és frissítések (hozzáadás, módosítás, törlés, DN módosítás) szöveges ábrázolásához. Az LDIF rekordokat tartalmazó fájlok segítségével adatok vihetők át a címtárszerverek között, vagy az LDAP eszközök - mint például az **ldapadd** és **ldapmodify** - bemenetként használhatják.

Az LDIF tartalomrekordok az LDAP címtártartalmat ábrázolják és tartalmaz egy sort, amely az objektumot azonosítja, és amelyet az objektum attribútum-érték párokat tartalmazó sorok követnek. Ezt a típusú fájlt az **ldapadd** Qshell segédprogram, a System i navigátor címtár importáló és exportáló eszköze, valamint a CPYFRMLDIF (LDIF2DB) és CPYTOLDIF (DB2LDIF) CL parancs használja.

Megjegyzés: A DB2LDIF parancsot ajánlatos egy önálló jobban futtatni.

Az LDIF változásrekordok címtárfrissítéseket ábrázolnak. Ezek a rekordok tartalmazzák a címtárobjektumot azonosító sort, amelyet az objektum változásait leíró sorok követik. A változások az objektumok hozzáadását, törlését, átnevezését és áthelyezését, valamint a meglévő objektumok módosítását foglalják magukban.

Ezen rekordok mindegyikéhez kétféle bemeneti stílus áll rendelkezésre: Az RFC 2849 (The LDAP Data Interchange Format (LDIF) - Technical Specification) által megadott szabványos LDIF stílus; és egy régebbi nem szabványos módosítási stílus. A szabványos LDIF stílus használata javasolt. Az itt dokumentált régebbi stílus olyan régebbi eszközökkel való használatra javasolt, amely ezt a stílust használják vagy állítják elő.

Bemeneti stílusok

Az **ldapmodify** és **ldapadd** Qshell segédprogramok kétféle bemenetet fogadnak el. A bemenet típusát az **ldapmodify** vagy **ldapadd** számára biztosított első bemeneti sor formátuma határozza meg.

Az ldapmodify vagy ldapadd parancs első bemeneti sorának meg kell jelölnie a hozzáadni vagy módosítani kívánt címtár bejegyzés megkülönböztetett nevét. A bemeneti sor formátuma a következő:

```
dn: megkülönböztetett_név
```

vagy

```
megkülönböztetett_név
```

ahol a dn: literál karaktersorozat, a megkülönböztetett_név a módosítandó (vagy hozzáadandó) címtárbejegyzés megkülönböztetett név. Ha a dn: megtalálható, akkor a bemeneti stílus RFC 2849 LDIF stílus lesz. Ha ez nem található, akkor a bemeneti stílus módosítási stílus lesz.

Megjegyzés:

1. Az **ldapadd** parancs az **ldapmodify -a** paranccsal egyenértékű.
2. Az **ldapmodify** és **ldapadd** segédprogram nem támogatja a base64 kódolt megkülönböztetett neveket.

Kapcsolódó hivatkozás

“ldapmodify és ldapadd” oldalszám: 216
Az LDAP modify-entry (bejegyzésmódosító) és LDAP add-entry (bejegyzés-felvevő) parancssori segédprogram.

“ldapsearch” oldalszám: 234
Az LDAP keresés parancssori segédprogram.

RFC 2849 LDIF bemenet

Az RFC 2849: Az LDAP adatcsere formátum (LDIF) által meghatározott szabványos LDIF stílus használata ajánlott. Az LDIF fájlok elhagyható version és charset direktívákkal kezdődhetnek: version: 1, illetve charset: ISO-8859-1.

A charset direktíva akkor hasznos, ha olyan, egyéb platformokon futó fájlrendszereket használ, amelyek a fájlok CCSID címkézését nem támogatják. i5/OS alatt a szabványos viselkedés értelmében az LDIF fájlok UTF-8 (CCSID 1208) kódolásban kerülnek megnyitásra, majd a rendszer a fájlrendszernek lehetővé teszi az adatok fájl CCSID azonosítójáról aUTF-8 kódolásra történő átalakítását. Ennek megfelelően a charset direktíva használata általában nem szükséges.

Az elhagyható version és charset sor után több change record található, az alábbiakban leírt módon.

Az RFC 2849 LDIF bemenet használata esetében az attribútumtípusokat és az értékeket egymástól egy (:) vagy kettő kettőspont (::) választja el. Továbbá az egyedi attribútumértékeket érintő módosítások egymástól egy changetype: bemeneti sor felhasználásával kerülnek elválasztásra. Az RFC 2849 LDIF esetében a bemeneti sorok általános formátuma:

```
change_record
<üres sor>
change_record
<üres sor>
.
.
.
```

Az RFC 2849 LDIF stílusú bemeneti fájl néhány, egymástól üres sorral elválasztott change_record sorkészletből áll. Az egyes change_record blokkok formátuma:

```
dn: <DN>
[changetype: {modify|add|modrdn|moddn|delete}]
change_clause
change_clause
.
.
.
```

Ennek megfelelően egy change_record a módosítani kívánt címtárbejegyzés megkülönböztetett nevéből, a címtárbejegyzésen elvégezni kívánt módosítás típusát jelző (nem kötelező) sorból, illetve néhány change_clause sorból áll. Ha a changetype: sort kihagyja, akkor a rendszer feltételezi, hogy a módosítás típusa modify, hacsak a parancsot nem ldapmodify -a vagy ldapadd formában hívta meg, ekkor ugyanis a changetype feltételezett értéke add.

Ha a módosítás típusa modify, akkor az egyes change_clause az alábbi formátumú sorok készleteként kerül meghatározásra:

```
add: {attrtype}
{attrtype}{sep}{value}
.
.
.
-
```

vagy

```
replace: {attrtype}
{attrtype}{sep}{value}
.
.
.
-
```

vagy

```
delete: {attrtype}
[{attrtype}{sep}{value}]
.
.
.
-
```

vagy

```
{attrtype}{sep}{value}
.
.
.
```

A replace megadása esetén az attribútum összes létező értéke felülírásra kerül a megadott attribútumkészlettel. Az add megadása esetén a meglévő attribútumértékek kiegészítésre kerülnek. Ha a delete mellé attribútum-érték pár rekordot

nem ad meg, akkor a megadott attribútum valamennyi értéke eltávolításra kerül. Ha a delete után legalább egy attribútum-érték pár rekordot megad, akkor csak az attribútum-érték pár rekordban megadott értékek kerülnek eltávolításra.

Az add: *attrtype*, replace: *attrtype*, illetve delete: *attrtype* sorok (módosításjelzők) megadása esetén a rendszer egy kötőjelet (-) tartalmazó sort vár az adott *attrtype* módosítások végének jelzésére. Az attribútum-érték párokat a rendszer a módosítás jelző és a kötőjelet tartalmazó sor között várja. Ha a changetype sort kihagyja, akkor a changetype feltételezett értéke ldapadd esetén add, ldapmodify esetén pedig replace.

Az attribútumérték megadható szöveges karaktersorozatként, base-64 kódolt értékként, illetve fájl URL címként, a használt elválasztó (*sep*) függvényében.

attrtype: érték
az egyedülálló kettőspont (:) meghatározza, hogy az érték az *érték* karaktersorozat.

attrtype:: base64karaktersorozat
a dupla kettőspont (: :) meghatározza, hogy a *base64karaktersorozat* egy több-byte-os karaktereket tartalmazó bináris érték vagy UTF-8 karaktersorozat base 64 kódolású karaktersorozat formátumú ábrázolása.

attrtype:< fájlURL
a kettőspont és a balra nyitott szögletes zárójel (:<) meghatározza, hogy az értéket a fájlURL fájlból kell beolvasni. Az alábbi fájl URL sor például meghatározza, hogy a jpegPhoto attribútum értéke a /tmp/photo.jpg fájlban található:

jpegphoto:< file:///tmp/photo.jpg

Az elválasztó és az attribútumérték közötti szóközszerű karakterek figyelmen kívül maradnak. Az attribútumértékek több sorban is megadhatók, ehhez a következő bemeneti sor elején adjon meg egy szóköz karaktert. Ha elválasztóként dupla kettőspontot használ, akkor a rendszer a bemenetet base64 formátumban várja. A formátum olyan kódolás, amelyben a bináris byte-ok hármasával, négy szövegkarakter használatával kerülnek ábrázolásra.

Több attribútumérték több {attrtype}{sep}{value} meghatározás segítségével adható meg.

Ha a módosítás típusa add, akkor az egyes change_clause az alábbi formátumú sorok készleteként kerül meghatározásra:

```
{attrtype}{sep}{value}
```

Hasonlóan a modify módosítás típusnál az elválasztó sep, és értéke lehet egyetlen kettőspont (:), dupla kettőspont (: :), illetve kettőspont és balra nyitott szögletes zárójel (:<). Az elválasztó és az attribútumérték közötti szóközszerű karakterek figyelmen kívül maradnak. Az attribútumértékek több sorban is megadhatók, ehhez a következő bemeneti sor elején adjon meg egy szóköz karaktert. Ha elválasztóként dupla kettőspontot használ, akkor a rendszer a bemenetet base64 formátumban várja.

Ha a módosítás típusa modrdn vagy moddn, akkor minden change_clause az alábbi formátumú sorok készleteként kerül meghatározásra:

```
newrdn: érték
deleteoldrdn:{0|1}
[newsuperior: newSuperiorDn]
```

Ezek a paraméterek a modify RDN (átnevezés) vagy modifyDN (áthelyezés) LDAP műveletek esetében adhatók meg. A newrdn beállítás értéke az az új RDN, amelyet az RDN módosítása művelet során fel kíván használni. Ha az attribútumot a régi RDN helyen kívánja elmenteni, akkor a deleteoldrdn beállításnak adjon 0 értéket. A régi RDN helyen található attribútumértékek eltávolításához adjon meg 1-et. A newsuperior beállítás értéke az új felettes (szülő) megkülönböztetett neve a bejegyzés áthelyezése során.

Ha a módosítás típusa delete, akkor change_clause nincs megadva.

LDIF stílus példák:

A témakör példát ad az **ldapmodify** parancs érvényes bemenetére RFC 2849 LDIF stílus alkalmazása esetén.

Új bejegyzés hozzáadása

A következő példa új bejegyzést ad a címtárhoz a cn=Tim Doe, ou=Részlege, o=Vállalata, c=US név felhasználásával, feltételezve, hogy az **ldapadd** vagy **ldapmodify -a** meghívásra került:

```
dn: cn=Tim Doe, ou=Részlege, o=Vállalata, c=US
changetype:add
cn: Tim Doe
sn: Doe
objectclass: organizationalperson
objectclass: person
objectclass: top
```

A következő példa új bejegyzést ad a címtárhoz a cn=Tim Doe, ou=Részlege, o=Vállalata, c=US név felhasználásával, feltételezve, hogy az **ldapadd** vagy **ldapmodify -a** meghívásra került. Ne feledje el, hogy a jpegphoto attribútum betöltésre került a /tmp/timdoe.jpg fájlból.

```
dn: cn=Tim Doe, ou=Részlege, o=Vállalata, c=US
changetype:add
cn: Tim Doe
sn: Doe
jpegphoto:< file:///tmp/timdoe.jpg
objectclass: inetorgperson
objectclass: organizationalperson
objectclass: person
objectclass: top
```

Attribútumtípusok hozzáadása

A következő példa két új attribútumtípust ad a meglévő bejegyzéshez. Ne feledje el, hogy a registeredaddress attribútumhoz két érték tartozik:

```
dn: cn=Tim Doe, ou=Részlege, o=Vállalata, c=US
changetype: modify
add:telephonenumber
telephonenumber: 888 555 1234
-
add: registeredaddress
registeredaddress: td@vállalata.com
registeredaddress: ttd@vállalata.com
```

Bejegyzés nevének módosítása

A következő példa megváltoztatja a meglévő bejegyzés nevét cn=Tim Tom Doe, ou=Részlege, o=Vállalata, c=US értékre. A régi cn=Tim Doe RDN megmarad a cn attribútum további attribútumértékeként. Az új cn=Tim Tom Doe RDN-t az LDAP szerver automatikusan hozzáadja a bejegyzés cn attribútumának értékeihez:

```
dn: cn=Tim Doe, ou=Részlege, o=Vállalata, c=US
changetype:modrdn
newrdn: cn=Tim Tom Doe
deleteoldrdn: 0
```

A következő példa áthelyezi a cn=Tim Doe bejegyzést az ou=Új részleg alá. Az RDN (cn=Tim Doe) változatlan marad.

```
dn: cn=Tim Doe, ou=Részlege, o=Vállalata, c=US
changetype:moddn
newrdn: cn=Tim Doe
deleteoldrdn: 0
newsuperior: ou=Új részleg, o=Vállalata, c=US
```

Attribútumértékek cseréje

A következő példa lecseréli a telephonenumber és registeredaddress attribútum attribútumértékét a megadott attribútumértékekre.

```
dn: cn=Tim Tom Doe, ou=Részlege, o=Vállalata, c=US
changetype: modify
replace: telephonenumber
telephonenumber: 888 555 4321
-
replace: registeredaddress
registeredaddress: tim@vállalata.com
registeredaddress: timtd@vállalata.com
```

Attribútumok törlése és hozzáadása

A következő példa törli a telephonenumber attribútumot, töröl egy registeredaddress attribútumértéket és felveszi a description attribútumot:

```
dn: cn=Tim Tom Doe, ou=Részlege, o=Vállalata, c=US
changetype: modify
add: description
description: Ez egy nagyon hosszú attribútumérték,
 amely folytatódik a második sorban.
 Ne feledkezzen el a folytatott sorok elején lévő
 szóközről annak jelzése érdekében, hogy
 a sor folytatott.
-
delete: telephonenumber
-
delete: registeredaddress
registeredaddress: tim@vállalata.com
```

Bejegyzés törlése

A következő példa törli a cn=Tim Tom Doe, ou=Részlege, o=Vállalata, c=US nevű címtárbejegyzést:

```
dn: cn=Tim Tom Doe, ou=Részlege, o=Vállalata, c=US
changetype:delete
```

LDIF módosítási stílus bemenet

Az **ldapmodify** vagy **ldapadd** parancs bemenetének régebbi nem szabványos módosítási stílusa nem olyan rugalmas, mint az RFC 2849 LDIF stílus. Azonban bizonyos esetekben egyszerűbb ezt használni, mint az LDIF stílust.

Módosítási stílus bemenet használata esetén az attribútumtípusokat és értékeket egyenlőségjel (=) határolja. A módosítási stílus bemeneti sorainak általános formátuma a következő:

```
change_record
<üres sor>
change_record
<üres sor>
.
.
.
```

A módosítási stílus bemeneti fájlja egy vagy több, egymástól üres sorral elválasztott *change_record* sorból áll. A *change_record* formátuma a következő:

```
megkülönböztetett_név
[+|-]{attrtype} = {value_line1[\
value_line2[\
...value_lineN]]}
.
.
.
```

Ennek megfelelően egy *change_record* a módosítani kívánt címtárbejegyzés megkülönböztetett nevéből, és legalább egy attribútummódosítási sorból áll. Minden attribútummódosítási sor egy elhagyható hozzáadás vagy törlés jelzőből (+ vagy -), egy attribútumtípusból és egy attribútumértékből áll. Ha a pluszjel (+) van megadva, akkor a módosítási típus értéke **hozzáadás**. Ha a kötőjel (-) van megadva, akkor a módosítási típus értéke törlés. Törlési módosítás esetén az egyenlőségjelet (=) és az *értéket* ki kell hagyni a teljes attribútum eltávolítása érdekében. Ha a hozzáadás vagy törlés jelző nincs megadva, akkor a módosítási típus hozzáadásra van állítva, hacsak a -r kapcsoló nem kerül alkalmazásra. Ebben az esetben a módosítási típus értéke helyettesítés. A kezdő és befejező üres helyek eltávolításra kerülnek az attribútumértékekből. Ha a kezdő üres helyek szükségesek az attribútumértékekhez, akkor a bemenet RFC 2849 LDIF stílusát kell használni. A sorok fordított törtvonallal (\) folytathatók (a sor utolsó karaktere a fordított törtvonal). Ha egy sor folytatott, akkor a fordított törtvonal eltávolításra kerül és az eredményül kapott sor hozzáfűzésre kerül közvetlenül a fordított törtvonalat megelőző karakter után. A bemeneti sor végén található új sor karakter nem képezi az attribútumérték részét.

Több attribútumérték került megadásra több az *attrtype=value* specifikációval.

Ha a támogatási bináris értékek a fájlokból (-b) paraméter van megadva, akkor a '/' jellel kezdődő *érték* jelzi a fájlnév értékét. A következő sor például jelzi, hogy a jpegphoto attribútum kiolvasásra kerül a /tmp/photo.jpg fájlból:

jpegphoto=/tmp/photo.jpg

Módosítási stílus példák:

A témakör példát mutat az **ldapmodify** parancs érvényes bemenetére módosítási stílus alkalmazásával.

Új bejegyzés hozzáadása

A következő példa hozzáad egy új bejegyzést a címtárhoz cn=Tim Doe, ou=Részlege, o=Vállalata, c=US néven:

```
cn=Tim Doe, ou=Részlege, o=Vállalata, c=US
cn=Tim Doe
sn=Doe
objectclass=organizationalperson
objectclass=person
objectclass=top
```

Új attribútumtípus hozzáadása

A következő példa két új attribútumtípust ad a meglévő bejegyzéshez. Ne feledje el, hogy a registeredaddress attribútumhoz két érték tartozik:

```
cn=Tim Doe, ou=Részlege, o=Vállalata, c=US
+telephonenumber=888 555 1234
+registeredaddress=td@vállalata.com
+registeredaddress=ttd@vállalata.com
```

Attribútumértékek cseréje

Feltételezve, hogy a parancsmeghívás a következő volt:

```
ldapmodify -r ...
```

A következő példa lecseréli a telephonenumber és registeredaddress attribútum attribútumértékét a megadott attribútumértékekre. Ha a **-r** parancssori paraméter meg van adva, akkor az attribútumértékek hozzáadásra kerülnek az attribútumértékek meglévő halmazához.

```
cn=Tim Doe, ou=Részlege, o=Vállalata, c=US
telephonenumber=888 555 4321
registeredaddress: tim@vállalata.com
registeredaddress: timtd@vállalata.com
```

Attribútumtípus törlése

A következő példa töröl egy registeredaddress attribútumértéket a meglévő bejegyzésből.

```
cn=Tim Doe, ou=Részlege, o=Vállalata, c=US
-registeredaddress=tim@vállalata.com
```

Attribútum hozzáadása

A következő példa felvesz egy description attribútumot. A description attribútumérték több sorba terjed ki:

```
cn=Tim Doe, ou=Részlege, o=Vállalata, c=US
+description=Ez egy nagyon hosszú attribútumérték, \
amely folytatódik a második sorban. \
Ne feledkezzen meg a sor végén lévő fordított törtvonalról \
annak jelzéséhez, hogy a \
sor folytatott.
```

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 találhatók. Az attribútumok az ldapmodify paranccsal módosíthatók.

Kapcsolódó fogalmak

“Sémaellenőrzés” oldalszám: 31
A szerver inicializálásakor a sémafájlokat beolvassa és ellenőrzi, hogy következetesek és helyesek-e.

Kapcsolódó hivatkozás

“ldapmodify és ldapadd” oldalszám: 216
Az LDAP modify-entry (bejegyzésmódosító) és LDAP add-entry (bejegyzés-felvevő) parancssori segédprogram.

Címtárinformációs fa

Az alábbi információk a Directory Server címtár-információs fa (DIT) leírását tartalmazzák.

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

Az alábbi információk az ibmslapd.conf fájl beállítása során használt Directory Server attribútumok leírását tartalmazzák.

- 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) atttribútum, amely az objektum nevét tartalmazza.

Szintaxis
Címtár karaktersorozat

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

Default
1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL modell

Szintaxis
Címtár karaktersorozat

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.

Default
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.

Default
TRUE

Szintaxis
Logikai

Maximális hossz
5

Érték Egyértékű

ibm-slapdACLCacheSize

Leírás Az ACL gyorsítótárban tárolt bejegyzések maximális száma.

Default
25000

Szintaxis
Egész

Maximális hossz
11

Érték Egyértékű

ibm-slapdAdminDN

Leírás A Directory Server adminisztrátori kapcsolódási DN-je.

Default
cn=root

Szintaxis
DN

Maximális hossz
Korlátlan

Érték Egyértékű

ibm-slapdAdminGroupEnabled

Leírás Megadja, hogy az adminisztrátori csoport jelenleg engedélyezve van-e. Ha az értéke TRUE, akkor a szerver engedélyezni fogja az adminisztrátori csoport tagjainak a bejelentkezést.

Default
FALSE

Szintaxis
Logikai

Maximális hossz
128

Érték Egyértékű

ibm-slapdAdminPW

Leírás A Directory Server adminisztrátori kapcsolódási jelszava.

Default
secret

Szintaxis
Bináris

Maximális hossz
128

Érték Egyértékű

ibm-slapdAllowAnon

Leírás Megadja, hogy engedélyezettek-e a névtelen kapcsolatok.

Default
True

Szintaxis
Logikai

Maximális hossz
128

Érték Egyértékű

ibm-slapdAllReapingThreshold

Leírás Megadja, hogy hány kapcsolatot kell fenntartai a szerveren, mielőtt a kapcsolatkezelés aktiválásra kerülne.

Default
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.

Default
0

Szintaxis
Directory string pontos egyezéssel

Maximális hossz
1024

Érték Egyértékű

ibm-slapdBoundReapingThreshold

Leírás Megadja, hogy hány kapcsolatot kell fenntartai a szerveren, mielőtt a névtelen és kötött kapcsolatok kezelése aktiválásra kerülne.

Default
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.

Default
/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.

Default
Nincs

Szintaxis
Címtár karaktersorozat

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.

Default
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 elkezdi beállítani az attribútum-gyorsítótárat.

```
Minimum = T000000
Maximum = T235959
```

Default

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
```

Default

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.

Default

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)
```

Default

0

Szintaxis

Egész

Maximális hossz
11

Érték Egyértékű

ibm-slapdCLIErrors

Leírás Fájl elérési út vagy eszköz az ibmslapd hosztgépen, amelybe a CLI hibaüzenetek kiíródnak.

Default
/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.

Default
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 értékeket 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).

Default
15

Szintaxis
Egész

Maximális hossz
50

Érték Egyértékű

ibm-slapdDbInstance

Leírás A célterület DB2 adatbázispéldányát adja meg.

Default
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.

Default
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.

Default
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 kliens kérésben megadott minden derefAliases elemtől. Az engedélyezett értékek: **soha**, **találat**, **keresés** és **mindig**.

Default
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.

Default
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 adminisztrátori csoporttag Digest MD5 felhasználónevét. Akkor kell, ha az adminisztrátor hitelesítésére MD5 Digest eljárást használnak.

Default
Nincs

Szintaxis
Címtár karaktersorozat

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.

Default
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.

Default
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 állítva a szerver LDAP_UNWILLING_TO_PERFORM kiterjesztett eredménnyel visszautasít minden eseményértesítés bejegyzésére vonatkozó klienskérést.

Default
TRUE

Szintaxis
Logikai

Maximális hossz
5

Érték Egyértékű

ibm-slapdEntryCacheSize

Leírás A bejegyzés gyorsítótárban tárolt bejegyzések maximális száma.

Default
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.

Default
/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

Default
50

Szintaxis
Egész

Maximális hossz
1024

Érték Egyértékű

ibm-slapdEThreadActivate

Leírás Megadja, hogy mely feltételek aktiválják a vészszálat Az alábbi értékek egyike kell, hogy legyen:

S Csak méret

T Csak idő

SOT Méret vagy idő

SAT Méret és idő

Default
SAT

Szintaxis
Karaktersorozat

Maximális hossz
1024

Érték Egyértékű

ibm-slapdEThreadEnable

Leírás Megadja, hogy aktív-e a vészszál

Default
True

Szintaxis
Logikai

Maximális hossz
1024

Érték Egyértékű

ibm-slapdETimeThreshold

Leírás Megadja, hogy hány percenként kerülnek eltávolításra elemek a feladatsorból, mielőtt a vészszál aktiválásra kerül.

Default
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.

Default
100

Szintaxis
Egész

Maximális hossz
11

Érték Egyértékű

ibm-slapdFilterCacheSize

Leírás A Keresési szűrő gyorsítótárban tárolt bejegyzések maximális számát adja meg.

Default
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.

Default
300

Szintaxis
Egész

Hossz 11

Számosság
Egyszeres

Használat
Címtárművelet

Felhasználó által módosítható
Igen

Hozzáférési osztály
Kritikus

Lemezterület
Nem

ibm-slapdIncludeSchema

Leírás Egy sémameghatározásokat tartalmazó fájl elérési útját adja meg a Directory Server szervergépen.

Default

- /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.

Default
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.

Default
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 Kerberosszal együtt.

Default
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).

Default
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.

Default
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.

Default
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.

Default
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.

Default
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)

Default
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.

Default
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.

Default
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.

Default
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
```

Default
nincs

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
```

Default
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
```

Default
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
```

Default
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
```

Default
5

Szintaxis
Egész

Maximális hossz
11

Érték Egyértékű

ibm-slapdMaxPendingChangesDisplayed

Leírás A megjelenítendő, függőben lévő módosítások maximális száma.

Default
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
```

Default
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 kliens kéréseket 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.

Default
FALSE

Szintaxis
Logikai

Hossz 5

Számosság
Egyszeres

Használat
directoryOperation

Felhasználó által módosítható
Igen

Hozzáférési osztály
kritikus

Objektumosztály
ibm-slapdRdbmBackend

Lemezterület
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.

Default
3

Szintaxis
Egész

Hossz 11

Számosság
Egyszeres

Használat
directoryOperation

Felhasználó által módosítható
Igen

Hozzáférési osztály
kritikus

Lemezterület
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.

Default
50

Szintaxis
Egész

Hossz 11

Számosság
Egyszeres

Használat
directoryOperation

Felhasználó által módosítható
Igen

Hozzáférési osztály
kritikus

Lemezterület
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:

```
kulcsszó
fájlnév
init_function [argumentumok...]
```

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.

Default
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.)

Default
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.

Default
nincs

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.

Default
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).

Default
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.

Default
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 legutoljára 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 fájl, 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 fájlokba íródnak.

Default
/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.

Default
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.)

Default
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.

Default
nincs

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.

Default
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.

Default
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.

Default
3

Szintaxis
cis

Hossz 11

Számosság
Egyszeres

Használat
directoryOperation

Felhasználó által módosítható
Igen

Hozzáférési osztály
kritikus

Objektumosztály
ibm-slapdRdbmBackend

Lemezterület
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 kliensкéréseket 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.

Default
FALSE

Szintaxis
Logikai

Hossz 5

Számosság
Egyszeres

Használat
directoryOperation

Felhasználó által módosítható
Igen

Hozzáférési osztály
kritikus

Objektumosztály
ibm-slapdRdbmBackend

Lemezterület
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.

Default
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.

Default
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:

6. 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.

Default
/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.

Default
nincs

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.

Default
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.

Default
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 szervert.

Default

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)

Default
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.

Default
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.

Default
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.

Default
FALSE

Szintaxis
Logikai

Maximális hossz
5

Érték Egyértékű

ibm-slapdVersion

Leírás Az IBM Slapd verziószáma.

Default

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.

Default
120

Szintaxis
Egész

Maximális hossz
1024

Érték Egyértékű

objectClass

Leírás Az objectClass (objektumosztály) attribútum értéke adja meg, hogy a bejegyzés milyen típusú objektum.

Szintaxis
Címtár karaktersorozat

Maximális hossz
128

Érték Többértékű

Objektumazonosítók (OID)

Az alábbi információk a Directory Server termékben használt objektumazonosítók (OID) leírását tartalmazzák.

A Directory Server az alábbi táblázatokban látható objektumazonosítókat használja. Ezek az OID-k a root DSE-ben találhatók. A root DSE bejegyzés információkat tartalmaz magáról a szerverről. Ismerje meg a kiterjesztett műveletek és vezérlőelemek objektumazonosítóit (OID), beleértve az alábbi vezérlőelemekhez és kiterjesztett műveletekhez tartozó kérés- és válaszadatok kódolását, a Tivoli szoftver információs központban.

Vezérlőelemek

7. táblázat: Támogatott Directory Server vezérlőelemek

Név	OID	Legkorábbi i5/OS vagy OS/400 kiadás	Legkorábbi IBM Tivoli Directory Server változat	Leírás
DSA IT kezelése	2.16.840.1.1137.30.3.4.2	V4R5	V3.2	A hivatkozott bejegyzések normál bejegyzésekként kezelése.
“Tranzakciók” oldalszám: 51	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 részleteket az “Operációs rendszer leképzett háttérobjektumok” oldalszám: 85 témakör tartalmaz.
os400-dltusrprf-pgpopt	1.3.18.0.2.10.9	V5R2		Felhasználói profil beállítások törlése az elsődleges csoportból. További részleteket az “Operációs rendszer leképzett háttérobjektumok” oldalszám: 85 témakör tartalmaz.
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. Lásd: “Keresési paraméterek” oldalszám: 48.
Oldalakra bontott keresés	1.2.840.113556.1.4.319	V5R2 PTF-fel	V4.1	A keresési eredmények oldalakra bontva visszaadása (nem egyben). Lásd: “Keresési paraméterek” oldalszám: 48.
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.

7. táblázat: Támogatott Directory Server vezérlőelemek (Folytatás)

Név	OID	Legkorábbi i5/OS vagy OS/400 kiadás	Legkorábbi IBM Tivoli Directory Server változat	Leírás
"Jelszó-irányelv" oldalszám: 78	1.3.6.1.4.1.42.2.27.8.5.1	V5R3	V5.1	Extra jelszó irányelv információk visszaadása a kliens számára.
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 felhatalmazás" oldalszám: 64	2.16.840.1.113730.3.4.18	V5R4	V5.2	A kliensalkalmazás 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.
Bejegyzés frissítése vezérlőelem	1.3.18.0.2.10.24	V6R1	V6.0	A szerver belső használatára fenntartott vezérlőelem, amely a replikációs ütközések feloldásának támogatására szolgál.
Replikációs ütközések feloldása nélkül	1.3.19.0.2.10.27	V6R1	V6.0	A szerver belső használatára fenntartott vezérlőelem, amely a replikációs ütközések feloldásának támogatására szolgál.
Replikáció nélkül vezérlőelem	1.3.19.0.2.10.23	V6R1	V6.0	A vezérlőelem megadásával az adminisztrátor kérheti, hogy a társított művelet más szerverekre ne kerüljön replikálásra. A vezérlőelem vezérlő értékkel nem rendelkezik.

7. táblázat: Támogatott Directory Server vezérlőelemek (Folytatás)

Név	OID	Legkorábbi i5/OS vagy OS/400 kiadás	Legkorábbi IBM Tivoli Directory Server változat	Leírás
Megfigyelés vezérlés	1.3.18.0.2.10.22	V6R1	V6.0	A vezérlőelemet a jogosult kliensek (például proxy szerverek) használják az olyan kéréseket kezdeményező kliensek azonosítására, amelyek esetleg több szerveren keresztül kerülhet továbbításra.
Csoportjogosultság vezérlőelem	1.3.18.0.2.10.21	V6R1	V6.0	A vezérlőelem segítségével a helyi szerver csoporttagság helyett a kliens hitelesítési azonosságának csoporttagsága érvényesíthető. A vezérlőelem a proxy hitelesítés vezérlőelemmel együttesen kerül felhasználásra.
Csoportok csak módosítása vezérlőelem	1.3.18.0.2.10.25	V6R1	V6.0	A vezérlőelemmel rendelkező műveleteket (delete vagy modrdn/dn) a háttérszerverek olyan különleges műveletként ismerik fel, amely során a dn nem törlésre vagy átnevezésre kerül, hanem ehelyett a dn-t tartalmazó csoportok úgy módosulnak, hogy a cél dn-re mutató hivatkozást tagjaik között törlik vagy átnevezik.
Csoport kihagyása hivatkozásintegritási vezérlőelem	1.3.18.0.2.10.26	V6R1	V6.0	A csoport hivatkozásintegritási feldolgozásának kihagyása delete vagy modrdn kérés esetében. A változtatás az ACI és csoporttagságokban nem jelenik meg.

7. táblázat: Támogatott Directory Server vezérlőelemek (Folytatás)

Név	OID	Legkorábbi i5/OS vagy OS/400 kiadás	Legkorábbi IBM Tivoli Directory Server változat	Leírás
AES csatlakozás vezérlőelem	1.3.18.0.2.10.28	V6R1	V6.0	A vezérlőelem lehetővé teszi, hogy az IBM Tivoli Directory Server a fogyasztó szerver felé a frissítéseket egy korábban AES felhasználásával kódolt jelszóval továbbítsa.

Kiterjesztett műveletek

8. táblázat: Objektumazonosítók kiterjesztett műveletekhez

Név	OID	Legkorábbi i5/OS vagy OS/400 kiadás	Legkorábbi IBM Tivoli Directory Server változat	Leírás
Események regisztrálása	1.3.18.0.2.12.1	V4R5	V3.2	Tivoli Directory Server eseménytámogatás eseményregisztrációs kérés
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	Tranzakciós kontextus indítása
Tranzakció befejezése	1.3.18.0.2.12.6	V4R5	V3.2	Tranzakciós kontextus befejezése (véglegesítés/visszagörgetés)
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:

9. táblázat: További kiterjesztett műveletek

Név	OID	Legkorábbi i5/OS kiadás	Legkorábbi IBM Tivoli Directory Server változat	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 ibm-replicagroup=default 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 részfát egy olyan állapotba hozza, amelyben nem fogad további klienskéréseket (illetve megszünteti ezt az állapotot); pontosabban csak olyan kéréseket, amelyek a címtáradminisztrátorként bejelentkezett klienstől 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 ibm-replicagroup=default 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 ibm-replicagroup=default 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. A hívónak a címtár-adminisztrátornak kell lennie.

9. táblázat: További kiterjesztett műveletek (Folytatás)

Név	OID	Legkorábbi i5/OS kiadás	Legkorábbi IBM Tivoli Directory Server változat	Leírás
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: “ldapexop” oldalszám: 223 -op uniqueattr. A hívónak a címtár-adminisztrátornak kell lennie.
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: 223 -op getattributes
Felhasználótípus-kérés	1.3.18.0.2.12.37	V5R3	V5.2	Kérés a kapcsolat felhasználó felhasználótípusának bekérésére
Replikációs hibanapló kiterjesztett művelet	1.3.18.0.2.12.56	V6R1	V6.0	Az IBM replikációs hibavezérlő kiterjesztett kérés segítségével megjeleníthető a hibanapló, a naplóból bejegyzések újrapróbálhatók, illetve a naplóbejegyzések törölhetők. A hívónak címtár-adminisztrátornak kell lennie, vagy a társított replikációs kontextus ibm-replicagroup=default objektumára vonatkozóan írási jogosultsággal kell rendelkeznie.
Csoport kiértékelés kiterjesztett művelet	1.3.18.0.2.12.50	V6R1	V6.0	Lekéri az összes olyan csoportot, amelyhez a felhasználó tartozik. A hívónak a címtár-adminisztrátornak kell lennie.
Replikációs topológia kiterjesztett művelet	1.3.18.0.2.12.54	V6R1	V6.0	Egy adott replikációs környezetben található replikációs topológiával kapcsolatos bejegyzések replikációjának aktiválása. A hívónak címtár-adminisztrátornak kell lennie vagy a társított replikációs kontextus ibm-replicagroup=default objektumára vonatkozóan írási jogosultsággal kell rendelkeznie.
Fiókállapot kiterjesztett művelet	1.3.18.0.2.12.58	V6R1	V6.0	A kiterjesztett művelet a szervernek továbbítja egy userPassword attribútumot tartalmazó bejegyzés megkülönböztetett nevét, majd a szerver visszaküldi a lekérdezett felhasználói fiók állapotát (nyitott, zárolt vagy lejárt). A hívónak a címtár-adminisztrátornak kell lennie.

9. táblázat: További kiterjesztett műveletek (Folytatás)

Név	OID	Legkorábbi i5/OS kiadás	Legkorábbi IBM Tivoli Directory Server változat	Leírás
Fájl megszerzése kiterjesztett művelet	1.3.18.0.2.12.73	V6R1	V6.0	A szerveren található fájl tartalmának visszaadása. A hívónak a címtár-adminisztrátornak kell lennie. A kiterjesztett művelet a LostAndFound naplót, illetve a Tivoli Directory Server megfigyelési naplót egyaránt támogatja. A megfigyelési napló nem a címtárszerver i5/OS biztonsági megfigyelési képességeivel kapcsolatos.
Sorok megszerzése kiterjesztett művelet	1.3.18.0.2.12.22	V6R1	V6.0	Naplófájl sorainak lekérésére irányuló kérés. A hívónak a címtár-adminisztrátornak kell lennie. A kiterjesztett művelet a LostAndFound naplót, illetve a Tivoli Directory Server megfigyelési naplót egyaránt támogatja. A megfigyelési napló nem a címtárszerver i5/OS biztonsági megfigyelési képességeivel kapcsolatos.
Sorok számának megszerzése kiterjesztett művelet	1.3.18.0.2.12.24	V6R1	V6.0	Egy naplófájlban található sorok számának lekérése. A hívónak a címtár-adminisztrátornak kell lennie. A kiterjesztett művelet a LostAndFound naplót, illetve a Tivoli Directory Server megfigyelési naplót egyaránt támogatja. A megfigyelési napló nem a címtárszerver i5/OS biztonsági megfigyelési képességeivel kapcsolatos.

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.

10. 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.

10. táblázat: A támogatott és engedélyezett funkciók objektumazonosítója (Folytatás)

Név	OID	Leírás
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.
Szolgáltatásbénításos támadások kivédése	1.3.18.0.2.32.9	A szerver támogatja a szolgáltatásbénításos támadások ellen védő funkciót, beleértve az írás/olvasási időkorlátokat és a vészszálak használatát.
Bejegyzések és részfák dinamikus frissítése	1.3.18.0.2.32.15	A szerver támogatja a bejegyzések és részfák dinamikus konfigurációs frissítését.
Álnévhivatkozás-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.
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, lekérdezhetők 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.
Képrnyő 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).
Képenyő 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).
Képenyő 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.

10. táblázat: A támogatott és engedélyezett funkciók objektumazonosítója (Folytatás)

Név	OID	Leírás
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.
IBMpolicies replikációs részfa	1.3.18.0.2.32.18	A szerver támoatja a cn=IBMpolicies 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
Szűrt utalások szerver képesség	1.3.18.0.2.32.36	Azt jelöli, hogy a kiterjesztett szűrt utalások támogatottak. Más szóval az utalások szűrt értéke a keresési kérések esetében egyesítésre kerül az eredeti szűrővel.
Globális adminisztrátori csoport szerver képesség	1.3.18.0.2.32.38	Azt jelöli, hogy a globális adminisztrátori csoport használata támogatott.
Összehasonlító képesség felülvizsgálata	1.3.18.0.2.32.40	Azt jelöli, hogy az összehasonlító művelet felülvizsgálata támogatott.
AES jelszótitkosítás	1.3.18.0.2.32.39	Azt jelöli, hogy az AES jelszótitkosítás támogatott.
Maximális bejegyzésméret	1.3.18.0.2.32.51	A replikációs ütközések feloldása során kerül felhasználásra. A szám alapján az ellátó eldöntheti, hogy a bejegyzést a replikációs ütközés feloldásához a cél szerverhez ismételten hozzá kell-e adni.
LostAndFound naplófájl	1.3.18.0.2.32.52	Olyan fájl, amely a replikációs ütközés feloldásának eredményeként felülírt bejegyzéseket archiválja.
Naplókezelés	1.3.18.0.2.32.41	Azt jelöli, hogy a naplófájl-hozzáférés kiterjesztett műveletek, illetve a Tivoli Directory Server megfigyelési napló támogatott.
Több szálon futó replikáció	1.3.18.0.2.32.42	
Replikáció során használt ellátók szerverkonfigurációja	1.3.18.0.2.32.43	
IBMPolicies replikációs részfa	1.3.18.0.2.32.18	A cn=ibmpolicies részfa segítségével támogatja a cn=ibmpolicies és cn=schema replikációjának konfigurálását.

ACL mechanizmusok objektumazonosítói

A következő táblában az ACL mechanizmusok objektumazonosítói láthatók.

11. 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

Kapcsolódó fogalmak

“Vezérlőelemek és kiterjesztett műveletek” oldalszám: 94
A vezérlőelemek és kiterjesztett műveletek segítségével az LDAP protokoll a protokoll módosítása nélkül kiterjeszthető.

IBM Tivoli Directory Server megfelelőség

A Directory Server kompatibilis az egyéb platformokon rendelkezésre álló IBM Tivoli Directory Server termékekkel. Az alábbi táblázat az IBM Tivoli Directory Server termék i5/OS Directory Server adott változatának megfelelő változatát tartalmazza. A táblázat különösen annak megállapítása során lehet hasznos, hogy az i5/OS Directory Server teljesíti-e egy adott termék címtárszerverre vonatkozó előfeltételeit.

12. táblázat: IBM Tivoli Directory Server megfelelőség

i5/OS Directory Server	IBM Tivoli Directory Server
V6R1	IBM Tivoli Directory Server 6.0
V5R4	IBM Tivoli Directory Server 5.2
V5R3	IBM Directory Server 5.1
V5R2 (PTF SI08487)	IBM Directory Server 4.1
V5R2 (GA)	IBM SecureWay Directory Server 3.2.2

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:

- Az adminisztrátorok 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.

Kapcsolódó feladatok

“Directory Server beállítása” oldalszám: 102
A Directory Server beállításainak személyre szabásához futtassa a Directory Server konfigurációs varázslót.

Directory Server hibaelhárítása

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

Sajnos még az olyan megbízható szerverekkel is, 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 találhatók, amely a rendszer QSYSINC/H.LDAP könyvtárában helyezkedik el.

Az általános Directory Server problémákkal kapcsolatosan további információkat a Directory Server honlap (www.iseries.ibm.com/ldap) tartalmaz.

A Directory Server több olyan strukturált lekérdezési nyelvi (SQL) szervert használ, amelyek QSQSRVR 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 szerverjobokat indítja el a szerver, tudni, hogy mely QSQSRVR munkanaplókban kell keresni a további hibákat.

Amikor a Directory Server szabályosan indul el, az alábbihoz hasonló üzenetet generál.

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

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

Az üzenetek a szerver számára elindított QSQSRVR jobokra vonatkoznak. Az üzenetek száma eltérhet a szerver konfigurációjától és a szerver indításához szükséges QSQSRVR jobok számától.

A System i navigátor címtárszerverek **Adatbázis/utótagok** adatlapján a Directory Server által a szerver indítását követően a címtár műveletekre használt SQL szerverek összesített száma adható meg. A replikációhoz további SQL szerverek indulnak el.

Kapcsolódó tájékoztatás

Directory Server honlap

Hibafigyelés és hozzáférés-követés a Directory Server munkanaplója segítségével

Ha a Directory Server-en hiba fordul elő, és részletesebb tájékoztatást akar, egy másik lehetőség a QDIRSRV feladatnapló megtekintése.

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 a System i navigátorban, a Directory Server **Általános** lapján szabályozható.

QDIRSRV munkanapló megjelenítése, ha a szerver már elindult

Ha a szerver már elindult, az alábbi lépéseket követve tekintheti meg a QDIRSRV munkanaplót:

1. Az System i navigátorban bontsa ki a **Hálózat** részt.
2. Bontsa ki a **Szerverek** kategóriát.
3. Kattintson a **TCP/IP** lehetőségre.
4. Kattintson a jobb oldali egérgombbal a **IBM Directory Server** feliratra, majd válassza a **Szerver feladatok** menüpontot.
5. A **Fájl** menüben válassza ki a **Munkanapló** elemet.

QDIRSRV munkanapló megjelenítése, ha a szerver leállított

Ha a szerver még nem indult el, kövesse az alábbi lépéseket a QDIRSRV feladatnapló megtekintéséhez:

1. A System i navigátorban bontsa ki az **Alapműveletek** kategóriát.
2. Kattintson a **Nyomtatókimenet** elemre.
3. A QDIRSRV a **Felhasználó** oszlopban jelenik meg az System i navigátor jobboldali keretén belül. A munkanapló megtekintéséhez kattintson duplán a **Qpjoblog** elemre ugyanabban a sorban, a QDIRSRV-től balra.

   Megjegyzés: Lehetséges, hogy az System i 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: Bizonyos műveletek végrehajtása során a Directory Server egyéb rendszererőforrásokat használ. Ha ezen erőforrásokkal kapcsolatban fordul elő hiba, a munkanapló jelzi, hova lehet információért fordulni. Néhány esetben a Directory Server a hiba forrását nem képes meghatározni. Ilyenkor tekintse meg az SQL (Structured Query Language) szerver munkanaplóját, hátha a hiba az SQL szerverekkel kapcsolatos.

Hibakeresés TRCTCPAPP segítségével

Reprodukálható hibák esetén a Trace TCP/IP Application (TRCTCPAPP APP(*DIRSRV)) parancs segítségével futtathatja a hibák nyomkövetését.

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 nyomkövetés bejegyzéseinek segítségével azonban meghatározhatja, hogy két pont között valóban sor került-e adatcserére.

A Directory Server TCP/IP alkalmazás nyomon követése (TRCTCPAPP) parancsa segítségével megkeresheti a kliensekkel vagy az alkalmazásokkal kapcsolatos problémákat.

A TRCTCPAPP parancs segítségével az aktív szerver példányok nyomon követhetők. Például:

```
TRCTCPAPP APP(*DIRSRV) INSTANCE(QUSRDIR)
```

A nyomkövetés a STRTCPSVR parancs ’-h dft’ példányindítási értékének megadásával is elindítható. A parancs elindítja a szerverpéldány nyomkövetését, majd elindítja magát a szerverpéldányt. Például:

```
STRTCPSVR SERVER(*DIRSRV) INSTANCE(QUSRDIR ’-h dft’)
```

A nyomkövetés leállításához adja meg a következő parancsot:

TRCTCPAPP APP(*DIRSRV) SET(*OFF)

Kapcsolódó fogalmak

Kommunikációs nyomkövetés

Kapcsolódó tájékoztatás

TCP/IP alkalmazás nyomkövetése (TRCTCPAPP)

Hibák nyomkövetése az LDAP_OPT_DEBUG kapcsolóval

Az LDAP C API-kat használó kliensek problémáinak keresése.

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(  ld, 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 a parancssorba a következő parancsot:

```
DMPUSRTRC  ClientJobNumber
```

ahol ClientJobNumber a kliensjob száma.

Az információ interaktív megjelenítéséhez gépelje be a parancssorba a következő parancsot:

```
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. Gépelje be a parancssorba a következő parancsot.

   ```
   SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
   ```

   ahol QAP0ZDMP egy nullát tartalmaz és *xxx* az SAVF fájl megadott neve.

Kapcsolódó fogalmak

Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek
A Directory Server alkalmazás programozási felületekkel kapcsolatosan további információkat az Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek témakör tartalmaz.

Kapcsolódó tájékoztatás

Környezeti változó felvétele (ADDENVVAR)

Felhasználói nyomkövetés kiíratása (DMPUSRTRC)

Fizikai fájlmember megjelenítése (DSPPFM)

Mentési fájl létrehozása (CRTSAVF)

Objektum mentése (SAVOBJ)

GLEnnnn üzenetazonosítók

Az alábbi információk a GLE üzenetazonosítókat, illetve az üzenetazonosítók leírását tartalmazzák.

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 RANGE(GLE0050) MSGF(QGLDMSG)
```

Ez megadja az LDAP_INSUFFICIENT_ACCESS leírását.

tA 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 támoagott 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_SASLBIND_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)

Üzenetazonosító	Leírás
GLE0035	Az objektum levélobjektum (LDAP_IS_LEAF)
GLE0036	Álnévhivatkozás-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 címtárszerver túlterhelt (LDAP_BUSY)
GLE0052	Címtárszolgáltatási ügynök nem elérhető (LDAP_UNAVAILABLE)
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	Obejktumosztálysértés (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)

Üzenetazonosító	Leírás
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)
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 túlcsordulás (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)

Kapcsolódó tájékoztatás

Üzenetleírás megjelenítése (DSPMSGD)

Általános LDAP klienshibák

Az alábbi információk az általános LDAP kliens hibák leírását tartalmazzák.

Az általános LDAP kliens hibák ismerete segít a szerverrel kapcsolatos problémák megoldásában. Az LDAP kliens hibahelyzeteinek teljes leírását a Programozás témakör “Directory Server alkalmazás programozási felületek” szakasza tartalmazza.

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.

Kapcsolódó fogalmak

Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek
A Directory Server alkalmazás programozási felületekkel kapcsolatosan további információkat az Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek témakör tartalmaz.

ldap_search: Timelimit exceeded (Időhatár túllépés)

A hiba akkor következik be, ha a műveleteket az ldapsearch parancs lassan hajtja végre.

A hiba kiküszöbölésére az alábbi lépések közül egyet vagy mindkettőt végezze el:

- Növelje meg a Directory Server keresési idejét.
- Csökkentse a rendszer tevékenységét. Az éppen futó aktív LDAP kliensjobok számát is csökkentheti.

Kapcsolódó feladatok

“Keresési beállítások módosítása” oldalszám: 128
Az alábbi információk segítséget nyújtanak a felhasználó keresési képességeinek vezérlése során.

[Hibás LDAP művelet]: Műveleti hiba

Több körülmény is okozhatja ezt a hibát.

Egy adott példány esetében a hiba okával kapcsolatos információkat a QDIRSRV munkanapló, illetve a strukturált lekérdezési nyelv (SQL) szerver feladatnaplója tartalmaz.

Kapcsolódó fogalmak

“Directory Server hibaelhárítása” oldalszám: 304
Információk a problémák megoldásával kapcsolatban. Javaslatok szervizadatok begyűjtésére és bizonyos problémák megoldására.

Kapcsolódó feladatok

“Hibafigyelés és hozzáférés-követés a Directory Server munkanaplója segítségével” oldalszám: 304
Ha a Directory Server-en hiba fordul elő, és részletesebb tájékoztatást akar, egy másik lehetőség a QDIRSRV feladatnapló megtekintése.

ldap_bind: 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.

Kapcsolódó feladatok

“Hibafigyelés és hozzáférés-követés a Directory Server munkanaplója segítségével” oldalszám: 304
Ha a Directory Server-en hiba fordul elő, és részletesebb tájékoztatást akar, egy másik lehetőség a QDIRSRV feladatnapló megtekintése.

ldap_bind: Nem megfelelő hitelesítés

A szerver érvénytelen hitelesítési adatokat akkor ad vissza, ha 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 hibáról további részleteket a QDIRSRV feladatnaplóban talál.

Kapcsolódó feladatok

"Hibafigyelés és hozzáférés-követés a Directory Server munkanaplója segítségével" oldalszám: 304
Ha a Directory Server-en hiba fordul elő, és részletesebb tájékoztatást akar, egy másik lehetőség a QDIRSRV feladatnapló megtekintése.

[Hibás LDAP művelet]: Nem elegendő hozzáférés

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 hibáról további részleteket a QDIRSRV feladatnaplóban talál.

Kapcsolódó feladatok

"Hibafigyelés és hozzáférés-követés a Directory Server munkanaplója segítségével" oldalszám: 304
Ha a Directory Server-en hiba fordul elő, és részletesebb tájékoztatást akar, egy másik lehetőség a QDIRSRV feladatnapló megtekintése.

[Hibás LDAP művelet]: Nem lehet az LDAP szerverhez kapcsolódni

A hiba leggyakoribb oka például, hogy a kérés elküldésekor a szerver még nem üzemkész, illetve a megadott portszám érvénytelen.

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 hibáról további részleteket a QDIRSRV feladatnaplóban talál. Ha a Directory Server sikeresen elindult, akkor a QDIRSRV feladatnaplójában a Directory Server started successfully (A Directory Server sikeresen elindult) szövegű üzenet található.

Kapcsolódó feladatok

"Hibafigyelés és hozzáférés-követés a Directory Server munkanaplója segítségével" oldalszám: 304
Ha a Directory Server-en hiba fordul elő, és részletesebb tájékoztatást akar, egy másik lehetőség a QDIRSRV feladatnapló megtekintése.

[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 információkat a Programozás témakör “Directory Server alkalmazás programozási felületek” részében talál.

Kapcsolódó fogalmak

Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek
A Directory Server alkalmazás programozási felületekkel kapcsolatosan további információkat az Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek témakör tartalmaz.

Jelszó-irányelvekkel kapcsolatos hibák

Egy jelszó-irányelv engedélyezése néha váratlan hibákhoz vezethet.

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. Tekintse meg a bejegyzés pwdchangedtime és pwdaccountlockedtime attribútumát.

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.

Kapcsolódó hivatkozás

“Jelszó-irányelv javaslatok” oldalszám: 81
Lehetséges, hogy a jelszó-irányelvek nem mindig a várt módon viselkednek.

A QGLDCPYVL API hibaelhárítása

A Felhasználói nyomkövetés szolgáltatás használata megmagyarázhatja a hibát, illetve eldöntheti, ha segítségre van szükség.

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:

```
STRTRC SSNID(COPYVLDL) JOBTRCTYPE(*TRCTYPE) TRCTYPE((*DIRSRV *INFO))
CALL QGLDCPYVL PARM(...)
ENDTRC SSNID(COPYVLDL) DTALIB(QTEMP) PRTTRC(*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 a parancssorba.

   ```
   SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
   ```

   ahol QAP0ZDMP egy nullát tartalmaz és *xxx* az SAVF fájl megadott neve.

   Kapcsolódó fogalmak

Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek
A Directory Server alkalmazás programozási felületekkel kapcsolatosan további információkat az Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek témakör tartalmaz.

Kapcsolódó tájékoztatás

Nyomkövetés indítása (STRTRC)

Mentési fájl létrehozása (CRTSAVF)

Objektum mentése (SAVOBJ)

Kapcsolódó információk

A Directory Server témakörrel kapcsolatos IBM Redbooks kiadványok (PDF formátumban), webhelyek, illetve információs központ témakörök felsorolása az alábbiakban található. A PDF változatok bármelyikét szabadon megtekintheti vagy kinyomtathatja.

IBM Redbooks 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 webhely (www.ibm.com/servers/eserver/iseries/ldap)
- The Java Naming and Directory Interface (JNDI) Tutorial Web site (java.sun.com/products/jndi/tutorial/)

Egyéb információk

“Egyszerűsített címtárhozzáférési protokoll (LDAP) alkalmazás programozási felületek” a Programozás 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 képviseletek 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 szabadalmai lehetnek. Ezen dokumentum nem ad semmiféle licencet 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 szállítóihoz.

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 forgalmazói árak ettől eltérők lehetnek.

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. A példák nem kerültek minden körülmény 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
Domino
e(logo)server
eServer
i5/OS
IBM
iSeries
Java
Lotus
Lotus Notes
Operating System/400
OS/400
Redbooks
RDN
SecureWay
System i
Tivoli
UNIX
WebSphere
XT
400

Az Adobe, az Adobe logó, a PostScript, illetve a PostScript logó az Adobe Systems Incorporated védjegye vagy bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

A Microsoft, a Windows, a Windows NT és a Windows logó a Microsoft Corporation védjegye az Egyesült Államokban és/vagy más országokban.

A 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 felhasználásra, feltéve, hogy valamennyi tulajdonosi feljegyzés megmarad. 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