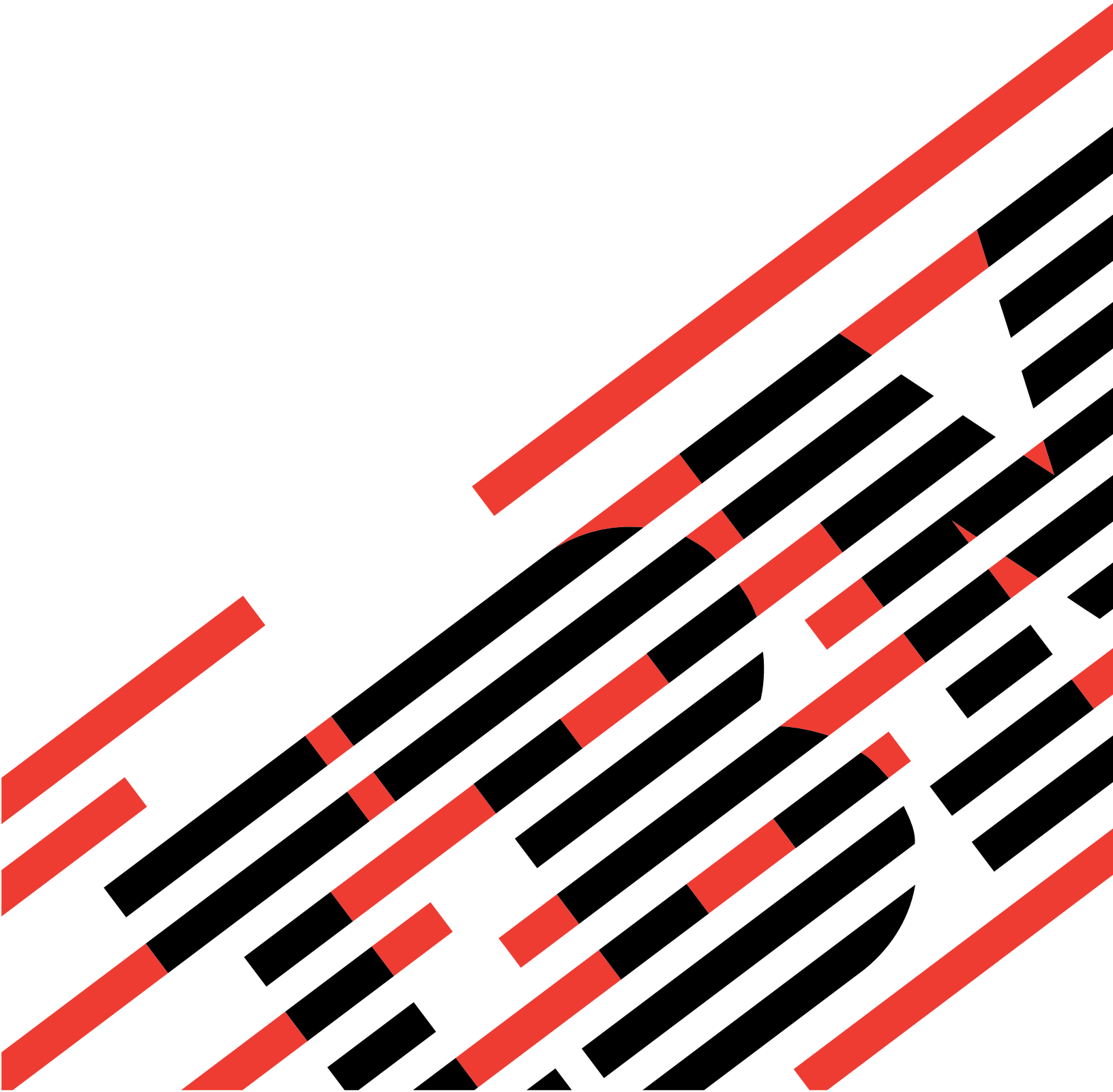
IBM

eserver

iSeries

Umrežavanje
Usluga Direktorija (LDAP)



IBM

@server

iSeries

Umrežavanje
Usluga Direktorija (LDAP)

Sadržaj

Dio 1. Usluge Direktorija (LDAP)

Usluge Direktorija daje Lightweight Directory Access Protocol (LDAP) poslužitelj na iSeries poslužitelju. LDAP se izvodi preko Transmission Control Protocol/Internet Protocol (TCP/IP) i popularan je kao usluga direktorija i za Internet i ne-Internet aplikacije.

Ako vam je poznat Usluge Direktorija, možda želite početi čitanjem o tome što je novo za ovo izdanje. Ako želite, možete ispisivati ili prikazivati PDF verziju podataka o Uslugama Direktorija.

Slijedeći predmeti predstavljaju Usluge Direktorija i daju informaciju za pomoć u administriranju LDAP poslužitelja na vašem iSeries poslužitelju:

Za dodatne informacije o Usluge Direktorija, posjetite Usluge Direktorija web stranicu .

LDAP poslužitelj kojeg Usluge Direktorija osigurava je IBM SecureWay Direktorij .

Poglavlje 1. Što je novo za V5R2

Usluge Direktorija imaju slijedeća poboljšanja i nova svojstva.

- Usluge Direktorija su dio osnovnog operacijskog sistema počevši od V5R1. Opcija 32 nije više dostupna od V5R2.
- Učinjena su nova sigurnosna poboljšanja za dalju zaštitu podataka pohranjenih na poslužitelju direktorija.
- LDAP poslužitelj direktorija se sad može koristiti kao kontroler domene za domenu Mapiranja identiteta poduzeća (EIM).
- Nova opcija je dostupna administratorima koja se može koristiti za dodjeljivanje administratorskog pristupa poslužitelju direktorijaza korisnike kojima je dan pristup identifikatoru funkcije (ID) Administratora usluga direktorija (QIBM_DIRSRV_ADMIN) operacijskog sistema kroz iSeries Navigator aplikacijsku podršku.
- Možete izabrati da vaš poslužitelj direktorija koristi specifične IP adrese ili možete izabrati da se koriste sve konfigurirane IP adrese na poslužitelju. Pogledajte “Promijenite port ili IP adresu” na stranici 19 za više informacija.
- **ldap_set_option** API ima novo debug svojstvo praćenja za V5R2. LDAP_OPT_DEBUG opcija se može koristiti za pomoć u dijagnosticiranju problema s klijentima koji koriste LDAP C API-je. Za više informacija, pogledajte “Koristite opciju LDAP_OPT_DEBUG za praćenje grešaka” na stranici 61 ili pogledajte API-je Usluga Direktorija u iSeries Informacijskom Centru  .

Kako vidjeti što je novo ili promijenjeno:

Da vam pomogne vidjeti gdje su načinjene tehničke promjene, ova informacija koristi:

-  sliku da označi gdje nova ili promijenjena informacija počinje.
-  da označi gdje nova ili promijenjena informacija završava.

Poglavlje 2. Ispis teme na pisač

Da pogledate ili spustite PDF verziju, izaberite Usluge Direktorija (LDAP) (oko 323 KB ili 66 stranica).

Ostale informacije

Također možete pogledati ili ispisati bilo koji od slijedećih PDF-ova:

- *Kuharica LDAP implementacije* .
- *razumijevanje LDAP-a* .
- *Korištenje LDAP-a za integraciju direktorija: pogled na IBM SecureWay Direktorij, Aktivni direktorij i Domino* .
- *Implementacija i praktično korištenje LDAP-a na iSeries poslužitelju* .

Ako pohranjujete PDF verziju na svojoj radnoj stanici za gledanje ili ispis:
1. Otvorite PDF u svom pregledniku (kliknite na gornju vezu).
2. Na izborniku preglednika kliknite **File**.
3. Kliknite **Save As...**
4. Idite do direktorija u koji želite pohraniti PDF dokument.
5. Kliknite **Save**.

Spuštanje Adobe Acrobat Reader-a

Ako trebate Adobe Acrobat Reader za gledanje ili ispis ovih PDF-ova, možete spustiti kopiju sAdobe Web stranice (www.adobe.com/products/acrobat/readstep.html) .

Poglavlje 3. Započnite s Usluge Direktorija

Usluge Direktorija daje Lightweight Directory Access Protocol (LDAP) poslužitelj na iSeries poslužitelju. LDAP se izvodi preko Transmission Control Protocol/Internet Protocol (TCP/IP) i dobiva na popularnosti kao usluga direktorija i za Internet i ne-Internet aplikacije. Vi izvodite većinu zadataka postava i upravljanja OS/400-baziranog LDAP poslužitelja direktorija kroz Grafičko korisničko sučelje (GUI) od iSeries Navigator. Za administriranje Usluge Direktorija, morate imati iSeries Navigator instaliran na PC-ju koji je povezan na vaš iSeries poslužitelj. Usluge Direktorija možete koristiti sa aplikacijama koje podržavaju LDAP kao što je aplikacija za poštu koja traži adrese e-pošte s LDAP poslužitelja.

Osim LDAP poslužitelja, Usluge Direktorija obuhvaćaju i:

- OS/400-osnovni LDAP klijent. Ovaj klijent uključuje skup sučelja aplikativnog programa (API-ja) koje možete koristiti u OS/400 programima da kreirate vlastite klijent aplikacije. Za informacije o ovim API-jima, pogledajte predmet Usluge Direktorija pod Programiranje u iSeries Informativni Centar.
- Verzija 3.2 IBM SecureWay Oprema za razvoj softvera klijenta direktorija (SDK). SDK uključuje Windows LDAP klijenta i slijedeće alate:
  - IBM SecureWay Alat upravljanja direktorijem, koji vam daje grafičko korisničko sučelje za upravljanje sadržajem direktorija.
  - pomoćne programe reda za naredbe (ldapsearch, ldapadd, itd.)
  - C LDAP API (datoteke knjižnice, datoteke zaglavlja i primjere izvornog koda)
  - IBM JNDI LDAP dobavljač usluga (ibmjndi.jar)
  - online dokumentaciju za sve navedene stavke. Pogledajte readme datoteku za lokacije i imena tih HTML datoteka.

Ako ste koristili Usluge Direktorija s ranijim izdanjem OS/400, pogledajte “Migrirajte na V5R2 iz ranijeg izdanja Usluge Direktorija” na stranici 11.

Ako želite pročitati uvod u LDAP, pogledajte “LDAP osnove” na stranici 8. Ako ste koristili LDAP poslužitelje na drugim platformama trebali biste odvojiti nekoliko minuta za čitanje ovog predmeta jer sadržava neke OS/400-specifične informacije.

Kad se familijarizirate s osnovnim informacijama, nastavite s “Planirajte svoj poslužitelj LDAP direktorija” na stranici 11.

Ako trebate informacije o instaliranju i konfiguriranju poslužitelja direktorija, pogledajte “Instalirajte i konfigurirajte Usluge Direktorija” na stranici 14.

Dokumentacija

Usluge Direktorija Informativni Centar predmet daje pregled LDAP i koncentrira se specifično na upravljanju LDAP poslužiteljem direktorija na OS/400. Ova dokumentacija također daje punu dokumentaciju za SecureWay SDK klijenta direktorija. Za dodatne LDAP informacije, posavjetujte se s LDAP referencama kao slijedeće:

- *Kuharica LDAP implementacije*  .
- *Razumijevanje LDAP-a*  .
- *Korištenje LDAP za integraciju direktorija: Pogled na IBM SecureWay Direktorij, Aktivni direktorij i Domino*  .
- *Implementacija i praktično korištenje LDAP-a na iSeries poslužitelju*  .

- *LDAP: Programiranje aplikacija koje podržavaju direktorije s Lightweight Directory Access Protocol*, autori Tim Howes i Mark Smith.
- *Razumijevanje i razvoj LDAP Usluga Direktorija*, autori Mark C. Smith, Gordon S. Good i Tim Howes.

Dodatne informacije o Usluge Direktorija na iSeries poslužitelju dostupne su u home stranici Usluga Direktorija iSeries poslužitelja .

Bilješka: Neki materijali sadržani u ovom dokumentu su izvedeni iz LDAP dokumentacije koju je osiguralo sveučilište u Michiganu. Copyright © 1992-1996, Regents of the University of Michigan, Sva prava pridržana.

LDAP osnove

Lakokategorni protokol za pristup direktorijima (LDAP) je protokol koji radi preko protokola za kontrolu prijenosa/Internet protokola (TCP/IP). LDAP verzija 2 se formalno definira u Internet Engineering Task Force (IETF) zahtjevu za komentar (RFC) 1777, *Lightweight Directory Access Protocol*. LDAP verzija 3 se formalno definira u IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*. Ove RFC-e (zahtjeve) možete pogledati na Internetu na slijedećoj URL adresi:

http://www.ietf.org

LDAP posluživanje direktorija slijedi klijent/poslužitelj model. Jedan ili više LDAP poslužitelja sadrže podatke direktorija. LDAP klijent se povezuje na LDAP poslužitelj i izdaje zahtjev. Poslužitelj uzvraća odgovorom ili pokazivačem (preporuke) koja upućuje na neki drugi LDAP poslužitelj.

Načini upotrebe LDAP-a:

Pošto je LDAP usluga direktorija više nego baza podataka, informacije u LDAP direktoriju su uobičajeno opisne, bazirane na atributima informacije. LDAP korisnici općenito češće čitaju podatke u direktoriju nego što ih mijenjaju. Ažuriranja su obično jednostavne promjene tipa sve ili ništa. Među uobičajene načine upotrebe LDAP direktorija spadaju online telefonski imenici i imenici e-pošte.

Struktura LDAP direktorija:

Model LDAP servisnog direktorija je baziran na **slogovima** (koji se nazivaju i **objektima**). Svaki slog se sastoji od jednog ili više **atributa**, kao što su ime ili adresa i **tip**. Tipovi se obično sastoje od mnemoničkih nizova kao što su cn za uobičajeno ime ili mail za e-mail adresu.

Direktorij iz primjera u Slika 1 na stranici 10 prikazuje slog za Tim Jonesa koji obuhvaća *mail* i *telephoneNumber* atribute. Neki drugi mogući atributi obuhvaćaju *fax*, *title*, *sn* (za prezime) i *jpegPhoto*.

Svaki direktorij ima **shemu**, koja je skup pravila koji određuju strukturu i sadržaj direktorija. Trebali biste koristiti IBM SecureWay Alat upravljanja direktorijem (DMT) za uređivanje datoteka sheme za vaš LDAP poslužitelj. Nakon što instalirate Usluge Direktorija, datoteke su locirane na vašem sistemu u /QIBM/UserData/OS400/DirSrv.

Bilješka: Originalne kopije default silogičkih datoteka su smještene u /QIBM/ProdData/OS400/DirSrv. Ako trebate zamijeniti datoteke u UserData direktoriju, možete kopirati ove datoteke u /QIBM/ProdData/OS400/DirSrv direktorij.

Svaki slog direktorija ima posebni atribut zvan **objectClass**. Ovaj atribut kontrolira atribute koji su potrebni i dopušteni u nekom slogu. Drugim riječima, vrijednosti objectClass atributa određuju shematska pravila koje slog mora poštivati.

Svaki direktorij također ima i slijedeće **operativne atribute**, koje LDAP poslužitelj automatski održava:

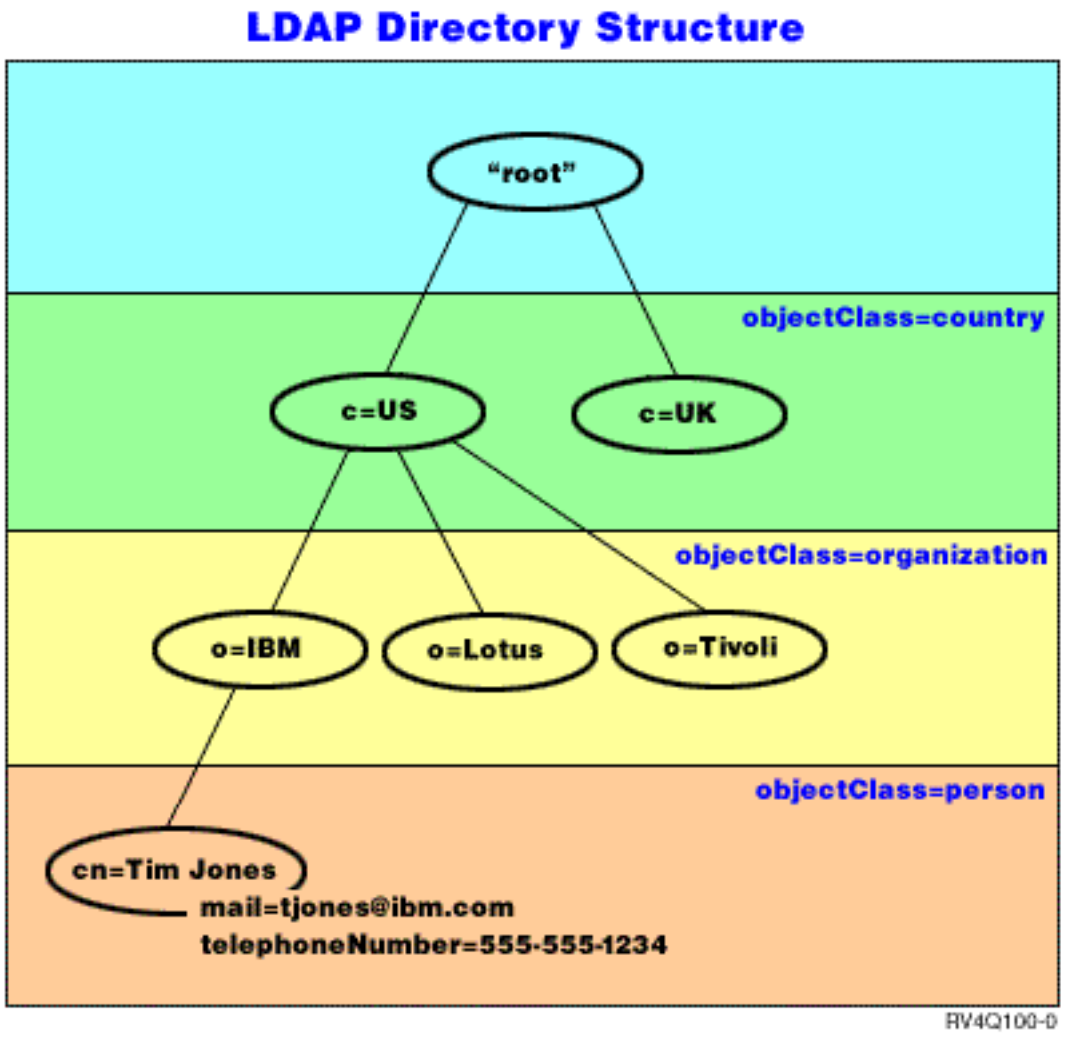
- CreatorsName, koji sadrži povezni DN korišten kod kreiranja sloga.
- CreateTimestamp, koji sadrži vrijeme kad je slog kreiran.
- modifiersName, Koji sadrži povezni DN korišten kod zadnje prepravke sloga (u početku je to isto kao CreatorsName).
- modifyTimestamp, koji sadrži vrijeme kad je slog zadnji puta prepravljan (u početku je to isto kao CreateTimestamp).

Tradicionalno, slogovi u LDAP direktoriju su raspoređeni u hijerarhijskoj strukturi koja odražava političke, zemljopisne ili organizacijske granice (vidjeti Slika 1 na stranici 10). Upisi koji predstavljaju zemlje pojavljuju se na vrhu hijerarhije. Upisi koji predstavljaju države ili nacionalne udruge zauzimaju drugu razinu na dolje u hijerarhiji. Slogovi koji se potom nalaze ispod toga predstavljaju ljude, organizacijske jedinice, pisače, dokumente ili druge stvari.

Pri strukturiranju svoga direktorija niste ograničeni samo na tradicionalnu hijerarhiju. Struktura komponenti domene, na primjer, dobiva na popularnosti. Takvom strukturom, upisi se tvore od dijelova TCP/IP imena domena. Na primjer, dc=ibm,dc=com može biti povoljniji od o=ibm,c=us.

LDAP se poziva na upise sa **prepoznatljivim imenima** s (DN). Ta prepoznatljiva razlikovna imena se sastoje od imena samog upisa kao i od imena, u poretku od dna prema vrhu, objekata iznad njega u direktoriju. Na primjer, kompletan DN za upis u donjem lijevom uglu Slika 1 na stranici 10 je cn=Tim Jones, o=IBM, c=US. Svaki upis ima barem jedan atribut koji se koristi za imenovanje upisa. Ovaj atribut koji određuje ime se naziva **relativno razlikovno ime (RDN)** upisa. Upis iznad toga RDN se naziva njegovim **višim razlikovnim imenom**. U gornjem primjeru, cn=Tim Jones imenuje unos, pa je to RDN. o=IBM, c=US je nadređeni DN za cn=Tim Jones.

Ako želite dati LDAP poslužitelju mogućnost održavanja i upravljanja dijelom LDAP direktorija, trebate navesti viša razlikovna imena najviše razine u konfiguraciji poslužitelja. Ta razlikovna imena se nazivaju **sufiksi**. Poslužitelj može pristupiti svim objektima u direktoriju koji se nalaze ispod navedenog sufiksa u hijerarhiji direktorija. Na primjer, ako je LDAP poslužitelj sadržavao direktorij pokazan u Slika 1 na stranici 10, trebao bi imati sufiks o=ibm, c=us specificiran u svojoj konfiguraciji kako bi mogao odgovoriti klijentskim upitima u vezi s Tim Jones.



Slika 1. Osnovna struktura LDAP direktorija

Napomene o LDAP i Usluge Direktorija:

- Počevši s V4R5, i OS/400 LDAP poslužitelj i OS/400 LDAP klijent su bazirani na LDAP Verzija 3. Možete koristiti V2 klijenta s V3 poslužiteljem. Ipak, ne možete koristiti V3 klijenta s V2 poslužiteljem osim ako se ne vežete kao V2 klijent i koristite samo V2 API-je. Pogledajte LDAP V2/V3 razmatranja za više detalja.
- Windows LDAP klijent je također baziran na LDAP Verzija 3.
- Pošto je LDAP standard, svi LDAP poslužitelji dijele mnoštvo osnovnih karakteristika. Međutim, zbog razlika u provedbi, međusobno nisu potpuno kompatibilni. LDAP poslužitelj osiguran od Usluge Direktorija je jako kompatibilan s drugim poslužiteljima LDAP direktorija u IBM SecureWay Direktoriju i grupi proizvoda IBM Direktorija. Međutim, ne mora biti tako kompatibilan i s drugim LDAP poslužiteljima.
- Podaci za LDAP poslužitelj koji Usluge Direktorija osigurava prebivaju u OS/400 bazi podataka.

Dodatne informacije:

Za primjere korištenja LDAP direktorija, pogledajte slijedeće:

- Odlomak 1.6 Brzo pokretanje: Primjer javnog LDAP-a, u redbook *Razumijevanje LDAP-a*.
- Odlomak 3.3 Primjeri scenarija, u redbook Razumijevanje LDAP-a.

Ako želite saznati više o LDAP konceptima, pogledajte Poglavlje 5, “Usluge Direktorija koncepti i referentne informacije” na stranici 31.

Neki momenti vezani uz upotrebu LDAP V2 sa LDAP V3

Počevši s V4R5, i OS/400 LDAP poslužitelj i OS/400 LDAP klijent su bazirani na LDAP Verzija 3. Ne možete koristiti V3 klijenta s V2 poslužiteljem. Ipak, možete koristiti ldap_set_option() API za promjenu verzije V3 klijenta u V2. Zatim možete uspješno slati zahtjeve na V2 poslužitelj.

V2 klijenta možete koristiti sa V3 poslužiteljem. Imajte ipak na umu da kod zahtjeva za pretraživanjem V3 poslužitelj može poslati podatke natrag u punom rasponu UTF-8 formata, dok V2 klijent može biti u stanju obraditi samo podatke u IA5 skupu znakova.

Bilješka: LDAP verzija 2 se formalno definira u Internet Engineering Task Force (IETF) zahtjevu za komentar (RFC) 1777, *Lightweight Directory Access Protocol*. LDAP verzija 3 se formalno definira u IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*. Ove RFC-e (zahtjeve) možete pogledati na Internetu na slijedećoj URL adresi:

http://www.ietf.org 

Planirajte svoj poslužitelj LDAP direktorija

Prije nego što instalirate Usluge Direktorija i počnete konfigurirati LDAP direktorij, odvojite nekoliko minuta za planiranje direktorija. Važne stvari koje trebate uzeti u obzir su slijedeće:

- **Organizirajte direktorij**. Planirajte strukturu vašeg direktorija i odredite koje sufikse i atribute će vaš poslužitelj trebati.
- **Odlučite kako velik će biti vaš direktorij**. Onda možete procijeniti koliko memorije vam treba. Veličina direktorija ovisi o slijedećem:
  - Broju atributa u poslužiteljskoj shemi.
  - Broju upisa na poslužitelju.
  - Tipu informacija koje pohranjujete na poslužitelju.

  Na primjer, prazni direktorij koji koristi default shemu Usluga Direktorija zahtijeva otprilike 10 MB prostora. Direktorij koji koristi default shemu i sadrži 1000 slogova običnih podataka o zaposlenicima zahtijeva oko 30 MB prostora. Ovaj broj će se mijenjati ovisno atributima koje koristite. Također će se jako povećati ako ste pohranili velike objekte, kao što su slike, u direktorij.
- **Odlučite koje sigurnosne mjere ćete poduzeti**. Usluge Direktorija podržava korištenje Sloja sigurnih utičnica (SSL) i digitalnih certifikata kao i Sigurnosti translacijskog sloja (TLS) za sigurnost komunikacije. Počevši s V5R1, Kerberos provjera autentičnosti je također podržana.
- Usluge Direktorija dopušta vam kontrolu pristupa objektima direktorija s listama kontrole pristupa (ACL-ovi). Možete također koristiti OS/400 reviziju sigurnosti da zaštitite direktorij.

Migrirajte na V5R2 iz ranijeg izdanja Usluge Direktorija

V5R2 OS/400 predstavlja nova svojstva i mogućnosti za Usluge Direktorija. Te promjene utječu i na LDAP poslužitelj direktorija i na grafičko korisničko sučelje (GUI) iSeries Navigator-a. Da iskoristite prednosti novih GUI funkcija, trebate instalirati iSeries Navigator na PC koji može komunicirati preko TCP/IP-a s vašim iSeries poslužiteljem. iSeries Navigator je komponenta iSeries Access za Windows. Ako imate raniju verziju iSeries Navigator instaliranu, trebali bi ju nadograditi na V5R2.

V5R2 OS/400 podržava nadogradnje iz V4R5 i V5R1. Kad nadogradite na V5R2 OS/400, i podaci LDAP direktorija i datoteke sheme direktorija automatski migriraju da se prilagode V5R2 formatima. Ako imate Usluge Direktorija LDAP poslužitelj koji se izvodi pod V4R3 ili V4R4 OS/400 i želite migrirati poslužitelj na V5R2, trebate izvesti neke dodatne migracijske zadatke.

Kad nadograđujete na V5R2 OS/400, trebate biti svjesni nekih migracijskih pitanja:

- Kad nadograđujete na V5R2, Usluge Direktorija automatski migrira vaše datoteke sheme na V5R2 i briše stare datoteke sheme. Međutim, ako ste te datoteke shema obrisali ili preimenovali, Usluge Direktorija ih ne mogu migrirati. Možete dobiti grešku ili Usluge Direktorija može pretpostaviti da su datoteke već migrirane.
- Usluge Direktorija migrira podatke direktorija u V5R2 format prvi put kad pokrenete poslužitelj ili importirate LDIF datoteku. Planirajte tako da ostavite malo vremena da migracija potpuno završi. Ako nadograđujete na V5R2 iz V4R4 ili ranije, budite svjesni da će podaci direktorija trebati približno dvostruko više memorijskog prostora u V5R2 nego što je trebalo prije. To je zato što je u V4R4 ili ranijim verzijama, Usluge Direktorija podržavao samo IA5 skup znakova i pohranu podataka u ccsid 37 (format pojedinačnog bajta). Usluge Direktorija podržava puni ISO 10646 skup znakova.

  Nakon nadogradnje na V5R2, trebate pokrenuti poslužitelj jednom da migrirate postojeće podatke prije importiranja novih podataka. Ako pokušate importirati podatke prije nego što jednom pokrenete poslužitelj i nemate dovoljno ovlaštenje, importiranje neće uspjeti.
- V4R4 i ranija izdanja Usluga Direktorija nisu uzimali u obzir vremenske zone kod kreiranja unosa vremenske oznake. Počevši s V4R5, vremenska zona se koristi u svim dodacima i promjenama direktorija. zato, ako nadograđujete na V5R2 iz V4R4 ili ranije, Usluge Direktorija prilagođava postojeće createtimestamp i modifytimestamp atribute da odrazi ispravnu vremensku zonu. To čini oduzimanjem trenutno definirane vremenske zone na iSeries sistemu od vremenskih oznaka koje su pohranjene u direktoriju. Primjetite da ako trenutna vremenska zona nije ista vremenska zona koja je bila aktivna kad su unosi originalno kreirani ili preinačeni, nove vrijednosti vremenske oznake neće odražavati originalnu vremensku zonu.
- Slijedeći migraciju, LDAP poslužitelj direktorija će se automatski pokrenuti kada se pokrene TCP/IP. Ako ne želite da se poslužitelj direktorija automatski pokrene, koristite iSeries Navigator da promijenite postavke.

Migrirajte iz V4R3 ili V4R4 Usluge Direktorija u V5R2

V5R2 OS/400 ne podržava izravnu nadogradnju iz V4R3. Ako želite migrirati V4R3 ili V4R4 Usluge Direktorija LDAP poslužitelj u V5R2, možete slijediti jedan od slijedećih postupaka:

- Slip instalacija OS/400 iz V4R3 ili V4R4 na privremeno izdanje
- Spremanje knjižnice baze podataka i scratch instalacija OS/400 V4R3 ili V4R4 na V5R2

Slip instalacija OS/400 iz V4R3 ili V4R4 na privremeno izdanje

Iako nadogradnje iz V4R3 i V4R4 OS/400 na V5R2 nisu podržane, slijedeće nadogradnje su podržane:

- V4R3 i V4R4 nadograđen na V4R5
- V4R4 i V4R5 nadograđen na V5R1
- V4R5 i V5R1 nadograđen na V5R2

jedan način za migraciju vašeg Usluge Direktorija poslužitelja je nadogradnja na privremeno izdanje (V4R5 ili V5R1) i onda na V5R2. Za detaljne informacije o OS/400 instalacijskim postupcima, pogledajte *Instalacija softvera* . Slijedite ove općenite korake za izvođenje migracije:

1. Zabilježite promjene koje ste napravili u datotekama sheme u direktoriju /QIBM/UserData/OS400/DirSrv. Datoteke sheme migriraju automatski.
2. Za V4R4 ili V4R3, napravite slip instalaciju V4R5 ili V5R1 OS/400.
3. Napravite slip instalaciju na V5R2 OS/400.
4. Pokrenite poslužitelj Usluga direktorija ako već nije pokrenut.
5. Koristite Alat upravljanja direktorijem za promjenu datoteka sheme za bilo kakve promjene korisnika koje ste opazili u koraku 1.
6. Ponovo pokrenite poslužitelj Usluga direktorija.

Spremanje knjižnice baze podataka i scratch instalacija OS/400 iz V4R3 ili V4R4 u V5R2

Drugi način za migriranje vašeg Usluge Direktorija poslužitelja je spremanje knjižnice baze podataka koju Usluge Direktorija koristi u V4R3 ili V4R4 i zatim njeno vraćanje nakon scratch instaliranja V5R2. To preskače korak instaliranja privremenog izdanja. Ipak, postavke poslužitelja ne migriraju, pa morate rekonfigurirati postavke poslužitelja. Za detaljne informacije o OS/400 instalacijskim postupcima, pogledajte

Instalacija softvera  . Slijedite ove općenite korake za izvođenje migracije:

1. Zabilježite promjene koje ste napravili u datotekama sheme u direktoriju /QIBM/UserData/OS400/DirSrv. Datoteke sheme nisu migrirane automatski, tako da ako želite zadržati promjene trebat ćete ih opet ručno implementirati.
2. Zabilježite raznovrsne konfiguracijske postavke u svojstvima Usluge Direktorija poslužitelja, uključujući ime knjižnice baze podataka.
3. Spremite knjižnicu baze podataka koja je specificirana u konfiguraciji Usluge Direktorija poslužitelja.
4. Opazite konfiguraciju izdavanja.
5. Scratch instalirajte sistem na V5R2 OS/400.
6. Koristite EZ-postav da konfigurirate poslužitelj Usluga direktorija.
7. Vratite knjižnicu baze koju ste spremili u koraku 3.
8. Koristite Alat upravljanja direktorijem za promjenu datoteka sheme za bilo kakve promjene korisnika koje ste opazili u koraku 1.
9. Koristite iSeries Navigator da rekonfigurirate Usluge direktorija. Odredite knjižnicu baze koju ste spremili i vratili.
10. Koristite iSeries Navigator da rekonfigurirate izdavanje.
11. Ponovo pokrenite poslužitelj Usluga direktorija.

Pitanja nadogradnje

Kad vršite nadogradnju iz V4R3 u neko kasnije izdanje, trebate imati na umu slijedeće momente:

- **Migracija datoteke prstenova u bazu ključeva:**

  V3R2 Client Access se koristio datotekama prstenova ključeva za uspostavljanje veza sa Slojem sigurnih utičnica (SSL) prema LDAP poslužitelju direktorija. iSeries Access za Windows koristi spremišta certifikata, koji se ponekad nazivaju baze ključeva, za uspostavljanje SSL konekcija. Ako ste prije koristili datoteku prstenova ključeva sa svojim LDAP poslužiteljem direktorija, datoteka prstenova se mora konvertirati u bazu ključeva, da bi mogli i dalje koristiti SSL. Kad prvi put pokušate pokrenuti neku SSL vezu prema LDAP poslužitelju direktorija, iSeries Navigator će vas upozoriti na tu promjenu. Ako izaberete konverziju ključa, traži se da specificirate neke informacije za bazu ključeva prije nego se konverzija napravi.

  LDAP poslužitelj direktorija je također koristio datoteku prstena ključeva za svoje SSL veze u izdanju V4R3. Počev od V4R4 on koristi sistemsko spremište certifikata. Ako je vaš poslužitelj bio postavljen za upotrebu SSL u izdanju V4R3, sadržaj datoteke prstena ključeva će se migrirati u sistemsko spremište certifikata.
- **Uklonjene su dvije datoteke toka:**

  Slijedeće datoteke toka koje su koristile Usluge Direktorija u V4R3 više nisu potrebne i automatski se brišu kad instalirate kasnije izdanje:

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

  Sa ovim datotekama ne trebate ništa raditi. Ovo se spominje samo zato da se ne brinete ako primijetite da ih više nema na sistemu.

Budite svjesni da može biti dodatnih pitanja povezanih sa nadogradnjom trenutnog izdanja da drugih izdanja.

Instalirajte i konfigurirajte Usluge Direktorija

Usluge Direktorija (LDAP) se automatski instalira kad instalirate OS/400. Poslužitelj direktorija uključuje default konfiguraciju koja automatski pokreće poslužitelj direktorija kada je pokrenut TCP/IP. Poslužitelj direktorija također pokreće objavljivanje informacija o računalu iz OS/400 na poslužitelj direktorija. Da prilagodite postavke LDAP poslužitelja direktorija, izvedite Usluge Direktorija Čarobnjaka konfiguracije. Morate imati *ALLOBJ i *IOSYSCFG posebna ovlaštenja da koristite čarobnjaka.

Usluge Direktorija integrirane su u osnovni operacijski sistem počevši od V5R1 i Opcija 32 nije više dostupna od V5R2.

Konfigurirajte poslužitelj LDAP direktorija

Ako vaš sistem nije konfiguriran da objavljuje informacije drugom LDAP poslužitelju i nikakvi LDAP poslužitelji nisu poznati TCP/IP DNS poslužitelju, onda je Usluge Direktorija automatski instaliran s ograničenom default konfiguracijom. Usluge Direktorija osigurava čarobnjaka za pomoć u konfiguriranju poslužitelja LDAP direktorija za vaše specifične potrebe. Možete pokrenuti ovog čarobnjaka kao dio EZ-Postave ili pokrenuti čarobnjaka kasnije iz iSeries Navigator. Koristite se ovim čarobnjakom kad vršite početno konfiguriranje poslužitelja direktorija. Možete ga upotrijebiti i za ponovno konfiguriranje poslužitelja direktorija.

Bilješka: Kad koristite čarobnjaka za ponovnu konfiguraciju poslužitelja direktorija, konfiguriranje počinjete ni od čega. Originalna konfiguracija se briše, ona se ne mijenja. Ipak, podaci direktorija nisu obrisani, već ostaju pohranjeni u knjižnici koju ste odabrali prije instalacije (QUSRDIRDB po defaultu). Dnevnik promjena također ostaje nedirnut, u QUSRDIRCL knjižnici po defaultu.

Ako želite početi potpuno od početka, očistite ove dvije knjižnice prije nego što pokrenete čarobnjaka.

Ako želite promijeniti konfiguraciju poslužitelja direktorija, ali ne i potpuno je obrisati, kliknite desnom tipkom na **Direktorij** i izaberite **Svojstva**. Time se ne briše originalna konfiguracija.

Morate imati posebna ovlaštenja *ALLOBJ i *IOSYSCFG kad konfigurirate poslužitelj. Ako želite konfigurirati OS/400 reviziju sigurnosti, morate imati posebno ovlaštenje *AUDIT.

Za pokretanje Čarobnjaka konfiguracije Usluga Direktorija, načinite ove korake:

1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Konfiguriraj**.

Bilješka: Ako ste već konfigurirali poslužitelj direktorija, kliknite **Rekonfiguriraj**, a ne **Konfiguriraj**.

Slijedite upute u Čarobnjaku konfiguracije poslužitelja direktorija da konfigurirate vaš poslužitelj LDAP direktorija.

Bilješka: Knjižnicu u kojoj su pohranjeni podaci direktorija možete po želji staviti u pomoćnu korisničku memoriju (ASP) umjesto u sistemsku ASP. Ipak, ova knjižnica ne može biti pohranjena u Nezavisnom ASP-u i bilo kakav pokušaj konfiguriranja, rekonfiguriranja, ili pokretanja poslužitelja s knjižnicom u Nezavisnom ASP-u neće uspjeti.

Kad je čarobnjak završio, vaš poslužitelj LDAP direktorija ima osnovnu konfiguraciju. Ako izvodite Lotus Domino na vašem sistemu, onda port 389 (default port za LDAP poslužitelj) možda već koristi Domino LDAP funkcija. Morate učiniti nešto od slijedećeg:

- Promijenite port koji Lotus Domino koristi
- Promijenite port koji Usluge Direktorija koristi
- Koristite specifične IP adrese

Sad možete pokrenuti poslužitelj. Prije pokretanja poslužitelja, ipak, možda ćete htjeti učiniti nešto ili sve od slijedećeg:
- Importirati podatke u poslužitelj
- Aktivirati zaštitu Sloja sigurnih utičnica (SSL)
- Omogućiti Kerberos provjeru ovlaštenja
- Podesiti preporučitelja

Omogućite SSL na LDAP poslužitelju direktorija

Ako imate Upravitelj digitalnih certifikata instaliran na vašem sistemu, možete koristiti Sloj sigurnih utičnica (SSL) sigurnost za zaštitu pristupa vašem LDAP poslužitelju direktorija. Prije omogućavanja SSL-a na poslužitelju direktorija, možda će vam pomoći čitanje pregleda o korištenju SSL-a s Usluge Direktorija.

Da koristite SSL vezu kad administrirate vaš LDAP poslužitelj direktorija iz iSeries Navigator, ili da koristite SSL s Windows LDAP klijentom, morate imati jedan od proizvoda Klijentskog šifriranja (5722CE2 ili 5722CE3) instaliran na vašem PC-ju.

Ako aktivirate SSL na LDAP poslužitelju, koristite se sučeljem Upravitelja digitalnih certifikata. Možete pokrenuti Upravitelja digitalnih certifikata iz **Internet** foldera u iSeries Navigator, ili iz stranice **Mreža** u dijalogu **Svojstva** poslužitelja direktorija.

Za pokretanje Sučelja digitalnih certifikata iz stranice **Mreža**, slijedite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite karticu **Mreža**.
6. Kliknite na **Upravitelj digitalnih certifikata**.

   Upravitelj digitalnih certifikata će se lansirati u default Internet pregledniku.

Specifične korake koje trebate slijediti kod dodjeljivanja digitalnih certifikata poslužitelju direktorija potražite u napisu Zaštita LDAP poslužitelja direktorija.

Nakon što aktivirate SSL, možete promijeniti port koji LDAP poslužitelj direktorija koristi za zaštićene veze.

Omogućite Kerberos provjeru autentičnosti na poslužitelju LDAP direktorija

Ako imate Uslugu provjere autentičnosti mreže konfiguriranu na vašem sistemu, možete postaviti vaš poslužitelj LDAP direktorija da koristi Kerberos provjeru autentičnosti. Prije omogućavanja Kerberosa na poslužitelju direktorija, možda će vam pomoći čitanje pregleda o korištenju Kerberosa s Usluge Direktorija.

Za omogućavanje Kerberos provjere ovlaštenja, slijedite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite karticu **Kerberos**.
6. Označite **Omogući Kerberos provjeru ovlaštenja**.
7. Odredite ostale postavke na stranici **Kerberos** kako odgovaraju vašoj situaciji. Pogledajte stranice online pomoći za informacije o pojedinačnim poljima.

Default konfiguracija za Usluge Direktorija

LDAP poslužitelj direktorija se automatski instalira kad instalirate OS/400. Ta instalacija uključuje default konfiguraciju. Poslužitelj direktorija koristi default konfiguraciju kada je sve od sljedećeg istina:
- Administratori nisu izvodili Čarobnjaka konfiguracije Usluga Direktorija ili promijenili postavke direktorija sa stranica svojstava.
- Usluge Direktorija izdavanje nije konfigurirano.

- LDAP poslužitelj direktorija ne može naći nikakve LDAP DNS informacije.

Ako LDAP poslužitelj direktorija koristi default konfiguraciju, onda se dešava slijedeće:
- LDAP poslužitelj direktorija sa automatski pokreće kada se pokrene TCP/IP.
- Sistem kreira default administratora, cn=Administrator. Također generira lozinku koja se koristi interno. Ako kasnije trebate koristiti lozinku administratora, možete postaviti novu sa stranice svojstava Usluga Direktorija.
- Default sufiks je kreiran bazirano na IP imenu sistema. Sufiks sistemskog objekta je također kreiran bazirano na imenu sistema. Na primjer, ako je IP ime vašeg sistema mary.acme.com, sufiks je dc=mary,dc=acme,dc=com.
- LDAP poslužitelj direktorija koristi default knjižnicu podataka QUSRDIRDB. Sistem je kreira u sistem ASP.
- Poslužitelj koristi port 389 za nesigurne komunikacije. Ako je digitalni certifikat konfiguriran za LDAP, Sloj sigurnih utičnica (SSL) je omogućen i port 636 se koristi za sigurnu komunikaciju.

Sljedeći defaulti tada postoje za Usluge Direktorija izdavanje:
- Sistem izdaje informacije lokalnom LDAP poslužitelju direktorija
- Izdavanje ne koristi SSL
- Izdavanje koristi spremnike pod default sufiksom
- Za provjeru autentičnosti na poslužitelju direktorija, OS/400 koristi cn=Administrator ID i sistemski-generiranu lozinku.
- Sistem izdaje samo sistemske informacije

IBM SecureWay Alat upravljanja direktorijem

IBM SecureWay Alat upravljanja direktorijem (DMT) daje vam grafičko korisničko sučelje za upravljanjem sadržajem LDAP direktorija. Poslovi koje možete izvoditi s DMT obuhvaćaju slijedeće:
- Pregledavanje sheme direktorija
- Dodavanje, promjena i brisanje klasa objekata
- Dodavanje, promjena i brisanje atributa
- Prelistavanje i pretraživanje po stablu direktorija
- Dodavanje, promjena, gledanje i brisanje upisa
- Promjena RDN upisa
- Upravljanje ACL-ovima

DMT je dio Windows LDAP klijenta koji je uključen s Usluge Direktorija. Klijent se isporučuje u direktoriju integriranog datotečnog sustava.

Da instalirate Windows LDAP klijenta, uključujući DMT, na PC, slijedite ove korake:
1. U iSeries Navigator, proširite **Sistemi datoteka**.
2. Proširite **Dijeljene datoteke**.
3. Dva puta kliknite na **Qdirsrv**.
4. Dva puta kliknite na **UserTools**.
5. Dva puta kliknite na **Windows**.
6. Dva puta kliknite **setup.exe** i pokrenite instaliranje DMT. Slijedite upute na ekranu i završite instalaciju.

Dokumentacija za IBM SecureWay Alat upravljanja direktorijem (DMT) je locirana u datoteci dparent.htm. Ova datoteka se kopira u folder IBM SecureWay direktorija na vašem PC-ju kad instalirate klijenta.

Poglavlje 4. Administrirajte poslužitelj LDAP direktorija

Za administriranje poslužitelja LDAP direktorija, morate imati slijedeće skupove ovlaštenja:

- Za konfiguriranje poslužitelja ili mijenjanje konfiguracije poslužitelja: posebna ovlaštenja svih objekata (*ALLOBJ) i I/O konfiguracije sistema (*IOSYSCFG)
- Za pokretanje ili zaustavljanje poslužitelja: ovlaštenje Kontrola posla (*JOBCTL) i ovlaštenje objekta za naredbe Zaustavi TCP/IP (ENDTCP), Pokreni TCP/IP (STRTCP), Pokreni TCP/IP poslužitelj (STRTCPSVR) i Zaustavi TCP/IP poslužitelj (ENDTCPSVR)
- Za postavljanje revizijskog ponašanja poslužitelja direktorija: posebno ovlaštenje Revizija (*AUDIT)
- Za gledanje dnevnika posla poslužitelja: posebno ovlaštenje Kontrola spool-a (*SPLCTL)

Za upravljanje objektima direktorija (uključujući i liste kontrole pristupa, vlasništvo nad objektima i replike) trebate se spojiti na direktorij ili s DN administratora ili nekim drugim DN koji ima ispravno LDAP ovlaštenje. Ako se koristi integracija ovlaštenja, administrator može biti i projicirani korisnik koji ima ovlaštenje za funkcijski ID Administratora usluga direktorija.

Administriranje poslužitelja direktorija obuhvaća slijedeće poslove:

Pokrenite LDAP poslužitelj direktorija

Kad pokrećete LDAP poslužitelj, poduzmite ove korake:

1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Pokreni**.

   Poslužitelju direktorija može trebati nekoliko minuta za pokretanje, ovisno o brzini vašeg poslužitelja i iznosu dostupne memorije. Prvo pokretanje poslužitelja direktorija može trajati nekoliko minuta dulje nego obično jer poslužitelj mora kreirati nove datoteke. Slično tomu, kad poslužitelj pokrećete po prvi put nakon nadogradnje iz ranije verzije Usluga Direktorija, možda će trebati nekoliko minuta više nego obično jer poslužitelj mora migrirati datoteke. Možete provjeriti status poslužitelja povremeno da vidite je li se pokrenuo.

Bilješka: Poslužitelj direktorija se može pokrenuti i iz 5250 sesije tako da unesete naredbu STRTCPSVR *DIRSRV.

Uz to, ako vam je poslužitelj direktorija konfiguriran da se pokreće kad se pokrene TCP/IP, možete ga također pokretati tako da unesete naredbu STRTCP.

Zaustavite LDAP poslužitelj direktorija

zaustavljanje poslužitelja direktorija utječe na sve aplikacije koje koriste poslužitelj u vrijeme zaustavljanja. Ovo uključuje aplikacije Mapiranja identiteta poduzeća (EIM) koje trenutno koriste poslužitelj direktorija za EIM operacije. Sve aplikacije su odspojene od poslužitelja direktorija, ipak, one nisu spriječene u pokušaju ponovnog spajanja na poslužitelj.

Kad zaustavljate LDAP poslužitelj, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Zaustavi**.

   Poslužitelju direktorija treba nekoliko sekundi da se zaustavi, ovisno o brzini vašeg sistema, količini aktivnosti poslužitelja i količini dostupne memorije. Povremeno možete provjeravati status poslužitelja da vidite je li se već zaustavio.

Bilješka: Poslužitelj direktorija se može zaustaviti i iz 5250 sesije, tako da unesete naredbe ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL ili ENDTCP. ENDTCPSVR *ALL i ENDTCP također utječu na bilo koji TCP/IP poslužitelj koji se izvodi na vašem sistemu. ENDTCP će također zaustaviti i sam TCP/IP.

Provjerite status poslužitelja direktorija

iSeries Navigator prikazuje status poslužitelja direktorija u stupcu **Status** u desnom okviru.

Ako provjeravate status poslužitelja direktorija, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**. iSeries Navigator prikazuje status svih TCP/IP poslužitelja, uključujući poslužitelj direktorija, u stupcu **Status**. Za ažuriranje stanja poslužitelja, kliknite izbornik **Pogled** i izaberite **Osvježi**.
4. Ako želite pogledati dodatne informacije o statusu poslužitelja direktorija, desnom tipkom kliknite na **Direktorij** i izaberite **Status**. Tako će se prikazati broj aktivnih veza, kao i druge informacije poput prošlih i trenutnih razina aktivnosti.

   Osim što pruža dodatne informacije, gledanje statusa ovom opcijom može i uštedjeti vremena. Status poslužitelja direktorija možete osvježavati, a da ne oduzimate dodatno vrijeme potrebno za provjeru statusa ostalih TCP/IP poslužitelja.

Provjerite poslove na poslužitelju LDAP direktorija

Ponekad ćete htjeti pratiti pojedine poslove na LDAP poslužitelju. Kad provjeravate poslove na poslužitelju, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desno kliknite na **Direktorij** i izaberite **Poslovi poslužitelja**.

Omogućite obavještavanja o događajima

Usluge Direktorija podržava obavještavanja o događajima, što dopušta klijentima registraciju kod LDAP poslužitelja da ih obavijesti kad se specificirani događaj, kao što je dodavanje nečega direktoriju, desi.

Za omogućavanje obavještavanja o događajima za vaš poslužitelj, slijedite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.

4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite na **Događaji**.
6. Izaberite **Dozvoli klijentima da se registriraju za obavještavanje o događaju**.

Možete također specificirati maksimum registracija dozvoljenih za svaku vezu i maksimum ukupnih registracija koje poslužitelj dozvoljava.

Za dodatne informacije o obavještavanju o događajima, pogledajte Dodatak C: Obavještavanje o događajima u priručniku IBM SecureWay Direktorij verzija 3.2: Upute za klijentsko SDK programiranje  .

Specificirajte postavke transakcije

Usluge Direktorija podržava transakcije, što dopušta da se grupa operacija LDAP direktorija tretira kao jedna jedinica. Za više informacija, pogledajte “Transakcije” na stranici 35.

Da konfigurirate transakcijske postavke vašeg poslužitelja, slijedite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite **Transakcije**.
6. Specificirajte vaše postavke transakcija.

Bilješka: Transakcijske postavke mogu utjecati na performanse vašeg LDAP poslužitelja, pa možete eksperimentirati s različitim postavkama.

Promijenite port ili IP adresu

LDAP poslužitelj direktorija kojega aktiviraju Usluge Direktorija koristi se slijedećim default portovima:
- 389 za nezaštićene veze.
- 636 za zaštićene veze (ako ste kao aplikaciju koja može koristiti zaštićeni port koristili DCM za omogućavanje Usluga Direktorija).

Bilješka: Po defaultu, sve IP adrese definirane na lokalnom sistemu su povezane na poslužitelj.

Ako već koristite ove portove za drugu aplikaciju, možete ili dodijeliti drugi port za Usluge Direktorija, ili možete koristiti različite IP adrese za dva poslužitelja, ako aplikacije podržavaju povezivanje na specifičnu IP adresu.

Za primjer sukoba Domino LDAP poslužitelja s iSeries LDAP poslužiteljem Usluga Direktorija, pogledajte Host Domino LDAP i Usluge Direktorija na istom iSeries

Ako mijenjate portove koje koristi LDAP poslužitelj direktorija, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite na karticu **Mreža**.
6. Unesite odgovarajuće brojeve porta i zatim kliknite **OK**.

Da promijenite IP adresu na koju poslužitelj direktorija prihvaća konekcija, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.

4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite karticu **Mreža**.
6. Kliknite gumb **IP Adrese...**.
7. Izaberite **Koristite odabrane IP adrese** i izaberite IP adrese koje će poslužitelj koristiti za prihvaćanje konekcija.

Premjestite podatke LDAP direktorija između sistema

Vaš LDAP poslužitelj Usluga Direktorija može raditi neovisno o drugim poslužiteljima. Međutim, možda će vam biti korisno ako radi sa drugim poslužiteljima. To obuhvaća:
- "Importirajte LDIF datoteku"
- "Eksportirajte LDIF datoteke"
- "Postavite novu repliku poslužitelja direktorija"
- "Izdajte informacije poslužitelju direktorija" na stranici 24

Importirajte LDIF datoteku

Podatke između različitih LDAP poslužitelja direktorija možete prenositi pomoću LDAP Data Interchange Format (LDIF) datoteka. Pije nego počnete ovaj postupak, prenesite LDIF datoteku na vaš iSeries poslužitelj kao datoteku toka.

Ako importirate LDIF datoteku na LDAP poslužitelj direktorija, poduzmite ove korake:
1. Ako je poslužitelj direktorija pokrenut, zaustavite ga. Pogledajte "Zaustavite LDAP poslužitelj direktorija" na stranici 18 za informacije o zaustavljanju poslužitelj direktorija.
2. U iSeries Navigator, proširite **Mreža**.
3. Proširite **Poslužitelji**.
4. Kliknite na **TCP/IP**.
5. Desnom tipkom kliknite na **Direktorij** i izaberite **Alati**, a zatim **Import datoteke**.

Bilješka: Možete upotrijebiti i ldapadd servisni program i importirati LDIF datoteke.

Eksportirajte LDIF datoteke

Podatke između različitih LDAP direktorija možete prenositi pomoću datoteka LDAP Formata izmjenjivanja podataka (LDIF); vidjeti "LDAP format izmjenjivanja podataka" na stranici 32. U neku LDIF datoteku možete eksportirati sve ili dio svog LDAP direktorija.

Za eksport LDIF datoteke sa poslužitelja direktorija, načinite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom kliknite na **Direktorij** i izaberite **Alati**, a zatim **Eksport datoteke**.

Bilješka: Ako ne odredite lokaciju za eksportiranje LDIF datoteke, biti će spremljena u default direktorij specificiran u vašem OS/400 profilu korisnika. Ako niste mijenjali default direktorij, onda je default direktorij korijenski direktorij.

Bilješke:

1. Pazite da odredite ovlaštenje za LDIF datoteku da spriječite neovlašteni pristup podacima u direktoriju. Ako to činite, desnom tipkom kliknite na datoteku u iSeries Navigator, a zatim izaberite **Dozvole**.
2. Možete kreirati cijelu ili dio LDIF datoteke, pomoću servisnog programa ldapsearch; vidjeti "ldapsearch servisni program" na stranici 50. Koristite -L opciju i preusmjerite izlaz u datoteku.

Postavite novu repliku poslužitelja direktorija

Možete postaviti replike LDAP poslužitelja direktorija na poslužitelje direktorija na drugim iSeries poslužiteljima. Usluge Direktorija koriste standardnu LDAP verziju 3 protokola za replikaciju.

Bilješke:

1. Ne možete praviti replike između poslužitelja LDAP verzije 3 i LDAP verzije 2. Zato, sistem koji replicirate mora koristiti istu verziju LDAP-a kao sistem sa kojega replicirate. V4R3 i V4R4 OS/400 podržavaju LDAP verziju 2. V4R5 i kasnija izdanja podržavaju verziju 3
2. Možete replicirati Usluge Direktorija direktorij na IBM SecureWay V3.2 ili kasnije poslužitelje na drugim platformama. Da uradite ovo, vaš OS/400 poslužitelj direktorija mora biti konfiguriran za korištenje 3.2 ACI mehanizma. Ako poslužitelj naiđe na problem kad pokušava replicirati, prestati će replicirati. Ako se to dogodi, vaša će replika biti nepotpuna.

Kod postavljanja nove replike poslužitelja direktorija slijedite ove korake:

1. Ako to već niste učinili, konfigurirajte i glavni poslužitelj i repliku poslužitelja.

   Bilješka: Osigurajte da se shema i sufiksi podudaraju na oba poslužitelja.
2. Zaustavite glavni poslužitelj.
3. (opcijski) Podesite LDAP podatke za početnu replikaciju. Ovaj korak možete preskočiti, ako nemate inicijalnih podataka koje želite prenositi na poslužitelj replika sa glavnog poslužitelja.
4. (opcijski) Preselite LDAP podatke na glavni poslužitelj. Preskočite ovaj korak ako se nešto od slijedećega odnosi na vaš poslužitelj replika:
   - To je novi LDAP poslužitelj direktorija.
   - Ne sadrži podatke koje želite i dalje održavati.
5. Postavite novi poslužitelj replika.
6. Podesite glavni poslužitelj tako da ima novu repliku.
7. Pobrinite se da glavni poslužitelj dopušta ažuriranja:
   a. U iSeries Navigator, proširite sistem na kojem se izvodi glavni poslužitelj direktorija.
   b. Proširite **Mreža**.
   c. Proširite **Poslužitelji**.
   d. Kliknite na **TCP/IP**.
   e. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
   f. Ako već nije označena, označite kućicu **Omogući ažuriranja direktorija**.

Bilješka: Ove upute pretpostavljaju da su i glavni poslužitelji i replike poslužitelja na sistemima kojima upravljate sa iSeries Navigator na istom PC-u. Ako upravljate vašim sistemima sa različitih PC-a, možete se pomicati između dva PC-a da bi obavili ovaj zadatak. Ako se ili glavni ili poslužitelj replika izvode na IBM operacijskom sistemu različitom od OS/400, pogledajte dokumentaciju za tu platformu da postavite taj poslužitelj.

Postavite LDAP podatke za inicijalnu replikaciju

Možda imate podatke na glavnom LDAP poslužitelju direktorija koje želite dodati na novi poslužitelj replika. Ako to činite, najprije trebate eksportirati direktorij u neku LDIF datoteku. Dok se LDIF datoteka eksportira, morate spriječiti ažuriranje glavnog poslužitelja. To možete učiniti na jedan od slijedećih načina:

- Zaustavite LDAP poslužitelj direktorija. Ovisno o količini podataka u vašem direktoriju, ovo može zahtijevati da vaš poslužitelj ostane zaustavljen produljeni vremenski period.
- Promijenite svojstva poslužitelja tako da ažuriranja ne budu dopuštena. Time omogućujete poslužitelju da nastavi odgovarati zahtjevima za pretraživanje dok se eksportira LDIF datoteka. Ako ćete uzeti ovu opciju, slijedite ove korake:_
  1. U iSeries Navigator, proširite sistem na kojem se izvodi glavni poslužitelj direktorija.
  2. Proširite **Mreža**.
  3. Proširite **Poslužitelji**.
  4. Kliknite na **TCP/IP**.
  5. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
  6. Ako je polje **Omogući ažuriranje direktorija** označeno, skinite oznaku. Time ćete spriječiti ažuriranja direktorija dok se replikacija u potpunosti ne dovrši.
  7. Kliknite **OK**.
  8. Zaustavite, a zatim ponovo pokrenite, LDAP poslužitelj direktorija.

Nakon što zaustavite poslužitelj ili promijenite svojstva poslužitelja da ne dozvoli ažuriranja direktorija, izvedite ove poslove:

1. Eksportirajte direktorij u neku LDIF datoteku.
2. Prenesite LDIF datoteke na sistem na kojem će se izvoditi replika poslužitelja.

Nakon što je LDIF datoteka prenesena na sistem na kojem će se izvoditi replika poslužitelja, trebate unijeti podatke na repliku poslužitelja:

1. U iSeries Navigator, proširite sistem na kojem se izvodi replika poslužitelja direktorija.
2. Ako poslužitelj replika još nije zaustavljen, zaustavite ga sada. Osvježavajte status poslužitelja sve dok status ne bude **Zaustavljen**.
3. Proširite **Mreža**.
4. Proširite **Poslužitelji**.
5. Kliknite na **TCP/IP**.
6. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
7. Ako polje **Omogući ažuriranje direktorija** nije označeno, označite ga. Ovo će vam omogućiti da importirate podatke.
8. Kliknite **OK**.
9. Importirajte LDIF datoteku koju ste prenijeli u koraku 2.
10. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
11. Skinite oznaku na polju **Omogući ažuriranje direktorija**.

Premjestite LDAP podatke na glavni poslužitelj

Kad neki LDAP poslužitelj direktorija pretvorite u poslužitelj replika, podatke na njemu više ne možete ažurirati. Ako na poslužitelju kojega konfigurirate da bude replika LDAP poslužitelja direktorija imate podataka, vjerojatno ćete htjeti preseliti te podatke na glavni poslužitelj, tako da ih možete i dalje održavati. Da bi to učinili, slijedite ove korake:

1. U iSeries Navigator, proširite sistem na kojem se izvodi replika poslužitelja direktorija.
2. Proširite **Mreža**.
3. Proširite **Poslužitelji**.
4. Kliknite na **TCP/IP**.
5. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
6. Ako je polje **Omogući ažuriranje direktorija** označeno, skinite oznaku. Time ćete spriječiti ažuriranja direktorija dok se replikacija u potpunosti ne dovrši.
7. Kliknite **OK**.
8. Zaustavite LDAP poslužitelj direktorija.
9. Eksportirajte direktorij u neku LDIF datoteku.
10. Prenesite LDIF datoteke na sistem na kojem će se izvoditi glavni poslužitelj.

Nakon što je LDIF datoteka prenesena na sistem na kojem će se izvoditi glavni poslužitelj, trebate unijeti podatke na glavni poslužitelj:

1. U iSeries Navigator, proširite sistem na kojem se izvodi glavni poslužitelj direktorija.
2. Ako glavni poslužitelj direktorija još nije zaustavljen, zaustavite ga sada. Osvježavajte status poslužitelja sve dok status ne bude **Zaustavljen**.
3. Proširite **Mreža**.
4. Proširite **Poslužitelji**.
5. Kliknite na **TCP/IP**.
6. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
7. Ako polje **Omogući ažuriranje direktorija** nije označeno, označite ga. Ovo će vam omogućiti da importirate podatke.
8. Kliknite **OK**.
9. Importirajte LDIF datoteku koju ste prenijeli u koraku 10 prethodne procedure.
10. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
11. Skinite oznaku na polju **Omogući ažuriranje direktorija**.

Postavite novu repliku

Kod postavljanja novog poslužitelja replika slijedite ove korake.

Bilješka: Poslužitelj replika mora biti konfiguriran i zaustavljen prije nego što izvedete ovaj postupak.

1. U iSeries Navigator, proširite sistem na kojem se izvodi replika poslužitelja direktorija.
2. Proširite **Mreža**.
3. Proširite **Poslužitelji**.
4. Kliknite na **TCP/IP**.
5. Ako poslužitelj nije već zaustavljen, zaustavite poslužitelj sad. Osvježavajte status poslužitelja sve dok status ne bude **Zaustavljen**.
6. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
7. Kliknite na karticu **Replikacija**.
8. Izaberite **Upotreba poslužitelja replika** .
9. U polju **Ime korišteno od glavnog poslužitelja za ažuriranja**, izaberite ime za glavni poslužitelj za korištenje kada se prijavi na repliku poslužitelja kada izvodi promjene. To može biti razlikovno ime (DN) ili Kerberos korisnik.

   Ako izaberete DN:

   - Kliknite na gumb **Lozinka** pokraj polja **Ime koje koristi glavni poslužitelj za ažuriranje**. Unesite lozinku za glavni poslužitelj koja će se koristiti za prijavljivanje na poslužitelj replika kod izvođenja ažuriranja.

     Bilješka: Zapamtite lozinku i ime koje ste unijeli u koraku 9. Trebat će vam kad budete podešavali glavni poslužitelj za replikaciju.

   Ako izaberete **Dodaj Kerberos korisnika**:

   - Tražit će se od vas da unesete Kerberos ime (u obliku LDAP/*hostname*, gdje je *hostname* potpuno kvalificirano ime hosta glavnog poslužitelja) i default područje (kao ACME.COM) glavnog poslužitelja.

     Bilješka: Za korištenje Kerberos-a, morate imati Kerberos omogućen i na glavnom i na replikama poslužitelja.
10. U polju **URL glavnog poslužitelja** unesite ime glavnog poslužitelja u URL formatu. Ako vaš glavni poslužitelj koristi neki drugi port, a ne default, unesite broj toga porta kao dio URL-a.
11. Kliknite na karticu **Baza podataka**/**Sufiksi**. Ako sufiks koji želite replicirati nije na listi, dodajte ga.
12. (opcijski) Ako želite koristiti Sloj sigurnih utičnica (SSL) kod replikacije, poslužite se Upraviteljem digitalnih certifikata i aktivirajte SSL za taj poslužitelj. Upravitelj digitalnih certifikata možete pokrenuti s kartice **Mreža**. Dodatne informacije o aktiviranju SSL na poslužitelju direktorija možete vidjeti u “Omogućite SSL na LDAP poslužitelju direktorija” na stranici 15.
13. Kliknite **OK**.

Postavite glavni poslužitelj za novu repliku

Kod postavljanja glavnog poslužitelja za novu repliku slijedite ove korake.

Bilješka: Vaš glavni poslužitelj mora biti konfiguriran i pokrenut prije izvođenja ovog postupka.

1. U iSeries Navigator, proširite sistem na kojem se izvodi glavni poslužitelj direktorija.
2. Proširite **Mreža**.
3. Proširite **Poslužitelji**.
4. Kliknite na **TCP/IP**.
5. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
6. Ako već nije označena, označite kućicu **Omogući ažuriranja direktorija**.
7. Kliknite **OK**.
8. Zaustavite, a zatim ponovo pokrenite LDAP poslužitelj direktorija. Osvježavajte status poslužitelja sve dok status ne bude **Pokrenut**.
9. Desnom tipkom miša ponovo kliknite na **Direktorij** i izaberite **Svojstva**.
10. Kliknite na karticu **Replikacija**. iSeries Navigator će vas možda upitati da unesete podatke o vezi. Unesite te informacije i zatim kliknite **OK**.

11. Kliknite na **Dodaj**.
12. U polju **Poslužitelj** unesite ime poslužitelja replika u URL formatu.
13. Izaberite vašu metodu provjere ovlaštenja.

    Za korištenje razlikovnog imena (DN) i lozinke:

    a. Izaberite **Koristi DN i lozinku**.
    b. U polju **Poveži kao** unesite ime koje ste naveli u koraku 9 na stranici 23 kad ste postavili poslužitelj replika.
    c. Kliknite na **Lozinka** i unesite lozinku koju ste odredili u koraku 9 na stranici 23 kad ste postavili poslužitelj replika.

    Za upotrebu Kerberos-a:

    - Izaberite **Koristite Kerberos račun glavnog poslužitelja**. Glavni poslužitelj će koristiti svoje Kerberos principal ime za provjeru autentičnosti.

      Bilješka: Za korištenje Kerberos-a, morate imati Kerberos omogućen i na glavnom i na replikama poslužitelja.
14. Ako želite koristiti Sloj sigurnih utičnica (SSL) kod replikacije, poslužite se Upraviteljem digitalnih certifikata i aktivirajte SSL za taj poslužitelj. Upravitelj digitalnih certifikata možete pokrenuti s kartice **Mreža**. Za dodatne informacije o omogućavanju SSL-a na poslužitelju direktorija, pogledajte “Omogućite SSL na LDAP poslužitelju direktorija” na stranici 15.
15. Ako replika poslužitelja ne koristi default port, specificirajte broj porta u polju **Port**.
16. Ako ne želite ažurirati poslužitelj replika svaki puta kad se neki upis na glavnom poslužitelju promijeni, izaberite **Time**. Zatim navedite kako često želite da glavni poslužitelj ažurira repliku.
17. Kliknite **OK**.
18. Kliknite na karticu **Baza podataka**/**Sufiksi**. Ako sufiks koji želite replicirati nije na listi, dodajte ga.
19. Omogućite ažuriranja direktorija na svakom poslužitelju replika:
    a. U iSeries Navigator, proširite sistem na kojem se izvodi replika poslužitelja direktorija.
    b. Proširite **Mreža**.
    c. Proširite **Poslužitelji**.
    d. Kliknite na **TCP/IP**.
    e. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
    f. Ako polje **Omogući ažuriranje direktorija** nije označeno, označite ga.
    g. Kliknite **OK**.
20. Ako nisu pokrenuti svi poslužitelji replika, pokrenite ih sada.

Bilješka: Nijedan poslužitelj ne može biti istovremeno i glavni poslužitelj i poslužitelj replika.

Izdajte informacije poslužitelju direktorija

Možete konfigurirati vaš sistem da izdaje određene informacije u LDAP poslužitelj direktorija u istom ili različitom sistemu. OS/400 automatski izdaje ove informacije LDAP poslužitelju direktorija kad koristite iSeries Navigator da izmijenite ove informacije na OS/400. Informacije koje možete izdati uključuju sistem (sistemi i pisači), dijeljenja pisača, korisničke informacije i TCP/IP politiku Kvaliteta usluga. Za više informacija o Kvaliteti usluga, pogledajte LDAP konfiguracija i QoS .

Ako nadređeni DN kojem se izdaju podaci ne postoji, Usluge Direktorija ga automatski kreira. Možda ste također instalirali druge OS/400 aplikacije koje izdaju informacije u LDAP direktorij. Uz to, možete pozivati aplikativna programska sučelja (API) iz svojih programa i izdavati druge tipove podataka u LDAP direktorij.

Bilješke:

1. Kada konfigurirate OS/400 za izdavanje informacijskog tipa Korisnici u LDAP poslužitelj direktorija, on automatski eksportira unose iz sistemskog distribucijskog direktorija u LDAP poslužitelj. Da bi to učinio, on koristi QGLDSSDD_modrdn aplikativno programsko sučelje (API). Time i LDAP direktorij ostaje sinkroniziran s promjenama napravljenim u sistemskom distribucijskom direktoriju. Za informacije o

QGLDSSDD API-ju, pogledajte predmetOS/400 Usluge Direktorija pod Programiranje u iSeries Informativni Centar. Dostupne informacije obuhvaćaju slijedeće:
- Kako ručno pozvati ovaj API.
- Kako spriječiti eksportiranje pojedinih korisnika na LDAP poslužitelj.
- Kako on eksportira polja sistemskog distribucijskog direktorija.

2. Kada konfigurirate OS/400 za izdavanje informacijskog tipa Sistem u LDAP poslužitelj direktorija i selektirate jedan ili više pisača za izdavanje, sistem će automatski držati LDAP direktorij sinkroniziran sa promjenama koje su načinjene tim pisačima u sistemu. Informacije o pisaču koje mogu biti izdane uključuju lokaciju pisača, njegovu brzinu u stranicama po minuti, da li podržava dupleks i kolor, njegov tip i model te njegov opis. Ova informacija dolazi od opisa uređaja na sistemu koji se izdaje. U mrežnoj okolini, korisnici mogu koristiti ovu informaciju da pomognu izabrati pisač.
3. Možete također izdati OS/400 informacije u LDAP poslužitelj direktorija koje nisu u OS/400 ako konfigurirate taj poslužitelj da koristi IBM shemu.

Da konfigurirate vaš sistem da izdaje OS/400 informacije na LDAP poslužitelj direktorija, načinite ove korake:

1. U iSeries Navigator, desnom tipkom miša kliknite na vaš sistem i izaberite **Svojstva**.
2. Kliknite na karticu **Usluge Direktorija**.
3. Kliknite na tipove podataka koje želite objavljivati.

   Napomena:

   Ako planirate objavljivati više od jednog tipa podataka u istu lokaciju, možete uštedjeti na vremenu tako da izaberete više tipova podataka i konfigurirate ih istovremeno. Navigator Operacija će potom koristiti vrijednosti koje unesete kad konfigurirate jedan tip podataka kao default vrijednosti kad konfigurirate sve kasnije tipove podataka.
4. Kliknite **Detalji**.
5. Kliknite **Izdavanje sistemskih informacija** kućicu .
6. Navedite **Metodu provjere ovlaštenja** koju želite da poslužitelj koristi, kao i prikladne informacije o provjeri ovlaštenja.
7. Kliknite gumb **Uredi** pokraj polja**(Aktivan) Poslužitelj direktorija**. U dijalog koji se pojavi, unesite ime LDAP poslužitelja direktorija gdje želite izdati OS/400 informacije, tada kliknite **OK**.
8. U polju **Pod DN**, unesite nadređeno razlikovno ime (DN) gdje želite da informacije budu dodane u poslužitelj direktorija.
9. Ispunite polja u okviru **Veza poslužitelja** koja su prikladna vašoj konfiguraciji.

   Bilješka: Za izdavanje OS/400 informacija poslužitelju direktorija korištenjem SSL-a ili Kerberos-a, prvo trebate konfigurirati poslužitelj da koristi odgovarajući protokol. Pogledajte “Koristite Kerberos provjeru autentičnosti s poslužiteljem LDAP direktorija” na stranici 37 za više informacija o SSL i Kerberos.
10. Ako vaš poslužitelj ne koristi default port, unesite ispravni broj porta u polju **Port**.
11. Kliknite **Provjeri** da osigurate da nadređeni DN postoji na poslužitelju i da je informacija o vezi ispravna. Ako staza direktorija ne postoji, pojavit će se dijalog iz kojega ju možete kreirati.

    Bilješka: Ako viši DN ne postoji, a ne kreirate ga, onda objavljivanje neće biti uspješno.
12. Kliknite **OK**.

Bilješka: Možete također izdati OS/400 informacije u LDAP poslužitelj direktorija koji je na različitoj platformi. Morate izdati informacije o korisniku i sistemu poslužitelju direktorija koji koristi shemu koja je kompatibilna shemi Usluga Direktorija. IBM SecureWay definicije sheme Direktorija, koje uključuju iSeries Usluge Direktorija mogu se naći na Web stranici Usluge Direktorija.

Morate izdati dijeljenje pisača u u poslužitelj direktorija koji podržava Microsoftovu shemu Aktivni Direktorij. Izdavanje dijeljenja pisača u Aktivni Direktorij dopušta korisnicima da konfiguriraju iSeries pisače direktno sa svojeg Windows 2000 desktopa sa Windows 2000 čarobnjakom Dodaj pisač. Da bi to učinili u čarobnjaku Dodaj pisač, specificirajte da želite naći pisač u Windows 2000 Aktivnom direktoriju.

API za izdavanje OS/400 informacija poslužitelju direktorija

Usluge Direktorija daje ugrađenu podršku za izdavanje korisničkih i sistemskih informacija. Ove stavke su popisane na stranici **Usluge Direktorija** u dijalogu sistemska **Svojstva**. Možete koristiti konfiguraciju LDAP poslužitelja i izdavanje API za omogućavanje OS/400 programa koje pišete za izdavanje drugih tipova informacija. Ovi tipovi informacija se onda pojavljuju na stranici**Usluge Direktorija** isto tako. Kao i korisnici i sistemi, oni su inicijalno onemogućeni i konfigurirate ih korištenjem istog postupka. Program koji dodaje podatke u LDAP direktorij se naziva izdavački agent. Tip podataka koji se objavljuje onako kako se pojavljuje na stranici **Usluge Direktorija**, naziva se ime agenta.

Slijedeći API-ji će vam omogućiti da objavljivanje ugradite u svoje programe:

QgldChgDirSvrA
: Aplikacija koristi CSVR0500 format za inicijalno dodavanje imena agenta koje je označeno kao onemogućeni unos. Upute za korisnike aplikacije bi ih trebale uputiti da koriste iSeries Navigator za odlazak na stranicu svojstava Usluga Direktorija i konfiguriranje izdavačkog agenta. Primjeri imena agenata su imena agenata sistema i korisnika automatski dostupna na stranici **Usluge direktorija**.

QgldLstDirSvrA
: Koristite LSVR0500 format ovog API-ja da popišete trenutno dostupne agente na vašem sistemu.

QgldPubDirObj
: Ovaj API upotrijebite za objavljivanje podataka.

Za detaljne informacije o ovim API-jima, pogledajte Lightweight Directory Access Protocol (LDAP) predmet pod Programiranje u iSeries Informativni Centar.

Specificirajte poslužitelj za referale direktorija

Ako dodjeljujete referalne poslužitelje nekom poslužitelju direktorija, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom kliknite na **Direktorij**, zatim izaberite **Svojstva**.
5. Kliknite **Dodaj**.
6. Na upit odredite ime referalnog poslužitelja u URL formatu. U nastavku su primjeri prihvatljivih URL-a za LDAP:
   - ldap://test.server.com
   - ldap://test.server.com:400
   - ldap://9.9.99.255

   Bilješka: Ako referalni poslužitelj ne koristi default port, specificirajte ispravan broj porta kao dio URL-a, kako je port 400 specificiran u drugom primjeru iznad.
7. Kliknite **OK**.

Dodajte sufikse poslužitelju LDAP direktorija

Dodavanje sufiksa u LDAP poslužitelj direktorija omogućava poslužitelju da upravlja tim dijelom stabla direktorija.

Bilješka: Ne možete dodati sufiks koji je pod drugim sufiksom već na poslužitelju. Na primjer, ako su o=ibm, c=us bili sufiks na vašem poslužitelju, ne možete dodati ou=rochester, o=ibm, c=us.

Ako dodajete sufiks u poslužitelj direktorija, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.

5. Kliknite na karticu **Baza podataka**/**Sufiksi**.
6. U polju **Novi sufiks** upišite ime novoga sufiksa.
7. Kliknite na **Dodaj**.
8. Kliknite **OK**.

Bilješka: Dodavanje sufiksa usmjerava poslužitelj na dio direktorija, ali ne kreira objekte. Ako objekt koji odgovara novom sufiksu nije prethodno postojao, morate ga kreirati kao što bi kreirali bilo koji drugi objekt.

Uklonite sufikse s poslužitelja direktorija

Ako brišete sufiks iz LDAP poslužitelja direktorija, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite na karticu **Baza podataka**/**Sufiksi**.
6. Kliknite na sufiks koji želite brisati da ga izaberete.
7. Kliknite **Ukloni**.

Bilješka: Sufiks možete brisati, a da pritom ne morate brisati objekte direktorija koji su ispod njega. Podaci time postaju nedostupni iz poslužitelja direktorija. Ipak, možete kasnije vratiti pristup podacima dodavanjem natrag sufiksa.

Spremanje i vraćanje Usluge Direktorija informacija

Usluge Direktorija pohranjuju informacije na slijedećim lokacijama:

- Knjižnica baze podataka (QUSRDIRDB po defaultu), koja sadržava sadržaj poslužitelja direktorija.
- QDIRSRV2 knjižnica, koja se koristi za pohranu informacija o izdavanju.
- QUSRSYS knjižnica, koja pohranjuje razne stavke u objektima koji počinju sa QGLD (specificirajte QUSRSYS/QGLD* da ih spremite).
- Ako konfigurirate poslužitelj direktorija da zapisuje promjene u direktoriju, koristi se knjižnica baza nazvana QUSRDIRCL.

Ako se sadržaj direktorija redovno mijenja, trebate redovno pohranjivati knjižnicu baza i objekte u njoj. Podaci o konfiguraciji se pohranjuju i u slijedećem direktoriju:

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

Trebali bi spremiti i datoteke u tom direktoriju svaki puta kad mijenjate konfiguraciju ili koristite PTF-ove.

Pogledajte Backup i obnavljanje, SC41-5304 za informacije o spremanju i vraćanju OS/400 podataka.

Upravljajte vlasništvom i pristupom podacima direktorija

Upravljanje vlasništvom i pristupom podacima direktorija obuhvaća slijedeće poslove:
- “Radite sa svojstvima vlasništva objekata direktorija”
- “Rad s listama kontrole pristupa (ACL)” na stranici 28
- “Radite s ACL grupama” na stranici 28

Radite sa svojstvima vlasništva objekata direktorija

Ako određujete vlasnička svojstva objekata direktorija, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.

4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Ovlaštenje**.

   Ako već niste spojeni na poslužitelj direktorija, pojavit će se dijalog **Spajanje na poslužitelj direktorija**. Spojite se kao poslužitelj administrator ili kao vlasnik objekta sa čijim vlasničkim svojstvima želite raditi.
5. Iz stabla direktorija izaberite objekt sa čijim vlasničkim svojstvima želite raditi, a zatim kliknite **OK**.

Rad s listama kontrole pristupa (ACL)

Rad s listama kontrole pristupa (ACL) obuhvaća dodjelu izričitih i uključenih ACL-a objektima direktorija, dodavanje korisnika u ACL-e, brisanje korisnika iz ACL-a i pregledavanje objekata direktorija. Primijetite da počevši s V5R1 Usluge Direktorija podržava novi ACL model, tako da čak i ako ste koristili ACL-ove ranije, možda ćete se željeti ponovo upoznati sa njima.

Za rad sa ACL-ima poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Ovlaštenje**.

   Ako već niste spojeni na poslužitelj direktorija, pojavit će se dijalog **Spajanje na poslužitelj direktorija**. Spojite se kao poslužitelj administrator ili kao vlasnik objekta sa čijom ACL listom želite raditi.
5. Iz stabla direktorija izaberite objekt sa čijom ACL listom želite raditi, a zatim kliknite **OK**.
6. Kliknite karticu **ACL**.

Radite s ACL grupama

Za rad sa ACL grupama, poduzmite ove korake:
1. U iSeries Navigator, izaberite **Mreža**.
2. Izaberite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **ACL Grupe**.

Radite s administrativnim pristupom za ovlaštene korisnike

| Počevši s V5R2, možete dodijeliti administratorski pristup korisničkom profilima kojima je dan pristup | identifikatoru funkcije (ID) Administratora usluga direktorija (QIBM_DIRSRV_ADMIN).

| Na primjer, ako je korisničkom profilu JOHNSMITH dodijeljen pristup funkcijskom ID-u Administratora usluga | direktorija i opcija Dodijeli za administratorski pristup autoriziranom korisniku je selektirana u dijalogu | svojstava Direktorija, tada JOHNSMITH profil ima LDAP administratorsko ovlaštenje. Kad se ovaj profil | koristi za povezivanje na poslužitelj direktorija korištenjem slijedećeg DN-a, os400-| profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com, korisnik ima administratorsko ovlaštenje. | Sufiks sistemskih objekata u ovom primjeru je os400-sys=systemA.acme.com. Za više informacija o | projiciranim korisnicima, pogledajte “Projicirana pozadina operacijskog sistema” na stranici 38.

| Da bi selektirali ovu opciju, slijedite ove korake:
| 1. U iSeries Navigator, proširite **Mreža**.
| 2. Proširite **Poslužitelji**.
| 3. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
| 4. Na **Općenito** kartici pod **Administratorske informacije**, izaberite opciju **Dodijelite administratorski pristup autoriziranim korisnicima**.

| Za postavljanje funkcijskog ID-a ovlaštenja Administrator Usluge Direktorija u korisničkom profilu, slijedite | ove korake:
| 1. U iSeries Navigator, Desnom tipkom miša kliknite na ime sistema i izaberite **Administracija Aplikacije**.
| 2. Kliknite na karticu **Host Aplikacije**.
| 3. Proširite **Operacijski Sistem/400**.

4. Kliknite na **Administrator Usluga Direktorija** da bi osvijetlili opciju.
5. Kliknite na gumb **Prilagodi** .
6. Proširite **Korisnici**, **Grupe**, ili **Korisnik nije u grupi**, ovisno o tome koji odgovara korisniku kojeg želite.
7. Izaberite korisnika ili grupu koji će se dodati na listu **Dozvoljen pristup** .
8. Kliknite na gumb **Dodaj** .
9. Kliknite **OK** za spremanje promjena.
10. Kliknite **OK** na dijalogu **Administracija Aplikacija** .

Pratite pristup i promjene u LDAP direktoriju

Možete htjeti pratiti pristup i promjene u vašem LDAP direktoriju. Možete koristiti dnevnik promjena LDAP direktorija da pratite promjene u direktoriju. Dnevnik promjena se nalazi pod posebnim sufiksom cn=changelog. Pohranjen je u knjižnici QUSRDIRCL.

Da aktivirate dnevnik promjena, slijedite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite na karticu **Baza podataka/Sufiksi**.
6. Izaberite **Zapiši promjene direktorija**.
7. (opcijski) U **Maksimum unosa** navedite maksimalan broj upisa koji se čuvaju u dnevniku promjena.

   Bilješka: Iako je ovaj parametar opcijski, svakako razmotrite određivanje maksimalnog broja slogova. Ako ne navedete maksimalan broj slogova u dnevniku, u njemu će se čuvati svi podaci o promjenama i on može postati ogroman.

Klasa objekta changeLogEntry se koristi za prikazivanje promjena napravljenih u poslužitelju direktorija. Skup promjena je zadan poredanim skupom svih slogova unutar spremnika u dnevniku promjena kako je definirano klasom changeNumber. Informacije dnevnika promjena su samo za čitanje.

Svaki korisnik na listi kontrole pristupa za sufiks cn=changelog može pretraživati slogove u dnevniku promjena. Trebali bi izvoditi samo traženja na sufiksu dnevnika promjena cn=changelog. Nemojte pokušavati dodavati, brisati ili mijenjati nešto u sufiksu dnevnika promjena, čak i ako imate ovlaštenje za to. To može uzrokovati nepredviđene rezultate.

Primjer:

Primjer što slijedi koristi ldapsearch pomoćni program s naredbene linije za učitavanje svih slogova dnevnika promjena na poslužitelju:

```
ldapsearch -h ldaphost -D cn=admininistrator -w password -b cn=changelog  (changetype=*)
```

Omogućite reviziju objekta za poslužitelj direktorija

Usluge Direktorija podržava OS/400 sigurnosnu reviziju. Ako sistemska vrijednost QAUDCTL ima specificirano *OBJAUD, možete omogućiti reviziju objekta kroz iSeries Navigator.

Da omogućite reviziju objekta za Usluge Direktorija, slijedite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite karticu **Revizija**.
6. Izaberite postavke revizije koje želite koristiti za vaš poslužitelj.

Promjene u postavkama revizije će nastati čim kliknete **OK**. Nema potrebe da ponovo pokrećete LDAP poslužitelj direktorija. za više informacija, pogledajte “Usluge Direktorija sigurnost” na stranici 36

Prilagodite performanse poslužitelja LDAP direktorija

Performanse svog LDAP poslužitelja direktorija možete podesiti tako da promijenite nešto od slijedećeg:
- Veličinu traženja
- Maksimalno vrijeme dozvoljeno za traženje
- Poslužiteljeve transakcijske postavke
- Broj veza na bazu podataka i poslužiteljskih niti

Ako podešavate vrijednosti performansi poslužitelja direktorija, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite karticu **Performanse**.

Možete također prilagoditi performanse poslužitelja direktorija mijenjanjem broja veza na bazu podataka i poslužiteljskih niti koje poslužitelj koristi. Ako mijenjate ovu vrijednost, slijedite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite karticu **Baza podataka/Sufiksi**.

Poglavlje 5. Usluge Direktorija koncepti i referentne informacije

Sljedeće informacije o konceptu i uputama će vam pomoći da naučite kako raditi sa LDAP poslužiteljem Usluga Direktorija:

Ako trebate informacije o LDAP osnovama i planiranju LDAP poslužitelja, također pogledajte Poglavlje 3, "Započnite s Usluge Direktorija" na stranici 7.

LDAP liste kontrole pristupa (ACL)

U mnogim slučajevima, vjerojatno nećete trebati ograničavati pristup podacima na vašem poslužitelju LDAP direktorija. Na primjer, LDAP poslužitelj na intranetu vaše tvrtke može sadržavati telefonski imenik zaposlenika u tvrtki. Vjerojatno želite da svi zaposlenici mogu gledati podatke u tom imeniku.

Ipak, predsjednica vašeg poduzeća ne želi da svi zaposlenici mogu pristupiti njenom broju telefona. U tom slučaju, kreirat ćete **listu kontrole pristupa (ACL)**. S ovom ACL listom možete ograničiti pristup njenom upisu na poslužitelju samo na one zaposlene od kojih predsjednica želi primati pozive.

S ACL-ima možete nadzirati tko ima ovlaštenje za dodavanje i brisanje objekata u imeniku. Možete navesti i imaju li korisnici mogućnost čitanja, pisanja, pretraživanja i usporedbe atributa imenika. ACL-i mogu biti naslijeđeni ili eksplicitni. To jest, ACL-e možete koristiti na jedan od slijedećih načina:

- Eksplicitno odrediti ACL za neki određeni objekt.
- Odrediti da neki objekti nasljeđuju ACL od objekata koji su viši u hijerarhiji LDAP direktorija.

Možda predsjednica u prethodnom primjeru nije željela da svi zaposlenici mogu pristupiti njenom broju telefona. Ona je, međutim, htjela da rukovoditelji imaju pristup tom broju. U takvom slučaju, možete upotrijebiti **ACL grupu** i pojednostavniti davanje ovlaštenja rukovoditeljima. ACL grupe vam omogućuju davanje pristupa određenim grupama korisnika umjesto davanja ovlaštenja pojedinačno. Ovo je naročito korisno ako ista grupa ljudi treba pristup na više skupova objekata. Ako isti rukovoditelji koji imaju pristup broju telefona predsjednice, na primjer, kasnije trebaju pristup unosima plaća, možete ponovo koristiti ACL grupu.

ACL modeli

Sve verzije Usluga Direktorija podržavaju model dozvole na razini klase pristupa. U ovom modelu, svaki tip LDAP atributa ima klasifikaciju Normalno, Osjetljivo ili Kritično. Silogičke datoteke atributa nadziru ova razvrstavanja. Kad dodate korisnika ACL-u objekata, specificirate koje klasifikacije korisnik može čitati, pisati, tražiti i uspoređivati. U većini situacija, telefonski broj će biti klasificiran kao atribut Normalno. Zato, da date rukovoditeljima u gornjem primjeru pristup broju telefona predsjednice, trebate im dati pristup čitanja atributima Normalno u predsjedničinom objektu direktorija. Oni i dalje neće moći pristupiti informacijama Osjetljivo i Kritično. Sve verzije Usluga Direktorija podržavaju postavljanje dozvola na razini klase pristupa.

Usluge Direktorija također podržava model dozvola razine atributa. Pod tim modelom, možete specificirati ovlaštenja za čitanje, pisanje, pretraživanje i uspoređivanje za određene atribute, bez obzira na njihovu klasu pristupa. Razmotrite opet prethodni primjer. Pod modelom dozvola razine atributa, možete dati rukovoditeljima pristup čitanja za atribut telephoneNumber, čak i ako općenito nemaju pristup atributima Normalno.

Model dozvola razine atributa je kompatibilan samo s SecureWay Usluge Direktorija verzija 3.2 i višim poslužiteljima. Po defaultu ovo nije omogućeno. Opciju omogućavanja ovoga imate kad radite s ACL-ovima. Nakon što je omogućen, model može biti onemogućen samo rekonfiguriranjem poslužitelja i vraćanjem baze podataka direktorija. Prije nego odlučite omogućiti ovaj model, budite svjesni da njime nećete moći upravljati s bilo kojeg LDAP V2 klijenta (uključujući pred-V5R1 verzije iSeries Navigator) i da pokušaj da to učinite može oštetiti ACL unose.

Posebne ACL vrijednosti

Inicijalno, svi objekti u poslužitelju direktorija Usluga Direktorija imaju ACL koji sadrži posebnu ACL grupu, CN=Anybody, koja obuhvaća sve korisnike direktorija. Po defaultu, ova grupa ima pristup za čitanje, pretraživanje i usporedbu za sve atribute klase Normalno za sve objekte.

Možda želite da neki objekti imaju iste dozvole za pristup za sve korisnike koji se vežu na poslužitelj preko veze koja nije anonimna. U tu svrhu upotrebite posebnu grupu lista za kontrolu pristupa (ACL) cn=Authenticated.

Ako određujete koje dozvole pristupa neki objekt ima sam za sebe, možete upotrebiti posebni DN cn=this. Time omogućujete podređenim upisima koji nasljeđuju svoje ACL-e, da automatski budu ovlašteni za izvođenje operacija na svojim vlastitim objektima.

Dodatne informacije

Da upravljate ACL-ima kroz iSeries Navigator, ne trebate znati detalje o tome kako Usluge Direktorija implementiraju ACL-ove. Ipak, ako želite specificirati atribute povezane s ACL-om kod korištenja LDIF datoteka ili želite koristiti ACL-ove sa pomoćnim programima LDAP linije za naredbe, trebat ćete se upoznati sa atributima koje ACL-ovi koriste. Za informacije o ACL atributima, pogledajte referentni dokument Liste kontrole pristupa  iz IBM SecureWay dokumentacija Alata za upravljanje direktorijima  .

Ako trebate informacije o postavljanju i promjeni ACL-a i ACL grupa, slijedite ove veze:

“Rad s listama kontrole pristupa (ACL)” na stranici 28
“Radite s ACL grupama” na stranici 28

LDAP format izmjenjivanja podataka

LDAP format izmjenjivanja podataka (LDIF) daje vam jednostavan način prijenosa informacija direktorija između LDAP poslužitelja direktorija. LDIF datoteke drže upise o LDAP direktorijima u jednostavnom tekstualnom formatu. Format LDIF datoteka koje koristi poslužitelj direktorija se malo promijenio počevši sa izdanjem V4R5 Usluga Direktorija. LDIF datoteke se sastoje od niza redaka koji opisuju slog direktorija ili skup promjena u slogu direktorija. Ne mogu opisivati i jedno i drugo.

Općeniti format LDIF sloga je:

```
verzija: 1
dn: razlikovno ime
attrtype1: attrvalue1
...
```

gdje je:

- *verzija* prikaz verzije formata LDIF datoteke. Broj verzije mora biti 1. ako broj verzije nedostaje, smatra se da je LDIF datoteka u starijem LDIF formatu datoteke. Kad je LDIF datoteka verzija 1, sadržaj MORA biti enkodiran u UTF-8.
- *razlikovno ime* je prepoznatljivo jedinstveno ime sloga direktorija
- *attrtype1* je tip LDAP atributa (kao što je cn ili ou)
- *attrvalue1* je vrijednost atributa

Svaki upis može imati nekoliko atributa. Svaki atribut se pojavljuje na zasebnom retku. Ako je neki atribut dulji od jednog reda, može se nastaviti na slijedećem retku, a ispred njega dolazi znak za razmak ili blok.

Prazni redovi razdvajaju višestruke upise unutar iste LDIF datoteke. Svaka linija koja počinje ljestvama (#) je linija komentara i mora se ignorirati u rasčlambi LDIF datoteke.

Svako razlikovno ime i vrijednost atributa koja zadovoljava jedan od slijedećih uvjeta trebaju biti enkodirani u bazi 64:
- Sadržava oznaku povratka ili novoga reda.
- Počinje dvotočkom (:), SPACE, ili manje od (<).
- Završava razmakom.

Atributi enkodirani na bazi 64 se određuju upotrebom dvaju dvotočki između imena atributa i njegove vrijednosti.

Vanjske reference su URL formatu file:// . Trebali bi biti dvotočka i znak manje od (:<) između tipa atributa i vanjske referentne vrijednosti.

Evo nekih primjera LDIF datoteka:

Primjer 1: Jednostavna LDIF datoteka sa dva sloga

```
verzija: 1
   dn: cn=Barbara Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: osoba
   objectclass: organizationalPerson
   cn: Barbara Jensen
   cn: Barbara J Jensen
   cn: Babs Jensen
   sn: Jensen
   uid: bjensen
   telephonenumber: +1 408 555 1212
   opis: Veliki obožavatelj jedrenja.

   dn: cn=Bjorn Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: osoba
   objectclass: organizationalPerson
   cn: Bjorn Jensen
   sn: Jensen
   telephonenumber: +1 408 555 1212
   opis:Babs je veliki obožavatelj jedrenja i puno putuje u
   potrazi za savršenim uvjetima jedrenja.
   title:Direktor proizvodnje, Odjel štapova i kolutova
```

Primjer 2: Datoteka koja sadrži vrijednost enkodiranu na bazi 64

```
verzija: 1
   dn: cn=Gern Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: osoba
   objectclass: organizationalPerson
   cn: Gern Jensen
   cn: Gern O Jensen
   sn: Jensen
```

```
   uid: gernj
   telephonenumber: +1 408 555 1212
   opis:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvdSBhcmUhICBUaGlzIHZhbHVlIGlzIGJ
    hc2UtNjQtZW5jb2RlZCBiZWNhdXNlIGl0IGhhcyBhIGNvbnRyb2wgY2hhcmFjdGVyIGluIGl0ICh
    hIENSKS4NICBCeSB0aGUgd2F5LCB5b3Ugc2hvdWxkIHJlYWxseSBnZXQgb3V0IG1vcmUu
```

Primjer 3: Datoteka koja sadrži niz slogova koji se mijenjaju i komentare

Bilješka: LDIF datoteke sa slogovima promjena se ne može importirati izravno na poslužitelj. Ipak, podržani su od pomoćnih programa LDAP ljuske.

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

   # Brisanje postojećeg sloga
   dn: cn=Robert Jensen, ou=Rochester, o=Big Company, c=US
   changetype: delete

   # Promijenite relativno razlikovno ime unosa
   dn: cn=Paul Jensen, ou=Rochester, o=Big Company, c=US
   changetype: modrdn
   newrdn: cn=Paula Jensen
   deleteoldrdn: 1
```

Poredak upisa u LDIF datoteci je važan. U cilju uspješnog dodavanja nekog sloga navedenog u LDIF datoteci u LDAP direktorij, prvo mora u prostoru za ime direktorija postojati njegov glavni ili viši upis. U gornjem primjeru se drugi i treći slog ne bi mogli dodati kad ne bi postojao prvi slog.

Slično tomu, ako želite importirati LDIF datoteku na poslužitelj koji podržava izvjesne sufikse, LDIF datoteka mora imati slogove za te sufikse. Na primjer, kad bi vaš poslužitelj imao sufiks ou=Rochester, o=Big Company, c=US, LDIF datoteka prikazana gore bi se mogla importirati. No, ako bi vaš poslužitelj umjesto toga imao sufiks o=Big Company, c=US, morate imati slog za taj sufiks najprije određen u LDIF datoteci, kako je ovdje prikazano:

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

Format i sadržaj LDIF datoteke se određuju shemom na poslužitelju iz kojega se eksportiraju. LDIF datoteku možete importirati na bilo koji LDAP poslužitelj koji koristi identičnu shemu kao i poslužitelj sa kojega se datoteka eksportira. LDAP poslužitelji različitih prodavača koriste različite sheme (s različitim klasama objekata i atributima). Stoga ponekad nećete moći LDIF datoteku kreiranu na jednom poslužitelju importirati na drugi poslužitelj.

Zahtjev za komentar (RFC) na LDIF specifikacijama datoteke je dostupan na sljedećem URL-u:

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

Srodni postupci:

“Importirajte LDIF datoteku” na stranici 20
“Eksportirajte LDIF datoteke” na stranici 20

Pitanja podrške nacionalnim jezicima (NLS)

Počevši s V4R5, i OS/400 LDAP poslužitelj Usluga Direktorija i OS/400 LDAP klijent su bazirani na LDAP Verzija 3. Budite svjesni slijedećih NLS razmatranja:

- Podaci se prenose između LDAP poslužitelja i klijenata u UTF-8 formatu. Dopušteni su svi ISO 10646 znakovi.
- LDAP poslužitelj Usluga Direktorija koristi UTF-16 način mapiranja za pohranu podataka u bazu podataka.
- Poslužitelj i klijent provode usporedbe nizova bez obzira na veličinu slova. Algoritmi velikih slova neće biti ispravni za sve jezike (lokalizacije).

Za više informacija o UCS-2, pogledajte predmet Globalizacija pod Planiranje u iSeries Informativni Centar.

Vlasništvo nad objektima LDAP direktorija

Svaki objekt u LDAP direktoriju ima najmanje jednog vlasnika. Vlasnici objekata imaju tu moć da mogu brisati objekte. Vlasnici i administrator poslužitelja su jedini korisnici koji mogu mijenjati vlasnička svojstva i listu kontrole pristupa (ACL) objekta. Vlasništvo nad objektom može biti naslijeđeno ili eksplicitno. To jest, ako dodjeljujete vlasništvo, možete napraviti jednu od slijedećih stvari:

- Eksplicitno odrediti vlasništvo nad pojedinim objektom.
- Odrediti da neki objekti nasljeđuju vlasnike od objekata koji su viši u hijerarhiji LDAP direktorija.

Usluge Direktorija dopušta specificiranje višestrukih vlasnika za isti objekt. Možete također specificirati da objekt posjeduje samog sebe. Da to učinite uključite poseban DN cn=this u listi vlasnika objekta. Na primjer, pretpostavite da objekt cn=A ima vlasnika cn=this. Svaki korisnik će imati vlasnički pristup objektu cn=A, ako se spoji na poslužitelj kao cn=A.

Srodni postupci:

"Radite sa svojstvima vlasništva objekata direktorija" na stranici 27

LDAP referali direktorija

Referali dozvoljavaju da LDAP poslužitelji direktorija rade u timovima. Ako DN koji klijent zahtijeva nije u jednom direktoriju, poslužitelj može automatski poslati (uputiti) zahtjev na neki drugi LDAP poslužitelj.

Usluge Direktorija vam omogućuju da koristite dva različita tipa referala (preporučitelja ili upućivača). Možete odrediti i default referalne poslužitelje, kamo će LDAP poslužitelj klijente upućivati svaki puta kad DN nije u direktoriju. Možete također koristiti vašeg LDAP klijenta da dodate unose poslužitelju direktorija koji ima objectClass referal. Ovo vam omogućuje da odredite referalne poslužitelje koji se temelje pojedinim DN koje neki klijent zahtijeva.

Bilješka: Sa Uslugama Direktorija, referal objekti moraju sadržavati samo razlikovno ime (dn), objectClass (objectClass), i referal (ref) atribut. Pogledajte "ldapsearch servisni program" na stranici 50 primjer koji ilustrira ovo ograničenje.

Referalni poslužitelji su vrlo srodni s replika poslužiteljima. Pošto se podaci na replika poslužiteljima ne mogu mijenjati sa klijenata, replika upućuje sve zahtjeve za promjenu podataka u direktoriju glavnom poslužitelju.

Transakcije

Možete konfigurirati poslužitelj LDAP direktorija vašeg sustava da dopusti klijentima korištenje transakcija. Transakcija je grupa operacija LDAP direktorija koje se tretiraju kao jedna jedinica. Nijedna od pojedinačnih LDAP operacija koje čine transakciju nisu trajne dok se sve operacije u transakciji ne dovrše uspješno i transakcija je predana. Ako bilo koja operacija ne uspije ili je transakcija opozvana, ostale operacije se poništavaju. Ova sposobnost može pomoći korisnicima da LDAP operacije budu organizirane. Na primjer,

korisnik može postaviti transakciju na klijenta koji će obrisati nekoliko unosa u direktorij. Ako klijent izgubi vezu sa poslužiteljem u toku transakcije, niti jedan unos nije obrisan. Tako korisnik može jednostavno započeti transakciju ponovo, a ne provjeravati koji su unosi uspješno obrisani.

Slijedeće LDAP operacije mogu biti dio transakcije:

- dodaj
- promijeni
- promijeni RDN
- brisanje

Bilješka: Ne uključujte promjene u shemi direktorija (cn=schema suffix) u transakcijama. Iako ih je moguće uključiti, ne mogu se vratiti natrag ako transakcija ne uspije. To može uzrokovati da vaš poslužitelj direktorija ima nepredvidive probleme.

Za dodatne informacije o transakcijama, pogledajte dodatak Podrška ograničenih transakcija u IBM SecureWay Uputama za SDK programiranje klijenta direktorija .

Replicirani LDAP poslužitelji direktorija

Informacije pohranjene na replika LDAP poslužiteljima direktorija identične su informacijama na vašem glavnom LDAP poslužitelju direktorija. Dvije su glavne prednosti kad imate jednu ili više replika svoga LDAP direktorija:

- Replike omogućuju brže pretraživanje direktorija. Umjesto da svi izravni zahtjevi za pretraživanje idu na jedan poslužitelj, zahtjevi se mogu dijeliti na glavne i replicirane poslužitelje.
- Replike su zaštitna kopija glavnog poslužitelja. Ako glavni poslužitelj nije dostupan, replika može ispuniti zahtjev za pretraživanje i osigurati pristup podacima u direktoriju.

Replike poslužitelja se mogu samo čitati. Kad neki ovlašteni korisnik pokuša promijeniti neki upis na replici, ona taj zahtjev uputi na glavni poslužitelj direktorija.

Srodni postupak:

“Postavite novu repliku poslužitelja direktorija” na stranici 20

Usluge Direktorija sigurnost

Revizija sigurnosti

Počevši s V5R1, Usluge Direktorija podržavaju OS/400 reviziju sigurnosti. Stavke podložne reviziji uključuju sljedeće:

- Vezanje na i od poslužitelja direktorija.
- Promjene za dozvole objekata LDAP direktorija.
- Promjene u vlasništvu objekata LDAP direktorija.
- Kreiranje, brisanje, pretraživanje i promjene objekata LDAP direktorija.
- Promjene lozinke administratora ažuriranje razlikovnih imena (DN)
- Promjene lozinki korisnika.
- Import i eksport datoteka.

Možda ćete trebati napraviti promjene u vašim OS/400 postavkama revizije prije nego što revizija unosa direktorija proradi. Ako sistemska vrijednost QAUDCTL ima specificirano *OBJAUD, možete omogućiti reviziju objekata kroz iSeries Navigator. Za više informacija o reviziji, pogledajte *Sigurnost - uputa* ili predmet Revizija sigurnosti u iSeries Informativni Centar.

Provjera ovlaštenja za vezu i sigurnost

Usluge Direktorija pružaju sljedeće mehanizme koje možete koristiti za poboljšanje sigurnosti komunikacije između LDAP klijenata i LDAP poslužitelja direktorija:

- Veze sa Slojem sigurnih utičnica (SSL)
- Kerberos provjera ovlaštenja
- CRAM-MD5 šifriranje lozinke

Koristite Sloj sigurnih utičnica (SSL) i Sigurnost translacijskog sloja s poslužiteljem LDAP direktorija

Ako želite komunikaciju s LDAP poslužiteljem učiniti još sigurnijom, Usluge Direktorija mogu koristiti zaštitu sa Slojem sigurnih utičnica (SSL).

Za korištenje SSL-a sa Uslugama Direktorija, morate imati jedan od proizvoda Cryptographic Access Provider (5722-ACx) instaliran na vašem sistemu. Ako želite koristiti SSL iz iSeries Navigator, morate također imati instaliran jedan od proizvoda Client Encryption (5722-CEx) na vašem PC-u. Ovaj vam je softver potreban ako želite raditi nešto od slijedećeg:

- Konfigurirati i administrirati Usluge Direktorija sa svoje radne stanice koristeći se SSL vezom. To obuhvaća poslove koje izvodite iz iSeries Navigator.
- Koristiti SSL vezu s aplikacijama koje ste kreirali s Windows klijentskim sučeljima aplikativnog programa (API-jima).

SSL je standard za Internet zaštitu. SSL možete koristiti za komunikaciju sa LDAP klijentima kao i sa replikama LDAP poslužitelja. Možete klijentsku provjeru autentičnosti kao dodatak poslužiteljskoj provjeri autentičnosti da date dodatnu sigurnost vašim SSL vezama. Klijentska provjera autentičnosti zahtijeva da LDAP klijent prezentira digitalni certifikat koji potvrđuje identitet klijenta serveru prije uspostavljanja veze.

Da koristite SSL, morate imati Upravitelja digitalnih certifikata (DCM), opcija 34 od OS/400, instalirano na vašem sistemu. DCM pruža sučelje preko kojega možete kreirati i upravljati digitalnim certifikatima i spremištima certifikaata. Pogledajte dokumentaciju za Upravitelj digitalnih certifikata za informacije o digitalnim certifikatima i korištenju DCM-a. Za informacije o SSL na iSeries, pogledajte Osiguravanje aplikacija sa SSL-om. Za informacije o TLS na iSeries poslužitelju, pogledajte Podržani protokoli za SSL i Sigurnost transportnog sloja (TLS).

Koristite Kerberos provjeru autentičnosti s poslužiteljem LDAP direktorija

Usluge Direktorija vam dopušta da postavite poslužitelj LDAP direktorija za korištenje Kerberos provjere autentičnosti. Kerberos je mrežni protokol za provjeru autentičnosti koji koristi tajni ključ šifriranja da omogući dobru provjeru ovlaštenja za klijent/poslužitelj aplikacije.

Za omogućavanje Kerberos provjere autentičnosti, morate imati Cryptographic Service Provider proizvode (5722AC2 ili 5722AC3) instalirane na vašem sistemu. Morate također imati konfiguriranu uslugu mrežne provjere autentičnosti.

Kerberos podrška od Usluga Direktorija pruža podršku za GSSAPI SASL mehanizam. Ovo omogućuje i SecureWay i Windows 2000 LDAP klijentima korištenje Kerberos provjere autentičnosti s poslužiteljem LDAP direktorija.

Kerberos osnovno ime koje poslužitelj koristi ima sljedeći oblik:

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

service-name je LDAP, host-name je potpuno kvalificirano TCP/IP ime sistema i realm je default područje specificirano u Kerberos konfiguraciji sistema.

Na primjer, za sistem nazvan my-as400 u acme.com TCP/IP domeni, sa default Kerberos područjem ACME.COM, LDAP poslužitelj Kerberos osnovno ime bi bilo LDAP/my-as400.acme.com@ACME.COM. Default Kerberos područje je specificirano u Kerberos konfiguracijskoj datoteci (po defaultu, /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) s default_realm direktivom (default_realm = ACME.COM). Po dogovoru, imena Kerberos područja koriste velika slova, a imena hostova mala slova. LDAP/ mora biti napisano velikim slovima. Poslužitelj direktorija ne može biti konfiguriran da koristi Kerberos provjeru autentičnosti ako default područje nije konfigurirano.

Kad se koristi Kerberos provjera autentičnosti, LDAP poslužitelj direktorija pridružuje različito ime (DN) vezi koja određuje pristup podacima direktorija. Možete odabrati da DN poslužitelja bude pridruženo jednoj od sljedećih metoda:

- Poslužitelj može kreirati DN na osnovi Kerberos ID-a. Kad izaberete ovu opciju, Kerberos identitet oblika principal@realm generira DN oblika ibm-kn=principal@realm. ibm-kn= je ekvivalent za ibm-kerberosName=.
- Poslužitelj može pretražiti direktorij za razlikovno ime (DN) koje sadrži unos za Kerberos osnovu i područje. Kada odaberete ovu opciju, poslužitelj pretražuje direktorij za unos koji određuje ovaj Kerberos identitet kako slijedi:
  - Poslužitelj pretražuje direktorij za krbRealm-V2 objekt koji ima krbRealmName-V2 atribut koji se podudara s Kerberos područjem. Ako nađe takav unos, onda traži DN-ove koji su specificirani u princSubtree atributu za unos s krbPrincipalName atributom koji se podudara s imenom principala i imenom područja. Ako DN konfiguriran u krbAliasedObjectName sadržava DN prethodno nađenog unosa, onda se DN konfiguriran u krbAliasedObjectName koristi. Inače, koristi se DN unosa. Ova metoda se tipično koristi kad Kerberos KDC pohranjuje Kerberos osnovne informacije u LDAP direktoriju.
  - Ako gore opisano traženje ne uspije, onda poslužitelj traži unos direktorija koji koristi ibm-securityIdentities pomoćnu klasu i ima vrijednost altSecurityIdentities atributa KERBEROS:principal@realm. Ova metoda može biti korištena za pridruživanje Kerberos identiteta unosima direktorija kad KDC ne pohranjuje osnove u direktorij.

Morate imati datoteku tablice ključeva (keytab) koja sadržava ključ za osnove LDAP usluge. PogledajteInformativni Centar predmet Usluga mrežne provjere autentičnosti pod Sigurnost za više informacija o Kerberosu na iSeries poslužitelju. Odlomak Konfiguriranje usluge mrežne provjere autentičnosti sadržava informacije o dodavanju informacija u datoteke tablice ključeva.

Projicirana pozadina operacijskog sistema

Projicirana pozadina operacijskog sistema ima sposobnost mapiranja OS/400 objekata kao unosa unutar LDAP-dostupnog stabla direktorija. Projicirani objekti su LDAP prikazi OS/400 objekata umjesto stvarnih unosa pohranjenih u bazi podataka LDAP poslužitelja. S V5R2, OS/400 korisnički profili su jedini objekti koji se mapiraju ili projiciraju kao unosi unutar stabla direktorija. Mapiranje objekata korisničkog profila poznato je kao OS/400 korisnička projicirana pozadina.

LDAP operacije mapirane su na OS/400 objekte koji leže ispod i LDAP operacije izvode funkcije operacijskog sistema kako bi pristupile ovim objektima. Sve LDAP operacije izvedene na korisničkim profilima učinjene su pod ovlaštenjem korisničkog profila pridruženog vezi klijenta.

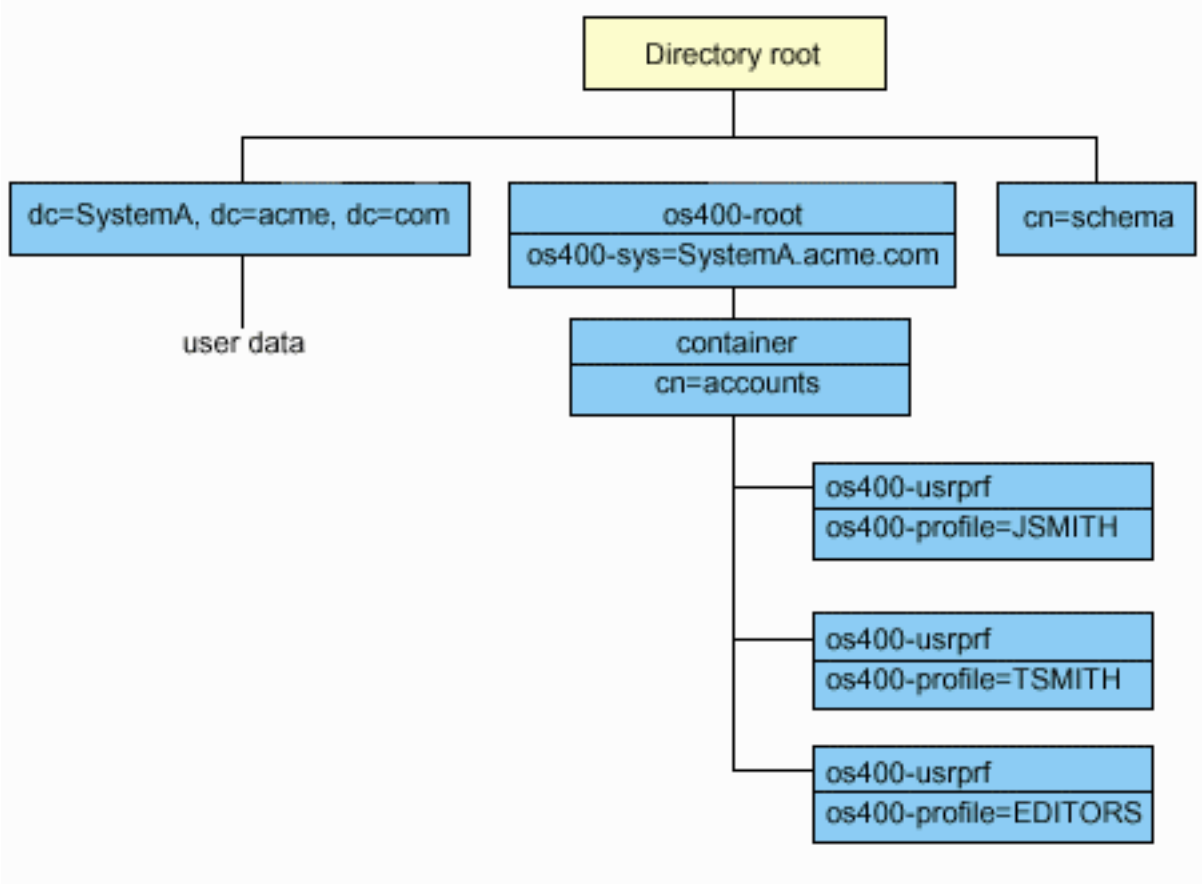
Za detaljnije informacije o projiciranoj pozadini operacijskog sistema, pogledajte slijedeće:

- “OS/400 informacijsko stablo direktorija projiciranih korisnika” na stranici 39
- “LDAP operacije” na stranici 39
- “DN-ovi povezivanja administratora i kopije” na stranici 43
- “OS/400 korisnički-projicirana shema” na stranici 43

OS/400 informacijsko stablo direktorija projiciranih korisnika

Slika ispod pokazuje primjer informacijskog stabla direktorija (DIT) za korisnički projiciranu pozadinu. Slika pokazuje i pojedinačne i grupne profile. Na slici, JSMITH i TSMITH su korisnički profili, što je naznačeno interno identifikatorom grupe (GID), GID=*NONE (ili 0); EDITORS je grupni profil, što je naznačeno interno GID-om različitim od nule.

Sufiks dc=SystemA,dc=acme,dc=com je uključen u sliku za referencu. Ovaj sufiks predstavlja beckend trenutne baze podataka koji upravlja drugim LDAP unosima. Sufiks cn=schema je trenutna poslužiteljska shema koja se koristi.



Korijen stabla je sufiks, koji je po defaultu os400-sys=*SystemA.acme.com*, gdje je *SystemA.acme.com* ime vašeg sistema. Objectclass je os400-root. Iako se DIT ne može preinačiti ili obrisati, možete rekonfigurirati sufiks sistemskog objekta. Ipak, morate osigurati da se trenutni sufiks ne koristi u ACL-ovima ili drugdje u sistemu gdje unose treba preinačiti ako se sufiks mijenja.

Na prethodnoj slici, spremnik, cn=accounts, je pokazan ispod korijena. Ovaj objekt se ne može preinačiti. Spremnik je smješten na ovoj razini u očekivanju drugih vrsta informacija ili objekata koji mogu biti projicirani od operacijskog sistema u budućnosti. Ispod spremnika cn=accounts su korisnički profili koji su projicirani kao objectclass=os400-usrprf. Na korisničke profile se odnose projicirani korisnički profili i poznati su LDAP-u u obliku os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com.

LDAP operacije

Slijede LDAP operacije koje se mogu izvesti korištenjem projiciranih korisničkih profila.

Povezivanje

LDAP klijent se može povezati na (dokazati autentičnost) LDAP poslužitelj koristeći projicirani korisnički profil. Ovo se postiže specificiranjem razlikovnog imena (DN) projiciranog korisničkog profila za DN povezivanja i ispravne lozinke OS/400 korisničkog profila za provjeru autentičnosti. Primjer DN korištenog u zahtjevu povezivanja bio bi os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com.

Klijent se mora povezati kao projicirani korisnik da pristupi informacijama u sistemskoj projiciranoj pozadini. Poslužitelj izvodi sve operacije koristeći ovlaštenje tog korisničkog profila. DN projiciranog korisničkog profila može se također koristiti u LDAP ACL-ima kao DN-ovi drugih LDAP unosa. Jednostavna metoda povezivanja je jedina metoda povezivanja koja je dozvoljena kad je projicirani korisnički profil specificiran u zahtjevu povezivanja.

Traženje

Sistemska projicirana pozadina podržava neke osnovne filtere traženja. Možete specificirati objectclass, os400-profil i os400-gid atribute u filterima traženja. Atribut os400-profil podržava džokere. Atribut os400-gid je ograničen na specificiranje (os400-gid=0), što je pojedinačni korisnički profil, ili !(os400-gid=0), što je grupni profil. Možete dohvatiti sve atribute korisničkog profila osim lozinke i sličnih atributa.

Za određene filtere, samo DN objectclass i os400-profil vrijednosti se vraćaju. Ipak, slijedna traženja mogu se voditi da vrate detaljnije informacije.

Slijedeća tablica opisuje ponašanje sistemski projicirane pozadine za operacije traženja.

Tablica 1. Ponašanje sistemske projicirane pozadine za operacije traženja

Traženje zahtijevano	Baza traženja	Opseg traženja	Filter traženja	Primjedbe
Vrati informacije za os400-sys=SystemA, (opcijski) za spremnike pod njim i (opcijski) za objekte u tim spremnicima.	os400-sys=SystemA.acme.com	baza, pod, ili jedan	objectclass=* objectclass=os400-root objectclass=spremnik objectclass=os400-usrprf	Vrati prikladne atribute i njihove vrijednosti bazirano na specificiranom opsegu i filteru. Hardcoded atributi i njihove vrijednosti se vraćaju za sufiks sistemskog objekta i spremnik pod njim.
Vrati sve korisničke profile.	cn=accounts, os400-sys=SystemA.acme.com	jedan ili pod	os400-gid=0	Samo vrijednosti razlikovnog imena (DN), objectclass i os400-profila se vraćaju za projicirane korisničke profile. Ako je bilo kakav drugi filter specificiran, LDAP_UNWILLING_TO_PERFORM se vraća.
Vrati sve grupne profile.	cn=accounts, os400-sys=SystemA.acme.com	jedan ili pod	(!(os400-gid=0))	Samo vrijednosti razlikovnog imena (DN), objectclass i os400-profila se vraćaju za projicirane korisničke profile. Ako je bilo kakav drugi filter specificiran, LDAP_UNWILLING_TO_PERFORM se vraća.

Tablica 1. Ponašanje sistemske projicirane pozadine za operacije traženja (nastavak)

Traženje zahtijevano	Baza traženja	Opseg traženja	Filter traženja	Primjedbe
Vrati sve korisničke i grupne profile.	cn=accounts, os400-sys=SystemA.acme.com	jedan ili pod	os400-profile=*	Samo vrijednosti razlikovnog imena (DN), objectclass i os400-profila se vraćaju za projicirane korisničke profile. Ako je bilo kakav drugi filter specificiran, LDAP_UNWILLING_TO_PERFORM se vraća.
Vrati informacije za specifični korisnički ili grupni profil kao što je korisnički profil JSMITH.	cn=accounts, os400-sys=SystemA.acme.com	jedan ili pod	os400-profile=JSMITH	Ostali atributi koje treba vratiti mogu se specificirati.
Vrati informacije za specifični korisnički ili grupni profil kao što je korisnički profil JSMITH.	os400-profile=JSMITH, cn=accounts, os400-sys=SystemA.acme.com	baza, pod, ili jedan	objectclass=os400-usrprf objectclass=* os400-profile=JSMITH	Ostali atributi koje treba vratiti mogu se specificirati. Čakiako se može specificirati opseg jedne razine, rezultati traženja neće vratiti nijednu vrijednost jer nema ničega ispod korisničkog profila JSMITH u DIT.
Vrati sve korisničke i grupne profile koji počinju s A.	cn=accounts, os400-sys=SystemA.acme.com	jedan ili pod	os400-profile=A*	Samo vrijednosti razlikovnog imena (DN), objectclass i os400-profila se vraćaju za projicirane korisničke profile. Ako je bilo kakav drugi filter specificiran, LDAP_UNWILLING_TO_PERFORM se vraća.
Vrati sve grupne profile koji počinju s G.	cn=accounts, os400-sys=SystemA.acme.com	jedan ili pod	(&(!(os400-gid=0)) (os400-profile=G*))	Samo vrijednosti razlikovnog imena (DN), objectclass i os400-profila se vraćaju za projicirane korisničke profile. Ako je bilo kakav drugi filter specificiran, LDAP_UNWILLING_TO_PERFORM se vraća.

Tablica 1. Ponašanje sistemske projicirane pozadine za operacije traženja (nastavak)

Traženje zahtijevano	Baza traženja	Opseg traženja	Filter traženja	Primjedbe
Vrati sve korisničke profile koji počinju s A.	cn=accounts, os400-sys=SystemA.acme.com	jedan ili pod	(&(os400-gid=0) (os400-profile=A*))	Samo vrijednosti razlikovnog imena (DN), objectclass i os400-profila se vraćaju za projicirane korisničke profile. Ako je bilo kakav drugi filter specificiran, LDAP_UNWILLING_TO_PERFORM se vraća.

Usporedi

LDAP operacije usporedbe može se koristiti za uspoređivanje vrijednosti atributa projiciranog korisničkog profila. Atributi os400-aut i os400-docpwd ne mogu se uspoređivati.

Dodaj i promijeni

Možete kreirati korisničke profile koristeći LDAP operaciju dodavanja i možete također mijenjati korisničke profile koristeći LDAP operaciju mijenjanja.

Obriši

Korisnički profili mogu se obrisati korištenjem LDAP operacije brisanja. Da specificirate ponašanje DLTUSRPRF OWNOBJOPT i PGPOPT parametara, dvije LDAP poslužiteljske kontrole su sada osigurane. Ove kontrole mogu biti specificirane u LDAP operaciji brisanja. Pogledajte naredbu Obriši korisnički profil (DLTUSRPRF) za više informacija o ponašanju ovih parametara.

Slijede kontrole i njihovi identifikatori objekata (OID-ovi) koji mogu biti specificirani u LDAP operaciji brisanja klijenta.

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  Slijedeće je vrijednost kontrole:
  - controlValue ::= ownObjOpt [newOwner]
  - ownObjOpt ::= *NODLT / *DLT / *CHGOWN

  Vrijednost kontrole ownObjOpt specificira akciju koju treba poduzeti ako korisnički profil posjeduje objekte. Vrijednost *NODLT pokazuje da se korisnički profil ne briše ako korisnički profil posjeduje objekte. Vrijednost *DLT pokazuje da se objekti u vlasništvu brišu i vrijednost *CHGOWN pokazuje da se vlasništvo prenese na drugi profil.

  Vrijednost newOwner specificira profil na koji se vlasništvo prenosi. Ova vrijednost je potrebna kad je ownObjOpt postavljeno na *CHGOWN.

  Primjeri vrijednosti kontrole su slijedeći:
  - *NODLT: specificira da se profil ne može obrisati ako posjeduje objekte
  - *CHGOWN SMITH: specificira da se vlasništvo nad objektima prenese na korisnički profil SMITH.
- Identifikator objekta (OID) je definiran u ldap.h kao LDAP_OS400_OWNOBJOPT_CONTROL_OID.
  - os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

    Vrijednost kontrole definirana je kako slijedi:

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

Vrijednost pgpOpt specificira akciju koju treba poduzeti ako je profil koji se briše primarna grupa za neke objekte. Ako je *CHGPGP specificirano, newPgp mora također biti specificirano. Vrijednost newPgp specificira ime profila primarne grupe ili *NONE. Ako je novi profil primarne grupe specificiran, vrijednost newPgpAut mora također biti specificirana. Vrijednost newPgpAut specificira ovlaštenje za objekte koje je dano novoj primarnoj grupi.

Primjeri vrijednosti kontrole su slijedeći:

- *NOCHG: specificira da se profil ne može obrisati ako je primarna grupa za neke objekte.
- *CHGPGP *NONE: specificira uklanjanje primarne grupe za objekte.
- *CHGPGP SMITH *USE: specificira promjenu primarne grupe u korisnički profil SMITH i dodjelu *USE ovlaštenja primarnoj grupi.

Ako jedna ili druga kontrola nije specificirana u brisanju, defaulti trenutno na snazi za QSYS/DLTUSRPRF naredbu se koriste.

ModRDN

Ne možete preimenovati projicirane korisničke profile jer to nije podržano od operacijskog sistema.

Import i eksport API-ja

API-ji QgldImportLdif i QgldExportLdif ne podržavaju import ili eksport podataka unutar sistemske projicirane pozadine.

DN-ovi povezivanja administratora i kopije

Možete specificirati projicirani korisnički profil kao DN povezivanja konfiguriranog administratora ili kopije. Koristi se lozinka korisničkog profila. Projicirani korisnički profili mogu također postati LDAP administratori ako su ovlašteni za identifikator funkcije Administratora poslužitelja direktorija (QIBM_DIRSRV_ADMIN). Višestrukim korisničkim profilima može se dodijeliti administratorski pristup.

Za više informacija, pogledajte “Radite s administrativnim pristupom za ovlaštene korisnike” na stranici 28.

OS/400 korisnički-projicirana shema

Klase objekata i atributi iz projicirane pozadine mogu se naći u poslužiteljskoj shemi. Imena LDAP atributa su u formatu os400–*nnn*, gdje je *nnn* tipično ključna riječ atributa (kao što je CRTUSRPRF ili CHGUSRPRF) u naredbama korisničkog profila. Pogledajte “OS/400 informacijsko stablo direktorija projiciranih korisnika” na stranici 39 za više informacija.

Usluge Direktorija i OS/400 podrška vođenja dnevnika

Usluge Direktorija koristi OS/400 podršku baze podataka za pohranjivanje informacija direktorija. Usluge Direktorija se koriste kontrolom predavanja kod pohranjivanja slogova direktorija u bazu. Ovo zahtijeva OS/400 podršku vođenja dnevnika.

Kad se pokrene poslužitelj ili LDIF alat za importiranje po prvi put, izrađuje se slijedeće:

- Dnevnik
- Prijemnik dnevnika
- Tablice baza potrebne za početak

Dnevnik QSQJRN je izgrađen u knjižnici baze koju ste konfigurirali. Primalac dnevnika QSQJRN0001 je na početku kreiran u knjižnici baze koju ste konfigurirali.

Vaša okolina, veličina direktorija i struktura, ili strategija spremanja i vraćanja mogu uzrokovati neke promjene od defaulta, uključujući kako se tim objektima upravlja i koji je korišteni prag za veličinu. Parametre naredbe za vođenje dnevnika možete po potrebi mijenjati. LDAP vođenje dnevnika je postavljeno po defaultu da briše stare primaoce. Ako je dnevnik promjena konfiguriran i želite sačuvati stare primaoce, izvedite slijedeću naredbu iz OS/400 reda za naredbe:

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

Ako je konfiguriran dnevnik promjene, možete obrisati njegove primaoce dnevnika sa slijedećom naredbom:

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

Za informacije o naredbama vođenja dnevnika, pogledajte predmet OS/400 naredbe pod Programiranje u iSeries Informativni Centar.

Poglavlje 6. LDAP servisni programi s linije naredbe

Usluge Direktorija uključuju pet pomoćnih programa koji vam dozvoljavaju da izvodite naredbe na LDAP poslužitelju direktorija s Qshell okoline za naredbe na OS/400. Ovi programi koriste LDAP API-e. Možete koristiti te pomoćne programe iz qsh reda za naredbe ili ih pozvati iz vaših programa. Možda će vam biti korisni i kao primjeri za programiranje. Kad instalirate Windows LDAP klijent koji je uključen s Usluge Direktorija, također instalirate kod koji je vrlo sličan izvornom kodu pomoćnih programa ljuske.

Ti programi su slijedeći:
- "Pomoćni programi ldapmodify i ldapadd", koji dodaje i preinačuje slogove u LDAP direktoriju.
- "Servisni program ldapdelete" na stranici 48, koji briše slogove iz LDAP direktorija.
- "ldapsearch servisni program" na stranici 50, koji traži slogove po LDAP direktoriju.
- "ldapmodrdn servisni program" na stranici 54, koji preinačuje relativno razlikovno ime (RDN) slogova u LDAP direktoriju.

Pogledajte "Napomene o korištenju SSL-a s LDAP pomoćnim programima reda za naredbe" na stranici 56, ako vam trebaju informacije o upotrebi SSL sa servisnim programima sa naredbene linije.

Pomoćni programi ldapmodify i ldapadd

Pomoćni program ldapmodify vam dozvoljava da promijenite unose ili dodate unose u LDAP poslužitelj direktorija iz ljuske za naredbe QSH na vašem sistemu. On koristi ldap_modify, ldap_add i ldap_delete sučelja aplikativnog programa (API-je). Pomoćni program ldapadd radi gotovo identično kao pomoćni program ldapmodify s izuzetkom automatskog uključivanja -a zastavice.

Format:

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

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

Bilješka: Ako ne unesete podatak za upis iz *datoteke* koristeći opciju **-f**, program će čekati da učita slogove iz standardnog skupa ulaznih podataka. Ako želite prekinuti čekanje, pritisnite tipku SysReq, a zatim izaberite 2. Završi prethodni zahtjev.

Dijagnostika:

Izlazni status je 0, ako nema grešaka. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

Kliknite ovdje da vidite primjere upotrebe ovih uslužnih pomoćnih programa.

Parametri:

-V	Određuje LDAP verziju koju program koristi za povezivanje na LDAP poslužitelj. Po defaultu koristi LDAP V3 vezu. Da izričito izaberete LDAP V3, specificirajte -V 3. Specificirajte -V 2 za izvođenje kao LDAP V2 aplikacija.
-a	Samo ldapmodify koristi ovaj parametar. To pokazuje da će pomoćni program dodati unose po defaultu radije nego ih modificirati. Upotreba ovoga parametra je ista kao i upotreba ldapadd.

-b	Pretpostavite da su sve vrijednosti koje počinju s `/ binarne vrijednosti i da je stvarna vrijednost u datoteci čija staza je specificirana na mjestu gdje se vrijednosti normalno pojavljuju.
-c	Kontinuirani operativni modus. Javljaju se poruke o greškama ali ldapmodify ili ldapadd nastavlja s modifikacijom ili dodavanjem. Default je izlaz iz programa nakon što se desi greška.
-r	Zamijeni postojeće vrijednosti po defaultu.
-M	Upravljajte referal objektima kao pravilnim unosima.
-n	Pokaži što bi bilo učinjeno ali ne mijenjaj upise. Korisno za analizu u spoju s -v.
-v	Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.
-F	Forsiraj promjene neovisno o sadržaju ulaznih redaka koji počinju s replikom: (po defaultu, replika: reci se uspoređuju prema LDAP hostu i portu poslužitelja da se utvrdi treba li primijeniti slog zapisa o replikaciji).
-R	Određuje da se preporuke ne slijede automatski.
-C *charset*	Određuje da nizovi uneseni kao ulazni podaci u servisni program budu prikazani u lokalnom skupu znakova (*charset*) i moraju se konvertirati u UTF-8. Koristite opciju **-C** charset, ako je kodna stranica ulaznog niza različita od kodne stranice posla. Pozovite se na dokumentaciju o ldap_set_iconv_local_charset() API da vidite koje *charset* vrijednosti su podržane.
-d *debuglevel*	Postavlja debug razinu na *debuglevel*.
-D *binddn*	Upotrijebi *binddn* za povezivanje na LDAP direktorij. *binddn* bi trebao biti znakovno prikazan DN.
-w *passwd*	Koristite *passwd* kao lozinku za provjeru ovlaštenja.
-m *mechanism*	Koristite *mechanism* da odredite SASL mehanizam koji klijent koristi za vezanje na poslužitelj. Klijent koristi ldap_sasl_bind_s() API. Dostupni mehanizmi uključuju CRAM-MD5 (šifrira lozinku), EXTERNAL (korišten sa SSL) i GSSAPI (Kerberos). Naredba zanemaruje **-m** parametar ako je postavljeno **-V 2**. Ako ne navedete **-m**, koristi se jednostavna provjera ovlaštenja.
-O*hopcount*	Odredite *hopcount* da postavite maksimum skokova koje će knjižnica klijenta napraviti kada traži referal. Default broj skokova je 10.
-h *ldaphost*	Određuje alternativni host na kojemu radi LDAP poslužitelj.
-p *ldapport*	Određuje alternativni port za Transmission Control Protocol (TCP) na kojemu LDAP osluškuje. Default LDAP port je 389. Ako nije naveden, a **-Z** je navedeno, koristi se default LDAP SSL port 636.
-f *file*	Čita podatke o modifikaciji sloga iz LDIF datoteke umjesto iz standardnog ulaza. Ako LDIF datoteka nije navedena, morate koristiti standardne ulazne podatke kad određujete slogove za ažuriranje u LDIF formatu.
-Z	Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Opcija **-Z** je podržana samo u verzijama ovoga alata koje imaju mogućnost rada sa SSL.
-K *keyfile*	Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva. Ako pomoćni program ne može locirati bazu ključeva, koristit će vrstno kodirani skup default povjerljivih korijena izdavača certifikata. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori. Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**.
-P *keyfilepw*	Određuje lozinku baze ključeva. Ova lozinka je obavezna za pristup šifriranim podacima u bazi ključeva (uključujući i privatni ključ). Ako je skrivena datoteka lozinki pridružena bazi podataka ključeva, lozinka se dobiva iz skrivene datoteke, a ovaj parametar nije potreban. Ovaj se parametar zanemaruje ako nisu navedeni ni **-Z** niti **-K**.

-N *certificatename*	Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru identiteta poslužitelja, klijentov certifikat nije potreban. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru identiteta klijenta i poslužitelja, klijentov certifikat je potreban. *certificatename* nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, *certificatename* nije potreban ako je jednostruk certifikat/privatni par ključeva u odredišnoj datoteci baze podataka ključeva. Ovaj se parametar zanemaruje ako nisu navedeni ni **-Z** niti **-K**.

Alternativni ulazni format:

Pomoćni program ldapmodify podržava zamjenski ulazni format kako bi održao kompatibilnost sa starijim verzijama pomoćnog programa. Ovaj format se sastoji od jednog ili više slogova-upisa razdvojenih praznim redovima. Svaki slog ima slijedeći format:

```
Prepoznatljivo (različito) ime (DN)
attr=vrijednost
[attr=vrijednost ...]
```

gdje je *attr* ime atributa, a *vrijednost* je vrijednost atributa. Po defaultu, vrijednosti se dodaju. Ako stavite **-r** oznaku naredbene linije, default je da se postojeće vrijednosti zamjenjuju novom. Napominjemo da je dopustivo da se neki atribut pojavljuje više puta (na primjer, jednom atributu možete dodati više od jedne vrijednosti). Također primjetite da možete koristiti obrnutu kosu crtu (\) da nastavite vrijednosti kroz linije i da sačuvate nove linije u samoj vrijednosti. Ako uklanjate neku vrijednost, ispred vrijednosti *attr* stavite crticu (-). Znak jednakosti (=) i vrijednost se izostavljaju ako se uklanja cijeli atribut. Ispred *attr* treba staviti znak zbrajanja (+), ako se dodaje neka vrijednost, a prisutna je oznaka **-r**.

Primjeri: ldapmodify i ldapadd

Primjer 1:

Ako postoji datoteka /**tmp**/**entrymods** i ima slijedeći sadržaj:

```
dn: cn=Modify Me, o=University of Higher Learning, c=US
changetype: modify
zamjena: pošta
pošta: modme@student.of.life.edu
-
dodaj: naslov
naslov: Grand Poobah
-
dodaj: jpegPhoto
jpegPhoto:< file:///tmp/modme.jpeg
-
briši: opis
-
```

Naredba ldapmodify -b -r -f /tmp/entrymods će napraviti slijedeće:

- Zamijeniti sadržaj Modify Me unosa atributa pošte s vrijednošću modme@student.of.life.edu.
- Dodati naslov Grand Poobah.
- Dodati sadržaj datoteke /**tmp**/**modme.jpeg** kao jpegPhoto.
- Potpuno ukloniti atribut opis.

Iste modifikacije možete izvesti sa starijim ldapmodify ulaznim formatom:

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

Naredba za upotrebu starijeg formata bila bi:

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

Primjer 2:

Pretpostavimo da datoteka /**tmp**/**newentry** postoji i ima slijedeći sadržaj:

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

Naredba ldapadd -f /tmp/entrymods će dodati novi upis za John Doea koristeći vrijednosti iz datoteke /tmp/newentry.

Primjer 3:

Ako postoji datoteka /**tmp**/**newentry** i ima slijedeći sadržaj:

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

Naredba ldapmodify -f /tmp/entrymods će ukloniti upis za John Doea.

Servisni program ldapdelete

Program ldapdelete vam omogućuje da brišete jedan ili više slogova sa LDAP poslužitelja direktorija. Izvodi se kroz QSH ovojnicu za naredbe u OS/400. Koristi ldap_delete sučelje za aplikativne programe (API).

Format:

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

Bilješka: Ako ne unesete *dn* argumente, naredba ldapdelete će čekati da učita listu DN-a iz standardnog ulaza. Ako želite prekinuti čekanje, pritisnite tipku SysReq, a zatim izaberite 2. Završi prethodni zahtjev.

Dijagnostika:

Izlazni status je 0, ako nema grešaka. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

Kliknite ovdje da vidite primjere upotrebe ldapdelete programa.

Parametri:

-V	Određuje LDAP verziju koju program koristi za povezivanje na LDAP poslužitelj. Po defaultu koristi LDAP V3 vezu. Da izričito izaberete LDAP V3, specificirajte -V 3. Specificirajte -V 2 za izvođenje kao LDAP V2 aplikacija.
-M	Upravljajte referal objektima kao pravilnim unosima.
-n	Pokaži što bi bilo učinjeno ali nemoj brisati upise. Korisno za analizu u spoju s **-v**.
-v	Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-c	Kontinuirani operativni modus. Greške se javljaju, ali ldapdelete će nastaviti s brisanjima. Default je izlaz iz programa nakon što se desi greška.
-R	Određuje da se preporuke ne slijede automatski.
-C *charset*	Određuje da se razlikovna imena (DN) koja služe kao ulazni podatak u ldapdelete servisni program prikazuju u lokalnom skupu znakova (*charset*). Upotrijebite **-C** *charset* i zamijenite default, tamo gdje nizovi znakova moraju biti uneseni u UTF-8. Koristite opciju **-C** charset, ako je kodna stranica ulaznog niza različita od kodne stranice posla. Pozovite se na dokumentaciju o ldap_set_iconv_local_charset() API da vidite koje *charset* vrijednosti su podržane.
-d *debuglevel*	Postavlja debug razinu na *debuglevel*.
-f *file*	Čitaj niz redaka iz *datoteke*, i izvedi jedno LDAP brisanje za svaki redak u datoteci. Svaki redak u datoteci treba sadržavati jedno jedino razlikovno ime (DN).
-D *binddn*	Upotrijebi *binddn* za povezivanje na LDAP direktorij. *binddn* bi trebao biti znakovno prikazan DN.
-w *passwd*	Koristite *passwd* kao lozinku za provjeru ovlaštenja.
-m *mehanizam*	Upotrijebi *mehanizam* kad se određuje SASL mehanizam koji će se koristiti za povezivanje na poslužitelj. Koristit će se ldap_sasl_bind_s() API. Dostupni mehanizmi uključuju CRAM-MD5 (šifrira lozinku), EXTERNAL (korišten sa SSL) i GSSAPI (Kerberos). Parametar -m se zanemaruje ako je određeno -V 2. Ako **-m** mije naveden, koristi se jednostavna provjera identiteta.
-O *hopcount*	Odredi *hopcount* da se podesi najveći broj skokova koje će klijentova knjižnica poduzeti u potjeri za preporučiteljima. Default broj skokova je 10.
-h *ldaphost*	Određuje alternativni host na kojemu radi LDAP poslužitelj.
-p *ldapport*	Određuje alternativni port za Transmission Control Protocol (TCP) na kojemu LDAP osluškuje. Default LDAP port je 389. Ako nije naveden, a **-Z** je navedeno, koristi se default LDAP SSL port 636.
-Z	Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Opcija **-Z** je podržana samo u verzijama ovoga alata koje imaju mogućnost rada sa SSL.
-K *keyfile*	Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva. Ako pomoćni program ne može locirati bazu ključeva, koristiti će vrstno kodirani skup default povjerljivih korijena izdavača certifikata. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori. Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**.
-P *keyfilepw*	Određuje lozinku baze ključeva. Ova lozinka je obavezna za pristup šifriranim podacima u bazi ključeva (uključujući i privatni ključ). Ako je skrivena datoteka lozinki pridružena bazi podataka ključeva, lozinka se dobiva iz skrivene datoteke, a ovaj parametar nije potreban. Ovaj se parametar zanemaruje ako nije određen ni **-Z** niti **-K**.
-N *certificatename*	Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru identiteta poslužitelja, klijentov certifikat nije potreban. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru identiteta klijenta i poslužitelja, klijentov certifikat je potreban. *certificatename* nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, *certificatename* nije potreban ako je jednostruk certifikat/privatni par ključeva u odredišnoj datoteci baze podataka ključeva. Ovaj se parametar zanemaruje ako nisu navedeni ni **-Z** niti **-K**.
dn	Određuje jedan ili više *dn* argumenata. Svaki *dn* bi trebao biti znakovno prikazan DN.

Primjer: ldapdelete

Slijedeća naredba će pokušati obrisati unos imenovan s commonName Delete Me izravno ispod organizacijskog unosa University of Life:

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

Možda će biti potrebno dati *binddn* i *passwd* (vidjeti opcije **-D** i **-w**).

ldapsearch servisni program

Pomoćni program ldapsearch vam dozvoljava da tražite unos u vašem LDAP poslužitelju direktorija iz QSH ljuske za naredbe u OS/400. On koristi ldap_search aplikativno programsko sučelje (API).

Pretraživanje se koristi filterom koji odgovara prikazu LDAP filtera kao niza znakova. Za više informacija o LDAP filterima pretraživanja, pogledajte ldap_search API informacije u predmetu OS/400 Usluge Direktorija pod Programiranje u iSeries Informativni Centar.

Ako ldapsearch program nađe jedan ili više slogova, on učitava atribute navedene u *attrs* i ispisuje slogove i vrijednosti u standardni izlaz. Ako ne listate atribute, program vraća sve atribute.

Format:

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

Dijagnostika:

Izlazni status je 0, ako nema grešaka. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

Izlazni format:

Ako ldapsearch nađe jedan ili više slogova, zapisuje svaki slog u standardni izlaz u obliku:

```
Razlikovno ime (DN)
attributename=vrijednost
attributename=vrijednost
attributename=vrijednost
...
```

Višestruki upisi su razdvojeni jednim praznim retkom. Ako koristite opciju **-F** kad određujete znak razdvajanja, na izlazu se prikaže taj znak umjesto znaka jednakosti (=). Ako koristite opciju **-t**, ime privremene datoteke zamjenjuje stvarnu vrijednost. Ako navedete opciju **-A**, ispisuje se samo dio attributename.

Kliknite ovdje da vidite primjere upotrebe ldapsearch programa.

Parametri:

-V	Određuje LDAP verziju koju program koristi za povezivanje na LDAP poslužitelj. Po defaultu koristi LDAP V3 vezu. Da izričito izaberete LDAP V3, specificirajte -V 3. Specificirajte -V 2 za izvođenje kao LDAP V2 aplikacija.
-n	Pokaži što bi bilo učinjeno ali nemoj izvoditi pretraživanje. Korisno za analizu u spoju sa **-v**.
-v	Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.
-t	Piše učitane vrijednosti u skup privremenih datoteka. Ovo je korisno kod baratanja sa binarnim vrijednostima kao što je jpegPhoto ili zvučni zapis.
-A	Učitaj samo atribute (bez vrijednosti). Ovo je korisno kad samo želite pogledati je li neki atribut prisutan u nekom slogu, a ne zanima vas pojedinačna vrijednost.

-B	Ne ispuštaj binarne vrijednosti s prikaza. Ovo je korisno kad se bavite vrijednostima koje se pojavljuju u izmijenjenom skupu znakova kao što je ISO-8859.1. Ova opcija je izravno vezana uz **-L**
-L	Prikaži rezultate traženja u LDIF formatu. Ova opcija također uključuje i opciju **-B**, a pritom se opcija **-F** zanemaruje.
-M	Upravljajte referal objektima kao pravilnim unosima.
-R	Određuje da se preporuke ne slijede automatski.
-C *charset*	Određuje da nizovi unešeni kao ulazni podaci u servisni program ldapsearch budu prikazani u lokalnom skupu znakova (*charset*). Ulazni niz obuhvaća filter, povezni DN i bazni DN. Slično, kod prikaza podataka, ldapsearch će konvertirati podatke primljene od LDAP poslužitelja u specificirane znakove. Koristite opciju **-C** charset, ako je kodna stranica ulaznog niza različita od kodne stranice posla. Pozovite se na dokumentaciju o ldap_set_iconv_local_charset() API da vidite koje *charset* vrijednosti su podržane. Također, ako su navedene i opcija -C i opcija -L, ulazni podaci se uzimaju kao da su u navedenom skupu znakova ali izlazni iz ldapsearch programa se uvijek ćuvaju u UTF-8 prikazu ili baznom 64-kodnom prikazu podataka, kad se otkriju znakovi koji se ne mogu ispisati. Ovo je taj slučaj pošto LDIF datoteke sadrže samo UTF-8 (ili bazni 64-kodni UTF-8) prikaz podataka u nizu.
-d *debuglevel*	Postavlja debug razinu na *debuglevel*.
-F *sep*	Upotrijebite *sep* kao separator polja između imena i vrijednosti atributa. Default separator je `=, osim ako je **-L** zastavica specificirana, u tom se slučaju ova opcija zanemaruje.
-f *file*	Čita niz redaka iz datoteke, izvodeći jedno LDAP traženje za svaki redak u datoteci. Svaki redak u datoteci treba sadržavati jedno jedino razlikovno ime (DN).
-D *binddn*	Upotrijebi *binddn* za povezivanje na LDAP direktorij. *binddn* bi trebao biti znakovno prikazan DN.
-w *passwd*	Koristite *passwd* kao lozinku za provjeru ovlaštenja.
-m *mehanizam*	Upotrijebite *mehanizam* kad određujete SASL mehanizam koji će se koristiti za povezivanje na poslužitelj. Koristit će se ldap_sasl_bind_s() API. Dostupni mehanizmi uključuju CRAM-MD5 (šifrira lozinku), EXTERNAL (korišten sa SSL) i GSSAPI (Kerberos). Parametar **-m** se zanemaruje ako je postavljeno **-V** 2. Ako **-m** mije naveden, koristi se jednostavna provjera identiteta.
-O *hopcount*	Odredi *hopcount* da se podesi najveći broj skokova koje će klijentova knjižnica poduzeti u potjeri za preporučiteljima. Default broj skokova je 10.
-h *ldaphost*	Određuje alternativni host na kojemu radi LDAP poslužitelj.
-p *ldapport*	Određuje alternativni port za Transmission Control Protocol (TCP) na kojemu LDAP osluškuje. Default LDAP port je 389. Ako nije naveden, a **-Z** je naveden, koristi se default LDAP SSL port 636.
-Z	Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Opcija **-Z** je podržana samo u verzijama ovoga alata koje imaju mogućnost rada sa SSL.
-K *keyfile*	Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva. Ako pomoćni program ne može locirati bazu ključeva, koristit će vrstno kodirani skup default povjerljivih korijena izdavača certifikata. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori. Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**.
-P *keyfilepw*	Određuje lozinku baze ključeva. Ova lozinka je obavezna za pristup šifriranim podacima u bazi ključeva (uključujući i privatni ključ). Ako je skrivena datoteka lozinki pridružena datoteci ključeva, lozinka se pribavlja iz tajne datoteke, a ovaj parametar nije potreban. Ovaj se parametar zanemaruje ako nisu navedeni ni **-Z** niti **-K**.

-N *certificatename*	Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru identiteta poslužitelja, klijentov certifikat nije potreban. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru identiteta klijenta i poslužitelja, klijentov certifikat je potreban. *certificatename* nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, *certificatename* nije potreban ako je jednostruk certifikat/privatni par ključeva u odredišnoj datoteci baze podataka ključeva. Ovaj se parametar zanemaruje ako nisu navedeni ni **-Z** niti **-K**.
-b *searchbase*	Upotrijebite *searchbase* kao ishodište u pretraživanju umjesto default vrijednosti. Ako **-b** nije naveden, servisni program će ispitati LDAP_BASEDN varijablu okoline i provjeriti ima li ona *searchbase* definiciju.
-s *scope*	Određuje raspon pretraživanja. *scope* treba biti base, one ili sub, da odredi radi li se o pretraživanju baznog objekta, jedne razine ili strukture ispod stabla. Default je sub.
-a *deref*	Određuje kako se radi dereferenciranje pseudonima. *deref* treba biti never, always, search ili find, da se odredi da se pseudonimi nikad ne dereferenciraju, uvijek dereferenciraju, dereferenciraju pri pretraživanju ili se dereferenciraju samo kad se locira bazni objekt za pretraživanje. Default je da se pseudonimi nikad ne dereferenciraju.
-l *timelimit*	Čekaj najviše *timelimit* sekundi da pretraživanje završi.
-z *sizelimit*	Ograniči rezultate traženja na najviše *sizelimit* slogova. Ovime postaje moguće odrediti gornju granicu broja slogova koji se vraćaju kod operacije pretraživanja.
filter	Određuje ime filtera kojega pretraživanje koristi.
attrs...	Određuje atribute koje program učitava, ako pretraživanje nađe jedan ili više slogova. Ako na popisu nemate nikakvih vrijednosti za *attrs*, servisni program vraća sve atribute..

Primjeri: ldapsearch

Primjer 1:

Naredba ldapsearch cn=john doe cn telephoneNumber izvodi pretraživanje podstabla (koristeći default bazu pretraživanja) za unose s commonName john doe. Pretraživanjem se učitavaju vrijednosti commonName i telephoneNumber i ispisuju na standardni izlaz. Ako se traženjem nađu dva sloga, izlazni podatak izgleda otprilike ovako:

```
cn=John E Doe, ou=College of Literature, Science, and the Arts,
ou=Studenti, ou=Ljudi, o=Škola za više obrazovanje, 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=Odsjek informatičke tehnologije,
ou=Katedra i kadar,
ou=Ljudi, o=Škola za više obrazovanje, c=US
cn=John Doe
cn=John B Doe 1
cn=John B Doe
telephoneNumber=+1 313 555-1111
```

Primjer 2:

Naredba ldapsearch -t uid=jed jpegPhoto audio izvodi pretraživanje podstbla koristeći default bazu traženja za unose s korisničkim id-jem jed. Pretraživanjem se učitavaju jpegPhoto i audio vrijednosti i zapisuju u privremene datoteke. Ako se pretraživanjem nađe jedan slog s jednom vrijednošću za svaki traženi atribut, izlazni podaci izgledaju otprilike ovako:

```
cn=John E Doe,
ou=Odsjek informatičke tehnologije,
ou=Katedra i kadar,
ou=Ljudi, o=Škola za više obrazovanje, c=US
audio=/tmp/ldapsearch-audio-a19924
jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

Primjer 3:

Naredba ldapsearch -L -s one -b c=US o=university* o description izvodi jednorazinsko pretraživanje na c=US razini. Ovo pretraživanje traži sve organizacije čije ime organizationName počinje sa university. Rezultati se prikažu u LDIF formatu. Učitavaju se vrijednosti atributa organizationName i vrijednosti atributa opisa i ispisuju na standardni izlaz koji izgleda slično ovomu:

```
dn: o=University of Alaska Fairbanks, c=US
o: University of Alaska Fairbanks
opis: Priprema Aljaske za bolje sutra
opis: samo čvor lista

dn: o=University of Colorado at Boulder, c=US
o: University of Colorado at Boulder
opis: Informacije koje nisu za osoblje
opis: Zavod za obrazovanje i istraživanje

dn: o=University of Colorado at Denver, c=US
o: University of Colorado at Denver
o: UCD
o: CU/Denver
o: CU-Denver
opis: Zavod za više obrazovanje i istraživanje

dn: o=University of Florida, c=US
o: University of Florida
o: UFl
opis: Oblikovanje mladih umova
...
```

Primjer 4:

Kako je već razmotreno u “LDAP referali direktorija” na stranici 35, LDAP direktoriji Usluga Direktorija mogu imati nekoliko referalnih objekata, pod uvjetom da oni sadrže samo slijedeće:

- Razlikovno ime (dn).
- Klasu objekta (objectClass).
- Referalni atribut (ref).

Ovaj primjer pokazuje pretraživanja u kojima je uključen i referalni objekt.

Pretpostavite da System_A holds drži referal unos:

```
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: referral
```

Svi atributi povezani s unosom trebaju prebivati na System_B.

System_B sadrži slog:

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

kad klijent izdaje zahtjev System_A i ne pošalje manageDsaIT kontrolu, onda poslužitelj vraća referal. Na primjer, korištenjem -M na ldapsearch LDAP poslužitelj na System_A odgovara klijentu slijedećim URL-om:

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

Klijent koristi ove informacije da izda zahtjev System_B. Ako unos na System_A sadržava atribute kao dodatakdn, objectclass i ref, poslužitelj ignorira ove atribute.

Kad klijent primi referalni odgovor sa poslužitelja, on ponovo izdaje zahtjev, ali ovaj puta poslužitelju na koga se odnosi vraćena adresa URL. Ako je pretraživanje obavljeno s jednorazinskim opsegom, referal zahtjev koristi osnovni zahtjev. Rezultati ovog pretraživanja su različiti ovisno o vrijednosti koju navedete za raspon pretraživanja (**-b**).

Ako navedete -s sub, kako je prikazano ovdje:

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

pretraživanje vraća sve atribute za sve unose sa sn=Jensen koji prebivaju u ili ispod ou=Rochester, o=Big Company, c=US i na System_A i System_B. Klijent prima referal od System_A i prtražuje System_B, vraćajući cn=Barb Jense,ou=Rochester,o=Big Company,c=US.

Ako navedete -s one, kako je prikazano ovdje:

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

pretraživanje ne vraća nijedan slog s niti jednog sistema. Umjesto toga, poslužitelj vraća klijentu referalnu URL adresu:

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

Klijent na to šalje zahtjev:

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

Vraća unos cn=Barb Jensen,ou=Rochester,o=Big Company,c=US.

ldapmodrdn servisni program

Servisni program ldapmodrdn vam omogućuje da mijenjate relativno razlikovno ime (RDN) slogova na LDAP poslužitelju direktorija. Koristite ih iz QSH ljuske za naredbe na OS/400. On koristi ldap_modrdn aplikativno programsko sučelje (API).

Format:

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

Bilješke:

1. Ako unesete argumente s naredbene linije *dn* i *rdn*, *rdn* će zamijeniti RDN upisa kojega je odredio DN, *dn*. U protivnom, sadržaj datoteke (standardnih ulaznih podataka, ako ne date oznaku **-f**) bi se trebao sastojati od jednog ili više slogova.

   ```
   Prepoznatljivo (različito) ime (DN)

   Relativno razlikovno ime (RDN)
   ```

Jedan ili više praznih redaka razdvaja svaki par DN/RDN.

2. Ako ne dobavite informacije unosa iz *file* kroz korištenje **-f** opcije (ili iz para reda za naredbe *dn* i *rdn*), naredba ldapmodrdn će čekati na čitanje unosa sa standardnog ulaza. Ako želite prekinuti čekanje, pritisnite tipku SysReq, a zatim izaberite 2. Završi prethodni zahtjev.

Dijagnostika:

Izlazni status je 0, ako nema grešaka. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

Kliknite ovdje da vidite primjer upotrebe ldapmodrdn servisnog programa.

Parametri:

-V	Određuje LDAP verziju koju program koristi za povezivanje na LDAP poslužitelj. Po defaultu koristi LDAP V3 vezu. Da izričito izaberete LDAP V3, specificirajte -V 3. Specificirajte -V 2 za izvođenje kao LDAP V2 aplikacija.
-r	Uklanja vrijednoasti za staro relativno razlikovno ime (RDN) iz sloga. Default je da se čuvaju stare vrijednosti.
-M	Upravljajte referal objektima kao pravilnim unosima.
-n	Pokaži što bi bilo učinjeno ali ne mijenjaj upise. Korisno za analizu u spoju sa **-v**.
-v	Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.
-c	Kontinuirani operativni modus. Greške se javljaju, ali ldapmodrdn će nastaviti s preinakama. Default je izlaz iz programa nakon što se desi greška.
-R	Određuje da se preporuke ne slijede automatski.
-C *charset*	Određuje da nizovi unešeni kao ulazni podaci u servisni program budu prikazani u lokalnom skupu znakova (*charset*) i moraju se konvertirati u UTF-8. Koristite opciju **-C** charset, ako je kodna stranica ulaznog niza različita od kodne stranice posla. Pozovite se na dokumentaciju o ldap_set_iconv_local_charset() API da vidite koje *charset* vrijednosti su podržane.
-d *debuglevel*	Postavlja debug razinu na *debuglevel*.
-D *binddn*	Upotrijebi *binddn* za povezivanje na LDAP direktorij. *binddn* bi trebao biti znakovno prikazan DN.
-w *passwd*	Koristite *passwd* kao lozinku za provjeru ovlaštenja.
-m *mehanizam*	Upotrijebi *mehanizam* kad se određuje SASL mehanizam koji će se koristiti za povezivanje na poslužitelj. Koristit će se ldap_sasl_bind_s() API. Dostupni mehanizmi uključuju CRAM-MD5 (šifrira lozinku), EXTERNAL (korišten sa SSL) i GSSAPI (Kerberos). Parametar -m se zanemaruje ako je određeno -V 2. Ako **-m** mije naveden, koristi se jednostavna provjera identiteta.
-O *hopcount*	Odredi *hopcount* da se podesi najveći broj skokova koje će klijentova knjižnica poduzeti u potjeri za preporučiteljima. Default broj skokova je 10.
-h *ldaphost*	Određuje alternativni host na kojemu radi LDAP poslužitelj.
-p *ldapport*	Određuje alternativni port za Transmission Control Protocol (TCP) na kojemu LDAP osluškuje. Default LDAP port je 389. Ako nije naveden, a **-Z** je navedeno, koristi se default LDAP SSL port 636.
-Z	Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Opcija **-Z** je podržana samo u verzijama ovoga alata koje imaju mogućnost rada sa SSL.

-K *keyfile*	Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze klučeva. Ako pomoćni program ne može locirati bazu ključeva, koristiti će vrstno kodirani skup default povjerljivih korijena izdavača certifikata. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori. Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**.
-P *keyfilepw*	Određuje lozinku baze ključeva. Ova lozinka je obavezna za pristup šifriranim podacima u bazi ključeva (uključujući i privatni ključ). Ako je skrivena datoteka lozinki pridružena bazi podataka ključeva, lozinka se dobiva iz skrivene datoteke, a ovaj parametar nije potreban. Ovaj se parametar zanemaruje ako nisu navedeni ni **-Z** niti **-K**.
-N *certificatename*	Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru identiteta poslužitelja, klijentov certifikat nije potreban. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru identiteta klijenta i poslužitelja, klijentov certifikat je potreban. *certificatename* nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, *certificatename* nije potreban ako je jednostruk certifikat/privatni par ključeva u odredišnoj datoteci baze podataka ključeva. Ovaj se parametar zanemaruje ako nisu navedeni ni **-Z** niti **-K**.
-f *file*	Čita podatke o preinaci sloga iz LDIF datoteke umjesto iz standardnih ulaznih podataka ili naredbene crte (tako da se navede *dn* i novi *rdn*). Standardni ulaz može također biti dobavljen iz datoteke (< datoteka).
dn rdn	Određuje razlikovno ime nekog upisa koji se preimenuje i novo relativno razlikovno ime toga upisa.

Primjer: ldapmodrdn

Recimo da ste već kreirali tekstualnu datoteku /**tmp**/**entrymods** i da ona ima slijedeći sadržaj:

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

Slijedeća naredba:

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

će promijeniti RDN upisa Modify Me iz Modify Me u The New Me. Stari cn, Modify Me se briše.

Napomene o korištenju SSL-a s LDAP pomoćnim programima reda za naredbe

Za korištenje značajki Sloja sigurnih utičnica (SSL) pomoćnih programa reda za naredbe, morate imati instaliran jedan od proizvoda Cryptographic Access Provider (5722-ACx).

“Koristite Sloj sigurnih utičnica (SSL) i Sigurnost translacijskog sloja s poslužiteljem LDAP direktorija” na stranici 37 raspravlja o korištenju SSL-a s Usluge Direktorija LDAP poslužiteljem. Ove informacije uključuju upravljanje i kreiranje povjerljivih Izdavača certifikata s Upraviteljem digitalnih certifikata.

Neki od LDAP poslužitelja kojima pristupa klijent koriste samo provjeru autentičnosti poslužitelja. Kod ovih poslužitelja trebate samo definirati jedan ili više glavnih certifikata u spremištu certifikata. Pomoću provjere identiteta poslužitelja se klijent uvjerava da ciljni LDAP poslužitelj ima certifikat koji je izdao jedan od pouzdanih izdavača certifikata (CA). Uz to, sve LDAP transakcije sa poslužiteljem koje teku preko SSL veze su šifrirane. To obuhvaća i LDAP vjerodajnice koje isporučuje neko aplikativno programsko sučelje (API) koje se koristi za povezivanje na poslužitelj direktorija. Na primjer, ako LDAP poslužitelj koristi visoko pouzdani VeriSign certifikat, trebate napraviti slijedeće:

1. Pribaviti CA certifikat od Verisign-a.
2. Upotrijebiti DCM za importiranje certifikata u spremište certifikata.
3. Upotrijebiti DCM i označiti ju pouzdanom.

Ako LDAP poslužitelj koristi privatno izdan poslužiteljski certifikat, administrator poslužitelja može vam dobaviti kopiju datoteke zahtjeva poslužiteljskog certifikata. Importirajte datoteku zahtjeva za certifikatom u svoje spremište certifikata i označite ga kao pouzdanog.

Ako koristite osnove servisne programe za pristup LDAP poslužitelju koji koriste provjeru identiteta i klijenta i poslužitelja, morate napraviti slijedeće:

- Definirajte jedan ili više pouzdanih glavnih certifikata u spremištu certifikata. Time se klijent uvjerava da je ciljnom LDAP poslužitelju certifikat izdao pouzdani izdavač certifikata (CA). Uz to, sve LDAP transakcije sa poslužiteljem koje teku preko SSL veze su šifrirane. To obuhvaća i LDAP vjerodajnice koje isporučuje neko aplikativno programsko sučelje (API) koje se koristi za povezivanje na poslužitelj direktorija.
- Kreirajte par ključeva i zatražite klijentov certifikat od nekog izdavača certifikata (CA). Nakon što primite potpisani certifikat od izdavača, primite ga i u datoteku prstenova ključeva na klijentu.

Poglavlje 7. Nalaženje problema Usluge Direktorija

Nažalost, čak i pouzdani poslužitelji kao što je LDAP poslužitelj Usluga Direktorija ponekad imaju problema. Kad vaš LDAP poslužitelj direktorija ima problema, informacije što slijede vam mogu pomoći da uočite što ne valja i kako riješiti teškoću.

- “Osnovni postupak otkrivanja i rješavanja problema kod Usluga Direktorija”
- “Uobičajene greške na LDAP klijentu” na stranici 61

Za više informacija o uobičajenim Usluge Direktorija problemima, pogledajte Usluge Direktorija home stranicu na slijedećem URL-u:

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

Osnovni postupak otkrivanja i rješavanja problema kod Usluga Direktorija

Možete naći povratne kodove za LDAP greške u ldap.h datoteci, koja se nalazi na vašem sistemu u QSYSINC/H.LDAP.

Kad dobijete grešku na vašem LDAP poslužitelju direktorija i želite više detalja, još jedna akcija koju možete poduzeti je da pogledate QDIRSRV dnevnik poslova. Za ponovljive greške, možete koristiti naredbu Prati TCP/IP aplikaciju (TRCTCPAPP APP(*DIRSRV)) da utvrdite trag grešaka. Pogledajte “Koristite TRCTCPAPP za pomoć u nalaženju problema” na stranici 60 za više informacija.

Usluge Direktorija koriste nekoliko SQL poslužitelja. Kad dođe do neke SQL greške, QDIRSRV dnevnik posla će obično sadržavati slijedeću poruku:

```
desila se SQL greška -1
```

U tim slučajevima će vas dnevnik posla QDIRSRV uputiti na dnevnike posla SQL poslužitelja. Međutim, u nekim slučajevima, QDIRSRV ne mora imati ovu poruku i uputu, čak i ako je neki SQL poslužitelj uzrokom problema. U tim slučajevima, pomoći će vam da znate koje SQL poslužitelje treba pokrenuti i za što ih Usluge Direktorija koriste.

Kad se LDAP poslužitelj direktorija normalno pokrene, on javi poruke slične ovima u nastavku:

Bilješka: Poruke i broj pokrenutih poslova na SQL poslužitelju mogu biti različiti u nekom od slijedećih slučajeva:

- Poslužitelj pokrećete po prvi puta.
- Migracija se treba tek desiti.
- Poslužitelj koristi dnevnik promjena.
- Vaš poslužitelj je postavljen da dozvoljava veći broj veza baze podataka.

```
                                                    Sistem:   WARMERS
Posao . :   QDIRSRV       Korisnik :   QDIRSRV       Broj . . . . :   174440

  >> CALL PGM(QSYS/QGLDSVR)
     Posao 057448/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057340/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057448/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057166/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057279/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057288/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Poslužitelj Usluga Direktorija uspješno pokrenut.
```

Usluge Direktorija koriste prvi SQL poslužitelj, 057448/QUSER/QSQSRVR, tokom podizanja LDAP poslužitelja. Usluge Direktorija mogu pokrenuti i dodatne poslužitelje tokom podizanja LDAP poslužitelja,

prema potrebi, ako poslužitelj pokrećete po prvi puta, ako se treba desiti migracija ili ako poslužitelj koristi dnevnik promjena. Nakon podizanja, ovi SQL poslužitelji se otpuštaju.

U ovom primjeru, nisu korišteni dodatni SQL poslužitelji za migraciju ili pokretanje poslužitelja i dnevnik promjena nije konfiguriran. Usluge Direktorija koristi slijedeći SQL poslužitelj (057340/QUSER/QSQSRVR) za replikaciju.

Zadnja veza u ovom primjeru (057288/QUSER/QSQSRVR) koristi se za dodavanje, preinaku, modrdn i brisanje operacija. Ostale veze se koriste za traženje, vezanje i uspoređivanje.

Na poslužiteljima direktorija **Baza podataka**/**Sufiksi** stranica Svojstava u iSeries Navigator specificirate ukupan broj SQL poslužitelja koji Usluge Direktorija koristi za operacije direktorija nakon pokretanja poslužitelja. Uz to, jedan SQL poslužitelj je uvijek konfiguriran za replikaciju.

Nadgledajte greške i pristup s Usluge Direktorija dnevnikom poslova

Gledanje u dnevnik posla LDAP poslužitelja može vas ponekad upozoriti na greške i pomoći vam u praćenju pristupa na poslužitelj.

Ako je poslužitelj pokrenut, a želite pogledati QDIRSRV dnevnik posla, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom kliknite na **Direktorij** i izaberite **Poslovi poslužitelja.**.
5. Iz izbornika **Datoteka** izaberite **Dnevnik posla**.

Ako je poslužitelj zaustavljen, a želite pogledati QDIRSRV dnevnik posla, poduzmite ove korake:
1. U iSeries Navigator, proširite **Osnovne operacije**.
2. Kliknite **Izlaz pisača**.
3. QDIRSRV se pojavljuje u **User** stupcu iSeries Navigator desnog panela. Ako želite pogledati dnevnik posla, dva puta kliknite **Qpjoblog** lijevo od QDIRSRV u istom redu.

   Bilješka: iSeries Navigator je možda konfiguriran da prikaže samo spool datoteke. Ako se QDIRSRV ne pojavi na listi, kliknite **Izlaz pisača**, zatim izaberite **Uključi** iz izbornika **Opcije**. Navedite **Sve** u polju **Korisnik**, a zatim kliknite **OK**.

Bilješka: Usluge Direktorija koriste druge sistemske resurse za izvođenje nekih poslova. Ako dođe do greške kod jednog od tih resursa, u dnevniku posla će biti naznačeno kamo ići po potrebne informacije. U nekim slučajevima Usluge Direktorija neće biti u stanju odrediti kamo pogledati. U tim slučajevima, pogledajte poslužiteljev Structured Query Language (SQL) dnevnik posla da vidite je li problem vezan za SQL poslužitelje.

Koristite TRCTCPAPP za pomoć u nalaženju problema

Vaš poslužitelj daje komunikacijsko praćenje za skupljanje podataka na komunikacijskoj liniji, kao što je sučelje mreže lokalnog područja (LAN) ili mreže širokog područja (WAN). Prosječan korisnik možda neće razumjeti cijeli sadržaj podataka praćenja. Ipak, možete koristiti unose praćenja za određivanje je li se izmjena podataka između dvije točke stvarno desila.

Naredba Prati TCP/IP aplikaciju (TRCTCPAPP) s *DIRSRV opcijom može se koristiti na LDAP poslužitelju direktorija za pomoć u nalaženju problema s klijentima ili aplikacijama.

Za detaljnije informacije o korištenju naredbe TRCTCPAPP s LDAP-om kao i ograničenjima na potrebna ovlaštenja, pogledajte Opis naredbe TRCTCPAPP (Prati TCP/IP aplikaciju).

Za općenite informacije o korištenju praćenja komunikacije, pogledajte Praćenje komunikacije.

Koristite opciju LDAP_OPT_DEBUG za praćenje grešaka

| Počevši s V5R2, možete koristiti LDAP_OPT_DEBUG opciju **ldap_set_option()** API-ja za praćenje
| problema s klijentima koji koriste LDAP C API-je. Debug opcija ima višestruke razine debug postavki koje
| možete koristiti kao pomoć u uklanjanju problema s ovim aplikacijama.

| Slijedeće je primjer omogućavanja klijentske debug opcije praćenja.

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

| Drugi način postavljanja debug razine je konfiguriranje brojčane vrijednosti za LDAP_DEBUG varijablu
| okruženja, za posao u kojem se klijentska aplikacija izvodi, na istu brojčanu vrijednost koju debugvalue
| imala ako se koristi **ldap_set_option()** API.

| Primjer omogućavanja praćenja klijenta korištenjem LDAP_DEBUG varijable okruženja je slijedeći:

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

| Nakon izvođenja klijenta koji stvara problem, upišite slijedeće u iSeries prompt:

```
| DMPUSRTRC    ClientJobNumber
```

| gdje je ClientJobNumber broj posla klijenta.

| Za interaktivni prikaz ovih informacija, upišite slijedeće u iSeries prompt:

```
| DSPPFM  QAPOZDMP  QPOZnnnnnn
```

| gdje je nnnnnn broj posla.

| Da sačuvate ove informacije kako bi ih poslali usluzi, poduzmite slijedeće korake:
| 1. Kreirajte SAVF datoteku koristeći naredbu kreiraj SAVF (CRTSAVF).
| 2. Upišite slijedeće u iSeries prompt za naredbe.

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

| gdje je *xxx* ime koje ste specificirali za SAVF datoteku.

Uobičajene greške na LDAP klijentu

Poznavanje uzroka uobičajenih grešaka na LDAP klijentu vam može pomoći da riješite probleme sa svojim poslužiteljem. Za potpun popis LDAP uvjeta klijentskih grešaka, pogledajte predmet OS/400 Usluge Direktorija pod Programiranje u iSeries Informativni Centar.

Poruke o greškama na klijentu imaju slijedeći format:

```
[Neuspjela LDAP operacija]:[LDAP klijent API stanje greške]
```

Bilješka: Objašnjenje ovih grešaka pretpostavlja da klijent komunicira s LDAP poslužiteljem na OS/400. Klijent koji s poslužiteljem komunicira na nekoj drugoj platformi može dobiti slične poruke o greškama ali će uzroci i rješenja najvjerojatnije biti drugačiji.

Uobičajene greške obuhvaćaju slijedeće:

- "ldap_search: Vremensko ograničenje prekoračeno" na stranici 62
- "[Neuspjela LDAP operacija]: Greška operacija" na stranici 62

- “ldap_bind: Nema takvog objekta”
- “ldap_bind: Neodgovarajuća provjera identiteta”
- “[Neuspjela LDAP operacija]: Nedostatan pristup”
- “[neuspjela LDAP operacija]: Ne mogu kontaktirati LDAP poslužitelj”
- “[neuspjela LDAP operacija]: Ne mogu se povezati na ssl poslužitelj” na stranici 63

ldap_search: Vremensko ograničenje prekoračeno

Ove se dešava kad ldapsearches radi sporo. Ako ispravljate ovu grešku, napravite jednu od slijedećih stvari ili obje:

- Povećajte granicu vremena pretraživanja za LDAP poslužitelj direktorija. Vidjeti “Prilagodite performanse poslužitelja LDAP direktorija” na stranici 30, ako trebate informacije kako se to radi.
- Smanjite aktivnost na vašem sistemu. Možete i smanjiti broj aktivnih poslova LDAP klijenta koji se izvode.

[Neuspjela LDAP operacija]: Greška operacija

Ovu grešku može generirati nekoliko stvari. Da dobijete informacije o uzroku ove greške za određenu instancu, pogledajte u QDIRSRV i Structured Query Language (SQL) dnevnike posla poslužitelja kako je opisano u “Osnovni postupak otkrivanja i rješavanja problema kod Usluga Direktorija” na stranici 59.

ldap_bind: Nema takvog objekta

Uobičajeni uzrok ove greške je da korisnik radi grešku upisivanja pri izvođenju operacije. Drugi uobičajeni uzrok je kad se LDAP poslužitelj pokušava povezati sa DN koji ne postoji. Ovo se često dešava kad korisnik navodi ono što pogrešno misli da je administratorov DN. Na primjer, korisnik može specificirati QSECOFR ili Administrator, kad stvarni administratorov DN može biti nešto kao cn=Administrator.

Za detalje o greški, pogledajte QDIRSRV dnevnik posla opisan u “Osnovni postupak otkrivanja i rješavanja problema kod Usluga Direktorija” na stranici 59.

ldap_bind: Neodgovarajuća provjera identiteta

Poslužitelj vraća Pogrešna preporuka kad je lozinka ili DN povezivanja pogrešan. Poslužitelj vraća neodgovarajuća provjera autentičnosti kad se klijent pokušava povezati kao jedno od slijedećeg:

- Unos koji nema userpassword atribut
- Unos koji predstavlja OS/400 korisnika, koji ima UID atribut i nema userpassword atribut. Ovo uzrokuje da se usporedba vrši između specificirane lozinke i OS/400 korisnikove lozinke, koje se ne podudaraju.
- Unos koji predstavlja projiciranog korisnika i način povezivanja različit od zahtijevanog.

Ova greška se obično pojavi kad klijent pokušava povezivanje s lozinkom koja nije valjana. Za dobivanje detalja o grešci, pogledajte QDIRSRV dnevnik posla kao što je opisano u“Osnovni postupak otkrivanja i rješavanja problema kod Usluga Direktorija” na stranici 59.

[Neuspjela LDAP operacija]: Nedostatan pristup

Ova se greška obično pojavi kad DN koji se povezuje nema ovlaštenje za izvođenje operacije (kao što je dodavanje ili brisanje) koju zahtijeva klijent. Ako želite vidjeti pojedinosti o greški, pogledajte u dnevnik posla QDIRSRV kako je opisano u “Osnovni postupak otkrivanja i rješavanja problema kod Usluga Direktorija” na stranici 59.

[neuspjela LDAP operacija]: Ne mogu kontaktirati LDAP poslužitelj

Najuobičajeniji uzroci ove greške obuhvaćaju slijedeće:

- LDAP klijent postavi zahtjev prije nego je LDAP poslužitelj na specificiranom sistemu pokrenut i u odabranom stanju čekanja.
- Korisnik navede broj porta koji nije važeći. Na primjer, poslužitelj osluškuje na portu 386 ali klijentov zahtjev pokušava na portu 387.

Ako želite vidjeti pojedinosti o greški, pogledajte dnevnik posla QDIRSRV kako je opisano u “Osnovni postupak otkrivanja i rješavanja problema kod Usluga Direktorija” na stranici 59. Ako je poslužitelj Usluga direktorija uspješno pokrenut, poruka Poslužitelj Usluga direktorija uspješno pokrenut će biti u QDIRSRV dnevniku posla.

[neuspjela LDAP operacija]: Ne mogu se povezati na ssl poslužitelj

Ova greška se javlja kad LDAP poslužitelj odbije spajanje klijenta zato što se ne može uspostaviti SSL veza. To može biti uzrokovano nečim od slijedećeg:

- Podrška Upravljanja certifikatima odbija klijentov pokušaj povezivanja na poslužitelj. Koristite Upravitelj digitalnih certifikata da osigurate da su vaši certifikati ispravno postavljeni, zatim ponovo pokrenite poslužitelj i pokušajte se ponovo povezati.
- Korisnik možda nema pristup za čitanje *SYSTEM pohrani certifikata (po defaultu /QIBM/userdata/ICSS/Cert/Server/default.kdb).

Za OS/400 C aplikacije, dodatne informacije o SSL greški su dostupne. Pogledajte dokumentaciju za individualne API-je Usluga Direktorija za detalje.

Tiskano u Hrvatskoj