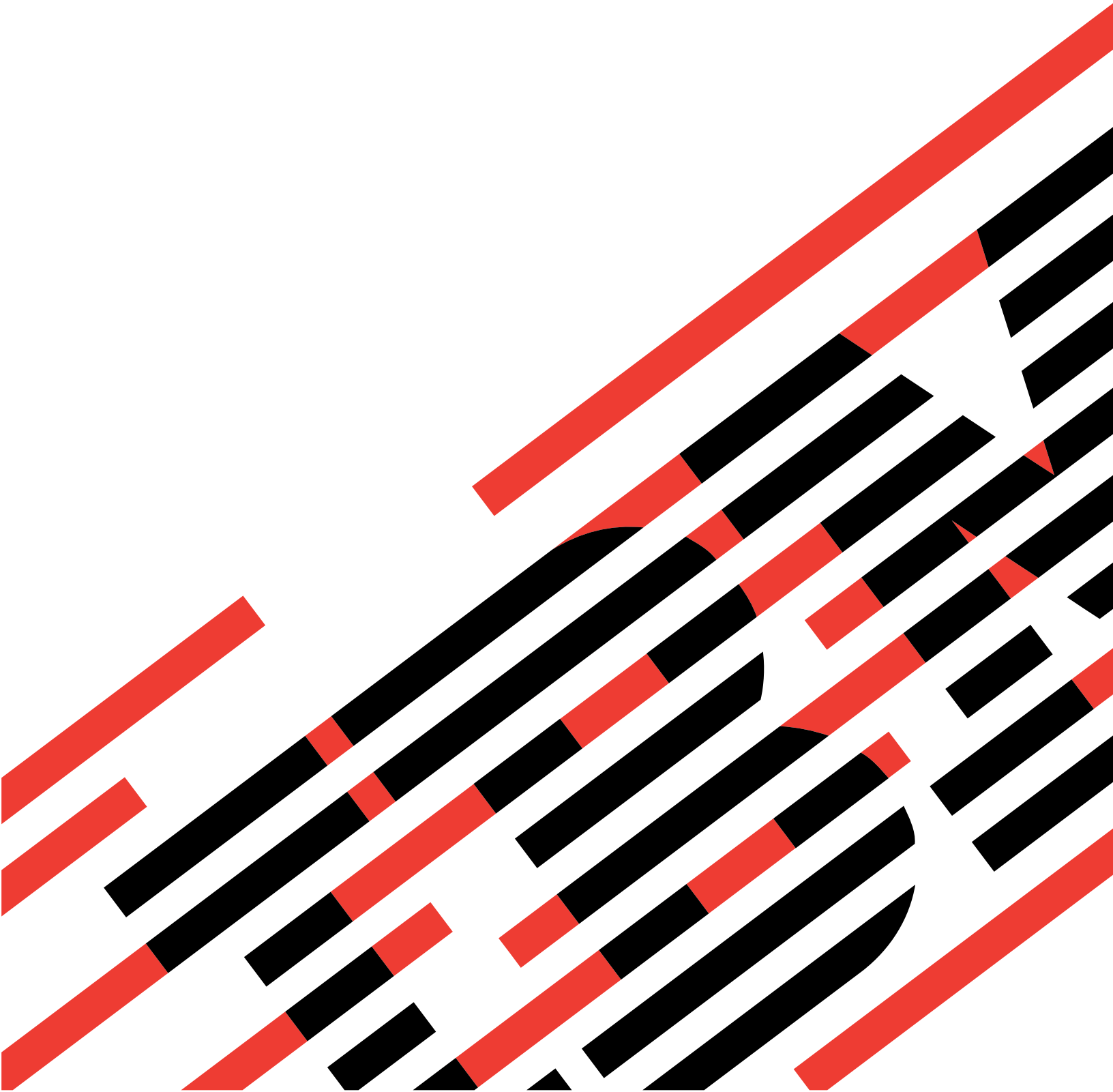
IBM

eserver

iSeries

Imeniške storitve za delo z omrežjem(LDAP)



IBM

@server

iSeries

Imeniške storitve za delo z omrežjem(LDAP)

Kazalo

Del 1. Imeniške storitve (LDAP)

Imeniške storitve nudijo v iSeries strežnik LDAP (Lightweight Directory Access Protocol). LDAP se izvaja prek TCP/IP (Transmission Control Protocol/Internet Protocol) in je popularen kot imeniška storitev za internetne in ne-internetne aplikacije.

Če Imeniške storitve že poznate, lahko preberete kaj je novega za to izdajo. Če želite, lahko natisnete ali prikažete informacije o Imeniških storitvah v obliki PDF.

Naslednje teme predstavljajo Imeniške storitve in nudijo informacije, ki vam bodo v pomoč pri upravljanju strežnika LDAP v strežniku iSeries:

Če želite dodatne informacije o Imeniških storitvah, obiščite spletno stran Imeniških storitev  .

Strežnik LDAP, ki nudi Imeniške storitve, je Imenik IBM SecureWay  .

Poglavje 1. Novosti za V5R2

Imeniške storitve imajo naslednje izboljšave in nove možnosti.

- Začenši z V5R1 so imeniške storitve del osnove operacijskega sistema. Začenši v V5R2 možnost 32 ni več na voljo.
- Nove izboljšave zaščite so bile izvedene za še boljšo zaščito poljubnih podatkov, shranjenih v imeniškem strežniku.
- Imeniški strežnik LDAP lahko zdaj uporabite kot krmilnik domene za domeno preslikave identitete podjetja (EIM).
- Na voljo je nova možnost za skrbnike, ki jo lahko uporabljajo za dodeljevanje skrbniškega dostopa do imeniškega strežnika za uporabnike, katerim je bil dan dostop do identifikatorja funkcije (ID) skrbnika imeniških storitev (QIBM_DIRSRV_ADMIN) operacijskega sistema prek podpore aplikacije Navigator iSeries .
- Izberete lahko, da imeniški strežnik uporablja specifične naslove IP ali pa vse konfigurirane naslove IP na strežniku. Za dodatne informacije glejte “Spreminjanje vrat ali naslova IP” na strani 19.
- API **ldap_set_option** ima novo funkcijo sledenja razhroščevanja za V5R2. Možnost LDAP_OPT_DEBUG lahko uporabite kot pomoč pri diagnosticiranju problemov z odjemalci, ki uporabljajo API-je C LDAP. Če želite podrobnejše informacije, preglejte “Uporaba možnosti LDAP_OPT_DEBUG za sledenje napak” na strani 61 ali preglejte API-je Imeniških storitev v Informacijskem centru iSeries .

Nasveti za prikaz novosti in sprememb:

Te informacije uporabljajo za označevanje tehničnih sprememb naslednje:

- Sliko , ki označuje, kje se začnejo nove ali spremenjene informacije.
- Sliko , ki označuje, kje se nove ali spremenjene informacije končajo.

Poglavje 2. Tiskanje tega poglavja

Če želite prikazati ali shraniti različico PDF, izberite Imeniške storitve (LDAP) (približno 323 KB ali 66 strani).

Druge informacije

Pregledate ali natisnete pa lahko tudi kateregakoli izmed naslednjih PDF-jev:

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

Če želite shraniti datoteko PDF na delovno postajo za prikaz ali tiskanje, naredite naslednje:
1. V pregledovalniku odprite različico PDF (kliknite zgornjo povezavo).
2. Na meniju pregledovalnika kliknite **Datoteka**.
3. Kliknite **Shrani kot...**
4. Poiščite imenik, v katerega želite shraniti datoteko PDF.
5. Kliknite **Shrani**.

Prenos programa Adobe Acrobat Reader

Če za pregledovanje ali tiskanje teh PDF-jev potrebujete program Adobe Acrobat Reader, lahko kopijo prenesete s spletne strani podjetja Adobe (www.adobe.com/products/acrobat/readstep.html) .

Poglavje 3. Prvi koraki v Imeniških storitvah

Imeniške storitve nudijo v iSeries strežnik LDAP (Lightweight Directory Access Protocol). LDAP se izvaja prek TCP/IP (Transmission Control Protocol/Internet Protocol) in je postal popularen kot imeniška storitev za internetne in ne-internetne aplikacije. Večino upravnih in nastavitvenih opravil lahko v imeniškem strežniku LDAP, ki temelji na OS/400, izvedete prek grafičnega uporabniškega vmesnika Navigatorja operacij. Za upravljanje Imeniških storitev morate imeti Navigator iSeries nameščen na PC-ju, ki je povezan s strežnikom iSeries. Imeniške storitve lahko uporabljate z aplikacijami, ki omogočajo LDAP, kot so aplikacije za pošto, ki iščejo naslove elektronske pošte v strežnikih LDAP.

Poleg strežnika LDAP vključujejo Imeniške storitve tudi naslednje:

- Odjemalec LDAP, ki temelji na OS/400. Ta odjemalec vsebuje niz vmesnikov uporabniških programov (API-jev), ki jih lahko v programih OS/400 uporabite za izdelavo svojih lastnih aplikacij. Če želite informacije o teh API-jih, preglejte temo Imeniške storitve pod Programiranje v Informacijskem centru iSeries.
- Različica 3.2 kompleta orodij IBM SecureWay Directory Client Software Development Kit (SDK). SDK vsebuje odjemalca LDAP Windows in naslednja orodja:
  - Orodja za upravljanje imenikov IBM SecureWay, ki nudijo grafični uporabniški vmesnik za upravljanje vsebine imenika.
  - Pomožni programi ukazne vrstice (ldapsearch, ldapadd, itd.)
  - API-ji LDAP C (datoteke knjižnice, datoteke oglavja in izvorna koda zgleda)
  - Ponudnika storitev LDAP JNDI IBM (ibmjndi.jar)
  - Zaslonska dokumentacija za vse omenjene postavke. V datoteki preberi boste našli imena ter nahajališča teh datotek HTML.

Če ste Imeniške storitve uporabili s predhodno različico OS/400, preglejte “Selitev v V5R2 iz prejšnje izdaje Imeniških storitev” na strani 11.

Za predstavitev LDAP preglejte “Osnove LDAP” na strani 8. Če ste uporabljali strežnike LDAP na drugih platformah, si vzemite nekaj minut, in preberite to temo, ker vsebuje nekaj informacij, ki so specifične za OS/400.

Ko se spoznate z osnovnimi informacijami, pojdite na razdelek “Načrtovanje imeniškega strežnika LDAP” na strani 11.

Če želite informacije o namestitvi in konfiguriranju imeniškega strežnika, preglejte “Namestite in konfiguriranje Imeniških storitev” na strani 14.

Dokumentacija

Tema Imeniške storitve v Informacijskem centru iSeries podaja pregled LDAP in se osredotoča na upravljanje imeniškega strežnika LDAP OS/400. Ta dokumentacija podaja tudi celotno dokumentacijo za SecureWay Directory Client SDK. Če želite dodatne informacije o LDAP, preglejte referenčne informacije LDAP, kot so:

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

- *LDAP: Programming Directory-enabled Applications with Lightweight Directory Access Protocol* , katerega avtorja sta Tim Howes in Mark Smith.
- *Razumevanje in razvitje imeniških storitev LDAP*, avtorjev Mark C. Smith, Gordon S. Good in Tim Howes.

Dodatne informacije o Imeniških storitvah na strežniku iSeries so na voljo na domači strani Imeniških storitev strežnika iSeries .

Opomba: Nekaj gradiva, ki je vključeno v tem dokumentu, je izpeljano iz dokumentacije LDAP Univerze v Michiganu. Copyright © 1992-1996, Regents of the University of Michigan, Vse pravice pridržane.

Osnove LDAP

LDAP (Lightweight Directory Access Protocol) je imeniška storitev, ki teče prek TCP/IP (Transmission Control Protocol/Internet Protocol). LDAP različice 2 je formalno definiran v IETF (Internet Engineering Task Force) Request for Comments (RFC) 1777, *Lightweight Directory Access Protocol*. LDAP različice 3 je formalno definiran v IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*. Te RFC-je lahko pregledate na internetnem naslovu:

http://www.ietf.org

Imeniške storitve LDAP sledijo modelu odjemalec/strežnik. En ali več strežnikov LDAP vsebujejo podatke imenikov. Odjemalec LDAP se poveže s strežnikom LDAP in izda zahtevo. Strežnik se odzove z odgovorom, ali s kazalcem (referenčnim kazalcem) na drugi strežnik LDAP.

Uporaba LDAP:

Ker je LDAP bolj podoben imeniški storitvi, kot pa bazi podatkov, so informacije v imeniku LDAP običajno opisne, temelječe na lastnostih. Uporabniki LDAP običajno prebirajo informacije v imeniku pogosteje, kot jih spreminjajo. Spremembe so običajno preproste spremembe vseh ali nobenih informacij. Splošna uporaba imenikov LDAP vključuje zaslonske telefonske imenike in imenike elektronske pošte.

Struktura imenikov LDAP:

Model imeniških storitev LDAP temelji na **postavkah** (ki jim rečemo **objekti**). Vsaka postavka je sestavljena iz ene ali več **lastnosti**, kot so ime ali naslov in **tip**. Tipi so običajno sestavljeni iz mnemoničnih nizov, kot sta cn za splošno ime (common name) in mail za naslov elektronske pošte.

Slika 1 na strani 10 kaže zgled imenika za postavko za Tim Jones, ki vključuje lastnosti *mail* in *telephoneNumber*. Nekatere druge mogoče lastnosti so *fax*, *title*, *sn* (za priimek) in *jpegPhoto*.

Vsak imenik ima **shemo**, v obliki niza pravil, ki določajo strukturo in vsebino imenika. Če želite urediti datoteke shem za strežnik LDAP, morate uporabiti orodja za upravljanje imenikov (DMT) IBM SecureWay.Po namestitvi Imeniških storitev so datoteke v sistemu v imeniku /QIBM/UserData/OS400/DirSrv.

Opomba: Izvirne kopije datotek privzete sheme so v imeniku /QIBM/ProdData/OS400/DirSrv. Če morate zamenjati datoteke v imeniku UserData, lahko te datoteke prekopirate v imenik /QIBM/ProdData/OS400/DirSrv.

Vsaka postavka imenika ima posebno lastnost z imenom **objectClass**. Ta lastnost krmili, katere lastnosti so zahtevane in dovoljene v postavki. Z drugimi besedami, vrednosti lastnosti objectClass določajo pravila sheme, ki se jim mora postavka podrejati.

Vsaka postavka imenika ima tudi naslednje **operativne lastnosti**, ki jih strežnik LDAP vzdržuje samodejno:

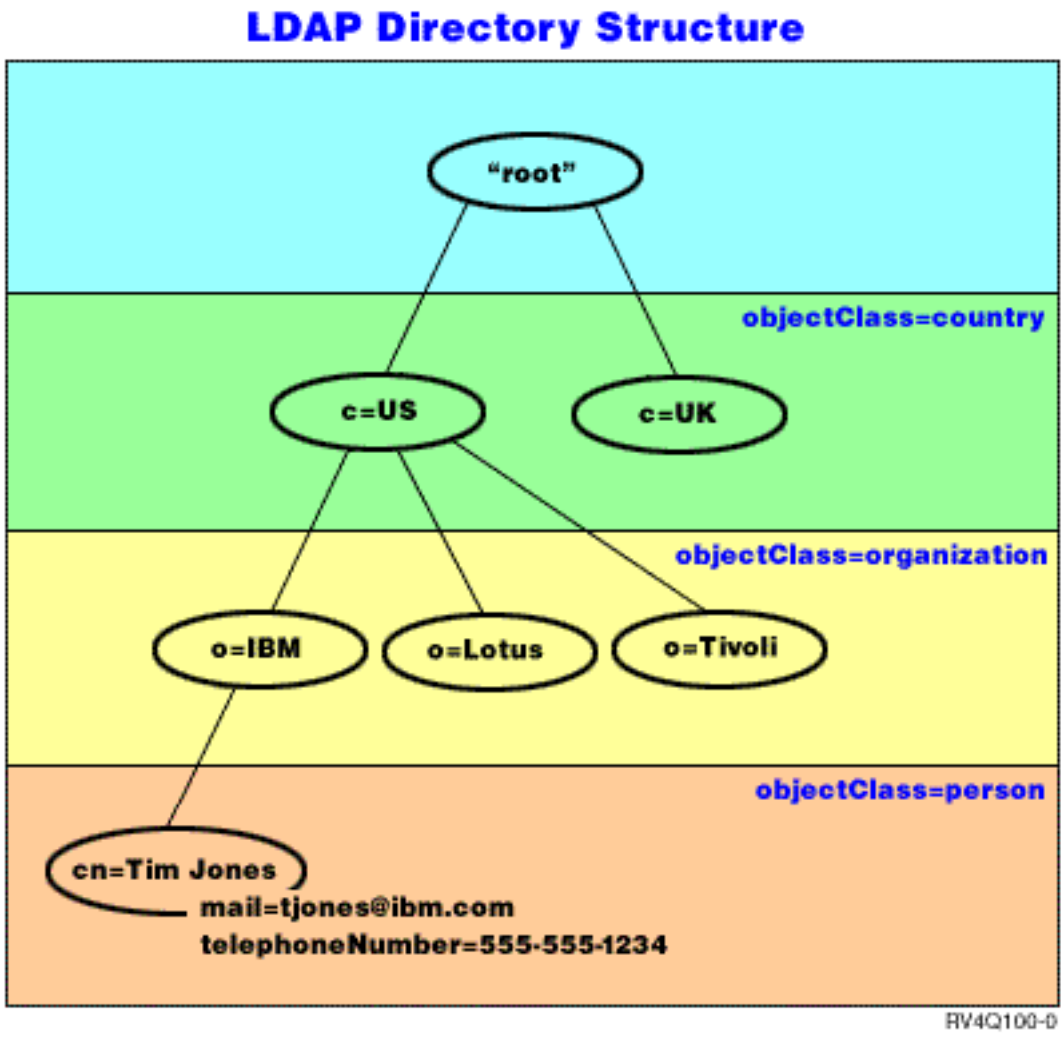
- CreatorsName, ki vsebuje povezovalni DN, uporabljen pri izdelavi postavke.
- CreateTimestamp, ki vsebuje podatek o času, v katerem je bila postavka izdelana.
- modifiersName, ki vsebuje povezovalni DN, uporabljen pri zadnjem spreminjanju postavke (izvirno je ta enak kot CreatorsName).
- modifyTimestamp, ki vsebuje čas zadnjega spreminjanja postavke (izvirno je ta enak kot CreateTimestamp).

Običajno so postavke imenika LDAP urejene v hierarhični strukturi, ki odraža politične, geografske in organizacijske omejitve (Slika 1 na strani 10). Postavke, ki predstavljajo države, se pojavljajo na vrhu hierarhije. Postavke, ki predstavljajo dežele (države) ali državne organizacije zasedajo drugo raven v hierarhiji. Spodnje postavke lahko predstavljajo ljudi, organizacijske enote, tiskalnike, dokumente ali druge postavke.

Pri strukturiranju imenika niste omejeni na običajno hierarhijo. Struktura komponenta domene je na primer tudi zelo popularna. V tej strukturi so postavke sestavljene kot deli imen domen TCP/IP. Na primer dc=ibm,dc=com lahko nastavite na o=ibm,c=us.

LDAP se nanaša na postavke z **razločevalnimi imeni** (DN-ji). Razločevalno ime je sestavljeno iz imena postavke, kot tudi iz imen objektov nad njo v imeniku, v vrstnem redu od spodaj navzgor. Celotno razločevalno ime za postavko v spodnjem levem kotu, ki jo vsebuje Slika 1 na strani 10, je na primer cn=Tim Jones, o=IBM, c=US. Vsaka postavka ima najmanj eno lastnost, ki je uporabljena za ime postavke. Ta lastnost za poimenovanje se imenuje **relativno razločevalno ime (RDN)** postavke. Postavka nad podanim RDN se imenuje **nadrejeno razločevalno ime**. V zgornjem zgledu cn=Tim Jones poimenuje postavko, torej je RDN. o=IBM, c=US je nadrejeni DN za cn=Tim Jones.

Če želite podati strežniku LDAP zmožnost upravljanja dela imenika LDAP, podajte v konfiguraciji strežnika najvišjo raven nadrejenih razločevalnih imen. Ta razločevalna imena se imenujejo **pripone**. Strežnik lahko dostopa do vseh objektov v imeniku, ki so pod podano pripono v hierarhiji imenikov. Če je na primer strežnik LDAP vsebovan v imeniku, ki ga kaže Slika 1 na strani 10, mora imeti v svoji konfiguraciji podano pripono o=ibm, c=us, da bo lahko odgovarjal poizvedbam odjemalcev, ki se nanašajo na Tim Jones.



Slika 1. Osnovna struktura imenikov LDAP

Notes o LDAP in Imeniških storitvah:

- Začenši z V4R5 strežnik LDAP OS/400 in odjemalec LDAP OS/400 temeljita na različici LDAP3. Odjemalca V2 lahko uporabite s strežnikom V3. Odjemalca V3 ne morete uporabiti s strežnikom V3, razen v primeru, da se povežete kot odjemalec V2 in uporabljate samo API-je V2. Če želite podrobnejše informacije, preglejte Problematika LDAP V2/V3.
- Odjemalec LDAP Windows temelji na LDAP različice 3.
- Ker je LDAP standarden, lahko vsi strežniki LDAP souporabljajo veliko osnovnih značilnosti. Zaradi razlik pri izvedbi niso v celoti združljivi med seboj. Strežnik LDAP, ki ga nudijo Imeniške storitve, je tesno združljiv z imeniškimi strežniki LDAP v skupini izdelkov v imeniku IBM SecureWay in skupini izdelkov imenikov IBM. Morda ne bodo združljivi z drugimi strežniki LDAP.
- Podatki za strežnik LDAP, ki jih nudijo Imeniške storitve, so v bazi podatkov OS/400.

Dodatne informacije:

Za zglede o uporabi imenikov LDAP preglejte naslednje:

- Razdelek 1.6 Hitri začetki: Zgled javnega LDAP v rdeči knjigi *Understanding LDAP*.
- Razdelek 3.3 Zgledi scenarijev v rdeči knjigi Understanding LDAP.

Če želite zvedeti več o pojmih LDAP, preglejte Poglavje 5, “Pojmi in referenčne informacije o Imeniških storitvah AS/400” na strani 31.

Premislek ob uporabi LDAP V2 z LDAP V3

Začenši z V4R5 strežnik LDAP OS/400 in odjemalec LDAP OS/400 temeljita na različici LDAP3. Odjemalca V3 lahko uporabite s strežnikom V2. Za spremembo različice odjemalca V3 v V2 lahko uporabite API ldap_set_option(). Nato lahko uspešno pošiljate zahteve odjemalcev strežniku V2.

Odjemalca V2 lahko uporabite s strežnikom V3. Zavedajte se, da lahko v zahtevah za iskanje strežnik V3 vrne podatke v popolnem območju formata UTF-8, medtem ko odjemalec V2 lahko obravnava samo podatke v naboru znakov IA5.

Opomba: LDAP različice 2 je formalno definiran v IETF (Internet Engineering Task Force) Request for Comments (RFC) 1777, *Lightweight Directory Access Protocol*. LDAP različice 3 je formalno definiran v IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*. Te RFC-je lahko pregledate na internetnem naslovu:

http://www.ietf.org

Načrtovanje imeniškega strežnika LDAP

Preden namestite Imeniške storitve in začnete s konfiguriranjem imenika LDAP, si vzemite nekaj minut za načrtovanje imenika. Ne pozabite razmisliti o naslednjih pomembnih stvareh:

- **Organiziranje imenika**. Načrtujte strukturo imenika in določite, katere pripone in lastnosti bo zahteval vaš strežnik.
- **Določitev velikosti imenika**. Nato lahko ocenite, koliko pomnilnika potrebujete. Velikost imenika je odvisna od:
  - Števila lastnosti v shemi strežnika.
  - Števila postavk v strežniku.
  - Tipa informacij, ki jih hranite v strežniku.

  Prazen imenik, ki uporablja privzeto shemo Imeniških storitev AS/400, zahteva na primer približno 10 MB prostora. Imenik, ki uporablja privzeto shemo, in vsebuje 1000 postavk tipičnih informacij o zaposlenih, zahteva približno 30 MB prostora. To število se spreminja glede na natančno število uporabljenih lastnosti. Zelo se poveča v primeru, če v imeniku hranite velike objekte, kot so slike.
- **Določanje varnostnih ukrepov**. Imeniške storitve omogočajo, da za zaščito komunikacij uporabite SSL (plast zaščitenih vtičnic) in digitalna potrdila ter zaščito prevajalne plasti (TLS) . Začenši v V5R1 je podprto tudi overjanje Kerberos.
- Imeniške storitve omogočajo, da s seznami za nadzorovanje dostopa (ACL-ji) nadzorujete dostop do objektov imenika. Za zaščiti imenikov lahko uporabite Beleženje zaščite OS/400.

Selitev v V5R2 iz prejšnje izdaje Imeniških storitev

OS/400 V5R2 predstavlja nove komponente in možnosti v Imeniških storitvah. Te spremembe se nanašajo na imeniški strežnik LDAP in na grafični uporabniški vmesnik (GUI) Navigatorja operacij. Da bi lahko izkoristili prednost novih možnosti GUI, morate namestiti Navigator iSeries v PC, ki lahko prek TCP/IP komunicira s strežnikom iSeries. Navigator iSeries je komponenta iSeries Access za Windows. Če imate nameščeno starejšo različico Navigatorja iSeries, jo morate nadgraditi v V5R2.

OS/400 V5R2 podpira nadgradnje iz V4R5 in V5R1. Če prehajate na OS/400 V5R2, se podatki imenika LDAP in datoteke sheme imenika samodejno preselijo, tako da ustrezajo formatom V5R2. Če imate strežnik LDAP Imeniških storitev, ki se izvaja v izdaji OS/400 V4R3 ali V4R4, in želite preiti na V5R2, morate izvesti nekaj opravil za selitev.

Če prehajate na OS/400 V5R1 se morate zavedati naslednje problematike selitve:

- Pri nadgradnji v različico V5R2 Imeniške storitve samodejno preselijo shematske datoteke v V5R2 in zbrišejo stare shematske datoteke. Če ste datoteke shem zbrisali ali preimenovali, jih Imeniške storitve en morejo preseliti. V tem primeru se lahko prikaže sporočilo o napaki ali pa Imeniške storitve privzamejo, da so bile datoteke že preseljene.
- Imeniške sttoritve preselijo imeniške podatke v format V5R2 pri prvem zagonu strežnika ali uvozu datoteke LDIF. Za dokončanje preselitve načrtujte nekaj časa. Če prehajate na V5R2 iz V4R4 ali starejše izdaje, se zavedajte, da bodo imeniški podatki v V5R2 zahtevali približno dvakrat več pomnilniškega prostora kot v prejšnji različici. V Imeniških storitvah V4R4 ali starejših je bil podprt samo nabor znakov IA5, podatki pa shranjeni v obliki ccsid 37 (enobajtni format). Imeniške storitve podpirajo celoten nabor znakov ISO 10646.

  Ko nadgradite v različico V5R2, morate pred uvozom novih podatkov zagnati strežnik za preselitev obstoječih podatkov. Če poskušate uvoziti podatke pred enim zagonom strežnika in nimate zadostnih pooblastil, uvažanje ne bo uspelo.
- V4R4 in predhodne različice Imeniških storitev pri izdelavi postavk časovnega žiga niso upoštevale nastavitev časovnih pasov. Začenši z različico V4R5 se časovni pas uporablja v vseh dodatkih in popravkih imenika. Zato pri nadgradnji v različico V5R2 iz V4R4 ali starejše, Imeniške storitve prilagodijo obstoječa atributa createtimestamp in modifytimestamp tako, da odražata pravilni časovni pas. To storijo tako, da odštejejo časovni pas, ki je trenutno definiran v sistemu iSeries od časovnih pasov, ki so shranjeni v imeniku. Če trenutni časovni pas (time) ni isti časovni pas, ki je bil aktiven pri izvirnem izdelovanju ali spreminjanju, nove vrednosti časovnega pasu ne bodo odražale izvirnega časovnega pasu.
- Po izvedeni selitvi se bo imeniški strežnik LDAP samodejno zagnal ob zagonu TCP/IP. Če ne želite samodejnega zagona imeniškega strežnika, lahko to nastavitev spremenite s pomočjo Navigatorja operacij.

Selitev iz Imeniških storitev V4R3 ali V4R4 v V5R2

V5R2 OS/400 ne podpira neposredne nadgradnje iz V4R3. Če želite strežnik LDAP Imeniških storitev V4R3 ali V4R4 preseliti v V5R2, lahko izvedete enega od naslednjih postopkov:

- Tiha namestitev OS/400 iz V4R3 ali V4R4 v vmesno izdajo
- Shranjevanje knjižnice baze podatkov V4R3 ali V4R4 in nato namestitev OS/400 V5R2 od začetka

Tiha namestitev OS/400 iz V4R3 ali V4R4 v vmesno izdajo

Čeprav nadgradnji iz OS/400 V4R3 in V4R4 v V5R2 nista podprti, so podprte naslednje nadgradnje:

- Nadgradnja iz V4R3 in V4R4 v V4R5
- Nadgradnja iz V4R4 in V4R5 v V5R1
- Nadgradnja iz V4R5 in V5R1 v V5R2

Eden od načinov selitve strežnika Imeniških storitev je nadgradnja na vmesno izdajo (V4R5 ali V5R1), in nato v V5R2. Če želite podrobnejše informacije o postopkih namestitve OS/400, preglejte *Namestitev programske opreme*  . Sledite splošnemu postopku za izvedbo selitve:

1. Zapišite si vse spremembe, ki jih izvedete v datotekah sheme v imeniku /QIBM/UserData/OS400/DirSrv. Daatoteke sheme se preselijo samodejno.
2. Za V4R4 ali V4R3 izvedite tiho namestitev OS/400 V4R5 ali V5R1.
3. Izvedite vrinjeno namestitev v OS/400 V5R2.
4. Če še ni zagnan, zaženite strežnik imeniških storitev.
5. S pomočjo orodij za upravljanje imenika spremenite datoteke shem za poljubne uporabniške spremembe, ki ste si jih zapisali v koraku 1.
6. Ponovno zaženite strežnik imeniških storitev.

Shranjevanje knjižnice baze podatkov V4R3 ali V4R4 in nato namestitev OS/400 V5R2 od začetka

Drug način za selitev strežnika Imeniških storitev je ta, da shranite knjižnico baz podatkov, ki jo Imeniške storitve uporabljajo v V4R3 ali V4R4, in jo nato po namestitvi V5R2 iz nič znova obnovite. S tem si prihranite korak namestitve vmesne izdaje. Nastavitve strežnika se ne preselijo, zato morate nastavitve strežnika ponovno konfigurirati. Če želite podrobnejše informacije o postopkih namesstitve OS/400, preglejte

Namestitev programske opreme  . Sledite splošnemu postopku za izvedbo selitve:

1. Zapišite si vse spremembe, ki jih izvedete v datotekah sheme v imeniku /QIBM/UserData/OS400/DirSrv. Datoteke sheme se ne preselijo samodejno. Če želite ohraniti spremembe, jih boste morali znova izvesti ročno.
2. Zapišite si različne nastavitve konfiguracije v lastnosti strežnika Imeniških storitev, vključno z imenom knjižnice baz podatkov.
3. Shranite knjižnico baz podatkov, ki ste jo podali v konfiguraciji strežnika Imeniških storitev.
4. Zapišite si konfiguracijo za objavljanje.
5. Sistem OS/400 V5R2 namestite iz nič.
6. EZ-Setup uporabite za konfiguriranje strežnika imeniških storitev.
7. Obnovite knjižnico baz podatkov, ki ste jo shranili v koraku 3.
8. S pomočjo orodij za upravljanje imenika spremenite datoteke shem za poljubne uporabniške spremembe, ki ste si jih zapisali v koraku 1.
9. S pomočjo Navigatorja operacij znova konfigurirajte Imeniške storitve. Podajte knjižnico baz podatkov, ki ste jo shranili in obnovili.
10. S pomočjo Navigatorja operacij znova konfigurirajte objavljanje.
11. Ponovno zaženite strežnik imeniških storitev.

Vprašanja ob posodabljanju

Pri posodabljanju iz V4R3 v katerokoli kasnejšo različico morate upoštevati naslednje:

- **Preselitev datoteke obroča ključev v bazo podatkov ključev:**

  Client Access različice V3R2 je za vzpostavitev povezav SSL uporabljal datoteke obročev ključev (plast zaščitenih vtičnic) z imeniškim strežnikom LDAP. iSeries Access za Windows uporablja za vzpostavitev povezav SSL prostore za potrdila, ki jim lahko včasih rečemo baze podatkov s ključi. Če ste z imeniškim strežnikom LDAP uporabljali datoteko obročev ključev, morate datoteko obročev ključev pretvoriti v bazo podatkov s ključi, da boste lahko še naprej uporabljali SSL. Pri prvem poskusu vzpostavitve povezave SSL z imeniškim strežnikom LDAP, vas bo Navigator iSeries opozoril na to spremembo. Če izberete pretvorbo ključa, boste morali vnesti nekaj informacij za bazo podatkov s ključi, preden se bo izvedla pretvorba.

  Imeniški strežnik LDAP je v V4R3 uporabljal datoteko obročev ključev tudi za svoje lastne povezave SSL. Začenši z V4R4 uporablja prostor za sistemska potrdila. Če je bil strežnik v V4R3 nastavljen za uporabo datoteke obročev ključev, se bo vsebina datoteke obročev ključev preselila v prostor za sistemska potrdila.
- **Dve tokovni datoteki sta bili odstranjeni:**

  Naslednji tokovni datoteki, ki so jih v V4R3 uporabljale Imeniške storitve, nista več potrebni, in se samodejno odstranita pri namestitvi kasnejše različice:

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

  S temi datotekami vam ni treba storiti ničesar. To je omenjeno samo zato, da vas ne bo skrbelo, ker datotek ni več v sistemu.

Zavedajte se, da so lahko s posodabljanjem iz drugih različic v trenutno različico povezane dodatne zahteve.

Namestite in konfiguriranje Imeniških storitev

Imeniške storitve (LDAP) se samodejno namestijo ob namestitvi OS/400. Imeniški strežnik vključuje privzeto konfiguracijo, ki samodejno zažene imeniški strežnik ob zagonu TCP/IP. Imeniški strežnik zažene tudi objavljanje informacij o računalniku iz OS/400 v imeniški strežnik. Če želite prilagoditi nastavitve imeniškega strežnika LDAP, zaženite Čarovnika za konfiguriranje Imeniških storitev. Če želite uporabiti čarovnika, morate imeti posebna pooblastila *ALLOBJ in *IOSYSCFG.

Začenši v V5R1 so Imeniške storitve integriranje v osnovni operacijski sistem in možnost 32 ni več na voljo, začenši v V5R2.

Konfiguriranje imeniškega strežnika LDAP

Če vaš sistem prej ni bil konfiguriran za objavo informacij na drugem strežniku LDAP in v strežniku DNS TCP/IP ni prijavljenega nobenega strežnika LDAP, bodo Imeniške storitve samodejno nameščene z omejeno privzeto konfiguracijo. Imeniške storitve nudijo čarovnika, ki vam bo pomagal pri konfiguriranju imeniškega strežnika LDAP za vaše razmere. Ta čarovnik lahko izvedete kot del programa EZ-Setup, oziroma ga izvedete pozneje iz Navigatorja iSeries. Tega čarovnika uporabite, ko prvikrat konfigurirate imeniški strežnik. Uporabite ga lahko tudi pri vnovični konfiguraciji imeniškega strežnika.

Opomba: Če čarovnika uporabljate za vnovično konfiguriranje imeniškega strežnika, začenjate konfigurirati od začetka. Izvirno konfiguracijo raje zbrišite kot pa spreminjajte. Podatki imenika se ne zbrišejo, vendar ostanejo shranjeni v knjižnici, ki ste jo izbrali med nameščanjem (QUSRDIRDB po privzetku). Dnevnik sprememb bo prav tako ostal nedotaknjen in bo po privzetku shranjen v knjižnici QUSRDIRCL.

Če želite začeti popolnoma od začetka, zbrišite ti dve knjižnici, preden poženete čarovnika.

Če želite spremeniti konfiguracijo imeniškega strežnika, vendar je ne nameravate popolnoma počistiti, z desno tipko miške kliknite **Imenik** in izberite **Lastnosti**. S tem ne zbrišete izvirne konfiguracije.

Za konfiguriranje strežnika morate imeti posebna pooblastila *ALLOBJ in *IOSYSCFG. Če želite konfigurirati beleženje zaščite OS/400, morate imeti tudi posebno pooblastilo *AUDIT.

Če želite zagnati čarovnika za konfiguracijo Imeniške storitve, storite naslednje:

1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom miške kliknite **Imenik** in izberite **Konfiguriraj**.

Opomba: Če ste imeniški strežnik že konfigurirali, raje kliknite **Znova konfiguriraj** kot pa **Konfiguriraj**.

Sledite navodilom, ki jih daje čarovnik za konfiguriranje imeniškega strežnika LDAP.

Opomba: Morda boste knjižnico, ki hrani podatke imenike, raje postavili v uporabniški pomožni pomnilniški prostor (ASP) kot pa v sistemski ASP. Te knjižnice ni mogoče shraniti v neodvisnem ASP-u in katerikoli poskus konfiguriranja, vnovičnega konfiguriranja ali zagona strežnika s knjižnico, ki obstaja v neodvisnem ASP-u, ne bo uspel.

Ko čarovnik konča, ima vaš imeniški strežnik LDAP osnovno konfiguracijo. Če v vašem sistemu teče program Lotus Domino, bo funkcija LDAP programa Domino morda že uporabljala vrata 389 (privzeta vrata za strežnik LDAP). Narediti morate eno od naslednjega:

- Spremeniti vrata, ki jih uporablja Lotus Domino
- Spremeniti vrata, ki jih uporabljajo Imeniške storitve
- Uporabiti določen naslov IP

Zdaj lahko zaženete strežnik. Pred zagonom strežnika boste morda želeli izvesti naslednje:
- uvoziti podatke v strežnik
- omogočiti zaščito SSL (Secure Sockets Layer)
- omogočiti overjanje Kerberos
- nastaviti referenčne kazalce

Omogočanje SSL v imeniškem strežniku LDAP

Če ste v sistem namestili Upravljalnik digitalnih potrdil, lahko za zaščito dostopa do imeniškega strežnika LDAP uporabite zaščito SSL (plast zaščitenih vtičnic). Pred omogočitvijo SSL v imeniškem strežniku je koristno, da preberete pregled uporabe SSL z Imeniškimi storitvami.

Če želite med upravljanjem imeniškega strežnika iz Navigatorja iSeries uporabiti povezavo SSL, oziroma če želite uporabiti SSL z odjemalcem Windows LDAP, morate imeti v PC-ju nameščenega enega izmed izdelkov Client Encryptions (5722CE2 ali 5722CE3).

Če želite v vašem strežniku LDAP omogočiti SSL, uporabite vmesnik Upravljalnika digitalnih potrdil. Upravljalnik digitalnih potrdil lahko poženete iz mape **Internet** v Navigatorju iSeries ali na strani **Omrežje** v pogovornem oknu **Lastnosti** imeniškega strežnika.

Če želite vmesnik digitalnega potrdila pognati s strani **Omrežje**, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Omrežje**.
6. Kliknite **Upravljalnik digitalnih potrdil**.

   Upravljalnik digitalnih potrdil se bo pognal v vašem privzetem pregledovalniku.

Če se želite seznaniti s specifičnimi koraki, ki jih potrebujete za dodeljevanje digitalnega potrdila imeniškemu strežniku, preglejte Zaščita imeniškega strežnika LDAP.

Ko je SSL omogočen, lahko spremenite vrata, ki jih imeniški strežnik LDAP uporablja za zaščitene povezave.

Omogočanje overjanja Kerberos v imeniškem strežniku LDAP

Če ste v sistemu konfigurirali storitev za omrežno overjanje, lahko imeniški strežnik LDAP nastavite tako, da bo uporabljal overjanje Kerberos. Preden omogočite Kerberos v imeniškem strežniku, preberite pregled uporabe Kerberos v sistemu Imeniških storitev, ki vam bo morda v pomoč.

Če želite omogočiti overjanje Kerberos, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Kerberos**.
6. Označite možnost **Omogoči overjanje Kerberos**.
7. Na strani **Kerberos** podajte še druge nastavitve, ki ustrezajo vašim razmeram. Če želite informacije o posameznih poljih, preglejte zaslonsko pomoč.

Privzeta konfiguracija za Imeniške storitve

Imeniški strežnik LDAP se samodejno namesti ob namestitvi OS/400. Ta namestitev vključuje privzeto konfiguracijo. Imeniški strežnik uporablja privzeto konfiguracijo, če veljajo vse naslednje navedbe:
- Skrbniki niso zagnali čarovnika za konfiguriranje Imeniških storitev ali spremenili nastavitev imenika na strani z lastnostmi.
- Objavljanje Imeniških storitev ni konfigurirano.

| • Imeniški strežnik LDAP ne more poiskati nobenih informacij DNS LDAP.

| Če imeniški strežnik LDAP uporablja privzeto konfiguracijo, pride do naslednjega:
| • Imeniški strežnik LDAP se samodejno zažene ob zagonu TCP/IP.
| • Sistem izdela privzetega skrbnika, cn=Administrator. Generira tudi geslo, ki se uporabi interno. Če morate
| geslo skrbnika uporabiti kasneje, lahko nastavite novega na strani lastnosti Imeniških storitev.
| • Izdela se privzeta pripona, ki temelji na imenu ID sistema. Na osnovi imena sistema se izdela tudi pripona
| sistemskih objektov. Če je ime IP sistema na primer ″mary.acme.com″, je pripona
| dc=mary,dc=acme,dc=com.
| • Imeniški strežnik LDAP uporablja privzeto podatkovno knjižnico QUSRDIRDB. Sistem jo izdela v
| sistemskem ASP.
| • Za nezaščitene komunikacije uporablja strežnik vrata 389. Če je bilo digitalno potrdilo konfigurirano za
| LDAP, je plast zaščitenih vtičnic omogočena, za zaščitene komunikacije pa se uporabijo vrata 636.

Nato obstajajo naslednje privzete vrednosti za objavljanje Imeniških storitev:
- Sistem objavlja informacije v lokalni imeniški strežnik LDAP
- Objavljanje ne uporabljajo SSL
- Objavljanje uporablja prostore pod privzeto pripono
- Za overjanje z imeniškim strežnikom uporablja OS/400 ID cn=Administrator in sistemsko generirano geslo.
- Sistem objavlja le sistemske informacije.

Orodje za uporavljanje imenikov IBM SecureWay

Orodje za upravljanje imenikov (DMT) IBM SecureWay nudi grafični uporabniški vmesnik za upravljanje vsebine imenika LDAP. Opravila, ki jih lahko izvajate z DMT, so naslednja:
- Pregledovanje sheme imenika
- Dodajanje, urejanje in brisanje razredov objektov
- Dodajanje, urejanje in brisanje atributov
- Pregledovanje in iskanje drevesa imenikov
- Dodajanje, urejanje, prikazovanje in brisanje postavk
- Urejanje RDN-jev postavk
- Upravljanje ACL-ov

DMT je del odjemalca LDAP Windows, ki je vključen v Imeniških storitvah. Odjemalec je dobavljen v imeniku integriranega datotečnega sistema.

Če želite v PC namestiti odjemalca LDAP Windows, vključno z DMT, storite naslednje:
1. V Navigatorju iSeries AS/400 razširite možnost **Datotečni sistemi**.
2. Razširite **Souporaba datotek**.
3. Dvokliknite **Qdirsrv**.
4. Dvokliknite **UserTools**.
5. Dvokliknite **Windows**.
6. Če želite namestiti DMT, dvokliknite **setup.exe**. Za zaključek namestitve sledite zaslonskim navodilom.

Dokumentacija Orodja za upravljanje imenikov (DMT) IBM SecureWay je v datoteki dparent.htm. Pri namestitvi odjemalca v PC se ta datoteka prekopira v mapo orodja IBM SecureWay.

Poglavje 4. Upravljanje imeniškega strežnika LDAP

Če želite upravljati imeniški strežnik LDAP, morate imeti enega od naslednjih naborov pooblastil:

- Za konfiguriranej strežnika ali spreminjanje konfiguracije strežnika: posebno pooblastilo za vse objekte (*ALLOBJ) in V/I konfiguracijo sistema (*IOSYSCFG)
- Za zagon ali zaustavitev strežnika: Pooblastilo za nadzor opravil (*JOBCTL) in pooblastilo objekta za ukaze za zaključevanje TCP/IP (ENDTCP), zagon TCP/IP (STRTCP), zagon strežnika TCP/IP (STRTCPSVR) in zaključevanje strežnika TCP/IP (ENDTCPSVR).
- Za nastavitev vedenja beleženja za imeniški strežnik: Posebno pooblastilo za beleženje (*AUDIT)
- Za prikaz dnevnika opravil strežnika: Posebno pooblastilo za nadzorovanje vmesnih datotek (*SPLCTL)

Če želite upravljati objekte imenika (vključno s seznami za nadzor dostopa, lastništvom objektov in kopijami), se povežite v imenik kot skrbnik DN ali kot drugi DN, ki ima ustrezna pooblastila LDAP. Če uporabljate integracijo pooblastil, je lahko skrbnik tudi projicirani uporabnik, ki ima pooblastilo za ID funkcije skrbnika imeniških storitev.

Upravljanje imeniškega strežnika zajema naslednje naloge:

Zagon imeniškega strežnika LDAP

Če želite zagnati imeniški strežnik LDAP, storite naslednje:

1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom miške kliknite **Imenik** in izberite **Zaženi**.

   Zagon imeniškega strežnika lahko traja nekaj časa in je odvisen od hitrosti strežnika in količine razpoložljivega pomnilnika. Prvi zagon imeniškega strežnika bo morda trajal nekoliko dlje, ker mora strežnik izdelati nove datoteke. Podobno bo pri prvem zagonu imeniškega strežnika po nadgradnji iz predhodne različice Imeniške storitve zagon trajal nekaj minut dlje kot običajno, ker mora strežnik preseliti datoteke. Periodično lahko preverite status strežnika in tako vidite, ali se je strežnik že zagnal.

Opomba: Imeniški strežnik lahko zaženete tudi iz seje 5250 tako, da vnesete ukaz STRTCPSVR *DIRSRV.

Če ste imeniški strežnik konfigurirali tako, da se zažene ob zagonu TCP/IP, ga lahko zaženete tudi z vnosom ukaza STRTCP.

Zaustavitev imeniškega strežnika

Zaustavitev imeniškega strežnika vpliva na vse aplikacije, ki uporabljajo strežnik v času zaustavitve. To zajema aplikacije preslikave identitete podjetja (EIM), ki trenutno uporabljajo imeniški strežnik za operacije EIM. Vse aplikacije prekinejo povezavo z imeniškim strežnikov, vendar jim ni preprečen ponoven poskus povezave s strežnikom.

Če želite imeniški strežnik LDAP zaustaviti, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom miške kliknite **Imenik** in izberite **Zaustavi**.

   Zaustavitev imeniškega strežnika lahko traja nekaj časa in je odvisna od hitrosti sistema, količine aktivnosti strežnika in količine razpoložljivega pomnilnika. Periodično lahko preverite status strežnika in tako vidite, ali se je že zaustavil.

Opomba: Imeniški strežnik lahko zaustavite iz seje 5250 tako, da vnesete ukaze ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL ali ENDTCP. ENDTCPSVR *ALL in ENDTCP vplivata tudi na vse druge strežnike TCP/IP, ki se izvajajo v sistemu. ENDTCP bo zaustavil tudi TCP/IP.

Preverjanje statusa imeniškega strežnika

Navigator iSeries prikazuje status imeniškega strežnika v desnem podoknu v stolpcu **Status**.

Če želite preveriti status imeniškega strežnika, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**. Navigator iSeries prikaže status vseh strežnikov TCP/IP, vključno z imeniškim strežnikom, v stolpcu **Status**. Če želite ažurirati status strežnikov, kliknite meni **Prikaz** in izberite **Osveži**.
4. Če želite pregledati podrobnejše informacije o statusu imeniškega strežnika, z desnim gumbom miške kliknite **Imenik** in izberite **Status**. Prikazale se bodo informacije o številu aktivnih povezav ter vse ostale informacije, kot so pretekle in trenutne ravni delovanja.

   Poleg dodatnih informacij, si s tem načinom prikaza statusa lahko prihranite čas. Status imeniškega strežnika lahko osvežite, ne da bi porabili dodaten čas, ki je zahtevan za preverjanje statusa drugih strežnikov TCP/IP.

Preverjanje opravil v imeniškem strežniku LDAP

Občasno boste morda želeli nadzorovati posamezna opravila v imeniškem strežniku LDAP. Če želite preveriti opravila strežnika, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom miške kliknite **Imenik** in izberite **Opravila strežnika**.

Omogočanje obveščanja o dogodkih

Imeniške storitve podpirajo prijavo dogodkov, kar odjemalcem omogoča, da se prijavijo v strežnik LDAP in bodo tako obveščeni v primeru, če pride do določenega dogodka kot je dodajanje vnosov v imenik.

Če želite v strežniku omogočiti obveščanje o dogodkih, storite naslednje:
1. V Navigator iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.

5. Kliknite **Dogodki**.
6. Izberite **Odjemalcem omogoči prijavo za obveščanje o dogodkih**.

Prav tako lahko za posamezno povezavo podate največje število dovoljenih prijav in skupno največje število prijav, ki jih bo dovolil strežnik.

Če želite dodatne informacije o prijavi dogodkov, preglejte Dodatek C: Prijava dogodkov v priročniku IBM SecureWay Directory Version 3.2: Client SDK Programming Reference .

Določitev nastavitev za transakcije

Imeniške storitve podpirajo transakcije, ki omogočajo, da je skupina operacij imenika LDAP obravnavana kot ena enota. Če želite več informacij, poglejte “Transakcije” na strani 35.

Če želite konfigurirati nastavitve transakcij za vaš strežnik, storite naslednje:
1. V Navigator iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite **Transakcije**.
6. Podajte nastavitve za transakcije.

Opomba: Nastavitve transakcij lahko vplivajo na zmogljivost strežnika LDAP, zato boste morda želeli preskusiti različne nastavitve.

Spreminjanje vrat ali naslova IP

Imeniški strežnik LDAP, ki ga omogočajo Imeniške storitve, uporablja naslednja privzeta vrata:
- 389 za nezaščitene povezave.
- 636 za zaščitene povezave (če ste uporabili Upravljalnik digitalnih potrdil za omogočanje Imeniških storitev AS/400 kot aplikacije, ki lahko uporabi zaščitena vrata).

Opomba: Po privzetku so vsi naslovi IP, definirani na lokalnem sistemu, povezani s strežnikom.

Če že uporabljate ta vrata za drugo aplikacijo, lahko Imeniškim storitvam dodelite drug naslov IP, ali pa uporabite druga naslova IP za dva strežnika, če aplikacije podpirajo povezovanje s specifičnim naslovom IP.

Zgled navzkrižja strežnika LDAP Domino s strežnikom LDAP imeniških storitev iSeries je na voljo v temi Host Domino LDAP in imeniške storitve na istem iSeries

Če želite spremeniti vrata, ki jih uporablja imeniški strežnik LDAP, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Omrežje**.
6. Vnesite ustrezne številke vrat in nato kliknite **Potrdi**.

Če želite spremeniti naslov IP, na katerem imeniški strežnik sprejema povezave, naredite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Omrežje**.

6. Kliknite gumb **Naslovi IP...**.
7. Izbreite **Uporabi izbrane naslove IP** in izberite naslove IP za strežnik, ki ga želite uporabiti pri sprejemanju povezav.

Prenos podatkov imenika LDAP med sistemi

Strežnik LDAP Imeniških storitev AS/400 se lahko izvaja neodvisno od drugih strežnikov. Verjetno se vam bo zdelo koristno, da deluje tudi z drugimi strežniki. To lahko vključuje:
- "Uvažanje datoteke LDIF"
- "Izvažanje datoteke LDIF"
- "Nastavitev nove kopije imeniškega strežnika"
- "Objavljanje informacij v imeniški strežnik" na strani 24

Uvažanje datoteke LDIF

Informacije med različnimi imeniškimi strežniki LDAP lahko prenesete s pomočjo datotek LDIF (format za izmenjavo podatkov) LDAP. Preden začnete s tem postopkom, prenesite datoteko LDIF v vaš strežnik iSeries kot tokovno datoteko.

Za uvoz datoteke LDIF v imeniški strežnik LDAP storite naslednje:
1. Če je imeniški strežnik zagnan, ga zaustavite. Če želite informacije o zaustavitvi imeniškega strežnika, preglejte "Zaustavitev imeniškega strežnika" na strani 18.
2. V Navigator iSeries razširite **Omrežje**.
3. Razširite **Strežniki**.
4. Kliknite **TCP/IP**.
5. Z desnim gumbom miške kliknite **Imenik** in izberite **Orodja** in nato **Uvozi datoteko**.

Opomba: Za uvoz datotek LDIF lahko uporabite pomožni program ldapadd.

Izvažanje datoteke LDIF

Informacije med različnimi imeniškimi strežniki LDAP lahko prenesete s pomočjo datotek LDIF (format za izmenjavo podatkov) LDAP. Preglejte "Format za izmenjavo podatkov LDAP" na strani 32. V datoteko LDIF lahko izvozite celoten ali samo del imenika LDAP.

Za izvoz datoteke LDIF v imeniški strežnik storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom miške kliknite **Imenik** in izberite **Orodja** in nato **Izvozi datoteko**.

   Opomba: Če ne podate mesta, v katerega želite izvoziti datoteko LDIF, bo shranjena v privzeti imenik, ki je podan v profilu uporabnika OS/400. Če privzetega imenika niste spremenili, je le-ta kar korenski imenik.

Opombe:
1. Za datoteko LDIF nastavite pooblastila in s tem preprečite nepooblaščen dostop do podatkov imenika. V ta namen z desnim gumbom miške kliknite datoteko v Navigatorju iSeries in nato izberite **Pooblastila**.
2. S pomočjo pomožnega programa LDIF lahko izdelate popolno ali delno datoteko LDIF. Preglejte "Pomožni program ldapsearch" na strani 50. Uporabite možnost -L in preusmerite izhodne podatke v datoteko.

Nastavitev nove kopije imeniškega strežnika

Kopije imeniškega strežnika LDAP lahko nastavite za imeniške strežnike v drugih strežnikih iSeries.Imeniške storitve uporabljajo za kopiranje standardni protokol LDAP različice 3.

Opombe:

1. Med strežnikoma LDAP različice 3 in LDAP različice 2 ne morete kopirati. Zato mora sistem, v katerega kopirate, uporabljati isto različico LDAP kot sistem, iz katerega kopirate. V4R3 in V4R4 programa OS/400 podpirata LDAP različice 2. V4R5 in novejše izdaje podpirajo LDAP različice 3
2. Imenik Imeniških storitev lahko prekopirate v strežnike IBM SecureWay V3.2 ali novejše na drugih platformah. Zato mora biti imeniški strežnik OS/400 konfiguriran za uporabo mehanizma 3.2 ACI. Če v strežniku pride do težave pri kopiranju, bo ta zaustavil kopiranje. V tem primeru kopija ne bo popolna.

Če želite nastaviti novo kopijo imeniškega strežnika, sledite naslednjemu postopku:

1. Če tega še niste storili, konfigurirajte glavni strežnik in strežnik za kopije.

   Opomba: Zagotovite, da se shemi in pripone ujemata v obeh strežnikih.
2. Zaustavite glavni strežnik.
3. (izbirno) Nastavite podatke LDAP za začetno kopiranje. Ta korak lahko preskočite, če nimate nobenih začetnih podatkov, ki jih želite prenesti iz glavnega strežnika v strežnik za kopije.
4. (izbirno) Podatke LDAP prenesite v glavni strežnik. Ta korak preskočite, če za vaš strežnik za kopije velja eno od naslednjega:
   - Je nov imeniški strežnik LDAP.
   - Ne vsebuje podatkov, ki bi jih še naprej želeli vzdrževati.
5. Nastavite nov strežnika za kopije.
6. Nastavite glavni strežnik za novo kopijo.
7. Zagotovite, da lahko glavni strežnik izvaja ažuriranja:
   a. V Navigatorju iSeries razširite ikono sistema, v katerem teče glavni imeniški strežnik.
   b. Razširite **Omrežje**.
   c. Razširite **Strežniki**.
   d. Kliknite **TCP/IP**.
   e. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
   f. Če še ni označena, označite možnost **Dopusti ažuriranja imenikov**.

Opomba: V teh navodilih je predpostavljeno, da so glavni strežnik in strežniki za kopije v sistemih, ki jih upravljate iz Navigatorja operacij v istem PC-ju. Če sisteme upravljate iz različnih PC-jev, se lahko premaknete iz enega PC-ja na drugega in nato opravite to nalogo. Če glavni strežnik ali strežnik za kopije tečeta v IBM-ovem operacijskem sistemu, ki ni OS/400, preglejte dokumentacijo te platforme o tem, kako nastaviti strežnik.

Nastavitev podatkov LDAP za začetno kopiranje

Morda imate v imeniškem strežniku LDAP že podatke, ki jih želite dodati v nov strežnik za kopije. V ta namen morate imenik najprej izvoziti v datoteko LDIF. Medtem ko se datoteka LDIF izvaža, morate preprečiti ažuriranje glavnega strežnika. To lahko storite na enega od naslednjih načinov:

- Zaustavite strežnik imenikov LDAP. Glede na količino podatkov v imeniku, lahko ta zahteva daljšo zaustavitev strežnika.
- Lastnosti strežnika spremenite tako, da ažuriranje ne bo mogoče. To mogoči strežniku, da nadaljuje z odgovarjanjem na poizvedbe med izvažanjem datoteke LDIF. Če želite izbrati to možnost, naredite naslednje:
  1. V Navigatorju iSeries razširite ikono sistema, v katerem teče glavni imeniški strežnik.
  2. Razširite **Omrežje**.
  3. Razširite **Strežniki**.
  4. Kliknite **TCP/IP**.
  5. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
  6. Če je možnost **Dopusti ažuriranje imenika** označena, zbrišite oznako. S tem boste preprečili ažuriranje imenika, dokler kopiranje ni v celoti nastavljeno.
  7. Kliknite **Potrdi**.
  8. Zaustavite in nato ponovno zaženite imeniški strežnik LDAP.

Po zaustavitvi strežnika ali spremembi lastnosti strežnika, s katerimi onemogočite ažuriranja strežnika, storite naslednje:

1. Imenik izvozite v datoteko LDIF.
2. Prenesite datoteko LDIF v sistem, v katerem bo tekel strežnik za kopije.

Po prenosu datoteke LDIF v sistem, kjer bo tekel strežnik za kopije, morate vanj uvoziti podatke:
1. V Navigatorju iSeries razširite ikono sistema, v katerem teče imeniški strežnik za kopije.
2. Če strežnik za kopije še ni zaustavljen, ga zaustavite zdaj. Status strežnika osvežujte tako dolgo, dokler ni **Zaustavljen**.
3. Razširite **Omrežje**.
4. Razširite **Strežniki**.
5. Kliknite **TCP/IP**.
6. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
7. Če možnost **Dopusti ažuriranje imenika** ni označena, jo označite. S tem boste dopustili uvoz podatkov.
8. Kliknite **Potrdi**.
9. Uvozite datoteko LDIF , ki ste jo prenesli v koraku 2.
10. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
11. Odstranite oznako **Dopusti ažuriranje imenika**.

Prenos podatkov LDAP v glavni strežnik

Ko imeniški strežnik LDAP postavite v vlogo strežnika za kopije, v njem ne morete več ažurirati podatkov. Če imate še podatke v strežniku, ki ga konfigurirate kot imeniški strežnik LDAP za kopije, jih boste morda želeli premakniti v glavni strežnik, da jih boste še naprej lahko vzdrževali. V ta namen naredite naslednje:
1. V Navigatorju iSeries razširite ikono sistema, v katerem teče imeniški strežnik za kopije.
2. Razširite **Omrežje**.
3. Razširite **Strežniki**.
4. Kliknite **TCP/IP**.
5. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
6. Če je možnost **Dopusti ažuriranje imenika** označena, zbrišite oznako. S tem boste preprečili ažuriranje imenika, dokler kopiranje ni v celoti nastavljeno.
7. Kliknite **Potrdi**.
8. Zaustavite imeniški strežnik LDAP.
9. Imenik izvozite v datoteko LDIF.
10. Prenesite datoteko LDIF v sistem, v katerem bo tekel glavni strežnik.

Po prenosu datoteke LDIF v sistem, kjer bo tekel glavni strežnik, morate vanj uvoziti podatke:
1. V Navigatorju iSeries razširite ikono sistema, v katerem teče glavni imeniški strežnik.
2. Če glavni imeniški strežnik še ni zaustavljen, ga zaustavite zdaj. Status strežnika osvežujte tako dolgo, dokler ni **Zaustavljen**.
3. Razširite **Omrežje**.
4. Razširite **Strežniki**.
5. Kliknite **TCP/IP**.
6. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
7. Če možnost **Dopusti ažuriranje imenika** ni označena, jo označite. S tem boste dopustili uvoz podatkov.
8. Kliknite **Potrdi**.
9. Uvozite datoteko LDIF , ki ste jo prenesli v koraku 10 prejšnjega postopka.
10. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
11. Odstranite oznako **Dopusti ažuriranje imenika**.

Nastavitev nove kopije

Sledite postopku za nastavitev novega strežnika za kopije.

Opomba: Pred izvedbo tega postopka morate strežnik za kopije konfigurirati in zaustaviti.
1. V Navigatorju iSeries razširite ikono sistema, v katerem teče imeniški strežnik za kopije.
2. Razširite **Omrežje**.
3. Razširite **Strežniki**.

4. Kliknite **TCP**/**IP**.
5. Če strežnik še ni zaustavljen, ga zaustavite zdaj. Status strežnika osvežujte tako dolgo, dokler ni **Zaustavljen**.
6. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
7. Kliknite jeziček **Replikacija**.
8. Izberite **Uporabi kot strežnik za kopije**.
9. V polju **Ime, ki ga glavni strežnik uporabi za ažuriranja** izberite ime, ki ga bo glavni strežnik uporabil, ko se prijavi v kopijo strežnika in izvede ažuriranja. To ime je lahko razločevalno ime (DN) ali uporabnik Kerberos.

   Če izberete DN:

   - Kliknite gumb **Geslo** poleg polja **Ime, ki ga glavni strežnik uporablja za ažuriranja**. Vnesite geslo za glavni strežnik, ki ga želite uporabiti za prijavo na strežnik za kopije, ko se izvaja ažuriranje.

     Opomba: Geslo in ime, ki ste ga podali v koraku 9, si zapišite in shranite na varno mesto. Potrebovali ju boste pri nastavitvi glavnega strežnika za kopiranje.

   Če izberete **Dodaj uporabnika Kerberos**:

   - Prikazal se bo poziv za vnos imena Kerberos (v obliki LDAP/*gostiteljsko_ime*, kjer je *gostiteljsko_ime* celotno ime glavnega strežnika) in privzetega področja (kot je ACME.COM) glavnega strežnika.

     Opomba: Če želite uporabiti Kerberos, morate v glavnem strežniku in kopiji strežnika omogočiti protokol Kerberos.
10. V polje **URL glavnega strežnika** vnesite ime glavnega strežnika v obliki URL. Če glavni strežnik ne uporablja privzetih vrat, vnesite številko vrat kot del URL.
11. Kliknite jeziček **Baza podatkov**/**Pripone**. Če pripone, ki jo želite kopirati, ni na seznamu, jo dodajte.
12. (izbirno) Če želite pri kopiranju uporabiti plast zaščitenih vtičnic (SSL), uporabite Upravljalnik digitalnih potrdil za omogočanje SSL na tem strežniku. Upravljalnik digitalnih potrdil lahko poženete na jezičku **Omrežje**. Če želite podrobnejše informacije o omogočanju SSL v imeniškem strežniku, preglejte razdelek “Omogočanje SSL v imeniškem strežniku LDAP” na strani 15.
13. Kliknite **Potrdi**.

Nastavitev glavnega strežnika za novo kopijo

Sledite postopku za nastavitev glavnega strežnika za novo kopijo.

Opomba: Glavni strežnik morate pred izvedbo tega postopka konfigurirati in zagnati.

1. V Navigatorju iSeries razširite ikono sistema, v katerem teče glavni imeniški strežnik.
2. Razširite **Omrežje**.
3. Razširite **Strežniki**.
4. Kliknite **TCP**/**IP**.
5. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
6. Če še ni označena, označite možnost **Dopusti ažuriranja imenikov**.
7. Kliknite **Potrdi**.
8. Imeniški strežnik LDAP zaustavite in ga nato znova poženite . Status strežnika osvežujte tako dolgo, dokler ni **Zagnan**.
9. Z desnim gumbom znova kliknite **Imenik** in izberite **Lastnosti**.
10. Kliknite jeziček **Replikacija**. Navigator iSeries bo morda zahteval vnos informacij o povezavi. Vnesite te informacije in nato kliknite **Potrdi**.
11. Kliknite **Dodaj.**
12. V polje **Strežnik** vnesite ime strežnika za kopije v obliki URL.
13. Izberite metodo overjanja.

    Če želite uporabiti razločevalno ime (DN) in geslo, storite naslednje:

    a. Izberite možnost **Uporabi DN in geslo**.

    b. V polje **Poveži kot** vnesite ime, ki ste ga podali v koraku 9, v katerem ste nastavili strežnik za kopije.

c. Kliknite **Geslo** in podajte geslo, ki ste ga podali v koraku 9 na strani 23, v katerem ste nastavili strežnik za kopije.

Če želite uporabiti protokol Kerberos, storite naslednje:

- Izberite možnost **Uporabi šifro Kerberos glavnega strežnika**. Glavni strežnik bo za overjanje uporabil svoje osnovno ime Kerberos.

  Opomba: Če želite uporabiti Kerberos, morate v glavnem strežniku in kopiji strežnika omogočiti protokol Kerberos.

14. Če želite pri kopiranju uporabiti plast zaščitenih vtičnic (SSL), uporabite Upravljalnik digitalnih potrdil za omogočanje SSL na tem strežniku. Upravljalnik digitalnih potrdil lahko poženete na jezičku **Omrežje**. Če želite podrobnejše informacije o omogočanju SSL v imeniškem strežniku, preglejte razdelek “Omogočanje SSL v imeniškem strežniku LDAP” na strani 15.
15. Če vaš strežnik za kopije ne uporablja privzetih vrat, podajte številko vrat v polje **Vrata**.
16. Če strežnika za kopije ne želite ažurirati po vsaki spremembi postavke v glavnem strežniku, izberite **Čas**. Nato podajte, kako pogosto naj glavni strežnik ažurira kopijo.
17. Kliknite **Potrdi**.
18. Kliknite jeziček **Baza podatkov**/**Pripone**. Če pripone, ki jo želite kopirati, ni na seznamu, jo dodajte.
19. Omogočite ažuriranje imenikov na vseh strežnikih za kopije:
    a. V Navigatorju iSeries razširite ikono sistema, v katerem teče imeniški strežnik za kopije.
    b. Razširite **Omrežje**.
    c. Razširite **Strežniki**.
    d. Kliknite **TCP/IP**.
    e. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
    f. Če možnost **Dopusti ažuriranje imenika** ni označena, jo označite.
    g. Kliknite **Potrdi**.
20. Če posamezni strežnik za kopije še ni zagnan, ga zaženite zdaj.

Opomba: Strežnik ne more biti glavni strežnik in strežnik za kopije.

Objavljanje informacij v imeniški strežnik

Sistem lahko konfigurirate za objavljanje določenih informacij v imeniškem strežniku LDAP na istem ali drugem sistemu. OS/400 samodejno objavlja te informacije na imeniški strežnik LDAP, če uporabljate Navigator iSeries za spreminjanje teh informacij v OS/400. Informacije, ki jih lahko objavite, zajemajo informacije o sistemu (sistemi in tiskalniki), souporabi tiskalnikov, informacije o uporabnikih ter Kakovost TCP/IP načel storitev. Če želite informacije o kakovosti storitev, preglejte Konfiguracija LDAP in QoS .

Če ne obstaja nadrejeni DN, v katerega so bili podatki objavljeni, ga bodo Imeniške storitve samodejno izdelale. Namestite lahko tudi druge aplikacije OS/400, ki objavljajo informacije v imeniku LDAP. Dodatno lahko iz svojih programov pokličete vmesnike uporabniškega programa (API-je) za objavo drugih tipov informacij v imeniku LDAP.

Opombe:

1. Če OS/400 konfigurirate za objavljanje tipa informacij Uporabniki v imeniški strežnik LDAP, samodejno izvozi postavke iz porazdeljevalnega imenika sistema v imenik LDAP. V ta namen uporabi vmesnik uporabniškega programa (API) QGLDSSDD. S tem ostaja imenik LDAP usklajen s spremembami, ki ste jih naredili v sistemskem razdeljevalnem imeniku. Če želite podrobnejše informacije o API-ju QGLDSSDD, preglejte temo Imeniške storitve OS/400 v Programiranje v Informacijskem centru iSeries. Razpoložljive informacije vključujejo naslednje:
   - Kako ročno poklicati ta API.
   - Kako preprečiti izvoz posameznih uporabnikov v strežnik LDAP.
   - Kako izvoziti polja sistemskega razdeljevalnega imenika.
2. Če OS/400 konfigurirate za objavljanje tipa informacij Sistem v imeniški strežnik LDAP in izberete eno ali več tiskalnikov za objavljanje, bo sistem samodejno ohranjal imenik LDAP usklajen s spremembami, ki so bile izvedene v teh tiskalnikih v sistemu. Informacije o tiskalnikih, ki jih lahko objavite, so: nahajališče

tiskalnika, hitrost in strani na minuto, možnost podpore dvosmerne povezave in barve, tip in model ter opis. Te informacije se pridobijo iz opisa naprave v sistemu, ki ga objavljate. V omrežnem okolju lahko uporabniki uporabijo te informacije kot pomoč pri izbiri tiskalnika.

3. Informacije OS/400 lahko objavite v imeniškem strežniku LDAP, ki ni OS/400, če ta strežnik konfigurirate tako, da uporablja shemo IBM.

Če želite sistem konfigurirati za objavljanje informacij OS/400 v imeniški strežnik LDAP, naredite naslednje:

1. V Navigatorju iSeries z desno tipko miške kliknite sistem in izberite **Lastnosti**.
2. Kliknite jeziček **Storitve imenika**.
3. Kliknite tipe informacij, ki jih želite objaviti.

   Nasvet:
   Če nameravate objavljati več tipov informacij na istem mestu, lahko prihranite čas tako, da za istočasno konfiguracijo izberete več tipov informacij. Navigator iSeries bo pri konfiguriranju naslednjih tipov informacij uporabil vrednosti, ki jih kot privzete vrednosti vnesete pri konfiguriranju prvega tipa informacij.
4. Kliknite **Podrobnosti**.
5. Kliknite potrditveno polje **Objavi sistemske informacije**.
6. Podajte **Metodo overjanja**, ki naj jo uporabi strežnik, kot tudi ustrezne informacije za overjanje.
7. Kliknite gumb **Uredi** poleg polja **(Aktivni) imeniški strežnik**. V prikazanem pogovornem oknu vnesite ime imeniškega strežnika, kjer želite objavljati informacije OS/400, nato pa kliknite **Potrdi**.
8. V polje **Pod RN** vnesite nadrejeno razločevalno ime (RN), kjer želite informacije dodati imeniškemu strežniku.
9. V okvirju **Povezava strežnika** izpolnite polja, ki ustrezajo vaši konfiguraciji.

   Opomba: Če želite objaviti informacije OS/400 na imeniškem strežniku z uporabo SSL ali Kerberos, morate imeniški strežnik najprej konfigurirati za uporabo ustreznega protokola. Preglejte “Uporaba overjanja Kerberos v imeniškem strežniku LDAP” na strani 37, kjer boste našli podrobnejše informacije o SSL in Kerberos.
10. Če imeniški strežnik ne uporablja privzetih vrat, vnesite pravilno številko vrat v polje **Vrata**.
11. Kliknite **Preveri**, s čimer zagotovite, da nadrejeno RN obstaja v sistemu in da so informacije o povezavi pravilne. Če pot imenika ne obstaja, se bo prikazalo pogovorno okno, ki vas bo pozvalo k izdelavi imenika.

    Opomba: Če razločevalno ime nadrejenega ne obstaja in ga ne izdelate, objava ne bo uspešna.
12. Kliknite **Potrdi**.

Opomba: Informacije OS/400 lahko objavite tudi na imeniškem strežniku LDAP z drugo platformo. Uporabniške in sistemske informacije morate objaviti v imeniškem strežniku, ki uporablja shemo, ki je združljiva s shemo Imeniške storitve. Definicije sheme imenikov IBM SecureWay, ki zajemajo Imeniške stritve iSeries lahko najdete na spletni strani imeniških storitev.

Souporabo tiskalnikov morate objaviti v imeniškem strežniku, ki podpira shemo Microsoftovega aktivnega imenika. Objavljanje souporabe tiskalnikov omogoča uporabnikom, da konfigurirajo tiskalnike iSeries neposredno na njihovem namizju Windows 2000 s pomočjo čarovnika za dodajanje tiskalnika Windows 2000. Če želite to narediti v čarovniku za dodajanje tiskalnika, podajte, da želite tiskalnik najti v aktivnem imeniku Windows 2000.

API-ji za objavljanje informacij OS/400 v imeniškem strežniku

Imeniške storitve nudijo vgrajeno podporo za objavljanje uporabniških in sistemskih informacij. Te postavke so navedene na strani **Imeniške storitve** v pogovornem oknu **Lastnosti** sistema.Konfiguracijo strežnika LDAP in API-je za objavljanje lahko uporabite za omogočanje programov OS/400, ki ste jih napisali za objavljanje drugih tipov informacij. Te informacije se nato pojavijo tudi na strani **Imeniške storitve**. Enako kot uporabniki in sistemi so na začetku onemogočene in jih lahko konfigurirate s pomočjo istega postopka. Program, ki doda podatke v imenik LDAP, se imenuje posrednik za objavljanje. Tip informacije, ki jo objavljate, kot se pojavlja na strani **Imeniške storitve**, se imenuje ime posrednika.

Vključevanje objavljanja v vaše programe bodo omogočili naslednji API-ji:

QgldChgDirSvrA
Aplikacija uporablja format CSVR0500 za začetno dodajanje imena posrednika, ki je označen kot onemogočena postavka. Navodila za uporabnike aplikacije bi jih morale spoznati z uporabo Navigatorja iSeries za premik na stran lastnosti Imeniških storitev za konfiguriranje posrednika za objavljanje. Zgledi imen posrednikov so imena posrednikov sistemov in uporabnikov, ki so samodejno na voljo na strani **Imeniške storitve**.

QgldLstDirSvrA
Če želite pregledati, kateri posredniki so trenutno na voljo v vašem sistemu, uporabite naslednji format API-ja LSVR0500.

QgldPubDirObj
Ta API uporabite za dejansko objavljanje informacij.

Če želite podrobnejše informacije o teh API-jih, preglejte temo LDAP (Lightweight Directory Access Protocol) v poglavju Programiranje v Informacijskem centru iSeries.

Podajanje strežnika za referenčne kazalce imenika

Če želite za imeniški strežnik dodeliti strežnike referenčnih kazalcev, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom miške kliknite **Imenik** in nato izberite **Lastnosti**.
5. Kliknite **Dodaj**.
6. V pozivu podajte ime strežnika referenčnih kazalcev v obliki URL. Sprejemljivi URL-ji LDAP:
   - ldap://test.server.com
   - ldap://test.server.com:400
   - ldap://9.9.99.255

   Opomba: Če strežnik referenčnih kazalcev ne uporablja privzetih vrat, podajte pravilno število vrat kot del URL-ja, kot so vrata 400 na primer podana v drugem zgornjem zgledu.
7. Kliknite **Potrdi**.

Dodajanje pripon v imeniški strežnik LDAP

Dodajanje pripon v imeniški strežnik LDAP omogoča strežniku, da upravlja ta del drevesa imenikov.

Opomba: Pripone, ki je na strežniku že pod drugo pripono, ne morete dodati. Če so na primer o=ibm, c=us priponi na strežniku, ne morete dodati ou=rochester, o=ibm, c=us.

Če želite dodati pripono v imeniški strežnik, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Baza podatkov**/**Pripone**.
6. V polje **Nova pripona** vpišite ime nove pripone.
7. Kliknite **Dodaj**.
8. Kliknite **Potrdi**.

Opomba: Če dodate pripono, bo ta strežnik usmerila na razdelek imenika, vendar pa ne bo izdelala objektov. Če objekt, ki ustreza novi priponi, predhodno ne obstaja, ga morate izdelati tako, kot ostale objekte.

Odstranjevanje pripon iz imeniškega strežnika

Če želite odstraniti pripono iz imeniškega strežnika LDAP, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Baza podatkov/Pripone**.
6. Kliknite pripono, ki jo želite odstraniti.
7. Kliknite **Odstrani**.

Opomba: Lahko se odločite za brisanje pripone, ne da bi zbrisali objekte imenika pod njo. S tem onemogočite dostop do podatkov iz imeniškega strežnika. Kasneje lahko ponoven dostop do podatkov pridobite tako, da pripono znova dodate.

Shranjevanje in obnavljanje informacij Imeniške storitve

Imeniške storitve shrani informacije na naslednja nahajališča:

- Knjižnica baz podatkov (privzeto QUSRDIRDB), ki vsebuje vsebino imeniških strežnikov.
- Knjižnica QDIRSRV2, namenjena za shranjevanje informacij za objavo.
- Knjižnica QUSRSYS, kjer so shranjene različne postavke v objektih, ki se začnejo s QGLD (če jih želite shraniti, podajte QUSRSYS/QGLD*).
- Če konfigurirate imeniški strežnik za beleženje sprememb imenika, uporablja ta knjižnico baze podatkov z imenom QUSRDIRCL.

Če se vsebina imenika redno spreminja, morate tudi knjižnico baze podatkov in objekte v njej redno shranjevati. Konfiguracijski podatki so shranjeni v naslednjem imeniku:

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

Tudi datoteke morate vedno shraniti v ta imenik, če spremenite konfiguracijo ali uveljavite PTF-je.

Če želite informacije o shranjevanju in obnavljanju podatkov OS/400, preglejte priročnik Izdelava varnostnih kopij in obnavljanje, SC41-5304 .

Upravljanje lastništva in dostopa do podatkov imenika

Upravljanje lastništva in dostopa do podatkov imenika vključuje naslednje naloge:
- “Delo z lastnostmi lastništva objektov imenika”
- “Delo s seznami za nadzor dostopa (ACL-i)” na strani 28
- “Delo s skupinami ACL” na strani 28

Delo z lastnostmi lastništva objektov imenika

Če želite nastaviti lastnosti lastništva objektov imenika, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom miške kliknite **Imenik** in izberite **Pooblastila**.

   Če ste že povezani z imeniškim strežnikom, se prikaže pogovorno okno **Povezava z imeniškim strežnikom**. Povežite se kot skrbnik strežnika ali kot lastnik objekta z lastnostmi lastništva, s katerimi želite delati.
5. Z drevesa imenikov izberite objekt z lastnostmi lastništva, s katerimi želite delati in nato kliknite **Potrdi**.

Delo s seznami za nadzor dostopa (ACL-i)

Delo s seznami za nadzor dostopa (ACL-I) vključuje dodeljevanje eksplicitnih in implicitnih ACL-ov objektom imenika, dodajanje uporabnikov v ACL-e, odstranjevanje uporabnikov iz ACL-ov in pregledovanje objektov imenika. Pomnite, da začenši z V5R1 Imeniške storitve podpirajo nov model ACL-jev, zato se morate z njim spoznati, čeprav ste ACL-je uporabljali že prej.

Če želite delati z ACL-i, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom miške kliknite **Imenik** in izberite **Pooblastila**.

   Če ste že povezani z imeniški strežnikom, se prikaže pogovorno okno **Povezava z imeniškim strežnikom**. Povežite se kot skrbnik strežnika ali kot lastnik objekta z ACL-om, s katerim želite delati.
5. Z drevesa imenikov izberite objekt z ACL-om, s katerim želite delati in nato kliknite **Potrdi**.
6. Kliknite jeziček **ACL**.

Delo s skupinami ACL

Če želite delati s skupinami ACL , storite naslednje:
1. V Navigatorju iSeries izberite **Omrežje**.
2. Izberite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom miške kliknite **Imenik** in izberite **Skupine ACL**.

Delo z administrativnim dostopom za pooblaščene uporabnike

| Začenši v V5R2 lahko dodelite skrbniški dostop profilom uporabnikov, ki jim je bil dan dostop do
| identifikatorja (ID-ja) funkcije skrbnika imeniških storitev (QIBM_DIRSRV_ADMIN).

| Če je na primer profilu uporabnika JOHNSMITH dodeljen dostop do ID-ja funkcije skrbnika imeniških storitev
| in je v pogovornem oknu Lastnosti imenika izbrana možnost Dodeli skrbniški dostop do pooblaščenih
| uporabnikov, ima profil JOHNSMITH nato pooblastilo skrbnika LDAP. Če se ta profil uporablja za
| povezovanje imeniškega strežnika z uporabo naslednjega DN, os400-
| profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com, ima uporabnik pooblastilo skrbnika.
| Pripona objekotv istema je v tem primeru os400-sys=systemA.acme.com. Če želite več informacij o
| projiciranih uporabnikih, preglejte “Ozadje, določeno z operacijskim sistemom” na strani 38.

| Če želite izbrati to možnost, naredite naslednje:
| 1. V Navigator iSeries razširite **Omrežje**.
| 2. Razširite **Strežniki**.
| 3. Z desno tipko miške kliknite **Imenik** in izberite **Lastnosti**.
| 4. Na jezičku **Splošno** pod **Informacije o skrbniku** izberite možnost **Dodeli skrbniški dostop pooblaščenim uporabnikom**.

| Če želite nastaviti ID funkcije pooblastila skrbnika imeniških storitev v profilu uporabnika, naredite naslednje:
| 1. V Navigatorju iSeries z desno tipko kliknite ime sistema in izberite **Upravljanje aplikacije**.
| 2. Kliknite jeziček **Gostiteljske aplikacije**.
| 3. Razširite možnost **Operating System/400**.
| 4. Kliknite **Skrbnik imeniških storitev**, da označite možnost.
| 5. Kliknite gumb **Prilagodi**.
| 6. Razširite **Uporabniki**, **Skupine** ali **Uporabniki niso v skupini**, kar je ustrezno za želenega uporabnika.
| 7. Izberite uporabnika ali skupino, ki ju želite dodati na seznam **Dostop dovoljen**.

8. Kliknite gumb **Dodaj**.
9. Kliknite **Potrdi,** da shranite spremembe.
10. Kliknite **Potrdi** v pogovornem oknu **Upravljanje aplikacije**.

Sledenje dostopom in spremembam v imeniku LDAP

Morda boste želeli slediti dostopom in spremembam v imeniku LDAP. Dnevnik sprememb imenika LDAP lahko uporabite za sledenje sprememb v imeniku. Dnevnik sprememb je na voljo pod posebno pripono cn=changelog. Shranjen je v knjižnici QUSRDIRCL.

Če želite omogočiti dnevnik sprememb, naredite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Baza podatkov/Pripone**.
6. Izberite **Beleži spremembe imenika**.
7. (izbirno) V polju **Največje število postavk** podajte največje število postavk, ki jih želite hraniti v dnevniku sprememb.

   Opomba: Čeprav je ta parameter izbiren, močno priporočamo, da podate največje število postavk. Če največjega števila postavk ne podate, bo dnevnik sprememb hranil vse postavke in lahko postane zelo velik.

Razred objekta changeLogEntry se uporablja za predstavitev sprememb, ki se uveljavijo na imeniškem strežniku. Niz sprememb je podan z zaporedjem vseh postavk v prostoru dnevnika sprememb, ki je označeno s število spremembe changeNumber. Informacije dnevnika sprememb so samo za branje.

Vsi uporabniki, ki so na Seznamu za nadzor dostopa za pripono cn=changelog, lahko iščejo postavke v dnevniku sprememb. Iskanja lahko izvajate samo za pripono dnevnika sprememb, cn=changelog. V priponi dnevnika sprememb ne poskušajte dodajati, spreminjati ali brisati, čeprav imate za to pooblastilo. To lahko pripelje do nepredvidljivih rezultatov.

Zgled:

Naslednji zgled uporablja ukaz pomožni program ukazne vrstice ldapsearch za pridobivanje vseh postavk dnevnika sprememb, ki so zabeležene na strežniku

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

Omogočanje beleženja objektov za imeniški strežnik

Imeniške storitve podpirajo beleženje zaščite OS/400. Če za sistemsko vrednost QAUDCTL podate *OBJAUD, lahko beleženje objektov omogočite prek Navigatorja operacij.

Če želite omogočiti beleženje objektov za Imeniške storitve, storite naslednje:
1. V Navigator iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Beleženje**.
6. Izberite nastavitev beleženja, ki jo želite uporabiti za strežnik.

Spremembe nastavitev beleženje bodo uveljavljene takoj, ko kliknete **Potrdi**. Imeniškega strežnika LDAP ni potrebno vnovič zaganjati. Če želite več informacij, poglejte “Zaščita Imeniške storitve” na strani 36.

Nastavljanje zmogljivosti imeniškega strežnika LDAP

Zmogljivost imeniškega strežnika LDAP lahko prilagodite tako, da spremenite nekaj od naslednjega:
- Velikost iskanj.
- Največji dovoljeni čas za iskanja.
- Nastavitve transakcij strežnika
- Število povezav baze podatkov in niti strežnika

Če želite prilagoditi vrednosti zmogljivosti imeniškega strežnika, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Zmogljivost**.

Nastavite lahko tudi zmogljivost imeniškega strežnika, tako da spremenite število povezav baze podatkov in niti strežnika, ki jih uporablja strežnik. Če želite spremeniti to vrednosti, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Baza podatkov**/**Pripone**.

Poglavje 5. Pojmi in referenčne informacije o Imeniških storitvah AS/400

Pri spoznavanju in izvajanju strežnika LDAP Imeniških storitev AS/400 vam bodo v pomoč naslednje pojmovne in referenčne informacije:

Za informacije o osnovah LDAP in načrtovanju strežnika LDAP preglejte tudi Poglavje 3, "Prvi koraki v Imeniških storitvah" na strani 7.

Seznami za nadzor dostopa LDAP (ACL)

V veliko primerih boste želeli omejiti dostop do podatkov v imeniškem strežniku LDAP. Strežnik LDAP v vašem podjetju lahko na primer vsebuje telefonski imenik zaposlenih v vašem podjetju. Verjetno boste želeli, da lahko vsi zaposleni vidijo podatke v tem imeniku.

Direktorica podjetja ne želi, da bi vsi zaposleni dostopali do njene telefonske številke. V tem primeru bi lahko izdelali **seznam za nadzor dostopa (ACL)**. S tem ACL-om lahko omejite dostop do postavke strežnika na tiste zaposlene, od katerih želi direktorica sprejemati klice.

Z uporabo seznamov za nadzor dostopa lahko nadzorujete, kdo ima pooblastilo za dodajanje in brisanje objektov imenika. Podate lahko, ali imajo uporabniki pravico za branje, pisanje, iskanje in primerjavo lastnosti imenika. ACL-i so lahko eksplicitni ali podedovani. ACL-je lahko uporabite na enega od naslednjih načinov:

- Eksplicitno nastavite ACL za podani objekt.
- Podate, da objekti podedujejo ACL-e od objektov, ki so višje v hierarhiji imenikov LDAP.

Morda direktorica v prejšnjem zgledu ni želela, da bi lahko vsi zaposleni dostopali do njene telefonske številke. Ona pa želi, da bi lahko do njene telefonske številke dostopali vsi menedžerji. V tem primeru si lahko pomagate s **skupino ACL** , ki poenostavi dodeljevanje pooblastil menedžerjem. Skupine ACL omogočajo, da raje dodeljujete dostop do specifičnih skupin uporabnikov, kot pa pooblastila na individualni osnovi. To je lahko posebno koristno, če potrebuje ista skupina ljudi dostop do več nizov objektov. Če na primer isti menedžerji, ki so imeli dostop do direktoričine telefonske številke, potrebujejo kasneje dostop do zapisov o plačah, bi lahko znova uporabili skupino ACL.

Modeli ACL

Vse različice Imeniške storitve podpirajo model z dovoljenji na ravni razreda dostopa. V tem modelu so tipi lastnosti LDAP razvrščeni na Normalne, Občutljive ali Kritične. Te razvrstitve krmilijo datoteke sheme lastnosti. Če v ACL objekta dodate uporabnika, podate, katere razvrstitve lahko uporabnik bere, piše, išče in primerja. V večini shem, bi bila telefonska številka razvrščena kot običajna lastnost. Zato bi lahko menedžerjem v zgornjem primeru za dostop do telefonske številke direktorice podali dostop za branje v običajnih lastnostih objekta imenika direktorice. Še vedno ne bi mogli dostopati do občutljivih in kritičnih informacij. Vse različice Imeniške storitve podpirajo nastavitev dovoljenj na ravni razreda dostopa.

Imeniške storitve podpira tudi model dovoljen ravni lastnosti. V tem modelu lahko za posamezne lastnosti podate pooblastila za branje, pisanje, iskanje in primerjanje, ne glede na njihov razred dostopa. Znova preučite zgornji zgled. V modelu dovoljenj na ravni lastnosti lahko menedžerjem za lastnost telephoneNumber dodelite dostop z branjem, kljub temu da na splošno nimajo dostopa do lastnosti Normalno.

Model dovoljenja na ravni lastnosti je združljiv samo s strežniki SecureWay Imeniških storitev različice 3.2 in novejšimi. Po privzetku ni omogočen. Pri delu z ACL-ji ga lahko omogočite. Ko to storite, lahko model onemogočite samo tako, da strežnik znova konfigurirate in obnovite bazo podatkov imenika. Preden se odločite, da boste omogočili ta model, si zapomnite, da ga ne boste mogli upravljati iz nobenega odjemalca LDAP V2 (vključno z različicami Navigator iSeries pred V5R1) in da boste s tem lahko pokvarili vnose ACL.

Posebne vrednosti ACL

Na začetku imajo vsi objekti v imeniškem strežniku Imeniških storitev AS/400 seznam za nadzor dostopa, ki vsebuje posebno skupino ACL, CN=Anybody, ki vključuje vse uporabnike imenika. Po privzetku ima ta skupina za vse objekte dostop z branjem, iskanjem in primerjanjem do lastnosti normalnega razreda.

Morda boste želeli, da imajo nekateri objekti iste dostopne pravice za vse uporabnike, ki se povezujejo z imeniškim strežnikom prek povezave, ki ni anonimna (anonymous). V ta namen uporabite skupino ACL (access control list) cn=Authenticated.

Če želite podati, katera dovoljenja za dostop ima objekt zase, raje uporabite posebni DN cn=this. Ta omogoča podrejenim postavkam, ki podedujejo njihove ACL-je, da so samodejno overjeni za izvajanje operacij na njihovih objektih.

Dodatne informacije

Če želite ACL-e upravljati s pomočjo Navigatorja operacij, vam ni treba poznati podrobnosti o tem, kako Imeniške storitve izvedejo ACL-je. Vendar, če želite med uporabo datotek LDIF podati lastnosti, povezane z ACL, oziroma uporabiti ACL-je v pomožnih programih ukazne vrstice LDAP, se boste morali seznaniti z lastnostmi, ki jih uporabljajo ACL-ji. Če želite informacije o lastnostih ACL, preglejte referenčni dokument seznama za nadzor dostopa  v IBM-ovi dokumentaciji SecureWay Orodja za upravljanje imenikov  .

Za podrobnejše informacije o nastavitvi in spreminjanju ACL-ov in skupin ACL preglejte vsebino naslednjih povezav:

“Delo s seznami za nadzor dostopa (ACL-i)” na strani 28
“Delo s skupinami ACL” na strani 28

Format za izmenjavo podatkov LDAP

Izmenjevalni format podatkov LDAP (LDIF) omogoča preprost način za prenos informacij o imeniku med imeniškimi strežniki LDAP. Datoteke LDIF hranijo postavke imenika LDAP v preprostem besedilnem formatu. Začenši z različico V4R5 Imeniških storitev AS/400 se je format datotek LDIF, ki ga uporablja imeniški strežnik, nekoliko spremenil. Datoteke LDIF sestavlja zaporedje vrstic, ki opisujejo postavko imenika ali niz sprememb za postavko imenika. Obeh hkrati ne moreta opisovati.

Splošni format postavke LDIF je naslednji:

```
version: 1
dn: razločevalno ime
attrtype1: vrednost atributa1
...
```

kjer je:

- *version* različica formata datoteke LDIF. Številka različice mora biti 1. Če številka različice manjka, se za datoteko LDIF upošteva stari format datoteke LDIF. Če je datoteka LDIF različice 1, MORA biti vsebina kodirana v obliki UTF-8.
- *razločevalno ime* razločevalno ime postavke imenika
- *attrtype1* tip lastnosti LDAP (kot je cn ali ou)
- *attrvalue1* vrednost lastnosti

Vsaka postavka ima lahko več lastnosti. Vsaka lastnost se pojavlja v svoji vrstici. Če je vrednost lastnosti daljša od ene vrstice, se lahko nadaljuje v naslednji vrstici tako, da je na začetku presledek ali tabulatorski znak.

Prazne vrstice ločujejo več postavk v isti datoteki LDIF. Vsaka vrstica, ki se začne z znakom lestvice (#), je komentar, in mora biti zanemarjena pri razčlenjevanju datoteke LDIF.

Vsako razločevalno ime ali vrednost atributa, ki ustreza enemu od naslednjih pogojev, mora biti zakodirana v obliki base-64:
- Vsebuje znake za pomik na začetek vrstice ali pomik v novo vrstico.
- Začne se z dvopičjem (:), presledkom ali znakom za manjše od (<).
- Konča se s presledkom.

Atributi, kodirani v Base-64, so določeni s pomočjo dveh dvopičij med imenom atributa in vrednostjo.

Zunanje reference so v formatu URL file://. Med tipom atributa in vrednostjo zunanje reference mora biti dvopičje in znak za manjše kot (:<).

Sledi nekaj zgledov datotek LDIF:

Zgled 1: Preprosta datoteka LDAP z dvema postavkama

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

   dn: cn=Bjorn Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Bjorn Jensen
   sn: Jensen
   telephonenumber: +1 408 555 1212
   description:Bab je ljubiteljica jadranja in pogosto potuje
   v kraje ob morju, kjer so dobri pogoji za jadranje.
   title:Product Manager, Rod and Reel Division
```

Zgled 2: Datoteka, ki vsebuje vrednost v obliki base-64-encoded

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

```
   uid: gernj
   telephonenumber: +1 408 555 1212
   description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvdSBhcmUhICBU
    aGlzIHZhbHVlIGlzIGJhc2UtNjQtZW5jb2RlZCBiZWNhdXNlIGl0IGhhcy
    BhIGNvbnRyb2wgY2hhcmFjdGVyIGluIGl0IChhIENSKS4NICBCeSB0aGUg
   d2F5LCB5b3Ugc2hvdWxkIHJlYWxseSBnZXQgb3V0IG1vcmUu
```

Zgled 3: Datoteka vsebuje niz zapisov s spremembami in komentarji

Opomba: Datotek LDIF, z zapisi o spremembah, ni mogoče uvoziti neposredno v strežnik. Podpirajo jih pomožni program lupine LDAP.

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

   # Zbriši obstoječo postavko
   dn: cn=Robert Jensen, ou=Rochester, o=Big Company, c=US
   changetype: delete

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

Vrstni red postavk v datoteki LDIF je pomemben. Za uspešno dodajanje postavke, ki je podana v datoteki LDIF, v imenik LDAP, mora v imenskem prostoru imenika najprej obstajati njena nadrejena postavka. V zgodnjem zgledu druge in tretje postavke ne bi bilo mogoče dodati, če prve postavke ne bi bilo.

Podobno, če želite datoteko LDIF uvoziti v imenik, ki podpira določene pripone, mora datoteka LDIF vsebovati postavke za te pripone. Če je strežnik imel pripone ou=Rochester, o=Big Company, c=US, bi zgoraj navedeno datoteko LDIF lahko uvozili. Če je imel strežnik namesto tega pripono o=Big Company, c=US, bi morali podati postavko za to pripono najprej v datoteki LDIF. Zgled:

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

Format in vsebina datotek LDIF sta določena s shemo strežnika, iz katerega se izvažata. Datoteko LDIF lahko uvozite v strežnik LDAP, ki uporablja enako shemo kot strežnik, v katerem ste datoteko izvozili. Strežniki LDAP različnih proizvajalcev uporabljajo različne sheme (z različnimi razredi objektov in lastnostmi). Zato morda v nek strežnik ne boste mogli uvoziti datoteke LDIF, ki jo je izdelal drug strežnik.

Specifikacije datoteke LDIF Request for Comments (RFC) je na voljo na naslednjem spletnem naslovu:

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

S tem povezani postopki:

“Uvažanje datoteke LDIF” na strani 20
“Izvažanje datoteke LDIF” na strani 20

Problematika podpore za državne jezike (NLS)

Začenši z V4R5 strežnik LDAP OS/400 in odjemalec LDAP OS/400 temeljita na različici LDAP3. Upoštevajte naslednjo problematiko NLS:

- Podatki med strežniki in odjemalci LDAP se prenesejo v obliki UTF-8. Dovoljeni so vsi znaki ISO 10646.
- Strežnik imeniških storitev LDAP uporablja za shranjevanje v bazi podatkov metodo preslikave UTF-16.
- Strežnik in odjemalec izvajata primerjave nizov, ki niso občutljive na velikost znakov. Algoritmi za velike črke ne bodo pravilni za vse jezike (državne nastavitve).

Če želite podrobnejše informacije o UCS-2, preglejte temo Globalizacija v tematiki Načrtovanje v Informacijskem centru.

Lastništvo objektov imenika LDAP

Vsak objekt v imeniku LDAP ima najmanj enega lastnika. Lastniki objekta lahko objekt zbrišejo. Lastniki in skrbnik strežnika so edini uporabniki, ki lahko za objekt spreminjajo lastnosti lastništva in lastnosti seznama za nadzor dostopa. Lastništvo objektov se lahko podeduje ali pa je eksplicitno. To pomeni, da lahko za dodeljevanje lastništva naredite eno od naslednjega:

- Eksplicitno nastavite lastništvo za podani objekt.
- Podate, da objekti podedujejo lastnike iz objektov, ki so višje v hierarhiji imenikov LDAP.

Imeniške storitve omogočajo, da podate več lastnikov za isti objekt. Podate lahko tudi, da je objekt lastnik samega sebe. V tem primeru vključite posebno razločevalno ime cn=this na seznamu lastnikov objekta. Predpostavimo, da ima objekt cn=A lastnika cn=this. Do objekta cn=A bo imel lastniški dostop poljubni uporabnik, če je povezan s strežnikom kot cn=A.

S tem povezana procedura:

"Delo z lastnostmi lastništva objektov imenika" na strani 27

Referenčni kazalci imenika LDAP

Referenčni kazalci omogočajo imeniškim strežnikom LDAP, da delujejo v skupinah. Če razločevalno ime (DN), ki ga zahteva odjemalec, ni v enem imeniku, lahko strežnik samodejno pošlje (napoti) zahtevo na katerikoli drug strežnik LDAP.

Imeniške storitve dopuščajo uporabo dveh tipov referenčnih kazalcev. Podate lahko privzete strežnike referenčnih kazalcev, na katere bo strežnik LDAP napotil odjemalce, če DN ni v imeniku. Odjemalca LDAP lahko uporabite tudi za dodajanje postavk v imeniški strežnik, ki ima referenčni kazalec (razred objektov) objectClass. S tem lahko podate referenčne kazalce, ki temeljijo na zahtevah odjemalcev za specifične DN.

Opomba: V Imeniških storitvah AS/400 morajo objekti referenčnih kazalcev vsebovati samo razločevalno ime (dn), razred objekta (objectClass) in lastnost referenčnega kazalca (ref). Preglejte razdelek "Pomožni program ldapsearch" na strani 50, kjer bosta našli zgled, ki ponazarja to omejitev.

Strežniki referenčnih kazalcev so tesno povezani s strežniki za kopije. Ker podatkov v strežniku za kopije ne morejo spreminjati odjemalci, strežniki za kopije vse zahteve za spreminjanje podatkov imenika napotijo v glavni strežnik.

Transakcije

Imeniški strežnik LDAP sistema lahko konfigurirate tako, da bo odjemalcem omogočal uporabo transakcij. Transakcija je skupina operacij imenika LDAP, obravnavanih kot ena enota. Nobena izmed posameznih operacij LDAP, ki sestavljajo transakcijo, ne bo dokončna, dokler se uspešno ne zaključijo vse operacije v transakciji in je le-ta odobrena. Če katera izmed operacij ne uspe ali pa je transakcija prekinjena, bodo druge operacije razveljavljene. S pomočjo te zmožnosti lahko uporabniki ohranijo razvrstitev operacij LDAP. Na primer, uporabnik želi v svojem odjemalcu nastaviti transakcijo, ki bo zbrisala nekaj vnosov v imenik. Če se

povezava med odjemalcem in strežnikom med transakcijo prekine, vnosi ne bodo zbrisani. Zato lahko uporabnik transakcijo preprosto še enkrat zažene in mu ni treba preverjati, kateri vnosi so bili uspešno zbrisani.

Del transakcije so lahko naslednje operacije LDAP:

- dodajanje
- spreminjanje
- spreminjanje RDN
- brisanje

Opomba: V transakcije ne vključujte sprememb sheme imenika (pripona cn=schema). Kljub temu, da jih je mogoče vključiti, zanje v primeru, če transakcija ne uspe, ne bo izdelana varnostna kopija. Zaradi tega lahko pride v imeniškem strežniku do nepredvidljivih težav.

Če želite dodatne informacije o transakcijah, preglejte dodatek Omejena podpora za transakcije v priročniku IBM SecureWay Directory Client SDK Programming Reference.

Imeniški strežnik LDAP za kopije

Informacije, ki so shranjene v imeniškem strežniku LDAP za kopije so identične informacijam v glavnem imeniškem strežniku LDAP. Če imate eno ali več kopij imenika LDAP, lahko izkoristite dve osnovni prednosti:

- Kopije pospešijo iskanje po imeniku. Namesto da vsi odjemalci iščejo neposredno po enem glavnem strežniku, lahko zahteve razdelite med glavni strežnik in strežnike za kopije.
- Kopije nudijo varnostne kopije glavnega strežnika. Če glavni strežnik ni na voljo, lahko kopija še vedno izpolnjuje zahteve za iskanje in nudi dostop do podatkov imenika.

Strežniki za kopije omogočajo samo branje. Če pooblaščeni uporabnik poskuša spremeniti postavko v strežniku za kopije, ta napoti zahtevo glavnemu imeniškemu strežniku.

S tem povezana procedura:

“Nastavitev nove kopije imeniškega strežnika” na strani 20

Zaščita Imeniške storitve

Beleženje zaščite

V različici V5R1 sistem Imeniške storitve sedaj podpira tudi beleženje zaščite OS/400. Beležene postavke so lahko naslednje:

- povezave in prekinitve povezav z imeniškim strežnikom
- spremembe dovoljenj za objekte imenika LDAP
- spremembe lastništva za objekte imenika LDAP
- izdelava, brisanje, iskanje in spreminjanje objektov imenika LDAP
- spremembe gesla skrbnika in ažuriranje razločevalnih imen (DN-jev)
- spremembe gesel uporabnikov
- uvozi in izvozi datotek

Pred začetkom delovanja beleženja vnosov v imenik boste morda morali spremeniti določene nastavitve v beleženju OS/400. Če ste za sistemsko vrednost QAUDCTL podali *OBJAUD, lahko beleženje objektov omogočite prek Navigatorja operacij. Za dodatne informacije o beleženju preglejte *Zaščita - Referenčni opis* ali temo Sledenje zaščite v Informacijskem centru.

Overjanje povezav in zaščita

Imeniške storitve nudi naslednje mehanizme, s pomočjo katerih lahko izboljšate zaščito komunikacij med odjemalci LDAP in imeniškim strežnikom LDAP:

- povezave SSL (plast zaščitenih vtičnic)
- overjanje Kerberos
- šifriranje gesel CRAM-MD5

Uporaba zaščite plasti zaščitnih vtičnic (SSL) in zaščite prevajalne plasti z imeniškim strežnikom LDAP

Za vzpostavitev varnejših komunikacij z imeniškim strežnikom LDAP lahko Imeniške storitve uporabljajo zaščito SSL (plast zaščitenih vtičnic).

Če želite v Imeniških storitvah AS/400 uporabiti SSL, morate biti v sistemu nameščen eden od izdelkov ponudnika šifriranega dostopa (5722-ACx). Če želite SSL uporabiti iz Navigatorja operacij, mora biti v vašem PC-ju nameščen eden od izdelkov za šifriranje odjemalca (5722-CEx). To programsko opremo potrebujete, če želite storiti karkoli od naslednjega:

- Konfigurirati in upravljati Imeniške storitve iz delovne postaje z uporabo povezave SSL. To vključuje opravila, ki jih izvajate v Navigatorju iSeries.
- Uporabiti povezavo SSL z aplikacijami, ki jo izdelate z vmesniki uporabniških programov odjemalcev Windows.

SSL je standard v internetni zaščiti. Uporabite ga lahko za komuniciranje z odjemalci LDAP, kot tudi s strežniki LDAP za kopije. Poleg overjanja strežnika lahko uporabite overjanje uporabnika, s čimer omogočite dodatno zaščito vaših povezav SSL. Overjanje odjemalca zahteva, da odjemalec LDAP predstavi digitalno potrdilo, ki potrjuje istovetnost odjemalca strežniku, preden se z njim vzpostavi povezava.

Če želite uporabiti SSL morate v svoj sistem namestiti Upravljalnik digitalnih potrdil (DCM), možnost 34 v OS/400. DCM nudi vmesnik, s katerim lahko izdelate in upravljate digitalna potrdila in prostore za potrdila. Če želite informacije o digitalnih potrdilih ter o uporabi DCM, preglejte dokumentacijo za Upravljalnik digitalnih potrdil. Če želite informacije o SSL v iSeries, preglejte Zaščita aplikacij s SSL. Če želite informacije o TLS v strežniku iSeries, preglejte Podprti protokoli SSL in zaščita prenosne plasti (TLS).

Uporaba overjanja Kerberos v imeniškem strežniku LDAP

Imeniške storitve omogočajo, da imeniški strežnik LDAP nastavite tako, da bo uporabljal overjanje Kerberos. Kerberos je omrežni protokol za overjanje, ki z uporabo tajnopisja tajnega ključa za odjemalsko strežniške aplikacije nudi močno overjanje.

Če želite omogočiti overjanje Kerberos, morate imeti v sistemu nameščenega enega izmed izdelkov Cryptographic Service Provider (5722AC2 ali 5722AC3). Prav tako pa mora biti konfigurirana storitev za omrežno overjanje.

Podpora Kerberos sistema Imeniške storitve nudi podporo za mehanizem SSL GSSAPI. S tem lahko odjemalca SecureWay in Windows 2000 LDAP v imeniškem strežniku LDAP uporabljata overjanje Kerberos.

Osnovno ime Kerberos, ki ga uporablja strežnik, ima naslednjo obliko:

```
ime-storitve/ime-gostitelja@področje
```

ime-storitve je LDAP, ime-gostitelja je celotno ime TCP/IP sistema, področje pa je privzeto področje, podano v konfiguraciji Kerberos tega sistema.

Na primer, če se sistem imenuje moj-as400 v domeni TCP/IP acme.com, kjer je privzeto področje Kerberos ACME.COM, bo osnovno ime Kerberos v strežniku LDAP LDAP/moj-as400.acme.com@ACME.COM.

Privzeto področje Kerberos je podano v konfiguracijski datoteki Kerberos (po privzetku /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) s smernico default_realm (default_realm = ACME.COM). Za imena področij Kerberos so po dogovoru uporabljene velike črke, za gostiteljska imena pa male. LDAP/ morate podati z velikimi črkami. Če ne konfigurirate privzetega področja, imeniškega strežnika ni mogoče konfigurirati za overjanje Kerberos.

Pri overjanju Kerberos bo imeniški strežnik LDAP povezal razločevalno ime (DN) s povezavo, ki določa dostop do podatkov imenika. DN strežnika lahko povežete z eno izmed naslednjih metod:

- Strežnik lahko izdela DN na osnovi ID-ja Kerberos. Če izberete to možnost, bo identiteta Kerberos oblike principal@področje izdelala DN oblike ibm-kn=principal@področje. ibm-kn= je enakovredno ibm-kerberosName.
- Strežnik lahko v imeniku poišče razločevalno ime (DN), ki vsebuje vnos za osnovno ime in področje Kerberos. Če izberete to možnost, bo strežnik v imeniku poiskal vnos, ki določa to identiteto Kerberos, na naslednji način:
  - Strežnik poišče v imeniku objekt krbRealm-V2, ki vsebuje lastnost krbRealmName-V2, povezano s področjem Kerberos. Če najde tak vnos, bo poiskal DN-je, podane za lastnost princSubtree postavke z lastnostjo krbPrincipalName, ki se ujema z osnovnim imenom in imenom področja. Če DN, konfiguriran v krbAliasedObjectName, vsebuje DN postavke, ki je bila predhodno najdena,potem se uporabi DN, konfiguriran v krbAliasedObjectName. V nasprotnem primeru se uporabi DN postavke. Ta metoda je običajno uporabljena v primeru, če KDC Kerberos informacije o osnovnem imenu Kerberos shrani v imenik LDAP.
  - Če zgoraj opisano iskanje ne uspe, bo strežnik poiskal vnos imenika, ki uporablja pomožni razred ibm-securityIdentities in vsebuje lastnost altSecurityIdentities z vrednostjo KERBEROS:principal@področje. Z uporabo te metode lahko v primeru, če KDC osnovna imena ne shrani v imenik, identitete Kerberos povežete z vnosi imenika.

Imeti morate datoteko s tabelo ključev (keytab), ki vsebuje ključ za osnovno ime storitve LDAP. Preglejte temo Informacijskega centra Storitve overjanja omrežja pod Zaščita, če želite podrobnejše informacije o Kerberosu na strežniku iSeries. Razdelek Konfiguriranje storitve za omrežno overjanje vsebuje informacije o dodajanju informacij v datoteke s tabelami ključev.

Ozadje, določeno z operacijskim sistemom

Sistemsko določeno ozadje lahko preslika objekte OS/400 kot postavke v drevesu imenikov, ki je dostopen LDAP. Projicirani objekti so predstavitve LDAP objektov OS/400 namesto dejanskih postavk, shranjenih v bazi podatkov strežnika LDAP. V V5R2 so profili uporabnikov OS/400 edini objekti, ki se preslikajo ali projicirajo kot postavke v drevesu imenikov. Preslikava objektov profila uporabnikov se nanaša na uporabniško projicirana ozadja OS/400.

Operacije LDAP se preslikajo na podrejene objekte OS/400 in operacije LDAP izvedejo funkcije operacijskega sistema, da lahko dostopajo do teh objektov. Vse operacije LDAP, ki se izvedejo na profilih uporabnikov, se izvedejo pod pooblastilom profila uporabnika, povezanega s povezavo odjemalca.

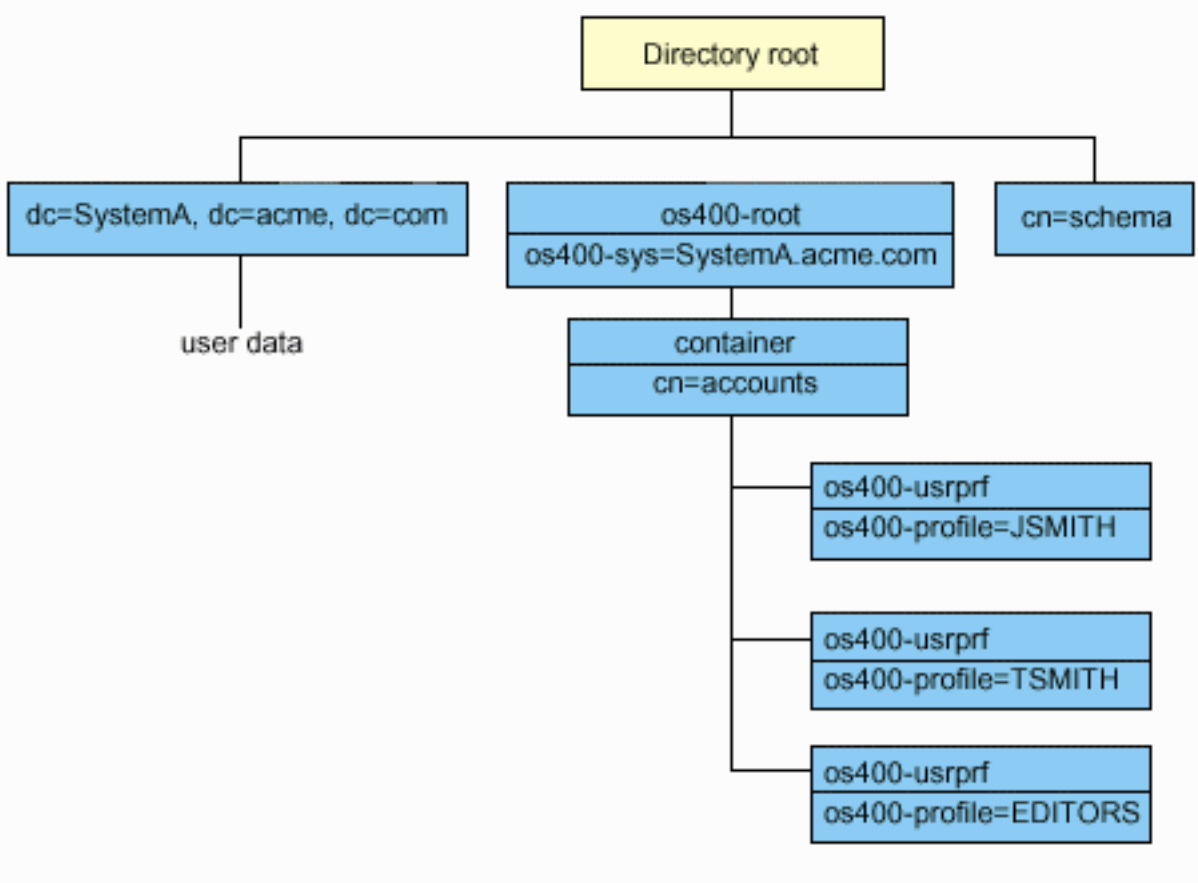
Če želite več informacij o ozadju, projiciranem z operacijskim sistemom, preglejte:

- “OS/400 uporabniško projicirano drevo informacij” na strani 39
- “Operacije LDAP” na strani 39
- “Povezovalni DN-ji skrbnika in kopije” na strani 43
- “OS/400 uporabniško projicirana shema” na strani 43

OS/400 uporabniško projicirano drevo informacij

Slika kaže zgled drevesa informacij imenika (DIT) za uporabniško projicirano ozadje. Prikazani so tako posamezni kot skupinski profili. Na sliki sta JSMITH in TSMITH uporabniška profila, kar je interno naznačeno z identifikatorjem skupine (GID), GID=*NONE (ali 0); EDITORS pa je skupinski profil, kar je interno naznačeno z neničelnim GID.

Pripona dc=SystemA,dc=acme,dc=com je na sliki zajeta kot referenca. Ta pripona predstavlja trenutno ozadje baze podatkov, ki upravlja druge postavke LDAP. Pripona cn=schema je trenutna shema, ki se uporablja prek celega strežnika.



Koren drevesa je pripona, katere privzeta vrednost je os400-sys=*SystemA.acme.com*, kjer je *SystemA.acme.com* ime vašega sistema. Razred objektov (objectclass) je os400-root. Čeprav DIT-a ni mogoče spremeniti ali zbrisati, lahko ponovno konfigurirate pripono objektov sistema. Zagotoviti morate, da se trenutna pripona ne uporablja v ACL-ih ali kjerkoli drugje v sistemu, kjer bi bilo potrebno spremeniti postavke, če bi prišlo do spremembe pripone.

Na prejšnji sliki je pod korenom prikazan vsebnik cn=accounts. Tega objekta ni mogoče spremeniti. Vsebnik je postavljen na to raven v pričakovanju drugih vrst informacij ali objektov, ki bi jih v prihodnje lahko projiciral operacijski sistem. Pod vsebnikom cn=accounts so uporabniški profili, ki so projicirani kot objectclass=os400-usrprf. Uporabniški profili se nanašajo na projicirane profile uporabnikov in so znani LDAP v obliki os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com.

Operacije LDAP

Z uporabo projiciranih profilov uporabnikov lahko izvedete naslednje operacije LDAP.

Povezovanje

Odjemalca LDAP lahko povežete (overite) s strežnikom LDAP z uporabo projiciranega profila uporabnika. To dosežete s podajanjem razločevalnega imena (DN) projiciranega profila uporabnika za povezovalni DN ter pravilnim geslom profila uporabnika OS/400 za overjanje. Zgled razločevalnega imena, uporabljenega v zahtevi za povezovanje, je os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com.

Odjemalec se mora povezati kot projicirani uporabnik, če želite dostopati do informacij v sistemsko projiciranem ozadju. Strežnik izvede vse operacije z uporabo pooblastila tega profila uporabnika. DN projiciranega profila uporabnika lahko uporabite tudi v ACL-ih LDAP, enako kot DN-je postavk LDAP. Preprosta metoda povezovanja je edina povezovalna metoda, ki je dovoljena, če je na zahtevi za povezovanje podan projiciran profil uporabnika.

Iskanje

Sistemsko projicirano ozadje podpira nekatere osnovne iskalne filtre. V iskalnih filtrih lahko podate atribute objectclass, os400-profile in os400-gid. Atribut os400-profile podpira univerzalne znake. Atribut os400-gid je omejen na podajanje (os400-gid=0), ki je posamezni uporabniški profil, ali !(os400-gid=0), ki je profil skupine. Prejmete lahko vse atribute profila uporabnika z izjemo gesla in podobnih atributov.

Za določene filtre sta vrnjeni le vrednosti DN objectclass in os400-profile, vendar lahko naslednja iskanja sestavite tako, da vrnejo podrobnejše informacije.

Naslednja tabela opisuje obnašanje sistemsko projiciranega ozadja za operacije iskanja.

Tabela 1. Obnašanje sistemsko projiciranega ozadja za operacije iskanja

Zahtevano iskanje	Iskanje osnove	Področje iskanja	Filter iskanja	Opombe
Vrne informacije za os400-sys=SystemA, (izbirno) za vsebnike pod njim ter (izbirno) za objekte v teh vsebnikih.	os400-sys=SystemA.acme.com	base, sub ali one	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	Vrne ustrezne atribute in njihove vrednosti na osnovi podanega območja in filtra. Programsko določeni atributi in njihove vrednosti so vrnjene za pripono sistemskih objektov ter vsebnikov pod njo.
Vrne vse uporabniške profile	cn=accounts, os400-sys=SystemA.acme.com	one ali sub	os400-gid=0	Za projicirane profile uporabnikov so vrnjeni le vrednosti razločevalnega imena (DN), objectclass in os400-profile. Če je podan katerikoli drug filter, je vrnjeno LDAP_UNWILLING_TO_PERFORM.
Vrne vse skupinske profile	cn=accounts, os400-sys=SystemA.acme.com	one ali sub	(!(os400-gid=0))	Za projicirane profile uporabnikov so vrnjeni le vrednosti razločevalnega imena (DN), objectclass in os400-profile. Če je podan katerikoli drug filter, je vrnjeno LDAP_UNWILLING_TO_PERFORM.

Tabela 1. Obnašanje sistemsko projiciranega ozadja za operacije iskanja (nadaljevanje)

Zahtevano iskanje	Iskanje osnove	Področje iskanja	Filter iskanja	Opombe
Vrne vse uporabniške in skupinske profile.	cn=accounts, os400-sys=SystemA.acme.com	one ali sub	os400-profile=*	Za projicirane profile uporabnikov so vrnjeni le vrednosti razločevalnega imena (DN), objectclass in os400-profile. Če je podan katerikoli drug filter, je vrnjeno LDAP_UNWILLING_TO_PERFORM.
Vrne informacije za specifični uporabniški ali skupinski profil, kot je uporabniški profil JSMITH.	cn=accounts, os400-sys=SystemA.acme.com	one ali sub	os400-profile=JSMITH	Podate lahko druge atribute, ki jih želite.
Vrne informacije za specifični uporabniški ali skupinski profil, kot je uporabniški profil JSMITH.	os400-profile=JSMITH, cn=accounts, os400-sys=SystemA.acme.com	bas, sub ali one	objectclass=os400-usrprf objectclass=* os400-profile=JSMITH	Podate lahko druge atribute, ki jih želite. Čeprav lahko podate območje ene ravni, rezultati iskanja ne bi vrnili vrednosti, ker ni v DIT ničesar pod profilom uporabnika JSMITH.
Vrne vse uporabniške in skupinske profile, ki se začenjajo z A.	cn=accounts, os400-sys=SystemA.acme.com	one ali sub	os400-profile=A*	Za projicirane profile uporabnikov so vrnjeni le vrednosti razločevalnega imena (DN), objectclass in os400-profile. Če je podan katerikoli drug filter, je vrnjeno LDAP_UNWILLING_TO_PERFORM.
Vrne vse skupinske profile, ki se začenjajo z G.	cn=accounts, os400-sys=SystemA.acme.com	one ali sub	(&(!(os400-gid=0)) (os400-profile=G*))	Za projicirane profile uporabnikov so vrnjeni le vrednosti razločevalnega imena (DN), objectclass in os400-profile. Če je podan katerikoli drug filter, je vrnjeno LDAP_UNWILLING_TO_PERFORM.
Vrne vse uporabniške profile, ki se začenjajo z A.	cn=accounts, os400-sys=SystemA.acme.com	one ali sub	(&(os400-gid=0) (os400-profile=A*))	Za projicirane profile uporabnikov so vrnjeni le vrednosti razločevalnega imena (DN), objectclass in os400-profile. Če je podan katerikoli drug filter, je vrnjeno LDAP_UNWILLING_TO_PERFORM.

Primerjava

Operacijo primerjave LDAP lahko uporabite za primerjavo vrednosti atributa ali projiciranega profila uporabnika. Atributov os400-aut in os400-docpwd ni mogoče primerjati.

Dodajanje in spreminjanje

Profile uporabnikov lahko izdelati z uporabo operacije dodajanja LDAP, prav tako pa lahko profile uporabnikov spremenite s pomočjo operacije spreminjanja LDAP.

Brisanje

Profile uporabnikov lahko zbrišete z uporabo operacije za brisanje LDAP. Če želite podati obnašanje parametrov DLTUSRPRF OWNOBJOPT in PGPOPT, sta na voljo dva krmilna elementa strežnika LDAP. Podate ju lahko pri operaciji brisanja LDAP. Če želite podrobnejše informacije o obnašanju teh parametrov, preglejte informacije o ukazu za brisanje profila uporabnika (DLTUSRPRF).

Na odjemalski operaciji brisanja LDAP lahko podate naslednje krmilne elemente ter njihove identifikatorje objektov (OID-e).

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  Sledi krmilna vrednost.
  - controlValue ::= ownObjOpt [newOwner]
  - ownObjOpt ::= *NODLT / *DLT / *CHGOWN

  Krmilna vrednost ownObjOpt podaja dejanje, ki ga je potrebno izvesti, če je profil uporabnik lastnik kateregakoli objekta. Vrednost *NODLT kaže, da se brisanje profila uporabnika ne izvede, če je profil uporabnika lastnik poljubnega objekta. Vrednost *DLT kaže, da se izvede brisanje lastniških objektov, vrednost *CHGOWN pa kaže, da se lastištvo prenese na drug profil uporabnika.

  Vrednost newOwner podaja profil, v katerega se prenese lastištvo. Ta vrednost je obvezna, če je ownObjOpt nastavljeno na *CHGOWN.

  Zgledi vrednosti krmilnih elementov:
  - *NODLT: podja, da profila ni mogoče zbrisati, če je lastnik kateregakoli objekta.
  - *CHGOWN SMITH: podaja prenos lastištva poljubnih objektov v profil uporabnika SMITH.
- Identifikator objekta (OID) je definiran v ldap.h kot LDAP_OS400_OWNOBJOPT_CONTROL_OID.
  - os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

    Vrednost krmilnega elementa je definirana takole:

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

    Krmilna vrednost pgpOpt podaja dejanje, ki ga je potrebno izvesti, če je profil uporabnika za brisanje primarna skupina za poljubne objekte. Če podate *CHGPGP, morate podati tudi newPgp. Vrednost newPgp podaja ime primarne skupine profilov ali *NONE. Če podate profil nove primarne skupine, morate podati tudi vrednost newPgpAut. Vrednost newPgpAut podaja pooblastilo za objekte, ki jim je podana nova primarna skupina.

  Zgledi vrednosti krmilnih elementov:
  - *NOCHG: podaja, da profila ni mogoče zbrisati, če je primarna skupina za katerikoli objekt.
  - *CHGPGP *NONE: podaja odstranitev primarne skupine za objekte.

– *CHGPGP SMITH *USE: podaja spreminjanje primarne skupine v profil uporabnika SMITH in dodelitev pooblastila *USE primarni skupini.

Če za brisanje ne podate nobenega od teh krmilnih elementov, se uporabijo privzete vrednosti, ki so trenutno v veljavi za ukaz QSYS/DLTUSRPRF.

ModRDN

Projiciranih profilov uporabnikov ne morete preimenovati, ker tega operacijski sistem ne podpira.

Uvažanje in izvažanje API-jev

API-ja QgldImportLdif in QgldExportLdif ne podpirata uvažanja ali izvažanja podatkov v sistemsko projiciranem ozadju.

Povezovalni DN-ji skrbnika in kopije

Projicirani profil uporabnika laho podate kot konfigurirani povezovalni DN skrbnika ali kopije. Uporablja se geslo profila uporabnika. Projicirani profili uporabnikov lahko postanejo tudi skrbniki LDAP, če so pooblaščeni identifikatorju funkcije skrbnika imeniškega strežnika (QIBM_DIRSRV_ADMIN). Skrbniški dostop lahko dodelite več profilom uporabnikov.

Če želite več informacij, poglejte “Delo z administrativnim dostopom za pooblaščene uporabnike” na strani 28.

OS/400 uporabniško projicirana shema

Razrede in lastnosti objektov iz projiciranega ozadja lahko najdete v shemi strežnika. Imena lastnosti LDAP so v formatu os400–*nnn*, kjer je *nnn* običajno ključna beseda lastnosti (kot je CRTUSRPRF ali CHGUSRPRF) v ukazih profila uporabnika. Za dodatne informacije glejte “OS/400 uporabniško projicirano drevo informacij” na strani 39.

Podpora za dnevnike v Imeniških storitvah OS/400

Za shranjevanje informacij o imenikih uporabljajo Imeniške storitve podporo za baze podatkov OS/400. Imeniške storitve uporabljajo krmiljenje odobritve za shranitev imeniških postavk v bazo podatkov. To zahteva podporo za vodenje dnevnika OS/400.

Pri prvem zagonu strežnika ali orodja za uvažanje LDIF, se izdela naslednje:

- Dnevnik
- Sprejemnik dnevnika
- Vse tabele baze podatkov, ki so potrebne na začetku

Dnevnik QSQJRN je izdelan v knjižnici baz podatkov, ki ste jo konfigurirali. Sprejemnik dnevnika QSQJRN0001 se v začetku izdela v knjižnici baz podatkov, ki ste jo konfigurirali.

Okolje, velikost in struktura imenika, strategija shranjevanja in obnavljanja lahko narekujejo nekatere spremembe od privzetih vrednosti, vključno z načinom upravljanja objektov ter uporabljenim pragom velikosti. Če je potrebno, lahko spremenite parametre ukaza za vodenje dnevnika. Beleženje LDAP je po privzetku nastavljeno za brisanje starih prejemnikov. Če je dnevnik sprememb konfiguriran in želite ohraniti stare prejemnike, v ukazni vrstici OS/400 izvršite naslednji ukaz:

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

Če ste konfigurirali dnevnik sprememb, lahko njegove sprejemnike dnevnika zbrišete z naslednjim ukazom:

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

Če želite informacije o ukazih za beleženje, preglejte temo Ukazi OS/400 v poglavju Programiranje v Informacijskem centru.

Poglavje 6. Pomožni programi v ukazni vrstici LDAP

Imeniške storitve vsebuje pet pomožnih programov, ki omogočajo, da izvedete dejanja v imeniškem strežniku LDAP iz ukaznega okolja Qshell v OS/400. Ti pomožni programi uporabljajo API-je LDAP. Te pomožne programe lahko uporabite iz ukazne vrstice qsh ali jih pokličete iz programov. Morda se vam zdijo primerni tudi kot zgledi za programiranje. Če namestite odjemalca LDAP Windows, ki je vključen v Imeniške storitve, namestite tudi kodo, ki je zelo podobna izvorni kodi za pomožne programe lupine.

Pomožni programi so naslednji:
- "Pomožna programa ldapmodify in ldapadd", ki dodajata oziroma popravljata postavke imenika LDAP.
- "Pomožni program ldapdelete" na strani 48, ki odstranjuje postavke iz imenika LDAP.
- "Pomožni program ldapsearch" na strani 50, ki išče postavke v imeniku LDAP.
- "Pomožni program ldapmodrdn" na strani 55, ki spreminja relativno razločevalno ime (RDN) postavk imenika LDAP.

Podrobnejše informacije o uporabi SSL s pomožnimi programi ukazne vrstice najdete v razdelku "Notes o uporabi SSL s pomožnimi programi ukazne vrstice SSL" na strani 57.

Pomožna programa ldapmodify in ldapadd

Pripomoček ldapmodify omogoča, da spremenite vnose ali jih dodate v imeniški strežnik prek ukazne lupine QSH vašega sistema. Uporablja vmesnike uporabniškega programa (API-je) ldap_modify, ldap_add in ldap_delete. Pomožni program ldapadd, deluje skoraj enako kot pomožni program ldapmodify, z izjemo, da se oznaka -a vključi samodejno.

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***]**

Opomba: Če ne podate informacij o postavki v *datoteka (file)* s pomočjo možnosti **-f**, bo pomožni program čakal na branje postavk iz standardnega vhodnega mesta. Če želite prekiniti čakanje, pritisnite tipko SysReq, in nato izberite 2. Končaj prejšnjo zahtevo.

Diagnostični podatki:

Če ni prišlo do napak, je izhodni status enak 0. Posledica napake pa je izhodni status, ki ni enak 0, ter diagnostično sporočilo, ki je izpisano poleg napake.

Kliknite tukaj, če želite videti zglede uporabe teh pomožnih programov.

Parametri:

-V	Podaja različico LDAP, ki jo pomožni program uporablja za povezovanje s strežnikom LDAP. Po privzetku uporablja povezavo V3 LDAP. Če želite izrecno izbrati LDAP V3, podajte -V 3. Če želite izvajanje kot aplikacija LDAP V2, podajte -V 2.
-a	Ta parameter uporablja samo pomožni program ldapmodify. Nakazuje, da bo pomožni program po privzetku raje dodajal postavke, kot pa jih spreminjal. Uporaba tega parametra je enaka uporabi ldapadd.

-b	S to možnostjo predpostavite, da so vse vrednosti, ki se začnejo z `/, dvojiške vrednosti, in da je njihova dejanska vrednost v datoteki, katere pot je podana na mestu, kjer se običajno pojavljajo vrednosti.
-c	Način nepretrganega delovanja. Sporočijo se napake, vendar pomožna programa ldapmodify ali ldapadd nadaljujeta s spreminjanjem oziroma dodajanjem. Privzeta vrednost določa izhod po sporočilu napak.
-r	S to možnostjo po privzetku zamenjate obstoječe vrednosti.
-M	Referenčne objekte upravlja kot navadne vnose.
-n	Prikažete, kaj bi se zgodilo, vendar dejanskega popravljanja postavk ne izvedete. Koristno pri razhroščevanju v povezavi z -v.
-v	Uporabite način z razlago, z veliko diagnostičnimi podatki, ki se zapišejo v standardni izhod.
-F	Vsilite uporabo vseh sprememb, ne glede na vsebino vhodnih vrstic, ki se začnejo s kopijo: (po privzetku se vrstice kopije primerjajo z gostiteljskim strežnikom LDAP in uporabljenimi vrati za odločitev, ali naj se dejansko uveljavi zapis dnevnika za kopiranje).
-R	Ta možnost podaja, da se referenčnim kazalcem ne sme slediti samodejno.
-C *charset*	Ta možnost podaja, da so nizi, ki so podani kot vhodni podatki pomožnemu programu, predstavljeni v lokalnem naboru znakov (*charset*) in morajo biti pretvorjeni v UTF-8. Če je kodna stran vhodnega niza drugačna od vrednosti kodne strani opravila, uporabite možnost nabora znakov**-C**. Preglejte dokumentacijo za ldap_set_iconv_local_charset() API, kjer boste našli podprte vrednosti za *charset*.
-d *debuglevel*	Nastavi raven iskanja napak na *debuglevel*.
-D *binddn*	Možnost *binddn* uporabite za povezovanje z imenikom LDAP. Parameter *binddn* mora biti razločevalno ime, predstavljeno z besedilom.
-w *passwd*	Za overjanje uporabite *passwd* kot geslo.
-m *mechanism*	Če želite podati mehanizem SASL, s katerim se bo odjemalec povezal s strežnikom, uporabite *mechanism*. Odjemalec uporablja API ldap_sasl_bind_s(). Razpoložljivi mehanizmi vključujejo CRAM-MD5 (šifrira geslo), EXTERNAL (uporabljen s SSL) in GSSAPI (Kerberos). Ukaz zanemari parameter **-m**, če je nastavljen **-V 2**. Če ne podate parametra **-m**, bo uporabljeno preprosto overjanje.
-O*hopcount*	Če želite nastaviti največje število preskokov, ki jih bo odjemalska knjižnica opravila pri zasledovanju referenčnih kazalcev, podajte *hopcount*. Privzeta vrednost za hopcount je 10.
-h *ldaphost*	S to možnostjo podate nadomestnega gostitelja, v katerem se izvaja strežnik LDAP.
-p *ldapport*	S to možnostjo podate nadomestna vrata TCP (Transmission Control Protocol), kjer posluša strežnik LDAP. Privzeta vrata LDAP so 389. Če vrata niso podana in podate možnost **-Z**, se uporabijo vrata SSL LDAP 636.
-f *file*	S to možnostjo preberete informacije o popravkih postavke iz datoteke LDIF namesto iz standardnega vhodnega mesta. Če datoteka LDIF ni podana, morate z uporabo standardnega vhodnega mesta podati zapise za ažuriranje v formatu LDIF.
-Z	To možnost uporabite, če povezava SSL komunicira s strežnikom LDAP. Možnost **-Z** podpirajo samo SSL-različice tega orodja.
-K *keyfile*	S to možnostjo podate datoteko baze podatkov ključev SSL. Če datoteka baze podatkov ključev ni v trenutnem imeniku, podajte celotno ime datoteke baze podatkov ključev. Če pomožni program ne more določiti položaja baze podatkov ključev, bo uporabil programsko določen niz privzetih overjenih skrbnikov služb za pooblastila. Datoteka baze podatkov ključev vsebuje običajno enega ali več potrdil služb za pooblastila (CA), ki jim zaupajo odjemalci. Ti tipi potrdil X.509 so običajno poznani kot overjena potrdila. Ta parameter učinkovito omogoča stikalo **-Z**.

-P *keyfilepw*	Podaja geslo baze podatkov ključev. To geslo se zahteva za dostop do šifriranih informacij v datoteki baze podatkov ključev (ki vključuje zasebni ključ). Če skrito datoteko z gesli povežete z datoteko baze podatkov, bo geslo prebrano iz skrite datoteke, ta parameter pa ne bo potreben. Ta parameter se zanemari, če ne podate **-Z** ali **-K**.
-N *certificatename*	S to možnostjo podate oznako, ki je povezava s potrdilom odjemalca v datoteki baze podatkov ključev. Pomnite, da v primeru, da je strežnik LDAP konfiguriran samo za overjanje strežnika, potrdilo odjemalca ni potrebno. Če je strežnik LDAP konfiguriran za overjanje odjemalca in strežnika, je zahtevano tudi potrdilo odjemalca. Parameter *certificatename* ni zahtevan, če ste kot privzetek določili par potrdilo/zasebni ključ. Prav tako *certificatename* ni potreben, če v določeni datoteki baze podatkov obstaja posamezni par potrdila in zasebnega ključa. Ta parameter se zanemari, če ne podate **-Z** ali **-K**.

Nadomestni vhodni format:

Pomožni program ldapmodify podpira nadomestni vhodni format, da lahko vzdržuje združljivost s starejšimi različicami programa. Ta format je sestavljen iz ene ali več postavk, ki so ločene s praznimi vrsticami. Vsaka postavka ima naslednji format:

```
Razločevalno ime (DN)
attr=vrednost
[attr=vrednost...]
```

kjer je *attr* ime lastnosti, *vrednost* pa vrednost lastnosti. Po privzetku se vrednosti dodajajo. Če podate oznako ukazne vrstice **-r**, se privzeti način spremeni tako, da se obstoječe vrednosti nadomeščajo z novimi. Pomnite, da je za podano lastnost dovoljeno, da se pojavi večkrat (za lastnost lahko dodate več vrednosti). Pomnite tudi, da lahko na koncu vrstice uporabite poševnico nazaj (\), ki podaja nadaljevanje vrednosti v naslednji vrstici in ohranja vrednosti prejšnje vrstice. Če želite vrednost odstraniti, postavite pred vrednost *attr* vezaj (-). Znak za enačaj (=) in vrednost uporabite, če želite odstraniti celotno lastnost. Če želite dodati vrednost, morate pred *attr* postaviti znak plus (+) ter podati tudi oznako **-r**.

Zgledi: ldapmodify in ldapadd

Zgled 1:

Če datoteka /**tmp**/**entrymods** obstaja in ima naslednjo vsebino:

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

bo ukaz ldapmodify -b -r -f /tmp/entrymods storil naslednje:

- Zamenjal bo vsebino lastnosti pošte postavke Modify Me z vrednostjo modme@student.of.life.edu.
- Dodal bo naziv Grand Poobah.
- Dodal bo vsebino datoteke /**tmp**/**modme.jpeg** kot sliko v obliki jpegPhoto.
- V celoti bo odstranil lastnost description.

Iste spremembe lahko izvedete s starejšim vhodnim formatom ldapmodify:

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

Ukaz za uporabo starega formata je naslednji:

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

Zgled 2:

Predpostavimo, da datoteka /**tmp**/**newentry** obstaja in ima naslednjo vsebino:

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

Ukaz ldapadd -f /tmp/entrymods bo dodal novo postavko za John Doe z uporabo vrednosti iz datoteke /tmp/newentry.

Zgled 3:

Če datoteka /**tmp**/**newentry** obstaja in ima vsebino:

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

bo ukaz ldapmodify -f /tmp/entrymods odstranil postavko za John Doe.

Pomožni program ldapdelete

S pomožnim programom ldapdelete lahko zbrišete eno ali več postavk iz imeniškega strežnika LDAP. Teče v ukazni lupini QSH programa OS/400. V ta namen uporablja vmesnik uporabniškega programa (API) ldap_delete.

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_**]...**

Opomba: Če argumentov *dn* ne podate, bo ukaz ldapdelete čakal na branje seznama razločevalnih imen iz standardnega vhodnega mesta. Če želite prekiniti čakanje, pritisnite tipko SysReq, in nato izberite 2. Končaj prejšnjo zahtevo.

Diagnostični podatki:

Če ni prišlo do napak, je izhodni status enak 0. Posledica napake pa je izhodni status, ki ni enak 0, ter diagnostično sporočilo, ki je izpisano poleg napake.

Kliknite tukaj, če videti zglede uporabe pomožnega programa ldapdelete.

Parametri:

-V	Podaja različico LDAP, ki jo pomožni program uporablja za povezovanje s strežnikom LDAP. Po privzetku uporablja povezavo V3 LDAP. Če želite izrecno izbrati LDAP V3, podajte -V 3. Če želite izvajanje kot aplikacija LDAP V2, podajte -V 2.
-M	Referenčne objekte upravlja kot navadne vnose.
-n	Prikažete, kaj bi se zgodilo, vendar dejanskega brisanja ne izvedete. Koristno pri razhroščevanju v povezavi z **-v**.
-v	Uporabite način z razlago, z veliko diagnostičnimi podatki, ki se zapišejo v standardni izhod.
-c	Način nepretrganega delovanja. Sporočijo se napake, vendar bo ldapdelete nadaljeval z brisanjem. Privzeta vrednost določa izhod po sporočilu napak.
-R	Ta možnost podaja, da se referenčnim kazalcem ne sme slediti samodejno.
-C *charset*	Ta možnost podaja, da so razločevalna imena (DN-ji), ki so podani kot vhodni podatki pomožnemu programu ldapdelete, predstavljeni v lokalnem naboru znakov (*charset*). Možnost **-C** *charset* uporabite, če želite nadomestiti privzeto vrednost, kjer morajo biti nizi podani v UTF-8. Če je kodna stran vhodnega niza drugačna od vrednosti kodne strani opravila, uporabite možnost nabora znakov**-C**. Preglejte dokumentacijo za ldap_set_iconv_local_charset() API, kjer boste našli podprte vrednosti za *charset*.
-d *debuglevel*	Nastavi raven iskanja napak na *debuglevel*.
-f *file*	Z možnostjo *file* preberete nize vrstic iz datoteke in izvedete eno brisanje LDAP za vsako vrstico v datoteki. Vsaka vrstica v datoteki bi morala vsebovati posamezno razločevalno ime (DN).
-D *binddn*	Možnost *binddn* uporabite za povezovanje z imenikom LDAP. Parameter *binddn* mora biti razločevalno ime, predstavljeno z besedilom.
-w *passwd*	Za overjanje uporabite *passwd* kot geslo.
-m *mechanism*	Možnost *mechanism* podaja mehanizem SASL, ki se uporablja za povezovanje s strežnikom. Uporabljen bo API ldap_sasl_bind_s(). Razpoložljivi mehanizmi vključujejo CRAM-MD5 (šifrira geslo), EXTERNAL (uporabljen s SSL) in GSSAPI (Kerberos). Parameter -m bo zanemarjen, če nastavite -V 2. Če parametra **-m** ne podate, bo uporabljeno preprosto overjanje.
-O *hopcount*	Možnost *hopcount* podajte za nastavitev največjega števila preskokov, ki jih bo izvedla knjižnica odjemalca pri zasledovanju referenčnih kazalcev. Privzeta vrednost za hopcount je 10.
-h *ldaphost*	S to možnostjo podate nadomestnega gostitelja, v katerem se izvaja strežnik LDAP.
-p *ldapport*	S to možnostjo podate nadomestna vrata TCP (Transmission Control Protocol), kjer posluša strežnik LDAP. Privzeta vrata LDAP so 389. Če vrata niso podana in podate možnost **-Z**, se uporabijo vrata SSL LDAP 636.
-Z	To možnost uporabite, če povezava SSL komunicira s strežnikom LDAP. Možnost **-Z** podpirajo samo SSL-različice tega orodja.
-K *keyfile*	S to možnostjo podate datoteko baze podatkov ključev SSL. Če datoteka baze podatkov ključev ni v trenutnem imeniku, podajte celotno ime datoteke baze podatkov ključev. Če pomožni program ne more določiti položaja baze podatkov ključev, bo uporabil programsko določen niz privzetih overjenih skrbnikov služb za pooblastila. Datoteka baze podatkov ključev vsebuje običajno enega ali več potrdil služb za pooblastila (CA), ki jim zaupajo odjemalci. Ti tipi potrdil X.509 so običajno poznani kot overjena potrdila. Ta parameter učinkovito omogoča stikalo **-Z**.
-P *keyfilepw*	Podaja geslo baze podatkov ključev. To geslo se zahteva za dostop do šifriranih informacij v datoteki baze podatkov ključev (ki vključuje zasebni ključ). Če skrito datoteko z gesli povežete z datoteko baze podatkov, bo geslo prebrano iz skrite datoteke, ta parameter pa ne bo potreben. Ta parameter se zanemari, če ne podate **-Z** ali **-K**.

-N *certificatename*	S to možnostjo podate oznako, ki je povezava s potrdilom odjemalca v datoteki baze podatkov ključev. Pomnite, da v primeru, da je strežnik LDAP konfiguriran samo za overjanje strežnika, potrdilo odjemalca ni potrebno. Če je strežnik LDAP konfiguriran za overjanje odjemalca in strežnika, je zahtevano tudi potrdilo odjemalca. Parameter *certificatename* ni zahtevan, če ste kot privzetek določili par potrdilo/zasebni ključ. Prav tako *certificatename* ni potreben, če v določeni datoteki baze podatkov obstaja posamezni par potrdila in zasebnega ključa. Ta parameter se zanemari, če ne podate **-Z** ali **-K**.
dn	Podaja enega ali več argumentov *dn*. Vsak *dn* mora biti razločevalno ime, predstavljeno z besedilom.

Zgled: ldapdelete

Naslednji ukaz bo poskušal zbrisati postavko s splošnim imenom (commonName) Delete Me neposredno pod organizacijsko postavko University of Life:

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

Morda boste morali vnesti *binddn* in *passwd* (glejte možnosti **-D** in **-w**).

Pomožni program ldapsearch

Pomožni program ldapsearch omogoča iskanje postavke v imeniškem strežniku iz ukazne lupine QSH v OS/400. Uporablja aplikacijski programerski vmesnik (API) ldap_search.

Iskanje uporablja filter, ki ustreza predstavitvi nizov za filtre LDAP. Če želite podrobnejše informacije o filtrih za iskanje, preglejte informacije o API-ju ldap_search v temi Imeniške storitve OS/400 pod Programiranje v Informacijskem centru.

Če pomožni program ldapsearch najde eno ali več postavk, prikliče lastnosti, ki ste jih podali z *attrs*, in postavke ter njihove vrednosti natisne v standardni izhod. Če ne podate nobenih lastnosti, se vrnejo vse lastnosti.

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...***]**

Diagnostični podatki:

Če ni prišlo do napak, je izhodni status enak 0. Posledica napake pa je izhodni status, ki ni enak 0, ter diagnostično sporočilo, ki je izpisano poleg napake.

Izhodni format:

Če ldapsearch najde eno ali več postavk, jih zapiše v standardni izhod v obliki:

```
Razločevalno ime (DN)
ime_lastnosti=vrednost
ime_lastnosti=vrednost
ime_lastnosti=vrednost
...
```

Postavke se med seboj ločene z eno prazno vrstico. Če uporabite možnost **-F** za podajanje razločevalnega znaka, prikaže rezultat ta znak namesto enačaja (=). Če uporabljate možnost **-t**, ime začasne datoteke zamenja dejansko vrednost. Če podate možnost **-A**, se zapiše samo del ime_lastnosti.

Kliknite tukaj, če videti zglede uporabe pomožnega programa ldapsearch.

Parametri:

-V	Podaja različico LDAP, ki jo pomožni program uporablja za povezovanje s strežnikom LDAP. Po privzetku uporablja povezavo V3 LDAP. Če želite izrecno izbrati LDAP V3, podajte -V 3. Če želite izvajanje kot aplikacija LDAP V2, podajte -V 2.
-n	Prikažete, kaj bi se zgodilo, vendar dejanskega iskanja ne izvedete. Koristno pri razhroščevanju v povezavi z **-v**.
-v	Uporabite način z razlago, z veliko diagnostičnimi podatki, ki se zapišejo v standardni izhod.
-t	Poiskane vrednosti zapišete v niz začasnih datotek. To je koristno pri ukvarjanju z dvojiškimi vrednostmi, kot so slike jpegPhoto ali zvok.
-A	Poiščete samo lastnosti (brez vrednosti). Ta možnost je koristna, če želite videti samo, ali lastnost obstaja v postavki, in vas ne zanimajo posamezne vrednosti.
-B	S to možnostjo ne zadržite prikaza dvojiških vrednosti. Koristna je v primeru, če se ukvarjate z vrednostmi, ki se pojavljajo v nadomestnih naborih znakov, kot je ISO-8859.1. To možnost vsebuje **-L**
-L	S to možnostjo prikažete rezultate iskanja v formatu LDIF. Ta možnost vključi tudi možnost **-B** in povzroči, da se možnost **-F** zanemari.
-M	Referenčne objekte upravlja kot navadne vnose.
-R	Ta možnost podaja, da se referenčnim kazalcem ne sme slediti samodejno.
-C *charset*	Ta možnost podaja, da so nizi, ki so podani kot vhodni podatki pomožnemu programu ldapsearch, predstavljeni v lokalnem naboru znakov (*charset*). Vhodni podatki vključujejo filter, povezovalni DN in osnovni DN. Podobno bo pri prikazu podatkov ldapsearch pretvoril sprejete podatke iz strežnika LDAP v podane znake. Če je kodna stran vhodnega niza drugačna od vrednosti kodne strani opravila, uporabite možnost nabora znakov**-C**. Preglejte dokumentacijo za ldap_set_iconv_local_charset() API, kjer boste našli podprte vrednosti za *charset*. Če sta podani obe možnosti, -C in -L, je predpostavljeno, da so vhodni podatki v podanem naboru znakov, izhodni podatki iz pomožnega programa ldapsearch pa se vedno ohranjajo v predstavitvi UTF-8 ali v predstavitvi base 64-encoded, ko so odkriti znaki, ki jih ni mogoče natisniti. To je zgled, ko standardne datoteke LDIF vsebujejo samo predstavitev niza znakov v obliki UTF-8 (ali base 64-encoded UTF-8).
-d *debuglevel*	Nastavi raven iskanja napak na *debuglevel*.
-F *sep*	Možnost *sep* uporabite kot ločilo polj med imeni in vrednostmi atributov. Privzeto ločilo je `=, razen če z oznako **-L** ne podate drugače. V tem primeru ta možnost ni upoštevana.
-f *file*	S to možnostjo preberete nize vrstic iz datoteke in izvedete eno iskanje LDAP za vsako vrstico v datoteki. Vsaka vrstica v datoteki bi morala vsebovati posamezno razločevalno ime (DN).
-D *binddn*	Možnost *binddn* uporabite za povezovanje z imenikom LDAP. Parameter *binddn* mora biti razločevalno ime, predstavljeno z besedilom.
-w *passwd*	Za overjanje uporabite *passwd* kot geslo.
-m *mechanism*	Z možnostjo *mechanism* podajte mehanizem SASL, ki se uporablja za povezovanje s strežnikom. Uporabljen bo API ldap_sasl_bind_s(). Razpoložljivi mehanizmi vključujejo CRAM-MD5 (šifrira geslo), EXTERNAL (uporabljen s SSL) in GSSAPI (Kerberos). Parameter **-m** se zanemari, če je nastavljen na **-V** 2. Če **-m** ne podate, se uporabi preprosto overjanje.
-O *hopcount*	Možnost *hopcount* podajte za nastavitev največjega števila preskokov, ki jih bo izvedla knjižnica odjemalca pri zasledovanju referenčnih kazalcev. Privzeta vrednost za hopcount je 10.
-h *ldaphost*	S to možnostjo podate nadomestnega gostitelja, v katerem se izvaja strežnik LDAP.

-p *ldapport*	S to možnostjo podate nadomestna vrata TCP (Transmission Control Protocol), kjer posluša strežnik LDAP. Privzeta vrata LDAP so 389. Če vrata niso podana in podate možnost **-Z**, se uporabijo vrata SSL (Secure Sockets Layer) LDAP 636.
-Z	To možnost uporabite, če povezava SSL komunicira s strežnikom LDAP. Možnost **-Z** podpirajo samo SSL-različice tega orodja.
-K *keyfile*	S to možnostjo podate datoteko baze podatkov ključev SSL. Če datoteka baze podatkov ključev ni v trenutnem imeniku, podajte celotno ime datoteke baze podatkov ključev. Če pomožni program ne more določiti položaja baze podatkov ključev, bo uporabil programsko določen niz privzetih overjenih skrbnikov služb za pooblastila. Datoteka baze podatkov ključev vsebuje običajno enega ali več potrdil služb za pooblastila (CA), ki jim zaupajo odjemalci. Ti tipi potrdil X.509 so običajno poznani kot overjena potrdila. Ta parameter učinkovito omogoča stikalo **-Z**.
-P *keyfilepw*	Podaja geslo baze podatkov ključev. To geslo se zahteva za dostop do šifriranih informacij v datoteki baze podatkov ključev (ki vključuje zasebni ključ). Če je skrita datoteka gesla povezana z datoteko baze podatkov ključev, se geslo pridobi iz skrite datoteke in ta parameter ni potreben. Ta parameter se zanemari, če ne podate **-Z** ali **-K**.
-N *certificatename*	S to možnostjo podate oznako, ki je povezava s potrdilom odjemalca v datoteki baze podatkov ključev. Pomnite, da v primeru, da je strežnik LDAP konfiguriran samo za overjanje strežnika, potrdilo odjemalca ni potrebno. Če je strežnik LDAP konfiguriran za overjanje odjemalca in strežnika, je zahtevano tudi potrdilo odjemalca. Parameter *certificatename* ni zahtevan, če ste kot privzetek določili par potrdilo/zasebni ključ. Prav tako *certificatename* ni potreben, če v določeni datoteki baze podatkov obstaja posamezni par potrdila in zasebnega ključa. Ta parameter se zanemari, če ne podate **-Z** ali **-K**.
-b *searchbase*	Možnost *searchbase* uporabite kot začetno točko za iskanje namesto privzete vrednosti. Če parametra **-b** ne podate, bo ta pomožni program preveril spremenljivko okolja LDAP_BASEDN in poiskal definicijo *searchbase*.
-s *scope*	S to možnostjo podajte območje iskanja. Parameter *scope* ima lahko vrednost base, one ali sub, s katero podate iskanje v osnovnem objektu, eno-nivojsko iskanje ali iskanje po poddrevesu. Privzeta vrednost je sub.
-a *deref*	S to možnostjo podate, kako se opravi dereferenciranje vzdevkov. Parameter *deref* lahko zavzame eno od vrednosti: never, always, search ali find. Z njimi podate, da se vzdevki nikoli (never) ne dereferencirajo, vedno (always) dereferencirajo, dereferencirajo pri iskanju ali dereferencirajo samo pri iskanju osnovnega objekta za iskanje. Privzeta vrednost je, da se vzdevki nikoli (never) ne dereferencirajo.
-l *timelimit*	Z možnostjo *timelimit* podate najdaljše obdobje za dokončanje iskanja.
-z *sizelimit*	S to možnostjo omejite rezultate iskanja na največ *sizelimit* postavk. S tem lahko postavite zgornjo mejo števila postavk, ki jih vrne operacija iskanja.
filter	Podaja ime filtra, ki ga uporablja iskanje.
attrs...	Možnost podaja lastnosti, ki jih poišče pomožni program, če iskanje najde eno ali več postavk. Če za parameter *attrs* ne podate nobenih vrednosti, pomožni program vrne vse lastnosti.

Zgledi: ldapsearch

Zgled 1:

Ukaz ldapsearch cn=john doe cn telephoneNumber izvede iskanje po poddrevesu (z uporabo privzete osnove za iskanje) za postavke s commonName john doe. Funkcija iskanja poišče vrednosti commonName in telephoneNumber ter jih natisne v standardno izhodno mesto. Če iskanje najde dve postavki, lahko rezultat izgleda takole:

```
cn=John E Doe, ou=College of Literature, Science, and the Arts,
ou=Students, ou=People, o=University of Higher Learning,
c=US
```

```
cn=John Doe
cn=John Edward Doe
cn=John E Doe 1
cn=John E Doe
telephoneNumber=+1 313 555-5432

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

Zgled 2:

Ukaz ldapsearch -t uid=jed jpegPhoto audio izvede iskanje po poddrevesu z uporabo privzete osnove za iskanje postavk, ki imajo ID uporabnika jed. Iskanje poišče vrednosti jpegPhoto in audio ter jih zapiše v začasne datoteke. Če iskanje najde eno postavko z eno vrednostjo za vsako zahtevano lastnost, lahko rezultat izgleda takole:

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

Zgled 3:

Ukaz ldapsearch -L -s one -b c=US o=university* o description izvede eno-nivojsko iskanje na ravni c=US. To iskanje išče vse organizacije, katerih organizationName (ime organizacije) se začne z university . Iskanje prikaže rezultate v formatu LDIF. Poišče vrednosti lastnosti organizationName in description ter jih natisne v standardno izhodno mesto, ki izgleda podobno naslednjemu:

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

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

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

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

Zgled 4:

Kot je bilo razloženo v razdelku “Referenčni kazalci imenika LDAP” na strani 35, lahko imeniki LDAP Imeniške storitve vsebujejo referenčne objekte, ki lahko vsebujejo le naslednje:

- Razločevalno ime (dn).
- Razred objektov (objectClass).

- Lastnost referenčnih kazalcev (ref).

Ta zgled prikazuje iskanja, kjer je vključen objekt referenčnega kazalca.

Predpostavimo, da vsebuje System_A postavko referenčnega kazalca:

```
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
```

Vse lastnosti, ki so povezane s postavko, bi morale biti v System_B.

System_B vsebuje postavko:

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

Ko odjemalec izda zahtevo sistemu System_A in ne pošlje krmilnega elementa manageDsaIT, strežnik vrne referenčni kazalec. Na primer, če uporabite -M s pomožnim programom ldapsearch, se strežnik LDAP na System_A odzove odjemalcu z naslednjim URL:

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

Odjemalec uporablja te informacije za izdajo zahteve v System_B. Če vsebuje postavka v System_A poleg dn, objectclass in ref še lastnosti, strežnik zanemari te lastnosti.

Če odjemalec iz strežnika sprejme odziv referenčnega kazalca, znova izda zahtevo, tokrat strežniku, na katerega se nanaša vrnjeni URL. Če je bilo iskanje izvedeno z enonivojskim območjem, zahteva referenčnega kazalca uporablja osnovno območje. Rezultati tega iskanja se spreminjajo glede na vrednost, ki jo podate za območje iskanja (**-b**).

Če podate -s sub, kot je prikazano tukaj:

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

vrne vse atribute za vse postavke z sn=Jensen, ki se nahajajo v ali pod ou=Rochester, o=Big Company, c=US na System_A in System_B. Odjemalec prejme referenčni kazalec iz System_A in preišče System_B ter vrne cn=Barb Jense,ou=Rochester,o=Big Company,c=US.

Če podate -s one, kot je prikazano tukaj:

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

iskanje ne vrne nobenih postavk iz nobenega sistema. Namesto tega vrne strežnik odjemalcu URL referenčni kazalec:

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

Odjemalec, ki je na vrsti, predloži zahtevo:

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

To vrne postavko cn=Barb Jensen,ou=Rochester,o=Big Company,c=US.

Pomožni program ldapmodrdn

Pomožni program ldapmodrdn omogoča spreminjanje relativnega razločevalnega imena (RDN) postavk v imeniškem strežniku LDAP. Uporabljate ga v ukazni lupini QSH v OS/400. V ta namen uporablja vmesnik uporabniškega programa (API) ldap_modrdn.

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***]**

Opombe:

1. Če podate argumenta ukazne vrstice *dn* in *rdn*, bo *rdn* zamenjal RDN postavke, ki je podana z DN, *dn*. V nasprotnem primeru lahko datoteko sestavlja (ali standardne vhodne podatke, če ne podate oznake **-f**) ena ali več postavk.

   ```
   Razločevalno ime (DN)

   Relativno razločevalno ime (RDN)
   ```

   Ena ali več praznih vrstic ločuje vsak par DN/RDN.
2. Če ne podate informacij o postavki v *datoteki (file)* s pomočjo možnosti **-f** (ali s parom *dn* in *rdn* v ukazni vrstici), bo ukaz ldapmodrdn pričakoval postavke iz standardnega vhodnega mesta. Če želite prekiniti čakanje, pritisnite tipko SysReq, in nato izberite 2. Končaj prejšnjo zahtevo.

Diagnostični podatki:

Če ni prišlo do napak, je izhodni status enak 0. Posledica napake pa je izhodni status, ki ni enak 0, ter diagnostično sporočilo, ki je izpisano poleg napake.

Kliknite tukaj, če želite prikazati zgled uporabe ldapmodrdn.

Parametri:

-V	Podaja različico LDAP, ki jo pomožni program uporablja za povezovanje s strežnikom LDAP. Po privzetku uporablja povezavo V3 LDAP. Če želite izrecno izbrati LDAP V3, podajte -V 3. Če želite izvajanje kot aplikacija LDAP V2, podajte -V 2.
-r	S to možnostjo odstranite relativno razločevalno ime (RDN) iz postavke. Privzeta vrednost določa ohranitev starih vrednosti.
-M	Referenčne objekte upravlja kot navadne vnose.
-n	Prikažete, kaj bi se zgodilo, vendar dejanskega spreminjanja ne izvedete. Koristno pri razhroščevanju v povezavi z **-v**.
-v	Uporabite način z razlago, z veliko diagnostičnimi podatki, ki se zapišejo v standardni izhod.
-c	Način nepretrganega delovanja. Sporočijo se napake, vendar bo ldapmodrdn nadaljeval s spremembami. Privzeta vrednost določa izhod po sporočilu napak.
-R	Ta možnost podaja, da se referenčnim kazalcem ne sme slediti samodejno.
-C *charset*	Ta možnost podaja, da so nizi, ki so podani kot vhodni podatki pomožnemu programu, predstavljeni v lokalnem naboru znakov (*charset*) in morajo biti pretvorjeni v UTF-8. Če je kodna stran vhodnega niza drugačna od vrednosti kodne strani opravila, uporabite možnost nabora znakov**-C**. Preglejte dokumentacijo za ldap_set_iconv_local_charset() API, kjer boste našli podprte vrednosti za *charset*.
-d *debuglevel*	Nastavi raven iskanja napak na *debuglevel*.

-D *binddn*	Možnost *binddn* uporabite za povezovanje z imenikom LDAP. Parameter *binddn* mora biti razločevalno ime, predstavljeno z besedilom.
-w *passwd*	Za overjanje uporabite *passwd* kot geslo.
-m *mechanism*	Možnost *mechanism* podaja mehanizem SASL, ki se uporablja za povezovanje s strežnikom. Uporabljen bo API ldap_sasl_bind_s(). Razpoložljivi mehanizmi vključujejo CRAM-MD5 (šifrira geslo), EXTERNAL (uporabljen s SSL) in GSSAPI (Kerberos). Parameter -m se ne upošteva, če je nastavljena možnost -V 2. Če parametra **-m** ne podate, bo uporabljeno preprosto overjanje.
-O *hopcount*	Možnost *hopcount* podajte za nastavitev največjega števila preskokov, ki jih bo izvedla knjižnica odjemalca pri zasledovanju referenčnih kazalcev. Privzeta vrednost za hopcount je 10.
-h *ldaphost*	S to možnostjo podate nadomestnega gostitelja, v katerem se izvaja strežnik LDAP.
-p *ldapport*	S to možnostjo podate nadomestna vrata TCP (Transmission Control Protocol), kjer posluša strežnik LDAP. Privzeta vrata LDAP so 389. Če vrata niso podana in podate možnost **-Z**, se uporabijo vrata SSL LDAP 636.
-Z	To možnost uporabite, če povezava SSL komunicira s strežnikom LDAP. Možnost **-Z** podpirajo samo SSL-različice tega orodja.
-K *keyfile*	S to možnostjo podate datoteko baze podatkov ključev SSL. Če datoteka baze podatkov ključev ni v trenutnem imeniku, podajte celotno ime datoteke baze podatkov ključev. Če pomožni program ne more določiti položaja baze podatkov ključev, bo uporabil programsko določen niz privzetih overjenih skrbnikov služb za pooblastila. Datoteka baze podatkov ključev vsebuje običajno enega ali več potrdil služb za pooblastila (CA), ki jim zaupajo odjemalci. Ti tipi potrdil X.509 so običajno poznani kot overjena potrdila. Ta parameter učinkovito omogoča stikalo **-Z**.
-P *keyfilepw*	Podaja geslo baze podatkov ključev. To geslo se zahteva za dostop do šifriranih informacij v datoteki baze podatkov ključev (ki vključuje zasebni ključ). Če skrito datoteko z gesli povežete z datoteko baze podatkov, bo geslo prebrano iz skrite datoteke, ta parameter pa ne bo potreben. Ta parameter se zanemari, če ne podate **-Z** ali **-K**.
-N *certificatename*	S to možnostjo podate oznako, ki je povezava s potrdilom odjemalca v datoteki baze podatkov ključev. Pomnite, da v primeru, da je strežnik LDAP konfiguriran samo za overjanje strežnika, potrdilo odjemalca ni potrebno. Če je strežnik LDAP konfiguriran za overjanje odjemalca in strežnika, je zahtevano tudi potrdilo odjemalca. Parameter *certificatename* ni zahtevan, če ste kot privzetek določili par potrdilo/zasebni ključ. Prav tako *certificatename* ni potreben, če v določeni datoteki baze podatkov obstaja posamezni par potrdila in zasebnega ključa. Ta parameter se zanemari, če ne podate **-Z** ali **-K**.
-f *file*	S to možnostjo preberete informacije o popravkih postavke iz datoteke LDIF namesto iz standardnega vhodnega mesta ali ukazne vrstice (tako da podate *dn* in novi *rdn*). Za standardno vhodno mesto lahko podate tudi datoteko (< file).
dn rdn	S to možnostjo podate razločevalno ime postavke, ki ga želite preimenovati z novim relativnim razločevalnim imenom za postavko.

Zgled: ldapmodrdn

Predpostavimo, da ste že izdelali besedilno datoteko /**tmp**/**entrymods** z naslednjo vsebino:

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

Ukaz:

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

bo spremenil RDN postavke Modify Me iz Modify Me v The New Me. Stari cn, Modify Me bo odstranjen.

Notes o uporabi SSL s pomožnimi programi ukazne vrstice SSL

Če želite uporabiti možnosti SSL (plast zaščitenih vtičnic) pomožnih programov ukazne vrstice, morate imeti nameščene izdelke ponudnika šifriranega dostopa (5722-ACx).

“Uporaba zaščite plasti zaščitnih vtičnic (SSL) in zaščite prevajalne plasti z imeniškim strežnikom LDAP” na strani 37 razlaga uporabo SSL s strežnikom LDAP Imeniških storitev. Te informacije zajemajo upravljanje in izdelovanje overjenih služb za pooblastila z upravljalnikom digitalnih potrdil.

Nekateri strežniki LDAP, do katerih dostopajo odjemalci, uporabljajo le overjanje strežnika. Za te strežnike morate v prostoru za potrdila samo definirati eno ali več overjenih potrdil. Z overjanjem strežnika je odjemalcu zagotovljeno, da je ciljnemu strežniku LDAP potrdilo izdala ena od overjenih služb za pooblastila (CA). Dodatno se zašifrirajo vse transakcije LDAP, ki tečejo prek povezave SSL s strežnikom. To vključuje poverilnice LDAP, ki jih podate v vmesnikih uporabniških programov, ki jih uporabljate za povezovanje z imeniškim strežnikom. Če na primer strežnik LDAP uporablja potrdilo Verisign, morate storiti naslednje:

1. Priskrbeti potrdilo CA pri Verisign.
2. Uporabiti upravljalnik digitalnih potrdil za uvoz potrdila v prostor za potrdila.
3. Uporabiti DCM za označitev potrdila kot overjenega.

Če uporablja strežnik LDAP zasebno izdano potrdilo strežnika, vam lahko skrbnik strežnika priskrbi kopijo datoteke z zahtevami za potrdila strežnika. Datoteko z zahtevami za potrdila uvozite v prostor za potrdila in jo označite kot overjeno.

Če uporabljate za dostop do strežnikov LDAP pomožne programe lupine, ki uporabljajo overjanje odjemalca in strežnika, morate narediti naslednje:

- V prostoru sistemskih potrdil morate definirati eno ali več overjenih potrdil. S tem je odjemalcu zagotovljeno, da je ciljnemu strežniku LDAP potrdilo izdala ena od overjenih služb za pooblastila (CA). Dodatno se zašifrirajo vse transakcije LDAP, ki tečejo prek povezave SSL s strežnikom. To vključuje poverilnice LDAP, ki jih podate v vmesnikih uporabniških programov, ki jih uporabljate za povezovanje z imeniškim strežnikom.
- Izdelati par ključev in od CA zahtevati potrdilo odjemalca. Po sprejemu podpisanega potrdila od CA, sprejmite potrdilo v datoteko obroča ključev na odjemalcu.

Poglavje 7. Odpravljanje težav v Imeniških storitvah

Na žalost imajo tudi zelo zanesljivi strežniki, kot je strežnik LDAP Imeniških storitev AS/400, včasih težave. Če ima imeniški strežnik LDAP težave, si lahko z naslednjimi informacijami pomagate pri odkrivanju in odpravljanju težav.

- “Osnovni postopki pri odpravljanju težav za Imeniške storitve”
- “Splošne napake odjemalca LDAP” na strani 61

Če želite dodatne informacije o splošnih težavah v Imeniških storitvah, preglejte domačo stran Imeniških storitev na naslednjem URL:

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

Osnovni postopki pri odpravljanju težav za Imeniške storitve

Povratne kode za napake LDAP lahko poiščete v datoteki ldap.h, ki je v sistemu v imeniku QSYSINC/H.LDAP.

Če pride v imeniškem strežniku LDAP do napake in želite zvedeti podrobnosti, preglejte dnevnik opravil QDIRSRV. Za reproduciranje napak lahko uporabite ukaz za sledenje aplikacije TCP/IP (TRCTCPAPP APP(*DIRSRV)), s katerim zaženete sledenje napak. Za dodatne informacije glejte “Uporaba TRCTCPAPP za pomoč pri iskanju težav” na strani 60.

Imeniške storitve uporabljajo strežnike SQL (Structured Query Language). Če pride do napake SQL, bo dnevnik opravil QDIRSRV običajno vseboval naslednje sporočilo:

```
Prišlo je do napake SQL -1
```

V teh primerih vas dnevnik opravil QDIRSRV napoti na dnevnike opravil strežnika SQL. V nekaterih primerih QDIRSRV morda ne bo vseboval tega sporočila in referenčnega kazalca, čeprav je strežnik SQL vzrok težave. V teh primerih je dobro vedeti, katere strežnike morate zagnati, in zakaj jih Imeniške storitve uporabljajo.

Če se imeniški strežnik LDAP zažene normalno, generira sporočila, ki so podobna naslednjim:

Opomba: Sporočila in število začetih opravil strežnika SQL se lahko razlikuje v naslednjih primerih:

- Če strežnik poženete prvič.
- Če morate opraviti selitev.
- Strežnik uporablja dnevnik sprememb.
- Strežnik je nastavljen tako, da omogoča višje število povezav z bazami podatkov.

```
                                                    Sistem:   WARMERS
 Opr.:QDIRSRV  Upor.:QDIRSRV   Številka . . :174440

  >> CALL PGM(QSYS/QGLDSVR)
     Opr 057448/QUSER/QSQSRVR upor. za obd. načina strežnika SQL.
     Opr 057340/QUSER/QSQSRVR upor. za obd. načina strežnika SQL.
     Opr 057448/QUSER/QSQSRVR upor. za obd. načina strežnika SQL.
     Opr 057166/QUSER/QSQSRVR upor. za obd. načina strežnika SQL.
     Opr 057279/QUSER/QSQSRVR upor. za obd. načina strežnika SQL.
     Opr 057288/QUSER/QSQSRVR upor. za obd. načina strežnika SQL.
     Strežnik imeniških storitev se je zagnal uspešno.
```

Imeniške storitve uporabljajo prvi strežnik SQL, 057448/QUSER/QSQSRVR, med zagonom strežnika LDAP. Imeniške storitve lahko med zagonom strežnika LDAP po potrebi požene dodatne strežnike SQL, če strežnik zaganjate prvič, če morate izvesti selitev oziroma strežnik uporablja dnevnik sprememb. Po zagonu se ti strežniki SQL sprostijo.

V tem zgledu niso uporabljeni nobeni dodatni strežniki za selitev ali zagon strežnika ter dnevnik sprememb ni konfiguriran. Imeniške storitve uporabljajo za kopiranje naslednji strežnik SQL (057340/QUSER/QSQSRVR).

Zadnja povezava v tem zgledu (057288/QUSER/QSQSRVR) je uporabljena za operacije dodajanja, spreminjanja, modrdn in brisanja. Ostale povezave so uporabljene za iskanje, povezovanje in primerjavo.

Na strani Lastnosti **Baze podatkov**/**pripon** imeniškega strežnika v Navigatorju iSeries podate skupno število strežnikov, ki jih Imeniške storitve uporabljajo za operacije imenikov po zagonu strežnika. Poleg tega je en strežnik SQL vedno konfiguriran za kopiranje.

Nadzorovanje napak in dostop do dnevnika opravil Imeniških storitev

S pregledovanjem dnevnika opravil za strežnik LDAP lahko vidite napake in nadzorujete dostop do strežnika.

Če se strežnik izvaja, pregledate dnevnik opravil QDIRSRV na naslednji način:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP**/**IP**.
4. Z desnim gumbom miške kliknite **Imenik** in izberite **Opravila strežnika**.
5. Z menija **Datoteka** izberite možnost **Dnevnik opravil**.

Če se strežnik ne izvaja (je zaustavljen), pregledate dnevnik opravil QDIRSRV na naslednji način:
1. V Navigatorju iSeries razširite **Osnovne operacije**.
2. Kliknite **Izhodni podatki tiskalnika**.
3. QDIRSRV se pojavi v stolcu **Uporabnik** v desnem podoknu Navigatorja iSeries. Če želite pregledati dnevnik opravil, dvokliknite **Qpjoblog**, levo od QDIRSRV v isti vrstici.

   Opomba: Navigator iSeries je lahko konfiguriran tako, da prikaže samo vmesne datoteke. Če se QDIRSRV na seznamu ne prikaže, kliknite **Izhodni podatki tiskalnika** in nato z menija **Možnosti** izberite **Vključi**. V polju **Uporabnik** podajte **Vsi** in nato kliknite **Potrdi**.

Opomba: Imeniške storitve uporabljajo za izvajanje nekaterih nalog druga sistemska sredstva. Če pride do napake v enem od teh sredstev, bo dnevnik opravil nakazal, kje najdete podrobnejše informacije. V nekaterih primerih Imeniške storitve morda ne bodo mogle določiti mesta podrobnejših informacij. V teh primerih poglejte v dnevnik opravil strežnikov SQL (Structured Query Language) (SQL), kjer boste videli, ali se težava nanaša na strežnike SQL.

Uporaba TRCTCPAPP za pomoč pri iskanju težav

Strežnik nudi sledenje komunikacij, s katerim lahko zberete podatke na komunikcijski liniji, kot je vmesnik lokalnega omrežja (LAN) ali prostranega omrežja (WAN) Povprečni uporabnik morda ne bo razumel celotne vsebine podatkov o sledenju, vendar lahko postavke sledenja uporabite za določitev, ali se je dejansko izvedla izmenjava podatkov med dvema točkama.

Ukaz za sledenje aplikacije TCP/IP (TRCTCPAPP) lahko uporabite z možnostjo *DIRSRV na imeniškem strežniku kot pomoč pri iskanju težav z odjemalci ali aplikacijami.

Če želite podrobnejše informacije o uporabi ukaza TRCTCPAPP z LDAP, kot tudi kot omejitve na zahtevanih pooblastilih, preglejte Opis ukaza TRCTCPAPP (Sledenje aplikacije TCP/IP).

Če želite splošne informacije o uporabi sledenja komunikacij, preglejte Sledenje komunikacij.

Uporaba možnosti LDAP_OPT_DEBUG za sledenje napak

| Začenši v V5R2 lahko uporabite možnost LDAP_OPT_DEBUG API-ja **ldap_set_option()** za sledenje težav
| z odjemalci, ki uporabljajo API-je C LDAP. Možnost razhroščevanja ima več nastavitev ravni razhroščevanja,
| ki so vam lahko v pomoč pri odpravljanju težav s temi aplikacijami.

| Primer omogočanja možnosti razgroščevanja sledenja odjemalca:

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

| Drugi način nastavitve ravni razhroščevanja je, da konfigurirate številčno vrednost spremenljivke okolja
| LDAP_DEBUG za opravilo, v katerem se izvaja odjemalska aplikacija, v isto številčno vrednost, kot bi bila
| debugvalue , če je uporabljen API **ldap_set_option()** .

| Zgled omogočanja sledenja odjemalca z uporabo spremenljivke okolja LDAP_DEBUG:

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

| Po zagonu odjemalca, ki ustvarja težavo, vnesite naslednje v poziv iSeries:

```
| DMPUSRTRC    ClientJobNumber
```

| kjer ClientJobNumber podaja številko opravila odjemalca.

| Če želite te informacije prikazati interaktivno, vnesite naslednje v poziv iSeries:

```
| DSPPFM  QAPOZDMP  QPOZnnnnnn
```

| kjer nnnnnn podaja številko opravila.

| Če želite te informacije shraniti, da bi jih poslali servisu, naredite naslednje:
| 1. Izdelajte datoteko SAVF z uporabo ukaza za izdelavo SAVF (CRTSAVF).
| 2. V ukazni poziv na iSeries vnesite naslednje:

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

| kjer *xxx* podaja ime, ki ste ga podali za datoteko SAVF.

Splošne napake odjemalca LDAP

Poznavanje vzrokov splošnih napak odjemalca LDAP vam lahko pomaga pri reševanju težav s strežnikom. Če želite prikazati celoten seznam stanj napak odjemalca LDAP, preglejte temo Imeniške storitve OS/400 v Programiranje v Informacijskem centru.

Sporočila o napakah odjemalca imajo naslednji format:

```
[Neuspela operacija LDAP]:[stanje napake API odjemalca LDAP]
```

Opomba: Razlaga teh napak predpostavlja, da odjemalec komunicira s strežnikom LDAP v OS/400. Odjemalec, ki komunicira s strežnikom na drugi platformi, lahko dobi podobna sporočila, vzroki in rešitve pa so lahko drugačni.

Splošna sporočila vključujejo naslednje:

- “ldap_search: Presežena je časovna omejitev” na strani 62
- “[Neuspela operacija LDAP]: Napaka v operaciji” na strani 62

- “ldap_bind: Takega objekta ni”
- “ldap_bind: Neustrezno overjanje”
- “[Napačna operacija LDAP]: Nezadosten dostop”
- “[Neuspela operacija LDAP]: Ne morem komunicirati s strežnikom LDAP”
- “[Neuspela operacija LDAP]: Nisem se uspel povezati s strežnikom ssl” na strani 63

ldap_search: Presežena je časovna omejitev

Do te napake pride, če se iskanja ldap izvajajo počasi. To napako popravite tako, da storite eno ali oboje:

- Povečate časovno omejitev za iskanje v imeniškem strežniku LDAP. Podrobnejše informacije o tem najdete v razdelku “Nastavljanje zmogljivosti imeniškega strežnika LDAP” na strani 30.
- Zmanjšajte delovanje vašega sistema. Zmanjšate lahko tudi število aktivnih opravil odjemalcev LDAP, ki se izvajajo.

[Neuspela operacija LDAP]: Napaka v operaciji

To napako lahko povzroči več stvari. Če želite v posameznem primeru dobiti informacije o vzroku te napake, preglejte dnevnike opravil strežnika QDIRSRV in SQL (Structured Query Language), kot je opisano v razdelku “Osnovni postopki pri odpravljanju težav za Imeniške storitve” na strani 59.

ldap_bind: Takega objekta ni

Običajen vzrok za to napako je napaka pri tipkanju med izvajanjem operacije. Drug splošen vzrok je v tem, da se odjemalec LDAP poskuša povezati z DN, ki ne obstaja. To se pogosto zgodi, ko uporabnik poda nekaj, za kar napačno misli, da je DN skrbnika. Na primer, uporabnik lahko poda QSECOFR ali Administrator, medtem ko je dejanski DN skrbnika podoben cn=Administrator.

Za podrobnosti o napaki preglejte dnevnik opravila QDIRSRV kot to opisuje “Osnovni postopki pri odpravljanju težav za Imeniške storitve” na strani 59.

ldap_bind: Neustrezno overjanje

Strežnik vrne neveljavna priporočila, če geslo ali povezovalni DN nista veljavna. Strežnik vrne neustrezno overjanje, če se odjemalec poskuša povezati kot eno od naslednjega:

- Postavka, ki nima lastnosti uporabniškega gesla
- Postavka, ki predstavlja uporabnika OS/400, ki ima lastnost UID in ne lastnosti uporabniškega gesla. To povzroči, da se izvede primerjava med podanim geslom in geslom uporabnika OS/400, ki se je ujemata.
- Postavka, ki predstavlja projektiranega uporabnika, zahtevana pa je bila povezovalna metoda, ki ni preprosta.

Do te napake običajno pride, ko se odjemalec poskuša povezati z geslom, ki ni veljavno. Če potrebujete podrobnosti o napaki, preglejte dnevnik opravila QDIRSRV kot to opisuje “Osnovni postopki pri odpravljanju težav za Imeniške storitve” na strani 59.

[Napačna operacija LDAP]: Nezadosten dostop

Do te napake običajno pride, če povezovalni DN nima pooblastila za izvajanje operacije (kot je dodajanje ali brisanje), ki jo zahteva odjemalec. Za podrobnejše informacije o tej napaki preglejte dnevnik opravil QDIRSRV, kot je opisano v razdelku “Osnovni postopki pri odpravljanju težav za Imeniške storitve” na strani 59.

[Neuspela operacija LDAP]: Ne morem komunicirati s strežnikom LDAP

Najpogostejši vzroki te napake so naslednji:

- Odjemalec LDAP izda zahtevo, še preden strežnik LDAP v podanem sistemu začne delovati in je v stanju izbirnega čakanja.

- Uporabnik poda številko vrat, ki ni veljavna. Strežnik na primer posluša na vratih 386, zahteva odjemalca pa poskuša uporabiti vrata 387.

Za podrobnejše informacije o tej napaki preglejte dnevnik opravil QDIRSRV, kot je opisano v razdelku “Osnovni postopki pri odpravljanju težav za Imeniške storitve” na strani 59. Če je bil strežnik imeniških storitev zagnan uspešno, boste v dnevniku opravil QDIRSRV zasledili sporočilo Strežnik imeniških storitev se je zagnal uspešno.

[Neuspela operacija LDAP]: Nisem se uspel povezati s strežnikom ssl

Do te napake pride takrat, ko strežnik LDAP zavrne povezavo odjemalca, ker povezave z zaščitenimi vtičnicami ni mogoče vzpostaviti. Lahko je posledica naslednjega:

- Podpora za upravljanje potrdil je zavrnila poskus odjemalca, da bi vzpostavil povezavo s strežnikom. S pomočjo Upravljalnika digitalnih potrdil zagotovite, da so vaša potrdila pravilno nastavljena, nato strežnik znova zaženite in poskusite vzpostaviti povezavo.
- Uporabnik morda nima bralnega dostopa do prostora za potrdila *SYSTEM (po privzetku /QIBM/userdata/ICSS/Cert/Server/default.kdb).

V aplikacijah C OS/400 so na voljo tudi dodatne informacije o napaki SSL. Za podrobnosti preglejte dokumentacijo posameznih API-jev Imeniške storitve.

Natisnjeno na Danskem