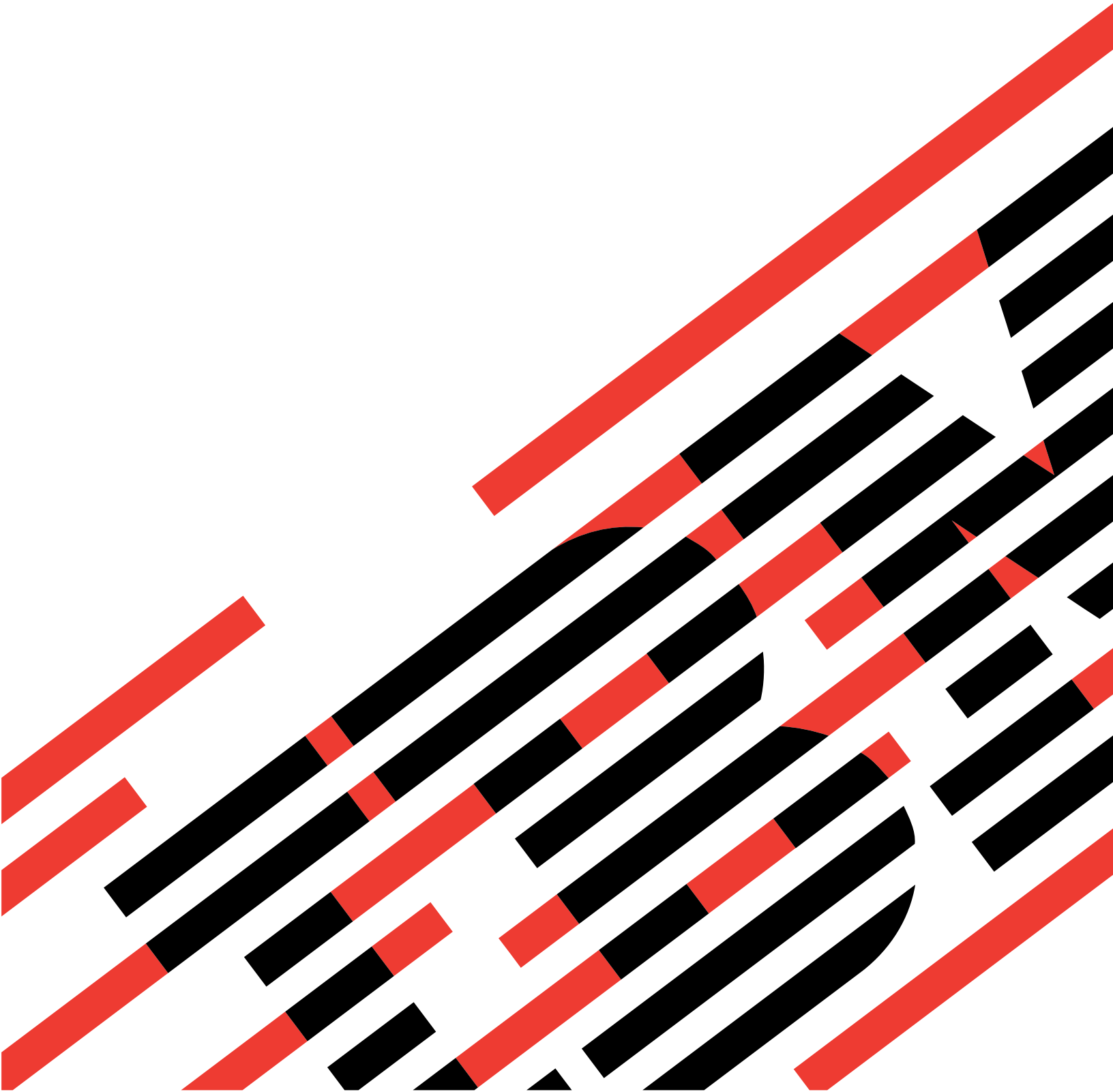
IBM

eserver

iSeries

IBM Poslužitelj direktorija (LDAP)

Verzija 5 Izdanje 3



IBM

@server

iSeries

IBM Poslužitelj direktorija (LDAP)

Verzija 5 Izdanje 3

Napomena

Prije korištenja ovih informacija i proizvoda koji podržavaju, pročitajte informacije u “Napomene”, na stranici 221.

Sedmo izdanje (kolovoz, 2005)

Ovo izdanje se odnosi na verziju 5, izdanje 3, modifikaciju 0 za IBM Operating System/400 (broj proizvoda 5722–SS1) i na sva naredna izdanja i modifikacije, sve dok se drukčije ne označi u novim izdanjima. Ova verzija ne radi na svim računalima sa smanjenim skupom instrukcija (RISC) niti na CISC modelima.

Sadržaj

Poglavlje 1. IBM Poslužitelj direktorija za iSeries (LDAP)

IBM Poslužitelj direktorija za iSeries (u daljnjem tekstu se naziva Poslužitelj direktorija) sadrži Lightweight Directory Access Protocol (LDAP) poslužitelj na iSeries poslužitelju. LDAP se izvodi preko Transmission Control Protocol/Internet Protocol (TCP/IP) i popularan je kao usluga direktorija i za Internet i ne-Internet aplikacije.

Sljedeća poglavlja sadrže informacije koje će vam pomoći da razumijete i koristite Poslužitelj direktorija na vašem iSeries poslužitelju:

Poglavlje 2. Što je novo za V5R3

Poslužitelj direktorija za iSeries (ranije poznat kao IBM Poslužitelj direktorija za iSeries) ima sljedeća poboljšanja i nova svojstva za V5R3:

- **Administracija i pristupanje korisnika:** Novi IBM Alat Web administracije poslužitelja direktorija zamjenjuje IBM Alat upravljanja direktorijom. Alat Web administracije sadrži funkcionalnost za upravljanje unosima korisnika, obradu poslužitelja direktorija i stabla direktorija iz jednog od uobičajenih Web sučelja. LDAP protokol se sada koristi za ispitivanje i ažuriranje opcija konfiguracije Poslužitelj direktorija.
- **Dinamičke grupe:** Dinamičke grupe omogućuju da se kreira ona grupa gdje su članovi unosi koji se podudaraju s filterom pretraživanja.
- **Ugniježđene grupe:** Ugniježđene grupe omogućuju da se kreira grupa čiji članovi uključuju sve članove drugih grupa.
- **Politika lozinke:** Poslužitelj direktorija sada podržava politiku lozinke koja uključuje pravila sintakse lozinke, povijest lozinke i onesposobljavanje unosa nakon previše pokušaja korištenja pogrešne lozinke.
- **Kontrole pristupa zasnovane na filteru:** Ovlaštenje za unose se sada može specificirati korištenjem kontrole pristupa zasnovane na filteru. Na primjer, možete specificiratri dozvole za unose s departmentNumber=abc ili dodijeliti pristup određenim tipovima unosa.
- **Replikacija:** Poboljšanja replikacije uključuju sposobnost postojanja više glavnih poslužitelja (ravnopravni poslužitelji), replikaciju podstabla, poboljšano raspoređivanje i kontroliranje replikacije, napredno nadgledanje i robusnije funkcije replikacije.
- **Sortirano pretraživanje:** Kontrola sortiranog pretraživanja omogućava klijentu da primi rezultate pretraživanja koji su sortirani na temelju liste kriterija gdje svaki kriterij predstavlja ključ sortiranja. Time se premješta odgovornost za sortiranje iz aplikacije klijenta na poslužitelja gdje će se to možda napraviti djelotvornije. Naredba ldapsearch je poboljšana s novim parametrima kako bi se omogućilo sortiranje rezultata pretraživanja. Postoje i novi LDAP API-ji za sortiranje rezultata pretraživanja.
- **Pretraživanje sa stranicom:** Kontrola stranice rezultata vam omogućuje da upravljate s količinom podataka koju vraća zahtjev pretraživanja. Možete zahtijevati podskup unosa (stranica) umjesto da odjednom primite sve rezultate. Naredni zahtjev za pretraživanjem prikazuje sljedeću stranicu rezultata tako dugo dok se operacija ne opozove ili dok se ne vrati posljednji rezultat. Naredba ldapsearch je bila poboljšana s novim parametrima kako bi se omogućilo da se rezultati pretraživanja stave na stranicu. Postoje i novi LDAP API-ji za stavljanje rezultata pretraživanja na stranicu.
- **Pomoćni programi reda za naredbe:** Novi su sljedeći pomoćni programi reda za naredbe:
  - ldapexop - osigurava sposobnost vezanja direktorija i izdaje jednu proširenu operaciju zajedno s bilo kojim podacima koji čine proširenu vrijednost operacije.
  - ldapdiff - usklađuje poslužitelj replike s njegovim glavnim poslužiteljem.
  - ldapchangepwd - šalje preinačene zahtjeve lozinke na LDAP poslužitelj.
- **Performanse:** Performanse su poboljšane za sve operacije. Osim toga, sve operacije sada može istovremeno izvoditi više klijenata.
- **Posebni znakovi u razlikovnim imenima (DN):** DN sada može sadržavati sljedeće posebne znakove: zarez, jednako, plus, manje od, veće od, znak za funtu, točka zarez i navodnici.
- **Pravila uspoređivanja za atribute niza:** Ako je atribut definiran jednom od dvije sintakse niza, Nizom direktorija ili IA5 nizom, poslužitelj će sada poštovati ponašanje uspoređivanja specificirano u shemi za atribut, ispravljajući tako grešku u prethodnim izdanjima. Možete definirati atribut tako da bude ili ne bude osjetljiv na velika i mala slova kod uspoređivanja. Ranije je poslužitelj dozvoljavao da se specificira pravilo uspoređivanja, ali ga je zanemarivao. Interno je poslužitelj tretirao IA5 niz kao da je osjetljiv na velika i mala slova, a Niz direktorija kao da nije osjetljiv na velika i mala slova. Ako je vaš poslužitelj definirao atribute kao IA5 niz s caseIgnoreMatch ili Niz direktorija s caseExactMatch, poslužitelj će se sada ispravno ponašati za te atribute.

Poglavlje 3. Ispisivi PDF-ovi

Za pregled ili učitavanje PDF verzije ovog dokumenta, izaberite Poslužitelj direktorija (LDAP) (oko 2700 KB).

Ostale informacije

Za pregled ili ispis PDF-ova povezanih priručnika i Redbooks pogledajte Poglavlje 10, “Povezane informacije”, na stranici 219.

Spremanje PDF datoteka

Da spremite PDF datoteku na vašu radnu stanicu za gledanje ili ispis:

1. Desno kliknite na PDF u vašem pretražitelju (desno kliknite na gornju vezu).
2. Kliknite na opciju koja sprema PDF lokalno.
3. Izaberite direktorij u koji želite spremiti PDF datoteku.
4. Kliknite **Save**.

Spuštanje Adobe Readera

Trebate Adobe Reader na vašem sistemu za gledanje ili ispis ovih PDF-ova. Možete spustiti besplatnu kopiju s Adobe Web stranice (www.adobe.com/products/acrobat/readstep.html)  .

Poglavlje 4. Koncepti poslužitelja direktorija

Poslužitelj direktorija implementira specifikacije Internet Engineering Task Force (IETF) LDAP V3. On isto tako uključuje poboljšanja koje je dodao IBM u funkcionalna područja i područja izvedbe. Ova verzija koristi IBM DB2 kao pomoćno pohranjivanje radi osiguranja integriteta transakcija LDAP operacija, operacija najbolje izvedbe i mogućnosti on-line sigurnosnog kopiranja i vraćanja. Međudjeluje s klijentima zasnovanim na IETF LDAP V3. Za koncepte i razmatranja koji se odnose na Poslužitelj direktorija, pogledajte sljedeće:

Direktoriji

Poslužitelj direktorija dozvoljava pristup tipu baze podataka koja pohranjuje informacije u hijerarhijsku strukturu sličnu načinu na koji je organiziran i5/OS integrirani sistem datoteka.

Ako je poznato ime objekta, njegove karakteristike se mogu dohvatiti. Ako nije poznato ime određenog pojedinačnog objekta, direktorij se može pretražiti kako bi se pronašla lista objekata koji odgovaraju određenim zahtjevima. Direktorij se obično pretražuju pomoću određenog kriterija, a ne samo pomoću predefiniranog skupa kategorija.

Direktorij je specijalizirana baza podataka koja ima karakteristike koje je odvajaju od relacijskih baza podataka za općenite svrhe. Za direktorij je karakteristično da mu se pristupa (čita ili pretražuje) puno češće nego ga se ažurira (piše). Budući direktoriji moraju podržavati velike količine zahtjeva za čitanjem, oni se u pravilu optimaliziraju za pristup čitanja. Budući direktoriji ne trebaju osigurati onoliko funkcija koliko baze podataka za općenite svrhe, oni se mogu optimalizirati kako bi ekonomično osigurali više aplikacija s brzim pristupom podacima direktorija u velikim distribuiranim okolinama.

Direktorij se može centralizirati ili distribuirati. Ako je direktorij centraliziran, postoji jedan poslužitelj direktorija (ili klaster direktorija) na lokaciji koja osigurava pristup na direktorij. Ako je direktorij distribuiran, postoji više poslužitelja, u pravilu geografski raspršenih, koji osiguravaju pristup na direktorij.

Kada je direktorij distribuiran, informacije koje su pohranjene u direktoriju se mogu particionirati ili replicirati. Kada su informacije particionirane, svaki poslužitelj direktorija pohranjuje jedinstven podskup informacija koje se ne preklapaju. To znači da svakog direktorija pohranjuje jedan i samo jedan poslužitelj. Tehnika kojom se particionira direktorij koristi LDAP upućivanje. LDAP upućivanja dozvoljavaju korisnicima da nazivaju Lightweight Directory Access Protocol (LDAP) zahtjeve istim ili drugačijim prostorima imena pohranjenim u drugim (ili istim)

poslužiteljima. Kada se repliciraju informacije, isti unos direktorija se pohranjuje od strane više poslužitelja. U distribuiranom direktoriju, neke informacije se mogu particionirati, a neke se mogu replicirati.

Model LDAP poslužitelja direktorija se bazira na unosima (koji se isto nazivaju objektima). Svaki unos se sastoji od jednog ili više atributa, kao što je ime ili adresa i tip. Tipovi se u pravilu sastoje od mnemoničkih nizova kao što je cn za zajedničko ime ili mail za adresu e-pošte.

Primjer direktorija u Slika 1 na stranici 9 prikazuje unos za Tim Jones koji uključuje atribute mail i telephoneNumber. Neki od drugih mogućih atributa mogu biti fax, title, sn (za prezime) i jpegPhoto.

Svaki direktorij ima shemu koja predstavlja skup pravila koja određuju strukturu i sadržaje direktorija. Shemu možete pregledati korištenjem Web administracijskog alata. Za više informacija o shemi, pogledajte “Shema” na stranici 15.

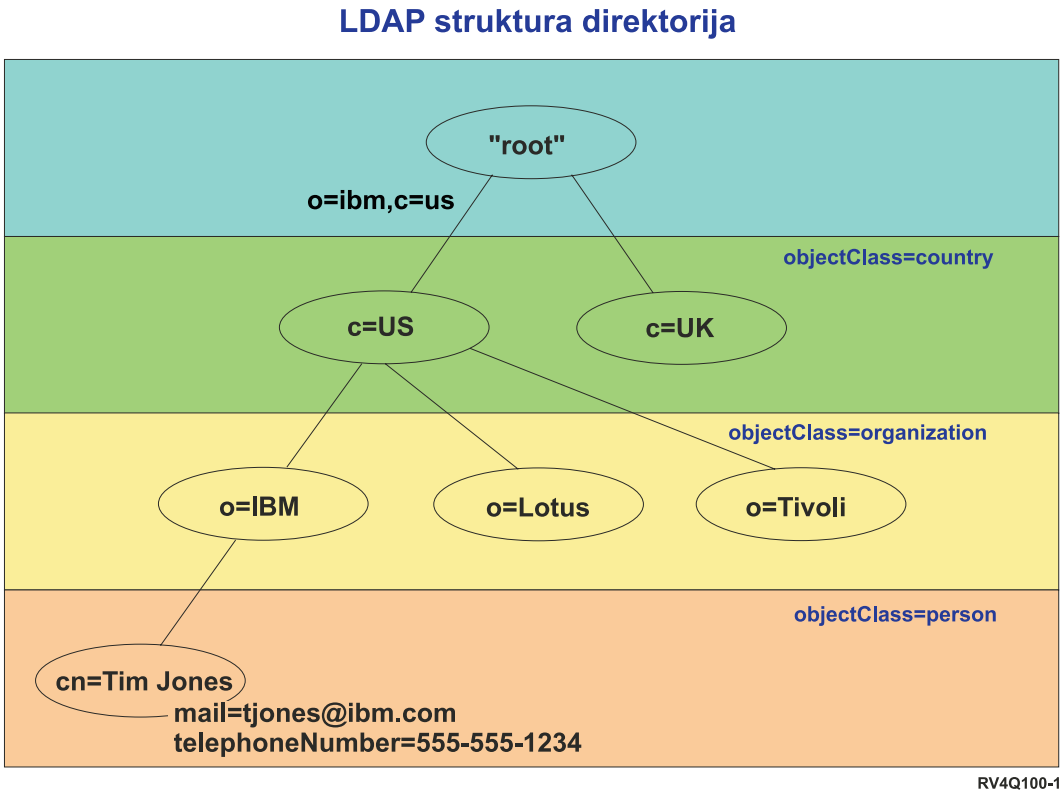
Svaki unos direktorija ima posebne atribute koji se nazivaju objectClass. Ovaj atribut kontrolira atribute koji su potrebni i dopušteni u nekom slogu. Drugim riječima, vrijednosti objectClass atributa određuju shematska pravila koje slog mora poštivati.

Osim atributa koje je definirala shema, unosi imaju i skup atributa koje održava poslužitelj. Ti atributi koji se nazivaju operativnim atributima, uključuju stvari kao što je vrijeme kada je unos bio kreiran i informacije kontrole pristupa. Za više informacija o operativnim atributima, pogledajte “Operativni atributi” na stranici 70.

Tradicionalno, slogovi u LDAP direktoriju su raspoređeni u hijerarhijskoj strukturi koja odražava političke, zemljopisne ili organizacijske granice (vidjeti Slika 1 na stranici 9). Na vrhu hijerarhije se nalaze unosi koji predstavljaju zemlje ili regije. Upisi koji predstavljaju države ili nacionalne udruge zauzimaju drugu razinu na dolje u hijerarhiji. Slogovi koji se potom nalaze ispod toga predstavljaju ljude, organizacijske jedinice, pisače, dokumente ili druge stvari.

LDAP se odnosi na unose s Razlikovnim imenima (DN-ovi). Ta prepoznatljiva razlikovna imena se sastoje od imena samog upisa kao i od imena, u poretku od dna prema vrhu, objekata iznad njega u direktoriju. Na primjer, potpuno DN za unos u donjem lijevom kutu od Slika 1 na stranici 9 je cn=Tim Jones, o=IBM, c=US. Svaki upis ima barem jedan atribut koji se koristi za imenovanje upisa. Taj atribut imenovanja se naziva Relativno razlikovno ime (RDN) unosa. Unos iznad zadanog RDN-a se naziva nadređenim Razlikovnim imenom. U gornjem primjeru, cn=Tim Jones imenuje unos tako da je to RDN. o=IBM, c=US je nadređeno DN za cn=Tim Jones. Za više informacija o DN-ovima, pogledajte “Razlikovna imena (DN-ovi)” na stranici 11.

Ako želite dati LDAP poslužitelju mogućnost održavanja i upravljanja dijelom LDAP direktorija, trebate navesti viša razlikovna imena najviše razine u konfiguraciji poslužitelja. Ta razlikovna imena se nazivaju sufiksima. Poslužitelj može pristupiti svim objektima u direktoriju koji se nalaze ispod navedenog sufiksa u hijerarhiji direktorija. Na primjer, ako LDAP poslužitelj sadrži direktorij koji je prikazan u Slika 1 na stranici 9, on treba imati sufiks o=ibm, c=us specificiran u svojoj konfiguraciji kako bi mogao odgovoriti na upite klijenta koji se odnose na Tim Jones.



Slika 1. Struktura LDAP direktorija

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

Recimo da želite kreirati direktorij korištenjem strukture komponente domene koja će sadržavati podatke o zaposlenicima kao što su imena, telefonski brojevi i adrese e-pošte. Koristite sufiks ili sadržaj imenovanja koji je zasnovan na TCP/IP domeni. Taj direktorij se može vizualizirati kao nešto što je slično sljedećem:

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

Kada se unesu u Poslužitelj direktorija ti bi podaci mogli stvarno izgledati kao nešto što je slično sljedećem:

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

# employees directory
dn: cn=employees,dc=ibm,dc=com
objectclass: top
```

```
objectclass: container
cn: employees

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

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

Primijetiti ćete da svaki unos sadrži vrijednosti atributa koje se nazivaju objectclass. Vrijednosti objectclass definiraju atribute koji su dozvoljeni u unosu, kao što je telephonenumber ili givenname. Dozvoljene klase objekata su definirane u shemi. Shema je skup pravila koja definiraju tip unosa koji je dozvoljen u bazi podataka.

Klijenti i poslužitelji direktorija

Direktorijima se obično pristupa korištenjem klijent-poslužitelj modela komunikacije. Obrade klijenta i poslužitelj mogu, ali ne moraju, biti na istom stroju. Poslužitelj može posluživati više klijenata. Aplikacija koja želi čitati ili pisati informacije u direktoriju ne pristupa izravno direktoriju. Umjesto toga, ona poziva funkciju ili sučelje programiranja aplikacije (API) koje uzrokuje slanje poruke na drugu obradu. Ta druga obrada pristupa informacijama u direktoriju u ime aplikacije koja je to zatražila. Rezultati pisanja ili čitanja se onda vraćaju na aplikaciju koja je to tražila.

API definira sučelje programiranja koje određeni programski jezik koristi za pristupanje usluzi. Format i sadržaj poruka koje su razmijenjene između klijenta i poslužitelja moraju odgovarati onom što je dogovoreno na protokolu. LDAP definira protokol poruke kojeg koriste klijenti direktorija i poslužitelji direktorija. Postoji i pridruženi LDAP API za C jezik i načini pristupa direktoriju iz Java aplikacije upotrebom Java imenovanja i Sučelja direktorija (JNDI).

Sigurnost direktorija

Direktorij bi trebao podržavati osnovne sposobnosti koje su potrebne kako bi se implementirala sigurnosna politika. Direktorij možda neće izravno osigurati potrebne sigurnosne sposobnosti, no one bi mogle biti integrirane u usluzi sigurnosti povjerljive mreže koja osigurava osnovne usluge sigurnosti. Prvo, potrebna je metoda kojom se provjerava autentičnost korisnika. Provjera autentičnosti provjerava da li su korisnici ono što tvrde da jesu. Ime korisnika i lozinka čine osnovu sheme za provjeru autentičnosti. Jednom kada se korisnicima provjeri autentičnost, mora se utvrditi da li oni imaju ovlaštenje ili dozvolu za izvođenje tražene operacije na određenom objektu.

Ovlaštenje se često puta bazira na listi kontrole pristupa (ACL-ovi). ACL je lista ovlaštenja koja se može pripojiti objektima i atributima u direktoriju. ACL ispisuje koji je tip pristupa dozvoljen ili nije dozvoljen za svakog korisnika ili grupu korisnika. Da se ACL-ovi naprave kraćim i lakšim za rukovanje, korisnici s istim pravima pristupa se često stavljaju u grupe.

Razlikovna imena (DN-ovi)

Svaki unos u direktorij ima razlikovno ime (DN). DN je ime koje jednoznačno identificira unos u direktorij. DN se sastoji od attribute=value parova koji su odvojeni zarezima, na primjer:

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

Bilo koji od atributa koji je definiran u shemi direktorija se može koristiti kako bi se sastavilo DN. Važan je poredak parova vrijednosti atributa komponente. DN sadrži jednu komponentu za svaku razinu hijerarhije direktorija od ishodišta pa do razine na kojoj prebivaju unosi. LDAP DN-ovi počinju s najspecifičnijim atributom (u pravilu neko ime) i nastavljaju se s progresivno širim atributima, često puta završavajući s atributom zemlje. Prva komponenta DN-a se naziva Relativno razlikovno ime (RDN). Ono identificira unos tako da se razlikuje od svih dugih unosa s istim nadređenim. U gornjim primjerima, RDN ″cn=Ben Gray″ odjeljuje prvi unos od drugog unosa, (s RDN ″cn=Lucille White″). Ta dva primjera DN-ova su inače ekvivalentna. Par atribut=vrijednost koji čini RDN za unos mora isto biti prisutan u unosu. (To nije istinito kod drugih komponenata DN-a.)

Slijedite sljedeći primjer kako bi kreirali unos za osobu:

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

Pravila DN izbjegavanja

Neki znakovi imaju posebna značenja u DN. Na primjer, = (jednako) odjeljuje ime i vrijednost atributa, a , (zarez) odvaja parove atribut=vrijednost. Posebni znakovi su **,** (zarez), **=** (jednako), **+** (plus), **<** (manje od), **>** (veće od), # (znak za broj), **;** (točka zarez), \ (obrnuta kosa crta) i **"** (navodnici, ASCII 34).

Posebni znak se može izbjeći u vrijednosti atributa kako bi se uklonilo posebno značenje. Kako bi izbjegle te posebne znakove ili druge znakove u vrijednosti atributa u DN nizu, koristite sljedeće metode:

1. Ako je znak koji se izbjegava jedan od posebnih znakova, neka se ispred njega nalazi obrnuta kosa crta (’\’ ASCII 92). Ovaj primjer prikazuje metodu izbjegavanja zareza u imenu organizacije:

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

   To je preferirana metoda.
2. U suprotnom, zamijenite znak koji se izbjegava obrnutom kosom crtom i s dvije hex znamenke koje čine jedan bajt u znakovnom kodu. Znakovni kod **mora** biti u UTF-8 skupu znakova.

   ```
   CN=L. Eagle,O=Sue\2C Grabbit and Runn,C=GB
   ```
3. Okružite cijelu vrijednost atributa sa **""** (navodnicima) (ASCII 34) koji nisu dio vrijednosti. Između para znakova navodnika se svi znakovi uzimaju takvim kakvi jesu, osim kod \ (obrnuta kosa crta). \ (obrnuta kosa crta) se može koristiti kako bi se izbjegla obrnuta kosa crta (ASCII 92) ili navodnici (ASCII 34), bilo koji od ranije spomenutih posebnih znakova ili hex parovi kao u metodi 2. Na primjer, kako bi izbjegli navodnike u cn=xyz"qrs"abc, ono postaje cn=xyz\"qrs\"abc ili kako bi izbjegli \:

   ```
   "trebate izbjeći jednu obrnutu kosu crtu na ovaj način \\"
   ```

   Drugi primjer, "\Zoo" nije ispravno jer se ’Z’ ne može izbjeći u tom kontekstu.

Pseudo DN-ovi

Pseudo DN-ovi se koriste kod definicije i procjene kontrole pristupa. LDAP direktorij podržava nekoliko pseudo DN-ova (na primjer, ″group:CN=THIS″ i ″access-id:CN=ANYBODY″), koji se koriste kako bi se označio prevelik broj DN-ova koji dijele zajedničke karakteristike, u odnosu na operaciju koja se izvodi ili na objekt u kojem se izvodi operacija. Za više informacija o kontroli pristupa, pogledajte “Poslužitelj direktorija - Sigurnost” na stranici 40.

Poslužitelj direktorija podržava tri pseudo DN-ova:

- access-id: CN=THIS

  Kada je specificirano kao dio ACL-a, to DN se odnosi na bindDN koji odgovara DN-u na kojem se izvodi operacija. Na primjer, ako se operacija izvodi na objektu ″cn=personA, ou=IBM, c=US″, a bindDn je ″cn=personA, ou=IBM, c=US″, dodijeljene dozvole su kombinacija onih danih za ″CN=THIS″ i onih danih za ″cn=personA, ou=IBM, c=US″.
- group: CN=ANYBODY

  Kada je specificirano kao dio ACL-a, to DN se odnosi na sve korisnike, čak i one koji nisu ovlašteni. Korisnici se ne mogu ukloniti iz te grupe, a ta grupa se ne može ukloniti iz baze podataka.
- group: CN=AUTHENTICATED

  Taj DN se odnosi na bilo koje DN koje je bilo ovlašteno od strane direktorija. Ne razmatra se metoda provjere autentičnosti.

  Bilješka: ″CN=AUTHENTICATED″ se odnosi na DN koji je bio ovlašten bilo gdje na poslužitelju, bez obzira na to gdje je smješten objekt koji predstavlja DN. No, treba ga koristiti s oprezom. Na primjer, pod jednim sufiksom ″cn=Secret″ može biti čvor koji se naziva ″cn=Confidential Material″ koji ima unos ″group:CN=AUTHENTICATED:normal:rsc″. Pod drugim sufiksom ″cn=Common″ može biti čvor ″cn=Public Material″. Ako ta dva stabla prebivaju na istom poslužitelju, vezivanje na ″cn=Public Material″ će se smatrati ovlaštenim i imat će dozvolu za normalnu klasu na objektu ″cn= Confidential Material″.

Neki primjeri pseudo DN-ova:

Primjer 1

Uzmite u obzir sljedeći ACL za objekta: cn=personA, c=US

```
AclEntry: access-id: CN=THIS:critical:rwsc
AclEntry: group: CN=ANYBODY: normal:rsc
AclEntry: group: CN=AUTHENTICATED: sensitive:rcs
```

Korisnik koji se povezuje kao	Bi primio
cn=personA, c=US	normal:rsc:sensitive:rcs:critical:rwsc
cn=personB, c=US	normal:rsc:sensitive:rsc
Anonimno	normal:rsc

U ovom primjeru, personA dobiva dozvolu koja je dodijeljena ″CN=THIS″ ID-u i dozvole koje su dane ″CN=ANYBODY″ i ″CN=AUTHENTICATED″ pseudo DN grupama.

Primjer 2

Uzmite u obzir sljedeći ACL za objekt: cn=personA, c=US AclEntry: access-id:cn=personA, c=US: object:ad

```
AclEntry: access-id: CN=THIS:critical:rwsc
AclEntry: group: CN=ANYBODY: normal:rsc
AclEntry: group: CN=AUTHENTICATED: sensitive:rcs
```

Za operacije koje se izvode ne cn=personA, c=US:

Korisnik koji se povezuje kao	Bi primio
cn=personA, c=US	object:ad:critical:rwsc
cn=personB, c=US	normal:rsc:sensitive:rsc
Anonimno	normal:rsc

U ovom primjeru, personA dobiva dozvole koje su dodijeljene ″CN=THIS″ ID-u i one koje su dodijeljene samom DN-u ″cn=personA, c=US″. Primijetite da dozvole grupe nisu dane jer postoji određeniji aclentry (″access-id:cn=personA, c=US″) za vezivanje DN-a (″cn=personA, c=US″).

Poboljšano DN obrađivanje

RDN sastavljen od DN-ova se može sastojati od više komponenata koje su povezene '+' operatorima. Poslužitelj poboljšava podršku za pretraživanje na unosima koji imaju takav DN. Sastavljen RDN se može specificirati u bilo kojem poretku kao baza za operaciju pretraživanja.

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

Poslužitelj podržava proširene operacije DN normalizacije. Proširene operacije DN normalizacije normaliziraju DN-ove korištenjem sheme poslužitelja. Ta proširena operacija može biti korisna za aplikacije koje koriste DN-ove. Za više informacija o proširenim operacijama, pogledajte "Kontrole i proširene operacije" na stranici 71.

Sintaksa razlikovnog imena

Službena sintaksa za Razlikovno ime (DN) je zasnovana na RFC 2253. Sintaksa Backus Naur Form (BNF) je definirana kako slijedi:

```
<ime> ::= <komponenta-imena> ( <odjelitelj-s-razmakom> )
          | <komponenta-imena> <odjelitelj-s-razmakom> <ime>

   <odjelitelj-s-razmakom> ::= <neobavezan-razmak>
                  <odjelitelj>
                  <neobavezan-prostor>

   <odjelitelj> ::=  "," | ";"

   <neobavezan-prostor> ::= ( <CR> ) *( " " )

   <komponenta-imena> ::= <atribut>
           | <atribut> <neobavezan-prostor> "+"
             <neobavezan-prostor> <komponenta-imena>

   <atribut> ::= <niz>
           | <tipka> <neobavezan-prostor> "=" <neobevezan-prostor> <niz>

   <tipka> ::= 1*( <znak> ) | "OID." <oid> | "oid." <oid>
   <znak> ::= slova, brojevi i razmak

   <oid> ::= <niz-znamenaka> | <niz-znamenaka> "." <oid>
   <niz-znamenaka> ::= 1*<znamenka>
   <znamenka> ::= znamenke 0-9

   <niz> ::= *( <znak-niza> | <par> )
             | '"' *( <znak-niza> | <posebno> | <par> ) '"'
             | "#" <hex>


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

   <par> ::= "\" ( <posebno> | "\" | '"')
   <znak-niza> ::= bilo koji znak osim <posebno> ili "\" ili '"'


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

Znak točka zarez (;) se može koristiti kako bi se odvojili RDN-ovi u razlikovnom imenu, iako je znak za zarez (,) tipičan znak iz sistema znakova.

Znakovi prazno mjesto (razmaci) se mnogu nalaziti s bilo koje strane zareza ili točke zareza. Znakovi za prazno mjesto se zanemaruju i točka zarez se zamjenjuje sa zarezom.

Osim toga, znakovi za razmak (' ' ASCII 32) mogu biti ispred ili iza '+' ili '='. Ti znakovi za razmak se zanemaruju kod raščlambe.

Sljedeći primjer prikazuje razlikovno ime koje je zapisano korištenjem sistema znakova koji je oblikovan tako da bude prikladan za uobičajene obrasce imena. Prvo je ime koje sadržava tri komponente. Prva od komponenata je složeno RDN. Složeno RDN sadrži više od jednog para atribut:vrijednost i može se koristiti kako bi se zasebno identificirao određeni unos u slučaju kada bi jednostavna CN vrijednost mogla biti dvosmislena:

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

Sufiks (kontekst imenovanja)

Sufiks (poznat i kao kontekst imenovanja) je DN koji identificira najviši unos u lokalno zadržanoj hijerarhiji direktorija. Budući se u LDAP-u koristi relativna shema imenovanja, taj DN je isto tako sufiks bilo kojeg drugog unosa unutar hijerarhije tog direktorija. Poslužitelj direktorija može imati više sufiksa, a svaki od njih identificira lokalno zadržanu hijerarhiju direktorija, na primjer o=ibm,c=us.

Direktoriju mora biti dodan specifičan unos koji se podudara sa sufiksom. Unos kojeg kreirate mora koristiti klasu objekta koja sadrži korišteni atribut imenovanja. Možete koristiti alat Web administracije ili pomoćni program Qshell ldapadd kako bi kreirali odgovarajući unos za taj sufiks. Za više informacija, pogledajte "Upravljanje unosima direktorija" na stranici 129 ili "ldapmodify i ldapadd" na stranici 157.

Konceptualno, postoji prostor globalnog LDAP imena. U prostoru globalnog LDAP imena ćete možda vidjeti DN-ove poput:

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

Sufiks ″o=IBM″ kaže poslužitelju da je samo prvi DN u imenu prostora kojeg sadržava poslužitelj. Pokušaji referenciranja objekata koji nisu unutar jednog od sufiksa rezultiraju greškom ″nema takvih objekata″ ili upućivanjem na drugi poslužitelj direktorija.

Poslužitelj može imati više sufiksa. Poslužitelj direktorija ima nekoliko predefiniranih sufiksa koji sadrže podatke koji su specifični za našu implementaciju:

- cn=schema sadrži LDAP dohvatljiv prikaz sheme
- cn=changelog sadrži dnevnik promjene poslužitelja, ako je omogućen
- cn=localhost sadrži ne-replicirane informacije koje kontroliraju neke aspekte operacije poslužitelja, na primjer, objekti konfiguracije replikacije
- cn=pwdpolicy sadrži poslužitelj-široku politiku lozinke
- ″os400-sys=system-name.mydomain.com″ sufiks omogućuje LDAP dohvatljiv za i5/OS objekte, trenutno ograničen na profile korisnika i grupe

Poslužitelj direktorija dolazi već konfiguriran s default sufiksom, dc=system-name,dc=domain-name, kako bi se olakšalo pokretanje s poslužiteljem. Vi ne morate koristiti taj sufiks. Možete dodati vlastite sufikse i obrisati ranije konfigurirane sufikse.

Postoje dvije obično korištene konvencije imenovanja za sufikse. Jedna se zasniva na TCP/IP domeni za vašu organizaciju. Druga se zasniva na imenu i lokaciji organizacije.

Na primjer, za danu TCP/IP domenu mycompany.com, možete izabrati sufiks kao što je dc=mycompany,dc=com, gdje se dc atribut odnosi na komponentu domene. U tom bi slučaju unos najviše razine kojeg kreirate u direktoriju mogao izgledati ovako (korištenjem LDIF-a, formata tekstovne datoteke za prikazivanje LDAP unosa):

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

Klasa objekta domena ima i neke neobavezne atribute koje ćete možda željeti koristiti. Pregledajte shemu ili uredite unos kojeg ste kreirali korištenjem alata Web administracije kako bi vidjeli dodatne atribute koje možete koristiti. Kako bi dobili dodatne informacije, pogledajte “Upravljanje shemom” na stranici 119.

Ako je ime vašeg poduzeća My Company, a ono se nalazi u Sjedinjenim državama, mogli bi izabrati sufiks koji izgleda kao nešto od sljedećeg:

```
o=My Company
o=My Company,c=US
ou=Widget Division,o=My Company,c=US
```

Gdje je ou ime klase objekta organizacijske jedinice, o je ime organizacije za klasu objekta organizacije, a c je standardna dvoslovna skraćenica za zemlju koja se koristi za imenovanje klase objekta zemlje. U ovom bi slučaju unos najviše razine kojeg kreirate mogao izgledati kao:

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

Aplikacije koje koristite bi mogle tražiti definiranje specifičnih sufiksa ili korištenje određenih konvencija imenovanja. Na primjer, ako se vaš direktorij koristi za upravljanje digitalnim certifikatima, od vas će se možda tražiti dio strukture vašeg direktorija tako da imena unosa odgovaraju podložnim DN-ima certifikata koje sadržava.

Unosi koji će se dodati u direktorij moraju imati sufiks koji odgovara DN vrijednosti kao što je ou=Marketing,o=ibm,c=us. Ako upit sadrži sufiks koji se ne podudara s bilo kojim sufiksom konfiguriranim za lokalnu bazu podataka, upit se odnosi na LDAP poslužitelj kojeg identificira default upućivanje. Ako je specificirano LDAP upućivanje, vraća se rezultat Objekt ne postoji.

Kako bi dobili dodatne informacije o tome kako se dodaje ili uklanja sufiks, pogledajte “Dodavanje i uklanjanje sufiksa Poslužitelja direktorija” na stranici 98.

Shema

Shema je skup pravila koji upravlja načinom na koji se podaci mogu pohraniti u direktorij. Shema definira dozvoljeni tip unosa, njihovu strukturu atributa i sintaksu atributa.

Podaci su pohranjeni u direktoriju korištenjem unosa direktorija. Unos se sastoji od klase objekta, koja je potrebna i njezinih atributa. Atributi mogu biti obavezni ili neobavezni. Klasa objekta specificira vrstu informacija koju unos opisuje i definira skup atributa koje sadrži. Svaki atribut ima jednu ili više pridruženih vrijednosti. Pogledajte “Upravljanje unosima direktorija” na stranici 129 kako bi dobili dodatne informacije o tome kako se upravlja unosima.

Za više informacija koje se odnose na shemu, pogledajte:

- “Provjera sheme” na stranici 30
- “iPlanet kompatibilnost” na stranici 31
- “Općenito i UTC vrijeme” na stranici 32

Shema IBM Poslužitelja direktorija

Shema za Poslužitelj direktorija je predefinirana, no, vi možete modificirati shemu ako imate dodatne zahtjeve. Za više informacija o tome kako se modificira shema, pogledajte “Upravljanje shemom” na stranici 119.

Poslužitelj direktorija sadrži podršku dinamičke sheme. Shema je objavljena kao dio informacije o direktoriju i dostupna je u Subschema unosu (DN=″cn=schema″). Možete ispitivati shemu korištenjem ldap_search() API-ja i modificirati je korištenjem ldap_modify(). Pogledajte poglavlje “API-ji Poslužitelja direktorija” kako bi dobili više informacija o tim API-jima.

Shema ima više informacija o konfiguraciji od onih koje su uključene u LDAP Verziju 3 Zahtjev za komentarima (RFC-ovi) ili standarde specifikacije. Na primjer, za dani atribut možete obznaniti koji se indeksi moraju održavati. Te dodatne informacije o konfiguraciji se održavaju u unosu podsheme na odgovarajući način. Dodatna klasa objekta je definirana za unos podsheme IBMsubschema, koja ima ″MAY″ atribute koji sadrže proširene informacije o shemi.

Poslužitelj direktorija definira jednu shemu za cijeli poslužitelj koja je dohvatljiva preko posebnog unosa direktorija, ″cn=schema″. Unos sadrži sve sheme koje su definirane za poslužitelj. Kako bi dohvatili informacije o shemi, možete izvoditi ldap_search korištenjem sljedećeg:

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

Shema sadrži vrijednosti za sljedeće tipove atributa:

- objectClasses (Za više informacija o objectClasses, pogledajte “Klase objekta” na stranici 18.)
- attributeTypes (Za više informacija o attributeTypes, pogledajte “Atributi” na stranici 19.)
- IBMAttributeTypes (Za više informacija o IBMAttributeTypes, pogledajte “Atributi IBMAttributeTypes” na stranici 22.)
- podudarajuća pravila (Za više informacija o podudarajućim pravilima, pogledajte “Pravila podudaranja” na stranici 23).
- ldap sintakse (Za više informacija o ldap sintaksama, pogledajte “Sintaksa atributa” na stranici 25).

Sintaksa o tim definicijama sheme je zasnovana na LDAP Verzija 3 RFC-ovima.

Primjer unosa sheme bi mogao sadržavati:

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

objectclasses=(  2.5.20.1
                 NAME 'subschema'
                 AUXILIARY MAY
                     ( dITStructureRules
                    $ nameForms
                    $ ditContentRules
                    $ objectClasses
                    $ attributeTypes
                    $ matchingRules
                    $ matchingRuleUse  ) )
objectclasses=( 2.5.6.1
                NAME 'alias'
                SUP top STRUCTURAL
                MUST aliasedObjectName )

attributeTypes=( 2.5.18.10
                 NAME 'subschemaSubentry'
                 EQUALITY distinguishedNameMatch
```

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

ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.5 DESC 'Binarno' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.7 DESC 'Booleov' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.12 DESC 'DN' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.15 DESC 'Niz direktorija' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.24 DESC 'Općenito vrijeme' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.26 DESC 'IA5 niz' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.27 DESC 'INTEGER' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.50 DESC 'Telefonski broj' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.53 DESC 'UTC vrijeme' )

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

Informacije o shemi se mogu preinačiti pomoću ldap_modify API-ja. Dodatne informacije potražite u poglavlju “API-ji Poslužitelja direktorija”. S DN ″cn=schema″ možete dodati, obrisati ili zamijeniti tip atributa ili klasu objekta. Pogledajte “Dinamička shema” na stranici 26 i “Upravljanje shemom” na stranici 119 kako bi dobili više informacija. Možete osigurati i potpuni opis. Možete dodati ili zamijeniti unos sheme s definicijom LDAP-a verzije 3 ili s definicijom IBM proširenja atributa ili s obje definicije.

Podrška uobičajene sheme

IBM Direktorij podržava standardnu shemu direktorija kako je to definirano u sljedećem:

- Internet Engineering Task Force (IETF)  LDAP Verzija 3 RFC-a, kao što je RFC 2252 i 2256.
- Directory Enabled Network (DEN) 
- The Common Information Model (CIM) sa Desktop Management Task Force (DMTF) 
- Lightweight Internet Person Schema (LIPS) sa Network Application Consortium 

Ova verzija LDAP-a uključuje LDAP Verzija 3 definiranu shemu u default konfiguraciji sheme. Sadrži i definicije DEN sheme.

IBM osigurava i skup proširenih zajedničkih definicija shema koje drugi IBM proizvodi dijele kada eksploatiraju LDAP direktorij. Oni uključuju:

- Objekte za aplikacije prazne stranice kao što su e-osoba, grupa, zemlja, organizacija, organizacijska jedinica i uloga, lokacija, stanje itd.
- Objekti za druge podsisteme kao što su računi, usluge i točke pristupa, autorizacija, provjera autentičnosti, sigurnosna politika itd.

Klase objekta

Klasa objekta specificira skup atributa koji se koriste za opisivanje objekta. Na primjer, ako ste kreirali klasu objekta **tempEmployee**, ona bi mogla sadržavati atribute koji su pridruženi trenutnom zaposleniku kao što je **idNumber**, **dateOfHire** ili **assignmentLength**. Može dodati prilagođene klase objekta koje odgovaraju potrebama vaše organizacije. Shema IBM Poslužitelja direktorija sadrži neke osnovne tipove klasa objekata, uključujući:

- Grupe
- Lokacije
- Organizacije
- Ljudi

Bilješka: Klase objekta koje su specifične za Poslužitelj direktorija imaju prefiks 'ibm-'.

Klase objekta su definirane karakteristikama tipa, nasljeđa i atributa.

Tip klase objekta

Klasa objekta može biti jednog od tri tipa:

Strukturalna:
Svaki unos mora pripadati jednoj i samo jednoj strukturalnoj klasi objekta koja definira bazni sadržaj unosa. Ta klasa objekta predstavlja objekt stvarnog svijeta. Budući svi unosi moraju pripadati klasi strukturalnog objekta, to je najuobičajeniji tip klase objekta.

Sažeta:
Taj tip se koristi kao nadklasa ili predložak za druge (strukturalne) klase objekta. Definira skup atributa koji su uobičajeni za skup strukturalnih klasa objekta. Ako su te klase objekata definirane kao podklase klase sažetka, one nasljeđuju definirane atribute. Atributi ne trebaju biti definirani za svaku od tih podređenih klasa objekta.

Pomoćna:
Taj tip označava dodatne atribute koji mogu biti pridruženi unosu koji pripada određenoj strukturalnoj klasi objekta. Iako unos može pripadati samo jednoj strukturalnoj klasi objekta, on može pripadati u više pomoćnih klasa objekta.

Nasljeđivanje klase objekta

Ova verzija Poslužitelja direktorija podržava nasljeđivanje objekta za klasu objekta i definicije atributa. Nova klasa objekta može biti definirana s nadređenim klasama (višestruko nasljeđivanje) i dodatnim ili promijenjenim atributima.

Svaki unos je dodijeljen jednoj klasi strukturalnog objekta. Sve klase objekta se nasljeđuju iz **vrha** sažete klase objekta. Mogu se nasljeđivati s drugih klasa objekta. Struktura klase objekta određuje popis potrebnih i dozvoljenih atributa za određeni unos. Nasljeđivanje klase objekta ovisi o redoslijedu definicija klase objekta. Klasa objekta se može naslijediti iz klase objekta koja joj prethodi. Na primjer, struktura klase objekta za unos osobe bi mogla biti definirana u LDIF datoteci kao:

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

U toj strukturi, organizationalPerson se nasljeđuje od person i top klasa objekta, dok se person klasa objekta nasljeđuje samo iz top klase objekta. Stoga, kada dodijelite organizationalPerson klasu objekta na unos, ona automatski nasljeđuje potrebne i dozvoljene atribute iz superiorne klase objekta (u ovom slučaju, person klase objekta).

Operacije ažuriranja sheme se uspoređuju s hijerarhijom klase sheme kako bi se utvrdila dosljednost prije nego se obradi ili preda.

Atributi

Svaka klasa objekta uključuje broj potrebnih atributa i neobaveznih atributa. Potrebni atributi su atributi koji moraju biti prisutni u unosima koji koriste klasu objekta. Neobavezni atributi su atributi koji mogu biti prisutni u unosima koji koriste klasu objekta.

Atributi

Svaki unos direktorija ima skup atributa koji su mu pridruženi preko njegove klase objekta. Dok klasa objekta opisuje tip informacije koju unos sadrži, stvarni podaci su sadržani u atributima. Atribut je predstavljen s jednim ili više ime-vrijednost parom koji sadrži specifične elemente podataka kao što je ime, adresa ili telefonski broj. Poslužitelj direktorija prikazuje podatke kao su što su ime-vrijednost parovi, opisni atribut, kao što je commonName (cn) i određeni dio informacija, kao što je John Doe.

Na primjer, unos za John Doe bi mogao sadržavati nekoliko ime-vrijednost parova atributa.

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

Dok su standardni atributi već definirani u shemi, vi možete kreirati, uređivati, kopirati ili brisati definicije atributa kako bi se zadovoljile potrebe vaše organizacije.

Atributi mogu biti definirani kao atributi s jednom vrijednosti ili s više vrijednosti. Atributi s više vrijednosti nisu poredani, pa aplikacija ne bi trebala ovisiti o tome da se skup vrijednosti za dani atribut vraća u određenom poretku. Ako vam je potreban poredan skup vrijednosti, razmotrite stavljanje popisa vrijednosti u atribut s jednom vrijednosti:

```
preference: 1.-pref 2.-pref 3.-pref
```

Ili razmotrite uključivanje informacije o poretku u vrijednost:

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

Atributi s više vrijednosti su korisni kada je unos poznat prema nekoliko imena. Na primjer, cn (zajedničko ime) ima više vrijednosti. Unos može biti definiran kao:

```
dn: cn=John Smith,o=My Company,c=US
objectclass: inetorgperson
sn: Smith
cn: John Smith
cn: Jack Smith
cn: Johnny Smith
```

To omogućava da pretraživanja za John Smith i Jack Smith vrate iste informacije.

Binarni atributi sadrže proizvoljni niz bajtova, na primjer JPEG fotografija i ne mogu se koristiti za traženje unosa.

Booleovi atributi sadrže nizove TRUE ili FALSE.

DN atributi sadrže LDAP razlikovna imena. Vrijednosti ne trebaju biti DN-ovi postojećih unosa, ali moraju imati valjanu DN sintaksu.

Atributi Niza direktorija sadržavaju tekstovni niz koji koristi UTF-8 znakove. Atributi mogu i ne moraju biti osjetljivi na velika i mala slova s obzirom na vrijednosti koje se koriste u filterima pretraživanja (zasnovano na odgovarajućem pravilu definiranom za atribut), no vrijednost se uvijek vraća onakva kakva je originalno unesena.

Atributi Općenitog vremena sadržavaju znakovni prikaz datuma i vremena 2000 godine korištenjem GMT vremena s neobaveznim pomakom GMT vremenske zone. Pogledajte “Općenito i UTC vrijeme” na stranici 32 kako bi dobili više detalja o sintaksi tih vrijednosti.

IA5 Atributi niza sadrže tekstovni niz koji koristi IA5 skup znakova (7-bit US ASCII). Atributi mogu i ne moraju biti osjetljivi na velika i mala slova s obzirom na vrijednosti koje se koriste u filterima pretraživanja (zasnovano na odgovarajućem pravilu definiranom za atribut), no vrijednost se uvijek vraća onakva kakva je originalno unesena. IA5 Niz dopušta i korištenje zamjenskog znaka za pretraživanja podniza.

Atributi Integer sadrže prikaz tekstovnog niza vrijednosti. Na primjer, 0 ili 1000.

Atributi Telephone Number sadrže tekstovni prikaz broja telefona. Poslužitelj direktorija ne nameće nikakvu određenu sintaksu za te vrijednosti. Sve sljedeće vrijednosti su valjane: (555)555-5555, 555.555.5555 i +1 43 555 555 5555.

UTC Time atributi koriste raniji format niza prije 2000 godine za prikazivanje datuma i vremena. Pogledajte “Općenito i UTC vrijeme” na stranici 32 kako bi dobili više informacija.

Za više informacija, pogledajte sljedeće:

- “Uobičajeni elementi podsheme”
- “Atribut objectclass”
- “Atribut attributetypes” na stranici 21
- “Atributi IBMAttributeTypes” na stranici 22
- “Pravila podudaranja” na stranici 23
- “Pravila indeksiranja” na stranici 24
- “Sintaksa atributa” na stranici 25

Uobičajeni elementi podsheme

Sljedeći elementi se koriste za definiranje temeljnih pravila vrijednosti atributa podsheme:

- alpha = ’a’ - ’z’, ’A’ - ’Z’
- number = ’0’ - ’9’
- anh = alpha / number / ’-’ / ’;’
- anhstring = 1 * anh
- keystring = alpha [anhstring]
- numericstring = 1 * number
- oid = descr / numericoid
- descr = keystring
- numericoid = numericstring *(″.″ numericstring)
- woid = whsp oid whsp ; postav oids-a bilo kojeg oblika (brojčani OID-ovi ili imena)
- oids = woid / (″(″ oidlist ″)″)
- oidlist = woid *(″$″ woid) ; opisi objekta koji se koriste kao imena elementa sheme
- qdescrs = qdescr / (whsp ″(″ qdescrlist ″)″ whsp)
- qdescrlist = [qdescr *(qdescr)]
- whsp ″’″ descr ″’″ whsp

Atribut objectclass

Atribut objectclasses ispisuje klase objekta koje podržava poslužitelj. Svaka vrijednost tog atributa prikazuje odvojenu definiciju klase objekta. Definicije klase objekta se mogu dodati, obrisati ili modificirati odgovarajućim preinakama objectclasses atributa unosa cn=schema. Vrijednosti objectclasses atributa imaju sljedeća temeljna pravila, kako je to definirano s RFC 2252:

```
ObjectClassDescription = "(" whsp
        numericoid whsp ; Objectclass identifikator
        [ "NAME" qdescrs ]
        [ "DESC" qdstring ]
        [ "OBSOLETE" whsp ]
        [ "SUP" oids ] ; Superiorne klase objekata
        [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ] ; default je structural
        [ "MUST" oids ] ; AttributeTypes
        [ "MAY" oids ] ; AttributeTypes
        whsp ")"
```

Na primjer, definicija person objectclass je:

(2.5.6.6 NAME 'person' DESC 'Definira unose koji općenito predstavljaju ljude. ' STRUCTURAL SUP top MUST (cn $ sn) MAY (userPassword $ telephoneNumber $ seeAlso $ description))

- OID za ovu klasu je 2.5.6.6
- Ime je ″person″
- To je strukturalna klasa objekta
- Ona nasljeđuje iz klase objekta ″top″
- Potrebni su sljedeći atributi: cn, sn
- Neobavezni su sljedeći atributi: userPassword, telephoneNumber, seeAlso, description

Za više informacija o tome kako se trebaju promijeniti klase objekata koje podržava poslužitelj, pogledajte "Upravljanje shemom" na stranici 119.

Atribut attributetypes

Atribut attributetypes ispisuje atribute koje podržava poslužitelj. Svaka vrijednost tog atributa predstavlja odvojenu definiciju atributa. Definicije atributa se mogu dodati, obrisati ili preinačiti odgovarajućim preinakama attributetypes atributa unosa cn=schema. Vrijednosti atributa attributetypes imaju sljedeća temeljna pravila, kako je to definirano s RFC 2252:

```
AttributeTypeDescription = "(" whsp
        numericoid whsp ; AttributeType identifikator
        [ "NAME" qdescrs ] ; ime korišteno u AttributeType
        [ "DESC" qdstring ] ; opis
        [ "OBSOLETE" whsp ]
        [ "SUP" woid ] ; izveden iz tog drugog AttributeType
        [ "EQUALITY" woid ; Ime pravila podudaranja
        [ "ORDERING" woid ; Ime pravila podudaranja
        [ "SUBSTR" woid ] ; Ime pravila podudaranja
        [ "SYNTAX" whsp noidlen whsp ]
        [ "SINGLE-VALUE" whsp ] ; default multi-valued
        [ "COLLECTIVE" whsp ] ; default not collective
        [ "NO-USER-MODIFICATION" whsp ]; default user modifiable
        [ "USAGE" whsp AttributeUsage ]; default userApplications
         whsp ")"

AttributeUsage =
        "userApplications" /
        "directoryOperation" /
        "distributedOperation" / ; DSA-podijeljeno
        "dSAOperation" ; DSA-određeno, vrijednost ovisi o poslužitelju
```

Vrijednosti pravila podudaranja i sintakse moraju biti jedna od vrijednosti definiranih sljedećim:

- "Pravila podudaranja" na stranici 23
- "Sintaksa atributa" na stranici 25

Samo ″userApplications″ atributi mogu biti definirani ili preinačeni u shemi. Atributi ″directoryOperation″, ″distributedOperation″ i ″dSAOperation″ su definirani poslužiteljem i imaju određeno značenje operacije poslužitelja.

Na primjer, atribut ″description″ ima sljedeće definicije:

(2.5.4.13 NAME ’description’ DESC ’Atribut zajednički CIM i LDAP shemi kako bi se osigurao podroban opis unosa objekta direktorija.’ EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications)

- Njegov OID je 2.5.4.13
- Njegovo ime je ″description″
- Njegova sintaksa je 1.3.6.1.4.1.1466.115.121.1.15 (Niz direktorija)

Za više informacija o tome kako da se promijene atributi tipa koje podržava poslužitelj, pogledajte “Upravljanje shemom” na stranici 119.

Atributi IBMAttributeTypes

IBMAttributeTypes atribut se može koristiti za definiranje informacije o shemi koju ne pokriva standard LDAP Verzija 3 za atribute. Vrijednosti IBMAttributeTypes moraju biti u skladu sa sljedećim temeljnim pravilima:

```
IBMAttributeTypesDescription = "(" whsp
        numericoid whsp
      [ "DBNAME"   qdescrs ]            ; najviše 2 imena (tablica, stupac)
      [ "ACCESS-CLASS" whsp IBMAccessClass whsp ]
      [ "LENGTH" wlen whsp ]            ; maksimalna dužina atributa
      [ "EQUALITY" [ IBMwlen ] whsp ]   ; kreiraj indeks za pravilo podudaranja
      [ "ORDERING" [ IBMwlen ] whsp ]   ; kreiraj indeks za pravilo podudaranja
      [ "APPROX" [ IBMwlen ] whsp ]   ; kreiraj indeks za pravilo podudaranja
      [ "SUBSTR" [ IBMwlen ] whsp ]   ; kreiraj indeks za pravilo podudaranja
      [ "REVERSE"  [ IBMwlen ] whsp ]   ; okreni indeks za podniz
      whsp ")"

   IBMAccessClass =
      "NORMAL"            / ; to je default
      "SENSITIVE"         /
      "CRITICAL"          /
      "RESTRICTED"        /
      "SYSTEM"            /
      "OBJECT"

   IBMwlen = whsp len
```

Numericoid
Koristi se za korelaciju vrijednosti u attributetypes s vrijednosti u IBMAttributeTypes.

DBNAME
Možete dobaviti najviše 2 imena, ako je potrebno, 2 imena su dana. Prvo je ime tablice koje se koristi za taj atribut. Drugo je ime stupca koje je korišteno za potpuno normaliziranu vrijednost atributa u tablici. Ako dobavite samo jedno ime, ono se koristi kao ime tablice kao i ime stupca. Ako ne dobavite nijedno DBNAME, onda se koristi kratko ime atributa (iz attributetypes).

ACCESS-CLASS
Klasifikacija pristupa za taj tip atributa. Ako je izostavljeno ACCESS-CLASS, ono se postavlja na normalno.

LENGTH
Maksimalna dužina tog atributa. Dužina je izražena kao broj bajtova. Poslužitelj direktorija je pripremljen za specificiranje dužine atributa. U attributetypes vrijednosti se niz:

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

može koristiti kako bi se označilo da attributetype s oid-om attr-oid ima maksimalnu dužinu.

EQUALITY, ORDERING, APPROX, SUBSTR, REVERSE
Ako se koristi bilo koji od tih atributa, indeks se kreira za odgovarajuće pravilo podudaranja. Neobavezna dužina specificira širinu indeksiranog stupca. Jedan indeks se koristi za implementiranje više pravila podudaranja. Poslužitelj direktorija dodjeljuje dužinu 500 ako ju nije osigurao korisnik. Poslužitelj može

koristiti i kraću dužinu od one koju je tražio korisnik ako to ima smisla. Na primjer, kada dužina indeksa premašuje maksimalnu dužinu atributa, dužina indeksa se zanemaruje.

Pravila podudaranja

Pravilo podudaranja osigurava upute za usporedbu niza za vrijeme operacije traženja. Ta pravila se dijele u tri kategorije:

- Jednakost
- Poredak
- Podniz

Pravila podudaranja jednakosti		
Pravilo podudaranja	**OID**	**Sintaksa**
caseExactIA5Match	1.3.6.1.4.1.1466.109.114.1	Sintaksa Niza direktorija
caseExactMatch	2.5.13.5 IA5	Sintaksa niza
caseIgnoreIA5Match	1.3.6.1.4.1.1466.109.114.2	IA5 Sintaksa niza
caseIgnoreMatch	2.5.13.2	Sintaksa Niza direktorija
distinguishedNameMatch	2.5.13.1	DN - razlikovno ime
generalizedTimeMatch	2.5.13.27	Sintaksa Općenitog vremena
ibm-entryUuidMatch	1.3.18.0.2.22.2	Sintaksa Niza direktorija
integerFirstComponentMatch	2.5.13.29	Sintaksa cijelog broja - integralni broj
integerMatch	2.5.13.14	Sintaksa cijelog broja - integralni broj
objectIdentifierFirstComponentMatch	2.5.13.30	Niz za sadržavanje OID-ova. OID je niz koji sadržava znamenke (0-9) i decimalne točke (.).
objectIdentifierMatch	2.5.13.0	Niz za sadržavanje OID-ova. OID je niz koji sadržava znamenke (0-9) i decimalne točke (.)
octetStringMatch	2.5.13.17	Sintaksa Niza direktorija
telephoneNumberMatch	2.5.13.20	Sintaksa telefonskog broja
uTCTimeMatch	2.5.13.25	Sintaksa UTC vremena

Stavljanje pravila podudaranja u poredak		
Pravilo podudaranja	**OID**	**Sintaksa**
caseExactOrderingMatch	2.5.13.6	Sintaksa Niza direktorija
caseIgnoreOrderingMatch	2.5.13.3	Sintaksa Niza direktorija
distinguishedNameOrderingMatch	1.3.18.0.2.4.405	DN - razlikovno ime
generalizedTimeOrderingMatch	2.5.13.28	Sintaksa Općenitog vremena

Podniz pravila podudaranja		
Pravilo podudaranja	**OID**	**Sintaksa**
caseExactSubstringsMatch	2.5.13.7	Sintaksa Niza direktorija
caseIgnoreSubstringsMatch	2.5.13.4	Sintaksa Niza direktorija
telephoneNumberSubstringsMatch	2.5.13.21	Sintaksa telefonskog broja

Bilješka: UTC-vrijeme je format vremenskog niza definiran s ASN.1 standardima. Pogledajte ISO 8601 i X680. Koristite tu sintaksu za pohranjivanje vrijednosti vremena u UTC formatu vremena. Pogledajte “Općenito i UTC vrijeme” na stranici 32.

Pravila indeksiranja

Pravila indeksa koja su pripojena atributima omogućuju brže vraćanje informacija. Ako je dan samo atribut, ne održavaju se nikakvi indeksi. Poslužitelj direktorija sadrži sljedeća pravila indeksiranja:

- Jednakost
- Poredak
- Procijenjeno
- Podniz
- Obrnuto

Specifikacije pravila indeksiranja za atribute: Specificiranje pravila indeksiranja za atribut kontrolira kreiranje i održavanje posebnih indeksa na vrijednostima atributa. To umnogome poboljšava vrijeme odgovora za pretraživanja s filterima koji uključuju te atribute. Pet mogućih tipova pravila indeksiranja se odnose na operacije koje su primijenjene u filteru pretraživanja.

Jednakost

Primjenjuje se na sljedeće operacije pretraživanja:

- equalityMatch ’=’

Na primjer:

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

Poredak

Primjenjuje se na sljedeće operacije pretraživanja:

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

Na primjer:

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

Procijenjeno

Primjenjuje se na sljedeće operacije pretraživanja:

- approxMatch ’~=’

Na primjer:

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

Podniz Odnosi se na operacije pretraživanja korištenjem sintakse podniza:

- podniz ’*’

Na primjer:

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

Obrnuto

Primjenjuje se na sljedeće operacije pretraživanja:

- ’*’ podniz

Na primjer:

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

Ako ništa drugo, preporuča se da specificirate jednako indeksiranje na bilo kojim atributima koji će se koristiti u filterima pretraživanja.

Sintaksa atributa

Sintaksa atributa definira dopustive vrijednosti za atribut. Poslužitelj koristi definiciju sintakse za atribut kako bi se provjerila valjanost podataka i odredilo kako treba upariti vrijednosti. Na primjer, ″Boolean″ atribut može imati samo vrijednosti ″TRUE″ i ″FALSE″..

Sintaksa	OID
Sintaksa atributa Type Description	1.3.6.1.4.1.1466.115.121.1.3
Binarno - niz okteta	1.3.6.1.4.1.1466.115.121.1.5
Boolean - TRUE/FALSE	1.3.6.1.4.1.1466.115.121.1.7
Sintaksa Niza direktorija	1.3.6.1.4.1.1466.115.121.1.15
Sintaksa Opisa pravila DIT Sadržaja	1.3.6.1.4.1.1466.115.121.1.16
Sintaksa Opisa pravila DITStructure	1.3.6.1.4.1.1466.115.121.1.17
DN - razlikovno ime	1.3.6.1.4.1.1466.115.121.1.12
Sintaksa Općenitog vremena	1.3.6.1.4.1.1466.115.121.1.24
IA5 Sintaksa niza	1.3.6.1.4.1.1466.115.121.1.26
IBM atribut Type Description	1.3.18.0.2.8.1
Sintaksa cijelog broja - integralni broj	1.3.6.1.4.1.1466.115.121.1.27
Sintaksa Opisa LDAP sintakse	1.3.6.1.4.1.1466.115.121.1.54
Opis pravila podudaranja	1.3.6.1.4.1.1466.115.121.1.30
Opis Koristi pravilo podudaranja	1.3.6.1.4.1.1466.115.121.1.31
Opis Oblika imena	1.3.6.1.4.1.1466.115.121.1.35
Sintaksa Opisa klase objekta	1.3.6.1.4.1.1466.115.121.1.37
Niz za sadržavanje OID-ova. OID je niz koji sadržava znamenke (0-9) i decimalne točke (.). Pogledajte “Identifikator objekta (OID)”.	1.3.6.1.4.1.1466.115.121.1.38
Sintaksa telefonskog broja	1.3.6.1.4.1.1466.115.121.1.50
Sintaksa UTC Vremena. UTC-vrijeme je format vremenskog niza definiran s ASN.1 standardima. Pogledajte ISO 8601 i X680. Koristite tu sintaksu za pohranjivanje vrijednosti vremena u UTC formatu vremena. Pogledajte “Općenito i UTC vrijeme” na stranici 32.	1.3.6.1.4.1.1466.115.121.1.53

Identifikator objekta (OID)

Identifikator objekta (OID) je niz decimalnih brojeva koji jednoznačno identificiraju objekt. Ti objekti su u pravilu klasa objekta ili atribut.

Ako nemate OID, možete specificirati klasu objekta ili ime atributa pridodanog iz **-oid**. Na primjer, ako kreirate atribut tempID, možete specificirati OID kao **tempID-oid**.

Jako je važno da se privatni OID-evi dobave od legitimnih ovlaštenja. Postoje dvije osnovne strategije za dobivanje legitimnih OID-ova:

- Registrirajte objekte s ovlaštenjem. Ta strategija može biti prikladna ako, na primjer, trebate malo OID-ova.
- Dobavite luk (luk je pojedinačno podstablo OID stabla) iz ovlaštenja i dodijelite svoje vlastite OID-ove kako je to potrebno. Ta strategija ima prednosti kada je potrebno više OID-ova ili kada dodjele OID-ova nisu stabilne.

American National Standards Institute (ANSI) je izdavač registracije za imena organizacije u Sjedinjenim državama pod globalnim procesom registracije kojeg je uspostavila International Standards Organization (ISO) i International Telecommunication Union (ITU). Više informacija o registraciji imena organizacije se može pronaći na ANSI Web stranici (www.ansi.org). ANSI OID luk za organizacije je 2.16.840.1. ANSI će dodijeliti broj (NEWNUM) i kreirati novi OID luk: 2.16.840.1.NEWNUM.

U većini zemalja ili regija, nacionalna udruga za standarde održava OID registar. Kao i kod ANSI luka, to su općeniti lukovi dodijeljeni pod OID 2.16. Možda će trebati malo istraživati kako bi se pronašlo OID ovlaštenje za određenu zemlju ili regiju. Nacionalna organizacija za standarde za vašu zemlju ili regiju može biti ISO član. Imena i kontaktne informacije o ISO članovima se mogu pronaći na ISO Web stranici  (www.iso.ch).

Internet Assigned Numbers Authority (IANA) dodjeljuje brojeve privatnog poduzeća, a to su OID-ovi u luku 1.3.6.1.4.1. IANA će dodijeliti broj tako (NEWNUM) da će novi OID luk biti 1.3.6.1.4.1.NEWNUM. Ti brojevi se mogu dobaviti na IANA Web stranici  (www.iana.org).

Jednom kada se organizaciji dodijeli OID, možete definirati svoje vlastite OID-ove pridodavanjem na kraj OID-a. Na primjer, pretpostavimo da je vašoj organizaciji dodijeljen izmišljen OID 1.1.1. Nijednoj drugoj organizaciji se neće dodijeliti OID koji počinje s ″1.1.1″. Možete kreirati čitav raspon za LDAP dodavanjem ″.1″ kako bi oblikovali 1.1.1.1. To možete dalje podijeliti u lance za klase objekata (1.1.1.1.1), tipove atributa (1.1.1.1.2) itd i dodijeliti OID 1.1.1.1.2.34 atributu ″foo″.

Unosi podsheme

Postoji jedan unos podsheme po poslužitelju. Svi unosi u direktoriju imaju uključen subschemaSubentry tip atributa. Vrijednost subschemaSubentry tipa atributa je DN unosa podsheme koja odgovara unosu. Svi unosi pod istim poslužiteljem dijele isti unos podsheme i njihov tip subschemaSubentry atributa ima istu vrijednost. Unos podsheme ima tvrdo kodirano DN ’cn=schema’.

Unos podsheme pripada klasama objekta ’top’, ’subschema’ i ’IBMsubschema’. ’IBMsubschema’ klasa objekta nema MUST atribute i jedan tip MAY atributa (’IBMattributeTypes’).

IBMsubschema klasa objekta

IBMsubschema klasa objekta se koristi samo u unosu podsheme kako slijedi:

```
( 1.3.18.0.2.6.174
NAME 'ibmSubSchema'
DESC 'IBM određena klasa objekta koja pohranjuje sve atribute i klase objekta za dani poslužitelj
 direktorija.'
SUP 'podshema'
STRUCTURAL MAY ( IBMAttributeTypes ) )
```

Ispitivanja sheme

API ldap_search() se može koristiti za ispitivanje unosa podsheme kako je to prikazano u sljedećem primjeru:

```
DN           : "cn=schema"
opseg pretraživanja : bazni
filter       : objectclass=subschema ili objectclass=*
```

Taj primjer vraća punu shemu. Da vratite sve vrijednosti tipova izabranog atributa, koristite attrs parametar u ldap_search. Ne možete dohvatiti samo određene vrijednosti određenog tipa atributa.

Pogledajte poglavlje “API-ji Poslužitelja direktorija” kako bi dobili više informacija o ldap_search API-ju.

Dinamička shema

Za izvođenje promjene dinamičke sheme, koristite ldap_modify API s DN-om ″cn=schema″. Smije se dodavati, obrisati ili zamijeniti samo jedan po jedan entitet sheme (na primjer, tip atributa ili klasa objekta).

Za brisanje unosa sheme, specificirajte atribut sheme koji definira unos sheme (objectclasses ili attributetypes) i za njegovu vrijednost OID u zagradama. Na primjer, za brisanje atributa s OID-om <attr-oid>:

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

Možete i dobaviti puni opis. U svakom slučaju, pravilo podudaranja koje se koristi za pronalaženje entiteta sistema koji će se obrisati je objectIdentifierFirstComponentMatch.

Za dodavanje ili zamjenu entiteta sheme, MORATE osigurati definiciju LDAP verzije 3 i MOŽETE osigurati IBM definiciju. U svakom slučaju morate osigurati samo definiciju ili definicije entiteta sheme na koju želite utjecati.

Na primjer, za brisanje tipa atributa 'cn' (njegov OID je 2.5.4.3), koristite ldap_modify() s:

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

Da dodate novu traku tipa atributa s OID 20.20.20 koja nasljeđuje iz atributa ″name″ i ima dužinu od 20 znakova:

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

LDIF verzija gore navedenog bi bila:

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

Kontrole pristupa

Dinamičke promjene sheme može izvoditi samo dobavljač replikacije ili DN administratora.

Replikacija

Kada se izvodi dinamička promjene sheme, ona se replicira.

Nedozvoljene promjene sheme

Nisu dozvoljene sve promjene sheme. U ograničenja promjene spada sljedeće:

- Sve promjene na shemi moraju ostaviti shemu u konzistentnom stanju.
- Tip atributa koji je nadtip drugog tipa atributa se ne smije obrisati. Tip atributa koji je ″MAY″ ili ″MUST″ tip atributa klase objekta se ne smije obrisati.
- Ne smije se obrisati klasa objekta koja je nadklasa druge klase.
- Ne mogu se dodati tipovi atributa ili klase objekta koje se odnose na nepostojeće entitete (na primjer, sintakse ili klase objekta).
- Tipovi atributa ili klase objekta se ne mogu modificirati na način da oni nakon modifikacije referenciraju nepostojeće entitete (na primjer, sintakse ili klase objekta).

Nisu dozvoljene promjene sheme koje utječu na operaciju poslužitelja. Poslužitelj direktorija treba sljedeće definicije sheme. One se ne smiju mijenjati.

Klase objekta:

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

Atributi:

- aclEntry
- aclPropagate
- aclSource
- aliasedObjectName, aliasedentryName
- businessCategory
- cn, commonName
- createTimestamp
- creatorsName
- description
- dn, distinguishedName
- entryOwner
- hasSubordinates
- ibm-entryChecksum
- ibm-entryChecksumOp
- ibm-entryUuid
- member
- modifiersName
- modifyTimestamp
- name
- o, organizationName, organization
- objectClass
- os400-acgcde
- os400-astlvl
- os400-atnpgm
- os400-audlvl
- os400-aut
- os400-ccsid
- os400-chridctl
- os400-cntryid
- os400-curlib
- os400-dlvry
- os400-docpwd
- os400-dspsgninf
- os400-eimassoc

- os400-gid
- os400-groupmember
- os400-grpaut
- os400-grpauttyp
- os400-grpprf
- os400-homedir
- os400-IaspStorageInformation
- os400-inlmnu
- os400-inlpgm
- os400-invalidSignonCount
- os400-jobd
- os400-kbdbuf
- os400-langid
- os400-lclpwdmgt
- os400-lmtcpb
- os400-lmtdevssn
- os400-locale
- os400-maxstg
- os400-msgq
- os400-objaud
- os400-outq
- os400-owner
- os400-password
- os400-passwordExpirationDate
- os400-passwordLastChanged
- os400-previousSignon
- os400-profile
- os400-prtdev
- os400-ptylmt
- os400-pwdexp
- os400-pwdexpitv
- os400-setjobatr
- os400-sev
- os400-spcaut
- os400-spcenv
- os400-srtseq
- os400-status
- os400-storageUsed
- os400-storageUsedOnIasp
- os400-supgrpprf
- os400-sys os400-text
- os400-uid
- os400-usrcls
- os400-usropt
- ou, organizationalUnit, organizationalUnitName

- owner
- ownerPropagate
- ownerSource
- ref
- replicaBindDN
- replicaBindMethod
- replicaCredentials, replicaBindCredentials
- replicaHost
- replicaPort
- replicaUpdateTimeInterval
- replicaUseSSL
- seeAlso

Sintakse:
Sve

Pravila podudaranja:
Sve

Provjera sheme

Kada se inicijalizira poslužitelj, čitaju se datoteke sheme i provjerava se njihova konzistentnost i ispravnost. Ako se provjerom utvrde greške, poslužitelj se ne inicijalizira i izdaje poruku o greški. Za vrijeme bilo koje promjene dinamičke sheme, dobivenoj shemi se isto tako provjerava konzistentnost i ispravnost. Ako se provjerom utvrde greške, vraća se greška i ne može se napraviti promjena. Neke provjere su dio temeljnih pravila (na primjer, tip atributa može imati najviše jedan nadtip ili klasa objekta može imati bilo koji broj nadklasa).

Sljedeće stavke se provjeravaju kod tipova atributa:
- Različiti tipovi atributa ne mogu imati isto ime ili OID.
- Hijerarhija nasljeđivanja tipova atributa nema cikluse.
- Nadtip tipa atributa mora isto tako biti definiran, iako se njegova definicija može prikazati kasnije ili u odijeljenoj datoteci.
- Ako je tip atributa podtip drugog, oboje imaju isti USAGE.
- Svi tipovi atributa imaju sintaksu koja je izravno definirana ili naslijeđena.
- Samo se operativni atributi mogu označiti kao NO-USER-MODIFICATION.

Sljedeće stavke se provjeravaju kod klasa objekta:
- Dvije različite klase objekta ne mogu imati isto ime ili OID.
- Hijerarhija nasljeđivanja klasa objekata nema cikluse.
- Nadklase klase objekta moraju isto biti definirane, iako se njihova definicija može prikazati kasnije ili u odijeljenoj datoteci.
- Moraju biti definirani i ″MUST″ i ″MAY″ tipovi atributa klase objekta, iako se njihova definicija može pojaviti kasnije ili u odijeljenoj datoteci.
- Svaka strukturalna klasa objekta je izravno ili neizravno podklasa one na vrhu.
- Ako klasa objekta sažetka ima nadklase, nadklasa mora biti isto klasa sažetka.

Provjera unosa na shemi

Kada se unos doda ili preinači putem LDAP operacije, unos se provjerava na shemi. Po defaultu se izvode sve provjere koje su ispisane u ovom odlomku. No, vi možete selektivno onemogućiti neka od provjeravanja sheme mijenjanjem razine provjeravanja sheme. To se izvodi pomoću iSeries Navigatora mijenjanjem vrijednosti polja **Provjera sheme** na

stranici **Baza podataka/Sufiksi** svojstva Poslužitelja direktorija. Pogledajte “Shema konfiguracije Poslužitelja direktorija” na stranici 184 kako bi dobili informacije o atributima konfiguracije sheme.

Kako bi bio u skladu sa shemom, unosu se provjeravaju sljedeći uvjeti:

S obzirom na klase objekta:

- Mora imati barem jednu vrijednost tipa atributa ″objectClass″.
- Može imati bilo koji broj pomoćnih klasa objekta uključujući i nijednu. To nije provjera već objašnjenje. Ne postoji opcija kojom bi se to onemogućilo.
- Može imati bilo koji broj klasa objekta sažetka, ali one moraju biti rezultat nasljeđivanja klase. To znači da za svaku klasu objekta sažetka koju ima unos ima i strukturalnu ili pomoćnu klasu objekta koju nasljeđuje izravno ili neizravno od klase objekta sažetka.
- Mora imati barem jednu strukturalnu klasu objekta.
- Mora imati barem jednu neposrednu ili baznu strukturalnu klasu objekta. To znači da sve strukturalne klase objekta koje su dobavljene s unosom moraju biti i nadklase točno jedne od njih. Najviše izvedena klasa objekta se naziva ″neposredna″ ili ″bazno strukturirana″ klasa objekta unosa ili jednostavno ″strukturalna″ klasa objekta.
- Ne može se promijeniti neposredna strukturalna klasa objekta (na ldap_modify).
- Za svaku klasu objekta koja je dobavljena s unosom se izračunava skup svih njezinih izravnih ili neizravnih nadklasa; ako jedna od tih nadklasa nije dobavljena s unosom, ona se automatski dodaje.
- Ako je razina provjeravanja sheme postavljena na **Verzija 3 (striktno)**, moraju biti dobavljene sve nadklase. Na primjer, kako bi kreirali unos s klasom objekta inetorgperson, moraju biti specificirane sljedeće klase objekta: person, organizationalperson i inetorgperson.

Valjanost tipova atributa za unos se određuje kako slijedi:

- Skup MUST tipova atributa za unos se izračunava kao unija skupova MUST tipova atributa svih njegovih klasa objekta, uključujući implicirane naslijeđene klase objekta. Ako skup MUST tipova atributa za unos nije podskup skupa tipova atributa koje sadržava unos, unos se odbacuje.
- Skup MAY tipova atributa za unos se izračunava kao unija skupova MAY tipova atributa svih njegovih klasa objekata, uključujući implicirane naslijeđene klase objekata. Ako skup tipova atributa koji su sadržani u unosu nije podskup unije skupova MUST i MAY tipova atributa za unos, unos se odbacuje.
- Ako je bilo koji od tipova atributa definiranih za unos označen kao NO-USER-MODIFICATION, unos se odbacuje.

Valjanost vrijednosti tipa atributa za unos se određuje kako slijedi:

- Za svaki tip atributa kojeg sadržava unos, ako tip atributa ima jednu vrijednost, a unos ima više od jedne vrijednosti, unos se odbacuje.
- Za svaku vrijednost atributa svakog tipa atributa kojeg sadržava unos, ako sintaksa nije u skladu s rutinom provjeravanja sintakse za sintaksu tog atributa, unos se odbacuje.
- Za svaku vrijednost atributa svakog tipa atributa koji je sadržan u unosu, ako je njegova dužina veća od maksimalne dužine koja je dodijeljena tom tipu atributa, unos se odbacuje.

Valjanost DN-a se provjerava kako slijedi:

- Provjerava se usklađenost sintakse s BNF za DistinguishedNames. Ako nije usklađena, unos se odbacuje.
- Verificirano je da se RDN sastoji od samo jednog tipa atributa koji je valjan za taj unos.
- Verificirano je da se vrijednosti tipa atributa korištene u RDN-u pojavljuju u unosu.

iPlanet kompatibilnost

Sintaktički analizator kojeg koristi Poslužitelj direktorija dopušta da se vrijednosti atributa tipova atributa sheme (objectClasses i attributeTypes) specificiraju korištenjem temeljnih pravila za iPlanet. Na primjer, descrs i numeric-oids se mogu specificirati okruženi jednostrukim navodnicima (kao da su qdescrs). No, informacija o shemi je uvijek dostupna preko ldap_search. Odmah nakon što se izvede jedna dinamička promjena (korištenjem ldap_modify) na vrijednosti atributa u datoteci, cijela datoteka se zamjenjuje onom u kojoj sve vrijednosti atributa slijede

specifikacije Poslužitelja direktorija. Budući se isti sintaktički analizator koristi na datotekama i ldap_modify zahtjevima, ispravno se rukuje i s ldap_modify koji koristi iPlanet temeljna pravila za vrijednosti atributa.

Kada se upit izvede na unosu podsheme iPlanet poslužitelja, rezultirajući unos može imati više od jedne vrijednosti za dani OID. Na primjer, ako određeni tip atributa ima dva imena (kao što je 'cn' i 'commonName'), onda se opis tog atributa dobavlja dvaput, jednom za svako ime. Poslužitelj direktorija može sintaktički analizirati shemu u kojoj se opis jednog tipa atributa ili klase objekta pojavljuje više puta s istim opisom (osim za NAME i DESCR). No, kada Poslužitelj direktorija izdaje shemu on dobavlja jedan opis takvog tipa atributa s ispisanim svim imenima (prvo je kratko ime). Na primjer, evo kako iPlanet opisuje atribut zajedničkog imena:

```
( 2.5.4.3 NAME 'cn'
  DESC 'Standardni atribut'
   SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

( 2.5.4.3 NAME 'commonName'
  DESC 'Standardni atribut, zamjensko ime za cn'
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Poslužitelj direktorija to ovako opisuje:

```
( 2.5.4.3 NAME ( 'cn' 'zajedničko ime' ) SUP ime )
```

Poslužitelj direktorija podržava podtipove. Ako ne želite da 'cn' bude podtip imena (koje odstupa od standarda), možete deklarirati sljedeće:

```
( 2.5.4.3 NAME ( 'cn' 'zajedničko ime' )
     DESC 'Standardni atribut'
     SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Prvo ime ('cn') se uzima kao preferirano ili kratko ime, a sva ostala imena nakon 'cn' kao zamjenska imena. Od ove točke nadalje se nizovi '2.3.4.3', 'cn' i 'commonName' (kao i njihovi ekvivalenti neosjetljivi na velika i mala slova) mogu izmjenjivo koristiti unutar sheme ili za unose koji su dodani na direktorij.

Općenito i UTC vrijeme

Postoje različita bilježenja koja se koriste kako bi se označio datum i informacije koje se odnose na vrijeme. Na primjer, četvrti dan siječnja godine 1999 se može napisati kao:

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

i na još mnogo drugih načina bilježenja.

Poslužitelj direktorija standardizira prikaz vremenske oznake tako da traži da LDAP poslužitelji podržavaju dvije sintakse:

- Sintaksa Općenitog vremena u obliku:

  ```
  YYYYMMDDHHMMSS[.|,fraction][(+|-HHMM)|Z]
  ```

  Postoji 4 znamenke za godinu i po 2 znamenke za mjesec, dan, sat, minutu i sekundu i nebavezno za djelić sekunde. Bez ikakvih drugih dodataka, za vrijeme i datum se pretpostavlja da su usklađeni s lokalnom vremenskom zonom. Da označite da je vrijeme izmjereno u Koordiniranom univerzalnom vremenu, dodajte veliko slovo Z vremenu ili razlici lokalnog vremena. Na primjer:

  ```
  "19991106210627.3"
  ```

  što označava lokalno vrijeme od 21 sati, 6 minuta i 27.3 sekundi 6 studenog 1999.

  ```
  "19991106210627.3Z"
  ```

  što označava koordinirano univerzalno vrijeme.

```
"19991106210627.3-0500"
```

što je lokalno vrijeme kao u prvom primjeru s razlikom od 5 sati u odnosu na koordinirano univerzalno vrijeme.

Ako označavate i neobavezan djelić sekunde, potrebna je točka ili zarez. Kod razlike lokalnog vremena, '+' ili '-' mora prethoditi vrijednosti sat-minuta

- Sintaksa Univerzalnog vremena u obliku:

```
YYMMDDHHMM[SS][(+ | -)HHMM)|Z]
```

Postoje po 2 znamenke za godinu, mjesec, dan, sat, minutu i neobavezna polja za sekunde. Kao i kod Općenitog vremena, može se specificirati neobavezna razlika vremena. Na primjer, ako je lokalno vrijeme 7.00 2. Siječnja 1999., a koordinirano univerzalno vrijeme je 12.00 2 Siječnja 1999., vrijednost UTC vremena je:

```
"9901021200Z"
     ili
"9901020700-0500"
```

Ako je lokalno vrijeme 7.00 2 Siječnja 2001, a koordinirano univerzalno vrijeme je 12.00 2 Siječnja 2001, vrijednost UTCT vremena je:

```
"0101021200Z"
     ili
"0101020700-0500"
```

UTCT vrijeme dopušta samo dvije znamenke za vrijednost godine, pa se ne preporuča njegovo korištenje.

Podržana pravila podudaranja su generalizedTimeMatch za jednakost i generalizedTimeOrderingMatch za nejednakost. Nije dozvoljeno traženje niza. Na primjer, valjani su sljedeći filteri:

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

Nisu valjani sljedeći filteri:

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

Objavljivanje

i5/OS omogućuje sposobnost da sistem objavljuje određene vrste informacija u LDAP direktorij. To znači, sistem će kreirati i ažurirati LDAP unose koji predstavljaju različite tipove podataka.

i5/OS ima ugrađenu podršku za objavljivanje sljedećih informacija LDAP poslužitelju:

Korisnici

Kada konfigurirate i5/OS za objavljivanje informacija tipa Korisnici u Poslužitelj direktorija, on automatski eksportira unose iz sistemskog distribucijskog direktorija u Poslužitelj direktorija. Da bi to napravio, on koristi QGLDSSDD_modrdn aplikativno programsko sučelje (API). Time i LDAP direktorij ostaje sinkroniziran s promjenama napravljenim u sistemskom distribucijskom direktoriju. Kako bi dobili informacije o QGLDSSDD API-ju, pogledajte "API-ji Poslužitelja direktorija" u poglavlju Programiranje.

Objavljivanje korisnika je korisno za omogućavanje pristupa LDAP traženja informacijama sa sistemskog distribucijskog direktorija (na primjer da se omogući pristup LDAP adresaru na LDAP-omogućene POP3 klijente za poštu kao što su Netscape Communicator ili Microsoft Outlook Express).

Objavljeni korisnici se isto tako mogu koristiti za podržavanje LDAP provjere autentičnosti s jednim korisnicima objavljenim iz direktorija distribucije sistema i s drugim korisnicima dodanim na direktorij na druge načine. Objavljeni korisnik ima uid atribut koji imenuje profil korisnika i nema userPassword atribut. Kada je primljen zahtjev za povezivanjem za ovakav unos, poslužitelj poziva i5/OS sigurnost da provjeri valjanost uid-a i lozinke

kao važećeg profila korisnika i lozinke za taj profil. Ako želite koristiti LDAP provjeru autentičnosti i želite da postojeći i5/OS korisnici mogu provjeriti autentičnost upotrebom njihovih i5/OS lozinki, a da se ne-i5/OS korisnici ručno dodaju u direktorij, trebate razmotriti ovu funkciju.

Sistemske informacije

Kada konfigurirate i5/OS za objavljivanje informacija tipa Sistem u Poslužitelj direktorija, objavljuju se sljedeći tipovi informacija:

- Osnovne informacije o tom stroju i izdanje operativnog sistema.
- Neobavezno, možete izabrati jedan ili više pisača koji će se objaviti, u tom slučaju će sistem automatski zadržati LDAP direktorij sinkroniziran s promjenama koje su učinjene na tim pisačima na sistemu.

U informacije pisača koje se mogu objaviti spadaju:

- Smještaj
- Brzina u stranicama po minuti
- Podrška za dupleks i boju
- Tip i model
- Opis

Te informacije dolaze od opisa uređaja na sistemu koji se izdaje. U mrežnoj okolini, korisnici mogu koristiti te informacije kao pomoć pri izboru pisača. Informacije se prvi put objavljuju kada se pisač izabere za objavljivanje i ažuriraju se kada se program za pisanje na pisač zaustavi ili pokrene ili kada se promijeni opis uređaja pisača.

Podjele pisača

Kada konfigurirate i5/OS za objavljivanje dijeljenja pisača, informacije o izabranim iSeries Netserver dijeljenjima pisača se objavljuju u konfigurirani poslužitelj Aktivnog direktorija. Objavljivanje dijeljenja pisača u Aktivni direktorij omogućuje korisnicima dodavanje iSeries pisača njihovom Windows 2000 desktopu pomoću Windows 2000 Čarobnjaka za dodavanje pisača. Da to učinite u Čarobnjaku za dodavanje pisača, specificirajte da želite pronaći pisač u Windows 2000 Aktivnom direktoriju. Podjele pisača morate objaviti na poslužitelju direktorija koji podržava Microsoft shemu Aktivnog direktorija.

TCP/IP Kvaliteta usluga

Poslužitelj TCP/IP Kvaliteta usluga (QOS) može biti konfiguriran tako da koristi politiku QOS podjele definirane u LDAP direktoriju koji koristi IBM definiranu shemu. TCP/IP QOS agenta objavljivanja koristi QOS poslužitelj kako bi pročitao informacije o politici; on definira poslužitelja, informacije o provjeri autentičnosti i gdje su na direktoriju pohranjene informacije o politici.

Možete kreirati i aplikaciju koja će objavljivati ili tražiti druge tipove informacija u LDAP direktoriju korištenjem ove okosnice definiranjem dodatnih agenta objavljivanja i korištenjem API-ja objavljivanja direktorija. Za više informacija, pogledajte “API-ji Poslužitelja direktorija” u poglavlju Programiranje.

Replikacija

Replikacija je tehnika koju koriste poslužitelji direktorija kako bi se poboljšala izvedba i pouzdanost. Proces replikacije zadržava usklađenima podatke u više direktorija.

Za informacije o tome kako se upravlja replikacijom pogledajte “Upravljanje replikacijom” na stranici 101. Za više informacija o replikaciji pogledajte sljedeće:

- “Pregled replikacije” na stranici 35
- “Terminologija replikacije” na stranici 36
- “Ugovori replikacije” na stranici 37

- “Kako se informacije replikacije pohranjuju u poslužitelju” na stranici 38
- “Sigurnosna razmatranja o informacijama replikacije” na stranici 38

Pregled replikacije

Replikacija ima dvije glavne koristi:

- Redundancija informacije - replike stvaraju sigurnosnu kopiju poslužitelja njihova dobavljača.
- Brza traženja - zahtjevi za traženjem se mogu raširiti između nekoliko različitih poslužitelja koji svi imaju isti sadržaj, umjesto na jednog poslužitelja. Time se smanjuje vrijeme odgovora za dovršenje zahtjeva.

Specifični unosi u direktorij se identificiraju kao ishodišta repliciranih podstabla tako da im se doda ibm-replicationContext objectclass. Svako podstablo se nezavisno replicira. Podstablo ide dolje kroz stablo informacija direktorija (DIT) dok ne dođe do unosa na listu ili drugih repliciranih podstabla. Unosi se dodaju ispod korijena repliciranog podstabla kako bi bile sadržane informacije o topologiji replikacije. Ti unosi su jedan ili više unosa grupe replike pod kojom su kreirana podstabla replike. Svakom podstablu replike su pridruženi ugovori replikacije koji identificiraju poslužitelje koje dobavlja (replicira) svaki poslužitelj i definiraju vjerodajnice i informacije o rasporedu.

Preko replikacije se promjene koje su učinjene na jednom direktoriju šire na još jedan ili više dodatnih direktorija. U stvari, promjena na jednom direktoriju se pojavljuje na više različitih direktorija. IBM Direktorij podržava prošireni glavni-podređeni model replikacije. Topologije replikacije su proširene tako da uključuju:

- Replikaciju podstabla Stabla informacije direktorija (DIT) na određenim poslužiteljima
- Više-razinsku topologiju koja se naziva kaskadna replikacija
- Dodjeljivanje uloge poslužitelja (glavni ili replika) pomoću podstabla.
- Višestruki glavni poslužitelji koji se nazivaju ravnopravnom replikacijom.

Prednost repliciranja pomoću podstabla je u tome da replika ne treba replicirati cijeli direktorij. Ono može biti replika dijela ili postabla direktorija.

Prošireni model mijenja koncept glavni i replika. Ti termini se više ne odnose na poslužitelje već na uloge koje poslužitelj ima ovisno o određenom repliciranom podstablu. Poslužitelj se može ponašati kao glavni za neka podstabla i kao replika za druga. Termin glavni se koristi za poslužitelj koji prihvaća ažuriranja klijenta za replicirano podstablo. Termin replika se koristi za poslužitelj koji prihvaća ažuriranja samo iz drugih poslužitelja koji su označeni dobavljačima za replicirano podstablo.

Postoje tri tipa direktorija kako je to definirano funkcijom: *glavni/ravnopravno*, *kaskadni* i *samo za čitanje*.

Tablica 1. Uloge poslužitelja

Direktorij	**Opis**
Glavni/ravnopravni	Glavni/ravnopravni poslužitelj sadrži informacije glavnog direktorija iz kojeg se ažuriranja šire na replike. Sve promjene se rade i pojavljuju na glavnom poslužitelju i glavni poslužitelj je odgovoran za širenje tih promjena na replike. Nekoliko poslužitelja se može ponašati kao glavni poslužitelj za informacije o direktoriju, s tim da je svaki glavni poslužitelj odgovoran za ažuriranje drugih glavnih poslužitelja i replika poslužitelja. To se naziva ravnopravnom replikacijom. Ravnopravna replikacija može poboljšati izvedbu i pouzdanost. Izvedba je poboljšana omogućavanjem lokalnom poslužitelju da rukuje ažuriranjima u široko distribuiranoj mreži. Pouzdanost se poboljšava omogućavanjem da backup glavni poslužitelj bude spreman za trenutno preuzimanje ako dođe do kvara na primarnom glavnom poslužitelju. **Bilješke:** 1. Glavni poslužitelji repliciraju sva ažuriranja klijenta, ali ne repliciraju ažuriranja koja su primljena iz drugih glavnih poslužitelja. 2. Ažuriranja na istom unosu koje izvodi više poslužitelja mogu uzrokovati nekonzistentnosti u podacima direktorija jer nema rješenja sukoba.

Tablica 1. Uloge poslužitelja (nastavak)

Direktorij	Opis
Kaskadni (prosljeđivanje)	Kaskadni poslužitelj je replika poslužitelj koji replicira sve promjene koje su poslane na njega. Razlika u odnosi na glavni/ravnopravni poslužitelj je u tome da glavni/ravnopravni poslužitelj replicira samo promjene koje čini klijent koji je povezan na tog poslužitelja. Kaskadni poslužitelj može smanjiti radno opterećenje replikacije iz glavnih poslužitelja u mreži koji sadrže mnoge široko raspršene replike.
Replika (samo za čitanje)	Dodatni poslužitelj koji sadrži kopiju informacije direktorija. Replike su kopije glavnih poslužitelja (ili podstabla). Replika osigurava backup repliciranog podstabla.

Ako replikacija ne uspije, ona se ponavlja čak i kada se ponovo pokrene poslužitelj. Može se koristiti prozor Upravljanje redovima u Web administracijskom alatu kako bi se pregledala neuspjela replikacija.

Možete tražiti ažuriranja na replika poslužitelju, no ažuriranje se u stvari prosljeđuje na glavni poslužitelj upućivanjem natrag na klijenta. Ako je ažuriranje uspješno, glavni poslužitelj onda šalje ažuriranje na replike. Tako dugo dok glavni poslužitelj ne dovrši replikaciju ažuriranja, promjena se ne odražava na replika poslužitelju na kojem je bila originalno zatražena. Promjene se repliciraju u poretku u kojem se rade na glavnom poslužitelju.

Ako više ne koristite repliku, morate ukloniti ugovor o replikaciji od dobavljača. Ostavljanje definicije uzrokuje to da poslužitelj stavlja u red sva ažuriranja i nepotrebno koristi prostor direktorija. Isto tako, dobavljač će i dalje pokušavati kontaktirati nepostojećeg potrošača da ponovo pokuša poslati podatke.

Terminologija replikacije

Neka terminologija koja se koristi kod opisivanja replikacije:

Kaskadna replikacija
Topologija replikacije u kojoj postoji više razina poslužitelja. Ravnopravni/glavni poslužitelj replicira na skup poslužitelja samo za čitanje (prosljeđivanje) koji se izmjenično repliciraju na druge poslužitelje. Takva topologija smanjuje posao replikacije iz glavnih poslužitelja.

Poslužitelj potrošača
Poslužitelj koji prima promjene preko replikacije iz drugog (dobavljač) poslužitelja.

Vjerodajnice
Identificira metodu i potrebne informacije koje dobavljač koristi kod povezivanja na potrošača. Kod jednostavnih povezivanja u to spada DN i lozinka. Vjerodajnice su pohranjene u unosu, a njihovo DN je specificirano u ugovoru replikacije.

Poslužitelj prosljeđivanja
Poslužitelj samo za čitanje koji replicira sve promjene koje je na njega poslao glavni ili ravnopravni poslužitelj. Zahtjevi za ažuriranjem klijenta se odnose na glavnog ili ravnopravnog poslužitelja.

Glavni poslužitelj
Poslužitelj na koji se može pisati (može se ažurirati) za dano podstablo.

Ugniježđeno podstablo
Podstablo unutar repliciranog podstabla direktorija.

Ravnopravan poslužitelj
Termin koji se koristi za glavnog poslužitelja kada postoji više glavnih poslužitelja za dano podstablo.

Ugovor replikacije
Informacije sadržane u direktoriju koji definira ’vezu’ ili ’stazu replikacije’ između dva poslužitelja. Jedan poslužitelj se naziva dobavljač (onaj koji šalje promjene), a drugi potrošač (onaj koji prima promjene). Ugovor sadrži sve informacije koje su potrebne za uspostavljanje veze od dobavljača do potrošača i raspoređivanje replikacije.

Kontekst replikacije
Identificira korijen podstabla replikacije. ibm-replicationContext pomoćna klasa objekta se može dodati na

unos kako bi ga se označilo kao korijen repliciranog područja. Informacije koje se odnose na topologiju replikacije se održavaju u skupu unosa kreiranih pod kontekstom replikacije.

Grupa replike
Prvi unos koji je kreiran pod kontekstom replikacije ima klasu objekta ibm-replicaGroup i predstavlja zbirku poslužitelja koji sudjeluju u replikaciji. Osigurava prikladnu lokaciju za postavljanje ACL-ova kako bi se zaštitile informacije o topologiji replikacije. Administracijski alati trenutno podržavaju jednu grupu replike pod svakim kontekstom replikacije pod imenom **ibm-replicagroup=default**.

Podstablo replike
Ispod unosa grupe replike se može kreirati jedan ili više unosa s objectclass ibm-replicaSubentry; jedan za svaki poslužitelj koji sudjeluje u replikaciji kao dobavljač. Podstablo replike identificira ulogu koju poslužitelj ima u replikaciji: glavni ili samo za čitanje. Poslužitelj samo za čitanje bi mogao imati ugovore replikacije koji podržavaju kaskadnu replikaciju.

Replicirano podstablo
Dio DIT-a koje je bilo replicirano iz jednog poslužitelja na drugi. Pod ovim oblikovanjem, dano podstablo se može replicirati na neke poslužitelje, a ne može se na druge. Na podstablo se može pisati na danom poslužitelju, dok ostala stabla mogu biti samo za čitanje.

Raspored
Replikacija može biti raspoređena tako da se događa u određeno vrijeme s prikupljenim promjenama na dobavljaču poslanim u paketu. Ugovor replike sadrži DN za unos koji dobavlja raspored.

Poslužitelj dobavljača
Poslužitelj koji šalje promjene na drugi poslužitelj (potrošač).

Ugovori replikacije

Ugovor replikacije je unos u direktorij s klasom objekta **ibm-replicationAgreement** koja je kreirana ispod podunosa replike za definiranje replikacije iz poslužitelja kojeg predstavlja podunos na drugi poslužitelj. Ti objekti su slični unosima replicaObject koji koriste prethodne verzije Poslužitelja direktorija. Ugovor replikacije se sastoji od sljedećih stavki:

- Ime prilagođeno korisniku koje se koristi kao atribut imenovanja za ugovor.
- Trebao bi se koristiti LDAP URL koji specificira poslužitelja, broj porta i to da li bi se trebao koristiti SSL.
- Id poslužitelja potrošača, ako je poznat. Poslužitelji direktorija prije V5R3 nemaju id poslužitelja.
- DN objekta koji sadrži vjerodajnice koje koristi dobavljač kako bi se povezao na potrošača.
- Neobavezni DN pointer na objekt koji sadrži informacije raspoređivanja replikacije. Ako atribut nije prisutan, promjene se odmah repliciraju.

Ime prilagođeno korisniku može biti ime poslužitelja potrošača ili neki drugi opisni niz.

Id poslužitelja potrošača se koristi od strane administrativnog GUI-a kako bi se prenijela topologija. Na temelju ID-a poslužitelja potrošača, GUI može pronaći odgovarajući podunos i njegove ugovore. Kao pomoć pri poboljšanju točnosti podataka, kada se dobavljač veže na potrošača, on vraća ID poslužitelja s ishodištem DSE-a i uspoređuje ga s vrijednosti u ugovoru. Ako se ne podudaraju ID-evi poslužitelja, zapisuje se upozorenje.

Budući se ugovor replikacije može replicirati, koristi se DN na objektu vjerodajnice. To omogućava da se vjerodajnice mogu pohraniti u nerepliciranom području direktorija. Repliciranje objekata vjerodajnice (iz kojih se moraju moći dobaviti 'prazan tekst' vjerodajnice) predstavlja potencijalno sigurnosno izlaganje. Sufiks cn=localhost je odgovarajuća default lokacija za kreiranje objekata vjerodajnice.

Klase objekata su definirane za svaku od podržanih metoda provjere autentičnosti:

- Jednostavno vezanje
- SASL
- EXTERNAL mehanizam sa SSL-om
- Kerberos provjera autentičnosti

Možete označiti da dio repliciranog podstabla neće biti repliciran dodavanjem ibm-replicationContext pomoćne klase na korijen podstabla, bez da se definira bilo koje podstablo replike.

Bilješka: Alat Web administracije se odnosi na ugovor kao 'redovi' kod pozivanja na skup promjena koje čekaju da budu zamijenjene pod danim ugovorom.

Kako se informacije replikacije pohranjuju u poslužitelju

Informacije replikacije se pohranjuju u direktoriju na tri mjesta:

- Konfiguracija poslužitelja, koja sadrži informacije o tome kako se drugi poslužitelji mogu ovlastiti na tog poslužitelja i izvoditi replikaciju (na primjer, kome ovaj poslužitelj dopušta da se ponaša kao dobavljač).
- U direktoriju na vrhu repliciranog podstabla. Ako je ″o=my company″ na vrhu repliciranog podstabla, izravno ispod njega će se kreirati objekt pod imenom ″ibm-replicagroup=default″ (ibm-replicagroup=default,o=my company). Ispod ″ibm-replicagroup=default″ objekta će biti dodatni objekti koji opisuju poslužitelje koji sadrže replike podstabla i ugovore između poslužitelja.
- Objekt pod imenom ″cn=replication,cn=localhost″ se koristi za sadržavanje informacija o replikaciji koje koristi samo jedan poslužitelj. Na primjer, objekt sadrži vjerodajnice koje koristi poslužitelj dobavljača, a koje su potrebne samo za poslužitelja dobavljača. Vjerodajnice se mogu smjestiti pod ″cn=replication,cn=localhost″ čime one postaju dostupne samo preko tog poslužitelja.

Sigurnosna razmatranja o informacijama replikacije

Pregledajte sigurnosna razmatranja za sljedeće objekte:

- ibm-replicagroup=default: Kontrole pristupa na tom objektu kontroliraju tko može pregledati ili promijeniti ovdje pohranjene informacije replikacije. Po defaultu, taj objekt nasljeđuje kontrolu pristupa iz svojeg nadređenog. Trebali bi razmotriti postavljanje kontrole pristupa na taj objekt kako bi se ograničio pristup informacijama o replikaciji. Na primjer, mogli bi definirati grupu koja sadrži korisnike koji će upravljati replikacijom. Ta grupa bi mogla postati vlasnik objekta ″ibm-replicagroup=default″ i drugim korisnicima bi se mogao onemogućiti pristup na objekt.
- cn=replication,cn=localhost: Postoje dva razmatranja sigurnosti za taj objekt:
  - Kontrola pristupa na objekt kontrolira tko smije pregledati ili ažurirati ovdje pohranjene objekte. Default kontrola korisnika omogućava anonimnim korisnicima da pročitaju većinu informacija osim lozinki i traži ovlaštenje administratora za dodavanje, promjenu ili brisanje objekta.
  - Objekti koji su pohranjeni u ″cn=localhost″ se nikad ne repliciraju na druge poslužitelje. Vjerodajnice replikacije možete smjestiti u spremnik na poslužitelju koji koristi vjerodajnicu i one neće biti dostupne drugim poslužiteljima. Alternativno, možete izabrati da ćete smjestiti vjerodajnice pod ″ibm-replicagroup=default″ objekt tako da više poslužitelja dijeli iste vjerodajnice.

Područja i predlošci korisnika

Objekti područja i predloška koji se nalaze u Web administracijskom alatu se koriste kako bi se oslobodilo korisnika potrebe razumijevanja nekih od najvažnijih LDAP pitanja.

Područje identificira zbirku korisnika i grupa. Ono specificira informacije u plosnatoj strukturi direktorija, kao što su lokacija korisnika i lokacija grupa. Područje definira lokaciju za korisnike (na primjer, ″cn=users,o=acme,c=us″) i kreira korisnike kao neposredno zavisne tom unosu (na primjer John Doe se kreira kao ″cn=John Doe,cn=users,o=acme,c=us″). Možete definirati više područja i dati im poznata imena (na primjer Web korisnici). Poznato ime mogu koristiti ljudi koji kreiraju i održavaju korisnike.

Predložak opisuje kako izgleda korisnik. On specificira objectclasses koje se koriste kada se kreiraju korisnici (strukturalna objectclass i bilo koje pomoćne klase koje želite). Predložak isto tako specificira izgled panela koji se koriste za kreiranje ili uređivanje korisnika (na primjer, imena kartica, default vrijednosti i atributi koji će se pojaviti na svakoj kartici).

Kada dodate novo područje, vi kreirate objekt ibm-područja u direktoriju. Objekt ibm-područja prati svojstva područja kao što su podaci o tome gdje su definirani korisnici i grupe i koji će se predložak koristiti. Objekt ibm-područja može

ukazivati na postojeći unos direktorija koji je nadređeni korisnicima ili može ukazivati na samog sebe (default) čineći se tako spremnikom za nove korisnike. Na primjer, možete imati postojeći cn=users,o=acme,c=us spremnik i kreirati područje pod imenom korisnici drugdje u direktoriju (možda u objektu spremnika pod nazivom cn=realms,cn=admin stuff,o=acme,c=us) koji identificira cn=users,o=acme,c=us kao lokaciju za korisnike i grupe. Time se kreira objekt ibm-područja:

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

Ili, ako nije bilo postojećeg cn=users,o=acme,c=us objekta, možete kreirati područje korisnici pod o=acme,c=us i to tako da ukazuje na samog sebe.

Administrator direktorija je odgovoran za upravljanje predloškom korisnika, područjem i grupama administracije područja. Nakon što se kreira područje, članovi te grupe administratora područja su odgovorni za upravljanje korisnicima i grupama unutar područja.

Za više informacija o tome kako se treba upravljati područjima i predlošcima korisnika, pogledajte “Upravljanje područjima i predlošcima korisnika” na stranici 138.

Pitanja podrške nacionalnim jezicima (NLS)

Vodite računa o sljedećim NLS razmatranjima:

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

Za više informacija o UCS-2, pogledajte “Globalizacija” u poglavlju Planiranje.

Referali LDAP direktorija

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

Poslužitelj direktorija vam omogućuje da koristite dva različita tipa referala. Možete specificirati default referalne poslužitelje gdje će LDAP poslužitelj referencirati klijente uvijek kada neki DN nije u direktoriju. Možete isto tako koristiti svojeg LDAP klijenta kako bi dodali unos u poslužitelj direktorija koji ima objectClass referal. Ovo vam omogućuje da odredite referalne poslužitelje koji se temelje na specifičnom DN-u koji neki klijent zahtijeva.

Bilješka: S Poslužitelj direktorija, objekti referala moraju sadržavati samo razlikovno ime (dn), objectClass (objectClass) i referalni (ref) atribut. Pogledajte “ldapsearch” na stranici 169 kako bi dobili primjere koji prikazuju to ograničenje.

Referalni poslužitelji su blisko povezani s replika poslužiteljima. S obzirom na to da se podaci na replika poslužiteljima ne mogu mijenjati iz klijenata, replika upućuje sve zahtjeve za promjenu podataka direktorija glavnom poslužitelju.

Transakcije

Možete konfigurirati Poslužitelj direktorija kako bi omogućili klijentima da koriste transakcije. (Za više informacija o postavkama transakcijama, pogledajte “Specificiranje postavki transakcije” na stranici 95.) Transakcija je grupa operacija LDAP direktorija koje se tretiraju kao jedna jedinica. Nijedna od pojedinačnih LDAP operacija koje čine transakciju nisu trajne dok se sve operacije u transakciji ne dovrše uspješno i transakcija je predana. Ako bilo koja operacija ne uspije ili je transakcija opozvana, ostale operacije se poništavaju. Ova sposobnost može pomoći korisnicima da LDAP operacije budu organizirane. Na primjer, korisnik može postaviti transakciju na klijenta koji će obrisati nekoliko unosa u direktorij. Ako klijent izgubi vezu s poslužiteljem u toku transakcije, niti jedan unos nije obrisan. Tako korisnik može jednostavno započeti transakciju ponovo, a ne provjeravati koji su unosi uspješno obrisani.

Sljedeće LDAP operacije mogu biti dio transakcije:

- dodavanje
- promjena
- promjena RDN
- brisanje

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

Poslužitelj direktorija - Sigurnost

Pogledajte sljedeće poglavlje za više informacija o sigurnosti Poslužitelja direktorija:

- “Revizija”
- “Sloj sigurnih utičnica (SSL) i Sigurnost sloja transporta s Poslužiteljem direktorija” na stranici 41
- “Kerberos provjera autentičnosti s Poslužiteljem direktorija” na stranici 41)
- “Grupe i uloge” na stranici 42
- “Lista kontrole pristupa” na stranici 47
- “Vlasništvo nad objektima LDAP direktorija” na stranici 58
- “Politika lozinke” na stranici 59
- “Provjera autentičnosti” na stranici 62

Revizija

Poslužitelj direktorija podržava OS/400 reviziju sigurnosti. Stavke podložne reviziji uključuju sljedeće:

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

Možda ćete trebati učiniti promjene na vašim i5/OS revizijskim postavkama prije nego će revizija unosa u direktorij proraditi. Ako sistemska vrijednost QAUDCTL ima specificirano *OBJAUD, možete omogućiti reviziju objekata kroz iSeries Navigator. Za više informacija o reviziji pogledajte poglavlje *Sigurnost - Referenca*  ili “Revizija sigurnosti”.

Sloj sigurnih utičnica (SSL) i Sigurnost sloja transporta s Poslužiteljem direktorija

Da bi vaša komunikacija s Poslužiteljem direktorija bila sigurnija, Poslužitelj direktorija može koristiti sigurnost Sloja sigurnih utičnica (SSL).

Za upotrebu SSL-a s Poslužitelj direktorija, morate imati proizvode Dobavljača kriptografičkog pristupa (5722-ACx) instalirane na vašem sistemu. Ako želite koristiti SSL iz iSeries Navigator, morate također imati instaliran jedan od proizvoda Client Encryption (5722-CEx) na vašem PC-u. Ovaj softver je potreban ako želite raditi nešto od sljedećeg:

- Konfigurirati i administrirati Poslužitelj direktorija iz svoje radne stanice pomoću SSL veze. To obuhvaća poslove koje izvodite iz iSeries Navigator.
- Koristiti SSL veze s aplikacijama koje kreirate sa sučeljem LDAP programa aplikacije klijenta (API-ji).

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

Za upotrebu SSL-a, morate imati Upravitelja digitalnih certifikata (DCM), opciju 34 za i5/OS instaliranu na vašem sistemu. DCM pruža sučelje preko kojega možete kreirati i upravljati digitalnim certifikatima i spremištima certifikata. Pogledajte poglavlje “Upravitelj digitalnih certifikata” kako bi dobili informacije o digitalnim certifikatima i korištenju DCM-a. Za više informacija o SSL-u na iSeries, pogledajte poglavlje “Sloj sigurnih utičnica (SSL)”. Za informacije o TLS na iSeries poslužitelju, pogledajte Podržani protokoli za SSL i Sigurnost transportnog sloja (TLS).

Kerberos provjera autentičnosti s Poslužiteljem direktorija

Poslužitelj direktorija omogućava vam da koristite Kerberos provjeru autentičnosti. Kerberos je mrežni protokol za provjeru autentičnosti koji koristi tajni ključ šifriranja da omogući dobru provjeru ovlaštenja za klijent/poslužitelj aplikacije.

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

Kerberos podrška za Poslužitelj direktorija osigurava podršku za GSSAPI SASL mehanizam. Ovo omogućuje i Poslužitelju direktorija i Windows 2000 LDAP klijentima upotrebu Kerberos provjere autentičnosti pomoću Poslužitelja direktorija.

Kerberos osnovno ime koje poslužitelj koristi ima sljedeći oblik:

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

service-name je ldap (ldap mora sadržavati mala slova), host-name je potpuno kvalificirano TCP/IP ime sistema, a realm je default područje specificirano u konfiguraciji Kerberos sistema.

Na primjer, kod sistema pod imenom my-as400 u acme.com TCP/IP domeni s default Kerberos područjem ACME.COM, Kerberos ime principala LDAP poslužitelja bi bilo ldap/my-as400.acme.com@ACME.COM. Default Kerberos područje je specificirano u Kerberos konfiguracijskoj datoteci (po defaultu, /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) s default_realm direktivom (default_realm = ACME.COM). Poslužitelj direktorija ne može biti konfiguriran da koristi Kerberos provjeru autentičnosti ako default područje nije konfigurirano.

Kada se koristi Kerberos provjera autentičnosti, Poslužitelj direktorija pridružuje razlikovno ime (DN) vezi koja određuje pristup podacima direktorija. Možete izabrati da DN poslužitelja bude pridruženo jednoj od sljedećih metoda:

- Poslužitelj može kreirati DN na osnovi Kerberos ID-a. Kad izaberete ovu opciju, Kerberos identitet oblika principal@realm generira DN oblika ibm-kn=principal@realm. ibm-kn= je ekvivalent za ibm-kerberosName=.

- Poslužitelj može pretražiti direktorij za razlikovno ime (DN) koje sadrži unos za Kerberos osnovu i područje. Kada izaberete tu opciju, poslužitelj traži u direktoriju unos koji specificira taj Kerberos identitet.

Morate imati datoteku tablice ključeva (keytab) koja sadržava ključ za osnove LDAP usluge. Pogledajte poglavlje u Informacijski Centar Usluge mrežne provjere autentičnosti pod Sigurnost za više informacija o Kerberosu na iSeries poslužitelju. Odlomak Konfiguriranje usluga mrežne provjere autentičnosti sadrži informacije o dodavanju informacija na datoteke tablice s ključem.

Grupe i uloge

Grupa je popis, zbirka imena. Grupa se može koristiti u **aclentry**, **ibm-fliterAclEntry** i **entryowner** atributima kako bi se kontrolirao pristup ili u aplikacijski-specificiranim korištenjima kao što je lista slanja poštom; pogledajte “Lista kontrole pristupa” na stranici 47. Grupe se mogu definirati kao statičke, dinamičke ili ugniježđene. Kako bi dobili informacije o tome kako se radi s grupama, pogledajte “Upravljanje korisnicima i grupama” na stranici 135.

Uloge su slične grupama u tome da su one prikazane u direktoriju od strane objekta. Osim toga, uloge sadržavaju grupe DN-ova.

Pogledajte sljedeće za više informacija:

- “Statičke grupe”
- “Dinamičke grupe”
- “Ugniježđene grupe” na stranici 44
- “Hibridne grupe” na stranici 44
- “Određivanje članstva grupe” na stranici 44
- “Klase objekta grupe za ugniježđene i dinamičke grupe” na stranici 46
- “Tipovi atributa grupe” na stranici 46
- “Uloge” na stranici 47

Statičke grupe

Statička grupa definira pojedinačno svakog člana korištenjem strukturalne klase objekata **groupOfNames**, **groupOfUniqueNames**, **accessGroup** ili **accessRole**; ili pomoćne klase objekata **ibm-staticgroup**. Te klase objekata traže atribut **member** (ili uniqueMember u slučaju groupOfUniqueNames). Statička grupa koja koristi **groupOfNames** ili **groupOfUniqueNames** strukturalne klase objekta mora imati barem jednog člana. Grupa koja koristi **accessGroup** ili **accessRole** strukturalnu klasu objekta može biti prazna. Statička grupa može biti definirana korištenjem pomoćne klase objekta: **ibm-staticGroup** koja ne traži **member** atribut i stoga može biti prazna.

Tipičan unos grupe je:

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

Svaki objekt grupe sadržava atribut s više vrijednosti koji se sastoji od DN-ova članova.

Nakon što se obriše grupa pristupa, grupa pristupa se briše i iz svih ACL-ova na kojim se je primijenila.

Dinamičke grupe

Dinamička grupa definira svoje članove drugačije nego statička grupa. Umjesto da se pojedinačno ispisuje, dinamička grupa definira svoje članove korištenjem LDAP pretraživanja. Dinamička grupa koristi strukturalnu klasu objekta **groupOfURLs** (ili pomoćnu klasu objekta **ibm-dynamicGroup**) i atribut, **memberURL** kako bi se definiralo pretraživanje pojednostavljene LDAP URL sintakse.

```
ldap:///<bazni DN pretraživanja> ? ? <opseg pretraživanja> ? <filter_pretraživanja>
```

Bilješka: Kako to primjer prikazuje, ime hosta ne smije biti prisutno u sintaksi. Preostali parametri su poput normalne ldap URL sintakse. Svako polje parametra mora biti odijeljeno s ?, čak i kada nije specificiran parametar. Normalno je popis atributa koji se vraća uključen između baznog DN-a i opsega pretraživanja. Taj parametar isto tako ne koristi poslužitelj kada određuje dinamičko članstvo, pa se može izostaviti, no odjelitelj **?** mora svejedno biti prisutan.

gdje je:

bazni DN pretraživanja
Točka od koje počinje pretraživanje u direktoriju. Ona može biti sufiks ili ishodište direktorija kao što je **ou=Austin**. Taj parametar je potreban.

opseg pretraživanja
Specificira raspon pretraživanja. Default opseg je bazni.

bazni Vraća informacije samo o baznom DN-u specificiranom u URL-u

jedan Vraća informacije o unosima jednu razinu ispod baznog DN-a specificiranog u URL-u. Ne uključuje bazni unos.

sub Vraća informacije o unosima na svim donjim razinama i uključuje bazni DN.

filter_pretraživanja
Da li je filter kojeg želite primijeniti na svim unosima unutar opsega pretraživanja. Pogledajte “opcija ldapsearch filtera” na stranici 172 kako bi dobili informacije o sintaksi filtera pretraživanja. Default je objectclass=*

Traženje dinamičkih članova je uvijek interno u poslužitelju, pa za razliku od potpunog ldap URL-a, ime hosta i broj porta nisu nikad specificirani, a protokol je uvijek **ldap** (nikad **ldaps**). Atribut **memberURL** može sadržavati bilo koji oblik URL-a, no poslužitelj koristi samo **memberURL**-ove koji počinju s **ldap:**/// kako bi odredio dinamičko članstvo.

Primjeri

Jedan unos u kojem se opseg postavlja na bazni, a filter se postavlja na objectclass=*:

```
ldap:///cn=John Doe, cn=Employees, o=Acme, c=US
```

Svi unosi koji su za 1-razinu ispod cn=Employees, a filter se postavlja na objectclass=*:

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

Svi unosi koji su ispod o-Acme s objectclass=person:

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

Ovisno o klasama objekta koje koristite za definiranje unosa korisnika, ti unosi možda neće sadržavati atribute koji su prikladni za određivanje članstva grupe. Možete koristiti pomoćnu klasu objekta, **ibm-dynamicMember**, kako bi proširili unose korisnika tako da uključuju **ibm-group** atribut. Taj atribut vam dozvoljava da dodate proizvoljne vrijednosti na svoje unose korisnika koji će služiti kao ciljevi za filtere vaših dinamičkih grupa. Na primjer:

Članovi te dinamičke grupe su unosi koji se nalaze izravno ispod cn=users,ou=Austin unosa koji imaju ibm-group atribut GROUP1:

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

Slijedi primjer člana cn=GROUP1,ou=Austin:

```
dn: cn=Group 1 member, cn=users, ou=austin
 objectclass: osoba
 objectclass: ibm-dynamicMember
 sn: member
 userpassword: memberpassword
 ibm-group: GROUP1
```

Ugniježđene grupe

Ugniježđavanje grupa omogućuje kreiranje hijerarhijskog odnosa koji se može koristiti kako bi se definirala naslijeđena članstva grupe. Ugniježđena grupa je definirana kao unos podređene grupe čiji je DN referenciran atributom sadržanim unutar unosa nadređene grupe. Nadređena grupa je kreirana proširivanjen jedne od klasa objekata strukturalne grupe (**groupOfNames**, **groupOfUniqueNames**, **accessGroup**, **accessRole** ili **groupOfURLs**) s dodavanjem **ibm-nestedGroup** pomoćne klase objekta. Nakon proširenja ugniježđene grupe, može se dodati nula ili više **ibm-memberGroup** atributa s njihovim vrijednostima postavljenim na DN-ove ugniježđenih podređenih grupa. Na primjer:

```
dn: cn=Group 2, cn=Groups, o=IBM, c=US
 objectclass: groupOfNames
 objectclass: ibm-nestedGroup
 objectclass: top
 cn: Group 2
 description: Grupa koja se sastoji od statičkih i ugniježđenih članova.
 member: cn=Person 2.1, cn=Dept 2, cn=Employees, o=IBM, c=US
 member: cn=Person 2.2, cn=Dept 2, cn=Employees, o=IBM, c=US
 ibm-memberGroup: cn=Group 8, cn=Nested Static, cn=Groups, o=IBM, c=US
```

Nije dozvoljeno uvođenje ciklusa u hijerarhiji ugniježđene grupe. Ako se utvrdi da je operacija ugniježđene grupe rezultirala cikličkom referencom, bilo izravno ili preko nasljeđivanja, to se smatra povredom ograničenja i stoga neće uspjeti pokušaj ažuriranja unosa.

Hibridne grupe

Sve klase objekta strukturalne grupe se mogu proširiti tako da je članstvo grupe opisano kombinacijom statičkih, dinamičkih i ugniježđenih tipova člana. Na primjer:

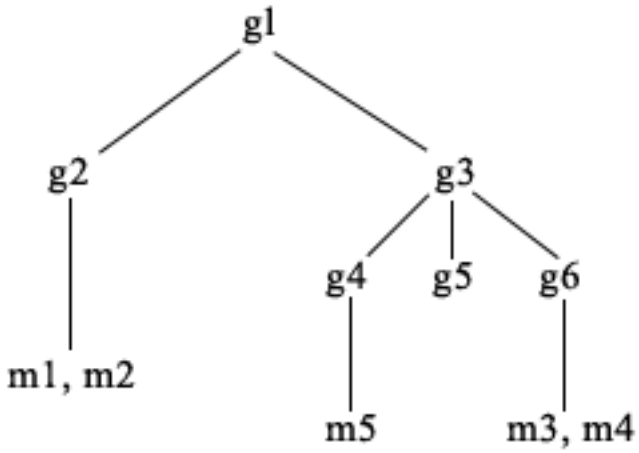
```
dn: cn=Group 10, cn=Groups, o=IBM, c=US
 objectclass: groupOfURLs
 objectclass: ibm-nestedGroup
 objectclass: ibm-staticGroup
 objectclass: top
 cn: Group 10
 description: Grupa koja se sastoji od statičkih, dinamičkih i ugniježđenih članova.
 memberURL: ldap:///cn=Austin, cn=Employees, o=IBM, c=US??one?objectClass=person
 ibm-memberGroup: cn=Group 9, cn=Nested Dynamic, cn=Groups, o=IBM, c=US
 member: cn=Person 10.1, cn=Dept 2, cn=Employees, o=IBM, c=US
 member: cn=Person 10.2, cn=Dept 2, cn=Employees, o=IBM, c=US
```

Određivanje članstva grupe

Dva operativna atributa se mogu koristiti kako bi se ispitalo nakupljeno članstvo grupe. Za dani unos grupe, **ibm-allMembers** operativni atribut nabraja skup nakupljenih članova grupe, uključujući statičke, dinamičke i ugniježđene članove kako to opisuje hijerarhija ugniježđene grupe. Za dani unos korisnika, **ibm-allGroups** operativni atribut nabraja skup nakupljenih grupa, uključujući grupe prethodnike u kojima taj korisnik ima članstvo.

Zahtjevatelj može primiti samo podskup ukupno zatraženih podataka, ovisno o tome kako su ACL-ovi bili postavljeni na podacima. Svatko može zatražiti **ibm-allMembers** i **ibm-allGroups** operativne atribute, ali vraćeni skup podataka sadrži samo podatke za LDAP unose i atribute na koje zahtjevatelj ima pravo. Korisnik koji traži **ibm-allMembers** ili **ibm-allGroups** atribut mora imati pristup vrijednostima atributa **member** ili **uniquemember** za grupu i ugniježđenu grupu kako bi se vidjeli statički članovi i mora biti u mogućnosti da izvodi pretraživanja specificirana u **memberURL** vrijednosti atributa kako bi se vidjeli dinamički članovi. Na primjer:

Primjeri hijerarhije



U ovom su primjeru **m1** i **m2** u atributu member od **g2**. ACL za **g2** omogućava **user1** da pročita atribut člana, no **user 2** nema pristup atributu member. Unos LDIF za **g2** unos je kako slijedi:

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

Unos **g4** koristi default aclentry koji omogućava **user1** i **user2** da pročita svoj member atribut. LDIF za **g4** unos je kako slijedi:

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

Unos **g5** je dinamička grupa koja dobiva svoja dva člana iz atributa memberURL. LDIF za **g5** unos je kako slijedi:

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

Unosi **m3** i **m4** su članovi grupe **g5** jer se podudaraju s **memberURL**. ACL za unos **m3** da ga traže i **user1** i **user2**. ACL za **m4** unose ne dopušta da ga traži **user2**. LDIF za **m4** je kako slijedi:

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

Primjer 1:

User 1 radi pretraživanje da bi dobavio sve članove grupe **g1**. User 1 ima pristup svim članovima tako da se oni svi vraćaju.

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


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

```
ibm-allmembers: CN=M2,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M3,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M4,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M5,CN=USERS,O=IBM,C=US
```

Primjer 2:

User 2 radi pretraživanje da bi dohvatio sve članove grupe **g1**. User 2 nema pristup članovima **m1** ili **m2** jer oni nemaju pristup atributu member za grupu **g2**. User 2 ima pristup atributu member za **g4** i stoga ima pristup članu **m5**. User 2 može izvoditi pretraživanje u grupi **g5** memberURL za unos **m3**, tako da su članovi ispisani ali ne mogu izvoditi pretraživanje za **m4**.

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


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

Primjer 3:

User 2 radi pretraživanje da bi vidio da li je **m3** član grupe **g1**. User 2 ima pristup za to pretraživanje, pa pretraživanje prikazuje da je **m3** član grupe **g1**.

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


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

Primjer 4:

User 2 radi pretraživanje da bi vidio da li je **m1** član grupe **g1**. User 2 nema pristup atributu member, tako da pretraživanje ne prikazuje da je **m1** član grupe **g1**.

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


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

Klase objekta grupe za ugniježđene i dinamičke grupe

ibm-dynamicGroup

Ta pomoćna klasa dopušta neobavezan **memberURL** atribut. Koristite ga sa strukturalnom klasom kao što je **groupOfNames** kako bi kreirali hibridnu grupu sa statičkim i dinamičkim članovima.

ibm-dynamicMember

Ta pomoćna klasa dopušta neobavezan **ibm-group** atribut. Koristite ga kao atribut filtera za dinamičke grupe.

ibm-nestedGroup

Ta pomoćna klasa dopušta neobavezan **ibm-memberGroup** atribut. Koristite ga sa strukturalnom klasom kao što je **groupOfNames** kako bi omogućili da se podgrupe ugnijezde unutar nadređene grupe.

ibm-staticGroup

Ta pomoćna klasa dopušta neobavezan **member** atribut. Koristite ga sa strukturalnom klasom kao što je **groupOfURLs** kako bi kreirali hibridnu grupu sa statičkim i dinamičkim članovima.

Bilješka: **ibm-staticGroup** je jedina klasa kod koje je **member** *neobavezan*, sve druge klase koje imaju **member** traže da postoji barem jedan 1 član.

Tipovi atributa grupe

ibm-allGroups

Prikazuje sve grupe kojima pripada unos. Unos može biti član izravno preko **member**, **uniqueMember** ili **memberURL** atributa ili neizravno preko **ibm-memberGroup** atributa. Taj **Samo za čitanje** operativni atribut nije dozvoljen u filteru pretraživanja. Atribut **ibm-allGroups** se može koristiti u zahtjevu za

uspoređivanjem kako bi se odredilo da li je unos član date grupe. Na primjer, kako bi odredili da li je ″cn=john smith,cn=users,o=my company″ član grupe ″cn=system administrators, o=my company″:

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

ibm-allMembers
Prikazuje sve članove grupe. Unos može biti član izravno preko **member**, **uniqueMember** ili **memberURL** atributa ili neizravno preko **ibm-memberGroup** atributa. Taj **Samo za čitanje** operativni atribut nije dozvoljen u filteru pretraživanja. Atribut **ibm-allMembers** se može koristiti u zahtjevu za uspoređivanjem kako bi se utvrdilo da li je DN član dane grupe. Na primjer, kako bi odredili da li je ″cn=john smith,cn=users,o=my company″ član grupe ″cn=system administrators, o=my company″:

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

ibm-group
je atribut kojeg uzima pomoćna klasa **ibm-dynamicMember**. Koristite ga kako bi definirali arbitrarne vrijednosti za kontroliranje članstva unosa u dinamičkim grupama. Na primjer, dodajte vrijednost ″Kuglački tim″ kako bi uključili unos u bilo koji **memberURL** koji ima filter ″ibm-group=Kuglački tim″.

ibm-memberGroup
je atribut kojeg uzima pomoćna klasa **ibm-nestedGroup**. Identificira podgrupe unosa nadređene grupe. Članovi svih takvih podgrupa se smatraju članovima nadređene grupe kada se obrađuju ACL-ovi ili **ibm-allMembers** i **ibm-allGroups** operativni atributi. Sami unosi podgrupe *nisu* članovi. Ugniježđeno članstvo je rekurzivno.

member
Identificira razlikovna imena za svakog člana grupe. Na primjer: member: cn=John Smith, dc=ibm, dc=com.

memberURL
Identificira URL koji je pridružen svakom članu grupe. Može se koristiti bilo koji tip označenog URL-a. Na primjer: memberURL: ldap:///cn=jsmith,dc=ibm,dc=com.

uniquemember
Identificira grupu imena koja su pridružena unosu, gdje je svakom imenu dan jedinstven identifikator kako bi se osigurala njegova jedinstvenost. Vrijednost za uniqueMember je DN kojeg slijedi uniqueIdentifier. Na primjer: uniqueMember: cn=John Smith, dc=ibm, dc=com 17.

Uloge

Autorizacija zasnovana na ulozi je konceptualan dodatak autorizaciji zasnovanoj na grupi i u nekim je slučajevima korisna. Kao član uloge, imate ovlaštenje da napravite ono što je potrebno za ulogu kako bi se obavio posao. Za razliku od grupe, uloga dolazi s uključenim skupom dozvola. Postoji ugrađena pretpostavka o tome koje se dozvole dobivaju (ili gube) članstvom u grupi.

Uloge su slične grupama u tome da su one prikazane u direktoriju od strane objekta. Osim toga, uloge sadržavaju grupe DN-ova. Uloge koje će se koristiti u kontroli pristupa moraju imati klasu objekta ’AccessRole’. ’Accessrole’ klasa objekta je podklasa ’GroupOfNames’ klase objekta.

Na primjer, ako postoji zbirka DN-ova kao što je ’sys admin’, vaša prva reakcija bi mogla biti da ih smatrate ’sys admin group’ (budući su grupe i korisnici najpoznatiji tipovi atributa privilegije). No, budući postoji skup dozvola koje očekujete da ćete primiti kao člana od ’sys admin’, zbirka DN-ova bi mogla biti točnije definirana kao ’sys admin role’.

Lista kontrole pristupa

Liste kontrole pristupa (ACL-ovi) sadrže sredstvo za zaštitu informacija pohranjenih u LDAP direktoriju. Administratori koriste ACL-ove kako bi ograničili pristup različitim dijelovima direktorija ili određenim unosima direktorija. Promjene na svakom unosu i atributu u direktoriju se mogu kontrolirati korištenjem ACL-ova. ACL za dani unos ili atribut se može naslijediti iz svojeg nadređenog unosa ili se može izričito definirati.

Najbolje je da oblikujete svoju strategiju kontrole pristupa kreiranjem grupa korisnika koje ćete koristiti kada ćete postavljati pristup za objekte i atribute. Postavite vlasništvo i pristup na najveću moguću razinu u drvu i ostavite da se kontrole nasljeđuju niz drvo.

Operativni atributi pridruženi kontroli pristupa, kao što su entryOwner, ownerSource, ownerPropagate, aclEntry, aclSource i aclPropagate su neobični po tome da su logički pridruženi svakom objektu, no mogu imati vrijednosti koje ovise o drugim objektima koji se nalaze više na stablu. Ovisno o tome kako su postavljene, te vrijednosti atributa mogu biti izričite na objektu ili naslijeđene od prethodnika.

Model kontrole pristupa definira dva skupa atributa: Informacije o kontroli pristupa (ACI) i entryOwner informacije. ACI definira pravila pristupanja koja su dana specificiranom subjektu s obzirom na operacije koje mogu izvoditi na objektima na koje se odnose. Atributi aclEntry i aclPropagate se odnose na ACI definiciju. Informacija entryOwner definira koji subjekti mogu definirati ACI za pridruženi objekt unosa. Atributi entryOwner i ownerPropagate se odnose na entryOwner definiciju.

Postoje dvije vrste lista kontrole pristupa koje možete izabrati: filter-zasnovani ACL-ovi i ne-filtrirani ACL-ovi. Ne-filtrirani ACL-ovi se odnose izravno na unos direktorija koji ih sadrži, ali se mogu proširiti na nijedan ili na sve njegove unose potomke. Filter-zasnovani ACL-ovi se razlikuju po tome što oni koriste filter-zasnovanu usporedbu upotrebom specificiranog filtera objekta za usporedbu ciljnih objekata sa stvarnim unosom koji se na njih odnosi.

Korištenjem ACL-ova administratori mogu ograničiti pristup na različite dijelove direktorija, određene unose direktorija i, na temelju imena atributa ili klase pristupa atributu, atribute sadržane u unosima. Svaki unos unutar LDAP direktorija ima skup pridruženih ACI-ja. U skladu s LDAP modelom, ACI i entryOwner informacije se prikazuju kao parovi atribut-vrijednost. Osim toga, LDIF sintaksa se koristi za administriranje tih vrijednosti. Ti atributi su:

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

Za informacije o tome kako se radi s ACL-ovima, pogledajte “Upravljanje listama kontrole pristupa (ACL-ovi)” na stranici 145. Za dodatne informacije pogledajte sljedeće:

- “Filtrirani ACL-ovi”
- “Sintaksa atributa kontrole pristupa” na stranici 49
- “AclEntry i ibm-filterAclEntry” na stranici 50
- “Vlasnik unosa” na stranici 52
- “Širenje” na stranici 52
- “Procjena pristupa” na stranici 53
- “Definiranje ACI-ja i vlasnika unosa” na stranici 54
- “Modificiranje vrijednosti ACI-ja i vlasnika unosa” na stranici 55
- “Brisanje vrijednosti ACI/vlasnik unosa” na stranici 57
- “Dohvaćanje vrijednosti ACI/vlasnik unosa” na stranici 58
- “Razmatranje replikacije podstabla” na stranici 58

Filtrirani ACL-ovi

Filter-zasnovani ACL-ovi koriste filter-zasnovanu usporedbu koja koristi specificirani filter objekta, kako bi se uparili ciljni objekti s efektivnim pristupom koji se na njih odnosi.

Filter-zasnovani ACL-ovi se nasljedno šire do svih usporedbom uparenih objekata u pridruženom podstablu. Iz tog razloga se aclPropagate atribut, koji se koristi da bi se zaustavilo širenje bez-filtriranih ACL-ova, ne odnosi na nove filter-zasnovane ACL-ove.

Default ponašanje filter-zasnovanih ACL-ova je da prikuplja od najniže sadržanog unosa, preko lanca unosa prethodnika, do unosa koji je sadržan na vrhu DIT-a. Učinkovit pristup se izračunava kao unija dodijeljenih ili odbijenih prava pristupa od strane sastavnih unosa prethodnika. Postoji iznimka od tog ponašanja. Kako bi se ostvarila kompatibilnost sa svojstvom replikacije podstabla i omogućila veća administrativna kontrola, atribut plafona se koristi kao sredstvo zaustavljanja skupljanja na unosu u kojem je sadržan.

Za filter-zasnovanu ACL-podršku se koristi novi skup atributa za kontrolu pristupa, umjesto da se spajaju filter-zasnovane karakteristike u postojeće bez-filtera zasnovane ACL-ove. Ti atributi su:

- ibm-filterAclEntry
- ibm-filterAclInherit

Atribut ibm-filterAclEntry ima isti format kao i aclEntry, uz dodatak u obliku komponente filtera objekta. Pridruženi atribut plafona je ibm-filterAclInherit. Po defaultu je postavljen na istinito. Kada je postavljen na lažno, on završava skupljanje.

Sintaksa atributa kontrole pristupa

Svakim od ovih atributa se može upravljati pomoću LDIF bilježenja. Sintaksa za nove atribute filter-zasnovanog ACL-a je modificirana verzija trenutnih atributa ne-filter-zasnovanog ACL-a. Sljedeće definira sintaksu za ACI i entryOwner atribute korištenjem baccus naur obrasca (BNF).

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

<aclPropagate> ::=  "true" | "false"
<ibm-filterAclEntry> ::=  <subject>  ":" <object filter>  [ ":"  <rights> ]

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

<ownerPropagate> ::= "true" | "false"

<subject> ::= <subjectDnType> ':' <subjectDn> |
                      <pseudoDn>

<subjectDnType> ::= "role" | "group" | "access-id"

<subjectDn> ::= <DN>

<DN> ::= razlikovno ime kako je to opisano u RFC 2251, odlomak 4.1.3.

<pseudoDn> ::= "group:cn=anybody" | "group:cn=authenticated" |
                       "access-id:cn=this"
<object filter> ::= filter pretraživanja niza kako je to definirano u RFC 2254, odlomak 4
                                (prošireno podudaranje nije podržano).
<rights> ::= <accessList> [":" <rights> ]

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

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

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

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

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

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

<attributeName> ::= ime za attributeType kako je to opisano u RFC 2251, odlomak 4.1.4.
                       (dozvoljeno je OID ili alfanumerički niz s izvornom
                        abecedom, "-" i ";")
```

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

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

<attributeClassAccess> ::= <class> ":" [<action> ":"]
                                     <attributePermissions>

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

AclEntry i ibm-filterAclEntry

Subjekt: Subjekt (entitet koji traži pristup kako bi operirao na objektu) se sastoji od kombinacije tipa DN-a (razlikovno ime) i DN-a. Valjani DN tipovi su: access-id, Grupa i Uloga.

DN identificira određeni access-id, ulogu ili grupu. Na primjer, subjekt može imati access-id: cn=personA, o=IBM ili grupu: cn=deptXYZ, o=IBM.

Budući je dvotočka (:) graničnik polja, DN koji sadržava dvotočke mora biti okružen s dvostrukim navodnicima (“”). Ako DN već sadrži znakove s dvostrukim navodnicima, ti znakovi se moraju izbjeći s obrnutom kosom crtom (\).

Sve grupe direktorija se mogu koristiti u kontroli pristupa.

Bilješka: Bilo koja grupa **AccessGroup**, **GroupOfNames**, **GroupofUniqueNames** ili **groupOfURLs** strukturalne klase objekta ili **ibm-dynamicGroup**, **ibm-staticGroup** pomoćne klase objekta se može koristiti za kontrolu pristupa.

Drugi DN tip koji se koristi unutar modela kontrole pristupa je uloga. Iako su uloge i grupe slične u primjeni, konceptualno se razlikuju. Kada se korisniku dodijeli uloga, postoji implicirano očekivanje da je potrebno ovlaštenje već bilo postavljeno kako bi se mogao izvoditi posao koji je pridružen toj ulozi. Kod članstva u grupi postoji ugrađena pretpostavka o tome koje su dozvole dobivaju (ili gube) članstvom u toj grupi.

Uloge su slične grupama u tome da su one prikazane u direktoriju od strane objekta. Osim toga, uloge sadržavaju grupe DN-ova. Uloge koje se koriste u kontroli pristupa moraju imati objectclass **AccessRole**.

Pseudo DN: LDAP direktorij sadrži nekoliko pseudo DN-ova. Oni se koriste kako bi se označio prevelik broj DN-ova koji u vrijeme vezivanja dijele zajedničke karakteristike u odnosu na operaciju koja se izvodi ili na ciljni objekt na kojem se izvodi operacija.

Trenutno su definirana tri pseudo DN-a:

group:cn=anybody
Odnosi se na sve subjekte, uključujući i one koji nisu ovlašteni. Svi korisnici automatski pripadaju toj grupi.

group:cn=authenticated
Odnosi se na bilo koje DN koje je ovlašteno za direktorij. Ne razmatra se metoda provjere autentičnosti.

access-id:cn=this
Odnosi se na DN povezivanja koje se podudara s DN-om ciljnog objekta na kojem se izvodi operacija.

Filter objekta: Taj parametar se odnosi samo na filtrirane ACL-ove. Filter pretraživanja niza, kako je to definirano u RFC 2254, se koristi kao format filtera objekta. Budući je ciljni objekt već poznat, niz se ne koristi za izvođenje stvarnog pretraživanja. Umjesto toga se izvodi filter-zasnovano uspoređivanje na ciljnom objektu kako bi se odredilo da li se dani skup ibm-filterAclEntry vrijednosti primjenjuje na njega.

Prava: Prava pristupa se mogu odnositi na cijeli objekt ili na atribute objekta. LDAP prava pristupa su diskretna. Jedno pravo ne implicira drugo pravo. Prava se mogu kombinirati kako bi se osigurala lista željenih prava koja slijedi

skup pravila koji će se kasnije objasniti. Prava se mogu sastojati od nespecificirane vrijednosti, a to označava da nisu dodijeljena prava pristupa subjektu na ciljnom objektu. Prava se sastoje od tri dijela:

Akcija:

Definirane vrijednosti su **dodijeli** ili **odbij**. Ako to polje nije prisutno, default je postavljen na **dodijeli**.

Dozvola:

Postoji šest osnovnih operacija koje se mogu izvoditi na objektu direktorija. Na temelju tih operacija se uzima bazni skup ACI dozvola. To su: dodaj unos, obriši unos, pročitaj vrijednost atributa, zapiši vrijednost atributa, traži atribut i usporedi vrijednost atributa.

Moguće dozvole atributa su: čitaj (r), piši (w), traži (s) i usporedi (c). Osim toga, dozvole objekta se odnose na unos u cjelini. Te dozvole su dodaj podređene unose (a) i obriši ovaj unos (d).

Sljedeća tablica sadrži sažetak dozvola koje su potrebne za izvođenje svake LDAP operacije.

Operacija	**Potrebna dozvola**
ldapadd	dodaj (na nadređenog)
ldapdelete	obriši (na objektu)
ldapmodify	zapiši (na atributima koji se modificiraju)
ldapsearch	• pretraži, čitaj (na atributima u RDN) • pretraži (na atributima specificiranim u filteru pretraživanja) • pretraži (na atributima vraćenim samo s imenima) • pretraži, čitaj (na atributima vraćenim s vrijednostima)
ldapmodrdn	zapiši (na RDN atributima)
ldapcompare	usporedi (na uspoređenom atributu)

Bilješka: Kod operacija pretraživanja subjekt mora imati pristup pretraživanja (s) za sve atribute u filteru pretraživanja ili se neće vratiti nijedan unos. Kod unosa vraćenih iz pretraživanja subjekt mora imati pristup pretraživanja (s) i čitanja (r) za sve atribute u RDN-u vraćenih unosa ili se ti unosi neće vratiti.

Cilj pristupa:

Te dozvole se mogu odnositi na cijeli objekt (dodaj podređeni unos, obriši unos), na pojedinačni atribut unutar unosa ili se mogu odnositi na grupe atributa (Klase pristupa atributu) kako je to dolje opisano.

Atributi koji traže slične dozvole za unos se zajedno grupiraju u klase. Atributi se mapiraju u njihove klase atributa u datoteci sheme direktorija. Te klase su diskretne; pristup jednoj klasi ne implicira pristup drugoj klasi. Dozvole su postavljene u odnosu na cijelu klasu pristupa atributu. Dozvole koje su postavljene na određenoj klasi atributa se odnose na sve atribute unutar te klase ako nisu specificirane pojedinačne dozvole pristupa atributu.

IBM definira tri klase atributa koje se koriste u procjeni pristupa atributima korisnika: **normalnu**, **osjetljivu** i **kritičnu**. Na primjer, atribut **commonName** spada u normalnu klasu, a atribut userpassword spada u kritičnu klasu. Korisnički definirani atributi pripadaju normalnoj klasi pristupa ako nije drugačije specificrano.

Definirane su i dvije druge klase pristupa: sistemska i ograničena. Atributi sistemske klase su:

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

To su atributi koje održava LDAP poslužitelj i njih mogu korisnici direktorija samo čitati. **OwnerSource** i **aclSource** su opisani u odlomku Širenje (pogledajte“Širenje” na stranici 52).

Ograničena klasa atributa koji definiraju kontrolu pristupa su:

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

Svi korisnici imaju pristup ograničenim atributima, ali samo **vlasnici unosa** mogu kreirati, promijeniti ili obrisati te atribute.

Bilješka: Atribut **ibm-effectiveAcl** je samo za čitanje.

Vlasnik unosa

Vlasnici unosa imaju potpunu dozvolu da izvode bilo koje operacije na objektu bez obzira na aclEntry. Osim toga, jedino vlasnici unosa smiju rukovati s aclEntry-jima za taj objekt. Vlasnik unosa je subjekt kontrole pristupa, on se može definirati kao pojedinci, grupe ili uloge.

Bilješka: Administrator direktorija je po defaultu jedan od vlasnika unosa za sve objekte u direktoriju, a vlasništvo nad unosom administratora direktorija se ne može ukloniti iz bilo kojeg objekta.

Širenje

Za unose na kojima je bio smješten aclEntry se smatra da imaju izričiti **aclEntry**. Slično tome, ako je **vlasnik unosa** bio postavljen na određenom unosu, taj unos ima izričitog vlasnika. To dvoje se ne isprepliće, unos s izričitim vlasnikom može, ali ne mora, imati izričiti **aclEntry**, a unos s izričitim **aclEntry** može imati izričitog vlasnika. Ako bilo koja od tih vrijednosti nije izričito prisutna na unosu, nedostajuća vrijednost se nasljeđuje iz čvora prethodnika u stablu direktorija.

Svaki izričiti **aclEntry** ili **entryOwner** se odnosi na unos na kojem je postavljen. Osim toga, vrijednost se može odnositi na sve potomke koji nemaju izričito postavljenu vrijednost. Te vrijednosti se smatraju raširenim; njihove se vrijednosti šire kroz stablo direktorija. Širenje određene vrijednosti se nastavlja tako dugo dok se ne dohvati druga vrijednost koja se širi.

Bilješka: Filter-zasnovani ACL-ovi se ne šire na način na koji se šire ne-filter-zasnovani ACL-ovi. Oni se šire do svih objekata uparenih uspoređivanjem u pridruženom podstablu. Pogledajte “Filtrirani ACL-ovi” na stranici 48 kako bi dobili više informacija o razlikama.

AclEntry i **entryOwner** mogu biti postavljeni tako da se odnose samo na određeni unos s vrijednosti širenja postavljenoj na ″false″ ili na unos i njegovo podstablo s vrijednosti širenja postavljenoj na ″true″. Iako se i **aclEntry** i **entryOwner** mogu širiti, njihovo širenje nije na bilo koji način povezano.

Atributi **aclEntry** i **entryOwner** dopuštaju više vrijednosti, no atributi širenja (**aclPropagate** i **ownerPropagate**) mogu imati samo jednu vrijednost za sve vrijednosti **aclEntry** ili **entryOwner** atributa unutar istog unosa.

Sistemski atributi **aclSource** i **ownerSource** sadrže DN učinkovitog čvora iz kojeg se procjenjuju **aclEntry** ili **entryOwner**. Ako takav čvor postoji, dodjeljuje se vrijednost **default**.

Definicije učinkovite kontrole pristupa objekta se mogu izvesti na temelju sljedeće logike:

- Ako postoji skup atributa izričite kontrole pristupa na objektu, onda je to definicija kontrole pristupa objekta.
- Ako ne postoje izričito definirati atributi kontrole pristupa, oni se prenose uz stablo direktorija dok se ne dosegne čvor prethodnik sa skupom širećih atributa kontrole pristupa.
- Ako nije pronađen nijedan takav čvor prethodnik, subjektu se dodjeljuje dolje opisani default pristup.

Administrator direktorija je vlasnik unosa. Pseudo grupi cn=anybody (svi korisnici) je dodijeljen pristup čitanja, pretraživanja i uspoređivanja nad atributima u normalnoj klasi pristupa.

Procjena pristupa

Pristup za određenu operaciju se dodjeljuje ili oduzima na temelju DN-a vezivanja subjekta za te operacije na ciljnom objektu. Obrađivanje se zaustavlja čim se može odrediti pristup.

Provjere pristupa se rade tako da se najprije pronađe učinkovita **entryOwnership** i **ACI** definicija, provjerava se vlasništvo nad unosom i onda se procjenjuju ASCI vrijednosti objekta.

Filter-zasnovani ACL-ovi se prikupljaju od najniže sadržanog unosa, uz lanac unosa prethodnika do najviše sadržanog unosa u DIT-u. Učinkovit pristup se izračunava kao unija dodijeljenih ili odbijenih prava pristupa od strane sastavnih unosa prethodnika. Postojeći skup pravila specificiranja i kombiniranja se koristi za procjenjivanje učinkovitog pristupa za filter zasnovane ACL-ove.

Filter-zasnovani i ne-filter-zasnovani atributi su međusobno isključivi unutar jednog sadržanog unosa direktorija. Nije dozvoljeno smještanje oba tipa atributa u isti unos i to se smatra povredom ograničenja. Operacije koje su pridružene kreiranju ili ažuriranju na direktoriju neće uspjeti ako se otkrije takvo stanje.

Kod izračunavanja učinkovitog pristupa, prvi ACL tip koji će se otkriti u lancu prethodnika unosa ciljnog objekta postavlja način izračunavanja. U filter-zasnovanom načinu, ne-filter-zasnovani ACL-ovi se zanemaruju kod izračunavanja učinkovitog pristupa. Isto tako, u ne filter-zasnovanom načinu se zanemaruju filter-zasnovani ACL-ovi kod izračunavanja učinkovitog pristupa.

Kako bi se ograničilo prikupljanje filter-zasnovanih ACL-ova kod izračunavanja učinkovitog pristupa, **ibm-filterAclInherit** atribut postavljen na vrijednost ″false″ se može smjestiti u unos između najvišeg i najnižeg pojavljivanja **ibm-filterAclEntry** u danom podstablu. To uzrokuje zanemarivanje podskupa **ibm-filterAclEntry** atributa iznad njega u lancu prethodnika ciljnog objekta.

U filter-zasnovanom ACL načinu, ako se ne primjenjuje filter-zasnovani ACL, primjenjuje se default ACL (cn=anybody - svatko ima dozvolu čitanja, pretraživanja i uspoređivanja atributa u normalnoj klasi pristupa). Ta se situacija može dogoditi kada se unos kojem se pristupa ne podudara s bilo kojim filterom specificiranim u **ibm-filterAclEntry** vrijednostima. Ako ne želite da se primjenjuje ta default kontrola pristupa, možda želite specificirati default filter ACL kao što je slijedi:

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

U tom primjeru se ne dodjeljuje nikakav pristup. Promijenite ga kako bi osigurali pristup kojeg želite primijeniti:

Po defaultu, administrator direktorija i glavni poslužitelj ili ravnopravni poslužitelj (za replikaciju) dobivaju potpuno pravo pristupa na sve objekte u direktoriju osim pristupa pisanja na atribute sistema. Drugi **vlasnici unosa** dobivaju potpuna prava pristupa objektima koji su pod njihovim vlasništvom osim pristupa pisanja na sistemske atribute. Svi korisnici imaju pravo pristupa čitanja na sistemskim i ograničenim atributima. Ta predefinirana prava se ne mogu mijenjati. Ako subjekt koji postavlja zahtjev ima **entryOwnership**, pristup se određuje gornjim default postavkama i zaustavlja se obrađivanje pristupa.

Ako subjekt koji postavlja zahtjev nije vlasnik objekta, onda se provjeravaju ACI vrijednosti za unose objekta. Prava pristupa se, kako je to definirano u ACI-ju za ciljni objekt, izračunavaju pravilima specificiranja i kombiniranja.

Pravilo specificiranja

Najodređenije aclEntry definicije su one koje se koriste u procjeni dozvola koje su dodijeljene/odbijene korisniku. Razine specificiranja su:

- Access-id je više određen od grupe ili uloge. Grupe i uloge su na istoj razini.
- Unutar iste **dnType** razine, pojedinačne dozvole razine atributa su određenije od dozvola razine klase atributa.
- Unutar iste razine atributa ili razine klase atributa, **odbijanje** je određenije od **dodjeljivanja**.

Pravilo kombiniranja

Dozvole koje su dodijeljene subjektima iste specificiranosti se kombiniraju. Ako se pristup ne može odrediti unutar iste razine specificiranosti, koriste se definicije pristupa od manje određene razine. Ako pristup nije određen nakon što su primijenjeni svi definirani ACI-ji, pristup se odbija.

Bilješka: Nakon što se u procjeni pristupa pronađe access-id **aclEntry** odgovarajuće razine, aclEntries razine grupe nisu uključeni u izračunavanje pristupa. Iznimka je u tome da ako su svi access-id **aclEntries** odgovarajuće razine definirani pod cn=this, onda se i svi **aclEntries** odgovarajuće razine grupe kombiniraju u procjeni.

Drugim riječima, unutar unosa objekta, ako definirani ACI unos sadrži access-id DN subjekta koji se podudara s DN-om povezivanja, onda se dozvole prvo procjenjuju zasnovano na tom aclEntry. Pod istim DN-om subjekta, ako su definirane podudarajuće dozvole razine atributa, one nadomještaju sve dozvole koje su definirane pod klasama atributa. Ako postoje sukobljujuće dozvole pod istom razinom definicije atributa ili klase atributa, odbijene dozvole nadjačavaju dodijeljene dozvole.

Bilješka: Definirana dozvola null vrijednosti sprječava uključenje manje specifične definicije dozvole.

Ako se pristup svejedno ne može odrediti, a svi pronađeni podudarajući aclEntry-ji su definirani pod ″cn=this″, onda se procjenjuje članstvo grupe. Ako korisnik pripada više nego jednoj grupi, korisnik prima kombinirane dozvole od tih grupa. Osim toga, korisnik automatski pripada cn=Anybody grupi, a možda i cn=Authenticated grupi ako je korisnik napravio ovlašteno vezanje. Ako su definirane dozvole za te grupe, korisnik prima specificirane dozvole.

Bilješka: Članstvo Grupa i Uloga se određuje za vrijeme vezanja i traje tako dugo dok ne nastupi drugo vezanje ili dok se ne primi zahtjev za odspajanjem. Ugniježđene grupe i uloge, to znači grupa ili uloga koja je definirana kao član druge grupe ili uloge, se ne rješavaju kod određivanja članstva niti kod procjene pristupa.

Na primjer, pretpostavimo da je attribute1 u osjetljivoj klasi atributa, a korisnik cn=Person A, o=IBM pripada grupama group1 i group2 s definiranim sljedećim aclEntry-ima:

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

Taj korisnik dobiva:

- Pristup ’rsc’ za attribute1, (iz 1. Definicija razine atributa nadomješta definiciju razine klase atributa).
- Ne dobiva pristup drugim atributima osjetljive klase u ciljnom objektu, (iz 1).
- Nisu dodijeljena nikakva druga prava (2 i 3 NISU uključeni u procjenu pristupa).

Kod drugog primjera sa sljedećim aclEntry-ima:

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

Korisnik:

- nema pristup atributima osjetljive klase, (iz 1. Null vrijednost definirana pod access-id sprječava uključivanje dozvole na atribute osjetljive klase iz group1).
- i ima pristup ’rsc’ atributima normalne klase (iz 2).

Definiranje ACI-ja i vlasnika unosa

Sljedeća dva primjera prikazuju administrativnu poddomenu koja se postavlja. Prvi primjer prikazuje jednog korisnika koji se dodjeljuje kao entryOwner za cijelu domenu. Drugi primjer prikazuje grupu koja je dodijeljena kao entryOwner.

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

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

Sljedeći primjer prikazuje kako se access-id ″cn=Person 1, o=IBM″ daje dozvola za čitanje, pretraživanje i uspoređivanje atributa attribute1. Dozvola se odnosi na bilo koji čvor u cijelom podstablu, na ili ispod čvora koji sadrži taj ACI, koji uspoređuje ″(objectclass=groupOfNames)″ filter usporedbe. Prikupljanje podudarajućih ibm-filteraclentry atributa u bilo kojim čvorovima prethodnicima je bilo završeno na tom unosu postavljanjem ibm-filterAclInherit atributa na ″false″.

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

ibm-filterAclInherit: false
```

Sljedeći primjer prikazuje kako se grupi ″cn=Dept XYZ, o=IBM″ daju dozvole za čitanje, pretraživanje i uspoređivanje atributa attribute1. Dozvole se odnose na cijelo podstablo ispod čvora koji sadrži taj ACI.

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

Sljedeći primjer prikazuje kako se ulozi ″cn=System Admins,o=IBM″ daju dozvole za dodavanje objekta ispod tog čvora i čitanje, pretraživanje i uspoređivanje atributa attribute2 i kritične klase atributa. Dozvole se odnose samo na čvor koji sadrži taj ACI.

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

Modificiranje vrijednosti ACI-ja i vlasnika unosa

Modificiraj-zamijeni

Modificiraj-zamijeni radi na isti način kao i svi drugi atributi. Ako vrijednost atributa ne postoji, kreirajte je. Ako vrijednost atributa postoji, zamijenite je.

Dani sljedeći ACI-ji za unos:

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

izvode sljedeće promjene:

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

Rezultirajući ACI je:

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

ACI vrijednosti za Dept ABC su izgubljene zamjenjivanjem.

Dani sljedeći ACI-ji za unos:

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

izvode sljedeće promjene:

```
dn: cn=some entry
changetype: modify
replace: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :grant:rsc

dn: cn=some entry
changetype: modify
replace: ibm-filterAclInherit
ibm-filterAclInherit: false
```

Rezultirajući ACI je:

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

ACI vrijednosti za Dept ABC su izgubljene zamjenjivanjem.

Modificiraj-dodaj

Ako za vrijeme ldapmodify-add ne postoji ACI ili entryOwner, ACI ili entryOwner se kreiraju s određenim vrijednostima. Ako postoji ACI ili entryOwner, onda dodajte određene vrijednosti za dani ACI ili entryOwner. Na primjer, dani ACI:

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

s preinakom:

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

bi proizveo aclEntry s više vrijednosti:

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

Na primjer, dani ACI:

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

s preinakom:

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

bi proizveo aclEntry s više vrijednosti:

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

Dozvole pod istim atributom ili klasom atributa se smatraju osnovnim građevnim blokovima, a akcije se smatraju kvalifikatorima. Ako se ista vrijednost dozvole dodaje više nego jednom, pohranjuje se samo jedna vrijednost. Ako se ista vrijednost dozvole dodaje više nego jednom s različitim vrijednostima akcije, koristi se posljednja vrijednost akcije. Ako je rezultirajuće polje dozvole prazno (″″), ta vrijednost dozvole je postavljena na null, a vrijednost akcije je postavljena na **dodijeli**.

Na primjer, ako je dan sljedeći ACI:

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

s preinakom:

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

proizvest će se aclEntry:

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

Na primjer, ako je dan sljedeći ACI:

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

s preinakom:

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

proizvest će se aclEntry:

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

Modificiraj-obriši

Kako bi obrisali određenu ACI vrijednost, koristite pravilnu ldapmodify-delete sintaksu.

Dani ACI:

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

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

proizvodi preostali ACI na poslužitelju :

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

Dani ACI:

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

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

proizvodi preostali ACI na poslužitelju :

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

Brisanje ACI ili entryOwner vrijednosti koja ne postoji rezultira s nepromijenjenim ACI ili entryOwner i vraća kod koji specificira da ne postoji vrijednost atributa.

Brisanje vrijednosti ACI/vlasnik unosa

S ldapmodify-obriši operacijom, entryOwner se može obrisati specificiranjem

```
dn: cn = neki unos
changetype: modify
delete: entryOwner
```

U ovom slučaju bi unos poprimio izričitog entryOwner. Automatski se uklanja i ownerPropagate. Taj unos bi naslijedio svojeg entryOwner iz čvora prethodnika u stablu direktorija u skladu s pravilom širenja.

Isto se može napraviti kako bi se aclEntry sasvim obrisao:

```
dn: cn = neki unos
changetype: modify
delete: aclEntry
```

Brisanje posljednje ACI ili entryOwner vrijednosti iz unosa nije isto kao i brisanje ACI-ja ili entryOwner. Unos može sadržavati ACI ili entryOwner bez vrijednosti. U tom se slučaju ništa ne vraća klijentu kada se ispituje ACI ili entryOwner, a postavka se širi na niže čvorove tako dugo dok se ne nadjača. Kako bi se spriječilo da postoje unosi kojima nitko ne može pristupiti, administrator direktorija uvijek ima puni pristup na unos čak i kada unos ima null ACI ili entryOwner vrijednost.

Dohvaćanje vrijednosti ACI/vlasnik unosa

Učinkovite ACI ili entryOwner vrijednosti se mogu jednostavno dohvatiti specificiranjem traženih ACL ili entryOwner atributa u pretraživanju, na primjer,

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

vraća sve ACL ili entryOwner informacije koje se koriste u procjeni pristupa objektu object A. Vodite računa o tome da možda neće sve vraćene vrijednosti izgledati točno onako kako su prvo definirane. Vrijednosti su ekvivalent originalnog obrasca.

Pretraživanje samo na ibm-filterAclEntry atributu vraća samo vrijednosti koje su specifične za sadržani unos.

Operativni atribut samo za čitanje, ibm-effectiveAcl, se koristi kako bi se prikazao prikupljeni učinkoviti pristup. Zahtjev pretraživanja za ibm-effectiveAcl vraća učinkoviti pristup koji se odnosi na ciljni objekt koji je zasnovan na: bez-filtera ACL-ovima ili filter ACL-ovima, ovisno o tome kako su oni bili distribuirani u DIT-u.

Budući bi filter-zasnovani ACL-ovi mogli proizaći iz nekoliko izvora prethodnika, pretraživanje na aclSource atributu proizvodi popis pridruženih izvora.

Razmatranje replikacije podstabla

Kako bi filter-zasnovan pristup bio uključen u replikaciju podstabla, svi ibm-filterAclEntry atributi moraju prebivati na pridruženom ibm-replicationContext unosu ili ispod njega.

Budući se učinkoviti pristup ne može prikupljati iz unosa prethodnika iznad repliciranog podstabla, ibm-filterAclInherit atribut mora biti postavljen na vrijednost **false** i prebivati na pridruženom ibm-replicationContext unosu.

Vlasništvo nad objektima LDAP direktorija

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

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

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

Za više informacija o radu sa svojstvima vlasništva, pogledajte “Upravljanje unosima direktorija” na stranici 129.

Politika lozinke

Kada se koriste LDAP poslužitelji za provjeru autentičnosti, važno je da LDAP poslužitelj podržava politike koje se odnose na istek dozvole, neuspjeli pokušaj prijave i pravila lozinke. Poslužitelj direktorija osigurava konfigurabilnu podršku za sve tri vrste politika. Ta politika se odnosi na sve unose direktorija koji imaju userPassword atribut. Ne možete definirati jednu politiku za jedan skup korisnika, a druge politike za druge skupove korisnika. Poslužitelj direktorija osigurava i mehanizam kojim će se klijenti obavijestiti o stanjima koja se odnose na lozinku (lozinka ističe kroz tri dana) i skup operativnih atributa koje administrator može koristiti za traženje takvih stvari kao što su korisnici s lozinkama koje su istekle ili korisnici sa zaključanim računima.

Za više informacija o tome kako treba raditi sa svojstvima politike, pogledajte “Postavljanje politike lozinke” na stranici 96.

Konfiguracija

Možete konfigurirati ponašanje poslužitelja s obzirom na lozinke u sljedećim područjima:

- Globalan ″on/off″ prekidač za omogućavanje i onemogućavanje politike
- Pravila za mijenjanje lozinki u koje spadaju:
  - Korisnici mogu promijeniti svoju lozinku. Vodite računa o tome da se ta politika primjenjuje kao dodatak bilo kojoj kontroli pristupa. Odnosno, kontrola pristupa mora dati korisniku ovlaštenje da promijeni userPassword atribut, kao i politiku lozinke koja omogućava korisnicima da promijene svoje vlastite lozinke. Ako je ta politika onesposobljena, korisnici ne mogu mijenjati svoje lozinke. Samo administrator ili drugi korisnik s ovlaštenjem za promjenu userPassword atributa može promijeniti lozinku za unos.
  - Lozinke se moraju promijeniti nakon resetiranja. Ako je ta politika omogućena, kada lozinku promijeni netko tko nije korisnik, lozinka se označava kao resetirana i korisnik ju mora promijeniti prije nego može izvoditi druge operacije direktorija. Zahtjev za vezanjem s resetiranom lozinkom je uspješan. Kako bi bili obaviješteni da se lozinka mora resetirati, aplikacija mora biti svjesna politike lozinke.
  - Korisnici moraju slati stare lozinke kada mijenjaju lozinku. Ako je ta politika omogućena, lozinka se može promijeniti samo zahtjevom za modificiranjem koji uključuje brisanje userPassword atributa (sa starom vrijednosti) i dodavanje nove userPassword vrijednosti. Time se osigurava da lozinku može promijeniti samo korisnik koji zna svoju lozinku. Administrator ili drugi korisnici koji su ovlašteni za promjenu userPassword atributa mogu uvijek postaviti lozinku.
- Pravila za istek lozinke u koje spadaju:
  - Lozinka nikad ne ističe ili lozinka ističe određeno vrijeme nakon što je zadnji put bila promijenjena.
  - Korisnici se ne obavještavaju kada ističe lozinka ili se korisnici upozoravaju na to određeno vrijeme prije nego lozinka istekne. Kako bi vas se obavijestilo da lozinka ističe, aplikacija mora biti svjesna politike lozinke.
  - Omogućen je određeni broj grace prijavljivanja nakon što istekne lozinka korisnika. Politika koja vodi računa o lozinki će biti obaviještena o broju preostalih grace prijavljivanja. Ako nisu dozvoljena grace prijavljivanja, korisnik ne može provjeriti autentičnost ili promijeniti svoju lozinku jednom kada ona istekne.
- Pravila za provjeru valjanosti u koja spadaju:
  - Konfigurabilna veličina lozinke povijesti koja govori poslužitelju da sačuva povijest posljednjih N lozinka i odbaci lozinke koji su se prethodno koristili.
  - Provjera sintakse lozinke koja uključuje postavljanje toga kako bi se poslužitelj trebao ponašati kada su lozinke raspršene. Ta postavka utječe na to da li bi poslužitelj trebao zamijeniti politiku pod bilo kojim od sljedećih uvjeta:
    - Poslužitelj pohranjuje raspršene lozinke.
    - Klijent predstavlja raspršenu lozinku poslužitelju (to se može dogoditi kada se prenose unosi između poslužitelja preko LDIF datoteke ako izvorni poslužitelj pohranjuje raspršene lozinke).

    U bilo kojem od tih slučaja poslužitelj možda neće moći primijeniti sva pravila sintakse. Podržana su sljedeća pravila sintakse: Minimalna dužina, minimalan broja znakova abecede, minimalan broj numeričkih ili posebnih znakova, broj ponovljenih znakova i broj znakova za koje se lozinka mora razlikovati od prethodne lozinke.
- Pravila za neuspjele lozinke u koja spadaju:

– Minimalno dozvoljeno vrijeme između mijenjanja lozinke koje sprječava da korisnik brzo prođe kroz skup lozinki i da se vrati natrag na svoju originalnu lozinku.
– Maksimalan broj neuspjelih pokušaja prijavljivanja prije nego se račun zaključa.
– Prilagodljivo trajanje zaključavanja lozinke. Nakon tog vremena se može koristiti prethodni zaključani račun. To može biti korisno kako bi se zaključao haker koji pokušava provaliti lozinku, a istovremeno je pomoć korisniku koji je zaboravio lozinku.
– Prilagodljivo vrijeme kroz koje poslužitelj prati neuspjele pokušaje prijavljivanja. Ako se unutar tog vremena dogodi maksimalan broj neuspjelih pokušaja prijavljivanja, račun je zaključan. Jednom kada to vrijeme istekne, poslužitelj odbacuje informacije o prethodnim neuspjelim pokušajima prijavljivanja na račun.

Postavke politike lozinke za poslužitelj direktorija su pohranjene u objektu ″cn=pwdpolicy″ koji izgleda kao:

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

Aplikacije koje vode računa o politici lozinke

Poslužitelj direktorija za podršku iSeries politike lozinke uključuje skup LDAP kontrola koje može koristiti aplikacija koja vodi računa o politici lozinke kako bi se primile informacije o dodatnim stanjima koji se odnose na politiku lozinke.

Aplikacija se može informirati o sljedećim stanjima upozorenja:

- Vrijeme koje je preostalo do isteka lozinke
- Broj preostalih grace prijava nakon što je lozinka istekla

Aplikacija se isto tako može informirati o sljedećim stanjima greške:

- Lozinka je istekla
- Račun je zaključan
- Lozinka je bila resetirana i mora se promijeniti
- Korisnik ne smije promijeniti svoju lozinku
- Prilikom mijenjanja lozinke se mora dobaviti stara lozinka
- Nova lozinka krši pravila sintakse
- Nova lozinka je prekratka
- Premalo je vremena prošlo od posljednjeg mijenjanja lozinke

- Nova lozinka je u povijesti

Koriste se dvije kontrole. Kontrola zahtjeva politike lozinke se koristi kako bi se informiralo poslužitelja da aplikacija želi biti informirana o stanjima koja se odnose na politiku lozinke. Tu kontrolu mora specificirati aplikacija nad svim operacijama za koje je zainteresirana, u pravilu je to početni zahtjev za vezanjem i svi zahtjevi za promjenom lozinke. Ako postoji kontrola zahtjeva politike lozinke, poslužitelj vraća kontrolu odgovora politike lozinke uvijek kada je prisutno bilo koje od gornjih stanja greške.

API-ji klijenta Poslužitelja direktorija sadrže skup API-ja koje mogu koristiti C aplikacije za rad s tim kontrolama. Ti API-ji su:

- ldap_parse_pwdpolicy_response
- ldap_pwdpolicy_err2string

Za aplikacije koje ne koriste te API-je, kontrole su definirane dolje. Morate koristiti sposobnosti koje osiguravaju LDAP klijent API-ji koji se koriste za obrađivanje kontrola. Na primjer, Java imenovanje i Sučelje direktorija (JNDI) imaju ugrađenu podršku za neke dobro poznate kontrole i također omogućuju građu za podršku kontrola koje JNDI ne prepoznaje.

Kontrola zahtjeva politike lozinke

```
Ime kontrole: 1.3.6.1.4.1.42.2.27.8.5.1
Kritičnost kontrole: FALSE
Vrijednost kontrole: Ništa
```

Kontrola odgovora politike lozinke

```
Ime kontrole: 1.3.6.1.4.1.42.2.27.8.5.1 (isto kao kontrola zahtjeva)
Kritičnost kontrole: FALSE
Vrijednost kontrole: BER kodirana vrijednost definirana u ASN.1 kako slijedi:
  PasswordPolicyResponseValue ::= SEQUENCE {
  warning [0] CHOICE OPTIONAL {
  timeBeforeExpiration [0] INTEGER (0 .. MaxInt),
  graceLoginsRemaining [1] INTEGER (0 .. maxInt) }
  error  [1] ENUMERATED OPTIONAL {
  passwordExpired   (0),
  accountLocked    (1),
  changeAfterReset   (2),
  passwordModNotAllowed (3),
  mustSupplyOldPassword (4),
  invalidPasswordSyntax (5),
  passwordTooShort   (6),
  passwordTooYoung   (7),
  passwordInHistory   (8) } }
```

Kao i drugi elementi LDAP protokola, BER kodiranje koristi implicitno označavanje.

Operativni atributi politike lozinke

Poslužitelj direktorija održava skup operativnih atributa za svaki unos koji ima userPassword atribut. Te atribute mogu tražiti ovlašteni korisnici, bilo korišteni u filterima pretraživanja ili vraćeni zahtjevom pretraživanja. Ti atributi su:

- pwdChangedTime - Atribut Općenitog vremena koji sadrži vrijeme kada je lozinka zadnji put bila promijenjena.
- pwdAccountLockedTime - Atribut Općenitog vremena koji sadrži vrijeme kada je račun bio zaključan. Ako račun nije zaključan, taj atribut nije prisutan.
- pwdExpirationWarned - Atribut Općenitog vremena koji sadrži vrijeme kada je prvi put klijentu bilo poslano upozorenje o isteku lozinke.
- pwdFailureTime - Atribut Općenitog vremena s više vrijednosti koji sadrži vremena prethodnih uzastopnih neuspjeha prijavljivanja. Ako je zadnje prijavljivanje bilo uspješno, taj atribut nije prisutan.
- pwdGraceUseTime - Atribut Općenitog vremena s više vrijednosti koji sadrži vremena prethodnih grace prijavljivanja.

- pwdReset - Booleov atribut koji sadrži vrijednost TRUE ako je lozinka bila resetirana pa ju korisnik mora promijeniti.

Replikacija Politike lozinke

Informacije politike lozinke poslužitelji dobavljača repliciraju za potrošače. Promjene na unosu cn=pwdpolicy se repliciraju kao globalne promjene, kao promjene na shemi. Repliciraju se i informacije o stanju politike lozinke za pojedinačne unose, tako da, ako je, na primjer, unos zaključan na poslužitelju dobavljača, ta akcija će se replicirati na bilo koje potrošače. No, promjene stanja politike lozinke na replici samo za čitanje se ne repliciraju na bilo koje druge poslužitelje.

Provjera autentičnosti

Kontrola pristupa unutar Poslužitelja direktorija je zasnovana na razlikovnom imenu (DN) koje je pridruženo danoj vezi. To DN je postavljeno kao rezultat vezanja na (prijavljivanje u) Poslužitelj direktorija.

Kada se Poslužitelj direktorija prvi puta konfigurira, sljedeći identeti se mogu koristiti kako bi se ovlastilo poslužitelja:

- anonimno
- administrator direktorija (cn=administrator po defaultu)
- projektirani i5/OS profil korisnika (pogledajte “Projicirana pozadina operacijskog sistema” na stranici 64)

Dobra ideja je kreiranje dodatnih korisnika kojima se može dati ovlaštenje za upravljanje različitim dijelovima direktorija bez da se traži da dijelite identitet administratora direktorija.

Iz LDAP perspektive postoje dvije okosnice za provjeru autentičnosti na LDAP-u:

- Jednostavno vezanje u kojem aplikacija osigurava DN i lozinku s praznim tekstom za taj DN
- Jednostavna provjera autentičnosti i Sigurnosni sloj (SASL) sadrži nekoliko dodatnih metoda provjere autentičnosti, uključujući CRAM-MD5, EXTERNAL, GSSAPI i OS400-PRFTKN.

Jednostavno vezanje (i CRAM-MD5)

Kako bi se koristilo jednostavno vezanje, klijent mora dobaviti DN postojećeg LDAP unosa i lozinku koja odgovara userPassword atributu za taj unos. Na primjer, mogli bi kreirati unos za John Smith kako slijedi:

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

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

Sada možete koristiti DN ″cn=John Smith,cn=users,o=acme,c=us″ u kontroli pristupa ili ga napraviti članom grupe korištene u kontroli pristupa.

Nekoliko predefiniranih klasa objekata omogućava da bude specificirana lozinka korisnika, uključujući (ali ne ograničavajući se na): person, organizationalperson, inetorgperson, organization, organizationalunit i druge.

Lozinke Poslužitelja direktorija su osjetljive na velika i mala slova. Ako kreirate unos s vrijednosti secret lozinke korisnika, neće uspjeti vezanje koje specificira lozinku SECRET.

Kod korištenja jednostavnog vezanja, klijent šalje lozinku s praznim tekstom na poslužitelja kao dio zahtjeva vezanja. To čini lozinku pogodnom za njuškanje razine protokola. SSL veza bi se mogla koristiti za zaštitu lozinke (sve informacije koje se šalju preko SSL veze su šifrirane). Ili se može koristiti CRAM-MD5 SASL metoda.

CRAM-MD5 metoda traži da svi poslužitelji imaju pristup na lozinku s praznim tekstom (zaštita lozinke je postavljena na ništa, a to u stvari znači da je lozinka pohranjena u obliku koji se može dešifrirati i vratiti kod pretraživanja kao prazan tekst). Klijent šalje DN na poslužitelja. Poslužitelj dohvaća vrijednost lozinke korisnika za unos i generira slučajan niz znakova. Slučajan niz znakova se šalje na klijenta. Klijent i poslužitelj raspršuju slučajan niz korištenjem lozinke kao ključa, a klijent šalje rezultat na poslužitelja. Ako se podudaraju dva raspršena niza, zahtjev za vezivanjem je uspješan, a lozinka nije nikad bila poslana na poslužitelja.

Kako bi se koristilo CRAM-MD5, poslužitelj mora biti konfiguriran tako da je zaštita lozinke Ništa, a QRETSVRSEC (Zadrži sigurnosne podatke poslužitelja) sistemska vrijednost mora biti 1 (Zadrži podatke).

Vezivanje kao objavljeni korisnik

Poslužitelj direktorija omogućuje načine za upotrebu LDAP unosa čija je lozinka ista onoj i5/OS profila korisnika na istom sistemu. Kako bi se to ostvarilo, unos mora:

- imati UID atribut, čija je vrijednost ime i5/OS profila korisnika
- ne imati atribut userPassword

Kada poslužitelj primi zahtjev za povezivanjem za unos koji ima UID vrijednost, ali nema userPassword, poslužitelj poziva i5/OS sigurnost da provjeri valjanost UID-a kao važećeg imena profila korisnika i specificirane lozinke kao ispravne lozinke za taj profil korisnika. Takav unos se naziva objavljeni korisnik zbog toga jer se objavljuje direktorij distribucije sistema (SDD) na LDAP-u koji kreira takve unose.

Vezivanje kao projektirani korisnik

LDAP unos koji predstavlja i5/OS profil korisnika se naziva projektirani korisnik. Možete koristiti DN projektiranog korisnika zajedno s ispravnom lozinkom za taj profil korisnika u jednostavnom vezanju. Na primjer, DN za korisnika JSMITH na sistemu my-system.acme.com bi bio:

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

SASL EXTERNAL vezanje

Ako je korišteno SSL ili TLS povezivanje s provjerom autentičnosti klijenta (na primjer, klijent ima privatan certifikat), može se koristiti SASL EXTERNAL metoda. Ta metoda govori poslužitelju da dohvati identitet klijenta iz vanjskog izvora, u ovom slučaju SSL povezivanje. Poslužitelj dohvaća javni dio certifikata klijenta (poslan na poslužitelja kao dio uspostavljanja SSL povezivanja) i ekstraktira DN subjekta. LDAP poslužitelj dodjeljuje to DN na povezivanje.

Na primjer, dani certifikat je dodijeljen na:

```
ime: John Smith
organizacijska jedinica: Engineering
organizacija: ACME
lokacija: Minneapolis
država: MN
zemlja: US
```

DN subjekta bi bio:

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

Primijetite da su cn, ou, o, l, st i c elementi korišteni prema poretku prikazanom za generiranje DN-a subjekta.

SASL GSSAPI vezanje

Mehanizam SASL GSSAPI vezanja se koristi kako bi se ovlastilo korisnika na poslužitelj korištenjem Kerberos ulaznice. Ovo je korisno kada je klijent učinio KINIT ili drugi oblik Kerberos provjere autentičnosti (na primjer, prijava na Windows 2000 domenu). U tom slučaju, poslužitelj provjerava valjanost ulaznice klijenta i onda dohvaća imena Kerberos principala i područja; na primjer, principal jsmith u području acme.com se normalno prikazuje kao jsmith@acme.com. Poslužitelj može biti konfiguriran za mapiranje tog identiteta na DN na jedan od dva načina:

- Generiranjem pseudo DN-a oblika ibm-kn=jsmith@acme.com
- Traženjem unosa koji ima ibm-securityidentities pomoćnu klasu i altsecurityidenties vrijednost u obliku KERBEROS:<principal>@<područje>.

Unos koji bi se mogao koristiti za jsmith@acme.com bi mogao izgledati kao:

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

Kako bi dobili informacije o tome kako se omogućuje Kerberos provjera autentičnosti, pogledajte “Omogućavanje Kerberos provjere autentičnosti na Poslužitelju direktorija” na stranici 119.

OS400-PRFTKN vezanje

OS400-PRFTKN SASL mehanizam vezanja se koristi kako bi se ovlastilo korisnika na poslužitelja korištenjem oznake profila (pogledajte API Generiranje oznake profila). Kada se koristi taj mehanizam, poslužitelj provjerava valjanost te oznake profila i pridružuje ju DN-u projiciranog profila korisnika s vezom (na primjer, os400-profile=JSMITH,cn=accounts,os400-system=my-as400.mycompany.com). Ako aplikacija već ima oznaku profila, tim mehanizmom se izbjegava potreba za dohvaćanjem imena profila korisnika i lozinke korisnika kako bi se izvodilo jednostavno vezanje. Kako bi mogli koristiti taj mehanizam, koristite ldap_sasl_bind s API, specificiranjem null DN, OS400-PRFTKN za mehanizam i berval (binarni podaci koji su kodirani korištenjem pojednostavljenih osnovnih pravila kodiranja) koji sadrži 32-bajtnu oznaku profila za vjerodajnice.

LDAP kao usluga provjera autentičnosti

LDAP se obično koristi kako bi se osigurala usluga provjere autentičnosti. Možete konfigurirati Web poslužitelja da mu se provjeri autentičnost na LDAP-u. Postavljanjem da se za više Web poslužitelja (ili drugih aplikacija) autentičnost provjerava na LDAP-u, možete postaviti registar jednog korisnika za te aplikacije umjesto da uvijek iznova definirate korisnika za svaku aplikaciju ili instancu Web poslužitelja.

Kako to radi? Ukratko, Web poslužitelj traži od korisnika ime korisnika i lozinku. Web poslužitelj preuzima te informacije i onda u LDAP direktoriju traži unos s tim korisničkim imenom (na primjer, možete konfigurirati Web poslužitelj tako da mapira ime korisnika u LDAP ’uid’ ili ’mail’ atribute). Ako pronađe točno jedan unos, Web poslužitelj onda šalje zahtjev za povezivanjem na poslužitelja korištenjem DN-a unosa kojeg je upravo pronašao i korisnički dobavljenu lozinku. Ako je vezanje uspješno, korisniku je sada provjerena autentičnost. SSL veze se mogu koristiti kako bi se zaštitile informacije o lozinki od njuškanja na razini protokola.

Web poslužitelj može isto tako pratiti DN koji je bio korišten tako da dana aplikacija može koristiti DN, možda pohranjivanjem podataka prilagođavanja u taj unos, drugi unos koji je njemu pridružen ili u odijeljenu bazu podataka korištenjem DN-a kao ključa za pronalaženje informacija.

Uobičajena alternativa za korištenje zahtjeva za vezanjem je korištenje LDAP operacije uspoređivanja. Na primjer, ldap_compare(ldap_session, dn, "userPassword", enteredPassword). To omogućava aplikaciji da koristi jednu LDAP sesiju umjesto da se pokreću i završavaju sesije kod svakog zahtjeva za provjerom autentičnosti.

Projicirana pozadina operacijskog sistema

Projicirana pozadina sistema ima sposobnost mapiranja i5/OS objekata kao unosa unutar LDAP-dohvatljivog direktorijskog stabla. Projicirani objekti su LDAP prikazi i5/OS objekata umjesto stvarnih unosa pohranjenih u bazu podataka LDAP poslužitelja. Korisnički profili su jedini objekti koji se mapiraju ili projiciraju unutar stabla direktorija. Mapiranje objekata profila korisnika se naziva projicirana pozadina i5/OS korisnika.

LDAP operacije su mapirane u pozadinske i5/OS objekte i izvode funkcije operacijskog sistema za pristup ovim objektima. Sve LDAP operacije izvedene na korisničkim profilima učinjene su pod ovlaštenjem korisničkog profila pridruženog vezi klijenta.

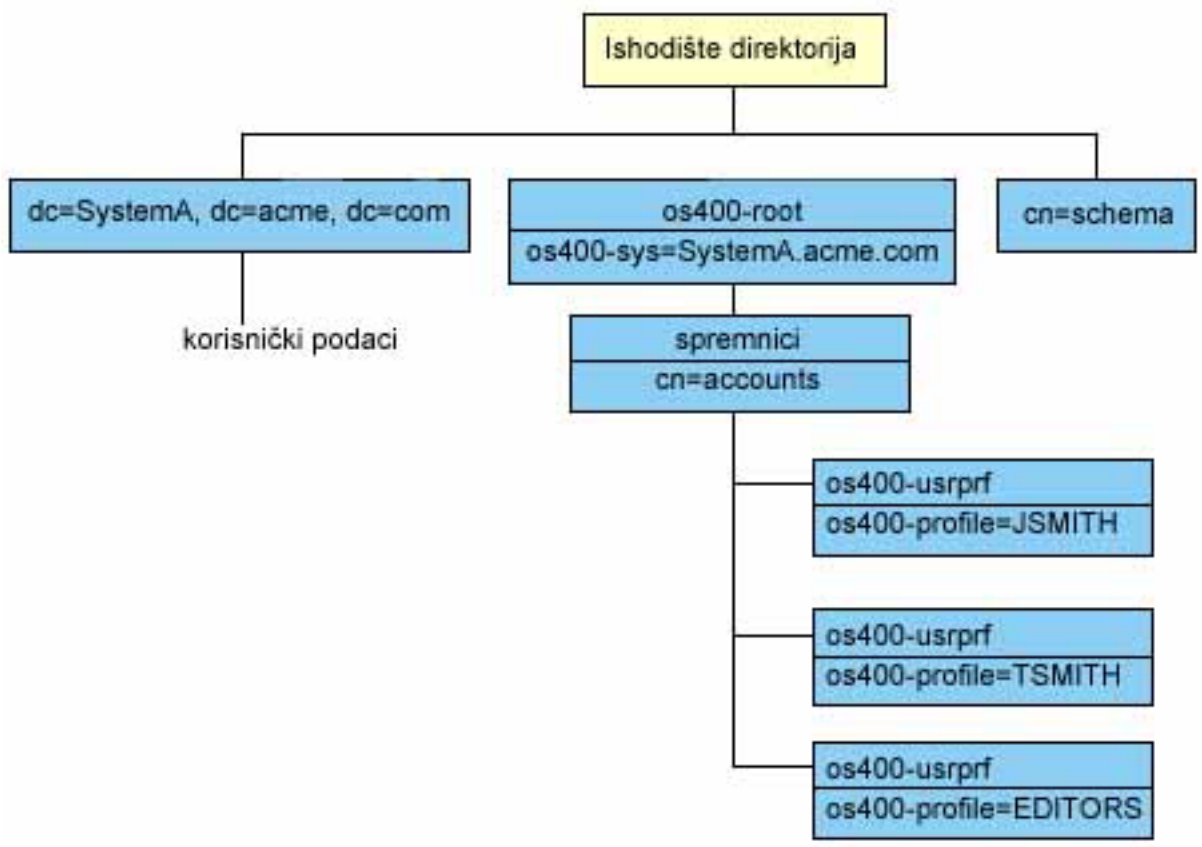
Za više informacija o projiciranoj pozadini operativnog sistema, pogledajte sljedeće:

- "i5/OS informacijsko stablo direktorija projicirano od strane korisnika"
- "LDAP operacije" na stranici 66
- "DN-ovi povezivanja administratora i replika" na stranici 69
- "i5/OS shema projicirana od strane korisnika" na stranici 69

i5/OS informacijsko stablo direktorija projicirano od strane korisnika

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

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



Korijen stabla je sufiks, koji je po defaultu os400-sys=*SystemA.acme.com*, gdje je *SystemA.acme.com* ime vašeg sistema. Klasa objekta je os400-root. Iako se DIT ne može preinačiti ili obrisati, možete rekonfigurirati sufiks sistemskog objekta. No, morate osigurati da se trenutni sufiks ne koristi u ACL-ovima ili drugdje na sistemu gdje bi se unosi trebali modificirati ako se promijeni sufiks.

Na prethodnoj slici, spremnik, cn=accounts, je pokazan ispod korijena. Ovaj objekt se ne može preinačiti. Spremnik je smješten na ovoj razini u očekivanju drugih vrsta informacija ili objekata koji mogu biti projektirani od operacijskog sistema u budućnosti. Ispod spremnika cn=accounts su korisnički profili koji su projektirani kao

objectclass=os400-usrprf. Na korisničke profile se odnose projektirani korisnički profili i poznati su LDAP-u u obliku os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com.

LDAP operacije

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

Povezivanje

LDAP klijent se može povezati na (dokazati autentičnost) LDAP poslužitelj koristeći projektirani korisnički profil. Ovo se postiže specificiranjem razlikovnog imena (DN) projiciranog profila korisnika za DN povezivanja i ispravne lozinke i5/OS profila korisnika za provjeru autentičnosti. Primjer DN korištenog u zahtjevu povezivanja bio bi os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com.

Klijent se mora povezati kao projektirani korisnik da pristupi informacijama u sistemskoj projiciranoj pozadini.

Dostupna su dva dodatna mehanizma za provjeru autentičnosti poslužitelja direktorija kao i5/OS korisnika:

- GSSAPI SASL vezanje. Ako je i5/OS konfiguriran za upotrebu Mapiranja identiteta u poduzeću (EIM), poslužitlej direktorija ispituje EIM da odredi postoji li asocijacija na lokalni i5/OS profil korisnika s početnog Kerberos identiteta. Ako postoji takva asocijacija, poslužitelj će pridružiti profil korisnika vezi i može se koristiti kako bi se pristupilo pozadini projiciranja sistema. Za više informacija o EIM-u, pogledajte poglavlje EIM.
- OS400-PRFTKN SASL vezanje. Oznaka profila se može koristiti za ovlaštenje na poslužitelj direktorija. Poslužitelj pridružuje vezi oznaku profila korisnika.

Poslužitelj izvodi sve operacije koristeći ovlaštenje tog korisničkog profila. DN projiciranog korisničkog profila može se također koristiti u LDAP ACL-ima kao DN-ovi drugih LDAP unosa. Jednostavna metoda povezivanja je jedina metoda povezivanja koja je dozvoljena kad je projektirani korisnički profil specificiran u zahtjevu povezivanja.

Traženje

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

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

Sljedeća tablica opisuje ponašanje sistemski projicirane pozadine za operacije traženja.

Tablica 2. Ponašanje sistemske projicirane pozadine za operacije traženja

Traženje zahtijevano	Baza traženja	Opseg traženja	Filter traženja	Primjedbe
Vrati informacije za os400-sys=SystemA, (opcijski) za spremnike pod njim i (opcijski) za objekte u tim spremnicima.	os400-sys=SystemA.acme.com	baza, pod ili jedan	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	Vrati prikladne atribute i njihove vrijednosti bazirano na specificiranom opsegu i filteru. Hardcoded atributi i njihove vrijednosti se vraćaju za sufiks sistemskog objekta i spremnik pod njim.

Tablica 2. Ponašanje sistemske projicirane pozadine za operacije traženja (nastavak)

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

Tablica 2. Ponašanje sistemske projicirane pozadine za operacije traženja (nastavak)

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

Usporedi

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

Dodaj i promijeni

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

Obriši

Korisnički profili mogu se obrisati korištenjem LDAP operacije brisanja. Da specificirate ponašanje DLTUSRPRF OWNOBJOPT i PGPOPT parametara, dvije LDAP poslužiteljske kontrole su sada osigurane. Ove kontrole mogu biti specificirane u LDAP operaciji brisanja. Pogledajte naredbu Briši profil korisnika (DLTUSRPRF) kako bi dobili više informacija o ponašanju tih parametara.

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

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  Kontrolna vrijednost je niz sljedećeg oblika:

  – controlValue ::= ownObjOpt [newOwner]

  – ownObjOpt ::= *NODLT / *DLT / *CHGOWN

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

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

  Primjeri vrijednosti kontrole su sljedeći:

– *NODLT: specificira da se profil ne može obrisati ako posjeduje objekte
– *CHGOWN SMITH: specificira da se vlasništvo nad objektima prenese na korisnički profil SMITH.

- Identifikator objekta (OID) je definiran u ldap.h kao LDAP_OS400_OWNOBJOPT_CONTROL_OID.
  – os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

    Kontrolna vrijednost je definirana kao niz sljedećeg oblika:

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

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

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

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

ModRDN

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

Import i eksport API-ja

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

DN-ovi povezivanja administratora i replika

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

Za više informacija, pogledajte “Rad s administrativnim pristupom za ovlaštene korisnike” na stranici 99.

i5/OS shema projicirana od strane korisnika

Klase objekata i atributi iz projicirane pozadine mogu se naći u poslužiteljskoj shemi. Imena LDAP atributa su oblika os400–*nnn*, gdje je *nnn* u pravilu ključna riječ atributa na naredbama profila korisnika. Na primjer, os400-usrcls atribut odgovara USRCLS parametru CRTUSRPRF naredbe. Vrijednosti atributa odgovaraju vrijednostima parametra koje prihvaćaju CRTUSRPRF i CHGUSRPRF naredbe ili vrijednostima prikazanim kada se prikazuje profil korisnika. Koristite alat Web administracije ili drugu aplikaciju kako bi pregledali definicije os400-usrprf klase objekta i pridružene os400-xxx atribute.

Poslužitelj direktorija i i5/OS podrška vođenju dnevnika

Poslužitelj direktorija koristi i5/OS podršku baze podataka za pohranu informacija za direktorij. Poslužitelj direktorija koristi kontrolu predavanja kod pohranjivanja slogova direktorija u bazu. Ovo zahtijeva i5/OS podršku vođenja dnevnika.

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

- Dnevnik
- Prijemnik dnevnika
- Tablice baza potrebne za početak

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

Vaša okolina, veličina direktorija i struktura ili strategija spremanja i vraćanja mogu uzrokovati neke promjene od defaulta, uključujući kako se tim objektima upravlja i koji je korišteni prag za veličinu. Parametre naredbe za vođenje dnevnika možete po potrebi mijenjati. LDAP vođenje dnevnika je postavljeno po defaultu da briše stare primaoce. Ako je dnevnik promjene konfiguriran i želite zadržati stare primaoce dnevnika, izvedite sljedeću naredbu iz i5/OS reda za naredbe:

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

Ako je konfiguriran dnevnik promjena, njegove stare primaoce zapisivanja možete obrisati sljedećom naredbom:

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

Za informacije o naredbama za vođenje dnevnika, pogledajte “OS/400 naredbe” u poglavlju Programiranje.

Operativni atributi

Postoji nekoliko atributa koji imaju posebno značenje na Poslužitelju direktorija, a koji se nazivaju operativnim atributima. To su atributi koje održava poslužitelj i oni odražavaju informacije o unosu kojima rukuje poslužitelj ili utječu na operaciju poslužitelja. Ti atributi imaju posebne karakteristike:

- Atribute ne vraća operacija pretraživanja ako oni nisu posebno zatraženi (imenom) u zahtjevu pretraživanja
- Atributi nisu dio bilo koje klase objekta. Poslužitelj kontrolira koji unosi imaju atribute.

Poslužitelj direktorija podržava sljedeće skupove operativnih atributa:

- creatorsName, createTimestamp, modifiersName, modifyTimestamp. Prisutni na svakom unosu. Ti atributi prikazuju DN vezanja i vrijeme kada je unos bio prvi put kreiran ili zadnji put preinačen. Možete koristiti te atribute u filterima pretraživanja kako bi, na primjer, pronašli sve unose koji su preinačeni nakon specificiranog vremena. Te atribute ne može preinačiti bilo koji korisnik.
- ibm-entryuuid. Prisutan na svakom unosu koji je kreiran kada je poslužitelj V5R3 ili noviji. Taj atribut je univerzalno jedinstven identifikator niza koji je dodijeljen svakom unosu od strane poslužitelja prilikom njegova kreiranja. To je korisno za aplikacije koje moraju razlikovati identično imenovane unose na različitim poslužiteljima. Atribut koristi DCE UUID algoritam kako bi generirao ID koji je jedinstven na svim unosima na svim poslužiteljima koji koriste vremensku oznaku, adresu adaptora i druge informacije.
- entryowner, ownersource, ownerpropagate, aclentry, aclsource, aclpropagate, ibm-filteracl, ibm-filteraclinherit, ibm-effectiveAcl. Za više informacija, pogledajte “Lista kontrole pristupa” na stranici 47.
- hasSubordinates. Prisutan na svakom unosu i ima vrijednost TRUE ako unos ima sebi podređene.
- numSubordinates. Prisutan na svakom unosu i sadrži više unosa koji su podređeni tom unosu.
- pwdChangedTime, pwdAccountLockedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdReset, pwdHistory. (atributi politike lozinke).
- subschemasubentry - Prisutan na svakom unosu i identificira lokaciju sheme za taj dio drveta. To je korisno kod poslužitelja s više shema ako želite pronaći shemu koju možete koristiti u tom dijelu drveta.

Kontrole i proširene operacije

Kontrole

Kontrole osiguravaju dodatne informacije poslužitelju kako bi kontrolirao kako interpretira dane zahtjeve. Na primjer, kontrola obriši podstablo može biti specificirana na LDAP zahtjevu brisanja, označavajući da bi poslužitelj trebao obrisati unos i sve njegove podređene unose, umjesto da briše samo specificirani unos. Kontrola se sastoji od tri dijela:

- Tipa kontrole, to je OID koji identificira kontrolu.
- Indikatora kritičnosti koji specificira kako bi se poslužitelj trebao ponašati ako ne podržava kontrolu. To je booleova vrijednost. FALSE označava da kontrola nije kritična i poslužitelj bi je trebao zanemariti ako je ne podržava. TRUE označava da je kontrola kritična i cijeli zahtjev bi trebao doživjeti neuspjeh (s greškom nepodržano kritično proširenje) ako poslužitelj ne može prihvatiti kontrolu.
- Neobavezna kontrolna vrijednost koja sadrži druge vrijednosti koje su specifične za kontrolu. Sadržaj kontrolne vrijednosti je specificiran korištenjem ASN.1 notacije. Sama vrijednost je BER kodiranje kontrolnih podataka.

Poslužitelj direktorija podržava sljedeće kontrole:

Ime	OID	Najranije OS/400 izdanje	Najranija verzija IBM Poslužitelja direktorija	Opis
Upravljanje s DSA IT	2.16.840.1.1137.30.3.4.2	V4R5	V3.2	Tretira referal objekte kao obične unose.
Transakcija	1.3.18.0.2.10.5	V4R5	V3.2	Označava operaciju kao dio transakcije.
OS/400 DLTUSRPRF OWNOBJOPT	1.3.18.0.2.10.8	V5R2		OS/400 briše opciju profila korisnika za vlasnika objekta. Pogledajte “Projicirana pozadina operacijskog sistema” na stranici 64 kako bi dobili detalje.
OS/400 DLTUSRPRF PGPOPT	1.3.18.0.2.10.9	V5R2		OS/400 briše opciju profila korisnika za primarnu grupu. Pogledajte “Projicirana pozadina operacijskog sistema” na stranici 64 kako bi dobili detalje.
Sortirano pretraživanje	1.2.840.113556.1.4.473 (zahtjev) i 1.2.840.113556.1.4.474 (dogovor)	V5R2 s PTF-om	V4.1	Sortira rezultate pretraživanja prije vraćanja unosa na klijenta.
Pretraživanje na stranici	1.2.840.113556.1.4.319	V5R2 s PTF-om	V4.1	Vraća klijentu rezultate pretraživanje u stranicama umjesto da vrati sve odjednom.

Ime	OID	Najranije OS/400 izdanje	Najranija verzija IBM Poslužitelja direktorija	Opis
Kontrola Brisanja drveta	1.2.840.113556.1.4.805	V5R3	V5.1	Ta kontrola je dodana zahtjevu Brisanje kako bi se označilo da će se obrisati specificirani unos i svi njegovi podređeni unosi. Korisnik mora biti administrator direktorija. Unos koji će se obrisati ne može biti kontekst replikacije.
Politika lozinke	1.3.6.1.4.1.42.2.27.8.5.1	V5R3	V5.1	Vraća klijentu posebne informacije o greški politike lozinke.
Administracija poslužitelja	1.3.18.0.2.10.15	V5R3	V5.1	Dozvoljava administratoru da izvodi operacije popravljanja koje bi se normalno odbile (na primjer: ažuriranje replike samo za čitanje, ažuriranje umirenog poslužitelja ili postavljanje određenih operativnih atributa).

Proširene operacije

Proširene operacije se koriste za pokretanje dodatnih operacija izvan jezgrenih LDAP operacija. Na primjer, proširene operacije su bile definirane za grupiranje skupa operacija u jednu transakciju. Proširena operacija se sastoji od:

- Ime zahtjeva, OID koji identificira određenu operaciju.
- Neobavezna vrijednost zahtjeva, sadrži druge informacije koje su specifične za operaciju. Sadržaj zahtijevane vrijednosti je specificiran korištenjem ASN.1 notacije. Sama vrijednost je BER kodiranje podataka zahtjeva.

Proširene operacije u pravilu imaju prošireni odgovor. Odgovor se sastoji od:

- Komponenti standardnog LDAP rezultata (kod greške, uspoređeni DN i poruka o greški)
- Imena odgovora, OID koji identificira tip odgovora
- Neobavezne vrijednosti koja sadrži druge informacije koje su specifične za odgovor. Sadržaj vrijednosti odgovora je specificiran korištenjem ASN.1 notacije. Sama vrijednost je BER kodiranje podataka odgovora.

Poslužitelj direktorija podržava sljedeće proširene zahtjeve:

Ime	OID	Najranije OS/400 izdanje	Najranija verzija IBM Poslužitelja direktorija	Opis
Registriraj događaje	1.3.18.0.2.12.1	V4R5	V3.2	
Deregistriraj događaje	1.3.18.0.2.12.3	V4R5	V3.2	

Ime	OID	Najranije OS/400 izdanje	Najranija verzija IBM Poslužitelja direktorija	Opis
Započni transakciju	1.3.18.0.2.12.5	V4R5	V3.2	
Završi transakciju	1.3.18.0.2.12.6	V4R5	V3.2	
Zahtjev DN normalizacije	1.3.18.0.2.12.30	V5R3	V5.1	

Definirane su dodatne proširene operacije koje ne bi trebao pokrenuti klijent. Te operacije se koriste pomoću ldapexop pomoćnog programa ili preko operacija koje izvodi Web Administracijski alat. Dolje su ispisane te operacije i ovlaštenja koja su potrebna za njihovo pokretanje:

Ime	OID	Najranije OS/400 izdanje	Najranija verzija IBM Poslužitelja direktorija	Opis
Kontroliraj replikaciju	1.3.18.0.2.12.16	V5R3	V5.1	Ta operacija izvodi traženu akciju na poslužitelju na kojem je izdana i prosljeđuje poziv do svih potrošača koji su u topologiji replikacije ispod nje. Klijent mora biti administrator direktorija ili imati ovlaštenje pisanja na ibm-replicagroup=default objektu za pridruženi kontekst replikacije.
Kontroliraj red replikacije	1.3.18.0.2.12.17	V5R3	V5.1	Ta operacija označava stavke kao već replicirane za specificirani ugovor. Ta operacija je dozvoljena samo kad klijent ima ovlaštenje za pisanje na ugovoru replikacije.
Umirivanje ili deumirivanje	1.3.18.0.2.12.17	V5R3	V5.1	Ta operacija stavlja podstablo u stanje u kojem ne prihvaća ažuriranja klijenta (ili prekida to stanje), osim za klijente koji su ovlašteni kao administratori direktorija na kojem postoji kontrola Administracije poslužitelja. Klijent mora biti ovlašten kao administrator direktorija ili imati ovlaštenje pisanja za ibm-replicagroup=default objekt za pridruženi kontekst replikacije.
Završi transakciju	1.3.18.0.2.12.19	V5R3	V5.1	

Ime	OID	Najranije OS/400 izdanje	Najranija verzija IBM Poslužitelja direktorija	Opis
Kaskadna kontrola replikacije	1.3.18.0.2.12.15	V5R3	V5.1	Ta operacija izvodi traženu akciju na poslužitelju na kojem je izdana i prosljeđuje poziv do svih potrošača koji su u topologiji replikacije ispod nje. Klijent mora biti administrator direktorija ili imati ovlaštenje pisanja na ibm-replicagroup=default objektu za pridruženi kontekst replikacije.
Ažuriraj konfiguraciju	1.3.18.0.2.12.28	V5R3	V5.1	Ta operacija se koristi kako bi se uzrokovalo da poslužitelj ponovo pročita specificirane postavke iz svoje konfiguracije. Operacija je dozvoljena samo kada je klijent administrator direktorija.

Poglavlje 5. Kako započeti s Poslužiteljem direktorija

Poslužitelj direktorija je automatski instaliran kada instalirate i5/OS. Poslužitelj direktorija uključuje default konfiguraciju. Da pokrenete Poslužitelj direktorija, napravite sljedeće:

1. Ako instalirate V5R3, a koristili ste Poslužitelj direktorija prethodnog izdanja, pregledajte razmatranja o migraciji. Za više informacija, pogledajte “Razmatranja o migraciji”.
2. Planiranje Poslužitelja direktorija. Za više informacija, pogledajte “Planiranje Poslužitelja direktorija” na stranici 79.
3. Da prilagodite postavke Poslužitelja direktorija, izvedite čarobnjaka Konfiguracije poslužitelja direktorija. Za više informacija, pogledajte “Konfiguriranje Poslužitelja direktorija” na stranici 80.
4. Pokrenite poslužitelj. Za više informacija, pogledajte “Pokretanje Poslužitelja direktorija” na stranici 94
5. Koristite Web administracijski alat za kreiranje ili uređivanje LDAP direktorija. Za više informacija, pogledajte “Web administracija” na stranici 82.
6. Pogledajte informacije u Poglavlje 7, “Administriranje Poslužitelja direktorija”, na stranici 93 odlomku za više informacija o tome kako se izvode razni zadaci Poslužitelja direktorija.

Razmatranja o migraciji

Poslužitelj direktorija je automatski instaliran kada instalirate i5/OS. Prvi puta kada se poslužitelj pokrene, on se automatski migrira na bilo koju postojeću konfiguraciju i podatke. To može uzrokovati dugi zastoj prije nego se poslužitelj pokrene prvi put.

Ako imate Poslužitelj direktorija koji se izvodi pod V5R2 ili V5R1, pogledajte “Migracija na V5R3 iz V5R2 ili V5R1”.

Ako imate Poslužitelj direktorija koji se izvodi pod V4R3, V4R4 ili V4R5, možete migrirati svoje podatke na V5R3. Za više informacija, pogledajte “Migracija podataka iz V4R3, V4R4 ili V4R5 na V5R3” na stranici 76.

Ako imate mrežu poslužitelja replikacije, pogledajte “Migracija mreže poslužitelja repliciranja” na stranici 77 kako bi dobili više informacija.

Ako koristite Kerberos, pogledajte “Promjena imena Kerberos usluga” na stranici 79.

Migracija na V5R3 iz V5R2 ili V5R1

V5R3 OS/400 uvodi nova svojstva i sposobnosti za Poslužitelj direktorija. Te promjene utječu i na LDAP poslužitelj direktorija i na grafičko korisničko sučelje (GUI) iSeries Navigator-a. Da iskoristite prednosti novih GUI funkcija, trebate instalirati iSeries Navigator na PC koji može komunicirati preko TCP/IP-a s vašim iSeries poslužiteljem. iSeries Navigator je komponenta iSeries Access za Windows. Ako imate instaliranu raniju verziju iSeries Navigator trebali bi je nadograditi na V5R3.

V5R3 OS/400 podržava nadogradnje iz V5R1 i V5R2. Kada nadograđujete V5R3 OS/400, LDAP podaci direktorija i datoteke sheme direktorija se automatski migriraju tako da se prilagode V5R3 formatima.

Kada nadograđujete V5R3 OS/400, trebali bi voditi računa o nekim stvarima koje se odnose na migraciju:

- Kada nadograđujete na V5R3, Poslužitelj direktorija automatski migrira vaše datoteke sheme na V5R3 i briše stare datoteke sheme. Međutim, ako ste te datoteke shema obrisali ili preimenovali, Poslužitelj direktorija ih ne može migrirati. Možete dobiti grešku ili Poslužitelj direktorija može pretpostaviti da su datoteke već migrirane.
- Poslužitelj direktorija migrira podatke direktorija na V5R3 format prvi puta kada pokrenete poslužitelja ili importirate LDIF datoteku. Planirajte tako da ostavite malo vremena da migracija potpuno završi.

Nakon što nadogradite V5R3, trebali bi jednom pokrenuti svoj poslužitelj kako bi migrirali postojeće podatke prije importiranja novih podataka. Ako pokušate importirati podatke prije nego što jednom pokrenete poslužitelj i nemate dovoljno ovlaštenje, importiranje neće uspjeti.

- Sljedeći migraciju, LDAP poslužitelj direktorija će se automatski pokrenuti kada se pokrene TCP/IP. Ako ne želite da se poslužitelj direktorija automatski pokrene, koristite iSeries Navigator da promijenite postavke.

Migracija podataka iz V4R3, V4R4 ili V4R5 na V5R3

V5R3 OS/400 ne podržava izravne nadogradnje iz V4R3, V4R4 ili V4R5. Ako želite migrirati V4R3, V4R4 ili V4R5 Poslužitelj direktorija na V5R3, možete slijediti bilo koju od sljedećih procedura:

- "Nadogradnja Poslužitelja direktorija iz V4R3, V4R4 ili V4R5 na privremeno izdanje"
- "Spremanje knjižnice baze podataka i instaliranje V5R3" na stranici 77

Prije nego počnete napravite sljedeće:

- Kad radite nadogradnju iz V4R3 u neko kasnije izdanje, trebate imati na umu sljedeće momente:
  - **Migracija datoteke prstenova u bazu podataka ključeva:**

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

    Sljedeće datoteke toka koje su koristile Poslužitelj direktorija u V4R3 više nisu potrebne i automatski se brišu kad instalirate kasnije izdanje:

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

    S ovim datotekama ne trebate ništa raditi. Ovo se spominje samo zato da se ne brinete ako primijetite da ih više nema na sistemu.
- V4R4 i ranija izdanja Poslužitelj direktorija nisu uzimala u obzir vremenske zone kod kreiranja unosa vremenske oznake. Počevši s V4R5, vremenska zona se koristi u svim dodacima i promjenama direktorija. Stoga, ako nadograđujete podatke iz V4R4 ili ranijeg, Poslužitelj direktorija podesite postojeće createtimestamp i modifytimestamp atribute kako bi odražavali ispravnu vremensku zonu. To čini oduzimanjem trenutno definirane vremenske zone na iSeries sistemu od vremenskih oznaka koje su pohranjene u direktoriju. Primijetite da ako trenutna vremenska zona nije ista vremenska zona koja je bila aktivna kad su unosi originalno kreirani ili preinačeni, nove vrijednosti vremenske oznake neće odražavati originalnu vremensku zonu.
- Ako nadograđujete podatke iz V4R4 ili ranijeg, vodite računa o tome da će podaci direktorija trebati približno dvostruko više prostora memorije od onoga koji je ranije bio potreban. To je zato što je u V4R4 ili ranijim verzijama, Poslužitelj direktorija podržavao samo IA5 skup znakova i podatke spremljene u ccsid 37 (format pojedinačnog bajta). Poslužitelj direktorija podržava puni ISO 10646 skup znakova. Nakon nadogradnje, trebali bi jednom pokrenuti poslužitelja kako bi se migrirali postojeći podaci prije nego se importiraju novi. Ako pokušate importirati podatke prije nego što jednom pokrenete poslužitelj i nemate dovoljno ovlaštenje, importiranje neće uspjeti.
- Isto tako, vodite računa o tome da mogu postojati dodatna pitanja vezana uz nadogradnju na trenutno izdanje iz drugih izdanja.

Nadogradnja Poslužitelja direktorija iz V4R3, V4R4 ili V4R5 na privremeno izdanje

Iako nadogradnje iz V4R3, V4R4 i V4R5 OS/400 na V5R3 nisu podržane, podržane su sljedeće nadogradnje:

- V4R3 i V4R4 nadograđen na V4R5
- V4R4 i V4R5 nadograđen na V5R1
- V4R5 i V5R1 nadograđen na V5R2
- V5R1 i V5R2 nadograđen na V5R3

Jedan od načina da migrirate svojeg Poslužitelj direktorija poslužitelja je da ga nadogradite na privremeno izdanje (V5R1 ili V5R2), onda na V5R3. Kako bi dobili dodatne informacije o OS/400 procedurama instalacije, pogledajte

Instalacija softvera  . Slijedite ove općenite korake za izvođenje migracije:

1. Zabilježite promjene koje ste napravili u datotekama sheme u direktoriju /QIBM/UserData/OS400/DirSrv. Datoteke sheme migriraju automatski.
2. Za V5R3, instalirajte V4R5.
3. Za V4R4 ili V4R5, instalirajte V5R1 ili V5R2.
4. Instalirajte na V5R3.
5. Ako već nije pokrenut, pokrenite Poslužitelj direktorija.
6. Koristite Web administracijski alat kako bi preinačili datoteke sheme za bilo koje promjene korisnika koje ste opazili u koraku 1.
7. Ponovo pokrenite Poslužitelj direktorija.

Spremanje knjižnice baze podataka i instaliranje V5R3

Možete migrirati svojeg Poslužitelj direktorija poslužitelja spremanjem knjižnice baze podataka koju Poslužitelj direktorija koristi u V4R3, V4R4 ili V4R5 i onda je vratiti nakon instaliranja V5R3. Time se preskače korak instaliranja privremenog izdanja. No, postavke poslužitelja nisu migrirane, tako da morate rekonfigurirati postavke poslužitelja.

Kako bi dobili detaljne informacije o OS/400 procedurama instalacije, pogledajte *Instalacija softvera* . Slijedite ove općenite korake za izvođenje migracije:

1. Zabilježite promjene koje ste napravili u datotekama sheme u direktoriju /QIBM/UserData/OS400/DirSrv. Datoteke sheme nisu migrirane automatski, tako da ako želite zadržati promjene trebat ćete ih opet ručno implementirati.
2. Zabilježite različite postavke konfiguracije u Poslužitelj direktorija svojstvima, uključujući ime knjižnice baze podataka.
3. Spremite knjižnicu baze podataka koja je specificirana u Poslužitelj direktorija konfiguraciji. Ako ste konfigurirali dnevnik promjena, onda se treba spremiti QUSRDIRCL knjižnica.
4. Zabilježite konfiguraciju objavljivanja.
5. Instalirajte V5R3 OS/400 na sistemu.
6. Koristite EZ-Postav kako bi konfigurirali Poslužitelj direktorija.
7. Vratite knjižnicu baze koju ste spremili u koraku 3. Ako ste spremili QUSRDIRCL knjižnicu u koraku 3, sada je vratite.
8. Koristite Web administracijski alat kako bi preinačili datoteke sheme za bilo koje promjene korisnika koje ste opazili u koraku 1.
9. Koristite iSeries Navigator kako bi rekonfigurirali Poslužitelj direktorija. Specificirajte knjižnicu baze podataka koja je ranije bila konfigurirana i koja je bila spremljena i vraćena u prethodnim koracima.
10. Koristite iSeries Navigator da rekonfigurirate izdavanje.
11. Ponovo pokrenite Poslužitelj direktorija.

Migracija mreže poslužitelja repliciranja

Prvi puta kada se pokrene glavni poslužitelj, on migrira informacije u direktorij koji kontrolira replikaciju. Unosi s klasom objekta replicaObject pod cn=localhost se zamjenjuju unosima koje koristi novi model replikacije (za više informacija pogledajte “Replikacija” na stranici 34). Glavni poslužitelj je konfiguriran da replicira sve sufikse u direktorij. Unosi ugovora su kreirani s atributom ibm-replicationOnHold postavljenim na true. Time se omogućava da se ažuriranja učinjena na glavnom poslužitelju akumuliraju za repliku dok replika ne bude spremna.

Ti unosi se nazivaju topologijom replikacije. Novi glavni poslužitelj se može koristiti s replikama koje izvode prethodne verzije; podaci koji se odnose na nove osobine se neće replicirati na poslužitelje stražnje-razine. Potrebno je eksportirati unose topologije replikacije iz glavnog poslužitelja i dodati ih na svaku repliku nakon što je poslužitelj replikacije bio migriran. Kako bi eksportirali unose, koristite alat Qshell red za naredbe “ldapsearch” na stranici 169 i spremite izlaz na datoteku. Naredba pretraživanja je slična sljedećem:

```
ldapsearch -h master-server-host-name -p master-server-port \
 -D master-server-admin-DN -w master-server-admin-password \
 -b ibm-replicagroup=default,suffix-entry-DN \
 -L "(|(objectclass=ibm-replicaSubEntry)(objectclass=ibm-replicationAgreement))" \
     > replication.topology.ldif
```

Ta naredbe kreira izlaznu LDIF datoteku pod imenom replication.topology.ldif u trenutnom radnom direktoriju. Datoteka sadrži samo nove unose.

Bilješka: Nemojte uključiti sljedeće sufikse:

- cn=changelog
- cn=localhost
- cn=pwdpolicy
- cn=schema
- cn=configuration

Uključite samo korisnički kreirane sufikse.

Ponovite naredbu za svaki unos sufiksa na glavnom poslužitelju, ali zamijenite “>” s “>>” kako bi pridodali podatke na izlaznu datoteku za naredna pretraživanja. Nakon što se datoteka dovrši, kopirajte je na replika poslužitelje.

Dodajte datoteku na replika poslužitelje nakon što su bili uspješno migrirani; nemojte dodati datoteke na poslužitelje koji se izvode na prethodnim verzijama poslužitelja direktorija. Morate pokrenuti i zaustaviti poslužitelja prije nego dodate datoteku.

Kako bi pokrenuli poslužitelja, koristite **Start** opciju u iSeries Navigatoru. Za više informacija, pogledajte “Pokretanje Poslužitelja direktorija” na stranici 94.

Kako bi zaustavili poslužitelja koristite **Stop** opciju u iSeries Navigatoru. Kako bi dobili dodatne informacije, pogledajte “Zaustavljanje poslužitelja direktorija” na stranici 94.

Kada dodajete datoteku na replika poslužitelja, vodite računa o tome da nije pokrenut replika poslužitelj. Kako bi dodali podatke, koristite opciju **Importiraj datoteku** u iSeries Navigatoru.

Nakon što se učitaju unosi topologije replikacije, pokrenite replika poslužitelja i nastavite s replikacijom. Replikaciju možete nastaviti na jedan od sljedećih načina:

- Na glavnom poslužitelju koristite **Upravljanje redovima u upravljanju replikacijom** u Web administracijskom alatu.
- Koristite **ldapexop** pomoćni program reda za naredbe. Na primjer:

  ```
  ldapexop -h ime-hosta-glavnog-poslužitelja -p port-glavnog-poslužitelja \
   -D master-server-admin-DN -w master-server-admin-password \
   -op controlrepl -action resume -ra DN-ugovora-replike
  ```

  Ta naredba nastavlja replikaciju za poslužitelj koji je definiran u unosu sa specificiranim DN-om.

Kako bi odredili koji se DN ugovora replike podudara s replika poslužiteljem, pogledajte replication.topology.ldif datoteku. Glavni poslužitelj će zapisati poruku da se je pokrenula replikacija za tu repliku i upozorenje da se ID poslužitelja replike ne podudara s ID-om replike poslužitelja. Kako bi ažurirali ugovor replike tako da koristi ispravan ID poslužitelja, koristite **Upravljanje replikom** u Web administracijskom alatu ili alat reda za naredbe **ldapmodify**. Na primjer:

```
ldapmodify -c -h ime-hosta-glavnog-poslužitelja -p port-glavnog-poslužitelja \
 -D admin-DN-glavnog-poslužitelja -w admin-lozinka-glavnog-poslužitelja
dn: DN-ugovora-replike
changetype: modify
replace: ibm-replicaConsumerID
ibm-replicaConsumerID: ID-replika-poslužitelja
```

Možete unijeti te naredbe izravno na red za naredbe ili možete spremiti naredbe u LDIF datoteci i isporučiti ih naredbi s **-i** *file* opcijom. Koristite **Završi prethodni zahtjev** da zaustavite naredbu.

Dovršena je migracija za tu repliku.

Kako bi nastavili koristiti repliku koja izvodi prethodnu verziju, svejedno je potrebno nastaviti replikaciju korištenjem alata reda za naredbe **ldapexop** ili **Upravljanje replikacijom** u Web administracijskom alatu za tu repliku. Ako je replika koja izvodi prethodnu verziju migrirana kasnije, koristite alat reda za naredbe **ldapdiff** kako bi uskladili podatke direktorija. Time se osigurava da se unosi ili atributi koji nisu bili replicirani ažuriraju na replici.

Promjena imena Kerberos usluga

Kod V5R3 se mijenja ime usluga koje koristi poslužitelj direktorija i API-ji klijenta za GSSAPI provjeru autentičnosti (Kerberos). Ta promjena nije kompatibilna s imenom usluga korištenim prije V5R3 (V5R2M0 PTF 5722SS1-SI08487 sadrži istu promjenu).

Prije ovog izdanja, i5/OS poslužitelj direktorija i API-ji klijenta su koristili ime usluge oblika LDAP/dns-host-name@Kerberos-realm kada je GSSAPI mehanizam (Kerberos) korišten za provjeru autentičnosti. To ime ne odgovara standardima koji definiraju GSSAPI provjeru autentičnosti prema kojoj bi ime principala trebalo započeti s ″ldap″ s malim slovom. Kao rezultat, niti i5/OS poslužitelj direktorija niti API-ji klijenata ne mogu međudjelovati s drugim proizvodima prodavača. To je posebno točno ako Kerberos centar distribucije ključa (KDC) ima imena principala osjetljiva na mala i velika slova. LDAP dobavljač usluge za JNDI, često korišten API Java LDAP klijent, je primjer klijenta uključenog s i5/OS koji koristi ispravno ime usluge.

V5R3M0 mijenja ime usluge kako bi bilo u skladu sa standardima. No, time uzrokuje vlastite probleme s kompatibilnosti.

- Poslužitelj direktorija koji je konfiguriran da koristi GSSAPI provjeru autentičnosti neće započeti instaliranje tog izdanja. To je posljedica toga što datoteka tablice ključeva ima vjerodajnice koje koriste staro ime usluge (LDAP/mysys.ibm.com@IBM.COM), dok poslužitelj traži vjerodajnice koje koriste novo ime usluge (ldap/mysys.ibm.com@IBM.COM).
- Poslužitelj direktorija ili LDAP aplikacija koja koristi LDAP API-je na V5R3M0 nije u mogućnosti provjeriti autentičnost starijih i5/OS poslužitelja ili klijenata. Kako bi to ispravili, trebali bi napraviti sljedeće:
  1. Ako KDC koristi imena principala osjetljiva na velika i mala slova, kreirajte račun korištenjem ispravnog imena usluge (ldap/mysys.ibm.com@IBM.COM).
  2. Ažurirajte datoteku tablice ključeva korištenu od i5/OS Poslužitelja direktorija da sadrži vjerodajnice za novo ime usluge. Možda bi bilo dobro da obrišete stare vjerodajnice. Možete koristiti Qshell pomoćni program tablice ključeva kako bi ažurirali datoteku tablice ključeva. Po defaultu, poslužitelj direktorija koristi /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab datoteku. Čarobnjak V5R3M0 Usluge provjere autentičnosti (Kerberos) u iSeries Navigatoru isto tako kreira unose tablice ključeva korištenjem novog imena usluge.
  3. Ažurirajte V5R2M0 i5/OS sisteme gdje se koristi GSSAPI primjenom PTF 5722SS1-SI08487.

Alternativno, možete izabrati da poslužitelji direktorija i API-ji klijenta nastave s korištenjem starog imena usluge. To bi moglo biti poželjno kada koristite Kerberos provjeru autentičnosti u pomiješanoj mreži sistema koji se izvode sa i bez PTF-ova. Kako bi to napravili, postavite LDAP_KRB_SERVICE_NAME varijablu okoline. To možete postaviti za cijeli sistem (potrebno za postavljanje imena usluga za poslužitelja) korištenjem sljedeće naredbe:

```
ADDENVVAR ENVVAR(LDAP_KRB_SERVICE_NAME)
```

ili QSH (kako bi utjecali da se LDAP pomoćni programi izvode iz ove QSH sesije):

```
export LDAP_KRB_SERVICE_NAME=1
```

Planiranje Poslužitelja direktorija

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

- **Organizirajte direktorij**. Planirajte strukturu vašeg direktorija i odredite koje sufikse i atribute će vaš poslužitelj trebati. Za više informacija, pogledajte “Direktoriji” na stranici 7, “Sufiks (kontekst imenovanja)” na stranici 14 i “Atributi” na stranici 19.
- **Odlučite kako velik će biti vaš direktorij**. Onda možete procijeniti koliko memorije vam treba. Veličina direktorija ovisi o sljedećem:
  - Broju atributa u poslužiteljskoj shemi.
  - Broju upisa na poslužitelju.
  - Tipu informacija koje pohranjujete na poslužitelju.

  Na primjer, prazan direktorij koji koristi default Poslužitelj direktorija shemu traži približno 10 MB prostora memorije. Direktorij koji koristi default shemu i sadrži 1000 slogova običnih podataka o zaposlenicima zahtijeva oko 30 MB prostora. Ovaj broj će se mijenjati ovisno atributima koje koristite. Također će se jako povećati ako ste pohranili velike objekte, kao što su slike, u direktorij.
- **Odlučite koje sigurnosne mjere ćete poduzeti**.

  Poslužitelj direktorija vam omogućava da primijenite politiku lozinke kako bi osigurali da korisnici povremeno mijenjaju svoje lozinke i da njihove lozinke odgovaraju potrebama sintaktičke lozinke organizacije.

  Poslužitelj direktorija podržava korištenje Sloja sigurnih utičnica (SSL) i Digitalnih certifikata kao i Sigurnosti sloja transporta (TLS) za sigurnost komunikacije. Podržana je i Kerberos provjera autentičnosti.

  Poslužitelj direktorija vam omogućava da kontrolirate pristup objektima direktorija s listama kontrole pristupa (ACL-ovi). Možete također koristiti i5/OS sigurnosnu reviziju za zaštitu direktorija.

  Osim toga trebate odlučiti koja će se politika lozinke primijeniti.
- **Izaberite DN administratora i lozinku**. Default DN administratora je cn=administrator. To je jedini identitet kojeg treba ovlaštenje kako bi se kreirali ili preinačili unosi direktorija kada se poslužitelj inicijalno konfigurira. Možete koristiti default DN administratora ili izabrati drugačiji DN. Trebate kreirati i lozinku za DN administratora.
- **Instalirajte potrebni softver za Web administracijski alat Poslužitelja direktorija**. Kako bi koristili Web administracijski alat Poslužitelja direktorija, sljedeći proizvodi moraju biti instalirani na iSeries poslužitelju.
  - IBM HTTP Poslužitelj za iSeries (5722-DG1)
  - IBM WebSphere Poslužitelj aplikacije - Express (5722-IWE Bazno i opcija 2)

  Pogledajte poglavlje IBM HTTP Poslužitelj kako bi dobili više informacija o IBM HTTP Poslužitelju za iSeries i IBM WebSphere Poslužitelj aplikacija - Express.

Konfiguriranje Poslužitelja direktorija

1. Ako vaš sistem nije bio konfiguriran kako bi objavljivao informacije drugom LDAP poslužitelju i nijedan LDAP poslužitelj nije poznat TCP/IP DNS poslužitelju, onda se Poslužitelj direktorija automatski instalira s ograničenom default konfiguracijom. Pogledajte “Default konfiguracija za Poslužitelj direktorija” na stranici 81 za više informacija. Poslužitelj direktorija sadrži čarobnjaka koji će vam pomoći kod konfiguriranja Poslužitelja direktorija za vaše specifične potrebe. Možete pokrenuti ovog čarobnjaka kao dio EZ-Setup-a ili pokrenuti čarobnjaka kasnije iz iSeries Navigator. Koristite se ovim čarobnjakom kad radite početno konfiguriranje poslužitelja direktorija. Možete ga upotrijebiti i za ponovno konfiguriranje poslužitelja direktorija.

   Bilješka: Kad koristite čarobnjaka za ponovnu konfiguraciju poslužitelja direktorija, konfiguriranje počinjete ni od čega. Originalna konfiguracija se briše, ona se ne mijenja. No, podaci direktorija se ne brišu, već umjesto toga ostaju pohranjeni u knjižnici koju ste izabrali na instalaciji (po defaultu QUSRDIRDB). Dnevnik promjena također ostaje nedirnut, u QUSRDIRCL knjižnici po defaultu.

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

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

   Morate imati posebna ovlaštenja *ALLOBJ i *IOSYSCFG kad konfigurirate poslužitelj. Ako želite konfigurirati OS/400 reviziju sigurnosti, morate imati posebno ovlaštenje *AUDIT.
2. Kako bi pokrenuli Poslužitelj direktorija Čarobnjak konfiguracije, poduzmite ove korake:

a. U iSeries Navigator, proširite **Mreža**.
b. Proširite **Poslužitelji**.
c. Kliknite na **TCP/IP**.
d. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Konfiguriraj**.

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

3. Slijedite upute u čarobnjaku Konfiguriraj Poslužitelj direktorija kako bi konfigurirali svoj Poslužitelj direktorija.

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

4. Kada se čarobnjak dovrši, vaš Poslužitelj direktorija ima osnovnu konfiguraciju. Ako izvodite Lotus Domino na vašem poslužitelju, onda bi port 389 (default port za LDAP poslužitelj) mogla koristiti Domino LDAP funkcija. Morate napraviti nešto od sljedećeg:
   - Promijenite port kojeg koristi Lotus Domino. Pogledajte " Host Domino LDAP i Poslužitelj direktorija na istom iSeries " u E-pošta poglavlju kako bi dobili više informacija.
   - Promijenite port kojeg koristi Poslužitelj direktorija. Pogledajte "Promjena porta ili IP adrese" na stranici 96 za više informacija.
   - Koristite određene IP adrese. Pogledajte "Promjena porta ili IP adrese" na stranici 96 za više informacija.
5. Kreirajte unose koji odgovaraju sufiksu ili sufiksima koje ste konfigurirali. Za više informacija, pogledajte "Dodavanje i uklanjanje sufiksa Poslužitelja direktorija" na stranici 98.

Možete napraviti nešto ili sve od sljedećeg prije nego nastavite:
- Importirati podatke na poslužitelj, pogledajte "Importiranje LDIF datoteke" na stranici 97.
- Omogućiti sigurnost Sloja sigurnih utičnica (SSL), pogledajte "Omogućavanje SSL-a na Poslužitelju direktorija" na stranici 117.
- Omogućiti Kerberos provjeru autentičnosti, pogledajte "Omogućavanje Kerberos provjere autentičnosti na Poslužitelju direktorija" na stranici 119.
- Postaviti referal, pogledajte "Specificiranje poslužitelja za referale direktorija" na stranici 97.

Default konfiguracija za Poslužitelj direktorija

Poslužitelj direktorija se automatski instalira kada instalirate OS/400. Ta instalacija uključuje default konfiguraciju. Poslužitelj direktorija koristi default konfiguraciju kada je sve od sljedećeg istina:
- Administratori nisu izvodili Poslužitelj direktorija Čarobnjak konfiguracije ili promijenili postavke direktorija sa stranicama postavke.
- Poslužitelj direktorija izdavanje nije konfigurirano.
- Poslužitelj direktorija ne može pronaći bilo koje LDAP DNS informacije.

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

Web administracija

Jedan ili više Poslužitelja direktorija se može administrirati pomoću Web administracijske konzole. Web administracijska konzola vam omogućava da:

- Dodate ili promijenite popis Poslužitelja direktorija koji se mogu administrirati.
- Administrirate Poslužitelj direktorija korištenjem Web administracijskog alata.
- Promijenite atribute Web administracijske konzole.

Kako bi koristili Web administracijsku konzolu, napravite sljedeće:

1. Ako je to prvi put da koristite Web administraciju Poslužitelja direktorija, prvo morate postaviti Web administraciju (pogledajte "Postavljanje Web administracije po prvi put") i onda nastaviti sa sljedećim korakom.
2. Prijavite se na Web administraciju Poslužitelja direktorija čineći nešto od sljedećeg:
   - Iz iSeries Navigatora izaberite poslužitelj i kliknite na **Mreža > Poslužitelji > TCP/IP**, desno kliknite na **Direktorij** i kliknite na **Administracija poslužitelja**.
   - Na stranici iSeries Zadaci (http://*vaš_poslužitelj*:2001) kliknite na **IBM Poslužitelj direktorija**.
3. Ako želite administrirati Poslužitelj direktorija, napravite sljedeće:
   a. Izaberite Poslužitelj direktorija koji želite administrirati u **LDAP Hostname** polju.
   b. Unesite DN prijave administratora koje koristite kako bi se vezali na poslužitelj direktorija.
   c. Unesite lozinku administratora.
   d. Kliknite na **Prijava**. Prikazuje se stranica IBM Web administracijski alat Poslužitelja direktorija. Za više informacija o stranici IBM Web administracijski alat Poslužitelja direktorija, pogledajte "Web administracijski alat" na stranici 84.
4. Ako želite dodati ili promijeniti popis Poslužitelja direktorija koji se mogu administrirati ili promijeniti atribute Web administracijske konzole, napravite sljedeće:
   a. Izaberite **Console Admin** u **LDAP Hostname** polju.
   b. Unesite prijavu administratora konzole.
   c. Unesite lozinku administratora konzole.
   d. Kliknite na **Prijava**. Prikazuje se stranica IBM Web administracijski alat Poslužitelja direktorija. Za više informacija o stranici IBM Web administracijski alat Poslužitelja direktorija, pogledajte "Web administracijski alat" na stranici 84.
   e. Kliknite na **Administracija konzole** i onda izaberite jedno od sljedećeg:
      - **Promjena prijave administratora konzole** kako bi promijenili ime prijave administratora konzole.
      - **Promjena lozinke administratora konzole** kako bi promijenili lozinku administratora konzole.
      - **Upravljanje poslužiteljima konzole** kako bi promijenili to koje Poslužitelje direktorija može administrirati Web konzola administracije.
      - **Upravljanje svojstvima konzole** kako bi promijenili svojstva Web administracijske konzole.

Postavljanje Web administracije po prvi put

Učinite sljedeće da prvi put postavite Alat za Web administraciju Poslužitelja direktorija.

1. Instalirajte IBM WebSphere Poslužitelj direktorija - Express (5722-IWE Bazni i opcija 2) i pridruženi potreban softver ako oni nisu već instalirani. Pogledajte poglavlje IBM HTTP Poslužitelj kako bi dobili više informacija.
2. Omogućite instancu poslužitelja sistemske aplikacije u HTTP ADMIN instanci poslužitelja.
   a. Pokrenite HTTP ADMIN instancu poslužitelja čineći jedno od sljedećeg.
      - U iSeries Navigatoru kliknite **Mreža -> Poslužitelji -> TCP/IP** i desno kliknite **HTTP Administracija**. Zatim kliknite **Pokreni**.
      - U i5/OS redu za naredbe upišite STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).
   b. Prijavite se na IBM Web administraciju za iSeries. Koristite i5/OS profil korisnika i lozinku za prijavu na stranicu iSeries Zadaci (http://*vaš_poslužitelj*:2001), zatim kliknite **IBM Web Administraciju za iSeries**.

c. Sa stranice Administracija HTTP poslužitelja *vaš_poslužitelj*, kliknite karticu **Upravljaj** i zatim kliknite karticu the **HTTP Poslužitelji**. Provjerite da je izabrano **ADMIN – Apache** na padajućoj listi Poslužitelj. Iz opcija na lijevom oknu na stranici, kliknite **Općenita konfiguracija poslužitelja**.

   Bilješka: Možda ćete trebati proširiti dio **Svojstva poslužitelja** da bi vidjeli opciju **Općenita konfiguracija poslužitelja**.

d. Postavite **Pokreni instancu poslužitelja sistemske aplikacije kada je pokrenut 'Admin' poslužitelj** na **Yes**.

e. Kliknite **OK**.

3. Postavite WebSphere Poslužitelj aplikacija da koristi SYSINST.
   a. Kliknite **WebSphere Poslužitelj aplikacija** s opcija na lijevom oknu.
   b. Izaberite **WebSphere Poslužitelj aplikacija – Express 5.0**.
   c. Iz padajuće liste **WebSphere instance**, izaberite **SYSINST**.

      Bilješka: Ako SYSINST nije prisutno na padajućoj listi, ponovno pokrenite ADMIN poslužitelj.

   d. Na padajućoj listi **Pokreni sve WebSphere poslužitelje aplikacija...**, izaberite **Yes**.
   e. Na padajućoj listi **Zaustavi sve WebSphere poslužitelje aplikacija...**, izaberite **Yes**.
   f. Kliknite **OK**.
4. Ponovno pokrenite instancu HTTP ADMIN poslužitelja klikom na gumb za ponovno pokretanje (drugi gumb na kartici **HTTP Poslužitelji**). Instancu HTTP ADMIN poslužitelja možete također zaustavljati i pokretati upotrebom iSeries Navigatora ili i5/OS reda za naredbe.

   Instancu HTTP ADMIN poslužitelja možete zaustaviti čineći jedno od sljedećeg.
   - U iSeries Navigatoru kliknite na **Mreža -> Poslužitelji -> TCP/IP** i desno kliknite na **HTTP administracija**. Zatim kliknite **Zaustavi**.
   - U i5/OS redu za naredbe upišite ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).

   Možete pokrenuti instancu HTTP ADMIN poslužitelja čineći jedno od sljedećeg.
   - U iSeries Navigatoru kliknite na **Mreža -> Poslužitelji -> TCP/IP** i desno kliknite na **HTTP administracija**. Zatim kliknite **Pokreni**.
   - U i5/OS redu za naredbe upišite STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).

   Pogledajte poglavlje IBM HTTP Poslužitelj kako bi dobili više informacija.
5. Prijavite se u Alat za Web administraciju Poslužitelja direktorija.
   a. Dovedite naprijed **Stranicu prijave** čineći jedno od sljedećeg.
      - Iz iSeries Navigatora, izaberite vaš poslužitelj i kliknite **Mreža -> Poslužitelji -> TCP/IP**, desno kliknite **IBM Poslužitelj direktorija** i kliknite **Administracija poslužitelja**.
      - Sa stranice iSeries Zadaci (http://*vaš_poslužitelj*:2001) kliknite **IBM Poslužitelj direktorija za iSeries**.
   b. Izaberite **Admin konzole** u polju **LDAP Ime hosta**.
   c. Upišite superadmin u polje **Ime korisnika**.
   d. Upišite tajna u polje **Lozinka**.
   e. Kliknite na **Prijava**. Prikazuje se stranica IBM Web administracijski alat Poslužitelja direktorija.
6. Promijenite prijavu administracije konzole.
   a. Kliknite **Administracija konzole** u lijevom oknu da proširite sekciju i zatim kliknite **Promijeni prijavu administratora konzole**.
   b. Upišite novo ime prijave administracije konzole u polju **Prijava administratora konzole**.
   c. Upišite trenutnu lozinku (tajno) u polje **Trenutna lozinka**.
   d. Kliknite **OK**.
7. Promijenite lozinku administracije konzole. Kliknite **Promijeni lozinku administratora konzole** u lijevom oknu.
8. Dodajte Poslužitelj direktorija kojeg želite administrirati. Kliknite **Upravljaj poslužiteljima konzole** u lijevom oknu.

Bilješka: Kod dodavanja i5/OS Poslužitelja direktorija, **Port administracije** se ne koristi i biti će zanemaren.

9. Ako želite promijeniti svojstva konzole. Kliknite **Upravljaj svojstvima konzole** u lijevom oknu.
10. Kliknite na **Odjava**. Kada se pojavi ekran Odjava uspješna, kliknite vezu **ovdje** za povratak na stranicu prijave Web administracije.

Nakon što ste po prvi puta konfigurirali konzolu, možete se uvijek vratiti na konzolu kako bi:

- Promijenili prijavu i lozinku administratora konzole.
- Promijenili koje Poslužitelje direktorija može administrirati Web administracijski alat.
- Promijenili svojstva konzole.

Web administracijski alat

Jednom kada se prijavite na Web administracijski alat, naići ćete na prozor aplikacije koja se sastoji od pet dijelova:

Područje uvodnika
Područje uvodnika je smješteno na vrh panela i sastoji se od imena aplikacije i IBM loga.

Područje navigacije
Područje navigacije koje je smješteno na lijevu stranu panela prikazuje proširive kategorije za različite zadatke sadržaja poslužitelja, kao što je:

Svojstva korisnika
Taj zadatak vam dozvoljava da promijenite trenutnu lozinku korisnika.

Upravljanje shemom
Taj zadatak vam omogućava da radite s klasama objekta, atributima, pravilima podudaranja i sintaksama.

Upravljanje direktorijom
Taj zadatak vam omogućava da radite s unosima direktorija.

Upravljanje replikacijom
Taj zadatak vam omogućava da radite s vjerodajnicama, topologijom, rasporedima i redovima.

Područja i predlošci
Taj zadatak vam omogućava da radite s predlošcima korisnika i područjima.

Korisnici i grupe
Taj zadatak vam omogućava da radite s korisnicima i grupama u definiranim područjima. Na primjer, ako želite kreirati novog Web korisnika, zadatak **Korisnici i grupe** radi s jednom klasom objekta grupe, groupOfNames. Vi ne možete oblikovati grupnu podršku.

Radno područje
Radno područje prikazuje zadatke koji su pridruženi izabranim zadacima u području navigacije. Na primjer, ako je izabrana sigurnost Upravljanje poslužiteljem u području navigacije, radno područje prikazuje stranicu Sigurnost poslužitelja i kartice koje sadrže zadatke koji se odnose na postavljanje sigurnosti poslužitelja.

Područje statusa poslužitelja
Područje statusa poslužitelja je locirano na vrhu radnog područja. Ikona na lijevoj strani područja statusa poslužitelja označava trenutni status poslužitelja. Uz ikonu je ime poslužitelja koji se administrira. Ikona na desnoj strani područja statusa poslužitelja osigurava vezu na online pomoć.

Područje status zadatka
Područje zadatka koje je smješteno ispod radnog područja prikazuje status trenutnog zadatka.

Poglavlje 6. Scenarij: MyCo, Inc. postavlja Poslužitelj direktorija

Situacija

Kao administrator računalnog sistema vašeg poduzeća, vi bi željeli smjestiti informacije o zaposlenicima kao što su brojevi telefona i adrese e-pošte za vašu organizaciju u središnje LDAP spremište.

Ciljevi

U ovom scenariju, MyCo, Inc. želi konfigurirati Poslužitelj direktorija i kreirati bazu podataka koja sadrži informacije o zaposlenicima, kao što su ime, adresa e-pošte i telefonski broj.

Ciljevi tog scenarija su kako slijedi:

- Da informacije o zaposlenicima učinite dostupnima bilo gdje u mreži zaposlenika i to za zaposlenike koji koriste Lotus Notes ili Microsoft Outlook Express klijent za poštu.
- Omogućiti upraviteljima da promijene podatke o zaposlenicima u bazi podataka direktorija, a i istovremeno ne omogućiti ne-upraviteljima da promijene podatke o zaposleniku.
- Dozvoliti da iSeries poslužitelj može objaviti podatke o zaposleniku u bazi podataka direktorija.

Detalji

Poslužitelj direktorija će se izvoditi na iSeries poslužitelju pod nazivom myiSeries.

Sljedeći primjer prikazuje informacije koje MyCo, Inc. želi uključiti u bazu podataka direktorija za svakog zaposlenika.

```
Ime: Jose Alvirez
Odjel: DEPTA
Broj telefona: 999 999 9999
Adresa e-pošte: jalvirez@my_co.com
```

Struktura direktorija za taj scenarij bi se mogla prikazati kao nešto slično sljedećem:

```
/
|
+- my_co.com
   |
   +- employees
      |
      +- Jose Alvirez
      |  DEPTA
      |  999-555-1234
      |  jalvirez@my_co.com
      |
      +- John Smith
      |  DEPTA
      |  999-555-1235
      |  jsmith@my_co.com
      |
      +  Managers group
         Jose Alvirez
         myiSeries.my_co.com
.
.
.
```

Svi zaposlenici (upravitelji i ne-upravitelji) postoje u stablu direktorija zaposlenika. Upravitelji pripadaju i grupi upravitelja. Članovi grupe upravitelja mogu imati ovlaštenje za promjenom podataka o zaposlenicima.

iSeries poslužitelj (myiSeries) treba imati ovlaštenje za mijenjanje podataka o zaposlenicima. U ovom scenariju, iSeries poslužitelj je smješten u stablo direktorija zaposlenika i postao je članom grupe upravitelja.

Ako želite da se unosi zaposlenika odvajaju od unosa iSeries poslužitelja, možete kreirati drugo stablo direktorija (na primjer: računala) i tamo dodati iSeries poslužitelj. iSeries poslužitelj će trebati imati isto ovlaštenje kao i upravitelji.

Preduvjeti i pretpostavke

Web administracijski alat je ispravno konfiguriran i izvodi se. Pogledajte “Web administracija” na stranici 82 za više informacija.

Koraci postava

Dovršite sljedeće zadatke:
1. “Detalji scenarija: Postav Poslužitelja direktorija”.
2. “Detalji scenarija: Kreiranje baze podataka direktorija” na stranici 87.
3. “Detalji scenarija: Objavljivanje iSeries podataka na bazi podataka direktorija” na stranici 89.
4. “Detalji scenarija: Unos informacija u bazu podataka direktorija” na stranici 90.
5. “Detalji scenarija: Testiranje baze podataka direktorija” na stranici 91.

Detalji scenarija: Postav Poslužitelja direktorija

Korak 1: Konfiguriranje Poslužitelja direktorija

Bilješka: Morate imati posebna ovlaštenja *ALLOBJ i *IOSYSCFG kad konfigurirate poslužitelj.

1. U iSeries Navigatoru kliknite na **Mreža —> Poslužitelji —> TCP/IP**.
2. Kliknite na **Konfiguriraj sistem kao Poslužitelj direktorija** u prozoru **Zadaci konfiguracije poslužitelja** u donjem desnom kutu iSeries Navigatora.
3. Pojavit će se **Čarobnjak konfiguracije poslužitelja direktorija**.
4. Kliknite na **Konfiguriraj lokalan LDAP poslužitelj direktorija** na prozoru **IBM Čarobnjak konfiguracije poslužitelja direktorija - Dobro došli!**.
5. Kliknite na **Sljedeće** na prozoru **IBM Čarobnjak konfiguracije poslužitelj direktorija - Dobro došli!**.
6. Izaberite **Ne** na prozoru **IBM Čarobnjak konfiguracije poslužitelja direktorija - Specificirajte postavke**. To vam omogućava da konfigurirate LDAP poslužitelj bez default postavki.
7. Kliknite na **Sljedeće** na prozoru **IBM Čarobnjak konfiguracije poslužitelja direktorija - Specificirajte postavke**.
8. Poništite izbor **Sistemski-generirano** na prozoru **IBM Čarobnjak konfiguracije poslužitelja direktorija - Specificirajte DN administratora** i unesite sljedeće:

DN administrator	cn=administrator
Lozinka	tajna
Potvrdi lozinku	tajna

Bilješka: Sve lozinke su specificirane u ovom scenariju samo kao primjeri. Kako bi spriječili kompromitiranje sigurnosti vašeg sistema ili lozinke, nikad ne bi smjeli koristiti ove lozinke kao dio vaše vlastite konfiguracije.

9. Kliknite na **Sljedeće** na prozoru **IBM Čarobnjak konfiguracije poslužitelja direktorija - Specificirajte DN administratora**.

10. Upišite dc=my_co,dc=com u **Sufiks** polje na **IBM Čarobnjak konfiguracije poslužitelja direktorija - Specificirajte sufikse**.
11. Kliknite na **Dodaj** na prozoru **IBM Čarobnjak konfiguracije poslužitelja direktorija - Specificirajte sufikse**.
12. Kliknite na **Sljedeće** na prozoru **IBM Čarobnjak konfiguracije poslužitelja direktorija - Specificirajte sufikse**.
13. Izaberite **Da, koristi sve IP adrese** na **IBM Čarobnjak konfiguracije poslužitelja direktorija - Izaberi IP adresu**.
14. Kliknite na **Sljedeće** na prozoru **IBM Čarobnjak konfiguracije poslužitelja direktorija - Izaberi IP adrese**.
15. Izaberite **Da** na prozoru **IBM Čarobnjak konfiguracije poslužitelja direktorija - Specificirajte TCP/IP preferencu**.
16. Kliknite na **Sljedeće** na prozoru **IBM Čarobnjak konfiguracije poslužitelja direktorija - Specificirajte TCP/IP preferencu**.
17. Kliknite na **Završetak** na prozoru **IBM Čarobnjak konfiguracije poslužitelja direktorija - Sažetak**.
18. Desno kliknite na **IBM Poslužitelj direktorija** i kliknite na **Start**.

Korak 2: Konfiguriranje Web administracijskog alata poslužitelja direktorija

1. Usmjerite svojeg pretražitelja na http://*myiSeries.my_co.com*:9080/IDSWebApp/IDSjsp/Login.jsp, gdje je *myiSeries.my_co.com* vaš iSeries poslužitelj.
2. Trebala bi se pojaviti stranica prijave. Kliknite na **LDAP Hostname** listu i izaberite **Console Admin**. Upišite superadmin za ime korisnika i tajna za lozinku. Kliknite na **Prijava**.
3. Konfiguriranje Web administracijskog alata za povezivanje na LDAP poslužitelj na vašem iSeriesu. Izaberite **Administracija konzole —> Upravljanje poslužiteljima konzole** u navigaciji s lijeve strane.
4. Kliknite **Dodaj**.
5. U polje **Dodaj poslužitelja** upišite myiSeries.my_co.com.
6. Kliknite na **Ok**. U listi se pojavljuje novi poslužitelj pod **Upravljanje poslužiteljima konzole**.
7. Kliknite na **odjava** u navigaciji s lijeve strane.
8. Na stranici prijava na Web administracijskom alatu kliknite na **LDAP Ime hosta** popis i izaberite poslužitelj koji ste upravo konfigurirali (**myiSeries.my_co.com**).
9. U polje **Ime korisnika** upišite cn=administrator, a u polje **Lozinka** upišite tajna. Kliknite na **Prijava**. Trebali bi vidjeti glavnu stranicu alata IBMWeb Administracijski alat Poslužitelja direktorija.

Detalji scenarija: Kreiranje baze podataka direktorija

Prije nego možete početi unositi podatke, morate kreirati prostor za podatke koji će se pohraniti.

Korak 1: Kreiranje baznog DN objekta

1. Kliknite na **Upravljanje direktorijom —> Upravljanje unosima**. Možete vidjeti popis objekata na osnovnoj razini direktorija. Budući je poslužitelj nov, vidjet ćete samo strukturalne objekte koji sadrže informacije o konfiguraciji.
2. Želite dodati novi objekt koji će sadržavati MyCo, Inc. podatke. Prvo kliknite na **Dodavanje...** na desnoj strani prozora. U sljedećem prozoru, spuštajte se kroz listu **Klasa objekta** kako bi izabrali **domenu** i kliknite na **Sljedeće**.
3. Ne želite dodati pomoćne klase objekta, pa kliknite ponovo na **Sljedeće**.
4. U prozoru **Unesi atribute** unesite podatke koji se podudaraju sa sufiksom kojeg ste ranije kreirali u čarobnjaku. Ostavite **Klasa objekta** padajući popis na **domeni**. Upišite dc=my_co u polje **Relativno DN**. Upišite dc=com u polje **Nadređeno DN**. Upišite my_co u **dc** polje.
5. Kliknite na **Završetak** na dnu prozora. Natrag na baznoj razini bi trebali vidjeti novi bazni DN.

Korak 2: Kreiranje predloška korisnika

Kreirati ćete predložak korisnika kao pomoć pri dodavanju MyCo, Inc. podataka o zaposlenicima.

1. Kliknite na **Područja i predlošci —> Dodavanje predloška korisnika**.
2. U polje **Ime predloška korisnika** upišite Zaposlenik.
3. Kliknite na gumb **Pregled...** koji se nalazi uz polje **Nadređeno DN**. Kliknite na bazni DN kojeg ste kreirali u prethodnom odlomku, **dc=my_co,dc=com** i kliknite na **Izbor**, s lijeve strane prozora.
4. Kliknite na **Sljedeće.**
5. U padajućem popisu **Strukturalna klasa objekta**
6. izaberite **inetOrgPerson** i kliknite na **Sljedeće**.
7. U padajućoj listi **Atribut imenovanja** izaberite **cn**.
8. U listi **Tabulatori** izaberite **Potrebno** i kliknite na **Uređivanje**.
9. U prozoru **Uređivanje kartice** birate polja koja će biti uključena u predložak korisnika. Potrebno je **sn** i **cn**.
10. U listi **Atributi** izaberite **departmentNumber** i kliknite na **Dodaj >>>**.
11. Izaberite **broj telefona** i kliknite na **Dodaj >>>**.
12. Izaberite **pošta** i kliknite na **Dodaj >>>**.
13. Izaberite **lozinka korisnika** i kliknite **Dodaj >>>**.
14. Kliknite na **OK** i onda **Završetak** da kreirate predložak korisnika.

Korak 3: Kreiranje područja

1. U Web Administracijskom alatu kliknite na **Područja i predlošci —> Dodaj područje**.
2. U polje **Ime područja** upišite zaposlenici.
3. Kliknite na **Pregled...** s lijeve strane polja **Nadređeno DN**.
4. Izaberite nadređeno DN koje ste kreirali **dc=my_co,dc=com** i kliknite na **Izbor** na desnoj strani prozora.
5. Kliknite na **Sljedeće**.
6. U sljedećem prozoru trebate samo promijeniti padajući popis **Predložak korisnika**. Izaberite predložak korisnika kojeg ste kreirali, **cn=employees,dc=my_co,dc=com**.
7. Kliknite na **Završetak**.

Korak 4: Kreiranje grupe upravitelja

1. Kreirajte grupu upravitelja.
   a. Kliknite na **Korisnici i grupe —> Dodaj grupu**.
   b. U polje **Ime grupe** upišite upravitelji.
   c. Provjerite da li su izabrani **zaposlenici** u listi povlačenja **Područje**.
   d. Kliknite na **Završetak**.
2. Konfigurirajte administratora grupe upravitelja za područje **zaposlenici**.
   a. Kliknite na **Područja i predlošci —> Upravljanje područjima**.
   b. Izaberite područje koje ste kreirali, **cn=employees,dc=my_co,dc=com** i kliknite na **Uređivanje**.
   c. S desne strane polja **Grupa administratora** kliknite na **Pregled...**.
   d. Izaberite **dc=my_co,dc=com** i kliknite na **Proširi**.
   e. Izaberite **cn=employees** i kliknite na **Proširi**.
   f. Izaberite **cn=managers** i kliknite na **Izaberi**.
   g. U prozoru **Uredi područje** kliknite na **OK**.
3. Dajte ovlaštenje upravljanja grupom preko **dc=my_co,dc=com** sufiksa.
   a. Kliknite na **Upravljanje direktorijom —> Upravljanje unosima**.
   b. Izaberite **dc=my_co,dc=com** i kliknite na **Uredi ACL...**.
   c. U prozoru **Uredi ACL** kliknite na karticu **Vlasnici**.
   d. Izaberite **Proširi korisnika** kućicu provjere. Svatko tko je član grupe upravitelja će postati vlasnikom **dc=my_co,dc=com** stabla podataka.

e. U **Tip** listi povlačenja izaberite **Grupa**.
f. U polje **DN (Razlikovno ime)** upišite cn=managers,cn=employees,dc=my_co,dc=com.
g. Kliknite **Dodaj**.
h. Kliknite na **Ok**.

Korak 5: Dodavanje korisnika kao upravitelja

1. U Web administracijskom alatu kliknite na **Korisnici i grupe —> Dodaj korisnika**.
2. Izaberite područje koje ste kreirali, **zaposlenici**, u padajućem izborniku **Područje** i kliknite na **Sljedeće**.
3. U **cn** polje upišite Jose Alvirez.
4. U polje ***sn** (prezime) upišite Alvirez.
5. U polje ***cn** (potpuno ime) upišite Jose Alvirez. cn se koristi kako bi se kreirao DN unosa. *cn je atribut objekta.
6. U polje **Broj_telefona** upišite 999 555 1234.
7. U polje **broj_odjela** upišite DEPTA.
8. U polje **pošta** upišite jalvirez@my_co.com.
9. U polje **lozinka_korisnika** upišite tajna.
10. Kliknite na karticu **Grupa korisnika**.
11. U listi **Dostupne grupe** izaberite **upravitelji** i kliknite na **Dodavanje —>**.
12. Na dnu prozora kliknite na **Završetak**.
13. Odjavite se iz Web administracijskog alata tako da kliknete na **Odjava** u navigaciji s lijeve strane.

Detalji scenarija: Objavljivanje iSeries podataka na bazi podataka direktorija

Konfigurirajte objavljivanje kako bi omogućili iSeries poslužitelju da automatski unese informacije o korisniku u LDAP direktorij. Informacije korisnika iz direktorija distribucije sistema se objavljuju u LDAP direktoriju.

Bilješka: Korisnici kreirani s iSeries Navigatorom dobivaju korisnički profil i unos korisnika direktorija distribucije sistema. Ako koristite CL naredbe za kreiranje korisnika, morate kreirati profil korisnika (**CRTUSRPRF**) i unos korisnika direktorija distribucije sistema (**WRKDIRE**). Ako vaši korisnici postoje samo kao profili korisnika i želite ih objaviti na LDAP direktoriju, morate za njih kreirati unose korisnika direktorija distribucije sistema.

Korak 1: Kreiranje iSeries poslužitelja kao korisnika Poslužitelja direktorija

1. Prijavite se na Web Administracijski alat (http://**myiSeries.my_co.com**:9080/IDSWebApp/IDSjsp/Login.jsp) kao administrator.
   a. Izaberite **myiSeries.my_co.com** u listi **LDAP Ime hosta**.
   b. Upišite cn=administrator u polje **Ime korisnika**.
   c. Upišite tajna u polje **Lozinka**.
   d. Kliknite na **Prijava**.
2. Izaberite **Korisnici i grupe —> Dodaj korisnika**.
3. Izaberite **zaposlenici** u listi **Područje**.
4. Kliknite na **Sljedeće**.
5. Upišite myiSeries.my_co.com u polje **cn**.
6. Upišite myiSeries.my_co.com u polje ***sn**.
7. Upišite myiSeries.my_co.com u polje ***cn**.
8. Upišite tajna u polje **Lozinka_korisnika** .
9. Kliknite na karticu **Grupa korisnika**.
10. Izaberite grupu **upravitelji**.

11. Kliknite na **Dodaj —>**.
12. Kliknite na **Završetak**.

Korak 2: Konfiguriranje iSeries poslužitelja za objavljivanje podataka

1. U iSeries Navigatoru desno kliknite na vaš iSeries u navigaciji s lijeve strane i izaberite **Svojstva**.
2. U kućici dijaloga **Svojstva** izaberite karticu **Poslužitelj direktorija**.
3. Izaberite **Korisnici** i kliknite na **Detalji**.
4. Izaberite kućicu provjere **Objavi informacije o korisniku**.
5. U odlomku **Gdje objaviti** kliknite na gumb **Uredi**. Pojavit će se prozor.
6. Upišite myiSeries.my_co.com.
7. U polje **Pod DN** upišite cn=employees,dc=my_co,dc=com.
8. U odlomku **Povezivanje poslužitelja** provjerite da li je default broj porta, **389**, unesen u polje **Port**. U padajućem popisu **Metoda provjere autentičnosti** izaberite **Razlikovno ime** i unesite cn=myiSeries,cn=employees,dc=my_co,dc=com u polje **Razlikovno ime**.
9. Kliknite na **Lozinka**.
10. Upišite tajna u polje **Lozinka**.
11. Upišite tajna u polje **Potvrdi lozinku**.
12. Kliknite **OK**.
13. Kliknite na gumb **Provjeri**. Time se osigurava da ste ispravno unijeli sve informacije i da se iSeries može povezati na LDAP direktorij.
14. Kliknite **OK**.
15. Kliknite **OK**.

Detalji scenarija: Unos informacija u bazu podataka direktorija

Kao upravitelj, Jose Alvirez sada dodaje i ažurira podatke za pojedince u svojem odjelu. Treba dodati neke dodatne informacije o Jane Doe. Jane Doe je korisnik na iSeries poslužitelju i njezine su informacije objavljene. Jose Alvirez treba dodati informacije i o zaposleniku John Smith. John Smith nije korisnik na iSeries poslužitelju. Jose Alvirez čini sljedeće:

Korak 1: Prijava na Web administracijski alat

Prijavite se na Web administracijski alat (http://**myiSeries.my_co.com**:9080/IDSWebApp/IDSjsp/Login.) čineći sljedeće:

1. Izaberite **myiSeries.my_co.com** u listi **LDAP Ime hosta**.
2. Upišite cn=Jose Alvirez,cn=myco employees,dc=my_co,dc=com u polje Ime korisnika.
3. Upišite tajna u polje lozinka.
4. Kliknite na **Prijava**.

Korak 2: Modificiranje podataka o zaposleniku

1. Kliknite na **Korisnici i grupe—> Upravljanje korisnicima**.
2. Izaberite **zaposlenici** u listi **Područje** i kliknite na **Pregled korisnika**.
3. Izaberite **Jane Doe** u listi korisnika i kliknite na **Uređivanje**.
4. Upišite DEPTA u polje **broj_odjela**.
5. Kliknite **OK**.
6. Kliknite na **Zatvori**.

Korak 3: Dodavanje podataka o zaposleniku

1. Kliknite na **Korisnici i grupe —> Dodaj korisnika**.

2. Izaberite **zaposlenici** u izborniku povlačenja **Područje** i kliknite na **Sljedeće**.
3. U **cn** polje upišite John Smith.
4. U ***sn** polje upišite Smith.
5. U ***cn** polje upišite John Smith.
6. U polje **Broj_telefona** upišite 999 555 1235.
7. U polje **broj_odjela** upišite DEPTA.
8. U polje **pošta** upišite jsmith@my_co.com.
9. Kliknite na **Završetak** na dnu prozora.

Detalji scenarija: Testiranje baze podataka direktorija

Nakon što ste unijeli podatke o zaposleniku u bazu podataka direktorija, testirajte bazu podataka direktorija i Poslužitelj direktorija čineći jedno od sljedećeg:

Pretražite bazu podataka direktorija koristeći svoj imenik adresa e-pošte

Informacije u LDAP direktoriju mogu lagano potražiti LDAP omogućeni programi. Mnogo klijenata e-pošte može pretraživati LDAP poslužitelje direktorija kao dio funkcije svojeg imenika adresa. Slijede primjeri postupaka za konfiguraciju Lotus Notes 6 i Microsoft Outlook Express 6. Postupak za većinu drugih e-mail klijenata biti će vrlo sličan.

Lotus Notes

1. otvorite svoj imenik.
2. Kliknite na **Akcije —> Novi —> Račun**.
3. Upišite myiSeries u polje **Ime računa**.
4. Upišite myiSeries.my_co.com u polje **Ime poslužitelja računa**.
5. Izaberite **LDAP** u polju **Protokol**.
6. Kliknite na karticu **Konfiguracija protokola**.
7. Upišite dc=my_co,dc=com u polje **Baza traženja**.
8. Kliknite na **Spremi i zatvori**.
9. Kliknite na **Kreiraj —> Pošta —> Memorandum**.
10. Kliknite na **Adresa...**.
11. Izaberite myiSeries u polju **Izaberi imenik**.
12. Upišite Alvirez u polje **Pretraživanje za**.
13. Kliknite na **Pretraživanje**. Pojavit će se podaci za Jose Alvireza.

Microsoft Outlook Express

1. Kliknite na **Alati —> Računi**.
2. Kliknite na **Dodaj —> Usluga direktorija**.
3. Upišite Web adresu za iSeries u polje **Poslužitelj Internet direktorija (LDAP)** (myiSeries.my_co.com).
4. Poništite izbor u kućici **Moj LDAP poslužitelj traži da se prijavim**.
5. Kliknite na **Sljedeće**.
6. Kliknite na **Sljedeće**.
7. Kliknite na **Završetak**.
8. Izaberite myiSeries.my_co.com (usluga direktorija koju ste upravo konfigurirali) i kliknite na **Svojstva**.
9. Kliknite na **Napredno**.
10. Upišite dc=my_co,dc=com u polje **Baza traženja**.
11. Kliknite na **Ok**.

12. Kliknite na **Zatvori**.
13. Upišite Ctrl+E kako bi otvorili prozor **Pronađi ljude**.
14. Izaberite myiSeries.my_co.com za listu **Pogledaj u**.
15. Upišite Alvirez u polje **Ime**.
16. Kliknite na **Pronađi sad**. Pojavit će se podaci za Jose Alvirez.

Pretražite bazu direktorija korištenjem ldapsearch naredbe reda za naredbe

1. Na sučelju baziranom na znakovima unesite CL naredbu **QSH** kako bi otvorili Qshell sesiju.
2. Unesite sljedeće kako bi dohvatili popis svih LDAP unosa u bazi podataka.

   ```
   ldapsearch –h myiSeries.my_co.com –b dc=my_co,dc=com objectclass=*
   ```

   Gdje je:

   –h ime glavnog stroja koji izvodi LDAP poslužitelja.

   –b je bazni DN pod kojim će se pretraživati.

   objectclass=*
   vraća sve unose u direktorij.

   Ta naredba vraća nešto što je slično sljedećem:

   ```
   dc=my_co,dc=com
   dc=my_co
   objectclass=domain
   objectclass=top

   cn=MyCo employee,dc=my_co,dc=com

   .
   .
   .

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

   sn=Alvirez
   departmentNumber=DEPTA
   mail=jalvirez@my_co.com
   telephoneNumber=999 999 9999
   objectclass=top
   objectclass=inetOrgPerson
   objectclass=organizationalPerson
   objectclass=person
   cn=Jose Alvirez

   .
   .
   .
   ```

   Prva linija svakog unosa se naziva razlikovno ime (DN). DN-ovi su poput potpunog imena datoteke svakog unosa. Neki od unosa ne sadrže podatke i oni su samo strukturalni. Oni s linijom **objectclass=inetOrgPerson** odgovaraju unosima koje ste kreirali za ljude. Jose Alvirez DN je **cn=Jose Alvirez,cn=MyCo Employees,dc=my_co,dc=com**.

Poglavlje 7. Administriranje Poslužitelja direktorija

Za administriranje Poslužitelja direktorija morate imati postavljena sljedeća ovlaštenja:

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

Za upravljanje objektima direktorija (uključujući i liste kontrole pristupa, vlasništvo nad objektima i replike) trebate se spojiti na direktorij ili s DN administratora ili nekim drugim DN koji ima ispravno LDAP ovlaštenje. Ako se koristi integracija ovlaštenja, administrator može biti i projicirani korisnik (pogledajte “Projicirana pozadina operacijskog sistema” na stranici 64) koji ima ovlaštenje nad ID-om funkcije Administratora poslužitelja direktorija (pogledajte “Rad s administrativnim pristupom za ovlaštene korisnike” na stranici 99).

Općeniti zadaci administracije

Zadaci sadržaja direktorija

- “Upravljanje listama kontrole pristupa (ACL-ovi)” na stranici 145

Zadaci objavljivanja

- “Objavljivanje informacija poslužitelju direktorija” na stranici 149

Pokretanje Poslužitelja direktorija

Za pokretanje Poslužitelja direktorija, poduzmite ove korake:

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

   Poslužitelju direktorija može trebati nekoliko minuta za pokretanje, ovisno o brzini vašeg poslužitelja i iznosu dostupne memorije. Prvo pokretanje poslužitelja direktorija može trajati nekoliko minuta dulje nego obično jer poslužitelj mora kreirati nove datoteke. Slično tome, pokretanje poslužitelja direktorija po prvi put nakon nadogradnje iz ranije verzije Poslužitelj direktorija, može trajati nekoliko minuta duže nego obično jer poslužitelj mora migrirati datoteke. Povremeno možete provjeravati status poslužitelja (pogledajte “Provjera statusa poslužitelja direktorija” na stranici 95) kako bi vidjeli da li je već pokrenut.

Poslužitelj direktorija se može pokrenuti iz sučelja baziranog na znakovima i unošenjem naredbe STRTCPSVR *DIRSRV. Uz to, ako vam je poslužitelj direktorija konfiguriran da se pokreće kad se pokrene TCP/IP, možete ga također pokretati tako da unesete naredbu STRTCP.

Način Samo konfiguracija

Poslužitelj direktorija se može konfigurirati u načinu samo konfiguracija iz sučelja zasnovanog na znakovima unošenjem naredbe TRCTCPAPP APP(*DIRSRV) ARGLIST(SAFEMODE).

Način samo konfiguracija pokreće poslužitelj s aktivnim samo cn=configuration sufiksom i ne ovisi o uspješnoj inicijalizaciji pozadina baze podataka.

Zaustavljanje poslužitelja direktorija

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

Poduzmite ove korake kako bi zaustavili Poslužitelj direktorija:

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

   Poslužitelju direktorija treba nekoliko sekundi da se zaustavi, ovisno o brzini vašeg sistema, količini aktivnosti poslužitelja i količini dostupne memorije. Povremeno možete provjeravati status poslužitelja (pogledajte “Provjera statusa poslužitelja direktorija” na stranici 95) kako bi vidjeli da li je već pokrenut.

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

Provjera statusa poslužitelja direktorija

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

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

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

Provjera poslova na Poslužitelju direktorija

Uvijek kada želite nadgledati određene poslove na Poslužitelju direktorija. Kad provjeravate poslove na poslužitelju, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desno kliknite na **Direktorij** i izaberite **Poslovi poslužitelja**.

Omogućavanje obavještavanja o događajima

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

Za omogućavanje obavještavanja o događajima za vaš poslužitelj, slijedite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite na **Događaji**.
6. Izaberite **Dozvoli klijentima da se registriraju za obavještavanje o događaju**.

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

Kako bi dobili dodatne informacije o obavještavanju o događajima, pogledajte odlomak Obavještavanje o događaju od IBM Poslužitelj direktorija Verzija 5.1 Referenca programiranja.

Specificiranje postavki transakcije

Poslužitelj direktorija podržava transakcije, što dopušta da se grupa operacija LDAP direktorija tretira kao jedna jedinica. Za više informacija, pogledajte “Transakcije” na stranici 40.

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

6. Specificirajte vaše postavke transakcija.

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

Promjena porta ili IP adrese

Poslužitelj direktorija koristi sljedeće default portove:
- 389 za nezaštićene veze.
- 636 za sigurne veze (ako ste koristili Upravitelja digitalnih certifikata za omogućavanje Poslužitelj direktorija aplikacije koja može koristiti siguran port).

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

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

Za primjer toga kako se Domino LDAP poslužitelj sukobljuje s Poslužiteljem direktorija, pogledajte Host Domino LDAP i Poslužitelj direktorija na istom iSeries

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

Da promijenite IP adresu na koju poslužitelj direktorija prihvaća povezivanja, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite karticu **Mreža**.
6. Kliknite gumb **IP Adrese...**.
7. Izaberite **Koristite izabrane IP adrese** i izaberite IP adrese koje će poslužitelj koristiti za prihvaćanje konekcija.

Postavljanje politike lozinke

Da postavite politiku lozinke, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite na karticu **Lozinka**.
6. Unesite informacije o politici lozinke. Neobavezno kliknite na **Zaključavanje i provjera valjanosti lozinke** kako bi specificirali dodatne informacije o lozinci i onda kliknite na **OK**.
7. Kliknite **OK**.

Bilješka: Možete koristiti i ldapmodify pomoćni program (pogledajte “ldapmodify i ldapadd” na stranici 157) kako bi postavili politiku lozinke.

Za više informacija o politici lozinke, pogledajte “Politika lozinke” na stranici 59.

Importiranje LDIF datoteke

Možete prenositi informacije o različitim Poslužiteljima direktorija korištenjem datoteka LDAP Format razmjene podataka (LDIF). Pogledajte “LDAP format razmjene podataka (LDIF)” na stranici 182 za više informacija. Prije nego počnete ovaj postupak, prenesite LDIF datoteku na vaš iSeries poslužitelj kao datoteku toka.

Za import LDIF datoteke na poslužitelj direktorija, poduzmite ove korake:
1. Ako je poslužitelj direktorija pokrenut, zaustavite ga. Pogledajte “Zaustavljanje poslužitelja direktorija” na stranici 94 kako bi dobili informacije o zaustavljanju poslužitelja direktorija.
2. U iSeries Navigator, proširite **Mreža**.
3. Proširite **Poslužitelji**.
4. Kliknite na **TCP/IP**.
5. Desnom tipkom kliknite na **Direktorij** i izaberite **Alati**, a zatim **Import datoteke**.

   Neobavezno, poslužitelj može replicirati novo importirane podatke kada se sljedeći put pokrene, ako izaberete **Repliciraj importirane podatke**. To je korisno kada dodajete nove unose na postojeće stablo direktorija na glavnom poslužitelju. Ako importirate podatke kako bi inicijalizirali replika (ili ravnopravnog) poslužitelja, u pravilu ne želite da se podaci repliciraju jer bi oni već mogli postojati na poslužiteljima za koje je taj poslužitelj dobavljač.

Bilješka: Možete koristiti i ldapadd pomoćni program (pogledajte “ldapmodify i ldapadd” na stranici 157) kako bi importirali LDIF datoteke.

Eksportiranje LDIF datoteke

Možete prenositi informacije između različitih Poslužitelja direktorija korištenjem datoteka LDAP Format razmjene podataka (LDIF), pogledajte “LDAP format razmjene podataka (LDIF)” na stranici 182. U neku LDIF datoteku možete eksportirati sve ili dio svog LDAP direktorija.

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

   Bilješka: Ako ne specificirate potpuno kvalificiranu stazu u koju će LDIF datoteka eksportirati podatke, datoteka će biti kreirana u home direktoriju specificiranom u vašem i5/OS profilu korisnika.

Bilješke:

1. Pazite da odredite ovlaštenje za LDIF datoteku da spriječite neovlašteni pristup podacima u direktoriju. Ako to činite, desnom tipkom kliknite na datoteku u iSeries Navigator, a zatim izaberite **Dozvole**.
2. Možete kreirati cijelu ili dio LDIF datoteke, pomoću servisnog programa ldapsearch; vidjeti “ldapsearch” na stranici 169. Koristite -L opciju i preusmjerite izlaz u datoteku.

Specificiranje poslužitelja za referale direktorija

Za dodjelu referal poslužitelja za poslužitelj direktorija, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom kliknite na **Direktorij**, zatim izaberite **Svojstva**.
5. Izaberite stranicu **Općenita** svojstva.
6. U polju **Novi referal**, specificirajte URL referalnog poslužitelja.
7. Na upit odredite ime referalnog poslužitelja u URL formatu. U nastavku su primjeri prihvatljivih URL-a za LDAP:

- ldap://test.server.com
- ldap://test.server.com:400
- ldap://9.9.99.255

Bilješka: Ako referalni poslužitelj ne koristi default port, specificirajte ispravan broj porta kao dio URL-a onako kako je port 400 specificiran u drugom gornjem primjeru.

8. Kliknite **Dodaj**.
9. Kliknite **OK**.

Dodavanje i uklanjanje sufiksa Poslužitelja direktorija

Dodavanje sufiksa Poslužitelju direktorija omogućava poslužitelju da upravlja tim dijelom stabla direktorija.

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

Ako dodajete sufiks u poslužitelj direktorija, poduzmite ove korake:
1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite karticu **Baza podataka/Sufiksi**.
6. U polju **Novi sufiks** upišite ime novoga sufiksa.
7. Kliknite **Dodaj**.
8. Kliknite **OK**.

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

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

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

Spremanje i vraćanje informacija Poslužitelja direktorija

Poslužitelj direktorija pohranjuje informacije na sljedećim lokacijama:

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

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

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

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

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

Rad s administrativnim pristupom za ovlaštene korisnike

Administratoru možete dodijeliti pristup profilima korisnika kojima je bio dan pristup na Administrator poslužitelja direktorija (QIBM_DIRSRV_ADMIN) identifikator funkcije (ID).

Na primjer, ako je profilu korisnika JOHHNSMITH dodijeljen pristup na ID funkcije Administratora poslužitelja direktorija i izabrana je opcija Dodijeli administratoru pristup ovlaštenim korisnicima iz dijaloga Svojstvo direktorija, onda JOHNSMITH profil ima ovlaštenje LDAP administratora. Kad se ovaj profil koristi za povezivanje na poslužitelj direktorija korištenjem sljedećeg DN-a, os400-profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com, korisnik ima administratorsko ovlaštenje. Sufiks sistemskih objekata u ovom primjeru je os400-sys=systemA.acme.com. Za više informacija o projiciranim korisnicima, pogledajte “Projicirana pozadina operacijskog sistema” na stranici 64.

Da bi selektirali ovu opciju, slijedite ove korake:

1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
4. Na **Općenito** kartici pod **Administratorske informacije**, izaberite opciju **Dodijelite administratorski pristup autoriziranim korisnicima**.

Kako bi postavili ID funkcije ovlaštenja Administratora poslužitelja direktorija u profilu korisnika, poduzmite ove korake:

1. U iSeries Navigator, Desnom tipkom miša kliknite na ime sistema i izaberite **Administracija Aplikacije**.
2. Kliknite na karticu **Host Aplikacije**.
3. Proširite **Operacijski Sistem/400**.
4. Kliknite na **Administrator poslužitelja direktorija** kako bi osvijetlili opciju.
5. Kliknite na gumb **Prilagodi** .
6. Proširite **Korisnici**, **Grupe** ili **Korisnik nije u grupi**, ovisno o tome koji odgovara korisniku kojeg želite.
7. Izaberite korisnika ili grupu koji će se dodati na listu **Dozvoljen pristup** .
8. Kliknite na gumb **Dodaj** .
9. Kliknite **OK** za spremanje promjena.
10. Kliknite **OK** na dijalogu **Administracija Aplikacija** .

Praćenje pristupa i promjena u LDAP direktoriju

Možda ćete htjeti pratiti pristup i promjene u vašem LDAP direktoriju. Možete koristiti dnevnik promjena LDAP direktorija kako bi mogli pratiti promjene nad direktorijom. Dnevnik promjena se nalazi pod posebnim sufiksom cn=changelog. Pohranjen je u knjižnici QUSRDIRCL.

Da aktivirate dnevnik promjena, slijedite ove korake:

1. U iSeries Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite na **TCP/IP**.
4. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
5. Kliknite na karticu **Dnevnik promjena**.
6. Izaberite **Zapiši promjene direktorija**.
7. (neobavezno) U polju **Maksimum unosa** specificirajte maksimalan broj unosa koje će sačuvati dnevnik promjena. U polju **Maksimalna starost** specificirajte koliko dugo se zadržavaju unosi dnevnika promjena.

Bilješka: Iako su ti parametri neobavezni, trebali bi razmotriti specificiranje maksimalnog broja unosa ili maksimalne starosti. Ako ne specificirate nijedno od toga, dnevnik promjena će čuvati sve unose i mogao bi postat vrlo velik.

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

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

Primjer:

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

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

Omogućavanje revizije objekta za Poslužitelj direktorija

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

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

Promjene u postavkama revizije će nastati čim kliknete **OK**. Nema potrebe za ponovnim pokretanjem Poslužitelja direktorija. Za više informacija, pogledajte “Poslužitelj direktorija - Sigurnost” na stranici 40

Podešavanje postavki pretraživanja

Možete postaviti parametre pretraživanja kako bi kontrolirali korisničke sposobnosti pretraživanja, kao što je pretraživanje stranice i sortirano pretraživanje.

Rezultati stranice vam omogućavaju da upravljate s količinom podataka koji su vraćeni od zahtjeva pretraživanja. Možete zahtijevati podskup unosa (stranica) umjesto da odjednom primite sve rezultate. Naredni zahtjev za pretraživanjem prikazuje sljedeću stranicu rezultata tako dugo dok se operacija ne opozove ili dok se ne vrati posljednji rezultat.

Sortirano pretraživanje omogućuje klijentu da primi rezultate pretraživanja koji su sortirani popisom kriterija, gdje svaki kriterij predstavlja ključ sortiranja. Time se premješta odgovornost za sortiranje iz aplikacije klijenta na poslužitelja.

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

Podešavanje postavki izvedbe

Postavke izvedbe vašeg Poslužitelja direktorija možete podesiti mijenjanjem bilo čega od sljedećeg:
- ACL veličine predmemorije, veličine predmemorije unosa, maksimalnog broja unosa koji se spremaju u predmemoriju filtera i najvećeg pretraživanja koje će se staviti u predmemoriju klijenta.
- Postavki transakcije poslužitelja
- Broja veza baza podataka i niti poslužitelja

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

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

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

Upravljanje replikacijom

Kako bi upravljali replikacijom, proširite kategoriju **Upravljanje replikacijom** Web administracijskog alata. Za više informacija o konceptima replikacije, pogledajte “Replikacija” na stranici 34.

Pogledajte sljedeće za više informacija:
- “Kreiranje topologije glavni-replika”
- “Kreiranje topologije glavni-prosljeditelj-replika” na stranici 106
- “Pregled kreiranja kompleksne topologije replikacije” na stranici 108
- “Kreiranje kompleksne topologije s ravnopravnom replikacijom” na stranici 108
- “Upravljanje topologijama” na stranici 111
- “Modificiranje svojstava replikacije” na stranici 114
- “Kreiranje rasporeda replikacije” na stranici 115
- “Upravljanje redovima” na stranici 116

Kreiranje topologije glavni-replika

Da definirate osnovnu topologiju glavni-replika, morate:
1. Kreirati glavni direktorij i definirati njegov sadržaj. Izaberite podstablo koje želite replicirati i specificirajte poslužitelja kao glavnog. Pogledajte “Kreiranje glavnog poslužitelja (replicirano podstablo)” na stranici 102.
2. Kreirati vjerodajnice koje će koristiti dobavljač. Pogledajte “Kreiranje vjerodajnica” na stranici 103.
3. Kreirati replika poslužitelja. Pogledajte “Kreiranje replika poslužitelja” na stranici 104.

4. Eksportirati topologiju iz glavnog poslužitelja na repliku. Pogledajte “Kopiranje podataka na repliku” na stranici 105.
5. Promijeniti konfiguraciju replike kako bi identificirali tko je ovlašten da replicira promjene i dodati referal na glavnog poslužitelja. Pogledajte “Dodavanje informacija o dobavljaču na repliku” na stranici 106.

Bilješka:

Ako unos na korijenu podstabla za koje želite da bude replicirano nije sufiks u poslužitelju, prije nego možete koristiti funkciju **Dodaj podstablo**, morate osigurati da su ACL-ovi definirani kako slijedi:

Za ne-filtrirane ACL-ove:

```
ownersource: <isti kao i DN unosa>
ownerpropagate: TRUE

aclsource: <isti kao i DN unosa>
aclpropagate: TRUE
```

Za filtrirane ACL-ove:

```
ibm-filteraclinherit: FALSE
```

Kako bi zadovoljili ACL zahtjeve, ako unos nije sufiks u poslužitelju, uredite ACL za taj unos u panelu **Upravljaj unosima**. Izaberite unos i kliknite na **Uredi ACL**. Ako želite dodati ne-filtrirane ACL-ove, izaberite tu karticu i izaberite kontrolnu kućicu kako bi specificirali da li su ili nisu ACL-ovi izričiti za ACL-ove i vlasnike. Provjerite da li su označeni **Proširi ACL-ove** i **Proširi vlasnika**. Ako želite dodati Filtrirane ACL-ove izaberite tu karticu i dodajte unos **cn=this** s ulogom **access-id** za ACL-ove i vlasnike. Provjerite da li je poništen izbor za **Prikupi filtrirane ACL-ove** i da je izabrano **Širi korisnika**. Pogledajte “Upravljanje listama kontrole pristupa (ACL-ovi)” na stranici 145 kako bi dobili detaljnije informacije.

U početku, **ibm-replicagroup** objekt kreiran ovom obradom nasljeđuje ACL-ove ishodišnog unosa za replicirano podstablo. Ti ACL-ovi bi mogli biti neprikladni za kontroliranje pristupa informacijama o replikaciji u direktoriju.

Kreiranje glavnog poslužitelja (replicirano podstablo)

Bilješka: Poslužitelj mora raditi da bi se mogao izvesti ovaj zadatak.

Taj zadatak označava unos kao korijen nezavisno repliciranog podstabla i kreira **ibm-replicasubentry** koji predstavlja tog poslužitelja kao jednog glavnog poslužitelja za podstablo. Kako bi kreirali replicirano podstablo, morate označiti podstablo kojeg želite da replicira poslužitelj.

Proširite kategoriju Upravljanje replikacijom u području navigacije i kliknite na **Upravljanje topologijom**.

1. Kliknite na **Dodaj podstablo**.
2. Unesite DN unosa korijena podstabla kojeg želite replicirati ili kliknite na **Pregled** kako bi proširili unose i kako bi izabrali unos koji će biti korijen podstabla.
3. URL referal glavnog poslužitelja je prikazan u obliku LDAP URL, na primjer:

   ```
   ldap://<myservername>.<mylocation>.<mycompany>.com
   ```

   Bilješka: URL referal glavnog poslužitelja je neobavezan. On se koristi samo:
   - Ako poslužitelj sadrži (ili će sadržavati) bilo koja podstabla samo za čitanje.
   - Kako bi se definirao URL referal koji je vraćen za ažuriranje i bilo koje podstablo samo za čitanje na poslužitelju.
4. Kliknite **OK**.
5. Novi poslužitelj je prikazan na panelu Upravljanje topologijom pod naslovom **Replicirana podstabla**.

Kreiranje vjerodajnica

Proširite kategoriju Upravljanja replikacijom u području navigacije Web administracijskog alata i kliknite na **Upravljanje vjerodajnicama**

1. Izaberite lokaciju koju želite koristiti i pohranite vjerodajnice s popisa podstabla. Web administracijski alat vam omogućava da definirate vjerodajnice na ovim lokacijama:
   - **cn=replication,cn=localhost**, koji čuvaju vjerodajnice samo na trenutnom poslužitelju.

     Bilješka: U većini slučajeva replikacije, preferira se smještanje vjerodajnica u cn=replication,cn=localhost jer ono osigurava veću sigurnost od repliciranih vjerodajnica koje su smještene na podstablu. No, postoje neke situacije u kojima nisu dostupne vjerodajnice smještene na cn=replication,cn=localhost.

     Ako pokušavate dodati repliku pod poslužitelja, na primjer poslužitelja A, a povezani ste na drugog poslužitelja s Web administracijskim alatom, poslužitelja B, polje **Izabrane vjerodajnice** ne prikazuje opciju **cn=replication,cn=localhost**. To je stoga jer ne možete čitati informacije ili ažurirati bilo koje informacije pod **cn=localhost** poslužiteljem A kada ste povezani na poslužitelja B.

     Opcija cn=replication,cn=localhost je dostupna samo kada je poslužitelj pod kojeg pokušavate dodati repliku isti onaj poslužitelj na kojeg ste povezani s Web administracijskim alatom.
   - Unutar repliciranog podstabla, u tom slučaju su vjerodajnice replicirane s ostatkom podstabla. Vjerodajnice koje su smještene u replicirano podstablo su kreirane ispod **ibm-replicagroup=default** unosa za to podstablo.

     Bilješka: Ako nije prikazano nijedno podstablo, otiđite na “Kreiranje glavnog poslužitelja (replicirano podstablo)” na stranici 102 radi uputa o kreiranju podstabla koje želite replicirati.
2. Kliknite **Dodaj**.
3. Unesite ime za vjerodajnice koje kreirate, na primjer, **mycreds**, cn= je već za vas ispunjeno u polju.
4. Izaberite tip metode za provjeru autentičnosti koju želite koristiti i kliknite na **Sljedeće**.
   - Ako ste izabrali jednostavnu provjeru autentičnosti vezanja:
     a. Unesite DN koji poslužitelj koristi za vezanje na repliku, na primjer, cn=any.
     b. Unesite lozinku koju poslužitelj koristi kada se povezuje na repliku, na primjer, tajna.
     c. Ponovo unesite lozinku da potvrdite da nema tiskarskih greški.
     d. Ako želite, unesite kratki opis vjerodajnica.
     e. Kliknite na **Završetak**.

     Bilješka: Možda ćete željeti zapisati DN vezanja vjerodajnice i lozinku za buduće korištenje. Ta lozinka će vam biti potrebna kod kreiranja ugovora o replici.
   - Ako ste izabrali Kerberos provjeru autentičnosti:
     a. Unesite DN Kerberos vezanja.
     b. Unesite lozinku vezanja.
     c. Ponovo unesite lozinku vezivanja kako bi je potvrdili.
     d. Ako želite, unesite kratki opis vjerodajnica. Nisu potrebne nikakve druge informacije. Pogledajte “Omogućavanje Kerberos provjere autentičnosti na Poslužitelju direktorija” na stranici 119 kako bi dobili dodatne informacije.
     e. Kliknite na **Završetak**.

     Po defaultu, dobavljač koristi vlastitog principala usluga za vezanje s potrošačem. Na primjer, ako je ime dobavljača master.our.org.com, a područje je SOME.REALM, DN je **ibm-Kn=ldap/master.our.org.com@SOME.REALM**. Vrijednost područja je osjetljiva na velika i mala slova. Ako postoji više od jednog dobavljača, morate specificirati principala i lozinku koje će koristiti svi dobavljači.

     Na poslužitelju na kojem ste kreirali vjerodajnice:

     a. Proširite **Upravljanje direktorijom** i kliknite na **Upravljanje unosima**.

b. Izaberite podstablo na kojem ste pohranili vjerodajnice, na primjer **cn=localhost** i kliknite na **Proširi**.
c. Izaberite **cn=replication** i kliknite na **Proširi**.
d. Izaberite kerberos vjerodajnice (ibm-replicationCredentialsKerberos) i kliknite na **Uredi atribute**.
e. Kliknite na karticu **Drugi atributi**.
f. Unesite **replicaBindDN**, na primjer, **ibm-kn=myprincipal@SOME.REALM**.
g. Unesite **replicaCredentials**. To je KDC lozinka koja se koristi za **myprincipal**.

Bilješka: Taj principal i lozinka bi trebali biti jednaki onima koje koristite kako bi se izvodio **kinit** iz reda za naredbe.

Na replici

a. Kliknite na **Upravljanje svojstvima replikacije** u području navigacije.
b. Izaberite dobavljača iz padajućeg izbornika **Informacije o dobavljaču** ili unesite ime repliciranog podstabla za koje želite konfigurirati vjerodajnice dobavljača.
c. Kliknite na **Uredi**.
d. Unesite DN vezanja replikacije. U ovom primjeru, **ibm-kn=myprincipal@SOME.REALM**.
e. Unesite i potvrdite **Lozinku vezanja replikacije**. To je KDC lozinka koja se koristi za **myprincipal**.

- Ako ste izabrali SSL s provjerom autentičnosti certifikata, onda ne trebate osigurati nikakve dodatne informacije ako koristite certifikat poslužitelja. Ako izaberete korištenje certifikata koji nije certifikat poslužitelja:
  a. Unesite ime datoteke ključa.
  b. Unesite lozinku datoteke ključa.
  c. Ponovo unesite lozinku datoteke ključa kako bi je potvrdili.
  d. Unesite oznaku ključa.
  e. Ako želite, unesite kratki opis.
  f. Kliknite na **Završetak**.

  Pogledajte “Omogućavanje SSL-a na Poslužitelju direktorija” na stranici 117 kako bi dobili dodatne informacije.

5. Na poslužitelju na kojem ste kreirali vjerodajnice postavite sistemsku vrijednost Dozvoli zadržavanje informacija sigurnosti poslužitelja (QRETSVRSEC) na 1 (zadrži podatke). Budući su vjerodajnice replikacije pohranjene u validacijskoj listi, to omogućuje poslužitelju da dohvati vjerodajnice za validacijske liste kada se povezuje na repliku.

Kreiranje replika poslužitelja

Bilješka: Poslužitelj mora raditi da bi se mogao izvesti ovaj zadatak.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje topologijom**.

1. Izaberite podstablo koje želite replicirati i kliknite na **Prikaži topologiju**.
2. Kliknite na strelicu uz izbor **Topologija replikacije** kako bi proširili popis poslužitelja dobavljača.
3. Izaberite poslužitelj dobavljača i kliknite na **Dodaj repliku**.

Na karticu **Poslužitelj** prozora **Dodajte repliku**:

- Unesite ime hosta i broj porta za repliku koju kreirate. Default port je 389 za ne-SSL i 636 za SSL. To su potrebna polja.
- Izaberite da li ćete omogućiti SSL komunikacije.
- Unesite ime replike ili ostavite to polje praznim kako bi se koristilo ime hosta.
- Unesite ID replike. Ako se izvodi poslužitelj na kojem kreirate repliku, kliknite na **Dobavi ID replike** kako bi se automatski popunilo to polje. To je nužno polje ako će poslužitelj kojeg dodajete biti ravnopravan poslužitelj ili poslužitelj prosljeđivanja. Preporuča se da svi poslužitelji budu na istom izdanju.

- Unesite opis replika poslužitelja.

Na kartici **Dodatno**:

1. Specificirajte vjerodajnice koje replika koristi za komuniciranje s glavnim poslužiteljem.

   Bilješka: Web administracijski alat vam omogućava da definirate vjerodajnice u ovim mjestima:
   - **cn=replication,cn=localhost**, čuvaju vjerodajnice samo na poslužitelju koji ih koristi.
   - Unutar repliciranog podstabla, u tom slučaju su vjerodajnice replicirane s ostatkom podstabla. Vjerodajnice koje su smještene u replicirano podstablo su kreirane ispod **ibm-replicagroup=default** unosa za to podstablo.

   Smještanje vjerodajnica u cn=replication,cn=localhost se smatra sigurnijim.

   a. Kliknite na **Izaberite**.
   b. Izaberite lokaciju za vjerodajnice koje želite koristiti. Preferira se da to bude cn=replication,cn=localhost.
   c. Kliknite na **Prikaži vjerodajnice**.
   d. Proširite popis vjerodajnica i izaberite jednu koju želite koristiti.
   e. Kliknite **OK**.

   Pogledajte “Kreiranje vjerodajnica” na stranici 103 za dodatne informacije o vjerodajnicama ugovora.
2. Specificirajte raspored replikacije iz padajućeg popisa ili kliknite na **Dodaj** da kreirate jedan. Pogledajte “Kreiranje rasporeda replikacije” na stranici 115
3. Iz popisa sposobnosti dobavljača možete poništiti izbor bilo kojih sposobnosti za koje ne želite da se repliciraju na potrošača.

   Ako vaša mreža ima različite poslužitelje na različitim izdanjima, na novijim izdanjima su dostupne sposobnosti koje nisu dostupne na ranijim izdanjima. Neke sposobnosti, kao što su ACL-ovi filtera i lozinka politike, koriste operativne atribute koji su replicirani s drugim promjenama. U većini slučajeva, ako se koriste te osobine, želite da ih podržavaju svi poslužitelji. Ako svi poslužitelji ne podržavaju neku sposobnost, nemojte ga koristiti. Na primjer, ne želite da različiti ACL-ovi budu učinkoviti na svakom poslužitelju. Međutim, postoje neki slučajevi kada ćete možda željeti koristiti sposobnost na poslužiteljima koji ju podržavaju, a da se promjene koje se odnose na sposobnost ne repliciraju na poslužitelj koji ne podržava sposobnost. U takvim slučajevima možete koristiti listu sposobnosti kako bi označili da ne želite da se neke sposobnosti repliciraju.
4. Kliknite na **OK** kako bi kreirali repliku.
5. Prikazuje se poruka koja označava da se moraju poduzeti dodatne akcije. Kliknite **OK**.

Bilješka: Ako dodajete više poslužitelja kao dodatne replike ili kreirate kompleksnu topologiju, nemojte nastaviti s “Kopiranje podataka na repliku” ili “Dodavanje informacija o dobavljaču na repliku” na stranici 106 dok ne dovršite definiranje topologije na glavnom poslužitelju. Ako kreirate *masterfile.ldif* nakon što ste dovršili topologiju, ona sadrži unose direktorije glavnog poslužitelja i potpunu kopiju ugovora topologije. Kada učitate tu datoteku na svakog od poslužitelja, svaki poslužitelj ima iste informacije.

Kopiranje podataka na repliku

Nakon kreiranja replike morate eksportirati topologiju iz glavnog poslužitelja na repliku.

1. Na glavnom poslužitelju kreirajte LDIF datoteku za podatke. Kako bi kopirali podatke sadržane na glavnom poslužitelju, napravite sljedeće:
   a. U iSeries Navigator, proširite **Mreža**.
   b. Proširite **Poslužitelji**.
   c. Kliknite na **TCP/IP**.
   d. Desnom tipkom kliknite na **Direktorij** i izaberite **Alati**, a zatim **Eksport datoteke**.
   e. Specificirajte ime izlazne LDIF datoteke (na primjer masterfile.ldif), neobavezno specificirajte podstablo koje će se eksportirati (na primjer subtreeDN) i kliknite na **OK**.
2. Na stroju na kojem kreirate repliku napravite sljedeće:
   a. Provjerite da li su replicirani sufiksi definirani u konfiguraciji replika poslužitelja.
   b. Zaustavite replika poslužitelj.

c. Kopirajte LDIF datoteku na repliku i napravite sljedeće:
   1) U iSeries Navigator, proširite **Mreža**.
   2) Proširite **Poslužitelji**.
   3) Kliknite na **TCP/IP**.
   4) Desnom tipkom kliknite na **Direktorij** i izaberite **Alati**, a zatim **Import datoteke**.
   5) Specificirajte ime ulazne LDIF datoteke (na primjer masterfile.ldif), neobavezno specificirajte da li želite replicirati podatke i kliknite na **OK**.

   Ugovori replikacije, rasporedi, vjerodajnice (ako su pohranjene u podstablu replikacije) i unosi podataka se učitavaju na repliku.

d. Pokrenite poslužitelj.

Dodavanje informacija o dobavljaču na repliku

Trebate promijeniti konfiguraciju replike kako bi identificirali tko je ovlašten da replicira promjene i dodati referala na glavnog poslužitelja.

Na stroju na kojem kreirate repliku:

1. Proširite **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje svojstvima replikacije**.
2. Kliknite **Dodaj**.
3. Izaberite dobavljača iz padajućeg izbornika **Replicirano podstablo** ili unesite ime repliciranog podstabla za koje želite konfigurirati vjerodajnice dobavljača. Ako uređujete vjerodajnice dobavljača, to polje se ne može uređivati.
4. Unesite DN vezanja replikacije. U ovom primjeru, cn=any.

   Bilješka: Možete koristiti bilo koju od te dvije opcije, ovisno o vašoj situaciji.
   - Postavite DN vezanja replikacije (i lozinku) i default referal za sva podstabla replicirana na poslužitelju korištenjem 'default vjerodajnice i referali'. To bi se moglo koristiti kada su sva podstabla replicirana iz istog dobavljača.
   - Postavite DN vezanja replikacije i lozinku neovisno za svako replicirano podstablo dodavanjem informacije o dobavljaču za svako podstablo. To bi se moglo koristiti kada svako podstablo ima drugačijeg dobavljača (odnosno, različiti glavni poslužitelj za svako podstablo).
5. Ovisno o tipu vjerodajnice, unesite i potvrdite lozinku vjerodajnice. (Ranije ste je zapisali za buduće korištenje.)
   - **Jednostavno vezanje** - Specificirajte DN i lozinku.
   - **Kerberos** - Ako vjerodajnice na dobavljaču ne identificiraju principale i lozinku, odnosno, koristit će se principal usluge poslužitelja, onda je DN vezanja ibm-kn=ldap/<*yourservername@yourrealm*>. Ako vjerodajnice imaju ime principala kao što je <*myprincipal@myrealm*>, koristite to kao DN. U svakom slučaju, lozinka nije potrebna.
   - **SSL w/ EXTERNAL vezanje** - Specificirajte DN subjekta za certifikat bez lozinke.

   Pogledajte "Kreiranje vjerodajnica" na stranici 103.
6. Kliknite **OK**.
7. Morate ponovno pokrenuti repliku kako bi primjene imale učinka.

Pogledajte "Modificiranje svojstava replikacije" na stranici 114 kako bi dobili dodatne informacije.

Replika je u suspendiranom stanju i ne dolazi do replikacije. Nakon što ste dovršili postavljanje vaše topologije replikacije, morate kliknuti na **Upravljanje redovima**, izabrati repliku i kliknuti na **Odgodi/nastavi** kako bi započeli replikaciju. Pogledajte "Upravljanje redovima" na stranici 116 kako bi dobili detaljnije informacije. Replika sada prima ažuriranja iz glavnog poslužitelja.

Kreiranje topologije glavni-prosljeditelj-replika

Za definiranje topologije glavni-prosljeditelj-replika, morate:

1. Kreirati glavni poslužitelj i replika poslužitelj. Pogledajte "Kreiranje topologije glavni-replika" na stranici 101.

2. Kreirati novi poslužitelj replike za originalnu repliku. Pogledajte “Kreiranje novog replika poslužitelja”.
3. Kopirajte podatke na replike. Pogledajte “Kopiranje podataka na repliku” na stranici 105.

Kreiranje novog replika poslužitelja

Ako ste postavili topologiju replikacije (pogledajte “Kreiranje glavnog poslužitelja (replicirano podstablo)” na stranici 102) s glavnim poslužiteljem (server1) i replika poslužiteljem (server2), možete promijeniti ulogu za poslužitelja server2 na onu poslužitelja prosljeđivanja. Kako bi to napravili, trebate kreirati novu repliku (server3) pod poslužiteljem server2.

1. Povežite Web administraciju s glavnim poslužiteljem (server1)
2. Proširite kategoriju Upravljanje replikacijom u području navigacije i kliknite na **Upravljanje topologijom**.
3. Izaberite podstablo koje želite replicirati i kliknite na **Prikaži topologiju**.
4. Kliknite na strelicu uz izbor **Topologija replikacije** kako bi proširili popis poslužitelja dobavljača.
5. Kliknite na strelicu uz izbor poslužitelja **server1** kako bi proširili popis poslužitelja.
6. Izaberite poslužitelj server2 i kliknite na **Dodaj repliku**.
7. Na karticu **Poslužitelj** prozora **Dodajte repliku**:
   - Unesite ime hosta i broj porta za repliku (server3) koju kreirate. Default port je 389 za ne-SSL i 636 za SSL. To su potrebna polja.
   - Izaberite da li ćete omogućiti SSL komunikacije.
   - Unesite ime replike ili ostavite to polje praznim kako bi se koristilo ime hosta.
   - Unesite ID replike. Ako se izvodi poslužitelj na kojem kreirate repliku, kliknite na **Dobavi ID replike** kako bi se automatski popunilo to polje. To je nužno polje ako će poslužitelj kojeg dodajete biti ravnopravan poslužitelj ili poslužitelj prosljeđivanja. Preporuča se da svi poslužitelji budu na istom izdanju.
   - Unesite opis replika poslužitelja.

   Na kartici **Dodatno**:

   a. Specificirajte vjerodajnice koje replika koristi za komuniciranje s glavnim poslužiteljem.

      Bilješka: Web administracijski alat vam omogućava da definirate vjerodajnice na dva mjesta:
      - **cn=replication,cn=localhost**, vjerodajnice se čuvaju samo na poslužitelju koji ih koristi.
      - Unutar repliciranog podstabla, u tom slučaju su vjerodajnice replicirane s ostatkom podstabla.

      Smještanje vjerodajnica u cn=replication,cn=localhost se smatra sigurnijim. Vjerodajnice koje su smještene u replicirano podstablo su kreirane ispod **ibm-replicagroup=default** unosa za to podstablo.

      1) Kliknite na **Izaberite**.
      2) Izaberite lokaciju za vjerodajnice koje želite koristiti. Preferira se da to bude cn=replication,cn=localhost.
      3) Kliknite na **Prikaži vjerodajnice**.
      4) Proširite popis vjerodajnica i izaberite jednu koju želite koristiti.
      5) Kliknite **OK**.

      Pogledajte “Kreiranje vjerodajnica” na stranici 103 za dodatne informacije o vjerodajnicama ugovora.

   b. Specificirajte raspored replikacije iz padajućeg popisa ili kliknite na **Dodaj** da kreirate jedan. Pogledajte “Kreiranje rasporeda replikacije” na stranici 115.

   c. Iz popisa sposobnosti dobavljača možete poništiti izbor bilo kojih sposobnosti za koje ne želite da se repliciraju na potrošača.

      Ako vaša mreža ima različite poslužitelje na različitim izdanjima, na novijim izdanjima su dostupne sposobnosti koje nisu dostupne na ranijim izdanjima. Neke sposobnosti, kao što su ACL-ovi filtera i lozinka politike, koriste operativne atribute koji su replicirani s drugim promjenama. U većini slučajeva, ako se koriste te osobine, želite da ih podržavaju svi poslužitelji. Ako svi poslužitelji ne podržavaju neku sposobnost, nemojte ga koristiti. Na primjer, ne želite da različiti ACL-ovi budu učinkoviti na svakom poslužitelju. Međutim, postoje neki slučajevi kada ćete možda željeti koristiti sposobnost na poslužiteljima koji ju podržavaju, a da se

promjene koje se odnose na sposobnost ne repliciraju na poslužitelj koji ne podržava sposobnost. U takvim slučajevima možete koristiti listu sposobnosti kako bi označili da ne želite da se neke sposobnosti repliciraju.

d. Kliknite na **OK** kako bi kreirali repliku.

8. Kopirajte podatke iz poslužitelja server2 na novog replika poslužitelja server3. Pogledajte “Kopiranje podataka na repliku” na stranici 105 kako bi dobili informacije kako da to napravite.
9. Dodajte ugovor dobavljača na poslužitelja server3 koji čini poslužitelja server2 dobavljačem za server3, a server3 potrošačem za server2. Pogledajte “Dodavanje informacija o dobavljaču na repliku” na stranici 106 kako bi dobili informacije kako to napraviti.

Uloge poslužitelj su predstavljene ikonama u Web administracijskom alatu. Sada je vaša topologija:

- server1 (glavni)
  - server2 (prosljeditelj)
    - server3 (replika)

Pregled kreiranja kompleksne topologije replikacije

Koristite ovaj pregled visoke razine kao vodič za postavljanje topologije kompleksne replikacije.

1. Pokrenite sve glavne poslužitelje ili buduće replike. To je potrebno stoga kako bi Web administracijski alat skupio informacije od poslužitelja.
2. Pokrenite ’prvi’ glavni poslužitelj i konfigurirajte ga kao glavnog za kontekst.
3. Učitajte podatke za podstablo koji će se replicirati na ’prvom’ glavnom poslužitelju, ako ti podaci nisu već učitani.
4. Izaberite podstablo koje će se replicirati.
5. Dodajte sve potencijalne ravnopravne glavne poslužitelje kao replike ’prvog’ glavnog poslužitelja.
6. Dodajte sve druge replike.
7. Premjestite ostale ravnopravne glavne poslužitelje kako bi ih promovirali.
8. Dodajte ugovore replike za replike svakog ravnopravnog glavnog poslužitelja.

   Bilješka: Ako bi se trebale kreirati vjerodajnice u **cn=replication,cn=localhost**, vjerodajnice se moraju kreirati na svakom poslužitelju nakon što su bile ponovo pokrenute. Replikacija od strane ravnopravnih poslužitelja neće uspjeti dok se ne kreiraju objekti replikacije.
9. Dodajte ugovore replike za druge glavne poslužitelje na svakog ravnopravnog glavnog poslužitelja. ’Prvi’ glavni poslužitelj već ima te informacije.
10. Umirite replicirano podstablo. Time se sprječava ažuriranje dok se kopiraju podaci na druge poslužitelje.
11. Koristite Upravljanje redom kako bi sve preskočili za svaki red.
12. Eksportirajte podatke za replicirano podstablo iz ’prvog’ glavnog poslužitelja.
13. Uznemirite podstablo.
14. Zaustavite replika poslužitelje i importirajte podatke za replicirano podstablo na svaku repliku i ravnopravnog glavnog poslužitelja. Nakon toga ponovo pokrenite poslužitelje.
15. Upravljajte svojstvima replikacije na svakom poslužitelju i ravnopravnom glavnom poslužitelju kako bi postavili vjerodajnice koje će koristiti dobavljači.

Kreiranje kompleksne topologije s ravnopravnom replikacijom

Ravnopravna replikacija je topologija replikacije u kojoj ima više glavnih poslužitelja. No, za razliku od okoline s više glavnih poslužitelja, nema nikakvog sistema za rješavanja sukoba između ravnopravnih poslužitelja. LDAP poslužitelji prihvaćaju ažuriranja koje osiguravaju ravnopravni poslužitelji i ažuriraju svoje vlastite kopije podataka. Ne vodi se računa o poretku u kojem su primljena ažuriranja ili o tome da li su višestruka ažuriranja u sukobu.

Za dodavanje dodatnih glavnih (ravnopravnih) poslužitelja, prvo trebate dodati poslužitelj kao samo za čitanje repliku postojećih glavnih poslužitelja (pogledajte “Kreiranje replika poslužitelja” na stranici 104), inicijalizirati podatke direktorija i onda promovirati poslužitelj tako da bude glavni poslužitelj (pogledajte “Premještanje ili promoviranje poslužitelja” na stranici 112).

U početku, **ibm-replicagroup** objekt kreiran ovom obradom nasljeđuje ACL-ove ishodišnog unosa za replicirano podstablo. Ti ACL-ovi bi mogli biti neprikladni za kontroliranje pristupa informacijama o replikaciji u direktoriju.

Kako bi bila uspješna operacija Dodaj podstablo, DN unosa kojeg dodajete mora imati ispravne ACL-ove, ako nije sufiks u poslužitelju.

Za ne-filtrirane ACL-ove :

- ownersource : <*DN unosa*>
- ownerpropagate : TRUE
- aclsource : <*DN unosa*>
- aclpropagate: TRUE

Filtrirani ACL-ovi :

- ownersource : <*DN unosa*>
- ownerpropagate : TRUE
- ibm-filteraclinherit : FALSE
- ibm-filteraclentry : <*bilo koja vrijednost*>

Koristite funkciju **Uredi ACL-ove** Web administracijskog alata da postavite ACL-ove za informacije o replikaciji koje su pridružene novo kreiranom repliciranom podstablu (pogledajte “Uređivanje lista kontrole pristupa” na stranici 113).

Replika je u suspendiranom stanju i ne dolazi do replikacije. Nakon što ste dovršili postavljanje vaše topologije replikacije, morate kliknuti na **Upravljanje redovima**, izabrati repliku i kliknuti na **Odgodi/nastavi** kako bi započeli replikaciju. Pogledajte “Upravljanje redovima” na stranici 116 kako bi dobili detaljnije informacije. Replika sada prima ažuriranja iz glavnog poslužitelja.

Ravnopravnu replikaciju koristite samo u okolinama u kojima je dobro poznat obrazac ažuriranja direktorija. Ažuriranja na određenim objektima unutar direktorija mora izvoditi samo jedan glavni poslužitelj. To je zato da se spriječi scenarij u kojem jedan poslužitelj briše objekt, a nakon toga drugi poslužitelj modificira objekt. Taj scenarij bi mogao rezultirati time da glavni poslužitelj primi naredbu brisanja koju slijedi naredba za modificiranje; tako nastaje sukob.

Kako bi definirali ravnopravni-proslijeditelj-replika topologiju koja se sastoji od dva ravnopravno-glavna poslužitelja, dva poslužitelja prosljeđivanja i četiri replike, morate:

1. Kreirati glavni poslužitelj i replika poslužitelj. Pogledajte “Kreiranje topologije glavni-replika” na stranici 101.
2. Kreirati dva dodatna replika poslužitelja za glavnog poslužitelja. Pogledajte “Kreiranje replika poslužitelja” na stranici 104.
3. Kreirati dvije replike ispod svakog od dva novo kreirana replika poslužitelja.
4. Promovirati originalnu repliku na poslužitelja. Pogledajte “Promoviranje poslužitelja tako da bude ravnopravan”.

   Bilješka: Poslužitelj kojeg želite promovirati na glavnog poslužitelja mora biti replika s listovima bez podložnih replika.
5. Kopirajte podatke iz glavnog poslužitelja na novi glavni poslužitelj i repliku. Pogledajte “Kopiranje podataka na repliku” na stranici 105.

Promoviranje poslužitelja tako da bude ravnopravan

Korištenjem topologije prosljeđivanja kreirane u “Kreiranje topologije glavni-prosljeditelj-replika” na stranici 106, možete promovirati poslužitelja tako da bude ravnopravan. U ovom ćete primjeru promovirati replika poslužitelja (server3) tako da bude ravnopravan na glavnom poslužitelju (server1).

1. Povežite Web administraciju na glavni poslužitelj (server1).
2. Proširite kategoriju Upravljanje replikacijom u području navigacije i kliknite na **Upravljanje topologijom**.
3. Izaberite podstablo koje želite replicirati i kliknite na **Prikaži topologiju**.
4. Kliknite na strelicu uz izbor **Topologija replikacije** kako bi proširili popis poslužitelja.

5. Kliknite na strelicu uz izbor poslužitelja **server1** kako bi proširili popis poslužitelja.
6. Kliknite na strelicu uz izbor poslužitelja **server2** kako bi proširili popis poslužitelja.
7. Kliknite na **server1** i kliknite na **Dodaj repliku**. Kreirajte poslužitelj server4. Pogledajte “Kreiranje replika poslužitelja” na stranici 104. Slijedite istu proceduru kako bi kreirali poslužitelj server5. Uloge poslužitelj su predstavljene ikonama u Web administracijskom alatu. Sada je vaša topologija:
   - server1 (glavni)
     - server2 (prosljeditelj)
       - server3 (replika)
     - server4 (replika)
     - server5 (replika)
8. Kliknite na **server2** i kliknite na **Dodaj repliku** kako bi kreirali poslužitelj server6.
9. Kliknite na **server4** i kliknite na **Dodaj repliku** kako bi kreirali poslužitelj server7. Slijedite istu proceduru kako bi kreirali poslužitelj server8. Sada je vaša topologija:
   - server1 (glavni)
     - server2 (prosljeditelj)
       - server3 (replika)
       - server6 (replika)
     - server4 (prosljeditelj)
       - server7 (replika)
       - server8 (replika)
     - server5 (replika)
10. Izaberite **server5** i kliknite na **Premjesti**.

    Bilješka: Poslužitelj kojeg želite premjestiti mora biti replika s listovima bez podređenih replika.
11. Izaberite **Topologija replikacije** kako bi promovirali repliku na glavnog poslužitelja. Kliknite na **Premjesti**.
12. Prikazan je panel **Kreiraj dodatne ugovore dobavljača**. Ravnopravna replikacija traži da svaki glavni poslužitelj bude dobavljač i potrošač svakom od drugih glavnih poslužitelja u topologiji i svakom od replika prve razine, server2 i server4. Server5 je već potrošač od server1, sada treba postati dobavljač za server1, server2 i server4. Provjerite da li je u kućicama ugovora dobavljača označeno:

Tablica 3.

	Dobavljač	Potrošač
✓	server5	server1
✓	server5	server2
✓	server5	server4

Kliknite na **Nastavak**.

Bilješka: U nekim će slučajevima iskočiti panel Izaberi vjerodajnice koji će od vas tražiti vjerodajnicu koja je smještena negdje drugdje, a ne na cn=replication,cn=localhost. U takvim situacijama morate osigurati objekt vjerodajnice koji se nalazi negdje drugdje, a ne na cn=replication,cn=localhost. Izaberite vjerodajnice koje će koristiti podstablo, oblikujte postojeće skupove vjerodajnica ili kreirajte nove vjerodajnice. Pogledajte “Kreiranje vjerodajnica” na stranici 103

.

13. Kliknite **OK**. Sada je vaša topologija:
    - server1 (glavni)
      - server2 (prosljeditelj)
        - server3 (replika)
        - server6 (replika)

- server4 (prosljeditelj)
  - server7 (replika)
  - server8 (replika)
- server5 (glavni)

- server5 (glavni)
  - server1 (glavni)
  - server2 (prosljeditelj)
  - server4 (prosljeditelj)

14. Kopirajte podatke iz poslužitelja server1 na sve poslužitelje. Pogledajte “Kopiranje podataka na repliku” na stranici 105 kako bi dobili informacije kako da to napravite.

Upravljanje topologijama

Topologije su specifične za replicirana podstabla.

- “Pregled topologije”
- “Dodavanje replike”
- “Uređivanje ugovora”
- “Premještanje ili promoviranje poslužitelja” na stranici 112
- “Degradacija glavnog” na stranici 112
- “Repliciranje podstabla” na stranici 112
- “Uređivanje podstabla” na stranici 113
- “Uklanjanje podstabla” na stranici 113
- “Umirivanje podstabla” na stranici 113
- “Uređivanje lista kontrole pristupa” na stranici 113

Pregled topologije

Bilješka: Poslužitelj mora raditi da bi se mogao izvesti ovaj zadatak.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje topologijom**.

1. Izaberite podstablo koje želite pregledati i kliknite na **Prikaži topologiju**.

Topologija se prikazuje u popisu Topologija replikacije. Proširite topologije tako da kliknete na plave trokutiće. Iz tog popisa možete:

- Dodati repliku.
- Uređivati informacije na postojećoj replici.
- Izabrati drugog poslužitelja dobavljača za repliku ili promovirati repliku na glavnog poslužitelja
- Obrisati repliku.

Dodavanje replike

Pogledajte “Kreiranje replika poslužitelja” na stranici 104.

Uređivanje ugovora

Možete promijeniti dodatne informacije za repliku:

Na kartici **Poslužitelj** možete promijeniti samo

- Ime glavnog poslužitelja
- Port
- Omogućavanje SSL-a
- Opis

Na kartici **Dodatno** možete promijeniti:

- Vjerodajnice - pogledajte “Kreiranje vjerodajnica” na stranici 103.
- Rasporede replikacija - pogledajte “Kreiranje rasporeda replikacije” na stranici 115.
- Promijenite svojstva koja su replicirana na repliku potrošača. Iz popisa sposobnosti dobavljača možete poništiti izbor bilo kojih sposobnosti za koje ne želite da se repliciraju na potrošača.
- Kada završite, kliknite na **OK**.

Premještanje ili promoviranje poslužitelja

1. Izaberite poslužitelj koji želite i kliknite na **Premjesti**.
2. Izaberite poslužitelj na kojeg želite premjestiti repliku ili izaberite **Topologija replikacije** kako bi promovirali repliku na glavnog poslužitelja. Kliknite na **Premjesti**.
3. U nekim će slučajevima iskočiti panel Izaberi vjerodajnice koji će od vas tražiti vjerodajnicu koja je smještena negdje drugdje, a ne na cn=replication,cn=localhost. U takvim situacijama morate osigurati objekt vjerodajnice koji se nalazi negdje drugdje, a ne na cn=replication,cn=localhost. Izaberite vjerodajnice koje će koristiti podstablo, oblikujte postojeće skupove vjerodajnica ili kreirajte nove vjerodajnice. Pogledajte “Kreiranje vjerodajnica” na stranici 103.
4. Prikazan je panel **Kreiraj dodatne ugovore dobavljača**. Izaberite ugovore dobavljača koji su prikladni za ulogu poslužitelja. Na primjer, ako se replika poslužitelj promovira da bude ravnopravan poslužitelj, morate kreirati ugovore dobavljača sa svim drugim poslužiteljima i njihovim replikama prve razine. Ti ugovori omogućuju promoviranom poslužitelju da se ponaša kao dobavljač za druge poslužitelje i njihove replike. Postojeći ugovori dobavljača iz drugih poslužitelja na novo promovirane poslužitelje su i dalje aktivni i ne trebaju se ponovo kreirati.
5. Kliknite **OK**.

Promjena u stablu topologije odražava premještanje poslužitelja.

Pogledajte “Kreiranje kompleksne topologije s ravnopravnom replikacijom” na stranici 108 za više informacija.

Degradacija glavnog

Da promijenite ulogu poslužitelja iz glavnog na repliku, napravite sljedeće:

1. Povežite Web administracijski alat na poslužitelj koji želite degradirati.
2. Kliknite na **Upravljanje topologijom**.
3. Izaberite podstablo i kliknite na **Prikaz topologije**.
4. Obrišite sve ugovore za poslužitelj koji želite degradirati.
5. Izaberite poslužitelj koji ćete degradirati i kliknite na **Premjesti**.
6. Izaberite poslužitelj pod koji ćete smjestiti poslužitelj koji ste degradirali i kliknite na **Premjesti**.
7. Kao što bi to napravili i za novu repliku, kreirajte nove ugovore dobavljača između poslužitelja koji ste degradirali i njegovog dobavljača. Pogledajte “Kreiranje replika poslužitelja” na stranici 104 za upute.

Repliciranje podstabla

Bilješka: Poslužitelj mora raditi da bi se mogao izvesti ovaj zadatak.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje topologijom**.

- Kliknite na **Dodaj podstablo**.
- Unesite DN podstabla koje želite replicirati ili kliknite na **Pregled** da proširite unose i izaberete unos koji će biti korijen podstabla.
- Unesite URL referal glavnog poslužitelja. To mora biti u obliku LDAP URL-a, na primjer:
  `ldap://<myservername>.<mylocation>.<mycompany>.com`
- Kliknite **OK**.
- Novi poslužitelj je prikazan na panelu Upravljanje topologijom pod naslovom **Replicirana podstabla**.

Uređivanje podstabla

Koristite ovu opciju kako bi promijenili URL glavnog poslužitelja kojemu to podstablo i njezine replike šalju ažuriranja. To trebate napraviti ako promijenite broj porta ili ime hosta glavnog poslužitelja, promijenite glavnog poslužitelja na drugog poslužitelja

1. Izaberite podstablo koje želite uređivati.
2. Kliknite na **Uredi podstablo**.
3. Unesite URL referal glavnog poslužitelja. To mora biti u obliku LDAP URL-a, na primjer:
   `ldap://<mynewservername>.<mylocation>.<mycompany>.com`

Ovisno o ulozi poslužitelja na tom podstablu (da li je glavni, replika ili proslijeditelj), na panelu će se pojavljivati različite oznake i gumbi.

- Kada je uloga podstabla replika, prikazuje se oznaka koja označava da se poslužitelj ponaša kao replika ili prosljeditelj, zajedno s gumbom **Napravi poslužitelj glavnim**. Ako se klikne na taj gumb, onda poslužitelj na kojeg je povezan Web administracijski alat postaje glavni poslužitelj.
- Kada je podstablo konfigurirano za replikaciju samo dodavanjem pomoćnih klasa (nema default grupe i podunosa), onda se prikazuje oznaka **To podstablo nije replicirano** zajedno s gumbom **Repliciraj podstablo**. Ako se klikne na taj gumb, dodaje se default grupa i podunos tako da poslužitelj s kojim je povezan Web administracijski alat postane glavnim.
- Ako nisu pronađeni podunosi za glavne poslužitelje, prikazuje se oznaka **Nije definiran glavni poslužitelj za to podstablo** zajedno s gumbom pod nazivom **Napravi poslužitelj glavnim**. Ako se klikne na taj gumb, dodaje se nedostajući podunos tako da poslužitelj s kojim je povezan Web administracijski alat postane glavnim.

Uklanjanje podstabla

1. Izaberite podstablo koje želite ukloniti.
2. Kliknite na **Brisanje podstabla**.
3. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**.

Podstablo se uklanja iz popisa **Replicirano podstablo**.

Bilješka: Ta će operacija uspjeti samo ako je prazan unos ibm-replicaGroup=default.

Umirivanje podstabla

Ta funkcija je korisna kada želite raditi održavanje ili promjene na topologiji. Ona minimizira broj ažuriranja koja se mogu napraviti na poslužitelju. Umireni poslužitelj ne prihvaća zahtjeve klijenta. Prihvaća zahtjeve samo od administratora koji koristi kontrolu Administracije poslužitelja.

Ta funkcija je booleova.

1. Kliknite na **Umiri/Uznemiri** kako bi umirili podstablo.
2. Kada se od vas zatraži da potvrdite akciju, kliknite na **OK**.
3. Kliknite na **Umiri/Uznemiri** kako bi podstablo izašlo iz umirenog stanja.
4. Kada se od vas zatraži da potvrdite akciju, kliknite na **OK**.

Uređivanje lista kontrole pristupa

Informacije o replikaciji (podunosi replike, ugovori replikacije, rasporedi, možda i vjerodajnice) su pohranjene pod posebnim objektom, **ibm-replicagroup=default**. Objekt ibm-replicagroup se nalazi odmah ispod unosa korijena repliciranog podstabla. Po defaultu, to podstablo nasljeđuje ACL iz unosa korijena repliciranog podstabla. Taj ACL možda neće biti prikladan za kontroliranje pristupa informacijama replikacije.

Potrebna ovlaštenja:

- Replikacija kontrole - Morate imati pristup za pisanje na ibm-replicagroup=default objekt (ili biti vlasnik/administrator).

- Replikacija kaskadne kontrole - Morate imati pristup za pisanje na ibm-replicagroup=default objekt (ili biti vlasnik/administrator).
- Red kontrole - Morate imati pristup za pisanje na ugovor replikacije.

Kako bi pregledali svojstva ACL-a korištenjem Web administracijskog alata i kako bi radili s ACL-ovima, pogledajte “Upravljanje listama kontrole pristupa (ACL-ovi)” na stranici 145.

Pogledajte “Lista kontrole pristupa” na stranici 47 kako bi dobili dodatne informacije.

Modificiranje svojstava replikacije

Proširite kategoriju **Upravljanje preslikom** u području navigacije i kliknite na **Svojstva upravljanja preslikom**. Morate se prijaviti na Alat za Web administraciju kao projicirani i5/OS korisnik s *ALLOBJ i *IOSYSCFG specijalnim ovlaštenjima da bi bilo prikazano Upravljaj svojstvima preslike.

Na ovom panelu možete:

- Promijeniti maksimalan broj promjena u stanju čekanja koje se vraćaju iz upita o statusu replikacije. Default je 200.
- Dodajte, uredite ili obrišite informacije o dobavljaču.

Bilješka: DN dobavljača može biti DN projiciranog i5/OS profila korisnika. Projicirani i5/OS profil korisnika ne smije imati LDAP administrativno ovlaštenje. Korisnik ne može biti korisnik s *ALLOBJ i *IOSYSCFG posebnim ovlaštenjima i nije mu se moglo dodijeliti administrativno ovlaštenje preko ID aplikacije administratora poslužitelja direktorija.

Za više informacija, pogledajte sljedeće:

- “Dodavanje informacija o dobavljaču”
- “Uređivanje informacija o dobavljaču” na stranici 115
- “Uklanjanje informacija o dobavljaču” na stranici 115

Dodavanje informacija o dobavljaču

1. Kliknite **Dodaj**.
2. Izaberite dobavljača iz padajućeg izbornika ili unesite ime repliciranog podstabla kojeg želite dodati kao dobavljača.
3. Unesite DN vezanja replikacije kako bi dobili vjerodajnice.

   Bilješka: Možete koristiti bilo koju od te dvije opcije, ovisno o vašoj situaciji.
   - Postavite DN vezanja replikacije (i lozinku) i default referal za sva podstabla replicirana na poslužitelju korištenjem ’default vjerodajnice i referali’. To bi se moglo koristiti kada su sva podstabla replicirana iz istog dobavljača.
   - Postavite DN vezanja replikacije i lozinku neovisno za svako replicirano podstablo dodavanjem informacije o dobavljaču za svako podstablo. To bi se moglo koristiti kada svako podstablo ima drugačijeg dobavljača (odnosno, različiti glavni poslužitelj za svako podstablo).
4. Ovisno o tipu vjerodajnice, unesite i potvrdite lozinku vjerodajnice. (Ranije ste je zapisali za buduće korištenje.)
   - **Jednostavno vezanje** - specificirajte DN i lozinku
   - **Kerberos** - specificirajte pseudo DN oblika ’ibm-kn=LDAP-service-name@realm’ bez lozinke
   - **SSL w/ EXTERNAL vezanje** - specificirajte DN subjekta za certifikat, bez dozvole

   Pogledajte “Kreiranje vjerodajnica” na stranici 103.
5. Kliknite **OK**.

Podstablo dobavljača se dodaje na listu informacije dobavljača.

Uređivanje informacija o dobavljaču

1. Izaberite podstablo dobavljača koje želite uređivati.
2. Kliknite na **Uredi**.
3. Ako uređujete **Default vjerodajnice i referal** koji se koriste za kreiranje cn=Glavni poslužitelj unosa pod cn=configuration, unesite URL za poslužitelj iz kojeg klijent želi primiti ažuriranja replike u polju Default LDAP URL dobavljača. To treba biti valjan LDAP URL (ldap://). U suprotnom, otiđite izravno na korak 4.
4. Unesite DN vezanja replikacije kako bi dobili nove vjerodajnice koje želite koristiti.
5. Unesite i potvrdite lozinku vjerodajnice.
6. Kliknite **OK**.

Uklanjanje informacija o dobavljaču

1. Izaberite podstablo dobavljača koje želite ukloniti.
2. Kliknite na **Briši**.
3. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**.

Podstablo se uklanja iz liste informacija o dobavljaču.

Kreiranje rasporeda replikacije

Možete neobavezno definirati rasporede replikacije kako bi rasporedili replikacije u određenom vremenu ili da nema replikacije u određenom vremenu. Ako ne koristite raspored, poslužitelj raspoređuje replikaciju uvijek kada se napravi promjena. To je ekvivalentno specificiranju rasporeda s trenutnom replikacijom koja počinje u 12:00 svakog dana.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje rasporedima**.

Na kartici **Tjedni raspored** izaberite podstablo za koje želite kreirati raspored i kliknite na **Prikaži rasporede**. Ako postoje rasporedi, oni se prikazuju u kućici **Tjedni rasporedi**. Kako bi kreirali ili dodali novi raspored:

1. Kliknite **Dodaj**.
2. Unesite ime za raspored. Na primjer **raspored1**.
3. Za svaki dan, od nedjelje do subote, dnevni raspored je specificiran kao **Ništa**. To znači da nisu raspoređeni događaji za ažuriranje replikacije. Još je aktivan zadnji događaj replikacije, ako je postojao. Budući se radi o novoj replici, pa ne postoje prethodni događaji replikacije, raspored se postavlja na neposrednu replikaciju.
4. Možete izabrati bilo koji dan i kliknuti na **Dodaj dnevni raspored** kako bi za njega kreirali dnevni raspored replikacije. Ako kreirate dnevni raspored, on postaje default raspored za svaki dan u tjednu. Možete:
   - Zadržati dnevni raspored kao default za svaki dan ili izabrati neki dan i promijeniti raspored natrag na ništa. Vodite računa o tome da je zadnji događaj replikacije koji se je dogodio i dalje aktivan za dan kada nije raspoređen nijedan događaj replikacije.
   - Modificirati dnevni raspored tako da izaberete dan i kliknete na **Uređivanje dnevnog rasporeda**. Vodite računa o tome da se dnevni raspored odnosi na sve dane koji koriste taj raspored, ne samo na dan kojeg ste izabrali.
   - Kreirati drugačiji dnevni raspored tako da izaberete dan i kliknete na **Dodavanje dnevnog rasporeda**. Nakon što kreirate taj raspored, on se dodaje na padajući izbornik **Dnevni raspored**. Taj raspored morate izabrati za svaki dan za koji želite da se koristi raspored.

   Pogledajte “Kreiranje dnevnog rasporeda” kako bi dobili više informacija o postavljanju dnevnih rasporeda.
5. Kada završite, kliknite na **OK**.

Kreiranje dnevnog rasporeda

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje rasporedima**.

Na kartici **Dnevni raspored** izaberite podstablo za koje želite kreirati raspored i kliknite na **Prikaži rasporede**. Ako postoje rasporedi, oni se prikazuju u kućici **Dnevni rasporedi**. Kako bi kreirali ili dodali novi raspored:

1. Kliknite **Dodaj**.
2. Unesite ime za raspored. Na primjer **ponedjeljak1**.

3. Izaberite postav vremenske zone, UTC ili lokalno.
4. Izaberite tip replikacije iz padajućeg izbornika:

   Odmah
   Izvodi bilo koja ažuriranja unosa u stanju čekanja od zadnjeg replikacijskog događaja i onda neprekidno ažurira raspored dok se ne dođe do sljedećeg raspoređenog događaja ažuriranja.

   Jednom
   Izvodi sva ažuriranja u stanju čekanja prije vremena pokretanja. Sva ažuriranja učinjena nakon vremena pokretanja čekaju do sljedećeg raspoređenog događaja replikacije.
5. Izaberite vrijeme pokretanja za događaj replikacije.
6. Kliknite **Dodaj**. Prikazuju se tip događaja replikacije i vrijeme.
7. Dodajte ili uklonite događaje kako bi dovršili svoj raspored. Popis događaja se osvježava u kronološkom poretku.
8. Kada završite, kliknite na **OK**.

Na primjer:

Tablica 4.

Tip replikacije	Vrijeme pokretanja
Odmah	12:00
Jednom	10:00
Jednom	14:00
Odmah	16:00
Jednom	20:00

U ovom rasporedu do prvog događaja replikacije dolazi u ponoć i ažuriraju se sve promjene u stanju čekanja prije tog vremena. Ažuriranja replikacije se rade onako kako se pojavljuju do 10:00. Ažuriranja napravljena između 10:00 i 14:00 čekaju do 14:00 da bi se replicirala. Sva ažuriranja napravljena između 14:00 i 16:00 čekaju na događaj replikacije koji je raspoređen za 16:00, nakon toga se ažuriranja replikacije nastavljaju do sljedećeg raspoređenog događaja replikacije u 20:00. Sva ažuriranja napravljena nakon 20:00 čekaju do sljedećeg raspoređenog događaja replikacije.

Bilješka: Ako su događaji replikacije raspoređeni previše blizu, moglo bi se desiti da se propusti događaj replikacije ako se još uvijek izvode ažuriranja iz prethodnog događaja kada je raspoređen sljedeći događaj.

Upravljanje redovima

Taj zadatak vam dozvoljava da nadgledate status replikacije za svaki ugovor replikacije (red) kojeg koristi taj poslužitelj.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje redovima**.

Izaberite repliku čijim redom želite upravljati.

- Ovisno o statusu replike, možete kliknuti na **Odgodi/nastavi** kako bi zaustavili ili pokrenuli replikaciju.
- Kliknite na **Prisili replikaciju** kako bi replicirali sve promjene u stanju čekanja bez obzira na to kada je raspoređena sljedeća replikacija.
- Kliknite na **Detalji reda** kako bi dobili više informacija o redu replike. Možete upravljati redom i iz ovog izbora.
- Kliknite na **Osvježi** kako bi ažurirali redove i obrisali poruke poslužitelja.

Detalji reda

Ako ste kliknuli na **Detalji reda**, prikazuju se tri kartice:

- Status
- Detalji o zadnjem pokušaju

- Promjene još u toku

Kartica **Status** prikazuje ime replike, njezino podstablo, njezin status i zapise o vremenima replikacije. S ovog panela možete odgoditi ili nastaviti replikaciju tako da kliknete na **Nastavak**. Kliknite na **Osvježi** da ažurirate informacije o redu.

Kartica **Detalji zadnjeg pokušaja** vam daje informacije o zadnjem pokušaju ažuriranja. Ako se unos ne može učitati, pritisnite na **Preskoči blokiranje unosa** kako bi nastavili replikaciju sa sljedećim unosom u stanju čekanja. Kliknite na **Osvježi** da ažurirate informacije o redu.

Kartica **Promjene u stanju čekanja** prikazuje sve promjene u stanju čekanja na replici. Ako je replikacija blokirana, možete obrisati sve promjene u stanju čekanja tako da kliknete na **Preskoči sve**. Kliknite na **Osvježi** kako bi ažurirali popis promjena u stanju čekanja tako da odražavaju bilo koje novo ažuriranje ili ažuriranja koja su bila obrađena.

Bilješka: Ako izaberete preskakanje promjena blokiranja, morate osigurati da se poslužitelj potrošača jednom ažurira. Pogledajte “ldapdiff” na stranici 178 za više informacija.

Omogućavanje SSL-a na Poslužitelju direktorija

Ako imate Upravitelj digitalnih certifikata instaliran na vašem sistemu, možete koristiti sigurnost Sloj sigurnih utičnica (SSL) kako bi zaštitili pristup na vaš Poslužitelj direktorija. Prije nego omogućite SSL na poslužitelju direktorija, možda bi bilo dobro da pročitate “Sloj sigurnih utičnica (SSL) i Sigurnost sloja transporta s Poslužiteljem direktorija” na stranici 41.

Za upotrebu SSL veze kada administrirate vaš Poslužitelj direktorija s iSeries Navigator ili za upotrebu SSL-a s Windows LDAP klijenta, morate imati jedan od proizvoda za Šifriranje klijenta (5722CE2 ili 5722CE3) instaliran na vaš PC.

Da omogućite SSL na vašem LDAP poslužitelju, napravite sljedeće:

1. **Pridružite certifikat Poslužitelju direktorija**
   a. Ako želite upravljati vašim Poslužiteljem direktorija preko SSL veze s iSeries Navigator, pogledajte Vodič za korisnike iSeries Access-a za Windowse (on se opcijski instalira na vaš PC kada instalirate iSeries Navigator). Ako planirate dopustiti SSL i ne-SSL veze na poslužitelja direktorija, mogli bi preskočiti ovaj korak.
   b. Pokrenite IBM Upravitelja digitalnih certifikata. Pogledajte Pokretanje Upravitelja digitalnih certifikata u poglavlju Upravitelj digitalnih certifikata za više informacija.
   c. Ako trebate dobaviti ili kreirati certifikate ili na drugi način postaviti svoj sistem certifikata, napravite to sada. Pogledajte Upravitelj digitalnih certifikata za više informacija o sistemu certifikata. Postoje dvije aplikacije poslužitelja i jedna aplikacija klijenta koje su pridružene Poslužitelju direktorija. One su:

      Aplikacija Poslužitelja direktorija
      Aplikacija Poslužitelja direktorija je sam poslužitelj.

      Aplikacija objavljivanja Poslužitelja direktorija
      Aplikacija objavljivanja Poslužitelja direktorija identificira certifikat kojeg koristi objavljivanje.

      Aplikacija klijenta Poslužitelja direktorija
      Aplikacija klijenta Poslužitelja direktorija identificira default certifikat kojeg koriste aplikacije koje koriste LDAP klijent ILE API-je.
   d. Kliknite na gumb **Izbor spremišta certifikata**.
   e. Izaberite ***SYSTEM**. Kliknite na **Nastavak**.
   f. Unesite prikladnu lozinku za *SYSTEM spremište certifikata. Kliknite na **Nastavak**.
   g. Kada se ponovo učita lijevi navigacijski izbornik, proširite **Upravljaj aplikacijama**.
   h. Kliknite na **Ažuriraj dodjeljivanje certifikata**.
   i. Na sljedećem ekranu izaberite aplikaciju **Poslužitelj**. Kliknite na **Nastavak**.
   j. Izaberite **Poslužitelj poslužitelja direktorija**.

k. Kliknite na **Ažuriraj dodjeljivanja certifikata** kako bi dodijelili certifikat Poslužitelju direktorija kojeg će koristiti kako bi uspostavio svoj identitet na iSeries Access za Windows klijentima.

Bilješka: Ako izaberete certifikat od CA čiji CA certifikat nije u vašoj iSeries Access za Windows bazi podataka ključa klijenta, trebat ćete ga dodati kako bi koristili SSL. Dovršite tu procedure prije nego počnete drugu.

l. Izaberite certifikat iz liste kojeg ćete dodijeliti poslužitelju.

m. Kliknite na **Dodijeli novi certifikat**.

n. DCM se ponovo učitava na stranicu **Ažuriraj dodjeljivanje certifikata** s potvrdnom porukom. Kada ste dovršili postavljanje certifikata za Poslužitelj direktorija, kliknite na **Gotovo**.

2. **Pridružite certifikat za objavljivanje Poslužitelja direktorija**. (neobavezan korak) Ako želite omogućiti objavljivanje iz sistema na Poslužitelj direktorija preko SSL veze, možda ćete željeti i pridružiti certifikat objavljivanju Poslužitelja direktorija. Time se identificira default certifikat i povjerljivi CA-ovi za aplikacije koje koriste LDAP ILE API-je koji ne specificiraju svoj id aplikacije ili zamjensku bazu podataka ključa.

   a. Pokrenite IBM Upravitelja digitalnih certifikata.

   b. Kliknite na gumb **Izbor spremišta certifikata**.

   c. Izaberite ***SYSTEM**. Kliknite na **Nastavak**.

   d. Unesite prikladnu lozinku za *SYSTEM spremište certifikata. Kliknite na **Nastavak**.

   e. Kada se ponovo učita lijevi navigacijski izbornik, proširite **Upravljaj aplikacijama**.

   f. Kliknite na **Ažuriraj dodjeljivanje certifikata**.

   g. Na sljedećem certifikatu izaberite aplikaciju **Klijent**. Kliknite na **Nastavak**.

   h. Izaberite **Objavljivanje Poslužitelja direktorija**.

   i. Kliknite na **Ažuriranje dodjele certifikata** da dodijelite certifikat objavljivanju Poslužitelja direktorija koji će uspostaviti njegov identitet.

   j. Izaberite certifikat iz liste kojeg ćete dodijeliti poslužitelju.

   k. Kliknite na **Dodjela novog certifikata**.

   l. DCM se ponovo učitava na stranicu **Ažuriraj dodjeljivanje certifikata** s potvrdnom porukom.

   Bilješka: Ti koraci pretpostavljaju da već objavljujete informacije na Poslužitelju direktorija s ne-SSL vezom. Pogledajte “Objavljivanje informacija poslužitelju direktorija” na stranici 149 za potpune informacije o postavljanju objavljivanja.

3. **Pridružite certifikat za klijenta Poslužitelja direktorija**. (neobavezan korak) Ako imate druge aplikacije koje koriste SSL veze na Poslužitelj direktorija, morat ćete dodijeliti certifikat klijentu Poslužitelja direktorija.

   a. Pokrenite IBM Upravitelja digitalnih certifikata.

   b. Kliknite na gumb **Izbor spremišta certifikata**.

   c. Izaberite ***SYSTEM**. Kliknite na **Nastavak**.

   d. Unesite prikladnu lozinku za *SYSTEM spremište certifikata. Kliknite na **Nastavak**.

   e. Kada se ponovo učita lijevi navigacijski izbornik, proširite **Upravljaj aplikacijama**.

   f. Kliknite na **Ažuriraj dodjeljivanje certifikata**.

   g. Na sljedećem certifikatu izaberite aplikaciju **Klijent**. Kliknite na **Nastavak**.

   h. Izaberite **klijenta Poslužitelja direktorija**.

   i. Kliknite na **Ažuriranje dodjele certifikata** da dodijelite certifikat klijentu Poslužitelja direktorija koji će uspostaviti njegov identitet.

   j. Izaberite certifikat iz liste kojeg ćete dodijeliti poslužitelju.

   k. Kliknite na **Dodijeli novi certifikat**.

   l. DCM se ponovo učitava na stranicu **Ažuriraj dodjeljivanje certifikata** s potvrdnom porukom.

Nakon što se omogući SSL, možete promijeniti port koji Poslužitelj direktorija koristi za sigurne veze.

Omogućavanje Kerberos provjere autentičnosti na Poslužitelju direktorija

Ako imate Uslugu provjere autentičnosti mreže konfiguriranu na vašem sistemu, možete postaviti svoj Poslužitelj direktorija tako da koristi Kerberos provjeru autentičnosti. Kerberos provjera autentičnosti se odnosi na korisnike i administratore. Prije omogućavanja Kerberosa na poslužitelju direktorija, možda će vam pomoći čitanje pregleda o korištenju Kerberosa s Poslužitelj direktorija.

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

Upravljanje shemom

Za više informacija o shemi, pogledajte “Shema” na stranici 15.

Shemom se može upravljati korištenjem Web administracijskog alata ili LDAP aplikacije poput ldapmodify u kombinaciji s LDIF datotekama. Kada prvi put definirate nove klase objekata ili atribute, možda je najprikladnije koristiti Web administracijski alat. Ako trebate kopirati novu shemu na druge poslužitelje (možda kao dio proizvoda ili alata kojeg razvijate), možda bi korisniji bio ldapmodify pomoćni program, pogledajte “Kopiranje sheme na druge poslužitelje” na stranici 128 kako bi dobili više informacija.

Pogledajte sljedeće za više informacija:
- “Pregled klasa objekata”
- “Dodavanje klase objekta” na stranici 120
- “Uređivanje klase objekta” na stranici 121
- “Kopiranje klase objekta” na stranici 122
- “Brisanje klase objekta” na stranici 123
- “Pregled atributa” na stranici 124
- “Dodavanje atributa” na stranici 124
- “Uređivanje atributa” na stranici 125
- “Kopiranje atributa” na stranici 126
- “Brisanje atributa” na stranici 128

Pregled klasa objekata

Možete pregledati klase objekata u shemi korištenjem Web administracijskog alata što je preferirana metoda ili korištenjem reda za naredbe.

Web administracija

Proširite **Upravljanje shemom** u području navigacije i kliknite na **Upravljanje klasama objekata**. Prikazan je panel samo za čitanje koji vam omogućava da pregledate klase objekata u shemi i njihove karakteristike. Klase objekata su prikazane u abecednom redu. Možete ići jednu stranicu natrag ili naprijed tako da kliknete na Prethodno ili Sljedeće. Polje uz te gumbe identificira stranicu na kojoj se nalazite. Možete koristite i padajući izbornik tog polja kako bi skočili na određenu stranicu. Prva klasa objekata ispisana na stranici je prikazana s brojem stranice kako bi lakše mogli locirati klasu objekata koju želite pregledati. Na primjer, ako ste tražili klasu objekata **person**, proširite padajući izbornik i

spuštajte se dolje tako dugo dok ne vidite **Stranica 14 od 16 nsLiServer** i **Stranica 15 od 16 printerLPR**. Budući je person prema abecedi između nsLiServer i printerLPR, izaberite Stranicu 14 i kliknite na **Kreni**.

Možete prikazati klase objekta sortirane prema tipu. Izaberite **Tip** i kliknite na **Sort**. Klase objekata su abecedno sortirane unutar njihova tipa, Sažetak, Pomoćno ili Strukturalno. Isto tako, poredak popisa možete obrnuti tako da izaberete **Silazno** i kliknete na **Sort**.

Nakon što locirate klasu objekta koju želite, možete pregledati njezin tip, nasljeđe, potrebne atribute ili neobavezne atribute. Proširite padajuće izbornike za nasljeđivanje, potrebne atribute i neobavezne atribute kako bi vidjeli potpuno ispisivanje za svaku osobinu.

Možete izabrati operacije klase objekata koje želite izvoditi iz desne trake s alatima, kao što je:

- Dodaj
- Uredi
- Kopiraj
- Briši

Kada ste gotovi kliknite na **Zatvori** kako bi se vratili na IBM Poslužitelj direktorija panel **Dobro došli**.

Red za naredbe

Kako bi pregledali klase objekata sadržane u shemi izdajte naredbu:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Dodavanje klase objekta

Web administracija

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje klasama objekta**. Kako bi kreirali novu klasu objekata:

1. Kliknite **Dodaj**.

   Bilješka: Tom panelu možete pristupiti tako da proširite **Upravljanje shemom** u području navigacije i nakon toga kliknete na **Dodaj klasu objekta**.
2. Na kartici **Općenita svojstva**:
   - Unesite **Ime klase objekta**. To je potrebno polje i ono opisuje funkciju klase objekta. Na primjer, **privZaposlenik** za klasu objekta koja se koristi za praćenje privremenih zaposlenika.
   - Unesite **Opis** klase objekta, na primjer, **Klasa objekta koja se koristi za privremene zaposlenike**.
   - Unesite **OID** za klasu objekta. To je potrebno polje. Pogledajte “Identifikator objekta (OID)” na stranici 25. Ako nemate OID, možete koristiti **Ime klase objekta** kojem je pridodano **-oid**. Na primjer, ako je ime klase objekta **privZaposlenik**, onda je OID **privZaposlenik-oid**. Možete promijeniti vrijednost tog polja.
   - Izaberite **Superiorna klasa objekta** iz padajućeg popisa. Time se određuje klasa objekata iz koje se nasljeđuju drugi atributi. U pravilu je **Superiorna klasa objekta top**, no može biti i druga klasa objekta. Na primjer, superiorna klasa objekta za **privZaposlenik** može biti **ePerson**.
   - Izaberite **Tip klase objekta**. Pogledate “Klase objekta” na stranici 18 kako bi dobili dodatne informacije o tipovima klase objekta.
   - Kliknite na karticu Atributi kako bi specificirali potrebne i neobavezne atribute za klasu objekta i pregledajte naslijeđene atribute ili kliknite na **OK** kako bi dodali novu klasu objekta ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekata** bez da činite promjene.
3. Na kartici **Atributi**:
   - Izaberite atribut iz abecednog popisa **Dostupni atributi** i kliknite na **Dodaj potrebnim** kako bi napravili atribut potrebnim ili kliknite na **Dodaj neobaveznim** kako bi napravili atribut neobaveznim za klasu objekata. Atribut je prikazan u odgovarajućem popisu izabranih atributa.

- Ponovite taj proces za sve atribute koje želite izabrati.
- Možete premještati atribute iz jednog popisa na drugi ili obrisati atribut iz izabranih popisa tako da ga izaberete i kliknete na odgovarajući **Premjesti** ili **Obriši** gumb.
- Možete pregledati popise potrebnih i neobaveznih naslijeđenih atributa. Naslijeđeni atributi se temelje na **Superiornoj klasi objekta** izabranoj na kartici **Općenito**. Ne možete promijeniti naslijeđene atribute. No, ako promijenite **Superiornu klasu objekta** na kartici **Općenito**, prikazuje se drugačiji skup naslijeđenih atributa.

4. Kliknite na **OK** kako bi dodali novu klasu objekta ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekata** bez da činite bilo kakve promjene.

Bilješka: Ako ste kliknuli na **OK** na kartici **Općenito** bez da ste dodali bilo koje atribute, možete dodati atribute uređivanjem nove klase objekta.

Red za naredbe

Kako bi dodali klasu objekta korištenjem reda za naredbe, izdajte sljedeću naredbu:

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

gdje <*filename*>sadrži:

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: ( <myobjectClass-oid> NAME '<myObjectClass>' DESC '<Klasa objekta koju sam
                 definirao za svoju LDAP aplikaciju>' SUP '<objectclassinheritance>'
                 <objectclasstype> MAY (<attribute1> $ <attribute2>))
```

Uređivanje klase objekta

Nisu dozvoljene sve promjene sheme. Pogledajte “Nedozvoljene promjene sheme” na stranici 27 kako bi promijenili ograničenja.

Web administracija

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje klasama objekta**. Kako bi uređivali klasu objekta:

1. Kliknite na radijski gumb koji se nalazi uz klasu objekta koju želite uređivati.
2. Kliknite na **Uredi**.
3. Izaberite karticu:
   - Koristite karticu **Općenito** kako bi:
     - Modificirali **Opis**.
     - Promijenili **Superiornu klasa objekta**. Izaberite Superiornu klasu objekta iz padajućeg popisa. Time se određuje klasa objekata iz koje se nasljeđuju drugi atributi. U pravilu je **Superiorna klasa objekta top**, no može biti i druga klasa objekta. Na primjer, superiorna klasa objekta za **privZaposlenik** može biti **ePerson**.
     - Promijenite **Tip klase objekta**. Izaberite tip klase objekta. Pogledate “Klase objekta” na stranici 18 kako bi dobili dodatne informacije o tipovima klase objekta.
     - Kliknite na karticu Atributi kako bi promijenili potrebne i neobavezne atribute za klasu objekta i pregledali naslijeđene atribute ili kliknite na **OK** kako bi primijenili svoje promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekta** bez bilo kakvih promjena.
   - Koristite karticu **Atributi** kako bi:

     Izaberite atribut iz abecednog popisa **Dostupni atributi** i kliknite na **Dodaj potrebnim** kako bi napravili atribut potrebnim ili kliknite na **Dodaj neobaveznim** kako bi napravili atribut neobaveznim za klasu objekata. Atribut je prikazan u odgovarajućem popisu izabranih atributa.

     Ponovite taj proces za sve atribute koje želite izabrati.

Možete premještati atribute iz jednog popisa na drugi ili obrisati atribut iz izabranih popisa tako da ga izaberete i kliknete na odgovarajući **Premjesti** ili **Obriši** gumb.

Možete pregledati popise potrebnih i neobaveznih naslijeđenih atributa. Naslijeđeni atributi se temelje na **Superiornoj klasi objekta** izabranoj na kartici **Općenito**. Ne možete promijeniti naslijeđene atribute. No, ako promijenite **Superiornu klasu objekta** na kartici **Općenito**, prikazuje se drugačiji skup naslijeđenih atributa.

4. Kliknite na **OK** kako bi primijenili promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekata** bez ikakvih promjena.

Red za naredbe

Pregledajte klase objekata koje su sadržane u shemi i izdajte naredbu:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Kako bi uređivali klasu objekta korištenjem reda za naredbe, izdajte sljedeću naredbu:

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

gdje <*filename*>sadrži:

```
dn: cn=schema
changetype: modify
replace: objectclasses
objectclasses: ( <myobjectClass-oid> NAME '<myObjectClass>' DESC '<Klasa objekta koju sam
                 definirao za svoju LDAP aplikaciju>' SUP '<newsuperiorclassobject>'
                 <newobjectclasstype> MAY (attribute1> $ <attribute2>
                  $ <newattribute3>) )
```

Kopiranje klase objekta

Web administracija

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje klasama objekta**. Kako bi kopirali klasu objekta:

1. Kliknite na radijski gumb uz klasu objekta koju želite kopirati.
2. Kliknite na **Kopiranje**.
3. Izaberite karticu:
   - Koristite karticu **Općenito** kako bi:
     - Modificirali **ime klase objekta**. Default ime je ime kopirane klase objekata kojoj je pridodana riječ COPY. Na primjer, **tempPerson** se kopirao kao **tempPersonCOPY**.
     - Modificirali **Opis**.
     - Modificirajte **OID**. Default OID je OID kopirane klase objekte kojoj je pridodana riječ COPY. Na primjer, **tempPerson-oid** se kopira kao **tempPerson-oidCOPY**.
     - Promijenili **Superiornu klasa objekta**. Izaberite superiornu klasu objekta iz padajuće liste. Time se određuje klasa objekata iz koje se nasljeđuju drugi atributi. U pravilu je **Superiorna klasa objekta top**, no može biti i druga klasa objekta. Na primjer, superiorna klasa objekta za **tempEmployeeCOPY** bi mogla biti **ePerson**.
     - Promijenite **Tip klase objekta**. Izaberite tip klase objekta. Pogledate “Klase objekta” na stranici 18 kako bi dobili dodatne informacije o tipovima klase objekta.
     - Kliknite na karticu **Atributi** kako bi promijenili potrebne i neobavezne atribute za klasu objekta i pregledali naslijeđene atribute ili kliknite na **OK** kako bi primijenili svoje promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekata** bez ikakvih promjena.
   - Koristite karticu **Atributi** kako bi:

     Izaberite atribut iz abecednog popisa **Dostupni atributi** i kliknite na **Dodaj potrebnim** kako bi napravili atribut potrebnim ili kliknite na **Dodaj neobaveznim** kako bi napravili atribut neobaveznim za klasu objekata. Atribut je prikazan u odgovarajućem popisu izabranih atributa.

     Ponovite taj proces za sve atribute koje želite izabrati.

Možete premještati atribute iz jednog popisa na drugi ili obrisati atribut iz izabranih popisa tako da ga izaberete i kliknete na odgovarajući **Premjesti** ili **Obriši** gumb.

Možete pregledati popise potrebnih i neobaveznih naslijeđenih atributa. Naslijeđeni atributi se temelje na **Superiornoj klasi objekta** izabranoj na kartici **Općenito**. Ne možete promijeniti naslijeđene atribute. No, ako promijenite **Superiornu klasu objekta** na kartici **Općenito**, prikazuje se drugačiji skup naslijeđenih atributa.

4. Kliknite na **OK** kako bi primijenili promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekata** bez ikakvih promjena.

Red za naredbe

Pregledajte klase objekata koje su sadržane u shemi i izdajte naredbu:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Izaberite klase objekta koje želite kopirati. Koristite editor za promjenu odgovarajućih informacija i spremanje promjena na <*filename*>. Nakon toga izdajte sljedeću naredbu:

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

gdje <*filename*>sadrži:

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( <mynewobjectClass-oid> NAME '<mynewObjectClass>'
                 DESC '<Nova klasa objekta koju sam
                   kopirao za svoju LDAP aplikaciju>'
                SUP '<superiorclassobject>'<objectclasstype> MAY (attribute1>
                $ <attribute2> $ <attribute3>) )
```

Brisanje klase objekta

Nisu dozvoljene sve promjene sheme. Pogledajte “Nedozvoljene promjene sheme” na stranici 27 kako bi promijenili ograničenja.

Web administracija

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje klasama objekta**. Kako bi obrisali klasu objekta:

1. Kliknite na radijski gumb koji se nalazi uz klasu objekta koju želite obrisati.
2. Kliknite na **Briši**.
3. Promptirani ste kako bi potvrdili brisanje klase objekta. Kliknite na **OK** kako bi obrisali klasu objekta ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekta** bez ikakvih promjena.

Red za naredbe

Pregledajte klase objekata koje su sadržane u shemi i izdajte naredbu:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Izaberite klasu objekta koju želite obrisati i izdajte sljedeću naredbu:

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

gdje <*filename*>sadrži:

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: (<myobjectClass-oid>)
```

Pregled atributa

Možete pregledati atribute u shemi korištenjem Web administracijskog alata, preferirane metode ili korištenjem reda za naredbe.

Web administracija

Proširite **Upravljanje shemom** u području navigacije i kliknite na **Upravljanje atributima**. Prikazuje se panel samo za čitanje koji vam omogućuje da pregledate atribute u shemi i njihove karakteristike. Atributi su prikazani u abecednom poretku. Možete ići jednu stranicu natrag ili naprijed tako da kliknete na Prethodno ili Sljedeće. Polje uz te gumbe identificira stranicu na kojoj se nalazite. Možete koristite i padajući izbornik tog polja kako bi skočili na određenu stranicu. Prva klasa objekata ispisana na stranici je prikazana s brojem stranice kako bi lakše mogli locirati klasu objekata koju želite pregledati. Na primjer, ako ste tražili atribut **authenticationUserID**, proširite padajući izbornik i spustite se dolje dok ne vidite **Stranica 3 od 62 applSystemHint** i **Stranica 4 od 62 authorityRevocatonList**. Budući je authenticationUserID prema abecedi između applSystemHint i authorityRevocatonList, izaberite Stranicu 3 i kliknite na **Kreni**.

Možete prikazati atribute sotrtirane prema sintaksi. Izaberite **Sintaksa** i kliknite na **Sort**. Ti atributi su sortirani abecedno unutar njihove sintakse. Pogledajte "Sintaksa atributa" na stranici 25 za ispisivanje ili tipove sintakse. Isto tako, poredak popisa možete obrnuti tako da izaberete **Silazno** i kliknete na **Sort**.

Nakon što pronađete atribut kojeg želite, možete pregledati njegovu sintaksu, da li ima više vrijednosti i klase objekta koje sadrži. Proširite padajući izbornik za klasu objekta kako bi vidjeli popis klasa objekata za atribut.

Kada ste gotovi kliknite na **Zatvori** kako bi se vratili na IBM Poslužitelj direktorija panel **Dobro došli**.

Red za naredbe

Kako bi pregledali atribute koji su sadržani u shemi i izdajte naredbu:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Dodavanje atributa

Koristite bilo koju od sljedećih metoda za kreiranje novog atributa. Web administracijski alat je preferirana metoda.

Web administracija

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje atributima**. Za kreiranje novog atributa:

1. Kliknite **Dodaj**.

   Bilješka: Tom panelu možete pristupiti proširivanjem **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Dodaj atribut**.
2. Unesite **Ime atributa**, na primjer, **tempId**. To je potrebno polje i mora započeti s abecednim znakom.
3. Unesite **Opis** atributa, na primjer, **ID broj dodijeljen privremenom zaposleniku**.
4. Unesite **OID** za atribut. To je potrebno polje. Pogledajte "Identifikator objekta (OID)" na stranici 25. Ako nemate OID, možete koristiti ime atributa kojem je pridodan -oid. Na primjer, ako je ime atributa **tempID**, onda je default OID **tempID-oid**. Možete promijeniti vrijednost tog polja.
5. Izaberite **Superiorni atribut** iz padajućeg izbornika. Superiorni atribut određuje atribut iz kojeg se nasljeđuju svojstva.
6. Izaberite **Sintaksu** iz padajućeg popisa. Pogledajte "Sintaksa atributa" na stranici 25 kako bi dobili dodatne informacije o sintaksi.
7. Unesite **Dužina atributa** koja specificira maksimalnu dužinu tog atributa. Dužina je izražena kao broj bajtova.
8. Izaberite **Dozvoli više vrijednosti** kontrolnu kućicu kako bi omogućili da atributi imaju više vrijednosti.

9. Izaberite pravilo podudaranja iz svakog od padajućih izbornika za pravila podudaranja jednakosti, poretka i podniza. Pogledajte “Pravila podudaranja” na stranici 23 kako bi dobili potpuni ispis pravila podudaranja.
10. Kliknite na karticu **IBM proširenja** kako bi specificirali dodatna proširenja za atribut ili kliknite na **OK** kako bi dodali novi atribut ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje atributima** bez promjena.
11. Na kartici **IBM proširenja**:
    - Modificirajte ime **DB2 tablice** . Poslužitelj generira ime DB2 tablice ako je to polje ostavljeno praznim. Ako unesete ime DB2 tablice, morate unijeti i ime DB2 stupca.
    - Modificirajte ime **DB2 stupca**. Poslužitelj generira ime DB2 stupca ako je to polje ostavljeno praznim. Ako unesete DB2 ime stupca, morate unijeti ime DB2 tablice.
    - Postavite **Klasa sigurnosti** tako da izaberete **normalno**, **osjetljivo** ili **kritično** iz padajućeg popisa.
    - Postavite **Pravila indeksiranja** izborom jednog ili više pravila indeksiranja. Pogledajte “Pravila indeksiranja” na stranici 24 kako bi dobili dodatne informacije o pravilima indeksiranja.

      Bilješka: Ako ništa drugo, preporuča se da specificirate indeksiranje Jednakosti na bilo kojim atributima koji će se koristiti u filterima pretraživanja.
12. Kliknite na **OK** da dodate nove atribute ili kliknite na **Opoziv** da se vratite na **Upravljanje atributima** bez ikakvih promjena.

Bilješka: Ako ste kliknuli na OK na kartici Općenito bez dodavanja bilo kojih proširenja, možete dodati proširenja uređivanjem novog atributa.

Red za naredbe

U sljedećem primjeru se dodaje definicija tipa atributa za atribut koji se naziva ″myAttribute″, sa sintaksom Niz direktorija (pogledajte “Sintaksa atributa” na stranici 25) i podudaranjem Jednakost sa zanemarivanjem velikih i malih slova (pogledajte “Pravila podudaranja” na stranici 23). IBM-specifični dio definicije govori da su atributi podataka pohranjeni u stupcu pod imenom ″myAttrColumn″ u tablici pod nazivom ″myAttrTable″. Ako ta imena nisu bila specificirana, ime stupca i ime tablice bi se postavilo na ″myAttribute″. Atribut je dodijeljen na ″normalnoj″ klasi pristupa, a vrijednosti imaju maksimalnu dužinu od 200 bajtova.

```
ldapmodify -D <admindn> -w <adminpw> -i myschema.ldif
```

gdje **myschema.ldif** datoteka sadrži:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' )
                 DESC 'Atribut kojeg sam definirao za svoju LDAP aplikaciju'
                 EQUALITY 2.5.13.2 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
                 USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                    ACCESS-CLASS normal LENGTH 200 )
```

Pogledajte “ldapmodify i ldapadd” na stranici 157 kako bi dobili više informacija o naredbi.

Uređivanje atributa

Nisu dozvoljene sve promjene sheme. Pogledajte “Nedozvoljene promjene sheme” na stranici 27 kako bi promijenili ograničenja.

Bilo koji dio definicije se može promijeniti prije nego imate dodane unose koji koriste atribut. Koristite bilo koju od slijedećih metoda kako bi uređivali atribut. Web administracijski alat je preferirana metoda.

Web administracija

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje atributima**. Kako bi uređivali atribut:

1. Kliknite na radijski gumb koji se nalazi uz atribut kojeg želite uređivati.
2. Kliknite na **Uredi**.
3. Izaberite karticu:
   - Koristite karticu **Općenito** kako bi:
     – Izaberite karticu, ili:
       - **Općenito** kako bi:
         - Modificirali **Opis**
         - Promijenili **Sintaksu**
         - Postavili **Dužina atributa**
         - Promijenili postavke **Više vrijednosti**
         - Izaberite **Pravilo podudaranja**
         - Promijenite **Superiorni atribut**
       - Kliknite na karticu **IBM proširenja** kako bi uređivali proširenja za atribut ili kliknite na **OK** kako bi primijenili svoje promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje atributima** bez promjena.
       - **IBM proširenja**, ako koristite IBM Poslužitelj direktorija kako bi:
         - Promijenili **Klasa sigurnosti**
         - Promijenili **Pravila indeksiranja**
     – Kliknite na **OK** kako bi primijenili svoje promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje atributima** bez ikakvih promjena.
4. Kliknite na **OK** kako bi primijenili promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje atributima** bez promjena.

Red za naredbe

Taj primjer dodaje indeksiranje na atribut, tako da pretraživanje bude brže. Koristite ldapmodify naredbu i LDIF datoteku kako bi promijenili definiciju:

```
ldapmodify -D <admindn> -w <adminpw> -i myschemachange.ldif
```

Gdje **myschemachange.ldif** datoteka sadrži:

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' ) DESC 'Atribut kojeg
                 sam definirao za moju LDAP aplikaciju' EQUALITY 2.5.13.2
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
replace: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                  ACCESS-CLASS normal LENGTH 200 EQUALITY SUBSTR )
```

Bilješka: Oba dijela definicije (**attributetypes** i **ibmattributetypes**) moraju biti uključeni u operaciju zamjene, iako se mijenja samo dio **ibmattributetypes**. Jedina promjena je dodavanje ″EQUALITY SUBSTR″ na kraj definicije kako bi se zatražili indeksi za podudaranje jednakosti i podniza.

Pogledajte “ldapmodify i ldapadd” na stranici 157 kako bi dobili više informacija o naredbi.

Kopiranje atributa

Koristite bilo koju od slijedećih metoda kako bi kopirali atribut. Web administracijski alat je preferirana metoda.

Web administracija

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje atributima**. Kako bi kopirali atribut:

1. Kliknite na radijski atribut uz atribut kojeg želite kopirati.
2. Kliknite na **Kopiranje**.
3. Modificirajte **Ime atributa**. Default ime je ime kopiranog atributa kojem je pridodana riječ COPY. Na primjer **tempID** se kopira kao **tempIDCOPY**.
4. Modificirajte **Opis** atributa, na primjer, **ID broj koji je dodijeljen privremenom zaposleniku**.
5. Modificirajte **OID**. Default OID je OID kopiranog atributa kojem je dodijeljena riječ COPYOID. Na primjer, **tempID-oid** se kopira kao **tempID-oidCOPYOID**.
6. Izaberite **Superiorni atribut** iz padajućeg izbornika. Superiorni atribut određuje atribut iz kojeg se nasljeđuju svojstva.
7. Izaberite **Sintaksu** iz padajućeg popisa. Pogledajte “Sintaksa atributa” na stranici 25 kako bi dobili dodatne informacije o sintaksi.
8. Unesite **Dužina atributa** koja specificira maksimalnu dužinu tog atributa. Dužina je izražena kao broj bajtova.
9. Izaberite **Dozvoli više vrijednosti** kontrolnu kućicu kako bi omogućili da atributi imaju više vrijednosti.
10. Izaberite pravilo podudaranja iz svakog od padajućih izbornika za pravila podudaranja jednakosti, poretka i podniza. Pogledajte “Pravila podudaranja” na stranici 23 kako bi dobili potpuni ispis pravila podudaranja.
11. Kliknite na karticu **IBM proširenja** kako bi modificirali dodatna proširenja za atribut ili kliknite na **OK** kako bi primijenili promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje atributima** bez ikakvih promjena.
12. Na kartici **IBM proširenja**:
    - Modificirajte ime **DB2 tablice** . Poslužitelj generira ime DB2 tablice ako je to polje ostavljeno praznim. Ako unesete ime DB2 tablice, morate unijeti i ime DB2 stupca.
    - Modificirajte ime **DB2 stupca**. Poslužitelj generira ime DB2 stupca ako je to polje ostavljeno praznim. Ako unesete DB2 ime stupca, morate unijeti ime DB2 tablice.
    - Modificirajte **Klasu sigurnosti** izborom **normalno**, **osjetljivo** ili **kritično** iz padajućeg popisa.
    - Modificirajte **Pravila indeksiranja** izborom jednog ili više pravila indeksiranja. Pogledajte “Pravila indeksiranja” na stranici 24 kako bi dobili dodatne informacije o pravilima indeksiranja.

      Bilješka: Ako ništa drugo, preporuča se da specificirate indeksiranje Jednako na bilo kojim atributima koji će se koristiti u filterima pretraživanja.
13. Kliknite na **OK** kako bi primijenili svoje promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje atributima** bez ikakvih promjena.

Bilješka: Ako ste kliknuli **OK** na kartici **Općenito** bez dodavanja bilo kakvih proširenja, možete dodati ili modificirati proširenja uređivanjem novog atributa.

Red za naredbe

Pregledajte atribute koji su sadržani u shemi i izdajte naredbu:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Izaberite atribut kojeg želite kopirati. Koristite editor za promjenu odgovarajućih informacija i spremanje promjena na <*filename*>. Nakon toga izdajte sljedeću naredbu:

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

gdje <*filename*>sadrži:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( <mynewAttribute-oid> NAME '<mynewAttribute>' DESC '<Novi
                atribut koji sam kopirao za svoju LDAP aplikaciju> EQUALITY 2.5.13.2
                SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
```

```
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                    ACCESS-CLASS normal LENGTH 200 )
```

Brisanje atributa

Nisu dozvoljene sve promjene sheme. Pogledajte “Nedozvoljene promjene sheme” na stranici 27 kako bi promijenili ograničenja.

Koristite bilo koju od slijedećih metoda kako bi obrisali atribut. Web administracijski alat je preferirana metoda.

Web administracija

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje atributima**. Kako bi obrisali atribut:

1. Kliknite na radijski gumb uz atribut kojeg želite obrisati.
2. Kliknite na **Briši**.
3. Promptirani ste kako bi potvrdili brisanje atributa. Kliknite na **OK** kako bi obrisali atribut ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje atributima** bez ikakvih promjena.

Red za naredbe

```
ldapmodify -D <admindn> -w <adminpw> -i myschemadelete.ldif
```

Gdje **myschemadelete.ldif** datoteka uključuje:

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

Pogledajte “ldapmodify i ldapadd” na stranici 157 kako bi dobili više informacija o toj naredbi.

Kopiranje sheme na druge poslužitelje

Za kopiranje sheme na druge poslužitelje, napravite sljedeće:

1. Koristite ldapsearch pomoćni program kako bi kopirali shemu u datoteku:

   ```
   ldapsearch -b cn=schema -L "(objectclass=*)" > schema.ldif
   ```

2. Datoteka sheme će uključivati klase objekta i atribute. Uredite LDIF datoteku tako da uključuje samo elemente sheme koje želite ili možda možete filtrirati ldapsearch izlaz korištenjem alata kao što je grep. Vodite računa o tome da stavite atribute prije nego klase objekta koje ih referenciraju. Na primjer, mogli bi završiti sa slijedećom datotekom (primijetite da svaka linija koja se nastavlja ima jedno prazno mjesto na kraju, a linija koja nastavlja ima barem jedno prazno mjesto na početku linije).

   ```
   attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Neki dio
     informacija.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1'  'myattr1' )
     ACCESS-CLASS normal LENGTH 500 )
   attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Neki dio
     informacija.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2'  'myattr2' )
     ACCESS-CLASS normal LENGTH 500 )
   objectclasses: ( myobject-oid NAME 'myobject' DESC 'Predstavlja
     nešto.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
   ```

3. Umetnite linije prije svake linije objectclasses ili attributetype kako bi izgradili LDIF direktive za dodavanje tih vrijednost na unos cn=schema. Svaka klasa objekta i atribut moraju biti dodani kao pojedinačne preinake.

```
dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Neki dio
  informacija.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
  USAGE userApplications )
IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1'  'myattr1' )
  ACCESS-CLASS normal LENGTH 500 )

dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Neki dio
  informacija.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
  USAGE userApplications )
IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2'  'myattr2' )
  ACCESS-CLASS normal LENGTH 500 )

dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( myobject-oid NAME 'myobject' DESC 'Predstavlja
  nešto.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

4. Učitajte shemu na druge poslužitelje korištenjem ldapmodify pomoćnog programa:

```
ldapmodify -D cn=administrator -w <password> -f schema.ldif
```

Upravljanje unosima direktorija

Za upravljanje unosima direktorija, proširite kategoriju **Upravljanje direktorijom** u području navigacije Web administracijskog alata.

Pogledajte sljedeće za više informacija:

- “Pregledavanje stabla”
- “Dodavanje unosa”
- “Brisanje unosa” na stranici 130
- “Uređivanje unosa” na stranici 130
- “Kopiranje unosa” na stranici 131
- “Uređivanje lista kontrole pristupa” na stranici 131
- “Dodavanje pomoćne klase objekta” na stranici 131
- “Brisanje pomoćne klase” na stranici 132
- “Promjena članstva grupe” na stranici 132
- “Pretraživanje unosa direktorija” na stranici 132
- “Promjena binarnih atributa” na stranici 134

Pregledavanje stabla

Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos na kojem želite raditi. Iz desne trake s alatima možete izabrati operaciju koju želite izvoditi.

Dodavanje unosa

Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije.

1. Kliknite na **Dodaj unos**.
2. Izaberite jednu **Strukturalnu klasu objekta** iz padajućeg popisa.
3. Kliknite na **Sljedeće**.

4. Iz kućice Dostupno izaberite bilo koje **Pomoćne klase objekta** koje želite koristiti i kliknite na **Dodaj**. Ponovite taj proces za svaku pomoćnu klasu objekta koju želite dodati. Možete i obrisati pomoćnu klasu objekta iz Kućice Izabrano tako da je izaberete i kliknete na **Ukloni**.
5. Kliknite na **Sljedeće**.
6. U polje **Relativno DN** unesite relativno razlikovno ime (RDN) unosa kojeg dodajete, na primjer, cn=John Doe.
7. U polje **Nadređeno DN** unesite razlikovno ime unosa drveta kojeg ste izabrali, na primjer, ou=Austin, o=IBM. Možete i kliknuti na **Pregled** kako bi izabrali Nadređeno DN iz popisa. Možete i proširiti izbor kako bi vidjeli druge izbore koji se nalaze niže u podstablu. Specificirajte svoj izbor i kliknite na **Izbor** kako bi specificirali Nadređeno DN koje želite. **Nadređeno DN** se postavlja na unos koji je izabran u stablu.

   Bilješka: Ako ste pokrenuli taj zadatak iz panela **Upravljanje unosima**, to polje je već ispunjeno za vas. Izabrali ste **Nadređeno DN** prije nego ste kliknuli na **Dodaj** kako bi pokrenuli proces dodaj unos.
8. Na kartici **Potrebni atributi** unesite vrijednosti za potrebne atribute. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
9. Kliknite na **Neobavezni atributi**.
10. Na karticu **Neobavezni atributi** unesite vrijednosti kako je to prikladno za neobavezne atribute. Pogledajte “Promjena binarnih atributa” na stranici 134 kako bi dobili informacije o dodavanju binarnih vrijednosti. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
11. Kliknite na OK kako bi kreirali unos.
12. Kliknite na **ACL** gumb kako bi modificirali listu kontrole pristupa za taj unos. Pogledajte “Lista kontrole pristupa” na stranici 47 kako bi dobili informacije o ACL-ovima.
13. Nakon što dovršite barem potrebna polja, kliknite na **Dodavanje** kako bi dodali novi unos ili kliknite na **Opoziv** kako bi se vratili na **Pregled stabla** bez ikakvih promjena na direktoriju.

Brisanje unosa

Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla, sufiks ili unos na kojem želite raditi. Kliknite na **Obriši** iz desne trake s alatima.

- Od vas se traži da potvrdite brisanje. Kliknite **OK**.
- Unos se briše iz unosa i vraćate se na listu unosa.

Uređivanje unosa

Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos na kojem želite raditi. Kliknite na **Uredi atribute** iz desne trake s alatima.

1. Na kartici **Potrebni atributi** unesite vrijednosti za potrebne atribute. Pogledajte “Promjena binarnih atributa” na stranici 134 kako bi dobili informacije o dodavanju binarnih vrijednosti. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
2. Kliknite na **Neobavezni atributi**.
3. Na karticu **Neobavezni atributi** unesite vrijednosti kako je to prikladno za neobavezne atribute. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
4. Kliknite na **Članstvo**.
5. Ako ste kreirali bilo koje grupe na kartici **Članstvo**:
   - Izaberite grupu iz **Dostupne grupe** i kliknite na **Dodaj** da napravite unos članom izabranog **Članstva statičke grupe**.
   - Izaberite grupu iz **Članstva statičke grupe** i kliknite na **Ukloni** kako bi uklonili unos iz izabrane grupe.
6. Ako je unos grupni unos, dostupna je kartica **Članovi**. Kartica **Članovi** prikazuje članove izabrane grupe. Možete dodati ili ukloniti članove iz grupe.

- Kako bi dodali člana grupi:
  a. Kliknite na karticu **Višestruke vrijednosti** uz karticu **Članovi** ili na kartici **Članovi** kliknite na **Članovi**.
  b. U polje Član unesite DN unosa kojeg želite dodati.
  c. Kliknite **Dodaj**.
  d. Kliknite **OK**.
- Da uklonite član iz grupe:
  a. Kliknite na **Višestruke vrijednosti** uz karticu **Članovi** ili kliknite na karticu **Članovi** i kliknite na **Članovi**.
  b. Izaberite unos koji želite ukloniti.
  c. Kliknite **Ukloni**.
  d. Kliknite **OK**.
- Da osvježite listu članova, kliknite na **Ažuriraj**.

7. Kliknite na **OK** da modificirate unos.

Kopiranje unosa

Ova funkcija je korisna ako kreirate slične unose. Kopija nasljeđuje sve atribute originala. Morate napraviti neke preinake na imenu novog unosa.

Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos, kao što je John Doe, na kojem želite raditi. Kliknite na **Kopiraj** iz desne trake s alatima.

- Promijenite RDN unos u DN polje. Na primjer, promijenite cn=John Doe u cn=Jim Smith.
- Na potrebnoj kartici s atributima promijenite unos na novi RDN. U ovom primjeru Jim Smith.
- Promijenite druge potrebne atribute na odgovarajući način. U ovom primjeru promijenite sn iz Doe u Smith.
- Kada ste dovršili potrebne promjene, kliknite na **OK** kako bi kreirali novi unos.
- Novi unos Jim Smith se dodajte na dno liste unosa.

Bilješka: Tom procedurom se kopiraju samo atributi unosa. Članstva grupe originalnog unosa se ne kopiraju na novi unos. Koristite funkciju Uredi atribute kako bi dodali članstvo.

Uređivanje lista kontrole pristupa

Kako bi pregledali ACL svojstva korištenjem pomoćnog programa Web administracijski alat i kako bi radili s ACL-ovima, pogledajte “Upravljanje listama kontrole pristupa (ACL-ovi)” na stranici 145.

Pogledajte “Lista kontrole pristupa” na stranici 47 kako bi dobili dodatne informacije.

Dodavanje pomoćne klase objekta

Koristite gumb **Dodaj pomoćne klase** na traci s alatima kako bi dodali klasu pomoćnog objekta na postojeći unos u stablu direktorija. Pomoćna klasa objekta osigurava dodatne atribute na unos na kojeg se dodaje.

Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos, kao što je John Doe, na kojem želite raditi. Kliknite na **Dodaj pomoćnu klasu** iz desne trake s alatima.

1. Iz kućice Dostupno izaberite bilo koje **Pomoćne klase objekta** koje želite koristiti i kliknite na **Dodaj**. Ponovite taj proces za svaku pomoćnu klasu objekta koju želite dodati. Možete i obrisati pomoćnu klasu objekta iz Kućice Izabrano tako da je izaberete i kliknete na **Ukloni**.
2. Na kartici **Potrebni atributi** unesite vrijednosti za potrebne atribute. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
3. Kliknite na **Neobavezni atributi**.

4. Na karticu **Neobavezni atributi** unesite vrijednosti kako je to prikladno za neobavezne atribute. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
5. Kliknite na **Članstvo**.
6. Ako ste kreirali bilo koje grupe na kartici **Članstvo**:
   - Izaberite grupu iz **Dostupne grupe** i kliknite na **Dodaj** da napravite unos članom izabranog **Članstva statičke grupe**.
   - Izaberite grupu iz **Članstva statičke grupe** i kliknite na **Ukloni** kako bi uklonili unos iz izabrane grupe.
7. Kliknite na **OK** da modificirate unos.

Brisanje pomoćne klase

Iako možete obrisati pomoćne klase za vrijeme procedure dodaj pomoćnu klasu, lakše je koristiti funkciju obriši pomoćnu klasu ako ćete brisati jednu pomoćnu klasu iz unosa. No, ako ćete obrisati više pomoćnih klasa iz unosa, možda je prikladnije korištenje funkcije dodavanje pomoćne klase.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos, kao što je John Doe, na kojem želite raditi. Kliknite na **Briši pomoćnu klasu** iz desne trake s alatima.
2. U listi pomoćnih klasa izaberite onu koju želite obrisati i pritisnite **OK**.
3. Od vas će se tražiti da potvrdite brisanje, kliknite na **OK**.
4. Pomoćna klasa se briše iz unosa i vi se vraćate na popis unosa.

Ponovite te korake za svaku pomoćnu klasu koju želite obrisati.

Promjena članstva grupe

Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije.

1. Kliknite na **Upravljanje unosima**.
2. Izaberite korisnika iz stabla direktorija i kliknite na ikonu **Uredi atribute** na traci s alatima.
3. Kliknite na karticu **Članstva**.
4. Kako bi modificirali članstvo za korisnika: Na panelu **Promijeni članstvo** se prikazuju **Dostupne grupe** na koje se može dodati korisnik, kao i **Članstvo statičke grupe** unosa.
   - Izaberite grupu iz **Dostupne grupe** i kliknite na **Dodaj** kako bi unos postao članom izabrane grupe.
   - Izaberite grupu iz **Članstvo statičke grupe** i kliknite ne **Ukloni** kako bi uklonili unos iz izabrane grupe.
5. Kliknite na **OK** kako bi spremili svoje promjene ili kliknite na **Opoziv** kako bi se vratili na prethodni panel bez da se spreme vaše promjene.

Pretraživanje unosa direktorija

Postoje tri opcije za pretraživanje stabla direktorija:

- Jednostavno pretraživanje koje koristi predefinirani skup kriterija pretraživanja
- Napredno pretraživanje koje koristi korisnički definiran skup kriterija pretraživanja
- Ručno pretraživanje

Opcije pretraživanja su dostupne proširivanjem kategorije **Upravljanje direktorija** u području navigacije, kliknite na **Pronađi unose**. Izaberite karticu **Filteri pretraživanja** ili **Opcije**.

Bilješka: Binarni unosi, kao što su lozinke, se ne mogu pretraživati.

Filteri pretraživanja

Izaberite jedan od slijedećih tipova pretraživanja:

Jednostavno pretraživanje

Jednostavno pretraživanje koristi default kriterij pretraživanja:

- Bazni DN je **Svi sufiksi**
- Opseg pretraživanja je **Podstablo**
- Veličina pretraživanja je **Neograničena**
- Ograničenje vremena je **Neograničeno**
- Dereferenciranje zamjenskog imena je **nikad**
- Referali potjere nisu izabrani (off)

Kako bi izvodili jednostavno pretraživanje:

1. Na kartici **Filter pretraživanja** kliknite na **Jednostavno pretraživanje**.
2. Izaberite klase objekta iz padajućeg popisa.
3. Izaberite određeni atribut za izabrani tip unosa. Ako ste izabrali traženje određenog atributa, izaberite atribut iz padajuće liste i unesite vrijednost atributa u kućicu **Isto kao**. Ako ne specificirate atribut, pretraživanje vraća sve unose direktorija izabranog tipa unosa.

Napredno pretraživanje

Napredno pretraživanje vam omogućava da specificirate ograničenja pretraživanja i omogućite filtere pretraživanja. Koristite Jednostavno pretraživanje kako bi koristili default kriterij pretraživanja.

- Kako bi izvodili napredno pretraživanje:
  1. Na kartici **Filter pretraživanja** kliknite na **Napredno pretraživanje**.
  2. Izaberite **Atribut** iz padajuće liste.
  3. Izaberite operator **Usporedba**
     - =Atribut je jednak vrijednosti.
     - ! Atribut nije jednak vrijednosti.
     - < Atribut je manji od ili jednak vrijednosti.
     - > Atribut je veći od ili jednak vrijednosti.
     - ~ Atribut je približno jednak vrijednosti.
  4. Unesite **Vrijednost** za usporedbu.
  5. Koristite gumbe operatora pretraživanja za kompleksne upite.
     - Ako ste već dodali barem jedan filter pretraživanja, specificirajte dodatni kriterij i kliknite na **AND**. **AND** naredba vraća unose koji se podudaraju za oba skupa kriterija pretraživanja.
     - Ako ste već dodali barem jedan filter pretraživanja, specificirajte dodatni kriterij i kliknite na **OR**. Naredba **OR** vraća unose koji se podudaraju s bilo kojim skupom kriterija pretraživanja.
  6.
     - Kliknite na **Dodaj** da dodate kriterij filtera pretraživanja naprednom pretraživanju.
     - Kliknite na **Obriši** da uklonite kriterij filtera pretraživanja iz naprednog pretraživanja.
     - Kliknite na **Reset** da obrišete sve filtere pretraživanja.

Ručno pretraživanje

Koristite tu metodu kako bi kreirali filter pretraživanja. Na primjer, kako bi pretraživali prezimena unesite sn=* u polje. Ako pretražujete više atributa, morate koristiti sintaksu filtera pretraživanja. Na primjer, kako bi pretraživali prezimena određenog unosa, unesite:

`(&(sn=*)(dept=<departmentname>))`

Opcije

Na **kartici Opcije**:

- **Pretražite bazni DN** - Izaberite sufiks iz padajuće liste kako bi pretraživali samo unutar tog sufiksa.

Bilješka: Ako ste pokrenuli taj zadatak iz panela **Upravljanje unosima**, to polje je već ispunjeno za vas. Izabrali ste **Nadređeno DN** prije nego ste kliknuli na **Dodaj** kako bi pokrenuli proces dodaj unos.

Možete izabrati i **Svi sufiksi** kako bi pretražili cijelo stablo.

- **Opseg pretraživanja**
  - Izaberite **Objekt** kako bi pretraživali samo unutar izabranog objekta.
  - Izaberite **Jedna razina** kako bi pretraživali samo neposredno podređene izabranog objekta.
  - Izaberite **Podstablo** kako bi pretraživali sve potomke izabranog unosa.
- **Granica veličine pretraživanja** - Unesite maksimalan broj unosa koje ćete pretraživati ili izaberite **Neograničeno**.
- **Granica vremena pretraživanja** - Unesite maksimalan broj sekundi za pretraživanje ili izaberite **Neograničeno**.
- Izaberite tip **Dereferenciranja zamjenskog imena** iz padajućeg popisa.
  - **Nikad** - Ako je izabrani unos zamjensko ime, on se ne dereferencira za pretraživanje, odnosno, pretraživanje zanemaruje referencu na zamjensko ime.
  - **Pronalaženje** - Ako je izabrani unos zamjensko ime, pretraživanje dereferencira zamjensko ime i pretražuje iz lokacije zamjenskog imena.
  - **Pretraživanje** - Izabrani unos se ne dereferencira, no dereferenciraju se svi unosi pronađeni u pretraživanju.
  - **Uvijek** - Dereferenciraju se sva zamjenska imena na koje se je naišlo kod pretraživanja.
- Izaberite **Referali potjere** kontrolnu kućicu kako bi slijedili referale na drugog poslužitelja ako se referal vrati u pretraživanju. Kada referal usmjerava pretraživanje na drugog poslužitelja, veza na poslužitelja koristi trenutne vjerodajnice. Ako ste prijavljeni kao Anoniman, možda ćete se trebati prijaviti na poslužitelja korištenjem ovlaštenog DN-a.

Pogledajte “Podešavanje postavki pretraživanja” na stranici 100 kako bi dobili dodatne informacije o pretraživanjima.

Promjena binarnih atributa

Ako atribut traži binarne podatke, gumb **Binarni podaci** je prikazan uz polje atributa. Ako atribut nema podatke, polje je prazno. Budući se binarni atributi ne mogu prikazati, ako atribut sadrži binarne podatke, polje prikazuje **Binarni podaci - 1**. Ako atribut sadrži više vrijednosti, polje se prikazuje kao padajući popis.

Kliknite na gumb **Binarni podaci** kako bi radili s binarnim atributima.

Možete importirati, eksportirati ili brisati binarne podatke.

Kako bi dodali binarne podatke na atribut:

1. Kliknite na gumb **Binarni podaci**.
2. Kliknite na **Importiraj**.
3. Možete unijeti ime staze za datoteku koju želite ili kliknuti na **Pregled** kako bi locirali i izabrali binarnu datoteku.
4. Kliknite na **Submitiraj datoteku**. Prikazat će se poruka Datoteka učitana.
5. Kliknite na **Zatvori**. Sada je prikazano **Binarni podaci - 1** pod **Unosi binarnih podataka**.
6. Ponovite proces importiranja za onoliko binarnih datoteka koliko ih želite dodati. Naredni upisi se ispisuju kao **Binarni podaci - 2**, **Binarni podaci -3** itd.
7. Kada završite s dodavanjem binarnih podataka, kliknite na **OK**.

Kako bi eksportirali binarne podatke:

1. Kliknite na gumb **Binarni podaci**.
2. Kliknite na **Eksportiraj**.
3. Kliknite na vezu **Binarni podaci koji će se učitati**.
4. Slijedite upute na vašem čarobnjaku kako bi prikazali binarnu datoteku ili je spremili na novu lokaciju.
5. Kliknite na **Zatvori**.
6. Ponovite proces importiranja za onoliko binarnih datoteka koliko ih želite eksportirati.

7. Kada završite s importiranjem binarnih podataka, kliknite na **OK**.

Kako bi obrisali binarne podatke:

1. Kliknite na gumb **Binarni podaci**.
2. Označite binarnu datoteku koju želite obrisati. Može se izabrati više datoteka.
3. Kliknite na **Briši**.
4. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**. Binarni podaci koji su bili označeni za brisanje se uklanjaju iz popisa.
5. Kada dovršite brisanje podataka, kliknite na **OK**.

Bilješka: Binarni atributi nisu pretražljivi.

Upravljanje korisnicima i grupama

Za upravljanje korisnicima i grupama, proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

Pogledajte sljedeće za više informacija:

- "Upravljanje korisnicima"
- "Upravljanje grupama" na stranici 136

Upravljanje korisnicima

Nakon što ste postavili svoja područja i predloške, možete ih popuniti korisnicima. Pogledajte sljedeće:

- "Dodavanje korisnika"
- "Pronalaženje korisnika unutar područja"
- "Uređivanje informacija o korisniku" na stranici 136
- "Kopiranje korisnika" na stranici 136
- "Uklanjanje korisnika" na stranici 136

Dodavanje korisnika

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Dodaj korisnika** ili kliknite na **Upravljaj korisnicima** i kliknite na **Dodaj**.
2. Iz padajućeg izbornika izaberite područje kojem želite dodati korisnika.
3. Kliknite na **Sljedeće**. Prikazat će se predložak koji je pridružen tom području. Popunite potrebna polja koja su označena zvjezdicom (*) i bilo koja druga polja na karticama. Ako ste već kreirali grupe unutar područja, možete dodati korisnika na jednu ili više grupa.
4. Kada ste završili, kliknite na **Završetak**.

Pronalaženje korisnika unutar područja

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Pronađi korisnika** ili kliknite na **Upravljaj korisnicima** i kliknite na **Pronađi**.
2. Izaberite područje koje želite pretraživati iz polja **Izbor područja**.
3. Unesite niz pretraživanja u polje **Atribut imenovanja**. Podržani su zamjenski znakovi, na primjer, ako ste unijeli ***smith**, rezultat su svi unosi čiji atribut imenovanja završava sa smith.
4. Možete izvoditi sljedeće operacije na izabranom korisniku:
   - **Uredi** - Pogledajte "Uređivanje informacija o korisniku" na stranici 136.
   - **Kopiraj** - Pogledajte "Kopiranje korisnika" na stranici 136.
   - **Obriši** - Pogledajte "Uklanjanje korisnika" na stranici 136.
5. Kada ste gotovi, kliknite na **OK**.

Uređivanje informacija o korisniku

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljaj korisnicima**.
2. Izaberite područje iz padajućeg izbornika. Kliknite na **Pregled korisnika**, ako korisnici nisu već prikazani u kućici **Korisnici**.
3. Izaberite korisnike koje želite uređivati i kliknite na **Uređivanje**.
4. Promijenite informacije na karticama, promijenite članstvo grupe.
5. Kada ste gotovi, kliknite na **OK**.

Kopiranje korisnika

Ako trebate kreirati više korisnika koji imaju većinom identične informacije, možete kreirati dodatne korisnike kopiranjem inicijalnog korisnika i modificiranjem informacija.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljaj korisnicima**.
2. Izaberite područje iz padajućeg izbornika. Kliknite na **Pregled korisnika**, ako korisnici nisu već prikazani u kućici **Korisnici**.
3. Izaberite korisnike koje želite kopirati i kliknite na **Kopiraj**.
4. Promijenite prikladne informacije za novog korisnika, na primjer potrebne informacije koje identificiraju određenog korisnika, kao što je sn ili cn. Informacije koje su zajedničke za oba korisnika se ne trebaju mijenjati.
5. Kada ste gotovi, kliknite na **OK**.

Uklanjanje korisnika

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljaj korisnicima**.
2. Izaberite područje iz padajućeg izbornika. Kliknite na **Pregled korisnika**, ako korisnici nisu već prikazani u kućici **Korisnici**.
3. Izaberite korisnika kojeg želite ukloniti i kliknite na **Brisanje**.
4. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**.
5. Korisnik se uklanja iz popisa korisnika.

Upravljanje grupama

Nakon što ste postavili svoja područja i predloške, možete kreirati grupe. Pogledajte sljedeće:

- “Dodavanje grupa”
- “Pronalaženje grupa unutar područja” na stranici 137
- “Uređivanje informacija grupe” na stranici 137
- “Kopiranje grupe” na stranici 137
- “Uklanjanje grupe” na stranici 137

Dodavanje grupa

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Dodaj grupu** ili kliknite na **Upravljaj grupama** i kliknite na **Dodavanje**.
2. Unesite ime grupe koju želite kreirati.
3. Iz padajućeg izbornika izaberite područje kojem želite dodati korisnika.
4. Kliknite na **Završetak** kako bi kreirali grupu. Ako već imate korisnike u području, možete kliknuti na **Sljedeće** i izabrati korisnike koji će se dodati grupi. Nakon toga kliknite na **Završetak**.

Pogledajte “Grupe i uloge” na stranici 42 kako bi dobili dodatne informacije.

Pronalaženje grupa unutar područja

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Pronađi grupu** ili kliknite na **Upravljaj grupama** i kliknite na **Pronađi**.
2. Izaberite područje koje želite pretraživati iz polja **Izbor područja**.
3. Unesite niz pretraživanja u polje **Atribut imenovanja**. Podržani su zamjenski znakovi, na primjer, ako ste unijeli ***klub**, rezultat su sve grupe koje imaju atribut imenovanja klub, na primjer, knjižni klub, šahovski klub, vrtni klub itd.
4. Možete izvoditi sljedeće operacije na izabranoj grupi:
   - **Uredi** - Pogledajte "Uređivanje informacija grupe".
   - **Kopiraj** - Pogledajte "Kopiranje grupe".
   - **Obriši** - Pogledajte "Uklanjanje grupe".
5. Kada ste gotovi, kliknite na **Zatvori**.

Uređivanje informacija grupe

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljaj grupama**.
2. Izaberite područje iz padajućeg izbornika. Kliknite na **Pregled grupa** ako grupe nisu već prikazane u kućici **Grupe**.
3. Izaberite grupu koju želite obrađivati i kliknite na **Uređivanje**.
4. Možete kliknuti na **Filter** kako bi ograničili broj **Dostupnih korisnika**. Na primjer, unošenje *smith u polje Prezime ograničava dostupne korisnike na one čije ime završava sa smith, kao što su Ann Smith, Bob Smith, Joe Goldsmith itd.
5. Možete dodati ili ukloniti korisnike iz grupe.
6. Kada ste gotovi, kliknite na **OK**.

Kopiranje grupe

Ako trebate kreirati više grupa koje imaju većinom iste članove, možete kreirati dodatne grupe kopiranjem inicijalne grupe i modificiranjem informacije.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljaj grupama**.
2. Izaberite područje iz padajućeg izbornika. Kliknite na **Pregled grupa** ako grupe već nisu prikazane u kućici **Grupe**.
3. Izaberite grupu koju želite kopirati i kliknite na **Kopiraj**.
4. Promijenite ime grupe u polju **Ime grupe**. Nova grupa ima iste članove kao i originalna grupa.
5. Možete modificirati članove grupe.
6. Kada ste gotovi, kliknite na **OK**. Kreirana je nova grupa i ona sadrži iste članove kao originalna grupa sa svim preinakama dodavanja ili uklanjanja koje ste izveli za vrijeme procedure kopiranja.

Uklanjanje grupe

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljaj grupama**.
2. Izaberite područje iz padajućeg izbornika. Kliknite na **Pregled grupa** ako grupe nisu već prikazane u kućici **Grupe**.
3. Izaberite grupu koju želite ukloniti i kliknite na **Brisanje**.
4. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**.
5. Grupa se uklanja iz popisa grupa.

Upravljanje područjima i predlošcima korisnika

Za upravljanje područjima i predlošcima korisnika, kliknite na **Područja i predlošci** u području navigacije Web administracijskog alata. Koristite područja i predloške korisnika kako bi olakšali drugima da unose podatke u direktorij. Za više informacija o konceptima područja i predložak korisnika, pogledajte “Područja i predlošci korisnika” na stranici 38.

Pogledajte sljedeće za više informacija:

- “Kreiranje područja”
- “Kreiranje administratora područja”
- “Kreiranje predloška” na stranici 139
- “Dodavanje predloška na područje” na stranici 141
- “Kreiranje grupa” na stranici 141
- “Dodavanje korisnika u područje” na stranici 141
- “Upravljanje područjima” na stranici 141
- “Upravljanje predlošcima” na stranici 142

Kreiranje područja

Za više informacija o konceptima područja i predložak korisnika, pogledajte “Područja i predlošci korisnika” na stranici 38.

Za kreiranje područja, napravite sljedeće:

1. Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.
2. Kliknite na **Dodaj područje**.
   - Unesite ime za područje. Na primjer, **realm1**.
   - Unesite Nadređeno DN koje identificira lokaciju područja. Taj unos je u obliku sufiksa, na primjer o=ibm,c=us. Taj unos može biti sufiks ili unos negdje drugdje u direktoriju. Možete kliknuti i na **Pregled** da izaberete lokaciju podstabla koju želite.
3. Kliknite na **Sljedeće** za nastavak ili kliknite na **Završetak**.
4. Ako ste kliknuli na **Sljedeće**, ponovo pregledajte informacije. U tom trenutku još niste stvarno kreirali područje tako da se mogu zanemariti **Predložak korisnika** i **Filter pretraživanja korisnika**.
5. Kliknite na **Završetak** da kreirate područje.

Kreiranje administratora područja

Kako bi kreirali administratora područja, morate kreirati grupu administracije za područje tako da napravite sljedeće:

1. Kreirajte grupu administracije područja.
   a. Proširite kategoriju **Upravljanje direktorijom** u području navigacije Web administracijskog alata.
   b. Kliknite na **Upravljanje unosima**.
   c. Proširite stablo i izaberite područje koje ste upravo kreirali, **cn=realm1,o=ibm,c=us**.
   d. Kliknite na **Uredi ACL**.
   e. Kliknite na karticu **Vlasnici**.
   f. Provjerite da li je označeno **Proširi korisnika**.
   g. Unesite DN za područje, **cn=realm1,o=ibm,c=us**.
   h. Promijenite **Tip** u grupu.
   i. Kliknite **Dodaj**.
2. Kreirajte unos administratora. Ako već nemate unos korisnika za administratora, morate ga kreirati.
   a. Proširite kategoriju **Upravljanje direktorijom** u području navigacije Web administracijskog alata.
   b. Kliknite na **Upravljanje unosima**.

c. Proširite drvo na lokaciju na kojoj želite da prebiva unos administratora.

   Bilješka: Smještanjem unosa administratora izvan područja se izbjegava da bi administrator mogao slučajno obrisati njega ili nju. U ovom primjeru bi lokacija mogla biti **o=ibm,c=us**.

d. Kliknite **Dodaj**.
e. Izaberite **Strukturalna klasa objekta**, na primjer **inetOrgPerson**.
f. Kliknite na **Sljedeće**.
g. Izaberite pomoćnu klasu objekta koju želite dodati.
h. Kliknite na **Sljedeće**.
i. Unesite potrebne atribute za unos. Na primjer,
   - **RDN** cn=JohnDoe
   - **DN** o=ibm,c=us
   - **cn** John Doe
   - **sn** Doe
j. Na kartici **Drugi atributi** provjerite da li vam je dodijeljena lozinka.
k. Kada ste završili, kliknite na **Završetak**.

3. Dodajte administratora na grupu administracije.
   a. Proširite kategoriju **Upravljanje direktorijom** u području navigacije Web administracijskog alata.
   b. Kliknite na **Upravljanje unosima**.
   c. Proširite stablo i izaberite područje koje ste upravo kreirali, **cn=realm1,o=ibm,c=us**.
   d. Kliknite na **Uredi atribute**.
   e. Kliknite na karticu **Članovi**.
   f. Kliknite na **Članovi**.
   g. U polje **Članovi** unesite DN administratora, u ovom primjeru **cn=John Doe,o=ibm,c=us**.
   h. Kliknite **Dodaj**. DN se prikazuje u popisu **Članovi**.
   i. Kliknite **OK**.
   j. Kliknite na **Ažuriraj**. DN se prikazuje u popisu **Trenutni članovi**.
   k. Kliknite **OK**.
4. Kreirali ste administratora koji može upravljati unosima unutar područja.

Kreiranje predloška

Nakon što ste kreirali područje, vaš slijedeći korak je kreiranje predloška korisnika. Predložak vam pomaže da organizirate informacije koje želite unijeti. Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite na **Dodaj predložak korisnika**.
   - Unesite ime za predložak, na primjer **template1**.
   - Unesite lokaciju na kojoj će predložak prebivati. U svrhu replikacije, locirajte predložak u podstablu područja koje će koristiti taj predložak. Na primjer, područje kreirano u prethodnim operacijama **cn=realm1,o=ibm,c=us**. Možete kliknuti na **Pregled** za izbor drugog podstabla za lokaciju predloška.
2. Kliknite na **Sljedeće**. Možete kliknuti na **Završetak** kako bi kreirali prazan predložak. Kasnije možete dodati informacije predlošku, pogledajte “Uređivanje predloška” na stranici 144.
3. Ako ste kliknuli na **Sljedeće**, za predložak izaberite strukturalnu klasu objekta, na primjer **inetOrgPerson**. Možete dodati i sve pomoćne klase objekta koje želite.
4. Kliknite na **Sljedeće**.
5. Tablica **Potrebno** je bila kreirana na predlošku. Možete modificirati informacije koje su sadržane na toj kartici.
   a. Izaberite **Potrebno** u izborniku kartice i kliknite na **Uredi**. Prikazan je panel **Uredi karticu**. Možete vidjeti ime kartice **Potrebno** i izabrane atribute koje treba klasa objekta, **inetOrgPerson**:

- *sn - prezime
- *cn - uobičajeno ime

Bilješka: * označava potrebne informacije.

b. Ako želite dodati dodatne informacije na tu karticu, izaberite atribut iz izbornika **Atributi**. Na primjer, izaberite **departmentNumber** i kliknite na **Dodaj**. Izaberite **employeeNumber** i kliknite na **Dodaj**. Izaberite **title** i kliknite na **Dodaj**. Izbornik **Izabrani atributi** sada izgleda:
   - title
   - employeeNumber
   - departmentNumber
   - *sn
   - *cn

c. Možete promijeniti način na koji se ta polja pojavljuju na predlošku tako da osvijetlite izabrane atribute i kliknete na **Premjesti gore** ili **Premjesti dolje**. Time se mijenja položaj atributa za jedan položaj. Ponavljajte tu proceduru tako dugo dok sve atribute ne stavite u željeni poredak. Na primjer,
   - *sn
   - *cn
   - title
   - employeeNumber
   - departmentNumber

d. Možete i modificirati svaki izabrani atribut.
   1) Osvijetlite atribut u kućici **Izabrani atributi** i kliknite na **Uredi**.
   2) Možete promijeniti ime prikaza polja kojeg koristite na predlošku. Na primjer, ako želite da se **brojOdjela** prikaže kao **Broj odjela**, unesite to u polje **Prikaz imena**.
   3) Možete osigurati i default vrijednost kojom će se popuniti polja atributa u predlošku. Na primjer, ako su većina korisnika koji će se unijeti članovi Odjela 789, možete unijeti 789 kao default vrijednost. Polje na predlošku će biti ispunjeno sa 789. Vrijednost se može promijeniti kada dodate stvarne informacije o korisniku.
   4) Kliknite **OK**.

e. Kliknite **OK**.

6. Kako bi kreirali drugu kategoriju kartice za dodatne informacije, kliknite na **Dodaj**.
   - Unesite ime za novu karticu. Na primjer, Informacije o adresi.
   - Za tu karticu izaberite atribute iz izbornika **Atributi**. Na primjer, izaberite **homePostalAddress** i kliknite na **Dodaj**. Izaberite **postOfficeBox** i kliknite na **Dodaj**. Izaberite **telephoneNumber** i kliknite na **Dodaj**. Izaberite **homePhone** i kliknite na **Dodaj**. Izaberite **facsimileTelephoneNumber** i kliknite na **Dodaj**. Izbornik **Izabrani atributi** sada izgleda:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone
     – facsimileTelephoneNumber
   - Možete promijeniti način na koji se ta polja pojavljuju na predlošku tako da osvijetlite izabrane atribute i kliknete na **Premjesti gore** ili **Premjesti dolje**. Time se mijenja položaj atributa za jedan položaj. Ponavljajte tu proceduru tako dugo dok sve atribute ne stavite u željeni poredak. Na primjer,
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – facsimileTelephoneNumber

– homePhone
- Kliknite **OK**.

7. Ponovite taj proces za onoliko kartica koliko ih želite kreirati. Kada ste gotovi, kliknite na **Završetak** kako bi kreirali predložak.

Dodavanje predloška na područje

Nakon što ste kreirali područje i predložak, trebate dodati predložak na područje. Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljaj područjima**.
2. Izaberite područje kojem želite dodati predložak, u ovom primjeru **cn=realm1,o=ibm,c=us** i kliknite na **Uredi**.
3. Spustite se na **Predložak korisnika** i proširite padajući izbornik.
4. Izaberite predložak, u ovom primjeru **cn=template1,cn=realm1,o=ibm,c=us**.
5. Kliknite **OK**.
6. Kliknite na **Zatvori**.

Kreiranje grupa

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Dodaj grupu**.
2. Unesite ime grupe koju želite kreirati. Na primjer **grupa1**.
3. Iz padajućeg izbornika izaberite područje kojem želite dodati korisnika. U ovom slučaju **područje1**.
4. Kliknite na **Završetak** kako bi kreirali grupu. Ako već imate korisnike u području, možete kliknuti na **Sljedeće** i izabrati korisnike koji će se dodati grupi grupa1. Nakon toga kliknite na **Završetak**.

Pogledajte “Grupe i uloge” na stranici 42 kako bi dobili dodatne informacije.

Dodavanje korisnika u područje

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Dodaj korisnika**.
2. Iz padajućeg izbornika izaberite područje kojem želite dodati korisnika. U ovom slučaju **područje1**.
3. Kliknite na **Sljedeće**. Prikazuje se predložak kojeg ste upravo kreirali, predložak1. Popunite potrebna polja koja su označena zvjezdicom (*) i bilo koja druga polja na karticama. Ako ste već kreirali grupe unutar područja, možete dodati korisnika na jednu ili više grupa.
4. Kada ste završili, kliknite na **Završetak**.

Upravljanje područjima

Nakon što ste postavili i popunili svoje početno područje, možete dodati dodatna područja ili preinačiti postojeća područja.

Proširite kategoriju **Područja i predlošci** u području navigacije i kliknite na **Upravljaj područjima**. Prikazuje se popis postojećih područja. Iz tog panela možete dodati područje, uređivati područje, ukloniti područje ili uređivati liste kontrole pristupa (ACL-ovi) područja. Za više informacija, pogledajte sljedeće:

- “Dodavanje područja”
- “Uređivanje područja” na stranici 142
- “Uklanjanje područja” na stranici 142
- “Uređivanje ACL-ova na području” na stranici 142

Dodavanje područja

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite na **Dodaj područje**.

- Unesite ime za područje. Na primjer, **područje2**.
- Ako imate područja koja postoje već od ranije, na primjer, **područje1**, možete izabrati to područje kako bi se njegove postavke kopirale na područje koje kreirate.
- Unesite Nadređeno DN koje identificira lokaciju područja. Taj unos je u obliku sufiksa, na primjer **o=ibm,c=us**. Možete kliknuti i na **Pregled** da izaberete lokaciju podstabla koju želite.

2. Kliknite na **Sljedeće** za nastavak ili kliknite na **Završetak**.
3. Ako ste kliknuli na **Sljedeće**, ponovo pregledajte informacije.
4. Izaberite **Predložak korisnika** iz padajućeg izbornika. Ako ste kreirali postavke iz područja koje je već ranije postojalo, predložak je već popunjen.
5. Unesite **Filter pretraživanja korisnika**.
6. Kliknite na **Završetak** da kreirate područje.

Uređivanje područja

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

- Kliknite na **Upravljaj područjima**.
- Izaberite područje koje želite uređivati iz popisa područja.
- Kliknite na **Uredi**.
  - Možete koristiti gumb **Pregled** za promjenu
    - Grupe administratora
    - Spremnika grupe
    - Spremnika korisnika
  - Možete izabrati drugi predložak iz padajućeg izbornika.
  - Kliknite na **Uređivanje** kako bi modificirali **Filter pretraživanja korisnika**.
- Kliknite na **OK** kada ste gotovi.

Uklanjanje područja

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljaj područjima**.
2. Izaberite područje koje želite ukloniti.
3. Kliknite na **Briši**.
4. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**.
5. Područje je uklonjeno iz popisa područja.

Uređivanje ACL-ova na području

Kako bi pregledali ACL svojstva korištenjem pomoćnog programa Web administracijski alat i kako bi radili s ACL-ovima, pogledajte “Upravljanje listama kontrole pristupa (ACL-ovi)” na stranici 145.

Pogledajte “Lista kontrole pristupa” na stranici 47 kako bi dobili dodatne informacije.

Upravljanje predlošcima

Nakon što ste kreirali vaš početni predložak, možete dodati više predložaka ili modificirati postojeće predloške.

Proširite kategoriju **Područja i predlošci** u području navigacije i kliknite na **Upravljaj predlošcima korisnika**. Prikazuje se popis postojećih predložaka. Iz tog panela možete dodati predložak, uređivati predložak, ukloniti predložak ili uređivati liste kontrole pristupa (ACL-ovi) predloška. Za više informacija, pogledajte sljedeće:

- “Dodavanje predloška korisnika” na stranici 143
- “Uređivanje predloška” na stranici 144
- “Uklanjanje predloška” na stranici 144
- “Uređivanje ACL-ova na predlošku” na stranici 144

Dodavanje predloška korisnika

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite na **Dodaj predložak korisnika** ili kliknite na **Upravljaj predlošcima korisnika** i kliknite na **Dodaj**.
   - Unesite ime za novi predložak. Na primjer, **predložak2**.
   - Ako imate predloške koji postoje od ranije, na primjer **predložak1**, možete izabrati predložak kako bi se njegove postavke kopirale na predložak kojeg kreirate.
   - Unesite Nadređeno DN koje identificira lokaciju predloška. Taj unos je u obliku DN-a, na primjer **cn=realm1,o=ibm,c=us**. Možete kliknuti i na **Pregled** da izaberete lokaciju podstabla koju želite.
2. Kliknite na **Sljedeće**. Možete kliknuti na **Završetak** kako bi kreirali prazan predložak. Kasnije možete dodati informacije na predložak, pogledajte "Uređivanje predloška" na stranici 144.
3. Ako ste kliknuli na **Sljedeće**, za predložak izaberite strukturalnu klasu objekta, na primjer **inetOrgPerson**. Možete dodati i sve pomoćne klase objekta koje želite.
4. Kliknite na **Sljedeće**.
5. Tablica **Potrebno** je bila kreirana na predlošku. Možete modificirati informacije koje su sadržane na toj kartici.
   a. Izaberite **Potrebno** u izborniku kartice i kliknite na **Uredi**. Prikazan je panel **Uredi karticu**. Možete vidjeti ime kartice **Potrebno** i izabrane atribute koje treba klasa objekta, **inetOrgPerson**:
      - *sn - prezime
      - *cn - uobičajeno ime

      Bilješka: * označava potrebne informacije.
   b. Ako želite dodati dodatne informacije na tu karticu, izaberite atribut iz izbornika **Atributi**. Na primjer, izaberite **departmentNumber** i kliknite na **Dodaj**. Izaberite **employeeNumber** i kliknite na **Dodaj**. Izaberite **title** i kliknite na **Dodaj**. Izbornik **Izabrani atributi** sada izgleda:
      - title
      - employeeNumber
      - departmentNumber
      - *sn
      - *cn
   c. Možete promijeniti način na koji se ta polja pojavljuju na predlošku tako da osvijetlite izabrane atribute i kliknete na **Premjesti gore** ili **Premjesti dolje**. Time se mijenja položaj atributa za jedan položaj. Ponavljajte tu proceduru tako dugo dok sve atribute ne stavite u željeni poredak. Na primjer,
      - *sn
      - *cn
      - title
      - employeeNumber
      - departmentNumber
   d. Možete i modificirati svaki izabrani atribut.
      1) Osvijetlite atribut u kućici **Izabrani atributi** i kliknite na **Uredi**.
      2) Možete promijeniti ime prikaza polja kojeg koristite na predlošku. Na primjer, ako želite da se **brojOdjela** prikaže kao **Broj odjela**, unesite to u polje **Prikaz imena**.
      3) Možete osigurati i default vrijednost kojom će se popuniti polja atributa u predlošku. Na primjer, ako su većina korisnika koji će se unijeti članovi Odjela 789, možete unijeti 789 kao default vrijednost. Polje na predlošku će biti ispunjeno sa 789. Vrijednost se može promijeniti kada dodate stvarne informacije o korisniku.
      4) Kliknite **OK**.
   e. Kliknite **OK**.
6. Kako bi kreirali drugu kategoriju kartice za dodatne informacije, kliknite na **Dodaj**.
   - Unesite ime za novu karticu. Na primjer, Informacije o adresi.

- Za tu karticu izaberite atribut iz izbornika **Atributi**. Na primjer, izaberite **homePostalAddress** i kliknite na **Dodaj**. Izaberite **postOfficeBox** i kliknite na **Dodaj**. Izaberite **telephoneNumber** i kliknite na **Dodaj**. Izaberite **homePhone** i kliknite na **Dodaj**. Izaberite **facsimileTelephoneNumber** i kliknite na **Dodaj**. Izbornik **Izabrani atributi** sada izgleda:
  - homePostalAddress
  - postOfficeBox
  - telephoneNumber
  - homePhone
  - facsimileTelephoneNumber
- Možete promijeniti način na koji se ta polja pojavljuju na predlošku tako da osvijetlite izabrane atribute i kliknete na **Premjesti gore** ili **Premjesti dolje**. Time se mijenja položaj atributa za jedan položaj. Ponavljajte tu proceduru tako dugo dok sve atribute ne stavite u željeni poredak. Na primjer,
  - homePostalAddress
  - postOfficeBox
  - telephoneNumber
  - facsimileTelephoneNumber
  - homePhone
- Kliknite **OK**.

7. Ponovite taj proces za onoliko kartica koliko ih želite kreirati. Kada ste gotovi, kliknite na **Završetak** kako bi kreirali predložak.

Uređivanje predloška

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

- Kliknite na **Upravljaj predlošcima korisnika**.
- Izaberite područje koje želite uređivati iz popisa područja.
- Kliknite na **Uredi**.
- Ako imate predloške koji postoje od ranije, na primjer predložak1, možete izabrati predložak tako da se njegove postavke kopiraju na predložak kojeg uređujete.
- Kliknite na **Sljedeće**.
  - Možete koristiti padajući izbornik kako bi promijenili strukturiranu klasu predloška
  - Možete dodati ili ukloniti pomoćne klase objekta.
- Kliknite na **Sljedeće**.
- Možete modificirati kartice i atribute koji su sadržani u predlošku. Pogledajte 5 na stranici 143 kako bi dobili informacije o tome kako da modificirate kartice.
- Kada ste završili, kliknite na **Završetak**.

Uklanjanje predloška

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljaj predlošcima korisnika**.
2. Izaberite predložak kojeg želite ukloniti.
3. Kliknite na **Briši**.
4. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**.
5. Predložak se uklanja iz popisa predložaka.

Uređivanje ACL-ova na predlošku

Proširite kategoriju **Područja i predložak** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljaj predlošcima korisnika**.
2. Izaberite predložak za kojeg želite uređivati ACL-ove.

3. Kliknite na **Uredi ACL**.

Kako bi pregledali ACL svojstva korištenjem pomoćnog programa Web administracijski alat i kako bi radili s ACL-ovima, pogledajte “Upravljanje listama kontrole pristupa (ACL-ovi)”.

Pogledajte “Lista kontrole pristupa” na stranici 47 kako bi dobili dodatne informacije.

Upravljanje listama kontrole pristupa (ACL-ovi)

Za više informacija o listama kontrole pristupa, pogledajte “Lista kontrole pristupa” na stranici 47.

Kako bi pregledali ACL svojstva korištenjem Web administracijskog alata i kako bi radili s ACL-ovima, napravite sljedeće:

1. Izaberite unos direktorija. Na primjer, cn=John Doe,ou=Advertising,o=ibm,c=US.
2. Kliknite na **Uredi ACL**. Prikazan je Uredi Acl panel s već izabranom karticom **Učinkoviti ACL-ovi**.

Taj panel ima pet kartica:

- “Učinkoviti ACL-ovi”
- “Učinkoviti vlasnici”
- “Ne-filtrirani ACL-ovi” na stranici 146
- “Filtrirani ACL-ovi” na stranici 147
- “Vlasnici” na stranici 148

Kartice **Učinkoviti ACL-ovi** i **Učinkoviti vlasnici** sadrže informacije samo za čitanje o ACL-ovima.

Učinkoviti ACL-ovi

Učinkoviti ACL-ovi su eksplicitni i naslijeđeni ACL-ovi izabranog unosa. Prava pristupa za određeni učinkoviti ACL možete pregledati tako da ga izaberete i kliknete na gumb **Pregled**. Otvara se panel **Pregled prava pristupa**.

Pregled prava pristupa

- Odlomak **Prava** prikazuje prava dodavanja i brisanja subjekta.
  - **Dodaj podređenog** dodjeljuje ili ne dodjeljuje subjektu pravo da doda unos direktorija ispod izabranog unosa.
  - **Obriši unos** dodjeljuje ili ne dodjeljuje subjektu pravo da obriše izabrani unos.
- Odlomak **Sigurnost** definira dozvole za klase sigurnosti. Atributi su grupirani u klase sigurnosti:
  - **Normalne** - Normalne klase atributa traže najmanje sigurnosti, na primjer, atribut commonName.
  - **Osjetljive** - Osjetljive klase atributa traže umjerenu količinu sigurnosti, na primjer homePhone.
  - **Kritične** - Kritične klase atributa traže najviše sigurnosti, na primjer, atribut userpassword.

  Svaka klasa sigurnosti ima dozvole koje su joj pridružene.
  - **Čitaj** - subjekt može čitati atribute.
  - **Piši** - subjekt može modificirati atribute.
  - **Traži** - subjekt može tražiti atribute.
  - **Usporedi** - subjekt može usporediti atribute.

Kliknite na **OK** kako bi se vratili na karticu Učinkoviti ACL-ovi.

Kliknite na **Opoziv** kako bi se vratili na panel Uredi ACL.

Učinkoviti vlasnici

Učinkoviti vlasnici su eksplicitni i naslijeđeni vlasnici izabranog unosa.

Ne-filtrirani ACL-ovi

Možete dodati nove ne-filtrirane ACL-ove na unos ili uređivati postojeće ne-filtrirane ACL-ove.

Ne-filtrirani ACL-ovi se mogu širiti. To znači da se informacije kontrole pristupa definirane za jedan unos mogu primijeniti na sve njegove podređene unose. ACL izvor je izvor trenutnog ACL-a za izabrani unos. Ako unos nema ACL, on nasljeđuje ACL od nadređenih objekata na temelju ACL postavki nadređenih objekata.

Unesite sljedeće informacije na karticu **Ne-filtrirani** ACL-ovi:

- ACL-ovi širenja - Izaberite kontrolnu kućicu **Širenje** kako bi dozvolili potomcima bez izričito definiranog ACL-a da nasljeđuju iz ovog unosa. Ako je kontrolna kućica izabrana, potomci nasljeđuju ACL-ove iz ovog unosa, a ako je ACL izričito definiran za unos podređenog, onda se acl koji je bio naslijeđen iz nadređenog zamjenjuje s novim ACL-om koji je bio dodan. Ako kontrolna kućica nije izabrana, unosi potomka bez izričito definiranog ACL će naslijediti ACL-ove iz onog koji je nadređen unosu koji je omogućio tu opciju.
- DN (Razlikovno ime) - Unesite **(DN) Razlikovno ime** entiteta koji traži pristup za izvođenje operacija na izabranom unosu, na primjer, cn=Marketing Group.
- Tip - Unesite **Tip** DN-a. Na primjer, izaberite access-id ako je DN korisnik.

Dodavanje i uređivanje prava pristupa

Kliknite na gumb **Dodaj** kako bi dodali DN u polje DN (Razlikovno ime) na ACL popisu ili na gumb Uredi kako bi modificirali ACL-ove postojećeg DN-a.

Paneli **Dodaj prava pristupa** i **Uredi prava pristupa** vam omogućavaju da postavite prava pristupa za nove ili postojeće liste kontrole pristupa (ACL-ovi). Polje **Tip** se postavlja na tip kojeg ste izabrali na panelu **Uredi ACL**. Ako dodajete ACL, sva druga polja postaju prazna. Ako uređujete ACL, polja sadrže vrijednosti koje su postavljene kada je zadnji put bio modificiran ACL.

Možete:

- Promijeniti ACL tip
- Postaviti prava dodavanja i brisanja
- Postaviti dozvole za klase sigurnosti

Kako bi postavili prava pristupa:

1. Izaberite **Tip** unosa za ACL. Na primjer, izaberite access-id ako je DN korisnik.
2. Odlomak **Prava** prikazuje prava dodavanja i brisanja subjekta.
   - **Dodaj podređenog** dodjeljuje ili ne dodjeljuje subjektu pravo da doda unos direktorija ispod izabranog unosa.
   - **Obriši unos** dodjeljuje ili ne dodjeljuje subjektu pravo da obriše izabrani unos.
3. Odlomak **Klasa sigurnosti** definira dozvole za klase atributa. Atributi su grupirani u klase sigurnosti:
   - Normalna - Normalne klase atributa traže najmanje sigurnosti, na primjer, atribut commonName.
   - Osjetljiva - Osjetljive klase atributa traže umjerenu količinu sigurnosti, na primjer homePhone.
   - Kritična - Kritične klase atributa traže najviše sigurnosti, na primjer, atribut userpassword.

   Svaka klasa sigurnosti ima dozvole koje su joj pridružene.
   - Čitaj - subjekt može čitati atribute.
   - Piši - subjekt može modificirati atribut.
   - Traži - subjekt može tražiti atribute.
   - Usporedi - subjekt može uspoređivati atribute.

   Osim toga, možete specificirati dozvole koje se temelje na atributu umjesto na klasi sigurnosti kojoj pripada atribut. Odlomak o atributima je ispisan ispod **Kritična klasa sigurnosti**.
   - Izaberite atribut iz padajućeg izbornika **Definiranje atributa**.

- Kliknite na **Definiraj**. Atribut se prikazuje s tablicom dozvola.
- Specificirajte da li želite da se dodijele ili ne dodijele svakoj od četiri klase sigurnosti dozvole koje su pridružene atributu.
- Tu proceduru možete ponoviti za više atributa.
- Da uklonite atribut, jednostavno izaberite atribut i kliknite na **Obriši**.
- Kada ste gotovi kliknite na **OK**.

Uklanjanje ACL-ova

ACL-ove možete ukloniti na dva načina:

- Izaberite radijski gumb koji se nalazi uz ACL kojeg želite obrisati. Kliknite **Ukloni**.
- Kliknite na **Ukloni sve** kako bi obrisali sve DN-ove iz popisa.

Filtrirani ACL-ovi

Možete dodati nove filtrirane ACL-ove na unos ili uređivati postojeće filtrirane ACL-ove.

Filter-zasnovani ACL-ovi koriste filter-zasnovanu usporedbu koja koristi specificirani filter objekta, kako bi se uparili ciljni objekti s efektivnim pristupom koji se na njih odnosi.

Default ponašanje filter-zasnovanih ACL-ova je da skuplja od najniže sadržanog unosa, preko lanca unosa prethodnika, do najvišeg unosa koji je sadržan u DIT-u. Učinkovit pristup se izračunava kao unija dodijeljenih ili odbijenih prava pristupa od strane sastavnih unosa prethodnika. Postoji iznimka od tog ponašanja. Kako bi se ostvarila kompatibilnost sa svojstvom replikacije podstabla i omogućila veća administrativna kontrola, atribut plafona se koristi kao sredstvo zaustavljanja skupljanja na unosu u kojem je sadržan.

Unesite sljedeće informacije na karticu Filtrirani ACL-ovi:

- Prikupite filtrirane ACL-ove -
  - Izaberite radijski gumb **Nije specificirano** kako bi uklonili ibm-filterACLInherit atribut iz izabranog unosa.
  - Izaberite radijski gumb **True** kako bi dozvolili da se ACL-ovi za izabrani unos akumuliraju iz tog unosa, preko lanca prethodnika do najvišeg filtriranog ACL sadržanog unosa u DIT-a.
  - Izaberite radijski gumb **False** kako bi zaustavili skupljanje filtriranih ACL-ova na izabranom unosu.
- DN (Razlikovno ime) - Unesite **(DN) Razlikovno ime** entiteta koji traži pristup za izvođenje operacija na izabranom unosu, na primjer, cn=Marketing Group.
- Tip - Unesite **Tip** DN-a. Na primjer, izaberite access-id ako je DN korisnik.

Dodavanje i uređivanje prava pristupa

Kliknite na gumb **Dodaj** kako bi dodali DN u polje DN (Razlikovno ime) na ACL popisu ili na gumb Uredi kako bi modificirali ACL-ove postojećeg DN-a.

Paneli **Dodaj prava pristupa** i **Uredi prava pristupa** vam omogućavaju da postavite prava pristupa za nove ili postojeće liste kontrole pristupa (ACL-ovi). Polje tip se postavlja na tip kojeg ste izabrali na panelu Uredi ACL. Ako dodajete ACL, sva druga polja postaju prazna. Ako uređujete ACL, polja sadrže vrijednosti koje su postavljene kada je zadnji put bio modificiran ACL.

Možete:

- Promijeniti ACL tip
- Postaviti prava dodavanja i brisanja
- Postaviti filter objekta za filtrirane ACL-ove
- Postaviti dozvole za klase sigurnosti

Kako bi postavili prava pristupa:

1. Izaberite **Tip** unosa za ACL. Na primjer, izaberite access-id ako je DN korisnik.
2. Odlomak **Prava** prikazuje prava dodavanja i brisanja subjekta.
   - **Dodaj podređenog** dodjeljuje ili ne dodjeljuje subjektu pravo da doda unos direktorija ispod izabranog unosa.
   - **Obriši unos** dodjeljuje ili ne dodjeljuje subjektu pravo da obriše izabrani unos.
3. Postavite filter objekta za filter zasnovanu usporedbu. U polje **Filter objekta** unesite željeni filter objekta za izabrani ACL. Kliknite na gumb **Uredi filter** kako bi dobili pomoć kod sastavljanja niza filtera pretraživanja. Trenutni filtrirani ACL se širi na sve podređene objekte u pridruženom podstablu koje se podudara s filterom u tom polju.
4. Odlomak **Klasa sigurnosti** definira dozvole za klase atributa. Atributi su grupirani u klase sigurnosti:
   - Normalna - Normalne klase atributa traže najmanje sigurnosti, na primjer, atribut commonName.
   - Osjetljiva - Osjetljive klase atributa traže umjerenu količinu sigurnosti, na primjer homePhone.
   - Kritična - Kritične klase atributa traže najviše sigurnosti, na primjer, atribut userpassword.

   Svaka klasa sigurnosti ima dozvole koje su joj pridružene.
   - Čitaj - subjekt može čitati atribute.
   - Piši - subjekt može modificirati atribut.
   - Traži - subjekt može tražiti atribute.
   - Usporedi - subjekt može uspoređivati atribute.

   Osim toga, možete specificirati dozvole koje se temelje na atributu umjesto na klasi sigurnosti kojoj pripada atribut. Odlomak o atributima je ispisan ispod **Kritična klasa sigurnosti**.
   - Izaberite atribut iz padajućeg izbornika **Definiranje atributa**.
   - Kliknite na **Definiraj**. Atribut se prikazuje s tablicom dozvola.
   - Specificirajte da li želite da se dodijele ili ne dodijele svakoj od četiri klase sigurnosti dozvole koje su pridružene atributu.
   - Tu proceduru možete ponoviti za više atributa.
   - Da uklonite atribut, jednostavno izaberite atribut i kliknite na **Obriši**.
   - Kada ste gotovi kliknite na **OK**.

Uklanjanje ACL-ova

ACL-ove možete ukloniti na dva načina:

- Izaberite radijski gumb koji se nalazi uz ACL kojeg želite obrisati. Kliknite **Ukloni**.
- Kliknite na **Ukloni sve** kako bi obrisali sve DN-ove iz popisa.

Vlasnici

Vlasnici unosa imaju potpune dozvole za izvođenje bilo kojih operacija na objektu. Vlasnici unosa mogu biti eksplicitni ili prošireni (naslijeđeni).

Unesite sljedeće informacije na karticu **Vlasnici**:

- Izaberite kontrolnu kućicu **Širi korisnike** kako bi omogućili potomcima bez izričito definiranog vlasnika da nasljeđuju iz tog unosa. Ako nije izabrana kontrolna kućica, unosi potomka bez izričito definiranog vlasnika će naslijediti vlasnika iz onog koji je nadređen tom unosu koji je omogućio tu opciju.
- DN (Razlikovno ime) - Unesite **(DN) Razlikovno ime** entiteta koji traži pristup za izvođenje operacija na izabranom unosu, na primjer, cn=Marketing Group.

  Korištenje cn=this s objektima koji šire svoja vlasništvo na druge objekte olakšava kreiranje podstabla direktorija u kojem je svaki objekt vlasnik sam sebi.
- Tip - Unesite **Tip** DN-a. Na primjer, izaberite access-id ako je DN korisnik.

Dodavanje vlasnika

Kliknite na **Dodaj** kako bi popisu dodali DN u polje **DN (Razlikovno ime)**.

Uklanjanje vlasnika

Možete ukloniti vlasnika na dva načina:

- Izaberite radijski gumb koji se nalazi uz DN vlasnika kojeg želite obrisati. Kliknite **Ukloni**.
- Kliknite na **Ukloni sve** kako bi iz popisa obrisali sve DN-ove vlasnika.

Objavljivanje informacija poslužitelju direktorija

Možete konfigurirati svoj sistem tako da objavljuje određene informacije u Poslužitelju direktorija na istom sistemu ili na drugom sistemu, kao i korisnički definirane informacije. OS/400 automatski objavljuje te informacije na Poslužitelj direktorija kada koristite iSeries Navigator kako bi promijenili te informacije na OS/400. U informacije koje možete objaviti spadaju sistem (sistemi i pisači), dijeljenja pisača, informacije korisnika i politike TCP/IP Kvaliteta usluga (kako bi dobili više informacija pogledajte “Objavljivanje” na stranici 33).

Ako nadređeno DN kojem se izdaju podaci ne postoji, Poslužitelj direktorija ga automatski kreira. Možda ste također instalirali druge OS/400 aplikacije koje izdaju informacije u LDAP direktorij. Osim toga, možete pozvati sučelje aplikativnog programa (API-ji) iz svojih vlastitih programa kako bi objavili druge tipove informacija na LDAP direktoriju.

Bilješka: Možete objaviti OS/400 informacije na poslužitelju direktorija koji se ne izvodi na OS/400 ako konfigurirate taj poslužitelj tako da koristi IBM shemu.

Kako bi konfigurirali svoj sistem tako da objavi OS/400 informacije u poslužitelj direktorija, poduzmite ove korake:

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

   Napomena:

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

   Bilješka: Za izdavanje OS/400 informacija poslužitelju direktorija korištenjem SSL-a ili Kerberos-a, prvo trebate konfigurirati poslužitelj da koristi odgovarajući protokol. Pogledajte “Kerberos provjera autentičnosti s Poslužiteljem direktorija” na stranici 41 kako bi dobili više informacija o SSL i Kerberos.
10. Ako vaš poslužitelj ne koristi default port, unesite ispravni broj porta u polju **Port**.
11. Kliknite **Provjeri** da osigurate da nadređeno DN postoji na poslužitelju i da je informacija o vezi ispravna. Ako staza direktorija ne postoji, pojavit će se dijalog iz kojega ju možete kreirati.

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

Bilješka: Možete također objaviti i5/OS informacije na poslužitelju direktorija koji je na drugoj platformi. Morate objaviti sistemske i korisničke informacije na poslužitelj direktorija koji koristi shemu koja je kompatibilna s IBM Poslužitelj direktorija shemom. Za više informacija o IBM shemi direktorija, pogledajte “Shema IBM Poslužitelja direktorija” na stranici 16.

API za izdavanje OS/400 informacija poslužitelju direktorija

Poslužitelj direktorija osigurava ugrađenu podršku za objavljivanje korisničkih i sistemskih informacija. Te stavke su ispisane na stranici **Poslužitelj direktorija** dijaloga **Svojstva** sistema. Možete koristiti konfiguraciju LDAP poslužitelja i izdavanje API za omogućavanje OS/400 programa koje pišete za izdavanje drugih tipova informacija. Ti tipovi informacija se onda pojavljuju i na stranici **Poslužitelj direktorija**. Poput korisnika i sistema i oni su početno onemogućeni i možete ih konfigurirati korištenjem iste procedure. Program koji dodaje podatke u LDAP direktorij se naziva izdavački agent. Tip informacije koji je objavljen kada se pojavi na stranici **Poslužitelj direktorija** se naziva ime agenta.

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

QgldChgDirSvrA
: Aplikacija koristi CSVR0500 format za inicijalno dodavanje imena agenta koje je označeno kao onemogućeni unos. Upute za korisnike aplikacije bi ih trebale uputiti da koriste iSeries Navigator kako bi išli na stranicu svojstva Poslužitelja direktorija i kako bi konfigurirali agent objavljivanja. Primjeri imena agenta su imena agenta sistema i korisnika koja su automatski dostupna na stranici **Poslužitelj direktorija**.

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

QgldPubDirObj
: Ovaj API upotrijebite za objavljivanje podataka.

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

Poglavlje 8. Rješavanje problema Poslužitelj direktorija

Nažalost, čak i pouzdani poslužitelji kao što je Poslužitelj direktorija ponekad imaju probleme. Kada vaš Poslužitelj direktorija ima probleme, sljedeće informacije vam mogu pomoći da utvrdite u čemu je problem i kako ga ispraviti.

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

"Nadgledanje grešaka i pristupa s dnevnikom poslova Poslužitelja direktorija" na stranici 152
Kada se pojavi greška na vašem Poslužitelju direktorija i želite više detalja, druga akcija koju možete poduzeti je pregledavanje QDIRSRV dnevnika posla.

"Upotreba TRCTCPAPP-a za pomoć u nalaženju problema" na stranici 152
Kod grešaka koje se ponavljaju, možete koristiti naredbu Prati TCP/IP aplikacije (TRCTCPAPP APP(*DIRSRV)) kako bi pratili greške.

"Upotreba opcije LDAP_OPT_DEBUG za praćenje grešaka" na stranici 153
Pratite probleme s klijentima koji koriste LDAP C API-je.

"Uobičajene greške na LDAP klijentu" na stranici 153
Poznavanje uzroka uobičajenih grešaka na LDAP klijentu vam može pomoći da riješite probleme sa svojim poslužiteljem.

Kako bi dobili dodatne informacije o uobičajenim Poslužitelj direktorija problemima, pogledajte Poslužitelj direktorija home stranicu (www.iseries.ibm.com/ldap).

Poslužitelj direktorija koristi nekoliko Structured Query Language (SQL) poslužitelja koji su iSeries QSQSRVR poslovi. Kad dođe do neke SQL greške, QDIRSRV dnevnik posla će obično sadržavati sljedeću poruku:

```
desila se SQL greška -1
```

U tim slučajevima će vas dnevnik posla QDIRSRV uputiti na dnevnike posla SQL poslužitelja. Međutim, u nekim slučajevima, QDIRSRV ne mora imati ovu poruku i uputu, čak i ako je neki SQL poslužitelj uzrokom problema. U tom slučaju je dobro da znate koje je poslove SQL poslužitelja pokrenuo poslužitelj, tako da znate u kojim QSQSRVR dnevnicima posla treba tražiti dodatne greške.

Kada se Poslužitelj direktorija normalno pokrene, on generira poruku koje je slična sljedećem:

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

  >> CALL PGM(QSYS/QGLDSVR)
     Posao 057448/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057340/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057448/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057166/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057279/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
Posao 057288/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Poslužitelj direktorija se je uspješno pokrenuo.
```

Poruke se odnose na QSQSRVR poslove koji su bili pokrenuti za poslužitelj. Broj poruka na vašem poslužitelju može biti drugačiji ovisno o konfiguraciji i broju QSQSRVR poslova koji su potrebni kako bi se ostvarilo pokretanje poslužitelja.

Na poslužiteljima direktorija **Baza podataka/Sufiksi** stranica Svojstava u iSeries Navigator specificirate ukupan broj SQL poslužitelja koji Poslužitelj direktorija koristi za operacije direktorija nakon pokretanja poslužitelja. Dodatni SQL poslužitelji su pokrenuti za replikaciju.

Nadgledanje grešaka i pristupa s dnevnikom poslova Poslužitelja direktorija

Pregledavanje dnevnika posla za vaš Poslužitelj direktorija vas može upozoriti na greške i pomoći vam da nadgledate pristupanje poslužitelju. Dnevnik posla sadrži:

- Poruke o operacijama poslužitelja i sve probleme unutar poslužitelja kao što su poslovi SQL poslužitelja ili neuspješne replikacije.
- Poruke koje se odnose na sigurnost, a koje odražavaju operacije klijenta kao što su krive lozinke.
- Poruke koje sadrže detalje o greškama klijenta kao što je nedostajanje potrebnih atributa.

Možda nećete željeti zapisivati greške klijenta ako ne ispravljate probleme klijenta. Zapisivanje grešaka klijenta možete kontrolirati na kartici **Općenita** svojstva Poslužitelja direktorija u iSeries Navigatoru.

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

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

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

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

Upotreba TRCTCPAPP-a za pomoć u nalaženju problema

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

Naredba Prati TCP/IP aplikaciju (TRCTCPAPP) s *DIRSRV opcijom se može koristiti na Poslužitelj direktorija kao pomoć u pronalaženju problema s klijentima ili aplikacijama.

Kako bi dobili detaljnije informacije o korištenjima TRCTCPAPP naredbe s LDAP kao i ograničenjima na potrebnim ovlaštenjima, pogledajte Opis naredbe TRCTCPAPP (Praćenje TCP/IP aplikacije).

Kako bi dobili općenite informacije o korištenju praćenja komunikacije, pogledajte Praćenje komunikacije.

Upotreba opcije LDAP_OPT_DEBUG za praćenje grešaka

Možete koristiti LDAP_OPT_DEBUG opciju **ldap_set_option()** API-ja kako bi pratili probleme s klijentima koji koriste LDAP C API-je. Debug opcija ima višestruke razine debug postavki koje možete koristiti kao pomoć u uklanjanju problema s ovim aplikacijama.

Sljedeće je primjer omogućavanja klijentske debug opcije praćenja.

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

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

Primjer omogućavanja praćenja klijenta korištenjem LDAP_DEBUG varijable okruženja je slijedeći:

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

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

```
DMPUSRTRC    ClientJobNumber
```

gdje je ClientJobNumber broj posla klijenta.

Za interaktivni prikaz ovih informacija, upišite sljedeće u iSeries prompt:

```
DSPPFM  QAPOZDMP  QP0Znnnnnn
```

gdje QAP0ZDMP sadrži nulu, a nnnnnn je broj posla.

Da sačuvate ove informacije za njihovo slanje servisu, poduzmite sljedeće korake:

1. Kreirajte SAVF datoteku koristeći naredbu kreiranje SAVF (CRTSAVF).
2. Upišite sljedeće u iSeries prompt za naredbe.

   ```
   SAVOBJ  OBJ(QAP0ZDMP  LIB(QTEMP)  DEV(*SAVF)  SAVF(xxx)
   ```

   gdje QAP0ZDMP sadrži nulu, a *xxx* je ime koje ste specificirali za SAVF datoteku.

Uobičajene greške na LDAP klijentu

Poznavanje uzroka uobičajenih grešaka na LDAP klijentu vam može pomoći da riješite probleme sa svojim poslužiteljem. Kako bi dobili potpuni popis stanja greške LDAP klijenta, pogledajte poglavlje "API-ji poslužitelja direktorija" pod Programiranje u iSeries Informacijski Centar.

Poruke o greškama na klijentu imaju slijedeći format:

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

Bilješka: Objašnjenje ovih grešaka pretpostavlja da klijent komunicira s LDAP poslužiteljem na i5/OS. Klijent koji s poslužiteljem komunicira na nekoj drugoj platformi može dobiti slične poruke o greškama ali će uzroci i rješenja najvjerojatnije biti drugačiji.

Uobičajene greške obuhvaćaju sljedeće:

- "ldap_search: Vremensko ograničenje prekoračeno" na stranici 154
- "[Neuspjela LDAP operacija]: Greška operacija" na stranici 154

- “ldap_bind: Nema takvog objekta”
- “ldap_bind: Neodgovarajuća provjera identiteta”
- “[Neuspjela LDAP operacija]: Nedostatan pristup”
- “[neuspjela LDAP operacija]: Ne mogu kontaktirati LDAP poslužitelj”
- “[neuspjela LDAP operacija]: Neuspjelo povezivanja na SSL poslužitelj” na stranici 155

ldap_search: Vremensko ograničenje prekoračeno

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

- Povećajte ograničenje vremena pretraživanja za Poslužitelj direktorija. Pogledajte “Podešavanje postavki izvedbe” na stranici 101 kako bi dobili informacije o tome kako se to čini.
- Smanjite aktivnost na vašem sistemu. Možete i smanjiti broj aktivnih poslova LDAP klijenta koji se izvode.

[Neuspjela LDAP operacija]: Greška operacija

Ovu grešku može generirati nekoliko stvari. Kako bi dobili informacije o uzroku te greške za određenu instancu, pogledajte QDIRSRV dnevnika posla (kako je to opisano u “Nadgledanje grešaka i pristupa s dnevnikom poslova Poslužitelja direktorija” na stranici 152) i dnevnike posla Structured Query Language (SQL) poslužitelja (kako je to opisano u Poglavlje 8, “Rješavanje problema Poslužitelj direktorija”, na stranici 151).

ldap_bind: Nema takvog objekta

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

Kako bi dobili detalje o greški, pogledajte QDIRSRV dnevnik posla kako je to opisano u “Nadgledanje grešaka i pristupa s dnevnikom poslova Poslužitelja direktorija” na stranici 152.

ldap_bind: Neodgovarajuća provjera identiteta

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

- Unos koji nema userpassword atribut
- Unos koji predstavlja i5/OS korisnika, koji ima atribut UID i nema atribut userpassword. Ovo uzrokuje da se usporedba radi između specificirane lozinke i lozinke i5/OS korisnika, koje se ne podudaraju.
- Unos koji predstavlja projiciranog korisnika i način povezivanja različit od zahtijevanog.

Ova greška se obično pojavi kad klijent pokušava povezivanje s lozinkom koja nije valjana. Za dobivanje detalja o grešci, pogledajte QDIRSRV dnevnik posla kao što je opisano u“Nadgledanje grešaka i pristupa s dnevnikom poslova Poslužitelja direktorija” na stranici 152.

[Neuspjela LDAP operacija]: Nedostatan pristup

Ova se greška obično pojavi kad DN koji se povezuje nema ovlaštenje za izvođenje operacije (kao što je dodavanje ili brisanje) koju zahtijeva klijent. Ako želite vidjeti pojedinosti o greški, pogledajte dnevnik posla QDIRSRV kako je opisano u “Nadgledanje grešaka i pristupa s dnevnikom poslova Poslužitelja direktorija” na stranici 152.

[neuspjela LDAP operacija]: Ne mogu kontaktirati LDAP poslužitelj

Najuobičajeniji uzroci ove greške obuhvaćaju sljedeće:

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

Ako želite vidjeti pojedinosti o greški, pogledajte dnevnik posla QDIRSRV kako je opisano u “Nadgledanje grešaka i pristupa s dnevnikom poslova Poslužitelja direktorija” na stranici 152. Ako je Poslužitelj direktorija uspješno pokrenut, poruka da je Poslužitelj direktorija uspješno pokrenut će biti u QDIRSRV dnevniku posla.

[neuspjela LDAP operacija]: Neuspjelo povezivanja na SSL poslužitelj

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

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

Za i5/OS C aplikacije dostupne su dodatne informacije o SSL greški. Pogledajte “Poslužitelj direktorija API-ji” u poglavlju Programiranje kako bi dobili više detalja.

Poglavlje 9. Upute

Pogledajte sljedeće za dodatne referentne informacije.

- “Pomoćni programi reda za naredbe”
- “LDAP format razmjene podataka (LDIF)” na stranici 182
- “Shema konfiguracije Poslužitelja direktorija” na stranici 184

Pomoćni programi reda za naredbe

Ovaj dio opisuje pomoćne programe koje mogu biti izvedene iz okoline naredbe Qshell na i5/OS. Pogledajte sljedeće naredbe za dodatne informacije:

- “ldapmodify i ldapadd”
- “ldapdelete” na stranici 160
- “ldapexop” na stranici 162
- “ldapmodrdn” na stranici 166
- “ldapsearch” na stranici 169
- “ldapchangepwd” na stranici 177
- “ldapdiff” na stranici 178
- “Napomene o upotrebi SSL-a s LDAP pomoćnim programima reda za naredbe” na stranici 181

Primijetite da neki nizovi moraju biti okruženi navodnicima kako bi se ispravno obradili u okolini Qshell naredbe. To se u pravilu odnosi na nizove koji su DN-ovi, filtere pretraživanja i popise atributa koje će vratiti ldapsearch. Kao primjere, pogledajte slijedeći popis.

- Nizovi koji sadržavaju razmake: "cn=John Smith,cn=users"
- Nizovi koji sadržavaju zamjenske znakove: "*"
- Nizovi koji sadržavaju zagrade: "(objectclass=person)"

Za više informacija o okolini Qshell naredbe, pogledajte poglavlje “Qshell”.

ldapmodify i ldapadd

Alati LDAP modificiraj-unos i LDAP dodaj-unos

Sinopsis

```
ldapmodify [-a] [-b] [-c] [-C charset] [-d debuglevel][-D binddn][-i file]
[-h ldaphost] [-k] [-K keyfile] [-m mechanism] [-M] [-N certificatename]
[-O maxhops] [-p ldapport] [-P keyfilepw] [-r] [-R] [-v] [-V]
[-w passwd | ?] [-Z]


ldapadd [-a] [-b] [-c] [-C charset] [-d debuglevel][-D binddn][-i file]
[-h ldaphost] [-k] [-K keyfile] [-m mechanism] [-M] [-N certificatename]
[-O maxhops] [-p ldapport] [-P keyfilepw] [-r] [-R] [-v] [-V] [-w passwd | ?]
[-Z]
```

Opis

ldapmodify je sučelje reda za naredbe na ldap_modify, ldap_add, ldap_delete i ldap_modrdn sučelju aplikativnog programiranja (API-ji). **ldapadd** je implementiran kao preimenovana verzija ldapmodify. Kada je dozvan ldapadd, **-a** (dodaj novi unos) oznaka se automatski postavlja.

ldapmodify otvara veze s LDAP poslužiteljem i povezuje se na poslužitelj. Možete koristiti **ldapmodify** kako bi modificirali ili dodali unose. Informacije unosa se čitaju iz standardnog unosa ili iz datoteke upotrebom **-i** opcije.

Kako bi prikazali pomoć sintakse za **ldapmodify** ili **ldapadd**, upišite

```
ldapmodify -?
```

ili

```
ldapadd -?
```

Opcije

-a Dodaj nove unose. Default akcija za **ldapmodify** je modificiranje postojećih unosa. Ako je dozvan kao **ldapadd**, ta oznaka je uvijek poznata.

-b Pretpostavimo da su sve vrijednosti koje počinju s `/' binarne vrijednosti i da je stvarna vrijednost u datoteci čija je staza specificirana umjesto vrijednosti.

-c Kontinuirani operativni način. Izvješteno je o greškama, no **ldapmodify** nastavlja s preinakama. U suprotnom je default akcija izlazak nakon izvještavanja o greški.

-C *charset*
Specificira da su nizovi dobavljeni kao ulaz u **ldapmodify** i **ldapadd** pomoćnim programima predstavljeni u lokalnom skupu znakova kako je to specificirano skupom znakova i mora se konvertirati u UTF-8. Koristite **-C** *charset* opciju ako se kodna stranica ulaznog niza razlikuje od vrijednosti kodne stranice posla. Pogledajte ldap_set_iconv_local_charset() API-je kako bi vidjeli podržane vrijednosti skupa znakova.

-d *debuglevel*
Postavite razinu LDAP otkrivanja grešaka na debuglevel.

-D*binddn*
Upotrijebite ***binddn*** za povezivanje na LDAP direktorij. ***binddn*** je niz-predstavljeno DN.

-h*ldaphost*
Specificirajte zamjenski host na kojem se izvodi ldap poslužitelj.

-i *file* Čita podatke o modifikaciji sloga iz LDIF datoteke umjesto iz standardnog ulaza. Ako LDIF datoteka nije navedena, morate koristiti standardne ulazne podatke kad određujete slogove za ažuriranje u LDIF formatu.

-k Specificira korištenje kontrole administracije poslužitelja.

-K*keyfile*
Specificirajte ime SSL datoteke ključeva baze podataka s default proširenjem **kdb**. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva. Ako nije specificirano ime datoteke baze podataka ključeva, taj pomoćni program će prvo tražiti prisutnost SSL_KEYRING varijable okoline s pridruženim imenom datoteke. Ako nije definirana SSL_KEYRING varijabla okoline, koristit će se sistemska datoteka prstena ključeva, ako postoji.

Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-m *mehanizam*
Koristite ***mechanism*** kako bi specificirali SASL mehanizam koji će se koristiti za vezivanje na poslužitelj. Koristi se ldap_sasl_bind_s() API. **-m** parametar se zanemaruje ako je postavljeno **-V 2**. Ako **-m** nije naveden, koristi se jednostavna provjera identiteta. Valjani mehanizmi su:

- CRAM-MD5 - štiti lozinku koja je poslana na poslužitelja.
- EXTERNAL - koristi SSL certifikat. Traži -Z.
- GSSAPI - koristi korisničke Kerberos vjerodajnice

-M Upravljajte referal objektima kao pravilnim unosima.

-N*certificatename*

Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti potreban. ***certificatename*** nije potrebno ako je par certifikat/privatni ključ označen kao default za datoteku baze podatka ključa. Slično, ***certificatename*** nije potreban ako je jednostruk par certifikat/privatan ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-O *maxhops*

Specificirajte ***maxhops*** kako bi postavili maksimalan broj skokova koje poduzima knjižnica klijenta kada traži referale. Default broj skokova je 10.

-p *ldapport*

Specificirajte zamjenski TCP port na kojem osluškuje ldap poslužitelj. Default LDAP port je 389. Ako nije specificirano **-p**, a specificirano je **-Z**, koristi se default LDAP SSL port 636.

-P*keyfilepw*

Određuje lozinku baze ključeva. Ta lozinka je potrebna kako bi se pristupilo šifriranim informacijama u datoteci baze podataka ključa, a to bi moglo uključivati jedan ili više privatnih ključeva. Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključa, lozinka se dobiva od datoteke skrivene lozinke, a **-P** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

-r Zamijeni postojeće vrijednosti po defaultu.

-R Određuje da se preporuke ne slijede automatski.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-V Specificira LDAP verziju koju koristi **ldapmodify** kada se povezuje na LDAP poslužitelj. Po defaultu, uspostavlja se LDAP V3 veza. Kako bi izričito izabrali LDAP V3, specificirajte **-V 3**. Specificirajte **-V 2** kako bi ga izvodili kao LDAP V2 aplikaciju.

-w *passwd* **| ?**

Koristite ***passwd*** kao lozinku za provjeru ovlaštenja. Koristite ? kako bi generirali prompt lozinke.

-Z Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

Format ulaza

Sadržaj datoteke (ili standardni ulaz ako nema **-i** oznake na redu za naredbe) bi se trebao prilagoditi LDIF formatu. Pogledajte “LDAP format razmjene podataka (LDIF)” na stranici 182 kako bi dobili više informacija o LDIF formatu.

Primjeri

Pod pretpostavkom da postoji datoteka /tmp/entrymods i da ima slijedeći sadržaj:

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

naredba:

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

će zamijeniti sadržaje unosa Modificiraj mene atributa pošte s vrijednosti modme@student.of.life.edu, dodati naslov Grand Poobah i sadržaje datoteke /tmp/modme.jpeg kao jpegPhoto i u potpunosti ukloniti atribut opisa. Te iste modifikacije se mogu izvoditi korištenjem starijeg ldapmodify formata ulaza:

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

i naredba:

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

Pod pretpostavkom da postoji datoteka /tmp/newentry i da ima sljedeće sadržaje:

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

naredba:

```
 ldapadd -i /tmp/entrymods
```

dodaje novi unos za John Doe, korištenjem vrijednosti iz datoteke /tmp/newentry.

Opaske

Ako informacija unosa nije dobavljena iz datoteke korištenjem **-i** opcije, **ldapmodify** naredba će čekati da pročita unose iz standardnog ulaza.

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

ldapdelete

Alat LDAP obriši-unos

Sinopsis

```
ldapdelete [-c] [-C charset] [-d debuglevel][-D binddn][-i file]
[-h ldaphost] [-k] [-K keyfile] [-m mechanism] [-M] [-n] [-N certificatename]
[-O maxops] [-p ldapport] [-P keyfilepw] [-R] [-s][-v] [-V version]
[-w passwd | ?] [-Z] [dn]...
```

Opis

ldapdelete je sučelje reda za naredbe na ldap_delete sučelju aplikativnog programiranja (API).

ldapdelete otvara vezu na LDAP poslužitelj, veže i briše jedan ili više unosa. Ako je dobavljen jedan ili više argumenata Razlikovnog imena (DN), brišu se unosi s tim DN-ovima. Svaki DN je niz-predstavljeni DN. Ako su dobavljeni DN argumenti, čita se lista DN-ova iz standardnog ulaza ili iz datoteke ako se koristi **-i** oznaka.

Kako bi prikazali pomoć sintakse za **ldapdelete**, upišite:

```
ldapdelete -?
```

Opcije

-c Kontinuirani operativni način. Izvještava se o greškama, ali **ldapdelete** nastavlja s preinakama. U suprotnom je default akcija da se izađe nakon izvještaja o greški.

-C *charset*
Specificira da su DN-ovi dobavljeni kao ulaz u **ldapdelete** pomoćni program, predstavljeni u lokalnom skupu znakova, kako je to specificirano s charset. Koristite **-C** *charset* opciju ako se kodna stranica ulaznog niza razlikuje od vrijednosti kodne stranice posla. Pogledajte ldap_set_iconv_local_charset() API-je kako bi vidjeli podržane vrijednosti skupa znakova.

-d *debuglevel*
Postavite razinu LDAP otkrivanja grešaka na debuglevel.

-D*binddn*
Upotrijebite ***binddn*** za povezivanje na LDAP direktorij. ***binddn*** je niz-predstavljeno DN.

-h*ldaphost*
Određuje alternativni host na kojemu radi LDAP poslužitelj.

-i *file* Čita serije linija iz datoteke izvodeći LDAP brisanje za svaku liniju u datoteci. Svaka linija u datoteci bi trebala sadržavati jedno razlikovno ime.

-k Specificira korištenje kontrole administracije poslužitelja.

-K*keyfile*
Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva.

Ako pomoćni program ne može locirati bazu ključeva, koristiti će čvrsto kodirani skup default povjerljivih korijena izdavača certifikata. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori.

Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-m *mehanizam*
Koristite ***mechanism*** kako bi specificirali SASL mehanizam koji će se koristiti za vezivanje na poslužitelj. **-m** parametar se zanemaruje ako je postavljeno **-V 2**. Ako **-m** nije naveden, koristi se jednostavna provjera identiteta.

-M Upravljajte referal objektima kao pravilnim unosima.

-n Prikazuje što bi se napravilo, ali ne modificira stvarno unose. Korisno za analizu u spoju s **-v**.

-N*certificatename*
Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti potreban. ***certificatename*** nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, ***certificatename*** nije potreban ako je jednostruk par certifikat/privatan ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-O *maxhops*
Specificirajte ***maxhops*** kako bi postavili maksimalan broj skokova koje poduzima knjižnica klijenta kada traži referale. Default broj skokova je 10.

-p *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje LDAP poslužitelj. Default LDAP port je 389. Ako nije specificirano **-p**, a specificirano je **-Z**, koristi se default LDAP SSL port 636.

-P*keyfilepw*
Određuje lozinku baze ključeva. Ta lozinka je potrebna za pristup do šifriranih informacija u datoteci baze podataka ključeva koji mogu uključivati jedan ili više privatnih ključeva. Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključa, lozinka se dobiva od datoteke skrivene lozinke, a **-P** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

-R Određuje da se preporuke ne slijede automatski.

-s Koristite tu opciju kako bi obrisali podstablo koje ima korijen na specificiranom unosu.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-V Specificira LDAP verziju koju koristi **ldapdelete** kada se povezuje na LDAP poslužitelj. Po defaultu, uspostavlja se LDAP V3 veza. Kako bi izričito izabrali LDAP V3, specificirajte **-V 3**. Specificirajte **-V 2** kako bi ga izvodili kao LDAP V2 aplikaciju.

-w *passwd* **| ?**
Koristite ***passwd*** kao lozinku za provjeru ovlaštenja. Koristite ? kako bi generirali prompt lozinke.

-Z Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

dn Specificira jedan ili više DN argumenata. Svako DN bi trebalo biti niz-predstavljeno DN.

Primjeri

Sljedeća naredba

```
ldapdelete -D cn=administrator -w secret "cn=Delete Me, o=University of Life, c=US"
```

pokušava obrisati unos koji je imenovan sa zajedničkim imenom ″Delete Me″ točno ispod University of Life unosa organizacije.

Opaske

Ako nisu dobavljeni DN argumenti, **ldapdelete** naredbe čekaju da pročitaju popis DN-ova iz standardnog ulaza.

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

ldapexop

Alat LDAP proširene operacije

Sinopsis

```
ldapexop [-C charset] [-d debuglevel][-D binddn][-e] [-h ldaphost]
[-help][-K keyfile] [-m mechanism] [-N certificatename]
[-p ldapport] [-P keyfilepw] [-?] [-v] [-w passwd | ?] [-Z]
-op {cascrepl | controlqueue | controlrepl |
quiesce | readconfig}
```

Opis

Pomoćni program **ldapexop** je sučelje reda za naredbe koje osigurava sposobnost za vezanje na poslužitelj direktorija i izdaje jednu proširenu operaciju zajedno s podacima koji čine vrijednost proširene operacije.

Pomoćni program **ldapexop** podržava standardni host, port, SSL i opcije provjere autentičnosti koje koriste svi pomoćni programi LDAP klijenta. Osim toga, definiran je skup opcija kako bi se specificirala operacija koja će se izvoditi i argumenti za svaku proširenu operaciju

Kako bi prikazali pomoć sintakse za **ldapexop**, upišite:

```
ldapexop -?
```

ili

```
ldapexop -help
```

Opcije

Opcije za ldapexop naredbu se dijele u dvije kategorije:

1. Općenite opcije koje specificiraju kako se treba spojiti na poslužitelj direktorija. Te opcije moraju biti specificirane prije opcija koje su specifične za operaciju.
2. Opcija proširene operacije koja identificira proširenu operaciju koja će se izvoditi.

Općenite opcije

Te opcije specificiraju metode povezivanja na poslužitelj i moraju biti specificirane prije **-op** opcije.

-C *charset*
: Specificira da su DN-ovi dobavljeni kao ulaz u **ldapexop** pomoćni program, predstavljeni u lokalnom skupu znakova, kako je to specificirano s charset. Koristite **-C** *charset* opciju ako se kodna stranica ulaznog niza razlikuje od vrijednosti kodne stranice posla. Pogledajte ldap_set_iconv_local_charset() API-je kako bi vidjeli podržane vrijednosti skupa znakova.

-d *debuglevel*
: Postavite razinu LDAP otkrivanja grešaka na debuglevel.

-D*binddn*
: Upotrijebite ***binddn*** za povezivanje na LDAP direktorij. ***binddn*** je niz-predstavljeno DN.

-e
: Prikazuje informacije o verziji LDAP knjižnice i nakon toga izlazi.

-h*ldaphost*
: Određuje alternativni host na kojemu radi LDAP poslužitelj.

-help
: Prikazuje sintaksu naredbe i informacije o upotrebljivosti.

-K*keyfile*
: Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva.

  Ako pomoćni program ne može pronaći bazu podataka ključa, koristi se sistemska baza podataka ključa. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori.

  Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-m *mehanizam*
: Koristite ***mechanism*** kako bi specificirali SASL mehanizam koji će se koristiti za vezivanje na poslužitelj. Koristiti će se ldap_sasl_bind_s() API. **-m** parametar se zanemaruje ako je postavljeno **-V 2**. Ako **-m** nije naveden, koristi se jednostavna provjera identiteta.

-N*certificatename*
: Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti

potreban. ***certificatename*** nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, ***certificatename*** nije potreban ako je jednostruk par certifikat/privatan ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-p *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje LDAP poslužitelj. Default LDAP port je 389. Ako nije specificirano **-p**, a specificirano je **-Z**, koristi se default LDAP SSL port 636.

-P*keyfilepw*
Određuje lozinku baze ključeva. Ta lozinka je potrebna za pristup do šifriranih informacija u datoteci baze podataka ključeva koji mogu uključivati jedan ili više privatnih ključeva. Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključa, lozinka se dobiva od datoteke skrivene lozinke, a **-P** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

-? Prikazuje sintaksu naredbe i informacije o upotrebljivosti.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-w *passwd* **| ?**
Koristite ***passwd*** kao lozinku za provjeru ovlaštenja. Koristite ? kako bi generirali prompt lozinke.

-Z Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

Opcija proširenih operacija

Opcija **-op** extended-op identificira proširene operacije koje će se izvoditi. Proširena operacija može biti jedna od slijedećih vrijednosti:

- **cascrepl**: kaskadna proširena operacija kontrole replikacije. Tražena akcija se odnosi na specificirani poslužitelj i propušta se svim replikama danog podstabla. Ako su bilo koje od tih replike prosljeđivanja, one propuštaju proširene operacije do njihovih replika. Operacija je kaskadna nad cijelom topologijom replikacije.

  -action quiesce | unquiesce | replnow | wait
  To je potreban atribut koji specificira akciju koja će se izvoditi.

  quiesce
  Nisu dozvoljena daljnja ažuriranja, osim od strane replikacije.

  unquiesce
  Nastavlja se s normalnom operacijom, prihvaćena su ažuriranja klijenta.

  replnow
  Replicira sve promjene u redu na sve replika poslužitelje čim je to moguće, bez obzira na raspored.

  wait Čeka da se sva ažuriranja repliciraju na sve replike.

  -rc *contextDn*
  To je potreban atribut koji specificira korijen podstabla.

  -timeout *secs*
  To je neobavezan atribut koji, ako je prisutan, specificira timeout period u sekundama. Ako nije prisutan ili je 0, operacija čeka neodređeno dugo.

  Primjer:

  ```
  ldapexop -op cascrepl -action -quiesce -rc "o=acme,c=us" -timeout 60
  ```

- **controlqueue**: proširena operacija replikacije kontrolnog reda. Ta operacija vam omogućava da obrišete ili uklonite promjene u stanju čekanja iz popisa promjena replikacije koje su se nagomilale i nisu se izvodile zbog kvarova replikacije. Ta operacija je korisna kada se podaci replike ručno popravljaju. Tu operaciju bi koristili kako bi preskočili izvođenje nekih nagomilanih kvarova.

-skip all | change-id
To je potreban atribut.
- **sve** označava preskakanje svih promjena u stanju čekanja za taj ugovor.
- **change-id** identificira jednu promjenu koja će se preskočiti. Ako poslužitelj trenutno ne replicira tu promjenu, zahtjev neće uspjeti.

-ra *agreementDn*
To je potreban atribut koji specificira DN ugovora replikacije.

Primjeri:
```
ldapexop -op controlqueue -skip all -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"

ldapexop -op controlqueue -skip 2185 -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"
```

- **controlrepl**: proširena operacija kontrole replikacije

-action suspend | resume | replnow
To je potreban atribut koji specificira akciju koja će se izvoditi.

-rc *contextDn* **| -ra** *agreementDn*
-rc *contextDn* je DN konteksta replikacije. Akcija se izvodi za sve ugovore za taj kontekst. **-ra** *agreementDn* je DN ugovora replikacije. Akcija se izvodi za specificirani ugovor replikacije.

Primjer:
```
ldapexop -op controlrepl -action suspend -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"
```

- **quiesce**: proširena operacija replikacije umirenog ili uznemirenog podstabla

-rc *contextDn*
To je potreban atribut koji specificira da li DN konteksta replikacije (podstablo) bude umiren ili uznemiren.

-end To je neobavezan atribut koji, ako je prisutan, specificira da se uznemiri podstablo. Ako nije specificiran, default je da se umiri podstablo.

Primjeri:
```
ldapexop -op quiesce -rc "o=acme,c=us"

ldapexop -op quiesce -end -rc "o=ibm,c=us"
```

- **readconfig**: ponovo čita proširene operacije datoteke konfiguracije

-scope entire | single<*DN unosa***><***attribute***>**
To je potreban atribut.
- **entire** označava da treba pročitati cijelu datoteku konfiguracije.
- **single** znači da treba pročitati jedan specificiran unos i atribut.

Primjeri:
```
ldapexop -op readconfig -scope entire

ldapexop -op readconfig -scope single "cn=configuration" ibm-slapdAdminPW
```

Bilješka: Sljedeći unosi označeni s:
- [1] odmah postaju učinkoviti
- [2] postaju učinkoviti na novim operacijama
- [3] postaju učinkoviti ako lozinka nije promijenjena (nije potrebno readconfig)

– [4] su podržani pomoćnim programom reda za naredbe na i5/OS, ali nisu podržani Poslužiteljem direktorija na i5/OS

```
cn=Configuration
ibm-slapdadmindn[2]
ibm-slapdadminpw[2, 3, 4]
ibm-slapderrorlog[1, 4]
ibm-slapdpwencryption[1]
ibm-slapdsizelimit[1]
ibm-slapdsysloglevel[1, 4]
ibm-slapdtimelimit[1]
cn=Front End, cn=Configuration
ibm-slapdaclcache[1]
ibm-slapdaclcachesize[1]
ibm-slapdentrycachesize[1]
ibm-slapdfiltercachebypasslimit[1]
ibm-slapdfiltercachesize[1]
ibm-slapdidletimeout[1]
cn=Event Notification, cn=Configuration
ibm-slapdmaxeventsperconnection[2]
ibm-slapdmaxeventstotal[2]
cn=Transaction, cn=Configuration
ibm-slapdmaxnumoftransactions[2]
ibm-slapdmaxoppertransaction[2]
ibm-slapdmaxtimelimitoftransactions[2]
cn=ConfigDB, cn=Config Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdreadonly[2]
cn=Directory, cn=RDBM Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdbulkloaderrors[1, 4]
ibm-slapdclierrors[1, 4]
ibm-slapdpagedresallownonadmin[2]
ibm-slapdpagedreslmt[2]
ibm-slapdpagesizelmt[2]
ibm-slapdreadonly[2]
ibm-slapdsortkeylimit[2]
ibm-slapdsortsrchallownonadmin[2]
ibm-slapdsuffix[2]
```

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

ldapmodrdn

Alat LDAP modificiraj-unos RDN

Sinopsis

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

Opis

ldapmodrdn je sučelje reda za naredbe na ldap_modrdn sučelje aplikativnog programiranja (API).

ldapmodrdn otvara vezu na LDAP poslužitelj, veže i modificira RDN unosa. Informacija unosa se čita iz standardnog ulaza korištenjem **- f** opcije ili iz para reda za naredbe dn i rdn.

Pogledajte “Razlikovna imena (DN-ovi)” na stranici 11 kako bi dobili informacije o RDN-ima (Relativna razlikovna imena) i DN-ima (Razlikovna imena).

Kako bi prikazali pomoć sintakse za **ldapmodrdn**, upišite:

```
ldapmodrdn -?
```

Opcije

-c Kontinuirani operativni način. Izvješteno je o greškama, no **ldapmodrdn** nastavlja s preinakama. U suprotnom je default akcija da se izađe nakon izvještaja o greški.

-C *charset*
Specificira da su nizovi dobavljeni kao ulaz na **ldapmodrdn** pomoćni program prikazani u lokalnom skupu znakova, kako je to specificirano s charset. Koristite **-C** *charset* opciju ako se kodna stranica ulaznog niza razlikuje od vrijednosti kodne stranice posla. Konzultirajte ldap_set_iconv_local_charset() API kako vidjeli podržane charset vrijednosti. Primijetite da su podržane vrijednosti za charset jednake vrijednostima podržanim za charset oznaku koja je neobavezno definirana u Verziji 1 LDIF datoteke.

-d *debuglevel*
Postavite razinu LDAP otkrivanja grešaka na debuglevel.

-D*binddn*
Upotrijebite ***binddn*** za povezivanje na LDAP direktorij. binddn bi trebao biti niz-predstavljeno DN.

-h*ldaphost*
Specificirajte zamjenski host na kojem se izvodi ldap poslužitelj.

-i *file* Pročitajte informacije o modifikaciji unosa iz datoteke umjesto iz standardnog ulaza ili reda za naredbe (specificiranjem rdn i newrdn). Standardni ulaz može biti dobavljen iz datoteke kao i (″< datoteke″).

-k Specificira korištenje kontrole administracije poslužitelja.

-K*keyfile*
Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva.

Ako pomoćni program ne može locirati bazu ključeva, koristiti će čvrsto kodirani skup default povjerljivih korijena izdavača certifikata. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori.

Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-m *mehanizam*
Koristite ***mechanism*** kako bi specificirali SASL mehanizam koji će se koristiti za vezivanje na poslužitelj. Koristi se ldap_sasl_bind_s() API. **-m** parametar se zanemaruje ako je postavljeno **-V 2**. Ako **-m** nije naveden, koristi se jednostavna provjera identiteta.

-M Upravljajte referal objektima kao pravilnim unosima.

-n Prikazuje što bi se napravilo, ali ne modificira stvarno unose. Korisno za analizu u spoju s **-v**.

-N*certificatename*
Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Primijetite da ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti, certifikat klijenta nije potreban. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti potreban. ***certificatename*** nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, ***certificatename*** nije potreban ako je jednostruk par certifikat/privatan ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-O*hopcount*
Specificirajte ***hopcount*** kako bi postavili maksimalan broj skokova knjižnice klijenta kada progoni referale. Default broj skokova je 10.

-p *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje ldap poslužitelj. Default LDAP port je 389. Ako nije specificiran, a specificirano je -Z, koristi se default LDAP SSL port 636.

-P*keyfilepw*
Određuje lozinku baze ključeva. Ta lozinka je potrebna kako bi se pristupilo šifriranim informacijama u datoteci baze podataka ključa (koja može sadržavati jedan ili više privatnih ključeva). Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključa, lozinka se dobiva od datoteke skrivene lozinke, a **-P** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

-r Uklonite stare RDN vrijednosti iz unosa. Default akcija je da se zadrže stare vrijednosti.

-R Određuje da se preporuke ne slijede automatski.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-V Specificira LDAP verziju koju koristi **ldapmodrdn** kada se povezuje na LDAP poslužitelj. Po defaultu, uspostavlja se LDAP V3 veza. Kako bi izričito izabrali LDAP V3, specificirajte **-V 3**. Specificirajte **-V 2** kako bi ga izvodili kao LDAP V2 aplikaciju. Aplikacija kao što je **ldapmodrdn** bira LDAP V3 kao preferirani protokol korištenjem ldap_init umjesto ldap_open.

-w *passwd* **| ?**
Koristite ***passwd*** kao lozinku za provjeru ovlaštenja. Koristite ? kako bi generirali prompt lozinke.

-Z Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

dn newrdn
Pogledajte slijedeći odlomak, “Format ulaza za dn newrdn”, kako bi dobili više informacija.

Format ulaza za dn newrdn

Ako su dani argumenti reda za naredbe *dn* i *newrdn*, *newrdn* zamjenjuje RDN unosa kojeg je specificirao DN, *dn*. U suprotnom, datoteka (ili standardan ulaz ako nema **- i** oznake) se sastoji od više od jednog unosa:

```
Razlikovno ime (DN)

Relativno razlikovno ime (RDN)
```

Kako bi se odvojio svaki par DN i RDN, može se koristiti jedna ili više praznih linija.

Primjeri

Pod pretpostavkom da datoteka /tmp/entrymods postoji i da ima sadržaj:

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

naredba:

```
ldapmodrdn -r -i /tmp/entrymods
```

mijenja RDN Modify Me unosa iz Modify Me u The New Me, a stari cn Modify Me se uklanja.

Opaske

Ako informacija o unosu nije dobavljena iz datoteke korištenjem **-i** opcije (ili iz para reda za naredbe *dn* i *rdn*), **ldapmodrdn** naredba čeka kako bi pročitala unose iz standardnog ulaza.

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

ldapsearch

Alat LDAP pretraživanja i primjer programa

Sinopsis

```
ldapsearch [-a deref] [-A] [-b searchbase] [-B] [-C charset] [-d debuglevel]
[-D binddn] [-F sep] [-h ldaphost] [-i file] [-K keyfile] [-l timelimit] [-L]
[-m mechanism] [-M] [-n] [-N certificatename][-o attr_type] [-O maxhops]
[-p ldapport] [-P keyfilepw] [-q pagesize]  [-R] [-s scope ] [-t] [-T seconds]
[-v] [-V version] [-w passwd | ?] [-z sizelimit] [-Z] filter [attrs...]
```

Opis

ldapsearch je sučelje reda za naredbe na ldap_search sučelje aplikativnog programiranja (API).

ldapsearch otvara vezu s LDAP poslužiteljem, povezuje i izvodi pretraživanja korištenjem filtera. Filter bi trebao biti u skladu s prikazom niza za LDAP filtere (pogledajte ldap_search u API-ji Poslužitelja direktorija kako bi dobili više informacija o filterima).

Ako **ldapsearch** pronađe jedan ili više unosa, dohvaćaju se atributi specificirani pomoću attr-ova i unosi i vrijednosti se ispisuju na standardan izlaz. Ako nijedan attr nije ispisan, vraćaju se svi atributi.

Kako bi prikazali pomoć sintakse za **ldapsearch**, upišite ldapsearch -?.

Opcije

-a deref
: Određuje kako se radi dereferenciranje pseudonima. deref bi trebao biti nešto od nikad, uvijek, pretraži ili pronađi da bi specificirao da se pseudonimi nikad ne dereferenciraju, da se uvijek deferenciraju, derefenciraju kod pretraživanja ili dereferenciraju samo kada se locira bazni objekt za pretraživanje. Default je da se pseudonimi nikad ne dereferenciraju.

-A
: Učitaj samo atribute (bez vrijednosti). Ovo je korisno kad samo želite pogledati je li neki atribut prisutan u nekom slogu, a ne zanima vas pojedinačna vrijednost.

-b searchbase
: Koristite searchbase kao početnu točku za pretraživanje umjesto defaulta. Ako **-b** nije specificirano, taj pomoćni program će ispitati LDAP_BASEDN varijablu okoline kako bi pronašao searchbase definiciju. Ako nije specificirano ni jedno ni drugo, default baza je postavljena na ″″.

-B
: Nemoj potisnuti prikaz ne-ASCII vrijednosti. To je korisno kada se radi s vrijednostima koje se pojavljuju u zamjenskim skupovima znakova kao što je ISO-8859.1. Tu opciju implicira **-L** opcija.

-C charset
: Specificira da su nizovi koji su dobavljeni kao ulaz za ldapsearch pomoćni program prikazani u lokalnom skupu znakova (kako je to specificirano s charset). Ulaz niza uključuje filter, DN vezanja i bazni DN. Slično tome, kada prikazuje podatke **ldapsearch** konvertira podatke koji su primljeni iz LDAP poslužitelja u specificirani skup znakova. Koristite **-C** *charset* opciju ako se kodna stranica ulaznog niza razlikuje od vrijednosti kodne stranice posla. Pogledajte ldap_set_iconv_local_charset() API-je kako bi vidjeli podržane vrijednosti skupa znakova. Isto tako, ako je specificirana **-C** opcija i **-L** opcija, za ulaz se pretpostavlja da se nalazi u specificiranom skupu znakova, ali izlaz iz **ldapsearch** se uvijek sačuva u svojem UTF-8 prikazu ili u baznom-64 kodiranom prikazu podataka kada se otkriju znakovi koji se ne mogu ispisati. To je tako jer standardne LDIF datoteke sadrže samo UTF-8 (ili bazni-64 kodirani UTF-8) prikaze podataka niza. Primijetite da su podržane vrijednosti za charset iste vrijednosti koje su podržane za charset oznaku koja je neobavezno definirana u verziji 1 LDIF datoteka.

-d debuglevel
Postavite razinu LDAP otkrivanja grešaka na debuglevel.

-D binddn
Koristite binddn kako bi se vezali na LDAP direktorij. binddn bi trebao biti niz-prikazani DN (pogledajte LDAP Razlikovna imena).

-e Prikažite informacije o verziji LDAP knjižnice i nakon toga izađite.

-F sep Koristite sep kao odjelitelje polja između imena atributa i vrijednosti. Default odjelitelj je `=', ako nije specificirana **-L** oznaka jer se u tom slučaju ta opcija zanemaruje.

-h ldaphost
Specificirajte zamjenski host na kojem se izvodi ldap poslužitelj.

-i file Čita sljedove linija iz datoteke i izvodi jedno LDAP pretraživanje za svaku liniju. U tom slučaju, filter koji je dan na redu za naredbe se tretira kao obrazac gdje se prvo pojavljivanje % zamjenjuje s linijom za datoteku. Ako je datoteka jedan ″-″ znak, onda se linije čitaju iz standardnog ulaza.

-K keyfile
Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva.

Ako pomoćni program ne može locirati bazu ključeva, koristiti će čvrsto kodirani skup default povjerljivih korijena izdavača certifikata. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori.

Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-l timelimit
Čeka do najviše timelimit sekundi kako bi se dovršilo pretraživanje.

-L Prikazuje rezultate traženja u LDIF formatu. Ta se opcija isto vraća na **-B** opciju i uzrokuje da se zanemari **-F** opcija.

-m mechanism
Koristite mechanism kako bi specificirali SASL mehanizam koji će se koristiti za vezanje na poslužitelj. Koristiti će se ldap_sasl_bind_s() API. **-m** parametar se zanemaruje ako je postavljeno **-V 2**. Ako **-m** nije naveden, koristi se jednostavna provjera identiteta.

-M Upravljajte referal objektima kao pravilnim unosima.

-n Prikazuje što bi se napravilo, ali ne modificira stvarno unose. Korisno za analizu u spoju s **-v**.

-N certificatename
Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva.

Bilješka: Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti potreban. *certificatename* nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, *certificatename* nije potreban ako je jednostruk certifikat/privatni par ključeva u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-o *attr_type*
Kako bi specificirali atribut koji će se koristiti za kriterij sortiranja rezultata pretraživanja, možete koristiti -o (poredak) parametar. Možete koristi više -o parametara kako bi detaljnije definirali poredak sortiranja. U

sljedećem primjeru, rezultati pretraživanja su prvo sortirani prezimenom (sn) a onda danim imenom, s time da se dano ime (givenname) sortira obrnutim poretkom (silazno) kako je specificirano minus znakom prefiksa (-):

```
-o sn -o -givenname
```

Stoga je sintaksa parametra sortiranja kako slijedi:

```
[-]<attribute name>[:<matching rule OID>]
```

gdje je

- attribute name ime atributa prema kojem želite sortirati.
- matching rule OID je neobavezan OID pravila podudaranja koje želite koristiti za sortiranje. OID atribut pravila podudaranja nije podržan od strane Poslužitelja direktorija, no drugi LDAP poslužitelji mogu podržavati taj atribut.
- Znak minusa (-) označava da rezultat mora biti sortiran u obrnutom poretku.
- Kritičnost je uvijek kritična.

Default ldapsearch operacija je da se ne sortiraju vraćeni rezultati.

-O maxhops

Specificirajte maxhops kako bi postavili maksimalan broj skokova knjižnice klijenta kada traži referale. Default broj skokova je 10.

-p ldapport

Specificirajte zamjenski TCP port na kojem osluškuje ldap poslužitelj. Default LDAP port je 389. Ako nije specificiran, a specificirano je -Z, koristi se default LDAP SSL port 636.

-P keyfilepw

Određuje lozinku baze ključeva. Ta lozinka je potrebna kako bi se pristupilo šifriranim informacijama u datoteci baze podataka ključa (koja može sadržavati jedan ili više privatnih ključeva). Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključa, lozinka se dobiva od datoteke skrivene lozinke, a **-P** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

-q *pagesize*

Kako bi specificirali podjelu rezultata u stranice možete koristiti dva parametra: -q (veličina stranice upita) i -T (vrijeme između pretraživanja u sekundama). U sljedećem primjeru, rezultati pretraživanja vraćaju stranicu (25 unosa) svakih 15 sekundi tako dugo dok se ne vrate svi rezultati za to pretraživanje. ldapsearch klijent rukuje svim nastavcima veze za svaki zahtjev podjele u stranice za vrijeme dok traje operacija pretraživanja.

Ti parametri mogu biti korisni kada klijent ima ograničene resurse ili kada je povezan preko veze s malom pojasnom širinom. Općenito, omogućava vam da kontrolirate brzinu kojem se podaci vraćaju iz zahtjeva za pretraživanjem. Umjesto da odjednom primite sve rezultate, možete dobivati po nekoliko unosa (stranicu). Osim toga, možete kontrolirati trajanje odgode između svakog zahtjeva za stranicom, dajući tako klijentu vremena da obradi rezultate.

```
 -q 25  -T 15
```

Ako je specificiran -v (opširno) parametar, ldapsearch nakon što se iz poslužitelja vrati svaka stranica unosa ispisuje koliko je unosa vraćeno do sada, na primjer, **Vraćeno je ukupno 30 unosa.**

Omogućeno je više -q parametara tako da možete specificirati različite veličine stranica za vrijeme trajanja jedne operacije pretraživanja. U sljedećem primjeru, prva stranica ima 15 unosa, druga stranica ima 20 unosa, a treći parametar završava operaciju rezultat/pretraživanje podijeljenu u stranice:

```
-q 15 -q 20 -q 0
```

U sljedećem primjeru, prva stranica ima 15 unosa, a sve druge stranice imaju 20 unosa nastavljajući sa zadnjom specificiranom **-q** vrijednosti dok se ne dovrši operacija pretraživanja:

```
-q 15 -q 20
```

Default ldapsearch operacija je da se vrate svi unosi u jednom zahtjevu. Nije napravljena nikakva podjela u stranice za default ldapsearch operaciju.

-R Određuje da se preporuke ne slijede automatski.

-s scope
Određuje raspon pretraživanja. scope bi trebao biti jedno od bazno, jedna ili pod kako bi se specificiralo pretraživanje baznog objekta, jedne-razine ili podstabla. Default je pod.

-t Piše učitane vrijednosti u skup privremenih datoteka. To je korisno kada se radi s ne-ASCII vrijednostima kao što je jpegPhoto ili audio.

-T *sekundi*
Vrijeme između pretraživanja (u sekundama). **-T** opcija je podržana samo kada je specificirana **-q** opcija.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-V Specificira LDAP verziju koju će koristiti ldapmodify kada se povezuje na LDAP poslužitelj. Po defaultu, uspostavlja se LDAP V3 veza. Kako bi izričito izabrali LDAP V3, specificirajte ″-V 3″. Specificirajte ″-V 2″ da se izvodi kao LDAP V2 aplikacija. Aplikacija kao što je ldapmodify bira LDAP V3 kao preferirani protokol korištenjem ldap_init umjesto ldap_open.

-w *passwd* **| ?**
Koristite ***passwd*** kao lozinku za provjeru ovlaštenja. Koristite ? kako bi generirali prompt lozinke. .

-z sizelimit
Ograničite rezultate pretraživanja na najviše sizelimit unosa. Time postaje moguće odrediti gornju granicu broja slogova koji se vraćaju kod operacije pretraživanja.

-Z Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

filter Specificira prikaz niza filtera koji će se primijeniti u pretraživanju. Jednostavni filteri mogu biti specificirani kao attributetype=attributevalue. Složeniji filteri su specificirani korištenjem bilježenja prefiksa u skladu sa sljedećim Backus Naur Form (BNF):

```
<filter> ::='('<filtercomp>')'
<filtercomp> ::= <and>|<or>|<not>|<simple>
<and> ::= '&' <filterlist>
<or> ::= '|' <filterlist>
<not> ::= '!' <filter>
<filterlist> ::= <filter>|<filter><filterlist>
<simple> ::= <attributetype><filtertype>
<attributevalue>
<filtertype> ::= '='|'~='|'<='|'>='
```

Konstrukt '~=' se koristi kako bi se specificiralo približno podudaranje. Prikaz za <*attributetype*> i

<*attributevalue*> su opisani u ″RFC 2252, LDAP V3 Definicije sintakse atributa″ . Osim toga, ako je filtertype '=' onda <*attributevalue*> može biti jedna * kako bi se omogućio test postojanja atributa ili može sadržavati tekst i zvjezdicu (*) pomiješano kako bi se omogućilo uspoređivanje niza.

Na primjer, filter ″mail=*″ pronalazi sve vrijednosti koje imaju atribut pošte. Filter ″mail=*@student.of.life.edu″ pronalazi sve unose koji imaju atribut pošte koji završava sa specificiranim nizom. Kada želite staviti zavjese u filter, izbjegnite ih sa znakom obrnuta kosa crta (\).

Bilješka: Filteru kao što je "cn=Bob *", gdje postoji razmak između Bob i zvjezdice (*), odgovara ″Bob Carter″ ali ne i ″Bobby Carter″ u IBM direktoriju. Razmak između ″Bob″ i zamjenskog znaka (*) utječe na rezultate pretraživanja koje koristi filtere.

Pogledajte ″RFC 2254, Prikaz niza LDAP Filtera pretraživanja″ kako bi dobili potpuniji opis dopustivih filtera.

Format izlaza

Ako je pronađen jedan ili više unosa, svaki unos se ispisuje na standardan izlaz u obliku:

```
Razlikovno ime (DN)

attributename=vrijednost

attributename=vrijednost

attributename=vrijednost

...
```

Višestruki upisi su razdvojeni jednim praznim retkom. Ako se **-F** opcija koristi kako bi se specificirao znak odjelitelj, on će se koristiti umjesto `=' znaka. Ako se koristi **-t** opcija, umjesto stvarne vrijednosti se koristi ime privremene datoteke. Ako je dana **-A** opcija, zapisuje se samo dio ″attributename″.

Primjeri

Sljedeća naredba:

```
ldapsearch "cn=john doe" cn telephoneNumber
```

izvodi pretraživanje podstabla (korištenjem default baze pretraživanja) za unose sa zajedničkim imenom (commonName) ″john doe″. Dohvaćaju se commonName i telephoneNumber vrijednosti i ispisuju se na standardan izlaz. Ispis bi mogao izgledati približno ovako ako se pronađu dva unosa:

```
  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
```

Naredba:

```
ldapsearch -t "uid=jed" jpegPhoto audio
```

izvodi pretraživanje podstabla korištenjem default baze pretraživanja za unose s id-om korisnika ″jed″. Dohvaćaju se vrijednosti jpegPhoto i audio i zapisuju se u privremene datoteke. Izlaz bi mogao izgledati slično ovome ako se pronađe jedan unos s jednom vrijednosti za svaki od traženih atributa:

```
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
```

Naredba:

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

izvodi pretraživanje jedne razine na c=US razini za sve organizacije čije ime organizacije (organizationName) počinje s university. Rezultati pretraživanja su prikazani u LDIF formatu (pogledajte LDAP Format razmjene podataka). Dohvatit će se vrijednosti atributa organizationName i description i ispisat će se na standardnom izlazu, a to će rezultirati izlazom koji je sličan ovome:

```
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


...
```

Naredba:

```
ldapsearch -b "c=US" -o ibm-slapdDN "objectclass=person" ibm-slapdDN
```

izvodi pretraživanje na razini podstabla na c=US razini za sve osobe. Kada se taj posebni atribut (ibm-slapdDN) koristi za sortirana pretraživanja, on sortira rezultate pretraživanja znakovnim prikazom Razlikovnog imena (DN). Izlaz bi mogao izgledati slično ovom:

```
cn=Al Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US

cn=Al Garcia,ou=Home Entertainment,ou=Austin,o=IBM,c=US

cn=Amy Nguyen,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Arthur Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US

cn=Becky Garcia,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Ben Catu,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Ben Garcia Jr,ou=Home Entertainment,ou=Austin,o=IBM,c=US

cn=Bill Keller Jr.,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Bob Campbell,ou=In Flight Systems,ou=Austin,o=IBM,c=US
```

Naredba:

```
ldapsearch –h hostname –o sn –b "o=ibm,c=us" "title=engineer"
```

vraća sve unose u IBM direktoriju zaposlenika koji imaju titulu inženjera (engineer), s tim da su rezultati sortirani prema prezimenu.

Naredba:

```
ldapsearch –h hostname –o -sn –o cn –b "o=ibm,c=us" "title=engineer"
```

vraća sve unose u IBM direktoriju zaposlenika koji imaju titulu inženjera (engineer), s tim da su rezultati sortirani prema prezimenu (u silaznom poretku), a onda i prema imenu (u uzlaznom poretku).

Naredba:

```
ldapsearch –h hostname –q 5 –T 3 –b o=ibm,c=us "title=engineer"
```

vraća pet unosa po stranici, s tim da postoji odgoda od 3 sekunde između stranica za sve unose u IBM direktoriju zaposlenika koji imaju titulu inženjera (engineer).

Ovaj primjer pokazuje pretraživanja u kojima je uključen i referalni objekt. Kako je to objašnjeno u “Referali LDAP direktorija” na stranici 39, Poslužitelj direktorija LDAP direktoriji mogu sadržavati referalne objekte, pod uvjetom da oni sadržavaju jedno od sljedećeg:

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

Pretpostavimo da ’System_A’ sadrži unos referala:

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

Svi atributi koji su pridruženi unosu bi trebali prebivati na ’System_B’.

System_B sadrži slog:

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

Kada klijent izdaje zahtjev na ’System_A’, LDAP poslužitelj na System_A odgovara klijentu s URL-om:

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

Klijent koristi te informacije kako bi izdao zahtjev na System_B. Ako unos na System_A sadrži atribute kao dodatak za dn, objectclass i ref, poslužitelj zanemaruje te atribute (ako ne specificirate **-R** oznaku koja označava da ne treba loviti referale).

Kad klijent primi referalni odgovor iz poslužitelja, on ponovo izdaje zahtjev, ali ovaj puta poslužitelju na koga se odnosi vraćena adresa URL. Novi zahtjev ima isti opseg kao i originalni zahtjev. Rezultati ovog pretraživanja su različiti ovisno o vrijednosti koju navedete za raspon pretraživanja (**-b**).

Ako ste specificirali -s base kao što je to ovdje prikazano:

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

pretraživanje vraća sve atribute za sve unose sa ’sn=Jensen’ koji prebivaju u ’ou=Rochester, o=Big Company, c=US’ na System_A i System_B.

Ako navedete -s sub, kako je prikazano ovdje:

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

pretraživanje vraća sve atribute za sve unose sa ’sn=Jensen’ koji prebivaju u ili ispod ’ou=Rochester, o=Big Company, c=US’ na System_A i System_B.

Ako navedete -s one, kako je prikazano ovdje:

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

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

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

Klijent na to šalje zahtjev:

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

To isto tako ne daje nikakve rezultate, jer unos

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
```

prebiva na

```
ou=Rochester, o=Big Company, c=US
```

Pretraživanje s -s one pokušava pronaći unose u razini koja je neposredno ispod

```
ou=Rochester, o=Big Company, c=US
```

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

ldapchangepwd

Alat LDAP modificiranja lozinke.

Sinopsis

```
ldapchangepwd -D binddn -w passwd | ? -n newpassword | ?
[-C charset] [-d debuglevel][-h ldaphost] [-K keyfile]
[-m mechanism] [-M]  [-N certificatename] [-O maxhops]
[-p ldapport] [-P keyfilepw]  [-R] [-v] [-V version]
[-Z] [-?]
```

Opis

Šalje zahtjev za modificiranjem lozinke na LDAP poslužitelj. Dopušta promjenu lozinke za unos direktorija.

Opcije

-C *charset*
: Specificira da su DN-ovi dobavljeni kao ulaz u **ldapdelete** pomoćni program, predstavljeni u lokalnom skupu znakova, kako je to specificirano s charset. Koristite **-C** *charset* opciju ako se kodna stranica ulaznog niza razlikuje od vrijednosti kodne stranice posla. Pogledajte ldap_set_iconv_local_charset() API-je kako bi vidjeli podržane vrijednosti skupa znakova.

-d *debuglevel*
: Postavite razinu LDAP otkrivanja grešaka na debuglevel.

-D*binddn*
: Upotrijebite ***binddn*** za povezivanje na LDAP direktorij. ***binddn*** je niz-predstavljeno DN.

-h*ldaphost*
: Specificirajte zamjenski host na kojem se izvodi ldap poslužitelj.

-K*keyfile*
: Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva.

  Ako pomoćni program ne može locirati bazu ključeva, koristiti će čvrsto kodirani skup default povjerljivih korijena izdavača certifikata. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori.

  Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-m *mehanizam*
: Koristite ***mechanism*** kako bi specificirali SASL mehanizam koji će se koristiti za vezivanje na poslužitelj. Koristiti će se ldap_sasl_bind_s() API. **-m** parametar se zanemaruje ako je postavljeno **-V 2**. Ako **-m** nije naveden, koristi se jednostavna provjera identiteta.

-M
: Upravljajte referal objektima kao pravilnim unosima.

-n *newpassword* **| ?**
: Specificira novu lozinku. Koristite ? kako bi generirali prompt lozinke.

-N*certificatename*
: Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti potreban. ***certificatename*** nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, ***certificatename*** nije potreban ako je jednostruk par certifikat/privatan ključ u odredišnoj datoteci baze

podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-O *maxhops*
Specificirajte ***maxhops*** kako bi postavili maksimalan broj skokova koje poduzima knjižnica klijenta kada traži referale. Default broj skokova je 10.

-p *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje ldap poslužitelj. Default LDAP port je 389. Ako nije specificirano **-p**, a specificirano je **-Z**, koristi se default LDAP SSL port 636.

-P*keyfilepw*
Određuje lozinku baze ključeva. Ta lozinka je potrebna za pristup do šifriranih informacija u datoteci baze podataka ključeva koji mogu uključivati jedan ili više privatnih ključeva. Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključa, lozinka se dobiva od datoteke skrivene lozinke, a **-P** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

-R Određuje da se preporuke ne slijede automatski.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-V *version*
Specificira LDAP verziju koju koristi **ldapdchangepwd** kada se povezuje na LDAP poslužitelj. Po defaultu, uspostavlja se LDAP V3 veza. Kako bi izričito izabrali LDAP V3, specificirajte **-V 3**. Specificirajte **-V 2** kako bi ga izvodili kao LDAP V2 aplikaciju. Aplikacija kao što je **ldapdchangepwd** bira LDAP V3 kao preferirani protokol korištenjem ldap_init umjesto ldap_open.

-w *passwd* **| ?**
Koristite ***passwd*** kao lozinku za provjeru ovlaštenja. Koristite ? kako bi generirali prompt lozinke.

-Z Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Za Poslužitelj direktorija na i5/OS, ako koristite -Z i ne koristite -K ili -N, biti će korišten certifikat pridružen ID-u aplikacije Klijent usluga direktorija.

-? Prikazuje sintaksnu pomoć za ldapchangepwd.

Primjeri

Sljedeća naredba

```
ldapchangepwd -D cn=John Doe -w a1b2c3d4 -n wxyz9876
```

mijenja lozinku za unos koji ima commonName ″John Doe″ s a1b2c3d4 u wxyz9876

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

ldapdiff

Alat LDAP usklađivanja replike.

Bilješka: Ta naredba bi se mogla izvoditi duže vrijeme ovisno o broju unosa (i atributa za te unose) koji se repliciraju.

Sinopsis

(Uspoređuje i usklađuje unose podataka između dva poslužitelja unutar okoline replikacije.)

```
ldapdiff -b baseDN -sh host -ch host [-a] [-C countnumber]
 [-cD dn] [-cK keyStore] [-cw password] -[cN keyLabel]
 [-cp port] [-cP keyStorePwd]  [-cZ] [-F] [-L filename] [-sD dn] [-sK keyStore]
 [-sw password] -[sN keyLabel] [-sp port] [-sP keyStorePwd]
 [-sZ] [-v]
```

ili

(Uspoređuje shemu između dva poslužitelja.)

```
 ldapdiff -S -sh host -ch host [-a] [-C countnumber][-cD dn]
 [-cK keyStore] [-cw password] -[cN keyLabel] [-cp port]
 [-cP keyStorePwd] [-cZ] [-L filename] [-sD dn]
 [-sK keyStore] [-sw password] [-sN keyLabel] [-sp port]
 [-sP keyStorePwd] [-sZ] [-v]
```

Opis

Taj alat usklađuje replika poslužitelj s njegovim glavnim poslužiteljem. Kako bi prikazali pomoć sintakse za **ldapdiff**, upišite:

```
ldapdiff -?
```

Opcije

Sljedeće opcije se odnose na **ldapdiff** naredbu. Postoje dvije podgrupe koje se točno određeno odnose na poslužitelja dobavljača ili poslužitelja potrošača.

-a Specificira korištenje kontrole administracije poslužitelja za pisanja na repliku samo za čitanje.

-b *baseDN*
Koristite searchbase kao početnu točku za pretraživanje umjesto defaulta. Ako **-b** nije specificirano, taj pomoćni program će ispitati LDAP_BASEDN varijablu okoline kako bi pronašao searchbase definiciju.

-C *countnumber*
Broji koliko unosa treba popraviti. Alat postoji ako je pronađeno više od specificiranog broja nepodudarnosti.

-F To je opcija popravka. Ako je specificirana, sadržaj replike potrošača se modificira kako bi se podudarao sa sadržajem dobavljača. To se ne može koristiti ako je specificirano i **-S**.

-L Ako nije specificirana **-F** opcija, koristite ovu opciju kako bi generirali LDIF datoteku za izlaz. LDIF datoteka se može koristiti kako bi se ažurirao potrošač tako da se uklone razlike.

-S Specificira uspoređivanje sheme na oba poslužitelja.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

Opcije za dobavljača replikacije

Sljedeće opcije se odnose na poslužitelj potrošača i označene su s početnim ’s’ u imenu opcije.

-sD *dn* Koristite ***dn*** za povezivanje na LDAP direktorij. ***dn*** je niz-predstavljeno DN.

-sh *host*
Specificira ime hosta.

-sK *keyStore*
Specificirajte ime SSL datoteke ključeva baze podataka s default proširenjem **kdb**. Ako taj parametar nije specificiran ili je vrijednost prazan niz (-sK″″), koristi se sistemski keystore. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva.

-sN *keyLabel*
Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je oznaka specificirana bez da je specificirano keystore, oznaka je identifikator aplikacije u Upravitelju digitalnih certifikata (DCM). Default oznaka (id aplikacije) je QIBM_GLD_DIRSRV_CLIENT. Ako je LDAP poslužitelj konfiguriran tako da

izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, potreban je certifikat klijenta. ***keyLabel*** nije potrebno ako je bio označen default par certifikat/privatni ključ. Slično tome, ***keyLabel*** nije potreban ako je jednostruk par certifikat/privatni ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-sZ** niti **-sK**.

-sp *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje ldap poslužitelj. Default LDAP port je 389. Ako nije specificirano **-sp**, a specificirano je **-sZ**, koristi se default LDAP SSL port 636.

-sP *keyStorePwd*
Određuje lozinku baze ključeva. Ta lozinka je potrebna za pristup do šifriranih informacija u datoteci baze podataka ključeva koji mogu uključivati jedan ili više privatnih ključeva. Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključeva, lozinka se dobiva od datoteke skrivene lozinke, a **-sP** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-sZ** niti **-sK**. Lozinka se ne koristi ako postoji skrivena datoteka koje se koristi za keystore.

-st *trustStoreType*
Specificirajte oznaku koja je pridružena certifikatu klijenta u pouzdanoj datoteci baze podataka. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti potreban. ***trustStoreType*** nije potreban ako je kao default određen par certifikat/privatni ključ. Slično tome, ***trustStoreType*** nije potreban ako je jednostruk certifikat/privatni par ključeva u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-sZ** niti **-sT**.

-sZ Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem.

Opcije za potrošača replikacije

Sljedeće opcije se odnose na poslužitelja potrošača i označene su s početnim 'c' u imenu opcije. Radi prikladnosti, ako je -cZ specificirano bez da se specificiraju vrijednosti za -cK, -cN ili -cP, te opcije koriste istu vrijednost koja je specificirana za SSL opcije dobavljača. Kako bi nadjačali opcije dobavljača i koristili default postavke, specificirajte -cK ″″ -cN ″″ -cP ″″.

-cD *dn* Koristite ***dn*** za povezivanje na LDAP direktorij. ***dn*** je niz-predstavljeno DN.

-ch *host*
Specificira ime hosta.

-cK *keyStore*
Specificirajte ime SSL datoteke baze podataka ključa s default proširenjem kdb. Ako je vrijednost prazan niz (-sK″″), koristi se sistemski keystore. Ako datoteka baze podataka ključeva nije u trenutnom direktoriju, navedite puno ime datoteke baze ključeva.

-cN *keyLabel*
Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je oznaka specificirana bez da je specificirano keystore, oznaka je identifikator aplikacije u Upravitelju digitalnih certifikata (DCM). Default oznaka (id aplikacije) je QIBM_GLD_DIRSRV_CLIENT. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, potreban je certifikat klijenta. ***keyLabel*** nije potrebno ako je bio označen default par certifikat/privatni ključ. Slično tome, ***keyLabel*** nije potreban ako je jednostruk par certifikat/privatni ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-cZ** niti **-cK**.

-cp *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje ldap poslužitelj. Default LDAP port je 389. Ako nije specificirano **-cp**, a specificirano je **-cZ**, koristi se default LDAP SSL port 636.

-cP *keyStorePwd*
Određuje lozinku baze ključeva. Ta lozinka je potrebna za pristup do šifriranih informacija u datoteci baze

podataka ključeva koji mogu uključivati jedan ili više privatnih ključeva. Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključeva, lozinka se dobiva od datoteke skrivene lozinke, a **-cP** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-cZ** niti **-cK**.

-cw *password* **| ?**
Koristite ***password*** kao lozinku za provjeru autentičnosti. Koristite ? kako bi generirali prompt lozinke.

-cZ Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem.

Primjeri

```
ldapdiff -b <baseDN> -sh <supplierhostname> -ch <consumerhostname> [options]
```

ili

```
ldapdiff -S  -sh <supplierhostname> -ch <consumerhostname> [options]
```

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

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

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

"Sloj sigurnih utičnica (SSL) i Sigurnost sloja transporta s Poslužiteljem direktorija" na stranici 41 raspravlja o upotrebi SSL-a s Poslužitelj direktorija LDAP poslužiteljem. Ove informacije uključuju upravljanje i kreiranje povjerljivih Izdavača certifikata s Upraviteljem digitalnih certifikata.

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

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

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

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

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

LDAP format razmjene podataka (LDIF)

Ova dokumentacija opisuje LDAP format razmjene podataka (LDIF), kao što ga koriste ldapmodify, ldapsearch i ldapadd pomoćni programi. LDIF koji je ovdje specificiran je podržan od strane pomoćnih programa poslužitelja dobavljenih s IBM direktorija.

LDIF se koristi kako bi prikazao LDAP unose u obliku teksta. Osnovni oblik LDIF unosa je:

```
dn: <distinguished name>
<attrtype> : <attrvalue>
<attrtype> : <attrvalue>
...
```

Linija se može nastaviti tako da se započne sljedeća linija s jednim razmakom ili tabulatorom, na primjer:

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

Više vrijednosti atributa je specificirano na odijeljenim linijama, na primjer:

```
cn: John E Doe
cn: John Doe
```

Ako <*attrvalue*> sadrži ne-US-ASCII znak ili počinje s razmakom ili dvotočkom ':', iza <*attrtype*> slijedi dvostruka dvotočka, a vrijednost je kodirana u baznoj-64 notaciji. Na primjer, vrijednost ″ begins with a space″ bi bila ovako kodirana:

```
cn:: IGJlZ2lucyB3aXRoIGEgc3BhY2U=
```

Više unosa unutar iste LDIF datoteke je odijeljeno praznom linijom. Višestruke prazne linije se smatraju logičkim krajem-datoteke.

Za više informacija, pogledajte sljedeće:

- "LDIF primjer"
- "Verzija 1 LDIF podrške" na stranici 183
- "Verzija 1 LDIF primjeri" na stranici 183

LDIF primjer

Slijedi primjer LDIF datoteke koja sadrži tri unosa.

```
dn: cn=John E Doe, o=University of High
 er Learning, c=US
cn: John E Doe
cn: John Doe
objectclass: osoba
sn: Doe

dn: cn=Bjorn L Doe, o=University of High
 er Learning, c=US
cn: Bjorn L Doe
cn: Bjorn Doe
objectclass: osoba
sn: Doe

dn: cn=Jennifer K. Doe, o=University of High
 er Learning, c=US
cn: Jennifer K. Doe
cn: Jennifer Doe
objectclass: osoba
sn: Doe
```

```
jpegPhoto:: /9j/4AAQSkZJRgABAAAAAQABAAD/2wBDABALD
 A4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQ
 ERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARESEhgVG
...
```

jpegPhoto u unosu od Jennifer Jensen je kodiran s baznim-64 formatom. Vrijednosti tekstualnog atributa mogu isto biti specificirane u baznom-64 formatu. No, ako je to slučaj, bazno-64 kodiranje mora biti u kodnoj stranici formata žice za protokol (odnosno za LDAP V2, IA5 niz znakova, a za LDAP V3, UTF-8 kodiranje).

Verzija 1 LDIF podrške

Pomoćni programi klijenta (ldapmodify i ldapadd) su bili poboljšani kako bi prepoznali posljednju verziju LDIF-a, a ona se identificira prisutnošću oznake ″version: 1″ na početku datoteke. Za razliku od originalne verzije LDIF-a, novija verzija LDIF-a podržava vrijednosti atributa koje su prikazane u UTF-8 (umjesto vrlo ograničenog US-ASCII).

No, ručno kreiranje LDIF datoteke koja sadrži UTF-8 vrijednosti bi moglo biti problematično. Kako bi se pojednostavio taj proces, podržano je proširenje skupa znakova na LDIF formatu. To proširenje omogućava da ime IANA skupa znakova bude specificirano u zaglavlju LDIF datoteke (zajedno s brojem verzije). Podržan je ograničen skup IANA skupova znakova.

Verzija 1 LDIF formata podržava i URL-ove datoteke. Time se osigurava fleksibilniji način za definiranje specifikacija datoteke. URL-ovi datoteke imaju slijedeći oblik:

```
attribute:< file:///path          (gdje sintaksa staze ovisi o platformi)
```

Na primjer, slijede valjane Web adrese datoteke:

```
jpegphoto:< file:///d:\temp\photos\myphoto.jpg    (DOS/Windows stil staze)
jpegphoto:< file:///etc/temp/photos/myphoto.jpg   (Unix stil staze)
```

Bilješka: Pomoćni programi IBM direktorija podržavaju novu URL specifikaciju datoteke, ali i stariji stil (″jpegphoto: /etc/temp/myphoto″), bez obzira na specifikaciju verzije. Drugim riječima, novi URL format datoteke se može koristiti bez dodavanja oznake verzije na vaše LDIF datoteke.

Verzija 1 LDIF primjeri

Možete koristiti neobaveznu oznaku skupa znakova tako da pomoćni programi automatski konvertiraju iz specificiranog skupa znakova u UTF-8 kao u sljedećem primjeru:

```
version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, o=University of New Mexico, c=US
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd
title: Associate Dean
title: [title in Spanish]
jpegPhoto:> file:///usr/local/photos/jgriego.jpg
```

U ovom se slučaju sve vrijednosti koje slijede ime atributa i jednu dvotočku prevode iz ISO-8859-1 skupa znakova u UTF-8. Vrijednosti koje slijede ime atributa i dvostruku dvotočku (kao što je description:: V2hhdCBhIGNhcm...) moraju biti bazno-64 kodirani i očekuje se da budu binarni ili UTF-8 znakovni nizovi. Za vrijednosti koje su pročitane iz datoteke, kao što je jpegPhoto atribut specificiran Web adresom u prethodnom primjeru, se očekuju da budu binarne ili UTF-8. Ne provodi se nikakav prijevod iz specificiranog ″charset″ u UTF-8 na tim vrijednostima.

U ovom primjeru LDIF datoteke bez oznake skupa znakova se očekuje da će sadržaj biti u UTF-8, baznom-64 kodiranom UTF-8 ili baznim-64 kodiranim binarnim podacima:

```
# IBM Directorysample LDIF datoteka
 #
 # Sufiks "o=IBM, c=US" bi se trebao definirati prije pokušaja učitavanja
 # tih podataka.
```

```
version: 1

dn: o=IBM, c=US
objectclass: top
objectclass: organization
o: IBM

dn: ou=Austin, o=IBM, c=US
ou: Austin
objectclass: organizationalUnit
seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

Ta ista datoteka bi se mogla koristiti bez verzije: 1 informacije zaglavlja, u prethodnim izdanjima IBM direktorija:

```
# IBM Directorysample LDIF datoteka
#
# Sufiks "o=IBM, c=US" bi se trebao definirati prije pokušaja učitavanja
# tih podataka.

dn: o=IBM, c=US
objectclass: top
objectclass: organization
o: IBM

dn: ou=Austin, o=IBM, c=US
ou: Austin
objectclass: organizationalUnit
seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

Bilješka: Vrijednosti tekstualnog atributa se mogu specificirati u baznom-64 formatu.

Shema konfiguracije Poslužitelja direktorija

Ove informacije opisuju Stablo informacija direktorija (DIT) i atribute koji se koriste za konfiguriranje ibmslapd.conf datoteke. U prethodnim izdanjima su postavke konfiguracije direktorija pohranjene u formatu vlasnika u datoteci konfiguracije. Postavke direktorija su sada pohranjene korištenjem LDIF formata u datoteci konfiguracije.

Datoteka konfiguracije se naziva ibmslapd.conf. Sada je dostupna i shema koju koristi datoteka konfiguracije. Tipovi atributa se mogu pronaći u v3.config.at datoteci, a klase objekta se nalaze u v3.config.oc datoteci. Atributi se mogu preinačiti korištenjem ldapmodify naredbe. Za više informacija o ldapmodify naredbi, pogledajte “ldapmodify i ldapadd” na stranici 157.

- “Stablo informacija direktorija”
- “Atributi” na stranici 193

Stablo informacija direktorija

cn=Configuration

- cn=Admin
- cn=Event Notification
- cn=Front End
- cn=Kerberos
- cn=Master Server
- cn=Referral
- cn=Schema
  - cn=IBM Directory
    - cn=Config Backends
      - cn=ConfigDB

- cn=RDBM Backends
  - cn=Directory
  - cn=ChangeLog
- cn=LDCF Backends
  - cn=SchemaDB

- cn=SSL
  - cn=CRL
- cn=Transaction

cn=Configuration

DN cn=Configuration

Opis To je unos najviše razine u DIT-u konfiguracije. Sadrži podatke koji su od globalnog interesa za poslužitelja, iako u stvari sadrži i svakovrsne stavke. Svaki atribut u tom unosu dolazi iz prve sekcije (globalna strofa) od ibmslapd.conf.

Broj 1 (potrebno)

Klasa objekta
ibm-slapdTop

Obavezni atributi

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

Neobavezni atributi

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (Depricirano)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion

cn=Admin

DN cn=Admin, cn=Configuration

Opis Globalne postavke konfiguracije za IBM Admin demon

Broj 1 (potrebno)

Klasa objekta
ibm-slapdAdmin

Obavezni atributi

- cn
- ibm-slapdErrorLog
- ibm-slapdPort

Neobavezni atributi

- ibm-slapdSecurePort

cn=Event Notification

DN cn=Event Notification, cn=Configuration

Opis Globalne postavke obavještavanja o događaju za Poslužitelj direktorija

Broj 0 ili 1 (neobavezno; potrebno samo ako želite omogućiti obavještavanje o događaju)

Klasa objekta
ibm-slapdEventNotification

Obavezni atributi

- cn
- ibm-slapdEnableEventNotification
- objectClass

Neobavezni atributi

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

cn=Front End

DN cn=Front End, cn=Configuration

Opis Globalne postavke okoline koje poslužitelj primjenjuje kod pokretanja.

Broj 0 ili 1 (neobavezno)

Klasa objekta
ibm-slapdFrontEnd

Obavezni atributi

- cn
- objectClass

Neobavezni atributi

- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdDB2CP
- ibm-slapdEntryCacheSize
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdPlugin
- ibm-slapdSetenv
- ibm-slapdIdleTimeOut

cn=Kerberos

DN cn=Kerberos, cn=Configuration

Opis Globalne postavke Kerberos provjere autentičnosti za Poslužitelj direktorija.

Broj 0 ili 1 (neobavezno)

Klasa objekta
ibm-slapdKerberos

Obavezni atributi

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

Neobavezni atributi

- Nijedan

cn=Master Server

DN cn=Master Server, cn=Configuration

Opis Kada konfigurirate repliku, taj unos sadrži vjerodajnice vezanja i referal URL glavnog poslužitelja.

Broj 0 ili 1 (neobavezno)

Klasa objekta
ibm-slapdReplication

Obavezni atributi

- cn
- ibm-slapdMasterPW (Obavezno ako se ne koristi Kerberos provjera autentičnosti.)

Neobavezni atributi

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Neobavezno ako se koristi Kerberos provjera autentičnosti.)
- ibm-slapdMasterReferral
- objectClass

cn=Referral

DN cn=Referral, cn=Configuration

Opis Taj unos sadrži sve unose referala iz prve sekcije (globalna strofa) od ibmslapd.conf. Ako ne postoje referali (po defaultu ne postoji nijedan), taj unos je neobavezan.

Broj 0 ili 1 (neobavezno)

Klasa objekta
ibm-slapdReferral

Obavezni atributi

- cn
- ibm-slapdReferral
- objectClass

Neobavezni atributi

- Nijedan

cn=Schemas

DN cn=Schemas, cn=Configuration

Opis Taj unos služi kao spremnik za sheme. Taj unos nije stvarno potreban jer se sheme mogu razlikovati na temelju klase objekta ibm-slapdSchema. On je uključen kako bi se poboljšala čitljivost DIT-a.

Trenutno je dozvoljen samo jedan unos sheme: cn=IBM Directory.

Broj 1 (potrebno)

Klasa objekta
Spremnik

Obavezni atributi

- cn
- objectClass

Neobavezni atributi

- Nijedan

cn=IBM Directory

DN cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Taj unos sadrži sve podatke konfiguracije sheme iz prve sekcije (globalna strofa) od ibmslapd.conf. Služi i kao spremnik za sve pozadine koje koriste shemu. Višestruke sheme nisu trenutno podržane, ali da jesu, onda bi postojao samo jedan ibm-slapdSchema unos po shemi. Primijetite da se smatra da su višestruke sheme nekompatibilne. Stoga se pozadina može pridružiti samo jednoj shemi.

Broj 1 (potrebno)

Klasa objekta
ibm-slapdSchema

Obavezni atributi

- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

Neobavezni atributi

- ibm-slapdSchemaAdditions

cn=Config Backends

DN cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Taj unos služi kao spremnik za Config pozadine.

Broj 1 (potrebno)

Klasa objekta
Spremnik

Obavezni atributi

- cn
- objectClass

Neobavezni atributi
Nijedan

cn=ConfigDB

DN cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Pozadina konfiguracije za konfiguraciju IBM Poslužitelja direktorija

Broj 0 - n (neobavezno)

Klasa objekta
ibm-slapdConfigBackend

Obavezni atributi

- ibm-slapdSuffix
- ibm-slapdPlugin

Neobavezni atributi

- ibm-slapdReadOnly

cn=RDBM Backends

DN cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Ovaj unos služi kao spremnik za RDBM pozadine. On učinkovito zamjenjuje rdbm liniju baze podataka iz ibmslapd.conf identificiranjem svih podunosa kao DB2 pozadina. Taj unos nije stvarno potreban jer se RDBM pozadine mogu razlikovati pomoću klase objekta ibm-slapdRdbmBackend. On je uključen kako bi se poboljšala čitljivost DIT-a.

Broj 0 ili 1 (neobavezno)

Klasa objekta
Spremnik

Obavezni atributi

- cn
- objectClass

Neobavezni atributi

- Nijedan

cn=Directory

DN cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Taj unos sadrži sve postavke konfiguracije baze podataka za default pozadinu RDBM baze podataka.

Iako se mogu kreirati višestruke pozadine s proizvoljnim imenima, Administracija poslužitelja pretpostavlja da je ″cn=Directory″ pozadina glavnog direktorija i da je ″cn=Change Log″ neobavezna pozadina dnevnika promjene. Samo su sufiksi koji su prikazani u ″cn=Directory″ konfigurabilni pomoću Administracije poslužitelja (osim za sufiks changelog koji je postavljen transparentno omogućavanjem dnevnika promjena).

Broj 0 - n (neobavezno)

Klasa objekta
ibm-slapdRdbmBackend

Obavezni atributi

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Neobavezni atributi

- ibm-slapdBulkloadErrors

- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Bilješka: Ako koristite **ibm-slapdUseProcessIdPw**, morate modificirati shemu kako bi napravili **ibm-slapdDbUserPW** neobaveznim.

cn=Change Log

DN cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Taj unos sadrži sve postavke konfiguracije baze podataka za pozadinu dnevnika promjene.

Broj 0 - n (neobavezno)

Klasa objekta
ibm-slapdRdbmBackend

Obavezni atributi

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Neobavezni atributi

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly

- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Bilješka: Ako koristite **ibm-slapdUseProcessIdPw**, morate modificirati shemu kako bi napravili **ibm-slapdDbUserPW** neobaveznim.

cn=LDCF Backends

DN cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Taj unos služi kao spremnik za LDCF pozadinu. On učinkovito zamjenjuje ldcf liniju baze podataka iz ibmslapd.conf identificiranjem svih pod unosa kao LDCF pozadine. Taj unos nije stvarno potreban jer se LDCF pozadine mogu razlikovati pomoću ibm-slapdLdcfBackend klase objekta. On je uključen kako bi se poboljšala čitljivost DIT-a.

Broj 1 (potrebno)

Klasa objekta
Spremnik

Obavezni atributi

- cn
- objectClass

Neobavezni atributi

- ibm-slapdPlugin

cn=SchemaDB

DN cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Taj unos sadrži sve podatke konfiguracije baze podataka iz sekcije ldcf baze podataka ibmslapd.conf.

Broj 1 (potrebno)

Klasa objekta
ibm-slapdLdcfBackend

Obavezni atributi

- cn
- objectClass

Neobavezni atributi

- ibm-slapdPlugin
- ibm-slapdSuffix

cn=SSL

DN cn=SSL, cn=Configuration

Opis Globalne postavke SSL povezivanja za Poslužitelj direktorija.

Broj 0 ili 1 (neobavezno)

Klasa objekta
ibm-slapdSSL

Obavezni atributi

- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

Neobavezni atributi

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

  Bilješka: **ibm-slapdSslCipherSpecs** je sada uklonjen. Umjesto toga koristite **ibm-slapdSslCipherSpec**. Ako koristite **ibm-slapdSslCipherSpecs**, poslužitelj će se konvertirati na podržane atribute.
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW

cn=CRL

DN cn=CRL, cn=SSL, cn=Configuration

Opis Ovaj unos sadrži podatke popisa opoziva certifikata iz prve sekcije (globalna strofa) od ibmslapd.conf. To je potrebno samo ako je ″ibm-slapdSslAuth = serverclientauth″ u cn=SSL unosu, a certifikati klijenta su bili izdani za CRL provjeru valjanosti.

Broj 0 ili 1 (neobavezno)

Klasa objekta
ibm-slapdCRL

Obavezni atributi

- cn
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPort
- objectClass

Neobavezni atributi

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword

cn=Transaction

DN cn = Transaction, cn = Configuration

Opis Specificira globalne postavke podrške transakcije. Podrška transakcije je osigurana korištenjem plugin-a:

```
extendedop /QSYS.LIB/QGLDTRANEX.SRVPGM tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

Poslužitelj (**slapd**) automatski učitava taj plug-in kod pokretanja ako vrijedi **ibm-slapdTransactionEnable = TRUE**. Plug-in ne treba biti izričito dodan na **ibmslapd.conf**.

Broj 0 ili 1 (neobavezno; potrebno samo ako želite koristiti transakcije.)

Klasa objekta
ibm-slapdTransaction

Obavezni atributi

- cn

- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

Neobavezni atributi

- Nijedan

Atributi

- cn
- ibm-slapdACIMechanism
- ibm-slapdACLAccess
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConcurrentRW
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdEnableEventNotification
- ibm-slapdEntryCacheSize
- ibm-slapdErrorLog
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword
- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdMasterDN

- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplDbConns
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSuffix
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTransactionEnable
- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- objectClass

cn

Opis Ovo je X.500 commonName atribut koji sadrži ime objekta.

Sintaksa
Niz direktorija

Maksimalna dužina
256

Vrijednost
Više-vrijednosti

ibm-slapdACIMechanism

Opis Određuje kojeg ACL modela koristi poslužitelj. (Podržano samo na i5/OS od verzije v3.2, zanemareno od drugih platformi.)

- 1.3.18.0.2.26.1 = IBM SecureWay v3.1 ACL model
- 1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL model

Default
1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL model

Sintaksa
Niz direktorija

Maksimalna dužina
256

Vrijednost
Više-vrijednosti.

ibm-slapdACLAccess

Opis Kontrolira da li je omogućen pristup na ACL-ove. Ako je postavljeno na TRUE, omogućen je pristup na ACL-ove. Ako je postavljeno na FALSE, onemogućen je pristup na ACL-ove.

Default
TRUE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdACLCache

Opis Kontrolira da li ili ne poslužitelj stavlja u predmemoriju ACL informacije.

- Ako je postavljeno na TRUE, poslužitelj stavlja ACL informacije u predmemoriju.
- Ako je postavljeno na FALSE, poslužitelj ne stavlja ACL informacije u predmemoriju.

Default
TRUE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdACLCacheSize

Opis Maksimalan broj unosa koji će se sačuvati u ACL predmemoriji.

Default
25000

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdAdminDN

Opis DN vezanja administratora za Poslužitelj direktorija.

Default
cn=root

Sintaksa
DN

Maksimalna dužina
Neograničena

Vrijednost
Jedna-vrijednost

ibm-slapdAdminPW

Opis Lozinka vezanja administratora za Poslužitelja direktorija.

Default
tajna

Sintaksa
Binarno

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdBulkloadErrors

Opis Staza datoteke ili uređaj na ibmslapd host stroju na koje će se zapisati bulkload poruke o greški.

Default
/var/bulkload.log

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdChangeLogMaxEntries

Opis Taj atribut koristi changelog plug-in kako bi specificirao maksimalan broj changelog unosa koji su dozvoljeni u RDBM bazi podataka. Svaki changelog ima vlastiti changeLogMaxEntries atribut.

```
Minimum = 0 (neograničeno)
Maksimum = 2,147,483,647 (32-bit, cijeli broj s predznakom)
```

Default
0

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdCLIErrors

Opis Staza datoteke ili uređaj na ibmslapd host stroju na koje će se zapisati CLI poruke o greški.

Default
/var/db2cli.log

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdConcurrentRW

Opis Postavljanjem toga na TRUE se omogućava da se pretraživanja nastave istodobno s ažuriranjima. To omogućava 'prljava čitanja', odnosno, rezultate koji možda neće biti konzistentni s predanim stanjem baze podataka.

Upozorenje: Taj atribut se depricira.

Default
FALSE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdDB2CP

Opis Specificira kodnu stranicu baze podataka direktorija. 1208 je kodna stranica za UTF-8 baze podataka.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdDBAlias

Opis Zamjensko ime DB2 baze podataka.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
8

Vrijednost
Jedna-vrijednost

ibm-slapdDbConnections

Opis Specificirajte broj DB2 veza koje će poslužitelj namijeniti DB2 pozadini. Vrijednost mora biti između 5 & 50 (uključno).

Bilješka: ODBCCONS varijabla okoline nadjačava vrijednost te direktive.
Ako je ibm-slapdDbConnections (ili ODBCCONS) manji od 5 ili veći od 50, poslužitelj će koristiti 5 ili 50. 1 dodatna veza će biti kreirana za replikaciju (čak i ako nije definirana replikacija). 2 dodatne veze će se kreirati za dnevnik promjene (ako je promjena omogućena).

Default
15

Sintaksa
Cijeli broj

Maksimalna dužina
50

Vrijednost
Jedna-vrijednost

ibm-slapdDbInstance

Opis Specificira instancu DB2 baze podataka za tu pozadinu.

Default
ldapdb2

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
8

Vrijednost
Jedna-vrijednost

Bilješka: Svi ibm-slapdRdbmBackend objekti moraju koristiti isti ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW i DB2 skup znakova.

ibm-slapdDbLocation

Opis Staza datoteke sistema na kojoj je locirana baza podatka pozadine.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdDbName

Opis Specificira ime DB2 baze podataka za tu pozadinu.

Default
ldapdb2

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
8

Vrijednost
Jedna-vrijednost

ibm-slapdDbUserID

Opis Specificira ime korisnika s kojim se treba vezati na DB2 bazu podataka za tu pozadinu.

Default
ldapdb2

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
8

Vrijednost
Jedna-vrijednost

Bilješka: Svi ibm-slapdRdbmBackend objekti moraju koristiti isti ibm-slapdDbInstance ibm-slapdDbUserID, ibm-slapdDbUserPW i DB2 skup znakova.

ibm-slapdDbUserPW

Opis Specificira lozinku korisnika s kojom se treba vezati na DB2 bazu podataka za tu pozadinu. Ta lozinka može biti šifriran tekst ili imask.

Default
ldapdb2

Sintaksa
Binarno

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

Bilješka: Svi ibm-slapdRdbmBackend objekti moraju koristiti isti ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW i DB2 skup znakova.

ibm-slapdEnableEventNotification

Opis Specificira da li treba omogućiti Obavještavanje o događaju. Mora biti postavljeno na TRUE ili FALSE.

Ako je postavljeno na FALSE, poslužitelj odbija sve zahtjeve klijenta kako bi se registrirale obavijesti o događaju s proširenim rezultatom LDAP_UNWILLING_TO_PERFORM.

Default
TRUE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdEntryCacheSize

Opis Maksimalan broj unosa koji će se sačuvati u predmemoriji unosa.

Default
25000

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdErrorLog

Opis Specificira stazu datoteke ili uređaj na stroju Poslužitelja direktorija na kojeg se zapisuju poruke o greški.

Default
/var/ibmslapd.log

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdFilterCacheBypassLimit

Opis Filteri pretraživanja kod kojih se podudara više od tog broja unosa se neće dodati na predmemoriju Filtera pretraživanja. Budući je popis ID-ova unosa koji se podudaraju s tim filterom uključen u ovu predmemoriju, ta postavka pomaže kako bi se ograničilo korištenje memorije. Vrijednost 0 označava da nema granice.

Default
100

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdFilterCacheSize

Opis Specificira maksimalan broj unosa koji će se zadržati u Predmemoriji filtera pretraživanja.

Default
25000

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdIdleTimeOut

Opis Maksimalno vrijeme kroz koje će se LDAP veza držati otvorenom kada nema aktivnosti na vezi. Vrijeme mirovanja za LDAP vezu je vrijeme (u sekundama) između zadnje aktivnosti na vezi i trenutnog vremena. Ako je vrijeme veze isteklo, na temelju toga što je vrijeme mirovanja veće od vrijednosti tog atributa, LDAP poslužitelj će očistiti i završiti LDAP vezu i tako je napraviti dostupnom za druge dolazne zahtjeve.

Default
300

Sintaksa
Cijeli broj

Dužina
11

Brojanje
Jedan

Korištenje
Operacija direktorija

Modificiranje korisnika
Da

Klasa pristupa
Kritično

Potrebno
Ne

ibm-slapdIncludeSchema

Opis Specificira stazu direktorija na stroju Poslužitelja direktorija koji sadrži definicije sheme.

Default

/etc/V3.system.at
/etc/V3.system.oc
/etc/V3.config.at
/etc/V3.config.oc
/etc/V3.ibm.at
/etc/V3.ibm.oc
/etc/V3.user.at
/etc/V3.user.oc
/etc/V3.ldapsyntaxes
/etc/V3.matchingrules

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Više-vrijednosti

ibm-slapdKrbAdminDN

Opis Specificira Kerberos ID od LDAP administratora (na primjer, ibm-kn=admin1@realm1). Koristi se kada se koristi Kerberos provjera autentičnosti kako bi se provjerila autentičnost administratora kada je prijavljen na sučelje Administracija. To se može specificirati umjesto ili kao dodatak adminDN i adminPW.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdKrbEnable

Opis Specificira da li poslužitelj podržava Kerberos. Mora biti TRUE ili FALSE.

Default
TRUE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdKrbIdentityMap

Opis Specificira da li treba koristiti Kerberos mapiranje poduzeća. Mora biti postavljeno na TRUE ili FALSE. Ako je postavljeno na TRUE, kada je klijent ovlašten s Kerberos ID, poslužitelj traži sve lokalne korisnike s podudarajućim Kerberos vjerodajnicama i dodaje DN-ove tih korisnika na vjerodajnice vezanja veze. Time se omogućava da se ACL-ovi zasnovani na DN-ovima LDAP korisnika mogu koristiti s Kerberos.

Default
FALSE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdKrbKeyTab

Opis Specificira Kerberos datoteku tablice ključeva LDAP poslužitelja. Ta datoteka sadrži privatni ključ LDAP poslužitelja koji je pridružen njegovom Kerberos računu. Ta datoteka se treba zaštititi (kao datoteka baze podataka ključa SSL poslužitelja).

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdKrbRealm

Opis Specificira Kerberos područje LDAP poslužitelja. Koristi se za objavljivanje ldapservicename atributa u ishodišnom DSE. Primijetite da LDAP poslužitelj može služiti kao spremište informacija računa za više KDC-ova (i područja), no LDAP poslužitelj, kao poslužitelj pod utjecajem Kerberosa, može biti član samo jednog područja.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
256

Vrijednost
Jedna-vrijednost

ibm-slapdLdapCrlHost

Opis Specificira ime hosta LDAP poslužitelja koji sadrži Liste opoziva certifikata (CRL-ovi) za provjeru valjanosti x.509v3 certifikata klijenta. Taj parametar je potreban kada se ibm-slapdSslAuth=serverclientauth i certifikati klijenta izdaju za CRL provjeru valjanosti.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
256

Vrijednost
Jedna-vrijednost

ibm-slapdLdapCrlPassword

Opis Specificira lozinku koju SSL na strani poslužitelja koristi za vezanje na LDAP poslužitelj koji sadrži Liste opoziva certifikata (CRL-ovi) za provjeru valjanosti x.509v3 certifikata klijenta. Taj parametar bi mogao biti potreban kada se ibm-slapdSslAuth=serverclientauth i certifikati klijenta izdaju za CRL provjeru valjanosti.

Bilješka: Ako LDAP poslužitelj koji sadrži CRL-ove dopušta neovlaštene pristupe na CRL-ove (odnosno, anonimni pristup), onda nije potrebno ibm-slapdLdapCrlPassword.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Binarno

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdLdapCrlPort

Opis Specificira port koji će se koristiti za povezivanje na LDAP poslužitelj koji sadrži Listu opoziva certifikata (CRL-ovi) za provjeru valjanosti x.509v3 certifikata klijenta. Taj parametar je potreban kada se ibm-slapdSslAuth=serverclientauth i certifikati klijenta izdaju za CRL provjeru valjanosti. (IP portovi nisu označeni, 16-bitni cijeli brojevi u rasponu od 1 - 65535)

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdLdapCrlUser

Opis Specificira DN vezanja kojeg SL na strani poslužitelja koristi za vezanje na LDAP poslužitelj koji sadrži Liste opoziva certifikata (CRL-ovi) za provjeru valjanosti x.509v3 certifikata klijenta. Taj parametar bi mogao biti potreban kada se ibm-slapdSslAuth=serverclientauth i certifikati klijenta izdaju za CRL provjeru valjanosti.

Bilješka: Ako LDAP poslužitelj koji sadrži CRL-ove dopušta neovlaštene pristupe na CRL-ove (odnosno, anonimni pristup), onda nije potrebno ibm-slapdLdapCrlUser.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
DN

Maksimalna dužina
1000

Vrijednost
Jedna-vrijednost

ibm-slapdMasterDN

Opis Specificira DN vezanja glavnog poslužitelja. Vrijednost se mora podudarati s replicaBindDN u replicaObject definiranom za glavnog poslužitelja. Kada se Kerberos koristi za ovlaštenje na repliku, ibm-slapdMasterDN mora specificirati DN prikaz Kerberos ID-a (na primjer, ibm-kn=freddy@realm1). Kada se koristi Kerberos, zanemaruje se MasterServerPW.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
DN

Maksimalna dužina
1000

Vrijednost
Jedna-vrijednost

ibm-slapdMasterPW

Opis Specificira lozinku vezanja glavnog replika poslužitelja. Vrijednost se mora podudarati s replicaBindDN u replicaObject definiranom za glavnog poslužitelja. Kada se Kerberos koristi za ovlaštenje na repliku, ibm-slapdMasterDN mora specificirati DN prikaz Kerberos ID-a (na primjer, ibm-kn=freddy@realm1). Kada se koristi Kerberos, zanemaruje se MasterServerPW.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Binarno

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdMasterReferral

Opis Specificira URL glavnog replika poslužitelja. Na primjer:

```
ldap://master.us.ibm.com
```

Za sigurnost postavljenu samo na SSL:

```
ldaps://master.us.ibm.com:636
```

Za sigurnost postavljenu na ništa i korištenje nestandardnog porta:

```
ldap://master.us.ibm.com:1389
```

Default
ništa

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
256

Vrijednost
Jedna-vrijednost

ibm-slapdMaxEventsPerConnection

Opis Specificira maksimalan broj obavještavanja o događaju koja se mogu registrirati po vezi.

```
Minimum = 0 (neograničeno)
Maksimum = 2,147,483,647
```

Default
100

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdMaxEventsTotal

Opis Specificira maksimalan ukupan broj obavještavanja o događaju koja se mogu registrirati za sve veze.

```
Minimum = 0 (neograničeno)
Maksimum = 2,147,483,647
```

Default
0

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdMaxNumOfTransactions

Opis Specificira maksimalan broj transakcija po poslužitelju.

```
Minimum = 0 (neograničeno)
Maksimum = 2,147,483,647
```

Default
20

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdMaxOpPerTransaction

Opis Specificira maksimalan broj operacija po transakciji.

```
Minimum = 0 (neograničeno)
Maksimum = 2,147,483,647
```

Default
5

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdMaxPendingChangesDisplayed

Opis Maksimalan broj promjena u toku koje će se prikazati.

Default
200

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdMaxTimeLimitOfTransactions

Opis Specificira maksimalnu timeout vrijednost u sekundama za transakcije koje su u toku.

```
Minimum = 0 (neograničeno)
Maksimum = 2,147,483,647
```

Default
300

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdPagedResAllowNonAdmin

Opis Da li bi poslužitelj trebao ili ne, dozvoliti vezanje ne-Administratora za zahtjeve s rezultatima podijeljenim u stranice na zahtjevima pretraživanja. Ako je vrijednost pročitana s ibmslapd.conf datoteke FALSE, poslužitelj će obrađivati samo one zahtjeve klijenta koje je poslao na izvođenje korisnik s Administrator ovlaštenjem. Ako klijentovi rezultati zahtjeva podijeljeni u stranice za operaciju pretraživanja nemaju Administrator ovlaštenje, a vrijednost pročitana iz ibmslapd.conf datoteke za taj atribut je FALSE, poslužitelj će vratiti klijentu povratni kod insufficientAccessRights; neće se izvoditi pretraživanje ili podjela u stranice.

Default
FALSE

Sintaksa
Booleov

Dužina
5

Brojanje
Jedan

Korištenje
directoryOperation

Modificiranje korisnika
Da

Klasa pristupa
kritično

Klasa objekta
ibm-slapdRdbmBackend

Potrebno
Ne

ibm-slapdPagedResLmt

Opis Maksimalan broj istaknutih rezultata zahtjeva pretraživanja koji su podijeljeni u stranice koji mogu istovremeno biti aktivni. Raspon = 0.... Ako klijent zahtjeva operaciju s rezultatima podijeljenim u stranice, a trenutno je aktivan maksimalan broj istaknutih rezultata podijeljenih u stranice, onda će poslužitelj vratiti klijentu povratni kod busy; neće se izvoditi pretraživanje ili podjela u stranice.

Default
3

Sintaksa
Cijeli broj

Dužina
11

Brojanje
Jedan

Korištenje
directoryOperation

Modificiranje korisnika
Da

Klasa pristupa
kritično

Potrebno
Ne

Klasa objekta
ibm-slapdRdbmBackend

ibm-slapdPageSizeLmt

Opis Maksimalan broj unosa koji će se vratiti iz pretraživanja za jednu stranicu kada je specificirana kontrola rezultata podijeljenih u stranice, bez obzira na veličinu stranice koja bi mogla biti specificirana na zahtjevu pretraživanja klijenta. Raspon = 0.... Ako je klijent premašio veličinu stranice, onda će se koristiti manja vrijednosti od vrijednosti klijenta i vrijednosti pročitane iz ibmslapd.conf.

Default
50

Sintaksa
Cijeli broj

Dužina
11

Brojanje
Jedan

Korištenje
directoryOperation

Modificiranje korisnika
Da

Klasa pristupa
kritično

Potrebno
Ne

Klasa objekta
ibm-slapdRdbmBackend

ibm-slapdPlugin

Opis Plugin je dinamički učitana knjižnica koja proširuje sposobnosti poslužitelja. Atribut ibm-slapdPlugin specificira poslužitelju kako treba učitati i inicijalizirati plug-in knjižnicu. Sintaksa je:

```
ime datoteke ključne riječi init_function [args...]
```

Sintaksa se malo razlikuje za svaku platformu zbog konvencija imenovanja knjižnice.

Većina plug-inova je neobavezna, no plug-in RDBM pozadine je potreban za sve RDBM pozadine.

Default
baza podataka /bin/libback-rdbm.dll rdbm_backend_init

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
2000

Vrijednost
Više-vrijednosti

ibm-slapdPort

Opis Specificira TCP/IP port koji se koristi za ne-SSL veze. Ne može imati istu vrijednost kao i ibm-slapdSecurePort. (IP portovi nisu označeni, 16-bitni cijeli brojevi u rasponu 1 - 65535.)

Default
389

Sintaksa
Cijeli broj

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdPWEncryption

Opis Specificira mehanizam kodiranja za lozinke korisnika prije nego se pohrane u direktorij. Mora biti specificiran kao none, imask, crypt ili sha (morate koristiti ključnu riječ **sha** kako bi dobili SHA-1 kodiranje). Vrijednost mora biti postavljena na none kako bi uspjelo SASL cram-md5 vezanje.

Default
ništa

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdReadOnly

Opis Atribut se normalno odnosi samo na pozadinu Direktorija. Specificira da li se može zapisati pozadina. Mora biti specificiran kao TRUE ili FALSE. Ako nije specificiran, postavlja se na FALSE. Ako je postavljen na TRUE, poslužitelj vraća LDAP_UNWILLING_TO_PERFORM (0x35) kao odgovor na bilo koji zahtjev klijenta koji mijenja podatke u bazi podataka samo za čitanje.

Default
FALSE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdReferral

Opis Specificira LDAP URL referala koji će se vratiti onda kada se sa zahtjevom ne podudaraju lokalni sufiksi. Koristi se za superiorne referale (odnosno, sufiks nije unutar konteksta imenovanja poslužitelja).

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
32700

Vrijednost
Više-vrijednosti

ibm-slapdReplDbConns

Opis Maksimalan broj veza baze podataka koje može koristiti replikacija.

Default
4

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdReplicaSubtree

Opis Identificira DN repliciranog podstabla

Sintaksa
DN

Maksimalna dužina
1000

Vrijednost
Jedna-vrijednost

ibm-slapdSchemaAdditions

Opis Atribut ibm-slapdSchemaAdditions se koristi kako bi se izričito identificiralo koja datoteka sadrži unose nove sheme. To je po defaultu postavljeno da bude /etc/V3.modifiedschema. Ako taj atribut nije definiran, poslužitelj se vraća na korištenje posljednje ibm-slapdIncludeSchema datoteke u prethodnim izdanjima.

Prije verzije 3.2, posljednji includeSchema unos u **slapd.conf** je bila datoteka na koju su se svi novi unosi sheme dodavali od strane poslužitelja ako je primio i dodao zahtjev klijenta. U pravilu je posljednja includeSchema V3.modifiedschema datoteka koja je prazna datoteka koja je instalirana samo u tu svrhu.

Bilješka: Naziv modificirana krivo upućuje jer ona samo pohranjuje nove unose. Promjene na postojećim unosima sheme se izvode u njihovim originalnim datotekama.

Default
/etc/V3.modifiedschema

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdSchemaCheck

Opis Specificira mehanizam provjeravanja sheme za operacije dodaj/modificiraj/obriši. Mora biti specificiran kao V2, V3 ili V3_lenient.

- V2 - Zadržava v2 i v2.1 provjeravanje. Preporuča se u svrhu migriranja.
- V3 - Izvodi v3 provjeravanje.
- V3_lenient - Nisu potrebne sve nadređene klase objekta. Potrebne su samo neposredne klase objekta kada se dodaju unosi.

Default
V3_lenient

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
10

Vrijednost
Jedna-vrijednost

ibm-slapdSecurePort

Opis Specificira TCP/IP port koji se koristi za SSL veze. Ne može imati istu vrijednost kao i ibm-slapdPort. (IP portovi nisu označeni, 16-bitni cijeli brojevi u rasponu 1 - 65535.)

Default
636

Sintaksa
Cijeli broj

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdSecurity

Opis Omogućuje SSL veze. Mora biti none, SSL ili SSLOnly.

- none - poslužitelj osluškuje samo na ne-ssl portu.
- SSL - poslužitelj osluškuje na ssl i ne-ssl portovima.
- SSLOnly - poslužitelj osluškuje samo na ssl portu.

Default
ništa

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
7

Vrijednost
Jedna-vrijednost

ibm-slapdServerId

Opis Identificira poslužitelj koji će se koristiti u replikaciji.

Sintaksa
IA5 niz s uspoređivanjem osjetljivim na velika i mala slova

Maksimalna dužina
240

Vrijednost
Jedna-vrijednost

ibm-slapdSetenv

Opis Poslužitelj izvodi **putenv()** za sve vrijednosti ibm-slapdSetenv kod pokretanja kako bi modificirao okolinu poslužitelja za vrijeme izvođenja. Varijable ljuske (kao što je %PATH% ili $LANG) se ne proširuju.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
2000

Vrijednost
Više-vrijednosti

ibm-slapdSizeLimit

Opis Specificira maksimalan broj unosa koji će se vratiti iz pretraživanja, bez obzira na ograničenje veličine koje je možda bilo specificirano na klijentovom zahtjevu za pretraživanje (Raspon = 0...). Ako je klijent premašio granicu, koristit će se manja vrijednost od vrijednosti klijenta i vrijednosti koja je pročitana iz **ibmslapd.conf**. Ako klijent nije premašio granicu i ima ograničenje kao admin DN, smatra se da ograničenje ne postoji. Ako klijent nije premašio ograničenje i nije ograničen kao admin DN, onda je ograničenje ono koje je pročitano iz **ibmslapd.conf** datoteke. 0 = neograničeno.

Default
500

Sintaksa
Cijeli broj

Maksimalna dužina
12

Vrijednost
Jedna-vrijednost

ibm-slapdSortKeyLimit

Opis Maksimalan broj uvjeta sortiranja (ključeva) koji mogu biti specificirani na jednom zahtjevu za pretraživanjem. Raspon = 0.... Ako je klijent propustio zahtjev pretraživanja s više ključeva sortiranja od dozvoljenih, a kritičnost kontrole sortiranog pretraživanja je FALSE, onda će poslužitelj poštovati vrijednost koja je pročitana iz ibmslapd.conf datoteke i zanemariti sve ključeve sortiranja na koje naiđe nakon što je dosegnuta granica - izvodit će se pretraživanje i sortiranje. Ako je klijent propustio zahtjev pretraživanja s više ključeva nego je dozvoljeno, a kritičnost kontrole sortiranog pretraživanja je TRUE, onda će poslužitelj vratiti klijentu povratni kod **adminLimitExceeded** - neće se izvoditi sortiranje ili pretraživanje.

Default
3

Sintaksa
cis

Dužina
11

Brojanje
Jedan

Korištenje
directoryOperation

Modificiranje korisnika
Da

Klasa pristupa
kritično

Klasa objekta
ibm-slapdRdbmBackend

Potrebno
Ne

ibm-slapdSortSrchAllowNonAdmin

Opis Da li bi poslužitelj trebao ili ne, dozvoliti vezanje ne-Administratora za sortiranje na zahtjevu pretraživanja. Ako je vrijednost pročitana s ibmslapd.conf datoteke FALSE, poslužitelj će obrađivati samo one zahtjeve klijenta koje je poslao na izvođenje korisnik s Administrator ovlaštenjem. Ako klijentov zahtjev za sortiranjem zahtjeva pretraživanja nema Administrator ovlaštenje, a vrijednost pročitana iz ibmslapd.conf datoteke za taj atribut je FALSE, poslužitelj će vratiti klijentu povratni kod insufficientAccessRights - neće se izvoditi pretraživanje ili sortiranje.

Default
FALSE

Sintaksa
Booleov

Dužina
5

Brojanje
Jedan

Korištenje
directoryOperation

Modificiranje korisnika
Da

Klasa pristupa
kritično

Klasa objekta
ibm-slapdRdbmBackend

Potrebno
Ne

ibm-slapdSslAuth

Opis Specificira tip provjere autentičnosti za ssl vezu, serverauth ili serverclientauth.

- serverauth - podržava provjeru autentičnosti poslužitelja na klijentu. To je default.
- serverclientauth - podržava provjeru autentičnosti klijenta i poslužitelja.

Default
serverauth

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
16

Vrijednost
Jedna-vrijednost

ibm-slapdSslCertificate

Opis Specificira oznaku koja identificira Osobni certifikat poslužitelja u datoteci baze podataka ključa. Ta oznaka je specificirana kada su privatni ključ poslužitelja i certifikat kreirani s **gsk4ikm** aplikacijom. Ako nije definirano ibm-slapdSslCertificate, default privatni ključ, kako je to definirano u datoteci baze podataka ključa, koristi LDAP poslužitelj za SSL veze.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdSslCipherSpec

Specificira metodu za SSL šifriranje za klijente koji pristupaju poslužitelju. Mora biti postavljen na jedno od sljedećeg:

Tablica 5. Metode SSL šifriranja

Atribut	Razina šifriranja
TripleDES-168	Trostruko DES šifriranje sa 168-bitnim ključem i SHA-1 MAC
DES-56	DES šifriranje s 56-bitnim ključem i SHA-1 MAC

Tablica 5. Metode SSL šifriranja (nastavak)

Atribut	Razina šifriranja
RC4-128-SHA	RC4 šifriranje sa 128-bitnim ključem i SHA-1 MAC
RC4-128-MD5	RC4 šifriranje sa 128-bitnim ključem i MD5 MAC
RC2-40-MD5	RC4 šifriranje sa 40-bitnim ključem i MD5 MAC
RC4-40-MD5	RC4 šifriranje sa 40-bitnim ključem i MD5 MAC
AES	AES šifriranje

Sintaksa
IA5 niz

Maksimalna dužina
30

ibm-slapdSslKeyDatabase

Opis Specificira stazu datoteke do SSL datoteke baze podataka ključa LDAP poslužitelja. Ta datoteka baze podataka ključa se koristi za rukovanje SSL vezama s LDAP klijenata, kao i za kreiranje sigurnih SSL veza do replika LDAP poslužitelja.

Default
/etc/key.kdb

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdSslKeyDatabasePW

Opis Specificira lozinku koja je pridružena SSL datoteci baze podataka ključa LDAP poslužitelja, kako je to specificirano na ibm-slapdSslKeyDatabase parametru. Ako datoteka baze podataka ključa LDAP poslužitelja ima pridruženu datoteku skrivene lozinke, onda se ibm-slapdSslKeyDatabasePW parametar može izostaviti ili postaviti na none.

Bilješka: Datoteka skrivene lozinke mora biti smještena u istom direktoriju kao i datoteka baze podataka ključa i mora imati isto ime datoteke kao i datoteka baze podataka ključa, no s ekstenzijom .sth umjesto .kdb.

Default
ništa

Sintaksa
Binarno

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdSslKeyRingFile

Opis Staza do SSL datoteke baze podataka ključa LDAP poslužitelja. Ta datoteka baze podataka ključa se koristi za rukovanje SSL vezama s LDAP klijenata, kao i za kreiranje sigurnih SSL veza do replika LDAP poslužitelja.

Default
key.kdb

Sintaksa
Niz direktorija s uspoređivanjem osjetljivim na velika i mala slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdSuffix

Opis Specificira kontekst imenovanja koji će se pohraniti u ovoj pozadini.

Bilješka: To ima isto ime kao i klasa objekta.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
DN

Maksimalna dužina
1000

Vrijednost
Više-vrijednosti

ibm-slapdSupportedWebAdmVersion

Opis Taj atribut definira najraniju verziju Web administracijskog alata koji podržava taj poslužitelj od cn=configuration.

Default

Sintaksa
Niz direktorija

Maksimalna dužina

Vrijednost
Jedna-vrijednost

ibm-slapdSysLogLevel

Opis Specificira razinu na kojoj se zapisuju statistike otkrivanja grešaka i operacije u datoteci slapd.errors. Mora biti specificirano kao l, m ili h.

- h - visoko (osigurava najviše informacija)
- m - srednje (default)
- l - nisko (osigurava najmanje informacija)

Default
m

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
1

Vrijednost
Jedna-vrijednost

ibm-slapdTimeLimit

Opis Specificira maksimalan broj sekundi koje se mogu potrošiti na zahtjev pretraživanja, bez obzira na bilo koje ograničenje vremena koje je možda specificirano na zahtjevu klijenta. Ako je klijent premašio granicu, koristit će se manja vrijednost od vrijednosti klijenta i vrijednosti koja je pročitana iz **ibmslapd.conf**. Ako klijent nije premašio granicu i ima ograničenje kao admin DN, smatra se da ograničenje ne postoji. Ako klijent nije premašio ograničenje i nije ograničen kao admin DN, onda je ograničenje ono koje je pročitano iz **ibmslapd.conf** datoteke. 0 = neograničeno.

Default
900

Sintaksa
Cijeli broj

Maksimalna dužina

Vrijednost
Jedna-vrijednost

ibm-slapdTransactionEnable

Opis Ako je učitan plugin transakcije, ali je ibm-slapdTransactionEnable postavljeno na FALSE, poslužitelj odbija sve StartTransaction zahtjeve s odgovorom LDAP_UNWILLING_TO_PERFORM.

Default
TRUE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdUseProcessIdPw

Opis Ako je postavljen na TRUE, poslužitelj zanemaruje ibm-slapdDbUserID i ibm-slapdDbUserPW atribute i koristi vlastite vjerodajnice obrade kako bi ovlastio na DB2.

Default
FALSE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdVersion

Opis IBM Slapd broj verzije

Default

Sintaksa
Niz direktorija s uspoređivanjem osjetljivim na velika i mala slova

Maksimalna dužina

Vrijednost
Jedna-vrijednost

objectClass

Opis Vrijednost objectClass atributa opisuje vrstu objekta kojeg predstavlja unos.

Sintaksa
Niz direktorija

Maksimalna dužina
128

Vrijednost
Više-vrijednosti

Poglavlje 10. Povezane informacije

Dolje su ispisani IBM Redbooks (u PDF formatu), Web stranice i Informacijski Centar poglavlja koja se odnose na poglavlje Poslužitelj direktorija. Možete pregledati ili ispisati sve PDF-ove.

Redbooks (www.redbooks.ibm.com)

- *Razumijevanje LDAP-a*, SG24-4986 .
- *Upotreba LDAP za Integraciju direktorija: Pogled na IBM SecureWay direktorij, Aktivni direktorij i Domino*, SG24-6163 .
- *Implementacija i Praktično korištenje LDAP-a na iSeries Poslužitelja*, SG24-6193 .

Web stranice

- IBM Poslužitelj direktorija za iSeries Web stranicu (www.ibm.com/servers/eserver/iseries/ldap)
- Web stranica priručnika za Java imenovanje i Sučelje direktorija (JNDI) (java.sun.com/products/jndi/tutorial/)

Ostale informacije

“API-ji Poslužitelja direktorija” u poglavlju Programiranje.

Dodatak. Napomene

Ove informacije su razvijene za proizvode i usluge koji se nude u SAD.

IBM možda ne nudi proizvode, usluge ili funkcije o kojima se raspravlja u ovom dokumentu u drugim zemljama. Posavjetujte se sa svojim lokalnim IBM predstavnikom za informacije o proizvodima i uslugama koji su trenutno dostupni u vašem području. Bilo koje upućivanje na IBM proizvod, program ili uslugu nema namjeru tvrditi da se samo taj IBM proizvod, program ili usluga mogu koristiti. Bilo koji funkcionalno ekvivalentan proizvod, program ili usluga koji ne narušava nijedno IBM pravo na intelektualno vlasništvo, se može koristiti kao zamjena. Međutim, na korisniku je odgovornost da procijeni i provjeri rad bilo kojeg ne-IBM proizvoda, programa ili usluge.

IBM može imati patente ili molbe za patente koje su još u toku, a koji pokrivaju predmet o kojem se govori u ovom dokumentu. Posjedovanje ovog dokumenta ne daje vam nikakvu dozvolu za korištenje tih patenata. Možete poslati upit za licence, u pismenom obliku, na:

| IBM Director of Licensing
| IBM Corporation
| North Castle Drive
| Armonk, NY 10504-1785
| U.S.A.

Za upite o licenci u vezi s dvo-bajtnim (DBCS) informacijama, kontaktirajte IBM-ov odjel intelektualnog vlasništva u vašoj zemlji ili pošaljite upite, u pisanom obliku na adresu:

| IBM World Trade Asia Corporation
| Licensing
| 2-31 Roppongi 3-chome, Minato-ku
| Tokyo 106-0032, Japan

Sljedeći odlomak se ne primjenjuje na Ujedinjeno Kraljevstvo ili bilo koju drugu zemlju gdje su takve izjave nekonzistentne s lokalnim zakonima: INTERNATIONAL BUSINESS MACHINES CORPORATION DAJE OVU PUBLIKACIJU “KAKVA JE ”, BEZ IKAKVIH JAMSTAVA, BILO IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA O NE-POVREĐIVANJU, PROĐI NA TRŽIŠTU ILI SPOSOBNOSTI ZA ODREĐENU SVRHU. Neke zemlje ne dozvoljavaju odricanje od izravnih ili posrednih jamstava u određenim transakcijama, zbog toga, se ova izjava možda ne odnosi na vas.

Ove informacije mogu sadržavati tehničke netočnosti ili tipografske pogreške. Promjene se povremeno rade u ovim informacijama; te promjene će biti uključene u nova izdanja publikacije. IBM može raditi poboljšanja i/ili promjene u proizvodu(ima) i/ili programu/ima opisanim u ovoj publikaciji, bilo kad, bez prethodne obavijesti.

Bilo koje upućivanje u ovim informacijama na ne-IBM Web stranice, služi samo kao pomoć i ni na kakav način ne služi za promicanje tih Web stranica. Materijali na tim Web stranicama nisu dio materijala za ovaj IBM proizvod i upotreba tih Web stranica je na vaš osobni rizik.

IBM može koristiti ili distribuirati bilo koje od informacija dobavljenih od vas na bilo koji način bez ikakvih obaveza prema vama.

Vlasnici licence za ovaj program, koji žele imati informacije o njemu u svrhu omogućavanja: (i) izmjene informacija između neovisno kreiranih programa i drugih programa (uključujući i ovaj) i (ii) uzajamne upotrebe informacija koje su bile izmijenjene, trebaju kontaktirati:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Takve informacije mogu biti dostupne, uz odgovarajuće termine i uvjete, uključujući u nekim slučajevima i plaćanje pristojbe.

Licencni program opisan u ovim informacijama i sav licencni materijal dostupan za njega IBM daje pod uvjetima IBM Ugovora s korisnikom, IBM Internacionalnog ugovora o programskoj licenci, IBM Ugovora o licenci za strojni kod ili bilo kojeg jednakovrijednog ugovora između nas.

Svi podaci o izvedbi koji su ovdje sadržani su utvrđeni u kontroliranoj okolini. Zbog toga se rezultati dobiveni u drugim operativnim okolinama mogu značajno razlikovati. Neka mjerenja su možda bila izvedena na sistemima na razvojnoj razini i ne postoji nikakvo jamstvo da će ta mjerenja biti ista na općenito dostupnim sistemima. Osim toga, neka mjerenja su možda bila procijenjena pomoću ekstrapolacije. Stvarni rezultati se mogu razlikovati. Korisnici ovog dokumenta bi trebali provjeriti primjenjive podatke za njihovo specifično okruženje.

Informacije koje se tiču ne-IBM proizvoda su dobivene od dobavljača tih proizvoda, njihovih objavljenih najava ili drugih dostupnih javnih izvora. IBM nije testirao te proizvode i ne može potvrditi točnost performansi, kompatibilnosti ili bilo koji drugi zahtjev vezan uz ne-IBM proizvod. Pitanja o sposobnostima ne-IBM proizvoda bi trebala biti adresirana na dobavljače tih proizvoda.

Sve izjave koje se odnose na buduća usmjerenja ili namjere IBM-a su podložne promjenama i mogu se povući bez najave, a predstavljaju samo ciljeve i smjernice.

Prikazane IBM cijene su njegove predložene maloprodajne cijene, trenutne su i podložne promjeni bez prethodne obavijesti. Cijene kod zastupnika se mogu razlikovati.

Ove informacije služe samo u svrhu planiranja. Ovdje sadržane informacije su podložne promjenama prije nego opisani proizvodi postanu dostupni.

Ove informacije sadrže primjere podataka i izvještaja koji se koriste u svakodnevnim operacijama. Da ih se što bolje objasni, primjeri uključuju imena pojedinaca, poduzeća, trgovačkih marki i proizvoda. Sva ta imena su izmišljena i svaka sličnost s imenima i adresama koja koriste stvarna poduzeća je potpuno slučajna.

LICENCA O AUTORSKOM PRAVU:

Ove informacije sadrže uzorke aplikativnih programa na izvornom jeziku, koji objašnjavaju tehnike programiranja na različitim operativnim platformama. Možete kopirati, modificirati i distribuirati te uzorke programa u bilo kojem obliku bez plaćanja IBM-u, u svrhe razvoja, upotrebe, marketinga ili distribucije aplikacijskih programa prilagođenih sučelju aplikativnog programiranja za operacijsku platformu za koju su uzorci programa napisani. Ti primjeri nisu temeljito testirani pod svim uvjetima. IBM zbog toga ne može jamčiti ili potvrditi pouzdanost, upotrebljivost ili funkcioniranje tih programa.

PODLOŽNO BILO KOJIM ZAKONSKIM JAMSTVIMA KOJA SE NE MOGU ISKLJUČITI,IBM, NJEGOVI RAZVIJAČI PROGRAMA I DOBAVLJAČI NE DAJU JAMSTVA ILI UVJETE, IZRIČITA ILI POSREDNA, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA ILI UVJETE ZA PROĐU NA TRŽIŠTU, SPOSOBNOST ZA ODREĐENU SVRHU I NE-KRŠENJE, VEZANO UZ PROGRAM ILI TEHNIČKU PODRŠKU, AKO POSTOJE.

IBM, RAZVIJAČI PROGRAMA ILI DOBAVLJAČI NISU NITI U KOJIM UVJETIMA ODGOVORNI ZA BILO ŠTO OD SLJEDEĆEG, ČAK I AKO SU OBAVIJEŠTENI O TAKVOJ MOGUĆNOSTI:

1. GUBITAK ILI OŠTEĆENJE PODATAKA;
2. POSEBNE, SLUČAJNE ILI NEIZRAVNE ŠTETE, ILI EKONOMSKE POSLJEDIČNE ŠTETE; ILI
3. GUBITAK PROFITA, POSLA, ZARADE, DOBROG GLASA ILI UŠTEDE.

| NEKA ZAKONODAVSTVA NE DOZVOLJAVAJU ISKLJUČENJE ILI OGRANIČENJE SLUČAJNIH ILI
| POSLJEDIČNIH ŠTETA, TAKO DA SE GORNJA OGRANIČENJA MOŽDA NE ODNOSE NA VAS.

Svaka kopija ili bilo koji dio ovih uzoraka programa ili bilo kojeg izvedenog rada mora sadržavati napomenu o autorskom pravu u obliku:

© (ime vašeg poduzeća) (godina). Dijelovi ovog koda su izvedeni iz IBM Corp. uzoraka programa. © Autorsko pravo IBM Corp. _unesite godinu ili godine_. Sva prava pridržana.

Ako gledate ove informacije kao nepostojanu kopiju, fotografije i slike u boji se možda neće vidjeti.

Zaštitni znaci

Sljedeći termini su zaštitni znaci International Business Machines Corporation u Sjedinjenim Državama, drugim zemljama ili oboje:

| AIX
| AIX 5L
| e(logo)server
| eServer
| i5/OS
| IBM
| iSeries
| pSeries
| xSeries
| zSeries

| Intel, Intel Inside (logos), MMX i Pentium su zaštitni znaci Intel Corporation u Sjedinjenim Državama, drugim
| zemljama ili oboje.

Microsoft, Windows, Windows NT i Windows logo su zaštitni znaci Microsoft Corporation u Sjedinjenim Državama, drugim zemljama ili oboje.

Java i svi Java-bazirani zaštitni znaci su zaštitni znaci Sun Microsystems, Inc. u Sjedinjenim Državama, drugim zemljama ili oboje.

| Linux je zaštitni znak Linus Torvalds u Sjedinjenim Državama, drugim zemljama ili oboje.

UNIX je registrirani zaštitni znak The Open Group u Sjedinjenim Državama i drugim zemljama.

Ostala imena poduzeća, proizvoda ili usluga mogu biti zaštitni znaci ili oznake usluga drugih.

| Termini i uvjeti za spuštanje i ispis informacija

| Dozvole za upotrebu informacija koje ste izabrali za spuštanje dodjeljuju se prema sljedećim terminima i uvjetima i
| nakon vašeg prihvaćanja.

| **Osobna upotreba:** Možete reproducirati ove informacije za vašu osobnu, nekomercijalnu upotrebu, uz osiguranje da
| su sve napomene o vlasništvu sačuvane. Ne smijete distribuirati, prikazivati ili raditi izvedena djela iz ovih publikacija
| ili bilo kojeg njihovog dijela, bez izričite suglasnosti IBM-a.

| **Komercijalna upotreba:** Možete reproducirati, distribuirati i prikazivati ove informacije isključivo unutar vašeg
| poduzeća, uz osiguranje da su sve napomene o vlasništvu sačuvane. Ne smijete izrađivati izvedene radove iz ovih
| informacija ili reproducirati, distribuirati ili prikazivati ove informacije ili bilo koji njihov dio izvan vašeg poduzeća,
| bez izričite dozvole IBM-a.

Osim kako je izričito dodijeljeno u ovoj dozvoli, nisu dane nikakve dozvole, licence ili prava, niti izričita niti posredna, na informacije ili bilo koje podatke, softver ili bilo koje drugo intelektualno vlasništvo sadržano unutar.

IBM rezervira pravo da bilo kad, po vlastitom nahođenju, povuče ovdje dodijeljene dozvole, ako je upotreba publikacija štetna za njegove interese ili je ustanovljeno od strane IBM-a da gornje upute nisu bile ispravno slijeđene.

Ne smijete spustiti, eksportirati ili reeksportirati ove informacije, osim kod potpune usklađenosti sa svim primjenjivim zakonima i propisima, uključujući sve zakone i propise o izvozu Sjedinjenih Država. IBM NE DAJE NIKAKVO JAMSTVO NA SADRŽAJ OVIH INFORMACIJA. INFORMACIJE SE DAJU ″KAKVE JESU″ I BEZ JAMSTAVA BILO KOJE VRSTE, IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA PROĐE NA TRŽIŠTU, NEKRŠENJA I PRIKLADNOSTI ZA ODREĐENU SVRHU.

Spuštanjem i ispisom informacija s ove stranice, naznačili ste da se slažete s ovim terminima i uvjetima.

Tiskano u Hrvatskoj