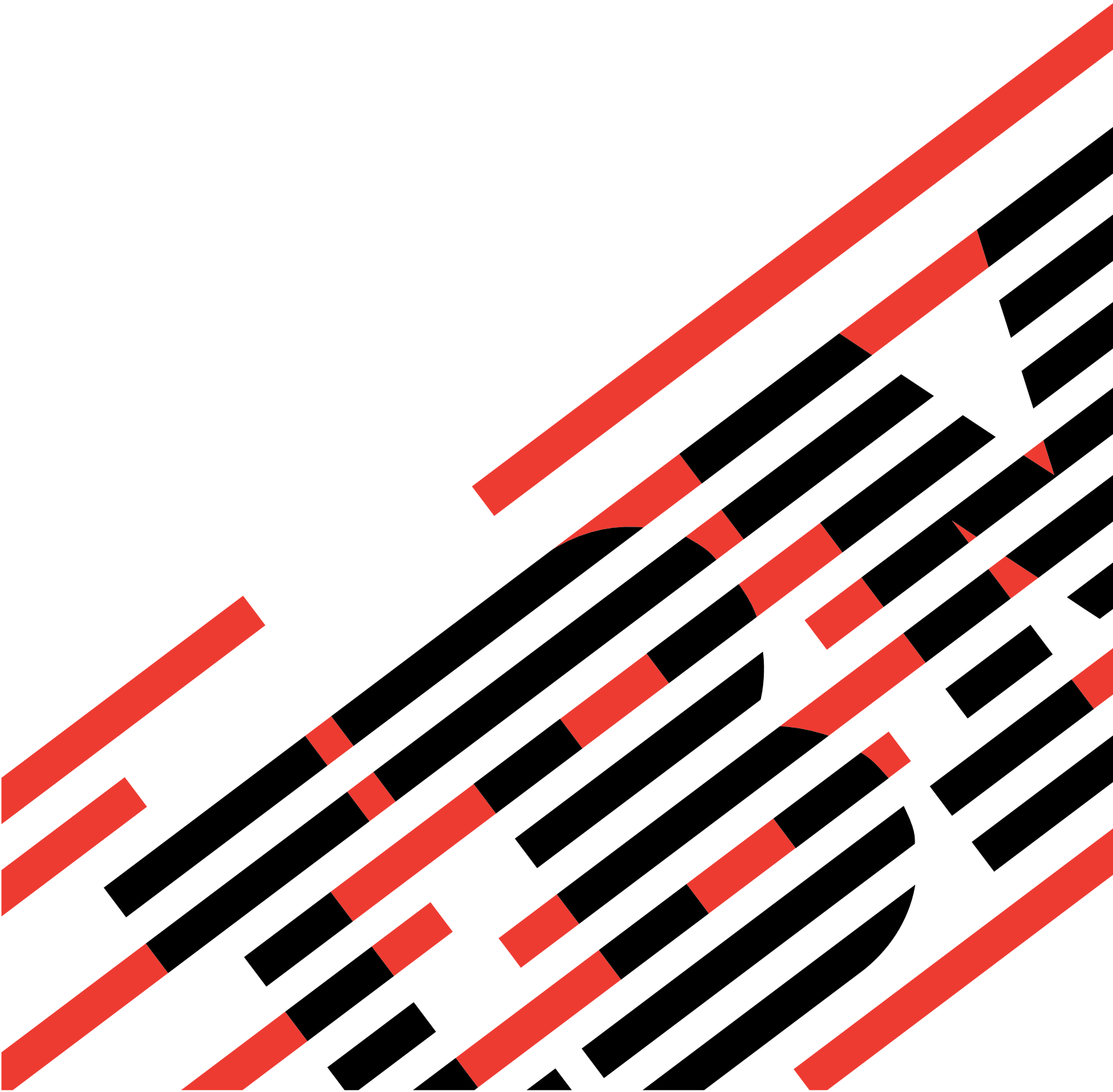
IBM

eserver

iSeries

IBM Directory Server (LDAP)

Različica 5 izdaja 3



IBM

@server

iSeries

IBM Directory Server (LDAP)

Različica 5 izdaja 3

Opomba

Preden začnete uporabljati te informacije in izdelek, ki so mu namenjene, preberite “Opombe”, na strani 221.

Sedma izdaja (avgust 2005)

Ta izdaja je namenjena za različico 5, izdajo 3 in raven popravkov 0 sistema IBM Operating System/400 (številka izdelka 5722–SS1) in za vse nadaljnje izdaje in popravke, dokler v novih izdajah ne bomo določili drugače. Te različice ni mogoče izvajati v vseh modelih računalnikov z zmanjšanim naborom znakov (RISC), niti v modelih CISC.

Kazalo

Poglavje 1. IBM Directory Server za iSeries (LDAP)

IBM Directory Server za iSeries (ki ga bomo od zdaj naprej imenovali imeniški strežnik), nudi strežnik LDAP (Lightweight Directory Access Protocol) v strežniku iSeries. LDAP se izvaja prek protokola TCP/IP (Transmission Control Protocol/Internet Protocol) in je popularen kot imeniška storitev za internetne in ne-internetne aplikacije.

V naslednjih temah boste našli informacije, ki vam bodo pomagale razumeti in uporabljati imeniški strežnik v strežniku iSeries:

Poglavje 2. Kaj je novega v V5R3

Directory Server za iSeries (ki se je predhodno imenoval IBM Directory Server za iSeries) vključuje v V5R3 naslednje izboljšave in nove možnosti:

- **Upravljanje in dostopnost uporabnikov:** novo IBM-ovo orodje za spletno upravljanje imeniškega strežnika nadomešča IBM-ovo orodje za upravljanje imenikov. Orodje za spletno upravljanje vključuje funkcije za upravljanje uporabniških vnosov, procesov imeniškega strežnika in imeniškega drevesa iz splošnega spletnega vmesnika. Protokol LDAP se zdaj uporablja za poizvedovanje in ažuriranje konfiguracijskih možnosti imeniškega strežnika.
- **Dinamične skupine:** dinamične skupine omogočajo izdelavo skupine, v katerih so člani postavke, ki ustrezajo iskalnemu filtru.
- **Ugnezdene skupine:** vgnezdene skupine omogočajo izdelavo skupine, katere člani vključujejo katerekoli člane drugih skupin.
- **Načelo za gesla:** imeniški strežnik zdaj podpira načelo za gesla, ki vključuje skladenjska pravila za gesla, zgodovino gesel in onemogočanje vnosov po preveč poskusih uporabe nepravilnih gesel.
- **Krmilni elementi dostopa na osnovi filtrov:** pooblastilo za vnose lahko zdaj določite s krmilnim elementom dostopa na osnovi filtrov. Tako lahko na primer določite pravice za vnose z departmentNumber=abc ali podelite dostop določenim vrstam vnosov.
- **Podvajanje:** izboljšave podvajanja vključujejo zmožnost za uporabo več glavnih strežnikov (enakovrednih strežnikov), podvajanje poddreves, izboljšano načrtovanje in krmiljenje podvajanja, izboljšano nadzorovanje in robustnejšo funkcijo podvajanja.
- **Razvrščeno iskanje:** krmilni element za razvrščeno iskanje omogoča, da prejme odjemalec rezultate iskanja, ki so razvrščeni na osnovi seznama kriterijev, na katerem vsak kriterij predstavlja ključ razvrščanja. S tem je odgovornost za razvrščanje prenesena iz odjemalca v strežnik, kjer je lahko opravljena bolj učinkovito. Ukaz ldapsearch smo izboljšali z novimi parametri, ki omogočajo razvrščanje iskalnih rezultatov. Za razvrščanje iskalnih rezultatov so na voljo tudi novi API-ji LDAP.
- **Iskanje po straneh:** krmilni element za rezultate po straneh omogoča upravljanje velikih količin podatkov, ki jih vrne iskalna zahteva. Namesto da prejmete vse rezultate naenkrat, lahko zahtevate podniz postavk (stran). Nadaljnje iskalne zahteve prikazujejo naslednjo stran rezultatov, dokler ni operacija preklicana ali dokler ni vrnjen zadnji rezultat. Ukaz ldapsearch smo izboljšali z novimi parametri, ki omogočajo razdelitev iskalnih rezultatov na strani. Za razdelitev iskalnih rezultatov na strani so na voljo tudi novi API-ji LDAP.
- **Pripomočki ukazne vrstice:** naslednji pripomočki ukazne vrstice so novi:
  - ldapexop - omogoča zmožnost za povezavo z imenikom in izdajo razširjene operacije z vsemi podatki, ki tvorijo vrednost razširjene operacije
  - ldapdiff - uskladi strežnik za podvajanje z njegovim glavnim strežnikom
  - ldapchangepwd - strežniku LDAP pošlje zahtevo za spremembo gesla.
- **Zmogljivost:** zmogljivost za vse operacije je izboljšana. Poleg tega lahko zdaj sočasno izvaja vse operacije več odjemalcev.
- **Posebni znaki v razločevalnih imenih (DN-jih):** DN lahko zdaj vsebuje naslednje posebne znake: vejice, enačaje, znak plus, znak večje kot, znak manjše kot, znak za funte, podpičje, poševnico nazaj in narekovaje.
- **Pravila primerjave za nizovne atribute:** če je atribut definiran z eno od dveh nizovnih skladenj - imeniški niz ali niz IA5 - bo strežnik zdaj sprejel vedenje primerjanja, podano v shemi za atribut, s čimer je odpravljena napaka iz prejšnjih izdaj. Atribut lahko definirate tako, da bodo velike in male črke pri primerjavi upoštevane ali zanemarjene. Strežnik je predhodno sicer omogočal definiranje pravila za primerjanje, vendar ga je zanemaril. Notranje je obravnaval strežnik niz IA5 z upoštevanjem velikih in malih črk, imeniški niz pa brez upoštevanja velikih in malih črk. Če je strežnik definiral atribute za niz IA5 s caseIgnoreMatch, za DirectoryString pa s caseExactMatch, se bo za ta atributa zdaj vedel pravilno.

Poglavje 3. Tiskanje PDF

Če si želite ogledati različico PDF tega dokumenta ali jo presneti iz oddaljenega računalnika, izberite Imeniški strežnik (LDAP) (okrog 2700 kB).

Druge informacije

Za prikaz ali natis datotek PDF povezanih priročnikov in Redbooks preglejte Poglavje 10, “S tem povezane informacije”, na strani 219.

Shranjevanje datotek PDF

Če želite shraniti datoteko PDF na delovno postajo za prikaz ali natis, naredite naslednje:

1. Z desno tipko miške kliknite datoteko PDF v pregledovalniku (z desno tipko miške kliknite zgornjo povezavo).
2. Kliknite možnost, ki shrani datoteko PDF lokalno.
3. Poiščite imenik, v katerega želite shraniti datoteko PDF.
4. Kliknite **Shrani**.

Prenos programa Adobe Reader

Za prikaz ali natis teh datotek PDF morate imeti v sistemu nameščen Adobe Reader. Njegovo brezplačno kopijo lahko presnamete s spletne strani Adobe (www.adobe.com/products/acrobat/readstep.html) .

Poglavje 4. Pojmi imeniškega strežnika

Imeniški strežnik izvršuje specifikacije LDAP V3 IETF (Internet Engineering Task Force). Vključuje tudi izboljšave, ki jih je dodal IBM v funkcijskih in zmogljivostnih področjih. Ta različica uporablja IBM DB2 kot podporno shranjevališče, ki nudi integriteto transakcij za operacije LDAP, visoko zmogljive operacije ter zmožnost sprotnega varnostnega kopiranja in obnavljanja. Sodeluje lahko z odjemalci, ki temeljijo na LDAP V3 IETF. Pojme in problematiko, povezane z imeniškim strežnikom, boste našli v naslednjih temah:

Imeniki

Imeniški strežnik omogoča dostop do tipa baze podatkov, ki shranjuje informacije v hierarhični strukturi, podobni ureditvi integriranega datotečnega sistema i5/OS.

Če je ime objekta znano, je mogoče pridobiti njegove značilnosti. Če ime določenega objekta ni znano, lahko izvedete v imeniku iskanje objektov, ki ustrezajo določeni zahtevi. Imenike lahko običajno preiščete z določenim kriterijem in ne samo z vnaprej definirano skupino kategorij.

Imenik je posebna baza podatkov z značilnostmi, ki ga ločujejo od relacijskih baz s splošnim namenom. Značilnost imenika je, da do njega dostopate (ga berete ali preiskujete) veliko pogosteje, kot ga ažurirate (pišete vanj). Ker morajo imeniki podpirati veliko količino bralnih zahtev, so običajno optimizirani za bralni dostop. Ker imeniki ne nudijo toliko funkcij kot baze podatkov s splošnim namenom, jih lahko optimizirate, da varčno nudijo več aplikacij s hitrim dostopom do imeniških podatkov v velikih porazdeljenih okoljih.

Imenik je lahko centraliziran ali porazdeljen. Če je imenik centraliziran, je na voljo en imeniški strežnik (ali gruča strežnikov) na enem mestu, ki omogoča dostop do imenika. Če je imenik porazdeljen, je na voljo več strežnikov, ki so običajno na geografsko ločenih mestih, ki nudijo dostop do imenika.

Če je imenik porazdeljen, je mogoče informacije, shranjene v imeniku, porazdeliti ali podvojiti. Če so informacije porazdeljene, hrani vsak strežnik unikatno in neprekrivajočo se skupino informacij. To pomeni, da hrani vsak imeniški vnos samo en strežnik. Imenik porazdelite z referenčnimi kazalci LDAP. Le-ti uporabnikom omogočajo, da dodelijo zahteve LDAP (Lightweight Directory Access Protocol) enakim ali različnim imenskim prostorom, ki so shranjeni na drugem (ali enakem) strežniku. Če so informacije podvojene (replicirane), hrani en imeniški vnos več kot en strežnik. V porazdeljenem imeniku so lahko nekatere informacije porazdeljene, druge pa podvojene.

Model imeniškega strežnika LDAP temelji na vnosih (ki jih imenujemo tudi objekti). Vsak vnos je sestavljen iz enega ali več atributov, kot so ime ali naslov in tip. Tipi so običajno sestavljeni iz skupine vročih črk, kot je na primer cn za splošno ime ali mail za naslov elektronske pošte.

Vzorčni imenik na sliki Slika 1 na strani 9 kaže vnos za osebo Tim Jones, ki vsebuje atributa mail in telephoneNumber. Drugi možni atributi so fax, title, sn (za priimek) in jpegPhoto.

Vsak imenik vsebuje shemo, ki je niz pravil, ki določajo strukturo in vsebino imenika. Shemo si lahko ogledate z orodjem za spletno upravljanje. Dodatne informacije o shemi boste našli v razdelku “Shema” na strani 15.

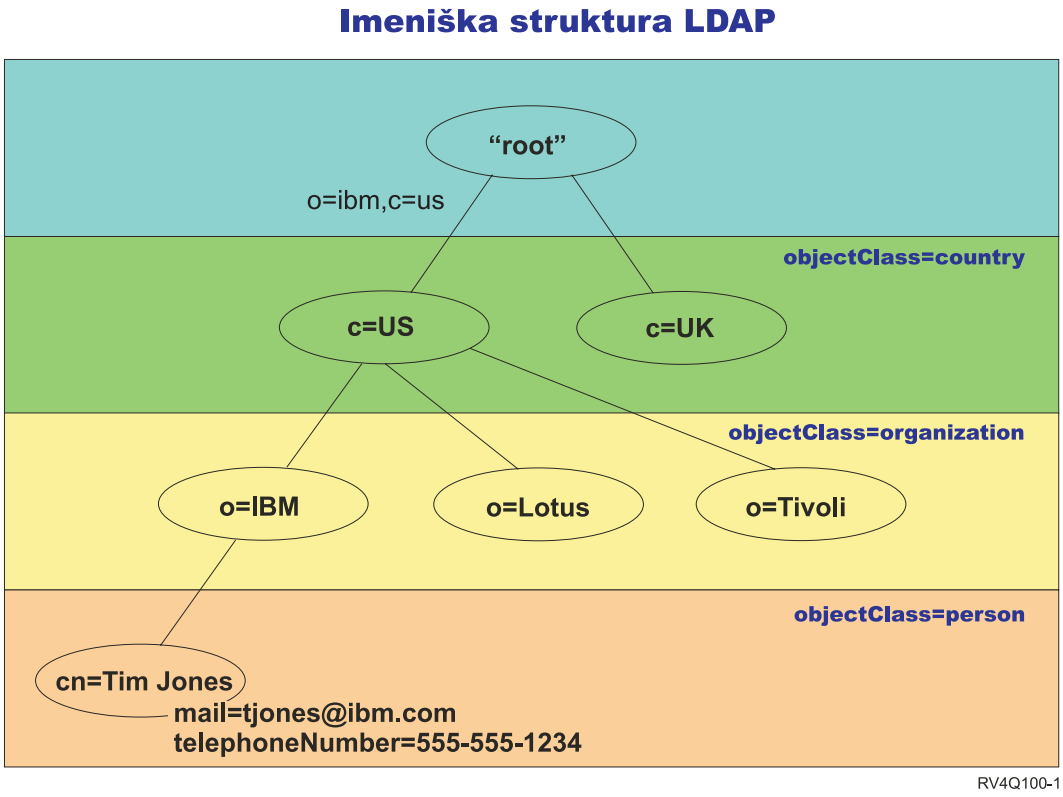
Vsak imeniški vnos ima poseben atribut, imenovan objectClass. Ta atribut krmili, kateri atributi so obvezni in dovoljeni v vnosu. Z drugimi besedami, vrednosti atributa objectClass določajo pravila sheme, ki se jim mora vnos podrejati.

Poleg atributov, ki jih definira shema, je z vnosi povezan tudi niz atributov, ki jih vzdržuje strežnik. Ti atributi, imenovani operacijski atributi, vsebujejo elemente, kot je na primer datum izdelave postavke in informacije za nadzor dostopa. Dodatne informacije o operacijskih atributih boste našli v razdelku “Operacijski atributi” na strani 70.

Običajno so vnosi imenika LDAP urejeni v hierarhični strukturi, ki odraža politične, geografske in organizacijske omejitve (Slika 1 na strani 9). Vnosi, ki predstavljajo države ali področja, so prikazani na vrhu hierarhije. Vnosi, ki predstavljajo dežele ali državne organizacije zasedajo drugo raven v hierarhiji. Spodnji vnosi lahko predstavljajo ljudi, organizacijske enote, tiskalnike, dokumente ali druge postavke.

LDAP se sklicuje na vnose z razločevalnimi imeni (DN-ji). Razločevalno ime je sestavljeno iz imena vnosa, kot tudi iz imen objektov nad njim v imeniku, v vrstnem redu od spodaj navzgor. Celoten DN za vnos v spodnjem levem vogalu slike Slika 1 na strani 9 je na primer cn=Tim Jones, o=IBM, c=US. Vsak vnos ima najmanj en atribut, ki je uporabljen za ime vnosa. Ta poimenovalni atribut se imenuje relativno razločevalno ime (RDN) vnosa. Vnos nad določenim RDN-jem se imenuje nadrejeno razločevalno ime. V zgornjem zgledu cn=Tim Jones poimenuje vnos, zato je RDN. o=IBM, c=US je nadrejeni DN za cn=Tim Jones. Dodatne informacije o DN-jih boste našli v razdelku “Razločevalna imena (DN-ji)” na strani 11.

Če želite podati strežniku LDAP zmožnost upravljanja dela imenika LDAP, podajte v konfiguraciji strežnika najvišjo raven nadrejenih razločevalnih imen. Ta razločevalna imena se imenujejo pripone. Strežnik lahko dostopa do vseh objektov v imeniku, ki so pod podano pripono v hierarhiji imenikov. Če vsebuje na primer strežnik LDAP imenik, prikazan v Slika 1 na strani 9, mora imeti v konfiguraciji podano pripono o=ibm, c=us, da bo lahko odgovarjal na odjemalske poizvedbe v zvezi s Tim Jonesom.



Slika 1. Imeniška struktura LDAP

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

Denimo, da želite izdelati imenik s strukturo domenske komponente, ki bo vsebovala podatke o uslužbencu, kot so na primer ime, telefonska številka in naslov elektronske pošte. Uporabite lahko pripono ali poimenovalni kontekst, temelječ na domeni TCP/IP. Ta imenik je lahko podoben naslednjemu:

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

Pri vnosu v imeniški strežnik so ti podatki lahko podobni naslednjim:

```
# 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: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: publisher
objectclass: ePerson
cn: Tim Jones
cn: "Jones, Tim"
sn: Jones
givenname: Tim
telephonenumber: 555-555-1234
mail: tjones@ibm.com

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

Opazili boste, da vsebuje vsak vnos vrednosti atributov, imenovane objectclass. Vrednosti objectclass definirajo, kateri atributi so dovoljeni v vnosu, kot sta na primer telephonenumber ali givenname. Dovoljeni objektni razredi so definirani v shemi. Shema je niz pravil, ki definirajo tipe vnosov, dovoljene v bazi podatkov.

Imeniški odjemalci in strežniki

Do imenikov se običajno dostopa z odjemalsko-strežniškim modelom komunikacij. Odjemalski in strežniški procesi so lahko na enem računalniku ali pa ne. Strežnik lahko streže številnim odjemalcem. Aplikacija, ki želi brati informacije iz imenika ali jih zapisati vanj, ne dostopi neposredno do imenika, pač pa namesto tega pokliče funkcijo ali aplikacijski programerski vmesnik (API), ki povzroči pošiljanje sporočila drugemu procesu. Ta drugi proces dostopi do informacij v imeniku v imenu zahtevniške aplikacije. Rezultati branja ali pisanja so vrnjeni zahtevniški aplikaciji.

API definira programerski vmesnik, ki ga uporabi določen programerski jezik za dostop do storitve. Format in vsebina sporočil, ki so izmenjana med odjemalcem in strežnikom, mora ustrezati dogovorjenemu protokolu. LDAP definira sporočilni protokol, ki ga uporabljajo imeniški odjemalci in imeniški strežniki. Na voljo je tudi povezani API LDAP za jezik C in načini za dostopanje do imenik iz aplikacije Java, ki uporablja Java Naming and Directory Interface (JNDI).

Zaščita imenika

Imenik mora podpirati osnovne zmožnosti, potrebne za izvedbo načela zaščite. Imenik osnovnih zmožnosti zaščite morda ne bo nudil neposredno, pač pa je lahko integriran s preverjeno storitvijo za omrežno zaščito, ki nudi osnovne zaščitne storitve. Najprej je potreben način za overjanje uporabnikov. Overjanje preveri, ali so uporabniki res tisti, za katere se predstavljajo. Osnovno shemo overjanja predstavljata ime uporabnika in geslo. Ko so uporabniki overjeni, je potrebno določiti, ali imajo pooblastilo ali pravico za izvedbo zahtevane operacije v določenem objektu.

Pooblastila pogosto temeljijo na seznamih za nadzor dostopa (ACL-jih). ACL je seznam pooblastil, ki so lahko dodana objektom in atributom v imeniku. ACL navaja, kakšna vrsta dostopa je dodeljena ali zavrnjena za vsakega uporabnika ali skupino uporabnikov. Da bi bili ACL-ji krajši in bi jih bilo lažje upravljati, so uporabniki z enakimi dostopnimi pravicami pogosto združeni v skupine.

Razločevalna imena (DN-ji)

Vsak vnos v imeniku ima razločevalno ime (DN). DN je ime, ki unikatno določa vnos v imeniku. Sestavljen je parov atribut=vrednost, ki so med seboj ločeni z vejicami, kot so na primer naslednji:

```
cn=Bogdan Grabnar,ou=urejanje,o=Delo,c=SL
cn=Lucija Varga,ou=urejanje,o=Delo,c=SL
cn=Timi Božič,ou=poročanje,o=Delo,c=SL
```

Za tvorbo DN-ja lahko uporabite katerekoli atribute, ki so definirani v imeniški shemi. Vrstni red parov atributov in vrednosti komponente je pomemben. DN vsebuje eno komponento za vsako raven imeniške hierarhije od korena pa do ravni, v kateri je vnos. DN-ji LDAP se začno z najbolj specifičnim atributom (običajno neka vrsta imena) in se nadaljujejo z vedno bolj splošnimi atributi, ki se pogosto končajo z atributom države. Prva komponenta DN-ja se imenuje relativno razločevalno ime (RDN) in razločuje vnos od vseh drugih vnosov z enakim nadrejenim vnosom. V zgornjem zgledu ločuje RDN ″cn=Bogdan Grabnar″ prvi vnos od drugega vnosa (z RDN-jem ″cn=Lucija Varga″). Sicer pa sta da dva DN-ja enakovredna. Par atribut=vrednost, ki tvori RDN za vnos, mora biti prisoten tudi v vnosu (to ne velja za druge komponente DN-ja).

Postavko za osebo izdelate takole:

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

Pravila za izpustitev znakov v DN-ju

Nekateri znaki imajo v DN-ju poseben pomen. Znak = (enačaj) na primer ločuje ime atributa in vrednost, znak , (vejica) pa ločuje pare atribut=vrednost. Posebni znaki so **,** (vejica), **=** (enačaj), **+** (plus), **<** (manjše kot), **>** (večje kot), # (znak za števila), **;** (podpičje), \ (poševnica nazaj) in **"** (narekovaj, ASCII 34).

V vrednosti atributa lahko posebne znake izpustite, če želite odstraniti poseben pomen. Za izpustitev posebnih znakov ali drugih znakov v vrednosti atributa niza DN uporabite naslednje načine:

1. Če je eden od znakov, ki ga želite izpustiti, posebni znak, pred njega vpišite poševnico nazaj (’\’ ASCII 92). Naslednji zgled kaže, kako lahko izpustite vejico v imenu podjetja:

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

   To je prednostni način.
2. Sicer pa lahko zamenjate znak, ki ga želite izpustiti, tudi s poševnico nazaj in dvema šestnajstiškima številkama, ki tvorita en bajt v kodi znaka. Koda znaka **mora** biti v kodnem naboru UTF-8.

   ```
   CN=L. Eagle,O=Sue\2C Grabbit and Runn,C=GB
   ```
3. Celotno vrednost atributa obdajte z **""** (narekovaji) (ASCII 34), ki niso del vrednosti. Vsi znaki med parom narekovajev, razen \ (poševnice nazaj), so prebrani takšni, kot so. Z znakom \ (poševnica nazaj) lahko izpustite poševnico nazaj (ASCII 92) ali narekovaje (ASCII 34), kateregakoli od predhodno omenjenih posebnih znakov ali šestnajstiške pare kot v drugem načinu. Če želite na primer preskočiti narekovaje v nizu cn=xyz"qrs"abc, uporabite cn=xyz\"qrs\"abc, če pa želite izpustiti \:

   ```
   "na ta način morate izpustiti eno poševnico nazaj \\"
   ```

   Drug zgled "\Zoo" ni veljaven, ker črke ’Z’ v tem kontekstu ni mogoče preskočiti.

Navidezni DN-ji

Navidezni DN-ji se uporabljajo v definiciji in vrednotenju krmiljenja dostopa. Imenik LDAP podpira več navideznih DN-jev (na primer ″group:CN=THIS″ in ″access-id:CN=ANYBODY″), ki se uporabljajo za sklic na večje število DN-jev, ki souporabljajo skupne značilnosti glede na operacijo, ki se izvaja ali objekt, v katerem se operacija izvaja. Dodatne informacije o krmiljenju dostopa boste našli v razdelku “Zaščita imeniškega strežnika” na strani 40.

Trije navidezni DN-ji, ki jih podpira imeniški strežnik:

- access-id: CN=THIS

  Če podate ta DN kot del ACL-ja, se sklicuje na bindDN, ki primerja DN, v katerem izvedete operacijo. Če izvedete operacijo na primer v objektu ″cn=personA, ou=IBM, c=US″ in je bindDn ″cn=personA, ou=IBM, c=US″, so dodeljena pravila, ki so kombinacija tistih, ki so dodeljena ″CN=THIS″ in tistih, ki so dodeljena ″cn=personA, ou=IBM, c=US″.
- group: CN=ANYBODY

  Če podate ta DN kot del ACL-ja, se sklicuje na vse uporabnike, celo na tiste, ki niso overjeni. Uporabnikov iz te skupine ni mogoče odstraniti, te skupine pa ni mogoče odstraniti iz baze podatkov.
- group: CN=AUTHENTICATED

  Ta DN se sklicuje na katerikoli DN, ki ga je overil imenik. Način overjanja ni pomemben.

  Opomba: ″CN=AUTHENTICATED″ se sklicuje na DN, ki je bil overjen kjerkoli v strežniku, ne glede na to, kje se nahaja objekt, ki predstavlja DN. Toda uporabljati ga morate previdno. Pod pripono ″cn=Secret″ je lahko na primer vozlišče, imenovano ″cn=Confidential Material″, ki vsebuje aclentry ″group:CN=AUTHENTICATED:normal:rsc″. Pod drugo pripono ″cn=Common″ je lahko vozlišče ″cn=Public Material″. Če sta ti dve drevesi v enakem strežniku, je povezava s ″cn=Public Material″ smatrana kot overjena in omogoči pravico za normalni razred v objektu ″cn= Confidential Material″.

Nekaj zgledov navideznih DN-jev:

1. zgled

Za objekt razmislite o naslednjem ACL-ju: cn=personA, c=US

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

Uporabnik, ki se povezuje kot	Prejme
cn=personA, c=US	normal:rsc:sensitive:rcs:critical:rwsc
cn=personB, c=US	normal:rsc:sensitive:rsc
Anonymous	normal:rsc

V tem zgledu prejme personA pravico, dodeljeno za ID ″CN=THIS″ in pravice, dodeljene skupinam navideznih DN-jev ″CN=ANYBODY″ in ″CN=AUTHENTICATED″.

2. zgled

Za objekt razmislite o naslednjem ACL-ju: 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 operacijo, izvedeno v cn=personA, c=US:

Uporabnik, ki se povezuje kot	Prejme
cn=personA, c=US	object:ad:critical:rwsc
cn=personB, c=US	normal:rsc:sensitive:rsc
Anonymous	normal:rsc

V tem zgledu prejme personA pravice, dodeljene ID-ju ″CN=THIS″ in tiste, ki so dodeljene samemu

DN-ju″cn=personA, c=US″. Pravice skupine niso dodeljene, ker obstaja bolj specifičen aclentry (″access-id:cn=personA, c=US″) za povezovalni DN (″cn=personA, c=US″).

Izboljšana obdelava DN-jev

Sestavljeni RDN DN-ja je lahko sestavljen iz več komponent, ki jih med seboj povezujejo operatorji ‘+’. Strežnik izboljšuje podporo za iskanje vnosov, ki vsebujejo takšne DN-je. Sestavljeni RDN lahko podate v kakršnemkoli vrstnem redu kot osnovo za iskalno operacijo.

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

Strežnik podpira razširjeno operacijo normalizacije DN-ja. Razširjene operacije normalizacije DN-jev normalizirajo DN-je s strežniško shemo. Ta razširjena operacija je lahko koristna za aplikacije, ki uporabljajo DN-je. Dodatne informacije o razširjenih operacijah boste našli v razdelku “Krmilni elementi in razširjene operacije” na strani 70.

Skladnja razločevalnega imena

Formalna skladnja razločevalnega imena (DN-ja) temelji na RFC-ju 2253. Skladnja BNF (Backus Naur Form) je definirana takole:

```
<name> ::= <name-component> ( <spaced-separator> )
          | <name-component> <spaced-separator> <name>

   <spaced-separator> ::= <optional-space>
                  <separator>
                  <optional-space>

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

   <optional-space> ::= ( <CR> ) *( " " )

   <name-component> ::= <attribute>
           | <attribute> <optional-space> "+"
             <optional-space> <name-component>

   <attribute> ::= <string>
           | <key> <optional-space> "=" <optional-space> <string>

   <key> ::= 1*( <keychar> ) | "OID." <oid> | "oid." <oid>
   <keychar> ::= letters, numbers, and space

   <oid> ::= <digitstring> | <digitstring> "." <oid>
   <digitstring> ::= 1*<digit>
   <digit> ::= digits 0-9

   <string> ::= *( <stringchar> | <pair> )
            | '"' *( <stringchar> | <special> | <pair> ) '"'
            | "#" <hex>


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

   <pair> ::= "\" ( <special> | "\" | '"')
   <stringchar> ::= katerikoli znak, razen <special> ali "\" ali '"'


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

Za ločevanje RDN-jev v razločevalnem imenu lahko uporabite podpičje (;), čeprav se v običajnem zapisu uporablja vejica (,).

Na katerikoli strani vejice ali podpičja so lahko presledki. Presledki so zanemarjeni, podpičje pa je zamenjano z vejico.

Znaki za presledek (’ ’ ASCII 32) so lahko vpisani tudi pred a ’+’ ali ’=’ ali za njima. Ti znaki za presledke so pri razčlenjevanju zanemarjeni.

Naslednji zgled je razločevalno ime v zapisu, primernem za splošne oblike imen. Najprej je vpisano ime, sestavljeno iz treh komponent. Prva komponenta je sestavljeni RDN. Sestavljeni RDN vsebuje več kot en par atribut:vrednost in ga lahko uporabite za jasno določanje specifičnega vnosa v primeru, kjer so podobne vrednosti CN lahko nejasne:

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

Pripona (kontekst poimenovanja)

Pripona (imenovana tudi poimenovalni kontekst) je DN, ki določa zgornji vnos v lokalno hranjeni imeniški hierarhiji. Zaradi relativne poimenovalne sheme, uporabljene v LDAP, je ta DN tudi pripona vseh drugih vnosov v tej imeniški hierarhiji. Imeniški strežnik ima lahko več pripon, od katerih vsaka določa lokalno hranjeno imeniško hierarhijo, kot je na primer o=ibm,c=us.

V imenik je potrebno dodati specifičen vnos, ki se ujema s pripono. Vnos, ki ga izdelate, mora uporabljati objectclass, ki vsebuje uporabljen atribut poimenovanja. Za izdelavo vnosa, ki ustreza tej priponi, lahko uporabite orodje za spletno upravljanje ali pripomoček Qshell ldapadd. Dodatne informacije boste našli v “Upravljanje imeniških vnosov” na strani 129 ali “ldapmodify in ldapadd” na strani 157.

S konceptualnega vidika obstaja globalni imenski prostor LDAP. V globalnem imenskem prostoru LDAP boste lahko našli DN-je, podobne naslednjim:

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

Pripona ″o=IBM″ pove strežniku, da je samo prvi DN imenski prostor, ki ga hrani strežnik. Poskusi sklica na objekte, ki niso znotraj ene od pripon, povzročijo napako, ki sporoči, da takšen objekt ni na voljo, ali sklic na drug imeniški strežnik.

Strežnik ima lahko več pripon. Imeniški strežnik ima več vnaprej definiranih pripon, ki hranijo podatke, specifične za našo izvedbo:

- cn=schema vsebuje shemo, do katere lahko dostopi predstavitev LDAP
- cn=changelog hrani dnevnik sprememb strežnika, če je na voljo
- cn=localhost vsebuje nepodvojene informacije, ki nadzorujejo nekatere vidike delovanja strežnika, kot so na primer konfiguracijski objekti podvajanja
- cn=pwdpolicy vsebuje načelo gesel za ves strežnik
- pripona ″os400-sys=system-name.mydomain.com″ nudi LDAP, do katerega lahko dostopajo objekti i5/OS, ki so trenutno omejeni na uporabniške profile in skupine

Imeniški strežnik je vnaprej konfiguriran s privzeto pripono dc=system-name,dc=domain-name, ki omogoča preprostejše začetno delo s strežnikom. Pripone ni potrebno uporabljati. Dodate lahko lastne pripone ali vnaprej konfigurirano pripono zbrišete.

Za pripone sta na voljo dve splošno uporabljani pravili o poimenovanju. Eno temelji na domeni TCP/IP za vaše podjetje, drugo pa na imenu in mestu podjetja.

Če je vaša domena TCP/IP na primer mycompany.com, lahko izberete pripono, kot je dc=mycompany,dc=com, kjer se atribut dc sklicuje na komponento domene. V tem primeru je vnos zgornje ravni, ki ga izdelate v imeniku, lahko podoben naslednjemu (z uporabo LDIF, besedilnega datotečnega formata za predstavitev vnosov LDAP):

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

Tudi objectclass domain vsebuje nekatere neobvezne atribute, ki jih lahko uporabite. Oglejte si shemo ali uredite izdelan vnos z orodjem za spletno upravljanje in si oglejte dodatne atribute, ki jih lahko uporabite. Dodatne informacije boste našli v “Upravljanje sheme” na strani 119.

Če je ime vašega podjetja My Company in ste iz Združenih držav Amerike, lahko izberete pripono, podobno naslednji:

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

Pri tem je ou ime za organizationalUnit objectclass, o je ime podjetja za organization objectclass, c pa standardna dvomestna okrajšava države, uporabljena za poimenovanje objektnega razreda države. V tem primeru je vnos zgornje ravni, ki ga izdelate, lahko podoben naslednjemu:

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

Aplikacije, ki jih uporabite, lahko zahtevajo, da definirate specifične pripone ali uporabite določeno pravilo o poimenovanju. Če na primer uporabljate imenik za upravljanje digitalnih potrdil, boste morda morali strukturirati del imenika, tako da se bodo imena vnosov ujemala z DN-ji predmetov potrdil, ki jih hrani.

Vnosi, ki jih želite dodati v imenik, morajo imeti pripono, ki se ujema z vrednostjo DN, kot je na primer ou=Marketing,o=ibm,c=us. Če vsebuje poizvedba pripono, ki se ne ujema z nobeno pripono, konfigurirano za lokalno bazo podatkov, je poizvedba usmerjena v strežnik LDAP, ki je določen s privzetim referenčnim kazalcem. Če ni podan noben privzeti referenčni kazalec LDAP, je vrnjen rezultat, ki kaže, da objekt ne obstaja.

Dodatne informacije o tem, kako dodati ali odstraniti pripono, boste našli v razdelku “Dodajanje in odstranjevanje pripon imeniškega strežnika” na strani 98.

Shema

Shema je niz pravil, ki določajo način, na katerega lahko shranite podatke v imeniku. Definira tip dovoljenih vnosov, strukturo njihovih atributov in skladnjo teh atributov.

Podatki so shranjeni v imeniku z imeniškimi vnosi. Vnos je sestavljen iz objektnega razreda, ki je obvezen, in atributov. Atributi so lahko obvezni ali neobvezni. Objektni razred določa vrsto informacij, ki jih opisuje vnos, in definira niz atributov, ki jih vsebuje. Z vsakim atributom je povezana ena ali več vrednosti. Dodatne informacije o upravljanju vnosov boste našli v razdelku “Upravljanje imeniških vnosov” na strani 129.

Dodatne informacije, povezane s shemo, boste našli v naslednjih temah:

IBM Directory Server

IBM Directory Server

Shema za imeniški strežnik je definirana vnaprej, vendar jo lahko spremenite, če imate dodatne zahteve. Dodatne informacije o spreminjanju sheme boste našli v razdelku “Upravljanje sheme” na strani 119.

Imeniški strežnik vključuje podporo za dinamične sheme. Shema je objavljena kot del imeniških informacij in je na voljo v vnosu Subschema (DN=″cn=schema″). Poizvedbo v shemi lahko izvedete z API-jem ldap_search() in jo spremenite z API-jem ldap_modify(). Dodatne informacije o teh API-jih boste našli v temi “API-ji imeniškega strežnika”.

Shema vsebuje več konfiguracijskih informacij, kot jih je bilo vključenih v RFC-je za LDAP različice 3 ali standardne specifikacije. Tako lahko na primer za podan atribut določite, katere indekse je potrebno vzdrževati. Te dodatne konfiguracijske informacije so vzdrževane v vnosu podsheme. Za vnos podsheme IBMsubschema je definiran dodaten objektni razred, ki vsebuje atribute ″MAY″, ki hranijo informacije o razširjeni shemi.

Imeniški strežnik definira eno shemo za celoten strežnik, do katere lahko dostopite prek posebnega imeniškega vnosa ″cn=schema″. Vnos vsebuje celo shemo, definirano za strežnik. Če želite pridobiti informacije o shemi, lahko takole izvedete ldap_search:

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

Shema podaja vrednosti za naslednje tipe atributov:

- objectClasses (dodatne informacije o objectClasses boste našli v “Objektni razredi” na strani 17.)
- attributeTypes (dodatne informacije o attributeTypes boste našli v “Atributi” na strani 19.)
- IBMAttributeTypes (dodatne informacije o IBMAttributeTypes boste našli v “Atribut IBMAttributeTypes” na strani 22.)
- pravila primerjanja (dodatne informacije o pravilih primerjanja boste našli v “Pravila za primerjanje” na strani 22).
- skladnje ldap (dodatne informacije o skladnjah ldap boste našli v “Skladnja atributa” na strani 24).

Skladnja definicij teh shem temelji na RFC-jih za LDAP različice 3.

Vnos vzorčne sheme lahko vsebuje naslednje:

```
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 'Dvojiško' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.7 DESC 'Boolova vrednost' )
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 'Imeniški niz' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.24 DESC 'Splošen čas' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.26 DESC 'Niz IA5' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.27 DESC 'Celo število' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.50 DESC 'Telefonska številka' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.53 DESC 'Čas UTC' )

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 lahko spremenite z API-jem ldap_modify. Dodatne informacije boste našli v temi “API-ji imeniškega strežnika”. Z DN-jem ″cn=schema″ lahko dodate, zbrišete ali zamenjate tip atributa ali objektni razred. Dodatne informacije boste našli v “Dinamična shema” na strani 26 in “Upravljanje sheme” na strani 119. Podate lahko tudi celoten opis. Vnos sheme lahko dodate ali zamenjate z definicijo LDAP različice 3 ali z definicijo pripone IBM-ovega atributa ali z obema definicijama.

Podpora za splošno shemo

IBM Directory podpira standardno imeniško shemo, kot je definirana v naslednjem:

- Internet Engineering Task Force (IETF) RFC-ji za LDAP različice 3 RFCs, kot je na primer RFC 2252 in 2256.
- Directory Enabled Network (DEN)
- Common Information Model (CIM) iz Desktop Management Task Force (DMTF)
- Lightweight Internet Person Schema (LIPS) iz Network Application Consortium

Ta različica LDAP vključuje definirano shemo LDAP različice 3 v privzeti konfiguraciji sheme. Poleg tega vključuje tudi definicije sheme DEN.

IBM nudi tudi niz definicij za razširjene splošne sheme, ki jih souporabljajo drugi IBM-ovi izdelki, ko uporabljajo imenik LDAP. Ti vključujejo naslednje:

- objekte za aplikacije belih strani, kot so oseba, skupina, država, podjetje, organizacijska enota in vloga, mesto itd.
- objekte za druge podsisteme, kot so šifre, storitve in dostopne točke, pooblastila, overjanje, načelo zaščite itd.

Objektni razredi

Objektni razred podaja niz atributov, uporabljenih za opis objekta. Če na primer izdelate objektni razred **tempEmployee**, lahko vsebuje atribute, povezane z začasnim uslužbencem, kot je na primer **idNumber**, **dateOfHire**

ali **assignmentLength**. Dodate lahko tudi prilagojene objektne razrede, ki ustrezajo potrebam vašega podjetja. Shema IBM Directory Server nudi nekaj osnovnih tipov objektnih razredov, vključno z naslednjimi:

- skupine
- mesta
- podjetja
- osebe

Opomba: Objektni razredi, ki so specifični za imeniški strežnik, imajo pripono 'ibm-'.

Objektni razredi so definirani z značilnostmi tipa, nasledstva in atributov.

Tip objektnega razreda

Za objektni razred je lahko uporabljen eden od treh tipov:

Strukturalni:
Vsak vnos mora pripadati samo enemu strukturalnemu objektnemu razredu, ki definira osnovno vsebino vnosa. Ta objektni razred predstavlja realni objekt. Ker morajo vsi vnosi pripadati strukturalnemu objektnemu razredu, je to najpogostejši tip objektnega razreda.

Abstraktni:
Ta tip se uporablja kot nadrejeni razred ali predloga za druge (strukturalne) objektne razrede. Definira niz atributov, ki so skupni nizu strukturalnih objektnih razredov. Če so ti objektni razredi definirani kot podrazredi abstraktnega razreda, nasledijo definirane atribute. Atributov ni potrebno definirati za vsak podrejeni objektni razred.

Pomožni:
Ta tip kaže dodatne atribute, ki jih lahko povežete z vnosom, ki pripada določenemu strukturalnemu objektnemu razredu. Čeprav lahko vnos pripada samo enemu strukturalnemu objektnemu razredu, lahko pripada več pomožnim objektnim razredom.

Nasledstvo objektnega razreda

Ta različica imeniškega strežnika podpira nasledstvo objektov za definicije objektnih razredov in atributov. Nov objektni razred lahko definirate z nadrejenimi razredi (več nasledstev) in z dodatnimi ali spremenjenimi atributi.

Vsak vnos je dodeljen enemu strukturalnemu objektnemu razredu. Vsi objektni razredi nasledijo iz abstraktnega objektnega razreda **top**, vendar pa lahko nasledijo tudi iz drugih objektnih razredov. Struktura objektnega razreda določa seznam obveznih in dovoljenih atributov za določen vnos. Nasledstvo objektnega razreda je odvisno od zaporedja definicij objektnega razreda. Objektni razred lahko nasledi samo iz objektnih razredov, ki so pred njim. Tako je lahko na primer struktura objektnega razreda za vnos osebe definirana v datoteki LDIF takole:

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

V tej strukturi organizationalPerson nasledi iz objektnih razredov person in top, objektni razred person pa samo iz objektnega razreda top. Ko torej dodelite objektni razred organizationalPerson vnosu, ta samodejno nasledi obvezne in dovoljene atribute iz nadrejenega objektnega razreda (ki je v tem primeru objektni razred person).

Preden so operacije ažuriranja sheme obdelane in potrjene, so zaradi skladnosti primerjane z razredno hierarhijo sheme.

Atributi

Vsak objektni razred vključuje številne obvezne in neobvezne atribute. Obvezni atributi so tisti, ki morajo biti prisotni v vnosih, ki uporabljajo objektni razred, neobvezni atributi pa tisti, ki so lahko prisotni v vnosih, ki uporabljajo objektni razred.

Atributi

Z vsakim imeniškim vnosom je prek njegovega objektnega razreda povezan niz atributov. Objektni razred opisuje tip informacij, ki jih vsebuje vnos, toda dejanski podatki so vsebovani v atributih. Atribut je predstavljen z enim ali več pari ime-vrednost, ki hranijo specifičen podatkovni element, kot je na primer ime, naslov ali telefonska številka. Imeniški strežnik predstavi podatke kot pare ime-vrednost, opisne atribute, kot je commonName (cn) in specifičen del informacij, kot je John Doe.

Vnos za John Doe lahko na primer vsebuje več parov ime-vrednost 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
```

Standardni atributi so že definirani v shemi, vendar lahko definicije atributov izdelujete, urejate, kopirate ali brišete, tako kot ustreza podjetju.

Atributi so lahko definirani z eno vrednostjo ali z več vrednostmi. Atributi z več vrednostmi niso urejeni, zato naj aplikacija ne bo odvisna od niza vrednosti za podani atribut, vrnjen v določenem vrstnem redu. Če potrebujete urejen niz vrednosti, uporabite za seznam vrednosti eno vrednost atributa:

```
preferences: 1st-pref 2nd-pref 3rd-pref
```

ali pa vključite v vrednost informacije o vrstnem redu:

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

Atributi z več vrednostmi so koristni, če je vnos znan po več imenih. cn (common name) je na primer vnos z več vrednostmi. Vnos je lahko definiran takole:

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

To pomeni, da bodo iskanja za John Smith in Jack Smith vrnila enake informacije.

Dvojiški atributi vsebujejo poljubni bajtni niz, kot je na primer fotografija JPEG, in jih ni mogoče uporabiti za iskanje vnosov.

Boolovi atributi vsebujejo nize TRUE ali FALSE.

Atributi DN vsebujejo razločevalna imena LDAP. Vrednosti niso nujno DN-ji obstoječih vnosov, vendar morajo uporabljati veljavno skladnjo.

Atributi imeniškega niza vsebujejo besedilni niz, ki uporablja znake UTF-8. Za atribute lahko določite natančno upoštevanje velikih in malih črk ali pa njihovo neupoštevanje glede na vrednosti, uporabljene v iskalnih filtrih (ki temeljijo na pravilu za primerjanje, definiranem za atribut), čeprav je vrednost vedno vrnjena v obliki, v kateri je bila izvorno vnesena.

Atributi splošnega časa vsebujejo nizovno predstavitev varnega datuma in časa za leto 2000 s časom GMT z neobveznim odmikom od časovnega pasu GMT. Dodatne informacije o skladnji teh vrednosti boste našli v razdelku “Splošni čas in čas UTC” na strani 32.

Atributi niza IA5 vsebujejo besedilni niz, ki uporablja nabor znakov IA5 (7-bitni US ASCII). Za atribute lahko določite natančno upoštevanje velikih in malih črk ali pa njihovo neupoštevanje glede na vrednosti, uporabljene v iskalnih filtrih (ki temeljijo na pravilu za primerjanje, definiranem za atribut), čeprav je vrednost vedno vrnjena v obliki, v kateri je bila izvorno vnesena. Niz IA5 omogoča tudi uporabo univerzalnega znaka za iskanja podnizov.

Celoštevilski atributi vsebujejo besedilno predstavitev vrednosti, kot je na primer 0 ali 1000.

Atributi telefonske številke vsebujejo besedilno predstavitev telefonske številke. Imeniški strežnik za te vrednosti ne zahteva nobene posebne skladnje. Sledijo veljavne vrednosti: (555)555-5555, 555.555.5555 in +1 43 555 555 5555.

Atributi časa UTC uporabljajo starejši nizovni format za predstavitev datuma in časa, ki ni prilagojen za leto 2000. Dodatne podatke boste našli v razdelku “Splošni čas in čas UTC” na strani 32.

Dodatne informacije boste našli v naslednjih temah:

- “Splošni elementi podsheme”
- “Atribut objectclass”
- “Atribut attributetypes” na strani 21
- “Atribut IBMAttributeTypes” na strani 22
- “Pravila za primerjanje” na strani 22
- “Pravila indeksiranja” na strani 24
- “Skladnja atributa” na strani 24

Splošni elementi podsheme

Za definiranje slovnice vrednosti atributov podsheme so uporabljeni naslednji elementi:

- 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 ; niz oid-jev katerekoli oblike (številski OID-ji ali imena)
- oids = woid / (″(″ oidlist ″)″)
- oidlist = woid *(″$″ woid) ; deskriptorji objektov, uporabljeni kot imena elementov sheme
- qdescrs = qdescr / (whsp ″(″ qdescrlist ″)″ whsp)
- qdescrlist = [qdescr *(qdescr)]
- whsp ″’″ descr ″’″ whsp

Atribut objectclass

Atribut objectclasses navaja objektne razrede, ki jih podpira strežnik. Vsaka vrednost tega atributa predstavlja ločeno definicijo objektnega razreda. Definicije objektnih razredov lahko dodate, zbrišete ali spremenite, tako da opravite ustrezne popravke v atributu objectclasses vnosa cn=schema. Vrednosti atributa objectclasses uporabljajo naslednjo slovnico, ki jo definira RFC 2252:

```
ObjectClassDescription = "(" whsp
        numericoid whsp ; identifikator Objectclass
        [ "NAME" qdescrs ]
        [ "DESC" qdstring ]
        [ "OBSOLETE" whsp ]
```

```
        [ "SUP" oids ] ; nadrejeni objectclasses
        [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ] ; privzetek je strukturalni
        [ "MUST" oids ] ; AttributeTypes
        [ "MAY" oids ] ; AttributeTypes
        whsp ")"
```

Definicija za objectlass person je na primer takšna:

(2.5.6.6 NAME 'person' DESC 'Definira vnose, ki na splošno predstavljajo osebe.' STRUCTURAL SUP top MUST (cn $ sn) MAY (userPassword $ telephoneNumber $ seeAlso $ description))

- OID za ta razred je 2.5.6.6
- Ime je ″person″
- To je strukturalni objektni razred
- Nasledstvo se izvede iz objektnega razreda ″top″
- Naslednja atributa sta obvezna: cn, sn
- Naslednji atributi so obvezni: userPassword, telephoneNumber, seeAlso, description

Dodatne informacije o tem, kako spremeniti objektne razrede, ki jih podpira strežnik, boste našli v razdelku "Upravljanje sheme" na strani 119.

Atribut attributetypes

Atribut attributetypes navaja atribut, ki ga podpira strežnik. Vsaka vrednost tega atributa predstavlja ločeno definicijo atributa. Definicije atributov lahko dodate, zbrišete ali spremenite z ustreznimi popravki atributa attributetypes vnosa cn=schema. Vrednosti atributa attributetypes uporabljajo naslednjo slovnico, ki jo definira RFC 2252:

```
AttributeTypeDescription = "(" whsp
        numericoid whsp ; identifikator AttributeType
        [ "NAME" qdescrs ] ; ime, uporabljeno v in AttributeType
        [ "DESC" qdstring ] ; opis
        [ "OBSOLETE" whsp ]
        [ "SUP" woid ] ; izhaja iz tega drugega AttributeType
        [ "EQUALITY" woid ; ime pravila za primerjanje
        [ "ORDERING" woid ; ime pravila za primerjanje
        [ "SUBSTR" woid ] ; ime pravila za primerjanje
        [ "SYNTAX" whsp noidlen whsp ]
        [ "SINGLE-VALUE" whsp ] ; privzetek je več vrednosti
        [ "COLLECTIVE" whsp ] ; privzetek je nezdružen
        [ "NO-USER-MODIFICATION" whsp ]; privzetek je uporabniško prilagodljiv
        [ "USAGE" whsp AttributeUsage ]; privzetek je userApplications
         whsp ")"

AttributeUsage =
        "userApplications" /
        "directoryOperation" /
        "distributedOperation" / ; v skupni rabi z DSA
        "dSAOperation" ; specifičen za DSA, vrednost je odvisna od strežnika
```

Za vrednosti pravil za primerjavo in skladnjo morate uporabiti eno od vrednosti, definirano z naslednjim:

- "Pravila za primerjanje" na strani 22
- "Skladnja atributa" na strani 24

V shemi lahko definirate ali spremenite samo atribute ″userApplications″. Atribute ″directoryOperation″, ″distributedOperation″ in ″dSAOperation″ definira strežnik in imajo poseben pomen za delovanje strežnika.

Definicija atributa ″description″ je na primer takšna:

(2.5.4.13 NAME 'description' DESC 'Atribut, skupen CIM in shemi LDAP, da nudi daljši opis vnosa imeniškega objekta.' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications)

- OID je 2.5.4.13
- Ime je ″description″
- Skladnja je 1.3.6.1.4.1.1466.115.121.1.15 (imeniški niz)

Dodatne informacije o tem, kako spremeniti tipe atributov, ki jih podpira strežnik, boste našli v razdelku “Upravljanje sheme” na strani 119.

Atribut IBMAttributeTypes

Z atributom IBMAttributeTypes lahko definirate informacije o shemi, ki niso vključene v standard LDAP različice 3 za atribute. Vrednosti IBMAttributeTypes morajo ustrezati naslednji slovnici:

```
IBMAttributeTypesDescription = "(" whsp
        numericoid whsp
      [ "DBNAME"   qdescrs ]            ; največ dve imeni (tabel, stolpec)
      [ "ACCESS-CLASS" whsp IBMAccessClass whsp ]
      [ "LENGTH" wlen whsp ]            ; najdaljša dolžina atributa
      [ "EQUALITY" [ IBMwlen ] whsp ]   ; izdelava indeksa za pravilo primerjanja
      [ "ORDERING" [ IBMwlen ] whsp ]   ; izdelava indeksa za pravilo primerjanja
      [ "APPROX"   [ IBMwlen ] whsp ]   ; izdelava indeksa za pravilo primerjanja
      [ "SUBSTR"   [ IBMwlen ] whsp ]   ; izdelava indeksa za pravilo primerjanja
      [ "REVERSE"  [ IBMwlen ] whsp ]   ; obratni indeks za podniz
      whsp ")"

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

   IBMwlen = whsp len
```

Numericoid
Uporabljen za korelacijo vrednosti v attributetypes z vrednostjo v IBMAttributeTypes.

DBNAME
Podate lahko največ dve imeni, če sta v resnici določeni dve. Prvo je ime tabele, uporabljene za ta atribut, drugo pa ime stolpca, uporabljenega za v celoti normalizirano vrednost atributa v tabeli. Če podate samo eno ime, je uporabljeno kot ime tabele, kot tudi kot ime stolpca. Če ne podate nobenega DBNAME, je uporabljeno kratko ime atributa (iz attributetypes).

ACCESS-CLASS
Klasifikacija dostopa za ta tip atributa. Če ACCESS-CLASS izpustite, je privzeta vrednost normalen.

LENGTH
Največja dovoljena dolžina tega atributa. Dolžina je izražena s številom bajtov. Imeniški strežnik določa predpis za določanje dolžine atributa. V vrednosti attributetypes lahko uporabite niz

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

da določite, da ima attributetype z oid attr-oid največjo dovoljeno dolžino.

EQUALITY, ORDERING, APPROX, SUBSTR, REVERSE
Če uporabite katerega od teh atributov, je izdelan indeks za ustrezno pravilo primerjanja. Neobvezna dolžina podaja širino indeksiranega stolpca. Za izvedbo več pravil za primerjanje je uporabljen en sam indeks. Če uporabnik ne poda dolžine, dodeli imeniški strežnik dolžino 500. Strežnik lahko uporabi tudi dolžino, krajšo od tiste, ki jo poda uporabnik, če je to ustrezno. Če na primer dolžina indeksa presega največjo dovoljeno dolžino atributa, je dolžina indeksa zanemarjena.

Pravila za primerjanje

Pravilo za primerjanje podaja smernice za primerjavo nizov med iskalno operacijo. Ta pravila so razdeljena v tri kategorije:

- enakost
- ureditev
- podniz

Pravila za primerjavo enakosti		
Pravilo za primerjanje	**OID**	**Skladnja**
caseExactIA5Match	1.3.6.1.4.1.1466.109.114.1	Skladnja imeniškega niza
caseExactMatch	2.5.13.5 IA5	Skladnja niza
caseIgnoreIA5Match	1.3.6.1.4.1.1466.109.114.2	Skladnja niza IA5
caseIgnoreMatch	2.5.13.2	Skladnja imeniškega niza
distinguishedNameMatch	2.5.13.1	DN - razločevalno ime
generalizedTimeMatch	2.5.13.27	Skladnja splošnega časa
ibm-entryUuidMatch	1.3.18.0.2.22.2	Skladnja imeniškega niza
integerFirstComponentMatch	2.5.13.29	Celoštevilska skladnja - integralno število
integerMatch	2.5.13.14	Celoštevilska skladnja - integralno število
objectIdentifierFirstComponentMatch	2.5.13.30	Niz za OID-je, ki vsebujejo. OID je niz, ki vsebuje številke (0-9) in decimalne pike (.).
objectIdentifierMatch	2.5.13.0	Niz za OID-je, ki vsebujejo. OID je niz, ki vsebuje številke (0-9) in decimalne pike (.)
octetStringMatch	2.5.13.17	Skladnja imeniškega niza
telephoneNumberMatch	2.5.13.20	Skladnja telefonske številke
uTCTimeMatch	2.5.13.25	Skladnja časa UTC

Pravila za primerjavo ureditve		
Pravilo za primerjavo	**OID**	**Skladnja**
caseExactOrderingMatch	2.5.13.6	Skladnja imeniškega niza
caseIgnoreOrderingMatch	2.5.13.3	Skladnja imeniškega niza
distinguishedNameOrderingMatch	1.3.18.0.2.4.405	DN - razločevalno ime
generalizedTimeOrderingMatch	2.5.13.28	Skladnja splošnega časa

Pravila za primerjavo podniza		
Pravilo za primerjavo	**OID**	**Skladnja**
caseExactSubstringsMatch	2.5.13.7	Skladnja imeniškega niza
caseIgnoreSubstringsMatch	2.5.13.4	Skladnja imeniškega niza
telephoneNumberSubstringsMatch	2.5.13.21	Skladnja telefonske številke

Opomba: UTC-Time je format časovnega niza, definiran s standardi ASN.1. Glejte ISO 8601 in X680. To skladnjo uporabite za shranjevanje časovnih vrednosti v formatu UTC-Time. Glejte “Splošni čas in čas UTC” na strani 32.

Pravila indeksiranja

Pravila indeksiranja, priključena atributom, omogočajo hitrejše pridobivanje informacij. Če je podan samo atribut, indeksi niso vzdrževani. Imeniški strežnik nudi naslednja pravila indeksiranja:

- enakost
- ureditev
- približen
- podniz
- obraten

Specifikacije pravil indeksiranja za atribute: Z določitvijo indeksirnega pravila za atribut lahko nadzorujete izdelavo in vzdrževanje posebnih indeksov za vrednosti atributov. S tem v veliki meri izboljšate odzivni čas za iskanja s filtri, ki vključujejo te atribute. Z operacijami, uporabljenimi v iskalnem filtru, je povezanih pet možnih vrst pravil za indeksiranje.

Enakost

Velja za naslednje iskalne operacije:

- equalityMatch '='

kot je na primer

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

Ureditev

Velja za naslednjo iskalno operacijo:

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

kot je na primer

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

Približen

Velja za naslednjo iskalno operacijo:

- approxMatch '~='

kot je na primer

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

Podniz Velja za iskalno operacijo, ki uporablja skladnjo podniza:

- substring '*'

kot je na primer

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

Obraten

Velja za naslednjo iskalno operacijo:

- '*' substring

kot je na primer

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

Priporočamo, da podate v atributih, ki bodo uporabljeni v iskalnih filtrih, vsaj indeksiranje po enakosti.

Skladnja atributa

Skladnja atributa definira dovoljene vrednosti za atribut. Strežnik uporablja definicijo skladnje za atribut za preverjanje veljavnosti podatkov in določitev, kako primerjati vrednosti. Atribut ″Boolean″ ima lahko samo vrednosti ″TRUE″ in ″FALSE″.

Skladnja	OID
Skladnja opisa tipa atributa	1.3.6.1.4.1.1466.115.121.1.3
Dvojiški - bajtni niz	1.3.6.1.4.1.1466.115.121.1.5
Boolova vrednost - TRUE/FALSE	1.3.6.1.4.1.1466.115.121.1.7
Skladnja imeniškega niza	1.3.6.1.4.1.1466.115.121.1.15
Skladnja opisa pravila za vsebino DIT	1.3.6.1.4.1.1466.115.121.1.16
Skladnja opisa pravila DITStructure	1.3.6.1.4.1.1466.115.121.1.17
DN - razločevalno ime	1.3.6.1.4.1.1466.115.121.1.12
Skladnja splošnega časa	1.3.6.1.4.1.1466.115.121.1.24
Skladnja niza IA5	1.3.6.1.4.1.1466.115.121.1.26
Opis tipa IBM-ovega atributa	1.3.18.0.2.8.1
Celoštevilska skladnja - integralno število	1.3.6.1.4.1.1466.115.121.1.27
Skladnja opisa skladnje LDAP	1.3.6.1.4.1.1466.115.121.1.54
Opis pravila za primerjanje	1.3.6.1.4.1.1466.115.121.1.30
Opis uporabe pravila za primerjanje	1.3.6.1.4.1.1466.115.121.1.31
Opis imenske oblike	1.3.6.1.4.1.1466.115.121.1.35
Skladnja opisa objektnega razreda	1.3.6.1.4.1.1466.115.121.1.37
Niz za OID-je, ki vsebujejo. OID je niz, ki vsebuje številke (0-9) in decimalne pike (.). Glejte “Identifikator objekta (OID)”.	1.3.6.1.4.1.1466.115.121.1.38
Skladnja telefonske številke	1.3.6.1.4.1.1466.115.121.1.50
Skladnja časa UTC. UTC-Time je format časovnega niza, definiran s standardi ASN.1. Glejte ISO 8601 in X680. To skladnjo uporabite za shranjevanje časovnih vrednosti v formatu UTC-Time. Glejte “Splošni čas in čas UTC” na strani 32.	1.3.6.1.4.1.1466.115.121.1.53

Identifikator objekta (OID)

Identifikator objekta (OID) je niz, sestavljen iz decimalnih števil, ki unikatno določa objekt. Ti objekti so običajno objektni razred ali atribut.

Če nimate OID-ja, lahko določite ime objektnega razreda ali atributa, ki mu priključite **-oid**. Če na primer izdelate atribut tempID, lahko določite OID kot **tempID-oid**.

Izredno pomembno je, da pridobite zasebne OID-je pri zakonitih službah. Zakonite OID-je lahko pridobite na dva osnovna načina:

- z registracijo objektov pri določeni službi; ta način je priročen, če ne potrebujete veliko OID-jev
- s pridobitvijo arc (arc je individualno poddrevo drevesa OID) pri določeni službi in z dodelitvijo lastnih OID-jev po potrebi; ta način je ustreznejši, če potrebujete veliko OID-jev ali če dodelitve OID-jev niso stalne.

ANSI (American National Standards Institute) je registracijska služba za imena podjetij v Združenih državah Amerike, ki deluje v skladu s postopkom globalne registracije, ki sta jo vzpostavili organizaciji ISO (International Standards Organization) in ITU (International Telecommunication Union). Dodatne informacije o registraciji imen podjetij boste našli na spletni strani ANSI  (www.ansi.org). ANSI OID arc za podjetja je 2.16.840.1. ANSI dodeli številko (NEWNUM), ki izdela nov OID arc: 2.16.840.1.NEWNUM.

V večini držav vzdržuje register OID-jev zveza za države standarde. Tako kot velja za ANSI arc, so ti arc-ji običajno dodeljeni pod OID 2.16. Da boste v določeni državi ali okrožju našli službo, pooblaščeno za OID-je, si boste morda

morali vzeti nekaj časa. Organizacija za države standarde v vaši državi je lahko članica ISO. Imena in kontaktne informacije o članicah ISO boste našli na spletni strani ISO  (www.iso.ch).

Služba IANA (Internet Assigned Numbers Authority) dodeli zasebne številke podjetij, ki so OID-ji, v arc-u 1.3.6.1.4.1. IANA dodeli število (NEWNUM), tako da bo novi OID arc 1.3.6.1.4.1.NEWNUM. Ta števila boste našli na spletni strani IANA  (www.iana.org).

Ko je vašemu podjetju dodeljen OID, lahko definirate lastne OID-je z dodajanjem na konec OID-ja. Denimo, da je bil vašemu podjetju dodeljen izmišljeni OID 1.1.1. OID, ki se začne z ″1.1.1″, ne bo dodeljen nobenemu drugemu podjetju. Območje za LDAP lahko izdelate tako, da obliki 1.1.1.1. dodate ″.1″. To lahko nadalje porazdelite v območja za objectclasses (1.1.1.1.1), attribute types (1.1.1.1.2) in tako naprej, in dodelite OID 1.1.1.1.2.34 atributu ″foo″.

Vnosi podsheme

To je en vnos podsheme na strežnik. Vsi vnosi v imeniku imajo vsebovan tip atributa subschemaSubentry. Vrednost tipa atributa subschemaSubentry je DN vnosa podsheme, ki ustreza vnosu. Vsi vnosi pod enim strežnikom souporabljajo enak vnos podsheme in njihov tipa atributa subschemaSubentry ima enako vrednost. Vnos podsheme ima programsko določen DN ’cn=schema’.

Vnos podsheme pripada objektnim razredom ’top’, ’subschema’ in ’IBMsubschema’. Objektni razred ’IBMsubschema’ nima nobenih atributov MUST in en tipi atributa MAY (’IBMattributeTypes’).

Objektni razred IBMsubschema

Objektni razred IBMsubschema se uporablja samo v vnosu podsheme, in sicer takole:

```
( 1.3.18.0.2.6.174
NAME 'ibmSubSchema'
DESC 'IBM-ov specifičen objektni razred, ki hrani vse atribute in objektne razrede za določen imeniški
 strežnik.'
SUP 'subschema'
STRUCTURAL MAY ( IBMAttributeTypes ) )
```

Poizvedbe v shemi

Za poizvedbo v vnosu podsheme lahko uporabite API ldap_search(), kot kaže naslednji zgled:

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

Ta zgled pridobi celotno shemo. Če želite pridobiti vse vrednosti izbranih tipov atributov, uporabite parameter attrs v ldap_search. Specifične vrednosti specifičnega tipa atributa ni mogoče pridobiti.

Dodatne informacije o API-ju ldap_search boste našli v temi “API-ji imeniškega strežnika”.

Dinamična shema

Če želite opraviti spremembo v dinamični shemi, uporabite API ldap_modify z DN-jem ″cn=schema″. Sočasno lahko dodate, zbrišete ali zamenjate samo eno enoto sheme (na primer tip atributa ali objektni razred).

Za brisanje vnosa sheme podajte atribut sheme, ki definira vnos sheme (objectclasses ali attributetypes), za njegovo vrednost pa OID v narekovajih. Takole na primer zbrišete atribut z OID-jem <attr-oid>:

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

Podate lahko tudi celoten opis. V vsakem primeru je pravilo za primerjanje, ki je uporabljeno za iskanje enote sheme za brisanje, objectIdentifierFirstComponentMatch.

Za dodajanje ali zamenjavo enote sheme MORATE podati definicijo LDAP različice 3, IBM-ovo definicijo pa LAHKO podate. V vsakem primeru pa morate podati samo definicijo ali definicije enote sheme, na katere želite vplivati.

Če želite na primer zbrisati tip atributa ’cn’ (njegov OID je 2.5.4.3), takole uporabite ldap_modify():

```
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);
```

Nov tip atributa z OID-jem 20.20.20, ki nasledi iz atributa ″name″ in ima dolžino 20 znakov, dodate takole:

```
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);
```

Različica LDIF zgornjega je takšna:

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

Krmilni elementi za dostop

Spremembe v dinamični shemi lahko izvajate samo z DN-jem oskrbnika podvajanja ali skrbnika.

Podvajanje

Če izvedete spremembo v dinamični shema, je podvojena.

Nedovoljene spremembe sheme

Vse spremembe v shemi niso dovoljene. Omejitve spreminjanja vključujejo naslednje:

- vsaka sprememba, ki jo opravite v shemi, mora pustiti shemo v skladnem stanju
- tipa atributa, ki je nadtip drugega tipa atributa, ni dovoljeno zbrisati; tipa atributa ″MAY″ ali ″MUST″ za objektni razred ni dovoljeno zbrisati
- objektnega razreda, ki je nadrazred drugega razreda, ni dovoljeno zbrisati
- tipov atributov ali objektnih razredov, ki se nanašajo na neobstoječe enote (na primer skladnje ali objektne razrede), ni mogoče dodati
- tipov atributov ali objektnih razredov ni dovoljeno spreminjati na način, ki povzroči, da se sklicujejo na neobstoječe enote (na primer skladnje ali objektne razrede).

Spremembe v shemi, ki vplivajo na delovanje strežnika, niso dovoljene. Imeniški strežnik zahteva naslednje definicije sheme, ki jih ne smete spreminjati.

Objektni razredi:

- 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

Skladnje:
Vse

Pravila za primerjanje:
Vsa

Preverjanje sheme

Ko je strežnik inicializiran, se izvede branje datotek shem in preverjene skladnosti in pravilnosti. Če preverjanje ne uspe, se strežnik ne inicializira in izda sporočilo o napaki. Tudi med spreminjanjem dinamične sheme se izvede preverjanje skladnosti in pravilnosti nastale sheme. Če preverjanje ne uspe, je vrnjena napaka, spreminjanje pa ne uspe. Nekateri deli preverjanja so del slovnice (na primer tip atributa ima lahko največ en nadtip, objektni razred pa kakršnokoli število nadrazredov).

V naslednjih postavkah se izvede preverjanje za tipe atributov:
- dva različna tipa atributov ne moreta imeti enakega imena ali OID-ja
- nasledstvena hierarhija tipov atributov nima ciklusov
- definiran mora biti tudi nadtip tipa atributa, čeprav je njegova definicija lahko prikazana kasneje ali pa v ločeni datoteki
- če je tip atributa nadtip drugega atributa, imata enako uporabo
- skladnja za vse tipe atributov je definirana neposredno ali je podedovana
- z oznako NO-USER-MODIFICATION so lahko označeni samo operacijski atributi.

V naslednjih postavkah se izvede preverjanje za objektne razrede:
- dva različna objektna razreda ne moreta imeti enakega imena ali OID-ja
- nasledstvena hierarhija objektnih razredov nima ciklusov
- definiran mora biti tudi nadrazred objektnega razreda, čeprav je njegova definicija lahko prikazana kasneje ali pa v ločeni datoteki
- definirati morate tudi tipe atributov ″MUST″ in ″MAY″ objektnega razreda, čeprav je njegova definicija lahko prikazana kasneje ali pa v ločeni datoteki
- vsak strukturalni objektni razred je posredni ali neposredni podrazred razreda top
- če ima abstraktni objektni razred nadrazrede, morajo biti abstraktni tudi nadrazredi.

Primerjava vnosa s shemo

Če vnos dodate ali spremenite z operacijo LDAP, je vnos primerjan s shemo. Po privzetku se izvedejo vsa preverjanja, navedena v tem razdelku, vendar pa lahko s spremembo ravni preverjanja sheme onemogočite nekatera od njih. To naredite v Navigatorju iSeries, tako da spremenite vrednost polja **Preverjanje sheme** na strani **Baza podatkov/pripone** v lastnostih imeniškega strežnika. Informacije o konfiguracijskih atributih sheme boste našli v razdelku “Konfiguracijska shema imeniškega strežnika” na strani 184.

Da bi vnos ustrezal shemi, so preverjeni naslednji pogoji:

Glede na objektne razrede:

- imeti morajo vsaj eno vrednost tipa atributa ″objectClass″
- vsebujejo lahko poljubno število pomožnih objektnih razredov, vključno z nič; to ni preverjanje, ampak pojasnilo in te možnosti ne morete onemogočiti
- vsebujejo lahko poljubno število abstraktnih objektnih razredov, vendar samo kot rezultat dedovanja razreda; to pomeni, da ima vnos za vsak abstraktni objektni razred tudi strukturalni ali pomožni objektni razred, ki podeduje posredno ali neposredno iz tega abstraktnega objektnega razreda
- imeti mora vsaj en strukturalni objektni razred
- imeti mora natančno eden najbližji ali osnovni strukturalni objektni razred; to pomeni, da morajo biti vsi strukturalni objektni razredi, ki so na voljo za ta vnos, tudi nadrazredi za natančno enega od njih; večina izpeljanih objektnih razredov se imenuje ″najbližji″ ali ″osnovni strukturalni″ objektni razred vnosa ali preprosto ″strukturalni″ objektni razred vnosa
- najbližjega strukturalnega objektnega razreda ni mogoče spremeniti (v ldap_modify)
- za vsak objektni razred, ki je na voljo za vnos, je izračunan niz vseh njegovih posrednih ali neposrednih podrazredov; če kateri od teh nadrazredov ni vključen v vnos, je samodejno dodan
- če je raven preverjanja sheme nastavljena na **različico 3 (striktna)**, morajo biti podani vsi strukturalni nadrazredi; če želite na primer izdelati vnos z objektnim razredom inetorgperson, morate podati naslednje objektne razrede: person, organizationalperson in inetorgperson.

Veljavnost tipov atributov za vnos je določena takole:

- niz tipov atributov MUST za vnos je izračunan kot zveza nizov tipov atributov MUST vseh njegovih objektnih razredov, vključno z vsebovanimi podedovanimi objektnimi razredi; če niz tipov atributov MUST za vnos ni podniz niza tipov atributov, vsebovanih v vnosu, je vnos zavrnjen
- niz tipov atributov MAY za vnos je izračunan kot zveza nizov tipov atributov MAY vseh njegovih objektnih razredov, vključno z vsebovanimi podedovanimi objektnimi razredi; če niz tipov atributov, vsebovanih v vnosu, ni podniz zveze nizov tipov atributov MUST in MAY za vnos, je vnos zavrnjen
- če je kateri od tipov atributov, definiranih za vnos, označen kot NO-USER-MODIFICATION, je vnos zavrnjen.

Veljavnost vrednosti tipov atributov za vnos je določena takole:

- za vsak tip atributa, vsebovan v vnosu, je vnos zavrnjen, če je tip atributa enojna vrednost, vnos pa ima več kot eno vrednost
- za vsako vrednost atributa vsakega tipa atributa, vsebovanega v vnosu, je vnos zavrnjen, če njegova skladnja ne ustreza rutini za preverjanje skladnje tega atributa
- za vsako vrednost atributa vsakega tipa atributa, vsebovanega v vnosu, je vnos zavrnjen, če je njegova dolžina večja od največje dovoljene dolžine, dodeljene temu atributu.

Veljavnost DN-ja je preverjena takole:

- preverjeno je, ali skladnja ustreza BNF za DistinguishedNames; če ne ustreza, je vnos zavrnjen
- preverjeno je, ali je RDN ustvarjen samo iz tipov atributov, ki so veljavni za ta vnos
- preverjeno je, ali so vrednosti tipov atributov, uporabljene v RDN-ju, na voljo v vnosu.

Združljivost z iPlanet

Razčlenjevalnik, ki ga uporablja imeniški strežnik, omogoča, da podate vrednosti atributov za tipe atributov sheme (objectClasses in attributeTypes) s slovnico iPlanet. Tako lahko na primer podate descrs in numeric-oids z obdajajočimi enojnimi narekovaji (kot če bi bili qdescrs). Toda informacije o shemi so vedno na voljo prek ldap_search. Takoj ko izvedete v vrednosti atributa datoteke eno dinamično spremembo (z ldap_modify), je cela datoteka zamenjana z datoteko, kjer vse vrednosti atributov upoštevajo specifikacije imeniškega strežnika. Ker je razčlenjevalnik, ki je uporabljen v datotekah in v zahtevah ldap_modify, enak, je tudi ldap_modify, ki uporablja slovnico iPlanet za vrednosti atributov, obravnavan pravilno.

Če izvedete poizvedbo v vnosu podsheme strežnika iPlanet, ima lahko nastali vnos več kot eno vrednost za podani OID. Če ima na primer določen tip atributa dve imeni (na primer ’cn’ in ’commonName’), je opis tega tipa atributa podan dvakrat, in sicer enkrat za vsako ime. Imeniški strežnik lahko razčleni shemo, kjer je opis enega tipa atributa ali objektnega razreda prikazan večkrat v enem opisu (razen za NAME in DESCR). Toda ko imeniški strežnik objavi shemo, poda en opis takšnega tipa atributa z vsemi navedenimi imeni (najprej je navedeno kratko ime). iPlanet opiše na primer atribut splošnega imena takole:

```
( 2.5.4.3 NAME 'cn'
  DESC 'Standard Attribute'
   SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

( 2.5.4.3 NAME 'commonName'
  DESC 'Standard Attribute, alias for cn'
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Imeniški strežnik ga opiše takole:

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

Imeniški strežnik podpira podtipe. Če ne želite, da je ’cn’ podtip imena (kar je odklon od standarda), lahko navedete naslednje:

```
( 2.5.4.3 NAME ( 'cn' 'commonName' )
     DESC 'Standard Attribute'
     SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Prvo ime (’cn’) je prednostno ali kratko ime, vsa druga imena za ’cn’ pa so nadomestna imena. Od te točke naprej lahko uporabljate nize ’2.3.4.3’, ’cn’ in ’commonName’ (kot tudi njihove enakovredne vrednosti, ki ne upoštevajo velikih in malih črk) izmenjaje v shemi in za vnose, dodane v imenik.

Splošni čas in čas UTC

Za označitev informacij, povezanih z datumom in časom, obstajajo različni zapisi. Četrti dan februarja v letu 1999 je lahko na primer zapisan takole:

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

kot tudi v številnih drugih zapisih.

Imeniški strežnik standardizira predstavitev časovnega žiga, saj zahteva, da strežniki LDAP podpirajo dve skladnji:

- skladnja splošnega časa, ki ima naslednjo obliko:

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

  Uporabljene so 4 številke za leto, 2 številki za vsak mesec, dan, uro, minuto in sekundo in neobvezen ulomek za sekundo. Brez vseh dodatkov je to datum in čas po lokalni časovni coni. Če želite pokazati, da je čas merjen po usklajenem univerzalnem času (CUT), dodajte času veliko črko Z ali razliko od lokalnega časa, Na primer:

  ```
  "19991106210627.3"
  ```

  ki je po lokalnem času 6 minut, 27.3 sekund čez 21.00 6. novembra 1999.

  ```
  "19991106210627.3Z"
  ```

  ki je usklajeni univerzalni čas.

  ```
  "19991106210627.3-0500"
  ```

  ki je lokalni čas kot v prvem zgledu s peturno razliko glede na usklajeni univerzalni čas.

  Če določite neobvezen ulomek sekunde, morate uporabiti vejico ali piko. Za razliko od lokalnega časa morate pred vrednost za minuto in uro vpisati ’+’ ali ’-’.

- skladnja univerzalnega časa, ki ima naslednjo obliko:
  ```
  LLMMDDHHMM[SS][(+ | -)HHMM)|Z]
  ```

  Uporabljeni sta dve števki za leto, mesec, dan, uro, minuto in neobvezno sekundno polje. Kot v GeneralizedTime, lahko tudi tu podate neobvezno časovno razliko. Če je po lokalnem času na primer dopoldan 2. januarja 1999, čas po usklajenem univerzalnem času pa je 12.00 2. januarja 1999, je vrednost za UTCTime:
  ```
  "9901021200Z"
       ali
  "9901020700-0500"
  ```

  Če je po lokalnem času na primer dopoldne 2. januarja 2001, po usklajenem univerzalnem času pa je 12.00 2. januarja 1001, je vrednost za UTCTime:
  ```
  "0101021200Z"
       ali
  "0101020700-0500"
  ```

  UTCTime omogoča samo dve števki za vrednost leta, zato njegove uporabe ne priporočamo.

Podprti pravilni za primerjanje sta generalizedTimeMatch za enakost in generalizedTimeOrderingMatch za neenakost. Iskanje podnizov ni dovoljeno. Naslednji filtri so na primer veljavni:

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

Naslednji filtri niso veljavni:

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

Objavljanje

i5/OS omogoča sistemu, da objavi določene informacije v imeniku LDAP, kar pomeni, da bo sistem izdelal in ažuriral vnose, ki predstavljajo različne tipe podatkov.

V i5/OS je vgrajena podpora za objavljanje naslednjih informacij v strežniku LDAP:

Uporabniki

Ko konfigurirate sistem i5/OS za objavljanje tipa informacij Uporabniki v imeniškem strežniku, ta samodejno izvozi vnose iz sistemskega razdeljevalnega imenika v imeniški strežnik. V ta namen uporabi vmesnik uporabniškega programa (API) QGLDSSDD. S tem ostane imenik LDAP usklajen s spremembami, ki ste jih naredili v sistemskem razdeljevalnem imeniku. Informacije o API-ju QGLDSSDD boste našli v razdelku teme Programiranje “API-ji imeniškega strežnika”.

Obljavljanje uporabnikov je uporabno za nudenje iskalnega dostopa LDAP do informacij iz sistemskega razdeljevalnega imenika (če želite na primer omogočiti dostop do osebnega imenika LDAP za poštne odjemalce POP3, omogočene za LDAP, kot sta na primer Netscape Communicator ali Microsoft Outlook Express).

Objavljene uporabnike lahko uporabite tudi za nudenje podpore overjanju LDAP z uporabniki, ki so objavljeni iz sistemskega razdeljevalnega imenika in z drugimi uporabniki, ki so dodani v imenik na druge načine. Objavljeni uporabnik ima atribut uid, ki poimenuje profil uporabnika, in nima atributa userPassword. Ko je prejeta povezovalna zahteva za takšen vnos, strežnik pokliče zaščito i5/OS, ki preveri ali sta uid in geslo veljavna za ta profil. O uporabi te možnosti razmislite, če želite uporabljati overjanje LDAP in želite, da bi obstoječi uporabniki i5/OS lahko izvajali overjanje s svojimi gesli i5/OS, uporabniki sistemov ne-i5/OS pa bi bili dodani v imenik ročno.

Sistemske informacije

Če konfigurirate i5/OS za objavljanje tipa informacij Sistem v imeniški strežnik, so objavljeni naslednji tipi informacij:

- osnovne informacije o tem računalniku in izdaji operacijskega sistema
- če želite, lahko izberete enega ali več tiskalnikov za objavljanje; v tem primeru bo sistem samodejno uskladil imenik LDAP s spremembami, opravljenimi v teh tiskalnikih v sistemu.

Informacije, ki jih lahko objavite v zvezi s tiskalniki, so:

- mesto
- hitrost v straneh na minuto
- podpora za dvostransko in barvno tiskanje
- tip in model
- opis

Te informacije se pridobijo iz opisa naprave v sistemu, ki ga objavljate. V omrežnem okolju lahko uporabniki uporabijo te informacije kot pomoč pri izbiri tiskalnika. Informacije so najprej objavljene, ko izberete tiskalnik za objavljanje, in ažurirane, ko zaustavite ali zaženete pisalnik tiskalnika ali spremenite opis tiskalniške naprave.

Tiskalniki v skupni rabi

Če konfigurirate i5/OS za objavljanje tiskalnikov v skupni rabi, so informacije o izbranih tiskalnikih v skupni rabi iSeries Netserver objavljene v konfiguriranem strežniku Active Directory. Z objavljanjem tiskalnikov v skupni rabi na strežniku Active Directory omogočite uporabnikom, da dodajo tiskalnike iSeries na namizje Windows s čarovnikom za dodajanje tiskalnikov, ki je del sistema Windows 2000. Da bi lahko to dejanje opravili s čarovnikom za dodajanje tiskalnikov, določite, da želite najti tiskalnik v Windows 2000 Active Directory. Tiskalnike v skupni rabi morate objaviti v imeniškem strežniku, ki podpira Microsoftovo shemo Active Directory.

TCP/IP Quality of Service

Strežnik TCP/IP Quality of Service (QOS) lahko konfigurirate za uporabljanje načela QOS v skupni rabi, definiranega v imeniku LDAP s shemo, ki jo definira IBM. Strežnik QOS uporablja objavni posrednik TCP/IP QOS za branje informacij o načelih, poleg tega pa definira strežnik, informacije o overjanju in mesto v imeniku, kjer so shranjene informacije o načelih.

Na ta način lahko tudi izdelate aplikacijo za objavljanje ali iskanje drugih vrst informacij v imeniku LDAP, tako da definirate dodatne objavne posrednike in uporabite API-je za objavljanje v imeniku. Dodatne informacije boste našli v razdelku teme Programiranje “API-ji imeniškega strežnika”.

Podvajanje

Podvajanje (replikacija) je tehnika, ki jo uporabljajo imeniški strežniki za izboljšanje zmogljivosti in zanesljivosti. Postopek podvajanja namreč skrbi za usklajenost podatkov v več imenikih.

Informacije o upravljanju podvajanja boste našli v razdelku “Upravljanje podvajanja” na strani 101. Dodatne informacije o podvajanju boste našli v naslednjih temah:

- “Pregled podvajanja” na strani 35
- “Izrazoslovje podvajanja” na strani 36
- “Dogovori o podvajanju” na strani 37
- “Kako so informacije o podvajanju shranjene v strežniku” na strani 38
- “Problematika zaščite za informacije o podvajanju” na strani 38

Pregled podvajanja

Podvajanje nudi dve glavni prednosti:

- Odvečne informacije - dvojniki varujejo vsebino strežnikov, ki jih oskrbujejo.
- Hitrejša iskanja - iskalne zahteve je mogoče razdeliti med več različnih strežnikov z enako vsebino; s tem se izboljša odzivni čas izpolnitve zahteve.

Specifični vnosi v imeniku so z dodatkom objektnega razreda ibm-replicationContext določeni kot izvori podvojenih poddreves. Vsako poddrevo je podvojeno neodvisno. Poddrevo se nadaljuje do imeniškega informacijskega drevesa (DIT), dokler ne doseže imenikov brez podrejenih imenikov ali drugih podvojenih poddreves. Pod koren podvojenega poddrevesa so dodani vnosi, ki vsebujejo informacije o topologiji podvajanja. Ti vnosi so za skupino, sestavljeno iz enega ali več dvojnikov, pod katerimi so izdelani podvnosi dvojnika. Z vsakim podvnosom dvojnika so povezani dogovori o podvajanju, ki določajo strežnike, v katerih izvajajo podvajanje posamezni strežniki, kot tudi definirajo informacije o poverilnicah in urnikih.

Če uporabite podvajanje, se sprememba, ki jo opravite v enem imeniku, razširi v enem ali več dodatnih imenikih. Tako se sprememba v enem imeniku odrazi v več različnih imenikih. IBM Directory podpira razširjeni model podvajanja med glavnimi in podrejenimi strežniki. Topologije podvajanja so razširjene, tako da vključujejo naslednje:

- podvajanje poddreves imeniškega informacijskega drevesa (DIT) v specifične strežnike
- večslojna topologija, imenovana tudi kaskadno podvajanje
- dodelitev strežniške vloge (glavni strežnik ali dvojnik) s poddrevesom
- več glavnih strežnikov, imenovanih podvajanje med enakovrednimi partnerji.

Prednost podvajanja s poddrevesi je, da dvojniku ni treba podvojiti celotnega imenika. Izdelan je lahko dvojnik dela ali poddrevesa imenika.

Razširjeni model spreminja koncept glavnega strežnika in dvojnika. Ta izraza se več ne nanaša na strežnike, pač pa na vloge, ki jih imajo strežniki v zvezi z določenim podvojenim poddrevesom. Strežnik lahko deluje kot glavni strežnik za nekatera poddrevesa in kot dvojnik za druga. Izraz glavni strežnik se uporablja za strežnik, ki sprejema popravke odjemalca za podvojeno poddrevo, izraz dvojnik pa za strežnik, ki samo sprejema popravke iz drugih strežnikov, ki so določeni kot oskrbniki podvojenega poddrevesa.

Glede na funkcijo obstajajo tri vrste imenikov: *glavni/enakovredni*, *kaskadni* in *samo za branje*.

Tabela 1. Strežniške vloge

Imenik	**opis**
Glavni/enakovredni	Glavni/enakovredni strežnik vsebuje informacije o glavnem imeniku, iz katerega so razširjeni popravki v dvojnike. Vse spremembe so izvedene na glavnem strežniku, kjer se tudi odvijajo, glavni strežnik pa je tudi odgovoren za razširjanje teh sprememb v dvojnike. Kot glavni strežnik za imeniške informacije lahko deluje več strežnikov, pri čemer je vsak glavni strežnik odgovoren za ažuriranje drugih glavnih strežnikov in dvojnikov. To se imenuje enakovredno podvajanje, ki lahko izboljša zmogljivost in zanesljivost. Zmogljivost je izboljšana zaradi lokalnega strežnika, ki obravnava popravke v porazdeljenem omrežju, zmogljivost pa zaradi nadomestnega glavnega strežnika, ki v primeru napake v primarnem glavnem strežniku takoj prevzame njegovo vlogo. **Opombe:** 1. Glavni strežniki podvajajo vse odjemalske popravke, ne podvajajo pa popravkov, ki jih prejmejo iz drugih glavnih strežnikov. 2. Popravki v istem vnosu, ki jih opravi več strežnikov, lahko povzročijo neskladja v imeniških podatkih, ker rešitve navzkrižij ni.
Kaskadni (odpošiljanje)	Kaskadni strežnik je strežnik za podvajanje, ki podvoji vse spremembe, ki so mu poslane. Od glavnega/enakovrednega strežnika se razlikuje v tem, da ta podvoji samo spremembe, ki jih opravijo odjemalci, povezani s tem strežnikom. Kaskadni strežnik olajša delo glavnih strežnikov v omrežju, ki vsebujejo veliko razpršenih dvojnikov.

Tabela 1. Strežniške vloge (nadaljevanje)

Imenik	opis
Dvojnik (samo za branje)	Dodatni strežnik, ki vsebuje kopijo imeniških informacij. Dvojniki so kopije glavnega strežnika (ali poddrevesa, katerega dvojnik je). Dvojnik nudi varnostno kopijo za podvojena poddrevesa.

Če podvajanje ne uspe, je ponovljeno, tudi če glavni strežnik zaženete na novo. Neuspelo podvajanje lahko preverite z oknom Upravljanje čakalnih vrst v orodju za spletno upravljanje.

Popravke lahko zahtevate v strežniku za podvajanje, toda popravek je dejansko odposlan glavnemu strežniku z vrnitvijo referenčnega kazalca odjemalcu. Če ažuriranje uspe, pošlje glavni strežnik popravek v dvojnike. Dokler glavni strežnik ne dokonča podvajanja popravka, se sprememba ne odrazi v strežniku za podvajanje, iz katerega je bila izvorno zahtevana. Podvajanje sprememb se izvaja v vrstnem redu, v katerem so bile opravljene v glavnem strežniku.

Če dvojnika ne uporabljate več, morate odstraniti dogovor o podvajanju oskrbnika. Neodstranjena definicija povzroči, da strežnik hrani vse popravke in uporablja nepotreben imeniški prostor, oskrbnik pa še naprej poskuša stopiti v stik z odsotnim potrošnikom, ki mu želi poslati podatke.

Izrazoslovje podvajanja

Sledi izrazoslovje, uporabljeno v opisovanju podvajanja:

Kaskadno podvajanje
Topologija podvajanja, v kateri obstaja več slojev strežnikov. Glavni/enakovredni strežnik izvaja podvajanje v niz strežnikov samo za branje (odpošiljanje), ki v zameno izvedejo podvajanje v druge strežnike. Takšna topologija razbremeni glavne strežnike.

Potrošniški strežnik
Strežnik, ki sprejema zahteva prek podvajanja iz drugega (oskrbniškega) strežnika.

Poverilnice
Določajo način in obvezne informacije, ki jih uporablja oskrbnik pri povezovanju s potrošnikom. Za preproste povezave to vključuje DN in geslo. Poverilnice so shranjene v vnosu, katerega DN je določen v dogovoru o podvajanju.

Strežnik za odpošiljanje
Strežnik samo za branje, ki podvoji vse spremembe, ki mu jih pošlje glavni ali enakovredni strežnik. Zahteve odjemalcev za ažuriranje so poslane glavnemu ali enakovrednemu strežniku.

Glavni strežnik
Strežnik, v katerega je mogoče pisati (ga ažurirati) za podano poddrevo.

Vgnezdeno poddrevo
Poddrevo znotraj podvojenega poddrevesa imenika.

Enakovredni strežnik
Izraz, uporabljen za glavni strežnik, če obstaja za določeno poddrevo več glavnih strežnikov.

Dogovor o podvajanju
Informacije, vsebovane v imeniku, ki definirajo ’povezavo’ ali ’pot podvajanja’ med dvema strežnikoma. Eden od strežnikov se imenuje oskrbnik (tisti, ki pošlje spremembe), drugi pa potrošnik (tisti, ki sprejme spremembe). Dogovor vsebuje vse informacije, potrebne za vzpostavitev povezave od oskrbnika do potrošnika in za načrtovanje podvajanja.

Kontekst podvajanja
Določa koren podvojenega poddrevesa. Vnosu lahko dodate pomožni objektni razred ibm-replicationContext, da označite vnos kot koren podvojenega področja. Informacije, povezane s topologijo podvajanja, so vzdrževane v nizu vnosov, ki so izdelani pod kontekstom podvajanja.

Skupina dvojnikov
Prvi vnos, ki je izdelan pod kontekstom podvajanja, ima objektni razred ibm-replicaGroup in predstavlja

zbirko strežnikov, ki sodelujejo v podvajanju. Kot takšen nudi primerno mesto za nastavitev ACL-jev za zaščito informacij o topologiji podvajanja. Orodja za upravljanje trenutno podpirajo eno skupino dvojnikov pod vsakim kontekstom podvajanja, imenovano **ibm-replicagroup=default**.

Podvnos dvojnika
Pod vnosom skupine dvojnikov lahko izdelate enega ali več vnosov z objektnim razredom ibm-replicaSubentry, in sicer enega za vsak strežnik, ki sodeluje v podvajanju kot oskrbnik. Podvnos dvojnika določa vlogo, ki jo ima strežnik v podvajanju: glavni strežnik ali strežnik samo za branje. Strežnik samo za branje lahko vsebuje dogovore o podvajanju, ki podpirajo kaskadno podvajanje.

Podvojeno poddrevo
Del DIT, ki je podvojen iz enega strežnika v drugega. V tej zasnovi je lahko določeno poddrevo podvojeno v nekaterih strežnikih, v drugih pa ne. V poddrevo določenega strežnika je mogoče pisati, druga poddrevesa pa so lahko samo za branje.

Urnik Izvedbo postopka podvajanja lahko načrtujete ob določeni uri, in sicer tako, da so spremembe oskrbnika združene in poslane v paketu. Dogovor o podvajanju vsebuje DN za vnos, ki oskrbi urnik.

Oskrbniški strežnik
Strežnik, ki pošilja spremembe drugim (potrošniškim) strežnikom.

Dogovori o podvajanju

Dogovor o podvajanju je vnos v imenik z objektnim razredom **ibm-replicationAgreement**, izdelan pod podvnosom dvojnika, da definira podvajanje iz enega strežnika, predstavljeno s podvnosom, v drug strežnik. Ti objekti so podobni vnosom replicaObject, ki so bili uporabljeni v prejšnjih različicah imeniškega strežnika. Dogovor o podvajanju je sestavljen iz naslednjih elementov:

- uporabniku prijazno ime, uporabljeno kot poimenovalni atribut za dogovor
- URL LDAP, ki določa strežnik, številko vrat in ali naj bo uporabljen SSL
- ID potrošniškega strežnika, če je znan; imeniški strežniki pred V5R3 nimajo ID-ja strežnika
- DN objekta s poverilnicami, ki jih uporablja oskrbnik za povezavo s potrošnikom
- neobvezni kazalec DN na objekt, ki vsebuje informacije o urniku podvajanja; če atribut ni prisoten, so spremembe podvojene takoj.

Uporabniku prijazno ime je lahko ime potrošniškega strežnika ali kakšen drug opisni niz.

ID potrošniškega strežnika uporablja upravni GUI za pregled topologije. Če je podan ID potrošniškega strežnika, lahko GUI najde ustrezni podvnos in njegove dogovore. Da bi bili podatki med povezovanjem oskrbnika s potrošnikom čim bolj natančni, pridobi ID strežnika iz korenskega DSE in ga primerja z vrednostjo v dogovoru. Če se ID-ja strežnikov ne ujemata, je zabeleženo opozorilo.

Ker je dogovor o podvajanju mogoče podvojiti, je uporabljen DN za objekt poverilnic, kar omogoča shranjevanje poverilnic v nepodvojeno področje imenika. Podvajanje objektov poverilnic (iz katerih je mogoče pridobiti poverilnice 'clear text') predstavlja možno luknjo v zaščiti. Pripona cn=localhost je ustrezno mesto za izdelovanje objektov poverilnic.

Za vsakega od podprtih načinov overjanja so definirani objektni razredi:

- preprosto povezovanje
- SASL
- mehanizem EXTERNAL s SSL
- overjanje Kerberos

Da določenega dela podvojenega poddrevesa ne želite podvojiti, lahko označite tako, da dodate korenu poddrevesa pomožni razred ibm-replicationContext, ne da bi definirali podvnose dvojnika.

Opomba: V orodju za spletno upravljanje se imenujejo dogovori tudi 'čakalne vrste', če gre za niz sprememb, ki čakajo na podvojitev pod določenim dogovorom.

Kako so informacije o podvajanju shranjene v strežniku

Informacije o podvajanju so shranjene v imeniku na treh mestih:

- V konfiguracija strežnika, ki vsebuje informacije o tem, kako se lahko drugi strežniki overijo za ta strežnik, da lahko izvajajo podvajanje (komu ta strežnik na primer dovoli, da deluje kot oskrbnik).
- V imeniku na vrhu podvojenega poddrevesa. Če je vrh podvojenega poddrevesa ″o=my company″, pod neposredno pod njim izdelan objekt, imenovan ″ibm-replicagroup=default″ (ibm-replicagroup=default,o=my company). Pod objektom ″ibm-replicagroup=default″ bodo dodatni objekti, ki opisujejo strežnike, v katerih so shranjeni dvojniki poddrevesa in dogovori med strežniki.
- Objekt, imenovan ″cn=replication,cn=localhost″, vsebuje informacije o podvajanju, ki jih uporablja samo en strežnik. Objekt, ki vsebuje poverilnice, ki jih uporablja oskrbniški strežnik, na primer potrebuje samo oskrbniški strežnik. Poverilnice lahko shranite pod ″cn=replication,cn=localhost″, da lahko do njih dostopa samo ta strežnik.

Problematika zaščite za informacije o podvajanju

Preglejte problematiko zaščite za naslednje objekte:

- ibm-replicagroup=default: krmilni elementi dostopa za ta objekt krmilijo, kdo si lahko ogleda ali spremeni informacije o podvajanju, shranjene tu. Po privzetku nasledi ta objekt krmilni element dostopa od svojega nadrejenega objekta. Krmilni element dostopa za ta objekt je dobro nastaviti tako, da omejuje dostop do informacij o podvajanju. Definirate lahko na primer skupino z uporabniki, ki bodo upravljali podvajanje. Ta skupina je lahko lastnik objekta ″ibm-replicagroup=default″, drugi uporabniki pa nimajo dostopa do tega objekta.
- cn=replication,cn=localhost: s tem objektom sta povezani dve vprašanji zaščite:
  - Krmilni element dostopa za ta objekt krmili, kdo si lahko ogleda ali ažurira objekte, shranjene tu. Privzeti krmilni element dostopa omogoča, da anonimni uporabniki preberejo večino informacij, razen gesel, in zahteva za dodajanje, spreminjanje ali brisanje objektov pooblastilo skrbnika.
  - Objekti, ki so shranjeni v ″cn=localhost″, niso nikoli podvojeni v druge strežnike. Poverilnice podvajanja lahko shranite v ta vsebnik na strežniku, ki uporablja poverilnice, saj tu do njih ne morejo dostopati drugi strežniki. Poverilnice lahko shranite tudi v objekt ″ibm-replicagroup=default″, tako da uporablja iste poverilnice več strežnikov.

Področja in uporabniške predloge

Objekti področij in predlog v orodju za spletno upravljanje se uporabljajo, da uporabniku ni potrebno razumeti nekaterih stvari v zvezi z LDAP.

Področja določa zbirko uporabnikov in skupin. Informacije podaja v jasni imeniški strukturi, kot so informacije o tem, kjer se nahajajo uporabniki in kje skupine. Področje definira mesto uporabnikov (na primer ″cn=users,o=acme,c=us″) in izdela uporabnike kot neposredno podrejene uporabnike tega vnosa (John Doe je na primer izdelan kot ″cn=John Doe,cn=users,o=acme,c=us″). Definirate lahko več področij, ki jim dodelite vsakdanja imena (na primer spletni uporabniki). Vsakdanje ime lahko uporabljajo tisti, ki izdelujejo in vzdržujejo uporabnike.

Predloga opisuje, kakšen je uporabnik, in podaja objektne razrede, uporabljene pri izdelovanju uporabnikov (strukturalne objektne razrede in vse želene podrejene razrede). Določa tudi postavitev oken, uporabljenih za izdelovanje ali urejanje uporabnikov (kot so na primer imena jezičkov, privzete vrednosti in atributi, ki so prikazani na vsakem jezičku).

Če dodate novo področje, izdelate v imeniku objekt ibm-realm. Le-ta sledi lastnostim področja, kot je na primer, kje so definirani uporabniki in skupine ter katero predlogo uporabiti. Objekt ibm-realm lahko kaže na obstoječi imeniški vnos, ki je nadrejen za uporabnika, ali pa na samega nase (privzetek), kar pomeni, da je na voljo kot vsebnik za nove uporabnike. Tako imate lahko na primer obstoječi vsebnik cn=users,o=acme,c=us in izdelate kjerkoli v imeniku (na primer v objektu vsebnika, imenovanem cn=realms,cn=admin stuff,o=acme,c=us) področje, imenovano uporabniki, ki določa cn=users,o=acme,c=us kot mesto za uporabnike in skupine. S tem izdelate objekt ibm-realm:

```
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: uporabniki
```

Če objekt cn=users,o=acme,c=us object na primer ne obstaja, lahko izdelate področje uporabniki pod o=acme,c=us, ki kaže samo nase.

Za upravljanje uporabniških predlog, področij in skupin skrbnikov področij je odgovoren skrbnik imenika. Ko je področje izdelano, so za upravljanje uporabnikov in skupin v tem področju odgovorni člani skupine skrbnikov področja.

Dodatne informacije o upravljanju področij in uporabniških predlog boste našli v “Upravljanje področij in uporabniških predlog” na strani 138.

Problematika podpore za državne jezike (NLS)

Upoštevati morate naslednjo problematiko, povezano z NLS:
- Podatki med strežniki in odjemalci LDAP se prenesejo v obliki UTF-8. Dovoljeni so vsi znaki ISO 10646.
- Imeniški strežnik uporablja za shranjevanje podatkov v bazi podatkov način preslikave UTF-16.
- Strežnik in odjemalec izvajata primerjave nizov, ki niso občutljive na velikost znakov. Algoritmi za velike črke ne bodo pravilni za vse jezike (državne nastavitve).

Dodatne informacije o UCS-2 boste našli v razdelku “Globalizacija” teme Načrtovanje.

Referenčni kazalci imenika LDAP

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

Imeniški strežnik omogoča uporabo dveh tipov referenčnih kazalcev. Podate lahko privzete strežnike referenčnih kazalcev, na katere bo napotil strežnik LDAP odjemalce, če katerikoli DN ni na voljo v imeniku. Za dodajanje vnosov v imeniški strežnik, ki uporablja referenčni kazalec objectClass, lahko uporabite tudi odjemalca LDAP. S tem lahko podate referenčne kazalce, ki temeljijo na zahtevah odjemalcev za specifične DN.

Opomba: V imeniškem strežniku morajo vsebovati objekti referenčnih kazalcev samo atribute razločevalnega imena (dn), objektnega razreda (objectClass) in referenčnega kazalca (ref). V razdelku “ldapsearch” na strani 169 boste našli zgled, ki kaže to omejitev.

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

Transakcije

Imeniški strežnik lahko konfigurirate tako, da odjemalcem omogoča uporabo transakcij. (Dodatne informacije o konfiguriranju transakcijskih nastavitev boste našli v razdelku “Določitev nastavitev za transakcije” na strani 95.) Transakcija je skupina operacij imenika LDAP, obravnavanih kot ena enota. Nobena izmed posameznih operacij LDAP, ki sestavljajo transakcijo, ne bo dokončna, dokler se uspešno ne zaključijo vse operacije v transakciji in je le-ta odobrena. Če katera izmed operacij ne uspe ali pa je transakcija prekinjena, bodo druge operacije razveljavljene. S pomočjo te zmožnosti lahko uporabniki ohranijo razvrstitev operacij LDAP. Uporabnik želi na primer v svojem odjemalcu nastaviti transakcijo, ki bo zbrisala nekaj vnosov v imenik. Če se povezava med odjemalcem in strežnikom med transakcijo prekine, vnosi ne bodo zbrisani. Zato lahko uporabnik transakcijo preprosto še enkrat zažene in mu ni treba preverjati, kateri vnosi so bili uspešno zbrisani.

Del transakcije so lahko naslednje operacije LDAP:

- dodajanje
- spreminjanje
- spreminjanje RDN
- brisanje

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

Zaščita imeniškega strežnika

Dodatne informacije o zaščiti imeniškega strežnika boste našli v naslednjih temah:

- "Beleženje"
- "Plast zaščitenih vtičnic (SSL) in zaščita plasti prenosa z imeniškim strežnikom"
- "Overjanje Kerberos z imeniškim strežnikom" na strani 41)
- "Skupine in vloge" na strani 41
- "Seznami za nadzor dostopa" na strani 47
- "Lastništvo objektov imenika LDAP" na strani 58
- "Načelo gesel" na strani 58
- "Overjanje" na strani 61

Beleženje

Imeniški strežnik podpira beleženje zaščite OS/400. Beležene postavke so lahko naslednje:

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

Pred začetkom delovanja beleženja vnosov v imenik boste morda morali spremeniti določene nastavitve v beleženju i5/OS. Če ste za sistemsko vrednost QAUDCTL podali *OBJAUD, lahko beleženje objektov omogočite prek

Navigatorja iSeries. Dodatne informacije boste našli v priročniku *Security - Reference*  ali v temi "Beleženje zaščite".

Plast zaščitenih vtičnic (SSL) in zaščita plasti prenosa z imeniškim strežnikom

Da bi bile komunikacije z imeniškem strežnikom bolj varne, lahko le-ta uporabi zaščito plasti zaščitenih vtičnic (SSL).

Za uporabo zaščite SSL z imeniškim strežnikom morate imeti v sistemu nameščenega enega od izdelkov ponudnikov šifriranega dostopa (5722-ACx). Če želite SSL uporabiti iz Navigatorja iSeries, morate imeti v PC-ju nameščenega enega od izdelkov za šifriranje odjemalca (5722-CEx). To programsko opremo potrebujete, če želite storiti karkoli od naslednjega:

- Konfigurirati in upravljati imeniški strežnik iz delovne postaje z uporabo povezave SSL. To vključuje opravila, ki jih izvajate v Navigatorju iSeries.
- Uporabljati povezavo SSL z aplikacijami, ki jih izdelate z vmesniki uporabniških programov (API-ji) odjemalca LDAP.

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

Za uporabo zaščite SSL morate imeti v sistemu nameščen Upravljalnik digitalnih potrdil (DCM), možnost i5/OS 34. DCM nudi vmesnik, s katerim lahko izdelate in upravljate digitalna potrdila in prostore za potrdila. Informacije o digitalnih potrdilih in uporabi DCM-ja boste našli v temi “Upravljalnik digitalnih potrdil”. Informacije o zaščiti SSL v iSeries boste našli v temi “Plast zaščitenih vtičnic (SSL)”. Če želite informacije o TLS v strežniku iSeries, preglejte razdelek Podprti protokoli SSL in zaščita plasti prenosa(TLS).

Overjanje Kerberos z imeniškim strežnikom

Imeniški strežnik omogoča uporabo overjanja Kerberos. Kerberos je omrežni protokol za overjanje, ki z uporabo tajnopisja tajnega ključa za odjemalsko strežniške aplikacije nudi močno overjanje.

Če želite omogočiti overjanje Kerberos, morate imeti v sistemu nameščenega enega izmed izdelkov ponudnika šifriranega dostopa (5722AC2 ali 5722AC3), konfigurirati pa morate tudi omrežno storitev overjanja.

Podpora imeniškega strežnika za overjanje Kerberos nudi podporo za mehanizem SSL GSSAPI. S tem je tako imeniškemu strežniku, kot tudi odjemalcem LDAP Windows 2000, omogočena uporaba overjanja Kerberos z imeniškim strežnikom.

Ime principala Kerberos, ki ga uporablja strežnik, ima naslednjo obliko:

```
storitveno-ime/ime-gostitelja@področje
```

storitveno-ime je ldap (ldap mora biti izpisan z malimi črkami), ime-gostitelja je celotno ime TCP/IP sistema, področje pa je privzeto področje, podano v konfiguraciji Kerberos sistemov.

Za sistem, imenovan my-as400, v domeni TCP/IP acme.com, ki uporablja privzeto področje Kerberos ACME.COM, bi se ime principala Kerberos za strežnik LDAP glasilo takole: ldap/my-as400.acme.com@ACME.COM. Privzeto področje Kerberos je podano v konfiguracijski datoteki Kerberos (po privzetku /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) s smernico privzeto_področje (privzeto_področje = ACME.COM). Če ne konfigurirate privzetega področja, imeniškega strežnika ni mogoče konfigurirati za overjanje Kerberos.

Če uporabite overjanje Kerberos, imeniški strežnik poveže razločevalno ime (DN) s povezavo, ki določi dostop do imeniških podatkov. DN strežnika lahko povežete z eno izmed naslednjih metod:

- Strežnik lahko izdela DN na osnovi ID-ja Kerberos. Če izberete to možnost, bo identiteta Kerberos oblike principal@področje izdelala DN oblike ibm-kn=principal@področje. ibm-kn= je enakovredno ibm-kerberosName=.
- Strežnik lahko v imeniku poišče razločevalno ime (DN), ki vsebuje vnos za osnovno ime in področje Kerberos. Če izberete to možnost, strežnik poišče v imeniku vnos, ki podajo to identiteto Kerberos.

Imeti morate datoteko s tabelo ključev (keytab), ki vsebuje ključ za osnovno ime storitve LDAP. Preglejte temo Informacijskega centra Omrežna storitev overjanja pod Zaščita, če želite podrobnejše informacije o Kerberosu na strežniku iSeries. V razdelku Konfiguriranje omrežne storitve overjanja boste našli podatke o dodajanju informacij v datoteke tabele ključev.

Skupine in vloge

Skupina je seznam ali zbirka imen. Uporabite jo lahko v atributih **aclentry**, **ibm-fliterAclEntry** in **entryowner** za krmiljenje dostopa ali za specifično uporabo aplikacij, kot je na primer seznam za razpošiljanje pošte; glejte “Seznami za nadzor dostopa” na strani 47. Skupine so lahko statične, dinamične ali vgnezdene. Informacije o delu s skupinami boste našli v razdelku “Upravljanje uporabnikov in skupin” na strani 135.

Vloge so podobne skupinam v tem, da so predstavljene v imeniku z objektom. Poleg tega vsebujejo vloge skupino DN-jev.

Dodatne informacije boste našli v naslednjih temah:

- "Statične skupine"
- "Dinamične skupine"
- "Vgnezdene skupine" na strani 43
- "Mešane skupine" na strani 44
- "Določanje članstva v skupini" na strani 44
- "Objektni razredi skupine za vgnezdene in dinamične skupine" na strani 46
- "Tipi atributov skupine" na strani 46
- "Vloge" na strani 47

Statične skupine

Statična skupina definira vsakega člana posamično, in sicer s strukturalnim objektnim razredom **groupOfNames**, **groupOfUniqueNames**, **accessGroup** ali **accessRole** ali s pomožnim objektnim razredom **ibm-staticgroup**. Ti objektni razredi zahtevajo atribut **member** (ali uniqueMember v primeru groupOfUniqueNames). Statična skupina, ki uporablja strukturalne objektne razrede **groupOfNames** ali **groupOfUniqueNames**, mora imeti vsaj enega člana. Skupina, ki uporablja strukturalne objektne razrede **accessGroup** ali **accessRole**, je lahko prazna. Statično skupino lahko definirate tudi s pomožnimi objektnimi razredi **ibm-staticGroup**, ki ne zahtevajo atributa **member** in so lahko zato prazni.

Značilen vnos skupine je takšen:

```
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
```

Vsak objekt skupine vsebuje atribut iz več vrednosti, ki je sestavljen iz DN-jev članov.

Če zbrišete skupino dostopa, je le-ta zbrisana iz vseh ACL-jev, v katerih je bila uporabljena.

Dinamične skupine

Dinamična skupina definira svoje člane drugače kot statična. Namesto da bi jih izpisala posamično, jih definira z iskanjem v LDAP. Dinamična skupina uporablja strukturalni objektni razred **groupOfURLs** (ali pomožni objektni razred **ibm-dynamicGroup**) in atribut **memberURL**, da definira iskanje s preprosto skladnjo URL-ja LDAP.

```
ldap:///<osnovni DN iskanja> ? ? <območje iskanja> ? <iskalni-filter>
```

Opomba: Kot kaže zgled, skladnja ne sme vsebovati imena gostitelja. Preostali parametri so podobni kot v običajni skladnji URL-ja LDAP. Vsako parametersko polje mora biti ločeno z znakom ?, čeprav ne podate nobenega parametra. Običajno bo seznam atributov za vrnitev vključen med osnovni DN in območje iskanja. Strežnik tega parametra ne uporabi pri določanju dinamičnega članstva, zato ga lahko izpustite, toda ločilo **?** mora biti kljub temo vpisano.

kjer je:

osnovni DN iskanja
: točka, na kateri se začne iskanje v imeniku; to je lahko pripona ali koren imenika, kot je na primer **ou=Austin**; ta parameter je obvezen

območje iskanja
: podaja obseg iskanja; privzeto območje je osnovno

  osnovni
  : vrne informacije samo o osnovnem DN-ju, ki je podan v URL-ju

ena vrne informacije o vnosih, ki so eno raven pod osnovnim DN-jem, podanim v URL-ju; osnovni vnos ni vključen

nižje vrne informacije o vnosih na vseh nižjih raven in vključuje osnovni DN

iskalni-filter
je filter, ki ga želite uporabiti za vnose v območju iskanja; dodatne informacije o skladnji iskalnega filtra boste našli v razdelku "možnost filtra ldapsearch" na strani 172; privzetek je objectclass=*

Iskanje dinamičnih članov se vedno izvaja notranje v strežniku, zato za razliko od celotnega URL-ja ldap nista ime gostitelja in številka vrat nikoli podana, protokol pa je vedno **ldap** (nikoli ni **ldaps**). Atribut **memberURL** lahko vsebuje kakršnokoli vrsto URL-ja, toda strežnik uporabi za določanje dinamičnega članstva samo tiste **memberURL**-je, ki se začno z **ldap:**///.

Primeri

En vnos, v katerem je privzeta vrednost za območje osnovno, privzeta vrednost za filter pa objectclass=*:

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

Vsi vnosi, ki so eno raven pod cn=Employees in filter, po privzetku uporabljajo objectclass=*:

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

Vsi vnosi, ki so pod o-Acme z objectclass=person:

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

Odvisno od objektnih razredov, ki jih uporabite za definiranje uporabniških vnosov, ti vnosi morda ne bodo vsebovali atributov, ki so primerni za določanje članstva v skupini. Za razširitev uporabniških vnosov, tako da bodo vključevali atribut **ibm-group**, lahko uporabite pomožni objektni razred **ibm-dynamicMember**. Ta atribut omogoča, da dodate uporabniškim vnosom poljubne vrednosti, ki služijo kot cilji za filtre dinamičnih skupin. Na primer:

Člani te dinamične skupine so vnosi, ki so neposredno pod vnosom cn=users,ou=Austin, ki uporablja atribut ibm-group GROUP1:

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

Sledi vzorčni član za cn=GROUP1,ou=Austin:

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

Vgnezdene skupine

Gnezdenje skupin omogoča izdelavo hierarhičnih odnosov, s katerimi lahko definirate podedovano članstvo v skupini. Vgnezdena skupina je definirana kot vnos podrejene skupine, na katere DN se sklicuje atribut, vsebovan v vnosu nadrejene skupine. Nadrejeno skupino izdelate z razširitvijo enega od objektnih razredov strukturalne skupine (**groupOfNames**, **groupOfUniqueNames**, **accessGroup**, **accessRole** ali **groupOfURLs**) z dodatkom pomožnega objektnega razreda **ibm-nestedGroup**. Po razširitvi vgnezdene skupine lahko dodate nič ali več atributov **ibm-memberGroup**, katerih vrednosti so nastavljene na DN-je vgnezdenih podrejenih skupin. Na primer:

```
dn: cn=Group 2, cn=Groups, o=IBM, c=US
 objectclass: groupOfNames
 objectclass: ibm-nestedGroup
 objectclass: top
 cn: Group 2
 description: skupina, sestavljena iz statičnih in vgnezdenih članov
```

```
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
```

Vpeljava ciklusov v hierarhijo vgnezdene skupine ni dovoljena. Če je določeno, da povzroči operacija v vgnezdeni skupini ciklično referenco, in sicer neposredno ali prek nasledstva, gre za kršitev omejitve, zato ažuriranje vnosa ne uspe.

Mešane skupine

Vse objektne razrede strukturalne skupine lahko razširite tako, da je članstvo v skupini opisano s kombinacijo tipov statičnih, dinamičnih in vgnezdenih članov. Na primer:

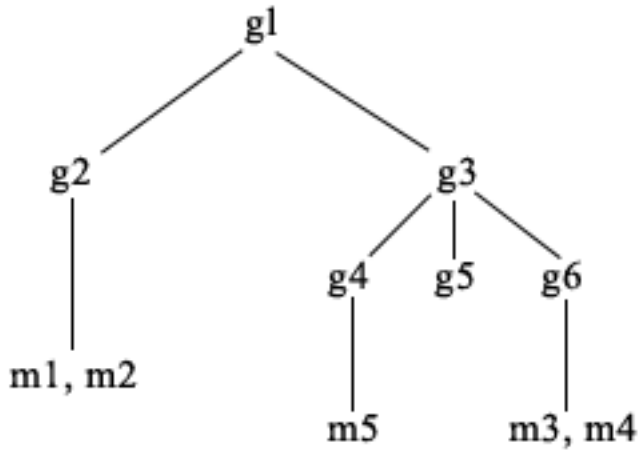
```
dn: cn=Group 10, cn=Groups, o=IBM, c=US
objectclass: groupOfURLs
objectclass: ibm-nestedGroup
objectclass: ibm-staticGroup
objectclass: top
cn: Group 10
description: skupina, sestavljena iz statičnih, dinamičnih in vgnezdenih članov
memberURL: ldap:///cn=Austin, cn=Employees, o=IBM, c=US??one?objectClass=person
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
```

Določanje članstva v skupini

Za poizvedbo o članstvu v združeni skupini lahko uporabita dva operacijska atributa. Za vnos določene skupine operacijski atribut **ibm-allMembers** prešteje združen niz članstev v skupini, vključno s statičnimi, dinamičnimi in vgnezdenimi člani, kot opisuje hierarhija vgnezdene skupine. Za vnos določenega uporabnika operacijski atribut **ibm-allGroups** prešteje združen niz skupin, vključno s prvotnimi skupinami, v katerih ima uporabnik članstvo.

Zahtevnik lahko prejme samo podniz skupno zahtevanih podatkov, odvisno od tega, kako so ACL-ji nastavljeni za podatke. Operacijska atributa **ibm-allMembers** in **ibm-allGroups** lahko zahteva kdorkoli, toda vrnjeni niz podatkov vsebuje samo podatke za vnose LDAP in atribute, do katerih lahko dostopa zahtevnik. Uporabnik, ki zahteva atribut **ibm-allMembers** ali **ibm-allGroups**, mora imeti dostop do vrednosti atributov **member** ali **uniquemember** za skupino in vgnezdene skupine, da lahko vidi statične člane, in zmožnost za izvedbo iskanj, podanih v vrednostih atributa **memberURL**, da lahko vidi dinamične člane. Na primer:

Zgledi hierarhije



Za ta zgled sta **m1** in **m2** v atributu member **g2**. ACL za **g2** omogoča, da **user1** prebere atribut member, toda **user 2** nima dostopa do atributa member. LDIF vnosa za vnos **g2** je takšen:

```
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
```

Vnos **g4** uporablja privzeti aclentry, ki omogoča, da tako **user1**, kot tudi **user2** prebereta njegov atribut member. LDIF za vnos **g4** je takšen:

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

Vnos **g5** je dinamična skupina, ki pridobi svoja dva člana iz atributa memberURL. LDIF za vnos **g5** je takšen:

```
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))
```

Vnosa **m3** in **m4** sta člana skupine **g5**, ker ustrezata **memberURL**. ACL za vnos **m3** omogoča, da ga iščeta tako **user1**, kot tudi **user2**. ACL za vnose **m4** ne omogoča, da ga išče **user2**. LDIF za **m4** je takšen:

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

1. zgled:

User 1 izvede iskanje, da poišče vse člane skupine **g1**. User 1 ima dostop do vseh članov, zato so vrnjeni vsi.

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


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

2. zgled:

User 2 izvede iskanje, da poišče vse člane skupine **g1**. User 2 nima dostopa do članov **m1** ali **m2**, ker nimata dostopa do atributa member za skupino **g2**. User 2 ima dostop do atributa member za **g4**, zato ima dostop do člana **m5**. User 2 lahko izvede iskanje v skupini **g5** memberURL za vnos **m3**, zato je ta član izpisan, toda iskanja za **m4** ne more izvesti.

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


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

3. zgled:

User 2 izvede iskanje, da ugotovi, ali je **m3** član skupine **g1**. User 2 ima dostop do izvedbo tega iskanja, zato iskanje pokaže, da je **m3** član skupine **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
```

4. zgled:

User 2 izvede iskanje, da vidi, ali je **m1** član skupine **g1**. User 2 nima dostopa do atributa member, zato iskanje ne pokaže, da je **m1** član skupine **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
```

Objektni razredi skupine za vgnezdene in dinamične skupine

ibm-dynamicGroup

Ta pomožni razred omogoča uporabo neobveznega atributa **memberURL**. Uporabite ga s strukturalnim razredom **groupOfNames** za izdelavo mešane skupine, ki vsebuje statične in dinamične člane.

ibm-dynamicMember

Ta pomožni razred omogoča uporabo obveznega atributa **ibm-group**. Uporabite ga kot atribut filtra za dinamične skupine.

ibm-nestedGroup

Ta pomožni razred omogoča uporabo neobveznega atributa **ibm-memberGroup**. Uporabite ga s strukturalnim razredom, kot je **groupOfNames**, da omogočite vgnezdenje podskupin znotraj nadrejene skupine.

ibm-staticGroup

Ta pomožni razred omogoča uporabo neobveznega atributa **member**. Uporabite ga s strukturalnim razredom **groupOfURLs** za izdelavo mešane skupine, ki vsebuje statične in dinamične člane.

Opomba: **ibm-staticGroup** je edini razred, za katerega je **član** *neobvezen*; vsi drugi razredi, ki uporabljajo atribut **member**, morajo imeti vsaj enega člana.

Tipi atributov skupine

ibm-allGroups

Prikaže skupino, v katero spada vnos. Vnos je lahko član neposredno z atributi **member**, **uniqueMember** ali **memberURL**, ali neposredno z atributom **ibm-memberGroup**. To je operacijski atribut **samo za branje**, ki ni dovoljen v iskalnem filtru. Atribut **ibm-allGroups** lahko uporabite v primerjalni zahtevi, da določite, ali je vnos član določene skupine. Takole na primer določite, ali je ″cn=john smith,cn=users,o=my company″ član skupine ″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

Prikaže vse člane v skupini. Vnos je lahko član neposredno z atributi **member**, **uniqueMember** ali **memberURL**, ali neposredno z atributom **ibm-memberGroup**. To je operacijski atribut **samo za branje**, ki ni dovoljen v iskalnem filtru. Atribut **ibm-allMembers** lahko uporabite v primerjalni zahtevi, da določite, ali je DN član določene skupine. Takole na primer določite, ali je ″cn=john smith,cn=users,o=my company″ član skupine ″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

To je atribut, ki ga uporablja pomožni razred **ibm-dynamicMember**. Z njim lahko definirate poljubne vrednosti, ki krmilijo članstvo vnosa v dinamičnih skupinah. Dodajte na primer vrednost ″Bowling Team″, tako da bo vključevala vnos v kateremkoli **memberURL**, ki uporablja filter ″ibm-group=Bowling Team″.

ibm-memberGroup
To je atribut, ki ga uporablja pomožni razred **ibm-nestedGroup**, in določa podskupine vnosa nadrejene skupine. Člani vseh takšnih podskupin so člani nadrejene skupine pri obdelavi vseh takšnih ACL-jev ali operacijskih atributov **ibm-allMembers** in **ibm-allGroups**. Sami vnosi podskupine *niso* člani. Vgnezdeno članstvo je rekurzivno.

member
Določa razločevalna imena za člane skupine, kot je na primer member: cn=John Smith, dc=ibm, dc=com.

memberURL
Določa URL, ki je povezan z vsakim članom skupine. Uporabite lahko katerikoli tip označenega URL-ja, kot je na primer memberURL: ldap:///cn=jsmith,dc=ibm,dc=com.

uniquemember
Določa skupino imen, povezanih z vnosom, v kateri je bil vsakemu imenu dodeljen unikatni identifikator, ki zagotavlja njegovo edinstvenost. Vrednost za atribut uniqueMember je DN, ki mu sledi unikatni identifikator, kot je na primer uniqueMember: cn=John Smith, dc=ibm, dc=com 17.

Vloge
Pooblaščanje, ki temelji na vlogah, je konceptualno dopolnilo k pooblaščanju, temelječem na skupinah, in je v nekaterih primerih zelo koristno. Kot član vloge imate pooblastilo izvesti tisto, kar je potrebno, da bi vloga dokončala opravilo. Za razliko od skupine ima vloga nastavljen impliciten niz dovoljenj. Samo članstvo v skupini ne določa, katera dovoljenja bodo pridobljena (ali izgubljena).

Vloge so podobne skupinam v tem, da so predstavljene v imeniku z objektom. Poleg tega vsebujejo vloge skupino DN-jev. Vloge, ki bodo uporabljene v krmiljenju dostopov, morajo imeti objektni razred 'AccessRole'. Objektni razred 'Accessrole' je podrazred objektnega razreda 'GroupOfNames'.

Če imate na primer zbirko DN-jev, kot je 'sys admin', boste ob omembi tega imena morda najprej pomislili na 'skupino sys admin' (ker so skupine in uporabniki najbolj znani tipi atributov pooblastil). Toda ker obstaja niz dovoljenj, za katera pričakujete, da jih boste prejeli kot član 'sys admin', je zbirka DN-jev morda bolj natančno definirana kot 'vloga sys admin'.

Seznami za nadzor dostopa
Seznami za nadzor dostopa (ACL-ji) omogočajo zaščito informacij, shranjenih v imeniku LDAP. Skrbniki z ACL-ji omejijo dostop do različnih delov imenika ali določenih imeniških vnosov. Spremembe v vsakem vnosu in atributu v imeniku lahko nadzorujete z ACL-ji. ACL za določen vnos ali atribut je lahko podedovan iz nadrejenega imenika ali pa je izrecno definiran.

Najbolje je, da z izdelavo skupin uporabnikov, ki jih boste uporabljali pri nastavljanju dostopa za objekte in atribute, oblikujete lastno strategijo za krmiljenje dostopa. Lastništvo in dostop nastavite v drevesu na najvišjo mogočo raven in pustite, da bodo krmilni elementi podedovani navzdol po drevesu.

Operacijski atributi, povezani s krmiljenjem dostopa, kot so entryOwner, ownerSource, ownerPropagate, aclEntry, aclSource in aclPropagate, so nenavadni po tem, da so logično povezani z vsakim objektom, vendar lahko vsebujejo vrednosti, odvisne od drugih objektov, ki so višje v drevesu. Odvisno od tega, kako so te vrednosti atributov vzpostavljene, so lahko eksplicitne za objekt ali podedovane od prednika.

Model za krmiljenje dostopa definira dva niza atributov: informacije o krmiljenju dostopa (ACI) in informacije o entryOwner. ACI definira dostopne pravice, podeljene določenemu subjektu v skladu z operacijami, ki jih lahko izvajajo v objektih, za katere so namenjene. Atributa aclEntry in aclPropagate sta namenjena za definicijo ACI. Informacije o entryOwner definirajo, kateri subjekti lahko definirajo ACI za povezani objekt vnosa. Atributa entryOwner in ownerPropagate se nanašata na definicijo entryOwner.

Izberete lahko med dvema vrstama seznamov za nadzor dostopa: ACL-ji, temelječi na filtrih in nefiltrirani ACL-ji. Nefiltrirani ACL-ji se nanašajo eksplicitno na imeniški vnos, ki jih vsebuje, in jih je mogoče razširiti v nobenega ali v

vseh podrejene vnose. ACL-ji, ki temeljijo na filtrih, so drugačni v tem, da uporabljajo primerjavo, temelječo na filtrih, ki uporablja določen objektni filter, ki primerja ciljne objekte z učinkovitim dostopom, ki velja za njih.

Z ACL-ji lahko skrbniki omejijo dostop do različnih delov imenika, določenih imeniških vnosov in na osnovi imena atributa ali razreda dostopa atributa tudi do atributov, vsebovanih v vnosih. Z vsakim vnosom v imeniku LDAP je povezan ACI. V skladu z modelom LDAP so informacije o ACI in entryOwner predstavljene kot pari atribut-vrednost. Poleg tega je za upravljanje teh vrednosti uporabljena skladnja LDIF. Atributi so:

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

Informacije o delu z ACL-ji boste našli v razdelku “Upravljanje seznamov za nadzor dostopa (ACL-jev)” na strani 145. Dodatne informacije boste našli v naslednjih temah:

- “Filtrirani ACL-ji”
- “Skladnja atributa za krmiljenje dostopa” na strani 49
- “AclEntry in ibm-filterAclEntry” na strani 49
- “EntryOwner” na strani 52
- “Razširjanje” na strani 52
- “Vrednotenje dostopa” na strani 52
- “Definiranje ACI-jev in lastnikov vnosov” na strani 54
- “Spreminjanje vrednosti ACI in lastnika vnosa” na strani 55
- “Brisanje vrednosti za ACI/lastnika vnosa” na strani 57
- “Pridobivanje vrednosti za ACI/lastnika vnosa” na strani 58
- “Problematika podvajanja poddrevesa” na strani 58

Filtrirani ACL-ji

ACL-ji, ki temeljijo na filtrih, uporabljajo primerjavo, temelječo na filtrih s podanim objektnim filtrom, s katerim primerjajo ciljne objekte z razpoložljivim dostopom, ki velja za njih.

ACL-ji, temelječi na filtrih, se razširijo na vse objekte, uporabljene v primerjavi v povezanem poddrevesu. Zaradi tega vzroka atribut aclPropagate, s katerim zaustavite razširjanje nefiltriranih ACL-jev, ne velja za nove ACL-je, temelječe na filtrih.

Privzeto vedenje ACL-jev, temelječih na filtrih, je kopičenje od najnižjega vnosa, ki vsebuje, do verige vnosov prednika, pa vse do najvišjega vnosa v DIT, ki vsebuje. Razpoložljiv dostop je izračunan kot zveza dostopnih pravic, ki jih odobrijo ali zavrnejo sestavni vnosi prednika. Vendar obstaja v tem vedenju izjema. Zaradi združljivosti s funkcijo podvajanja poddrevesa in da bi se omogočil večji nadzor nad upravljanjem, se uporablja atribut zgornje meje kot sredstvo za zaustavitev kopičenja v vnosu, v katerem je vsebovan.

Namesto združevanja na filtrih temelječih značilnosti v obstoječe ACL-je, ki ne temeljijo na filtrih, se uporablja nov nabor atributov za krmiljenje dostopa, namenjen posebej na podporo ACL-jem, temelječim na filtrih. Atributa sta:

- ibm-filterAclEntry
- ibm-filterAclInherit

Atribut ibm-filterAclEntry uporablja enak format kot aclEntry, le da mu je dodana komponenta objektnega filtra Povezan atribut zgornje meje je ibm-filterAclInherit. Po privzetku je nastavljen na true. Če je nastavljen na vrednost false, zaustavi kopičenje.

Skladnja atributa za krmiljenje dostopa

Te atribute lahko upravljate z zapisom LDIF. Skladnja novih atributov ACL, temelječih na filtrih, je v bistvu popravljena različica trenutnih atributov ACL, ki ne temeljijo na filtrih. Sledi skladnja atributov ACI in entryOwner v obliki BNF (baccus naur form).

```
<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> ::= razločevalno ime, kot je opisano v RFC-ju 2251, razdelek 4.1.3.

<pseudoDn> ::= "group:cn=anybody" | "group:cn=authenticated" |
                        "access-id:cn=this"
<object filter> ::= iskalni filter niza, kot je opisan v RFC-ju 2254, razdelek 4
                                (razširjeno primerjanje ni podprto)
<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 attributeType, kot je opisano v RFC-ju 2251, razdelek 4.1.4.
                       (OID ali črkovno-številski niz z začetno
                        črko, "-" in ";" sta dovoljena)

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

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

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

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

AclEntry in ibm-filterAclEntry

Subjekt: Subjekt (enota, ki zahteva dostop za delo v objektu) je sestavljena iz kombinacije tipa DN-ja (razločevalnega imena) in DN-ja. Veljavni tipi DN-jev so: access-id, group ali role.

DN identificira določen id-dostopa, vlogo ali skupino. Subjekt je lahko na primer access-id: cn=personA, o=IBM ali group: cn=deptXYZ, o=IBM.

Ker je ločilo polja dvopičje (:), mora biti DN, ki vsebuje dvopičja, obdan z dvojnimi narekovaji (“”). Če DN že vsebuje znake z dvojnimi narekovaji, jih morate preskočiti s poševnico nazaj (\).

Za krmiljenje dostopa lahko uporabite vse imeniške skupine.

Opomba: Uporabite lahko katerokoli skupino strukturalnih objektnih razredov **AccessGroup**, **GroupOfNames**, **GroupofUniqueNames** ali **groupOfURLs** ali pomožnih objektnih razredov **ibm-dynamicGroup** ali **ibm-staticGroup**.

Drug tip DN-ja, uporabljen v modelu krmiljenja dostopa, je vloga. Izvedba vlog in skupin je sicer podobna, vendar pa se njihov koncept razlikuje. Ko je uporabniku dodeljena vloga, obstaja implicitno pričakovanje, da je bilo potrebno pooblastilo za izvedbo opravila, povezanega s to vlogo, že nastavljeno. S samim članstvom v skupini pa ni povezana nobena predpostavka, katera pravice so podeljene (ali zavrnjene).

Vloge so podobne skupinam v tem, da so predstavljene v imeniku z objektom. Poleg tega vsebujejo vloge skupino DN-jev. Vloge, ki se uporabljajo v krmiljenju dostopa, morajo uporabljati objektni razred **AccessRole**.

Nepravi DN: Imenik LDAP vsebuje številne neprave DN-je, ki se uporabljajo za sklicevanje na veliko število DN-jev, ki v času povezovanja souporabljajo skupne značilnosti v zvezi z operacijo, ki se izvaja ali s ciljnim objektom, v katerem se izvaja operacija.

Trenutno so definirani trije nepravi DN-ji:

group:cn=anybody
Nanaša se na vse subjekte, vključno s tistimi, ki niso overjeni. V to skupino samodejno spadajo vsi uporabniki.

group:cn=authenticated
Nanaša se na katerikoli DN, ki je overjen v imeniku. Način overjanja ni pomemben.

access-id:cn=this
Nanaša se na povezovalni DN, ki primerja DN ciljnega objekta, v katerem se izvaja operacija.

Objektni filter: Ta parameter se nanaša samo na filtrirane ACL-je. Kot format objektnega filtra je uporabljen iskalni filter niza, kot je definiran v RFC-ju 2254. Ker je ciljni objekt že znan, se niz ne uporablja za dejansko izvedbo iskanja. Namesto tega je izvedena v ciljnem objektu primerjava, temelječa na filtru, ki določi, ali zanj velja podan niz vrednosti ibm-filterAclEntry.

Pravice: Dostope pravice lahko veljajo za celoten objekt ali pa za atribute objekta. Dostopne pravice LDAP so nepovezane, ker pomeni, da ena pravica ne pomeni tudi druge. Pravice lahko združite in izdelate seznam želenih pravic, ki sledijo nizu pravil, ki jih bomo razložili kasneje. Pravice so lahko brez podane vrednosti, kar pomeni, da ni subjektu ciljnega objekta podeljena nobena dostopna pravica. Pravice so sestavljene iz treh delov:

Dejanje:
Definirani vrednosti sta **odobri** ali **zavrni**. Če to polje ni prisotno, je uporabljena privzeta vrednost **odobri**.

Pravica:
V imeniškem objektu lahko izvedete šest osnovnih operacij. Iz teh operacij je izdelan osnovni niz pravic ACI. Te operacije so: dodajanje vnosa, brisanje vnosa, branje vrednosti atributa, zapis vrednosti atributa, iskanje atributa in primerjava vrednosti atributa.

Možna dovoljenja za atribute so: branje (r), pisanje (w), iskanje (s) in primerjava (c). Poleg tega veljajo dovoljenja objekta za vnos kot celoto. Ta dovoljenja so otroški vnosi (a) in zbrišejo ta vnos entry (d).

Naslednja tabela povzema dovoljenja, potrebna za izvedbo posameznih operacij LDAP.

Operacija	Potrebna pravica
ldapadd	dodajanje (v staršu)
ldapdelete	brisanje (v objektu)
ldapmodify	pisanje (v atributih, ki jih spreminjate)
ldapsearch	• iskanje, branje (v atributih v RDN-ju) • iskanje (v atributih, podanih v iskalnem filtru) • iskanje (v atributih, ki so vrnjeni samo z imeni) • iskanje, branje (v atributih, ki so vrnjeni z vrednostmi)
ldapmodrdn	pisanje (v atributih RDN)
ldapcompare	primerjava (v primerjanem atributu)

Opomba: Pri iskalnih operacijah mora imeti subjekt iskalni dostop (s) za vse atribute v iskalnem filtru, sicer ne bo vrnjen noben vnos. Za vrnjene vnose iskanja mora imeti subjekt iskalni (s) in bralni (r) dostop za vse atribute v RDN-ju vrnjenih vnosov, sicer ti vnosi ne bodo vrnjeni.

Cilj dostopa:

Ta dovoljenja lahko veljajo za celoten objekt (dodajanje otroškega vnosa, brisanje vnosa), za posamezen atribut znotraj vnosa ali pa za skupine atributov (dostopni razredi atributa).

Atributi, ki zahtevajo za dostop podobne pravice, so združeni v razrede. Atributi so preslikani v razrede atributov v imeniški datoteki sheme. Ti razredi niso povezani, kar pomeni, da dostop do enega razreda ne pomeni dostopa do drugega. Dovoljenja so nastavljena glede na dostopni razred atributa kot celote. Dovoljenja, nastavljena za določen razred atributa, veljajo za vse atributa znotraj tega dostopnega razreda, razen če ne podate ločenih dostopnih dovoljenj atributov.

IBM definira tri razrede atributov, ki se uporabljajo pri oceni dostopa do uporabniških atributov: **normalni**, **občutljivi** in **kritični**. Atribut **commonName** na primer spada v normalni razred, atribut userpassword pa v kritični razred. Uporabniško definirani atributi spadajo v normalni dostopni razred, razen če ne določite drugače.

Definirana sta še dva druga dostopna razreda: sistemski in omejeni. Atributi sistemskega razreda so:

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

To so atributi, ki jih vzdržuje strežnik LDAP in jih uporabniki imenika lahko samo berejo. Atributa **OwnerSource** in **aclSource** sta opisana v razdelku Razširjanje (glejte “Razširjanje” na strani 52).

Atributi omejenega razreda, ki definirajo krmiljenje dostopa, so:

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

Vsi uporabniki imajo bralni dostop do omejenih atributov, toda te atribute lahko izdelujejo, spreminjajo in brišejo samo **entryOwners**.

Opomba: Atribut **ibm-effectiveAcl** je samo za branje.

EntryOwner

Lastniki vnosov imajo polno dovoljenje za izvajanje katerihkoli operacij v objektu, ne glede na aclEntry. Poleg tega so lastniki vnosov tudi edini, ki lahko upravljajo aclEntires za ta objekt. EntryOwner je nadzorni subjekt dostopa, ki je lahko definiran za posameznike, skupine ali vloge.

Opomba: Skrbnik imenika je po privzetku eden od lastnikov vnosa za vse objekte v imeniku; entryOwnership za skrbnika imenika ni mogoče odstraniti iz nobenega objekta.

Razširjanje

Za vnose, v katere je bil postavljen aclEntry, pravimo, da imajo eksplicitni **aclEntry**. Podobno velja, če je nastavljen **entryOwner** za določen vnos, ko pravimo, da ima ta vnos eksplicitnega lastnika. Ti možnosti se med seboj ne prepletata, kar pomeni, da ima vnos z eksplicitnim lastnikom lahko eksplicitni **aclEntry** ali pa ne, vnos z eksplicitnim **aclEntry** pa ima lahko eksplicitnega lastnika. Če ena od teh vrednosti ni eksplicitno prisotna v vnosu, je manjkajoča vrednost podedovana iz vozlišča prednika v imeniškem drevesu.

Vsak eksplicitni **aclEntry** ali **entryOwner** velja za vnos, v katerem je nastavljen. Poleg tega lahko velja vrednost za vse potomce, ki nimajo eksplicitno nastavljene vrednosti. Za te vrednosti pravimo, da so razširjene v imeniškem drevesu. Razširjanje določene vrednosti se nadaljuje, dokler ni dosežena druga vrednost razširjanja.

Opomba: Razširjanje ACL-jev, temelječih na filtrih, ne poteka enako kot razširjanje ACL-jev, ki ne temeljijo na filtrih. Razširijo se v vse primerjane objekte primerjave v povezanem poddrevesu. Dodatne informacije o razlikah boste našli v temi “Filtrirani ACL-ji” na strani 48.

AclEntry in **entryOwner** lahko nastavite tako, da veljata samo za določen vnos z vrednostjo razširjanja, nastavljeno na ″false″, ali na vnos in njegovo poddrevo z vrednostjo razširjanja, nastavljeno na ″true″. Čeprav je razširjanje mogoče za **aclEntry** in **entryOwner**, njuno razširjanje na noben način ni povezano.

Atributa **aclEntry** in **entryOwner** imata lahko več vrednosti, toda atributa razširjanja (**aclPropagate** in **ownerPropagate**) imata lahko za vrednosti atributov **aclEntry** ali **entryOwner** znotraj istega vnosa samo eno vrednost.

Sistemska atributa **aclSource** in **ownerSource** vsebujeta DN razpoložljivega vozlišča, iz katerega je ocenjen **aclEntry** oziroma **entryOwner**. Če takšno vozlišče ne obstaja, je dodeljena **privzeta vrednost**.

Razpoložljive definicije za krmiljenje dostopa objekta so lahko izpeljane z naslednjo logiko:

- Če obstaja v objektu niz eksplicitnih atributov za krmiljenje dostopa, je to definicija za krmiljenje dostopa objekta.
- Če eksplicitno definirani atributi za krmiljenje dostopa ne obstajajo, prečkajte imeniško drevo navzgor, dokler ne dosežete vozlišča prednika z naborom atributov za krmiljenje dostopa, namenjenih za razširjanje.
- Če takšno vozlišče prednika ni najdeno, je subjektu odobren privzeti dostop, opisan spodaj.

Skrbnik imenika je lastnik vnosa. Nepravi skupini cn=anybody (vsi uporabniki) je odobren bralni, iskalni in primerjalni dostop do atributov v normalnem dostopnem razredu.

Vrednotenje dostopa

Dostop za določeno operacijo je odobren ali zavrnjen na osnovi povezovalnega DN-ja subjekta za to operacijo v ciljnem objektu. Obdelava se konča takoj, ko je mogoče določiti dostop.

Preverjanja dostopa se izvedejo tako, da se poišče razpoložljiva definicija **entryOwnership** in **ACI**, preveri se lastništvo objekta in ovrednotijo se vrednosti ACI objekta.

ACL-ji, temelječi na filtrih, se kopičijo od najnižjega vnosa, ki vsebuje, in vzdolž verige vnosov prednika do najvišjega vnosa v DIT, ki vsebuje. Razpoložljiv dostop je izračunan kot zveza dostopnih pravic, ki jih odobrijo ali zavrnejo sestavni vnosi prednika. Obstoječi niz pravil specifičnosti in združevanja se uporablja za vrednotenje razpoložljivega dostopa za ACL-je, temelječe na filtrih.

Atributi, ki temeljijo na filtrih, in tisti, ki ne temeljijo na filtrih, se znotraj posameznega imeniškega vnosa, ki vsebuje, medsebojno izključujejo. Postavitev obeh tipov atributov v en vnos ni dovoljena in predstavlja kršitev omejitve. Če je odkrito to stanje, operacije, ki so povezane z izdelavo ali ažuriranjem imeniškega vnosa, ne uspejo.

Pri izračunavanju razpoložljivega dostopa nastavi način izračuna prvi tip ACL-ja, ki bo odkrit v verigi prednika vnosa ciljnega objekta. V načinu, ki temelji na filtrih, so ACL-ji, ki ne temeljijo na filtrih, pri izračunu razpoložljivega dostopa zanemarjeni. Podobno velja v načinu, ki ne temelji na filtrih, ko so v izračunu razpoložljivega dostopa zanemarjeni ACL-ji, ki temeljijo na filtrih.

Da bi v izračunu razpoložljivega dostopa omejili kopičenje ACL-jev, ki temeljijo na filtrih, lahko postavite v vnos med najvišjo in najnižjo pojavitvijo atributa **ibm-filterAclEntry** v podanem poddrevesu atribut **ibm-filterAclInherit**, nastavljen na vrednost ″false″. S tem povzročite, da bo podniz atributov **ibm-filterAclEntry** nad njim v verigi prednika ciljnega objekta zanemarjen.

Če v načinu ACL-jev, temelječih na filtrih, ni v veljavi noben ACL, ki temelji na filtrih, je uveljavljen privzeti ACL (za cn=anybody je odobren bralni, iskalni in primerjalni dostop za atribute v normalnem dostopnem razredu). Do tega stanja lahko pride, če se vnos, do katerega dostopate, ne ujema z nobenim od filtrov, ki so podani v vrednostih **ibm-filterAclEntry**. Če ne želite uporabiti tega privzetega krmiljenja dostopa, lahko podate privzeti filter ACL, podoben naslednjemu:

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

Ta primer ne odobri nobenega dostopa. Če želite, ga spremenite, tako da bo omogočal želeni dostop.

Po privzetku imata skrbnik imenika in glavni ali enakovredni strežnik (za podvajanje) polne dostopne pravice do vseh objektov v imeniku, razen pisalnega dostopa do sistemskih atributov. Drugi **entryOwners** imajo polne dostopne pravice do objektov, katerih lastniki so, razen pisalnega dostopa do sistemskih atributov. Vsi uporabniki imajo bralne dostopne pravice za sistemske in omejene atribute. Teh vnaprej definiranih pravic ni mogoče spremeniti. Če ima zahtevniški objekt **entryOwnership**, je dostop določen z zgornjimi privzetimi nastavitvami, obdelava dostopa pa se ustavi.

Če zahtevniški objekt ni entryOwner, so preverjene vrednosti ACI za vnose objekta. Dostopne pravice, kot so definirane v ACI-jih za ciljni objekt, so izračunane s pravili specifičnosti in združevanja.

Pravilo specifičnosti

Pri vrednotenju pravic, ki so odobrene ali zavrnjene za uporabnike, se uporabljajo najbolj specifične definicije aclEntry. Ravni specifičnosti so:

- id-dostopa je bolj specifičen od skupine ali vloge, skupine in vloge pa so iste ravni.
- Znotraj iste ravni **dnType** so posamezne pravice na ravni atributov bolj specifične od pravic na ravni razreda atributov.
- Znotraj istega atributa ali ravni razreda atributov je **zavrni** bolj specifičen kot **odobri**.

Pravilo združevanja

Dovoljenja, ki so odobrena za objekte enake specifičnosti, so združena. Če dostopa ni mogoče določiti znotraj iste ravni specifičnosti, so uporabljene definicije dostopa manj specifične ravni. Če dostop po uveljavitvi vseh definiranih ACI-jev ni določen, je zavrnjen.

Opomba: Ko je v vrednotenju dostopa najdena ustrezna raven za id-dostopa **aclEntry**, aclEntries ravni skupine niso vključeni v vrednotenje dostopa. Izjema je, če so vsi **aclEntries** ustrezne ravni za id-dostopa definirani pod cn=this, ko so **aclEntries** ustrezne ravni skupine združeni v vrednotenju.

Če torej definiran vnos ACI znotraj vnosa objekta vsebuje DN subjekta za id-dostopa, ki ustreza povezovalnemu DN-ju, so dovoljenja najprej ovrednotena na osnovi tega aclEntry. Če so pod istim DN-jem subjekta definirana ustrezna dovoljenja na ravni atributa, izpodrinejo vsa dovoljenja, ki so definirana pod razredi atributov. Če so pod isto definicijo ravni atributa ali razreda atributov prisotna navzkrižna dovoljenja, zavrnjena dovoljenja nadomestijo odobrena.

Opomba: Definirano dovoljenje ničelne vrednosti preprečuje vključitev manj specifičnih definicij dovoljenj.

Če dostopa še vedno ni mogoče določiti in so vsi najdeni ustrezni aclEntries definirani pod ″cn=this″, je ovrednoteno članstvo v skupini. Če uporabnik pripada več kot eni skupini, prejme iz teh skupin združena dovoljenja. Poleg tega uporabnik samodejno pripada skupini cn=Anybody in po možnosti tudi skupini cn=Authenticated, če se je povezal brez overjanja. Če so definirana dovoljenja za te skupine, uporabnik prejme določena dovoljenja.

Opomba: Članstvo v skupini in vlogi je določeno v času povezovanja in traja do naslednjega povezovanja ali dokler ni prejeta zahteva za prekinitev povezave. Vgnezdene skupine in vloge - to so vloge ali skupine, ki so definirane kot člani druge skupine ali vloge - niso razrešene pri določanju članstva niti v vrednotenju dostopa.

Denimo, da je attribute1 v občutljivem razredu dostopa, uporabnik user cn=Person A, o=IBM pa pripada v group1 in group2 z naslednjimi definiranimi aclEntries:

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

Za tega uporabnika velja naslednje:

- dobi dostop ’rsc’ za attribute1, (iz 1. definicija na ravni atributa izpodrine definicijo na ravni razreda atributov)
- ne dobi nobenega dostopa do drugih atributov občutljivega razreda v ciljnem objektu (iz 1)
- odobrene niso nobene druge pravice (2 in 3 NISTA vključena v vrednotenje dostopa)

V drugem zgledu z naslednjimi aclEntries:

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

velja za uporabnika naslednje:

- ne dobi nobenega dostopa do atributov občutljivega razreda (iz 1. ničelna vrednost, definirana pod access-id, preprečuje vključitev dovoljenj v atribute občutljivega razreda iz group1)
- dobi dostop ’rsc’ za atribute normalnega razreda (iz 2).

Definiranje ACI-jev in lastnikov vnosov

Naslednja zgleda kažeta vzpostavitev upravne poddomene. Prvi zgled kaže enega uporabnika, ki je dodeljen kot entryOwner za celotno domeno, drugi zgled pa skupino, ki je dodeljena kot entryOwner.

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

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

Naslednji zgled kaže, kako so za access-id ″cn=Person 1, o=IBM″ dodeljena dovoljenja za branje, iskanje in primerjavo attribute1. Dovoljenje velja za vsa volišča v celotnem poddrevesu, ki so v vozlišču ali pod vozliščem, ki vsebuje ta ACI, ki ustreza filtru primerjave ″(objectclass=groupOfNames)″. Kopičenje ustreznih atributov ibm-filteraclentry v kateremkoli vozlišču prednika se konča v tem vnosu z nastavitvijo atributa ibm-filterAclInherit na vrednost ″false″.

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

ibm-filterAclInherit: false
```

Naslednji zgled kaže, kako so za group ″cn=Dept XYZ, o=IBM″ odobrena dovoljenja za branje, iskanje in primerjavo attribute1. Dovoljenje velja za celotno poddrevo pod vozliščem, ki vsebuje ta ACI.

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

Naslednji zgled kaže, kako so za role ″cn=System Admins,o=IBM″ odobrena dovoljenja za dodajanje objektov pod tem vozliščem ter za branje, iskanje in primerjavo attribute2 in kritičnega razreda atributov. Dovoljenje velja samo za vozlišče, ki vsebuje ta ACI.

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

Spreminjanje vrednosti ACI in lastnika vnosa

Modify-replace

Modify-replace deluje na enak način kot vsi drugi atributi. Če vrednost atributa ne obstaja, jo izdelajte. Če vrednost atributa obstaja, jo zamenjajte.

Za naslednje ACI-je za vnos:

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

opravite naslednjo spremembo:

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

Nastali ACI je takšen:

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

Vrednosti ACI za Dept ABC se med zamenjavo izgubijo.

Za naslednje ACI-je za vnos:

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

opravite naslednje spremembe:

```
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
```

Nastali ACI je takšen:

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

Vrednosti ACI za Dept ABC se med zamenjavo izgubijo.

Modify-add

Če ACI ali entryOwner med ldapmodify-add ne obstajata, sta izdelana s podanimi vrednostmi. Če ACI ali entryOwner obstajata, dodajte za določen ACI ali entryOwner podane vrednosti. ACI:

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

s popravkom:

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

na primer povzroči izdelavo aclEntry z več vrednostmi:

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

ACI:

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

s popravkom:

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

na primer povzroči izdelavo aclEntry z več vrednostmi:

```
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
```

Dovoljenja pod enakim atributom ali razredom atributov so smatrana za osnovne gradnike, dejanja pa za kvalifikatorje. Če dodate enako vrednost dovoljenja več kot enkrat, je shranjena samo ena vrednost. Če dodate enako vrednost dovoljenja več kot enkrat z različnimi vrednostmi dejanja, je uporabljena zadnja vrednost dejanja. Če je nastalo polje dovoljenja prazno (″″), je ta vrednost dovoljenja nastavljena na nič, vrednost dejanja pa na **odobri**.

Naslednji ACI:

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

s popravkom:

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

na primer ustvari naslednji aclEntry:

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

Naslednji ACI:

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

s popravkom:

```
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
```

na primer ustvari naslednji aclEntry:

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

Modify-delete

Za izbris določene vrednosti ACI uporabite običajno skladnjo ldapmodify-delete.

ACI:

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

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

ustvari preostali ACI v strežniku:

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

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

ustvari preostali ACI v strežniku:

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

Brisanje neobstoječe vrednosti za ACI ali entryOwner povzroči nespremenjeni ACI ali entryOwner in vrne kodo, ki podaja, da vrednost atributa ne obstaja.

Brisanje vrednosti za ACI/lastnika vnosa

Z operacijo ldapmodify-delete lahko zbrišete entryOwner takole:

```
dn: cn = some entry
changetype: modify
delete: entryOwner
```

V tem primeru vnos nima eksplicitnega lastnika vnosa. Tudi ownerPropagate je samodejno odstranjen. Ta vnos nasledi svojega lastnika vnosa iz vozlišča prednika v imeniškem drevesu, ki sledi pravilu za razširjanje.

Enak postopek lahko uporabite za celoten izbris lastnika vnosa:

```
dn: cn = some entry
changetype: modify
delete: aclEntry
```

Brisanje zadnje vrednosti za ACI ali entryOwner iz vnosa ni enako, kot če izbrišete ACI ali entryOwner. Možno je, da vsebuje vnos ACI ali entryOwner brez vrednosti. V tem primeru ni odjemalcu, ki izvaja poizvedbo v ACI ali entryOwner, vrnjena nobena vrednost, nastavitev pa se razširja v naslednjiška vozlišča, dokler ni nadomeščena. Da bi preprečili visenje vrednosti, do katerih ne more nihče dostopiti, ima skrbnik imenika vedno poln dostop do vnosa, čeprav ima vnos ničelno vrednost ACI ali entryOwner.

Pridobivanje vrednosti za ACI/lastnika vnosa

Razpoložljive vrednosti za ACI ali entryOwner lahko poiščete tako, da podate želene atribute za ACL ali entryOwner v iskanju:

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

na primer vrne vse informacije o ACL ali entryOwner, uporabljene pri vrednotenju dostopa do objekta A. Vrnjene vrednosti morda ne bodo natančno takšne, kot so bile pri prvem definiranju. Vrednosti so ekvivalenti izvirne oblike.

Iskanje samo v atributu ibm-filterAclEntry vrne vrednosti, ki so specifične za vnos, ki vsebuje.

Za prikaz združenega razpoložljivega dostopa je uporabljen operacijski atribut samo za branje ibm-effectiveAc1. Iskalna zahteva za ibm-effectiveAcl vrne razpoložljiv dostop, ki velja za ciljni objekt, ki temelji na ACL-jih s filtri ali brez filtrov, odvisno od tega, kako so bili porazdeljeni v DIT.

Ker lahko izhajajo na filtrih temelječi ACL-ji iz več izvorov prednika, ustvari iskanje v atributu aclSource seznam povezanih izvorov.

Problematika podvajanja poddrevesa

Da bi bil na filtrih temelječ dostop vključen v podvajanje poddrevesa, morajo biti atributi ibm-filterAclEntry v povezanem vnosu ibm-replicationContext ali pod njim.

Ker razpoložljivega dostopa ni mogoče zbrati iz vnosa prednika, ki je nad podvojenim poddrevesom, mora biti atribut ibm-filterAclInherit nastavljen na vrednost **false** in biti v povezanem vnosu ibm-replicationContext.

Lastništvo objektov imenika LDAP

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

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

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

Dodatne lastnosti o delu z lastnostmi lastništva boste našli v temi “Upravljanje imeniških vnosov” na strani 129.

Načelo gesel

Pri uporabi strežnikov LDAP za overjanje je pomembno, da strežnik LDAP podpira načela glede izteka gesel, neuspelih poskusov prijave in pravil za gesla. Imeniški strežnik nudi podporo, ki jo je mogoče konfigurirati za vse tri vrste teh načel. To načelo je uveljavljeno za vse imeniške vnose z atributom userPassword. Enega načela ne morete definirati za en niz uporabnikov in drugih načel za drug niz uporabnikov. Imeniški strežnik nudi tudi mehanizem za obveščanje odjemalcev o pogojih, povezanih z načeli gesel (geslo poteče v treh dneh) in niz operacijskih atributov, ki jih lahko uporabi skrbnik za iskanje stvari, kot so uporabniki s pretečenimi gesli ali zaklenjene šifre.

Dodatne informacije o delu z lastnostmi načel gesel boste našli v temi “Nastavitev načela za gesla” na strani 96.

Konfiguriranje

Vedenje strežnika lahko konfigurirate v skladu z gesli v naslednjih področjih:

- globalno stikalo za ″vklop/izklop″, ki omogoči ali onemogoči načelo gesel
- pravila za spreminjanje gesel, vključno z naslednjimi:
  - Uporabniki lahko spreminjajo svoja gesla. To načelo je v veljavi poleg krmiljenja dostopa. Krmiljenje dostopa mora dodeliti uporabniku pooblastilo za spreminjanje atributa userPassword, kot tudi načelo za gesla, ki uporabnikom omogoča, da spreminjajo svoja gesla. Če je to načelo onemogočeno, uporabniki svojih gesel ne morejo spreminjati. Geslo za vnos lahko spremenijo samo skrbnik ali drug uporabnik s pooblastilom za spreminjanje atributa userPassword.
  - Gesla je potrebno po vnovični nastavitvi spremeniti. Če je to načelo omogočeno in geslo spremeni kdorkoli, ki ni ta uporabnik, je geslo označeno kot na novo nastavljeno in ga mora uporabnik spremeniti, preden lahko izvede katero drugo imeniško operacijo. Povezovalna zahteva z na novo nastavljeni geslom uspe. Da bi lahko prejeli obvestilo o tem, da je potrebno geslo nastaviti na novo, mora aplikacija poznati načelo za gesla.
  - Uporabniki morajo pri spreminjanju gesla poslati staro geslo. Če omogočite to načelo, lahko spremeni geslo samo zahteva za spreminjanje, ki vključuje brisanje atributa userPassword (s staro vrednostjo) in dodajanje nove vrednosti userPassword. S tem je zagotovljeno, da bo svoje geslo spremenil samo uporabnik, ki ga pozna. Geslo lahko vedno nastavijo skrbnik ali drugi uporabniki, ki imajo pooblastilo za spreminjanje atributa userPassword.
- Pravila za potek gesel, vključno z naslednjimi:
  - Gesla nikoli ne potečejo ali pa potečejo v nastavljenem času od zadnje spremembe.
  - Uporabniku o poteku gesel niso obveščeni ali pa so obveščeni v določenem času pred potekom gesla. Da bi lahko prejeli obvestilo o bližajočem se poteku gesla, mora aplikacija poznati načelo za gesla.
  - Po poteku uporabniškega gesla omogoči nastavljeno število odloženih prijav. Aplikacija, ki pozna načelo za gesla, bo obveščena o številu preostalih odloženih prijav. Če odložene prijave niso omogočene, se uporabnik ne more overiti ali svojega gesla po izteku spremeniti.
- Pravila za preverjanje veljavnosti gesel, vključno z naslednjimi:
  - Nastavljiva velikost zgodovine gesel, ki pove strežniku, naj hrani zgodovino vsaj N gesel in zavrne predhodno uporabljena gesla.
  - Preverjanje skladnje gesel, vključno z nastavitvijo za vedenje strežnika, če so gesla razpršena. Ta nastavitev vpliva na to, ali naj strežnik v naslednjih primerih zanemari načelo:
    - strežnik shranjuje razpršena gesla
    - odjemalec poda strežniku razpršeno geslo (do tega lahko pride pri prenosu vnosov med strežniki prek datoteke LDIF, če izvorni strežnik hrani razpršena gesla)

    V obeh primerih strežnik morda ne bo uspel uveljaviti vseh skladenjskih pravil. Podprta so naslednja skladenjska pravila: najmanjša dolžina, najmanjše število abecednih znakov, najmanjše število številskih ali posebnih znakov, število ponovljenih znakov in število znakov, po katerih se mora geslo razlikovati od prejšnjega.
- Pravila za neuspele prijave, vključno z naslednjimi:
  - Najmanjši čas, dovoljen med spreminjanji gesel, ki preprečuje uporabniku, da bi hitro krožil v nizu gesel in se vrnil v izvorno geslo.
  - Največje število neuspelih poskusov prijav, preden se šifra zaklene.
  - Nastavljivo trajanje zaklenjenega gesla. Po tem času lahko uporabite prejšnjo zaklenjeno šifro. S tem lahko zaklenete hekerja, ki poskuša ugotoviti geslo in pomagate uporabniku, ki je svoje geslo pozabil.
  - Nastavljiv čas, ko strežnik sledi neuspelim poskusom prijav. Če je v tem času doseženo največje dovoljeno število neuspelih prijav, se šifra zaklene. Ko ta čas poteče, strežnik zavrže informacije o prejšnjih neuspelih poskusih prijav za šifro.

Nastavitve načel za gesla imeniškega strežnika so shranjene v objektu ″cn=pwdpolicy″:

```
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, ki poznajo načela za gesla

Podpora za načela gesel imeniškega strežnika za iSeries vključujejo skupino krmilnih elementov LDAP, ki jo lahko uporabljajo aplikacije, ki poznajo načela gesel, za sprejemanje obvestil o dodatnih pogojih, povezanih z načeli za gesla.

Aplikacija je lahko obveščena o naslednjih opozorilnih pogojih:

- preostali čas pred iztekom gesla
- preostalo število odloženih prijav po poteku gesla

Aplikacija je lahko obveščena tudi o naslednjih stanjih napake:

- geslo je poteklo
- šifra je zaklenjena
- geslo je bilo na novo nastavljeno in ga je potrebno spremeniti
- uporabnik ne sme spreminjati svojega gesla
- s spremenjenim geslom je potrebno podati staro geslo
- novo geslo krši skladenjska pravila
- novo geslo je prekratko
- geslo je bilo prezgodaj spremenjeno
- novo geslo je v zgodovini

Uporabljena sta dva krmilna elementa. Krmilni element za zahtevanje načela gesel se uporablja za obveščanje strežnika, da želi biti aplikacija obveščena o pogojih, povezanih z načeli gesel. Ta krmilni element mora podati aplikacija v vseh operacijah, ki jo zanimajo, običajno pa v začetni povezovalni zahtevi in v vseh zahtevah za spreminjanje gesel. Če je prisoten krmilni element za zahtevanje načela gesel, vrne strežnik krmilni element za odziv na načela gesel, če je prisotno katero od zgornjih stanj napake.

Odjemalski API-ji imeniškega strežnika vključujejo niz API-jev, ki jih lahko uporabljajo aplikacije C za delo s temi krmilnimi elementi. Ta API-ja sta:

- ldap_parse_pwdpolicy_response
- ldap_pwdpolicy_err2string

Za aplikacije, ki teh API-jev ne uporabljajo, so krmilni elementi definirani spodaj. Za obdelavo krmilnih elementov morate uporabiti zmožnosti, ki jih nudijo odjemalski API-ji LDAP. Java Naming and Directory Interface (JNDI) ima na primer vgrajeno podporo za nekatere znane krmilne elemente in nudi tudi ogrodje za podporne krmilne elemente, ki jih JNDI ne prepozna.

Krmilni element za zahtevanje načela gesel

```
Ime krmilnega elementa: 1.3.6.1.4.1.42.2.27.8.5.1
Kritičnost krmilnega elementa: FALSE
Vrednost krmilnega elementa: None
```

Krmilni element za odziv na načelo gesel

```
Ime krmilnega elementa: 1.3.6.1.4.1.42.2.27.8.5.1 (enako kot krmilni element za zahtevo)
Kritičnost krmilnega elementa: FALSE
Vrednost krmilnega elementa: kodirana vrednost BER, definirana v ASN.1 takole:
  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) } }
```

Tako kot drugi elementi protokola LDAP uporablja kodiranje BER implicitno označevanje.

Operacijski atributi načela gesel

Imeniški strežnik vzdržuje niz operacijskih atributov za vsak vnos z atributom userPassword. Te atribute lahko preiščejo pooblaščeni uporabniki, pa naj bodo uporabljeni v iskalnih filtrih ali vrnjeni v iskalni zahtevi. Atributi so:

- pwdChangedTime - atribut GeneralizedTime, ki vsebuje čas zadnjega spreminjanja gesla
- pwdAccountLockedTime - atribut GeneralizedTime, ki vsebuje čas zaklepanja šifre; če šifra ni zaklenjena, ta atribut ni prisoten
- pwdExpirationWarned - atribut GeneralizedTime, ki vsebuje čas pošiljanja prvega opozorila uporabniku o poteku gesla
- pwdFailureTime - atribut GeneralizedTime z več vrednostmi, ki vsebuje čase predhodnih zaporednih napak pri prijavi; če je zadnja prijava uspela, ta atribut ni prisoten
- pwdGraceUseTime - atribut GeneralizedTime z več vrednostmi, ki vsebuje čase prejšnjih odloženih prijav
- pwdReset - boolov atribut, ki vsebuje vrednost TRUE, če je bilo geslo na novo nastavljeno in ga mora uporabnik spremeniti.

Podvajanje načela gesel

Informacije o načelih gesel so podvojene iz oskrbniških strežnikov v potrošniške. Spremembe v vnosu cn=pwdpolicy so podvojene kot globalne spremembe, ravno tako kot spremembe v shemi. Podvojene so tudi informacije o stanju načela gesel za posamezne vnose, tako da je v primeru zaklenjenega vnosa v oskrbniškem strežniku to dejanje podvojeno na kateremkoli potrošniku. Spremembe stanja načela gesel v kopiji, ki je samo za branje, pa niso podvojene v nobenem drugem strežniku.

Overjanje

Krmiljenje dostopa v imeniškem strežniku temelji na razločevalnem imenu (DN-ju), ki je povezan z določeno povezavo. Ta DN je vzpostavljen kot rezultat povezovanja z imeniškim strežnikom (prijave vanj).

Pri prvem konfiguriranju imeniškega strežnika lahko uporabite za overjanje naslednje identitete:

- anonimen uporabnik
- skrbnik imenik (po privzetku cn=administrator)
- načrtovani profil uporabnika i5/OS (glejte “Ozadje, določeno z operacijskim sistemom” na strani 64)

Priporočamo, da izdelate dodatne uporabnike, ki jim lahko dodelite pooblastilo za upravljanje različnih delov imenika, ne da bi morali souporabljati identiteto skrbnika imenika.

S stališča LDAP obstajata dve ogrodji za overjanje v LDAP:

- preprosta povezava, pri kateri poda aplikacija DN in geslo v čistem besedilu za ta DN
- SASL (Simple Authentication and Security Layer), ki nudi številne dodatne načine overjanja, vključno s CRAM-MD5, EXTERNAL, GSSAPI in OS400-PRFTKN.

Preprosta povezava (in CRAM-MD5)

Za uporabo preproste povezave mora podati odjemalec DN obstoječega vnosa LDAP in geslo, ki ustreza atributu userPassword za ta vnos. Vnos za Johna Smitha lahko na primer izdelate takole:

```
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
```

DN ″cn=John Smith,cn=users,o=acme,c=us″ lahko zdaj uporabite v krmiljenju dostopa ali pa ga spremenite v člana skupine, uporabljene v krmiljenju dostopa.

Številni vnaprej definirani objektni razredi omogočajo, da podate userPassword, vključno (vendar ne omejeno) z naslednjimi: person, organizationalperson, inetorgperson, organization, organizationalunit in drugi.

Gesla imeniškega strežnika upoštevajo velike in male črke. Če izdelate vnos z vrednostjo za userPassword secret, povezava z geslom SECRET ne bo uspela.

Pri uporabi preproste povezave pošlje odjemalec strežniku geslo v čistem besedilu kot del povezovalne zahteve. Zaradi tega je mogoče pregledovanje gesla na ravni protokola. Za zaščito gesla lahko uporabite povezavo SSL (vse informacije, poslane prek povezave SSL, so šifrirane) ali pa način CRAM-MD5 SASL.

Način CRAM-MD5 zahteva, da ima strežnik dostop do gesla v čistem besedilu (zaščita gesla je nastavljena na nič, kar v resnici pomeni, da je geslo shranjeno v obliki, ki jo je mogoče dešifrirati, in vrnjeno v iskanjih kot čisto besedilo). Odjemalec pošlje DN strežniku. Strežnik prebere vrednost userPassword za vnos in ustvari naključni niz, ki je poslan odjemalcu. Odjemalec in strežnik razpršita naključni niz z geslom kot ključem, odjemalec pa pošlje rezultat strežniku. Če se razpršena niza ujemata, povezovalna zahteva uspe in geslo ni bilo nikoli poslano strežniku.

Za uporabo načina CRAM-MD5 mora biti strežnik konfiguriran tako, da je zaščita gesla Nič, sistemska vrednost QRETSVRSEC (Retain server security data - Ohrani podatke o zaščiti strežnika) pa 1 (Ohrani podatke).

Povezovanje kot objavljeni uporabnik

Imeniški strežnik nudi sredstva za uporabo vnosa LDAP, katerega geslo je uporabljeno za profil uporabnika i5/OS v istem sistemu. Da bi bilo to mogoče, mora veljati naslednje:

- vnos mora imeti atribut UID, katerega vrednost je ime profila uporabnika i5/OS
- vnos ne sme imeti atributa userPassword

Ko prejme strežnik povezovalno zahtevo za vnos z vrednostjo UID in brez atributa userPassword, pokliče funkcijo zaščite i5/OS, ki preveri, ali je UID veljavno ime profila uporabnika in ali je podano geslo pravilno za ta profil uporabnika. Takšen vnos se imenuje objavljeni uporabnik glede na objavljanje sistemskega razdeljevalnega imenika (SDD) v LDAP, ki ustvari takšne vnose.

Povezovanje kot načrtovani uporabnik

Vnos LDAP, ki predstavlja profil uporabnika i5/OS, se imenuje načrtovani uporabnik. DN načrtovanega uporabnika lahko skupaj s pravilnim geslom za ta profil uporabnika uporabite v preprosti povezavi. DN za uporabnika JSMITH v sistemu system my-system.acme.com je na primer takšen:

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

Povezovanje SASL EXTERNAL

Če uporabite pri overjanju odjemalca povezavo SSL ali TLS (če odjemalec na primer uporablja zasebno potrdilo), lahko uporabite način SASL EXTERNAL. Ta način pove strežniku, naj poišče identiteto odjemalca v zunanjem izvoru, ki je v tem primeru povezava SSL. Strežnik poišče javni del potrdila odjemalca (ki je poslano strežniku kot del vzpostavljanja povezave SSL) in povzame DN subjekta. Ta DN dodeli strežnik LDAP povezavi.

Za potrdilo, dodeljeno za:

```
common name: John Smith
organization unit: Engineering
organization: ACME
locality: Minneapolis
state: MN
country: US
```

bi bil DN subjekta takšen:

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

Elementi cn, ou, o, l, st in c so uporabljeni v prikazanem vrstnem redu, da ustvarijo DN subjekta.

Povezovanje SASL GSSAPI

Povezovalni mehanizem SASL GSSAPI se uporablja za overjanje v strežniku z dovolilnico Kerberos. Ta način je uporaben, če odjemalec izvede KINIT ali kakšno drugo obliko overjanja Kerberos (kot je na primer prijava v domeno Windows 2000). V tem primeru strežnik preveri veljavnost dovolilnice odjemalca, nato pa poišče ime principala in področja Kerberos; principal jsmith v področju acme.com je običajno izražen kot jsmith@acme.com. Strežnik lahko konfigurirate za preslikavo te identitete v DN na dva načina:

- tvorba navideznega DN-ja v obliki ibm-kn=jsmith@acme.com
- iskanje vnosa s pomožnim razredom ibm-securityidentities in vrednostjo altsecurityidenties v obliki KERBEROS:<principal>@<področje>.

Vnos, ki je lahko uporabljen za jsmith@acme.com, je lahko podoben naslednjemu:

```
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
```

Informacije o tem, kako omogočiti overjanje Kerberos, boste našli v razdelku “Omogočanje overjanja Kerberos v imeniškem strežniku” na strani 119.

Povezovanje OS400-PRFTKN

Povezovalni mehanizem OS400-PRFTKN SASL se uporablja za overjanje v strežniku z žetonom profila (glejte API Tvorba žetona profila). Pri uporabi tega mehanizma strežnik preveri veljavnost žetona profila in poveže DN načrtovanega profila uporabnika s povezavo (na primer os400-profile=JSMITH,cn=accounts,os400-system=my-as400.mycompany.com). Če aplikacija že ima žeton profila, se s tem mehanizmom izognete iskanju imena profila uporabnika in gesla za izvedbo preproste povezave. Za uporabo tega mehanizma uporabite API ldap_sasl_bind s, ki podaja ničelni DN, OS400-PRFTKN za mehanizem in berval (dvojiški podatki, kodirani s poenostavljenimi pravili za osnovno kodiranje), ki vsebuje 32-bajtni žeton profila za poverilnice.

LDAP kot overitvena storitev

LDAP se običajno uporablja za nudenje overitvene storitve. Za overjanje v LDAP lahko konfigurirate spletni strežnik. Z nastavitvijo več spletnih strežnikov (ali drugih aplikacij) za overjanje v LDAP lahko vzpostavite uporabniški register za te aplikacije, namesto da vedno znova definirate uporabnike za vsako aplikacijo ali primerek spletnega strežnika.

Kako to deluje? Spletni strežnik pozove uporabnika, naj vnese ime uporabnika in geslo. Spletni strežnik s temi informacijami izvede iskanje v imeniku LDAP, kjer išče vnos s tem imenom uporabnika (spletni strežnik lahko na primer konfigurirate tako, da preslika ime uporabnika v atributa LDAP 'uid' ali 'mail'). Če najde natančno en vnos, pošlje povezovalno zahtevo strežniku z DN-jem pravkar najdenega vnosa in uporabniško podanim geslom. Če povezava uspe, je uporabnik overjen. Za zaščito gesel pred pregledovanjem na ravni protokola lahko uporabite povezave SSL.

Spletni strežnik lahko tudi sledi uporabljenemu DN-ju, tako da ga lahko določena aplikacija uporabi, na primer tako, da shrani podatke o prilagajanju v ta vnos, v drug vnos, povezan z njim ali v ločeno bazo podatkov, ki uporablja DN kot ključ za iskanje informacij.

Alternativa uporabi povezovalne zahteve je uporaba primerjalne operacije LDAP, kot je na primer ldap_compare(ldap_session, dn, "userPassword", enteredPassword). S tem je aplikaciji namesto zagona in zaustavitve sej za vsako overitveno zahtevo omogočena uporaba ene seje LDAP.

Ozadje, določeno z operacijskim sistemom

Sistemsko določeno ozadje lahko preslika objekte i5/OS kot vnose v drevesu imenikov, ki je dostopen LDAP. Projicirani objekti so predstavitve LDAP objektov i5/OS namesto dejanskih vnosov, shranjenih v bazi podatkov strežnika LDAP. Uporabniški profili so edini objekti, ki so preslikani ali načrtovani kot vnosi znotraj imeniškega drevesa. Preslikava objektov profila uporabnikov se nanaša na uporabniško projicirana ozadja i5/OS.

Operacije LDAP se preslikajo na podrejene objekte i5/OS in operacije LDAP izvedejo funkcije operacijskega sistema, da lahko dostopajo do teh objektov. Vse operacije LDAP, ki se izvedejo na profilih uporabnikov, se izvedejo pod pooblastilom profila uporabnika, povezanega s povezavo odjemalca.

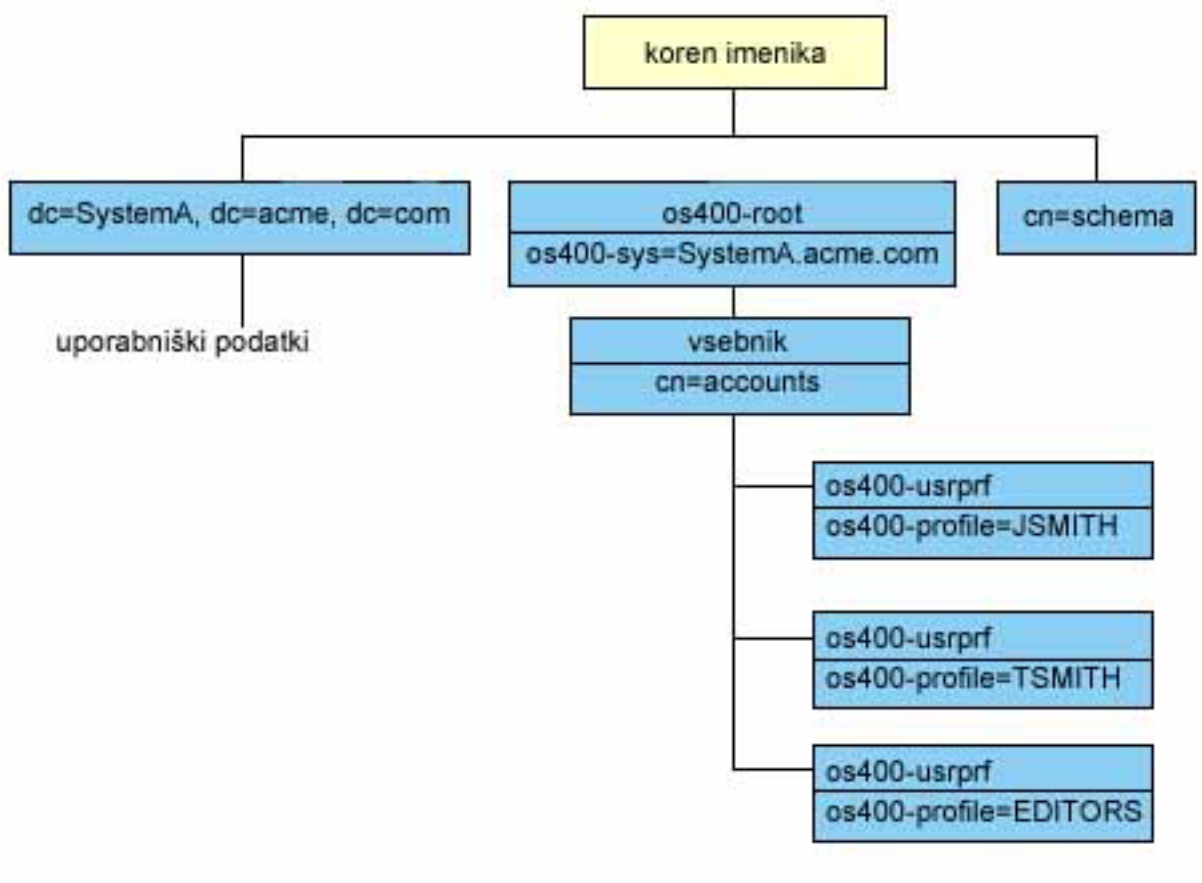
Podrobnejše informacije o ozadju, ki je določeno z operacijskim sistemom, boste našli v naslednjih temah:

- "Uporabniško projicirano drevo imeniških informacij i5/OS"
- "Operacije LDAP" na strani 65
- "Povezovalni DN-ji skrbnika in kopije" na strani 69
- "i5/OS uporabniško projicirana shema" na strani 69

Uporabniško projicirano drevo imeniških informacij i5/OS

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

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



Koren drevesa je pripona, katere privzeta vrednost je os400-sys=*SystemA.acme.com*, kjer je *SystemA.acme.com* ime vašega sistema. Razred objektov (objectclass) je os400-root. Čeprav DIT-a ni mogoče spremeniti ali zbrisati, lahko ponovno konfigurirate pripono objektov sistema. Vendar pa morate zagotoviti, da trenutna pripona ni uporabljena v ACL-jih ali kjerkoli drugje v sistemu, kjer je v primeru spremembe pripone potrebno spremeniti vnose.

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

Operacije LDAP

Z uporabo projiciranih profilov uporabnikov lahko izvedete naslednje operacije LDAP.

Povezovanje

Odjemalca LDAP lahko povežete (overite) s strežnikom LDAP z uporabo projiciranega profila uporabnika. To naredite tako, da podate razločevalno ime (DN) projiciranega profila uporabnika za povezovalni DN in pravilno geslo profila uporabnika i5/OS za overjanje. Zgled razločevalnega imena, uporabljenega v zahtevi za povezovanje, je os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com.

Odjemalec se mora povezati kot projicirani uporabnik, če želite dostopati do informacij v sistemsko projiciranem ozadju.

Za overjanje v imeniškem strežniku kot uporabnik i5/OS sta na voljo dodatna mehanizma:

- Povezovanje GSSAPI SASL. Če je i5/OS konfiguriran za uporabo EIM (Enterprise Identity Mapping), izvede imeniški strežnik poizvedbo v EIM, da določi, ali obstaja povezava z lokalnim profilom uporabnika i5/OS iz začetne identitete Kerberos. Če takšna povezava obstaja, strežnik poveže profil uporabnika s povezavo, ki jo lahko uporabite za dostopanje do sistemsko projiciranega ozadja. Dodatne informacije o EIM boste našli v temi EIM.
- Povezovanje OS400-PRFTKN SASL. Za overjanje v imeniškem strežniku lahko uporabite žeton profila. Strežnik poveže profil uporabnika žetona profila s povezavo.

Strežnik izvede vse operacije z uporabo pooblastila tega profila uporabnika. DN projiciranega profila uporabnika lahko uporabite tudi v ACL-ih LDAP, enako kot DN-je vnosov LDAP. Preprosta metoda povezovanja je edina povezovalna metoda, ki je dovoljena, če je na zahtevi za povezovanje podan projiciran profil uporabnika.

Iskanje

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

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

Naslednja tabela opisuje obnašanje sistemsko projiciranega ozadja za operacije iskanja.

Tabela 2. Obnašanje sistemsko projiciranega ozadja za operacije iskanja

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

Tabela 2. Obnašanje sistemsko projiciranega ozadja za operacije iskanja (nadaljevanje)

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

Primerjava

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

Dodajanje in spreminjanje

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

Brisanje

Profile uporabnikov lahko zbrišete z uporabo operacije za brisanje LDAP. Če želite podati obnašanje parametrov DLTUSRPRF OWNOBJOPT in PGPOPT, sta na voljo dva krmilna elementa strežnika LDAP. Podate ju lahko pri operaciji brisanja LDAP. Dodatne informacije o vedenju teh parametrov boste našli v opisu ukaza DLTUSRPRF (Delete User Profile - Zbriši profil uporabnika).

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

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  Krmilna vrednost je niz v naslednji obliki:
  - controlValue ::= ownObjOpt [newOwner]
  - ownObjOpt ::= *NODLT / *DLT / *CHGOWN

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

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

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

    Krmilna vrednost je definirana kot niz v naslednji obliki:

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

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

  Zgledi vrednosti krmilnih elementov:
  - *NOCHG: podaja, da profila ni mogoče zbrisati, če je primarna skupina za katerikoli objekt.
  - *CHGPGP *NONE: podaja odstranitev primarne skupine za objekte.
  - *CHGPGP SMITH *USE: podaja spreminjanje primarne skupine v profil uporabnika SMITH in dodelitev pooblastila *USE primarni skupini.

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

ModRDN

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

Uvažanje in izvažanje API-jev

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

Povezovalni DN-ji skrbnika in kopije

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

Če želite več informacij, poglejte “Delo z upravnim dostopom za pooblaščene uporabnike” na strani 99.

i5/OS uporabniško projicirana shema

Razrede in lastnosti objektov iz projiciranega ozadja lahko najdete v shemi strežnika. Imena atributov LDAP imajo obliko os400–*nnn*, kjer je *nnn* običajno ključna beseda atributa v ukazih profilov uporabnikov. Atribut os400-usrcls na primer ustreza parametru USRCLS ukaza CRTUSRPRF. Vrednosti atributov ustrezajo vrednostim parametrov, ki jih sprejmeta ukaza CRTUSRPRF in CHGUSRPRF, ali vrednostim, ki so prikazane pri prikazu profila uporabnika. Za prikaz definicij objektnega razreda os400-usrprf in povezanih atributov os400-xxx uporabite orodje za spletno upravljanje ali kakšno drugo aplikacijo.

Podpora za beleženje imeniškega strežnika in i5/OS

Imeniški strežnik uporablja za shranjevanje imeniških informacij podporo za bazo podatkov i5/OS. Za shranjevanje imeniških vnosov v bazo podatkov uporablja krmiljenje potrditev. Za to je potrebna podpora za beleženje i5/OS.

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

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

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

Okolje, velikost in struktura imenika, strategija shranjevanja in obnavljanja lahko narekujejo nekatere spremembe od privzetih vrednosti, vključno z načinom upravljanja objektov ter uporabljenim pragom velikosti. Če je potrebno, lahko spremenite parametre ukaza za vodenje dnevnika. Beleženje LDAP je po privzetku nastavljeno za brisanje starih prejemnikov. Če je dnevnik sprememb konfiguriran in želite ohraniti stare prejemnike, v ukazni vrstici i5/OS izvršite naslednji ukaz:

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

Če je konfiguriran dnevnik sprememb, lahko z naslednjim ukazom zbrišete njegove stare sprejemnike dnevnika:

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

Informacije o ukazih beleženja boste našli v razdelku Ukazi “OS/400” teme Programiranje.

Operacijski atributi

Na voljo je več atributov, ki imajo poseben pomen za imeniški strežnik, in jih imenujemo operacijski atributi. Vzdržuje jih strežnik in odražajo informacije, ki jih upravlja strežnik o vnosu ali vplivajo na delovanje strežnika. Z njimi so povezane posebne značilnosti:

- iskalna operacija ne vrne atributov, če niso posebej zahtevani (z imenom) v iskalni zahtevi
- atributi niso del nobenega objektnega razreda; kateri vnosi imajo atribute krmili strežnik

Imeniški strežnik podpira naslednje skupine operacijskih atributov:

- creatorsName, createTimestamp, modifiersName, modifyTimestamp. Predstavljeni so v vsakem vnosu. Ti atributi prikažejo povezovalni DN in čas prve izdelave ali čas zadnjega spreminjanja vnosa. Uporabite jih lahko v iskalnih filtrih, če želite na primer najti vse vnose, ki so bili spremenjeni po določeni uri. Spremeniti jih ne more noben uporabnik.
- ibm-entryuuid. Predstavljen je v vsakem vnosu, ki je izdelan, če strežnik uporablja izdajo V5R3 ali novejšo. Ta atribut je univerzalno unikaten identifikator niza, ki ga dodeli strežnik vsakemu vnosu pri izdelavi. Uporaben je za aplikacije, ki morajo razločevati med identično poimenovanimi vnosi na različnih strežnikih. Atribut z algoritmom DCE UUID ustvari ID, ki je unikaten v vseh vnosih na vseh strežnikih, in uporablja časovni žig, naslov vmesnika in druge informacije.
- entryowner, ownersource, ownerpropagate, aclentry, aclsource, aclpropagate, ibm-filteracl, ibm-filteraclinherit, ibm-effectiveAcl. Dodatne informacije boste našli v razdelku “Seznami za nadzor dostopa” na strani 47.
- hasSubordinates. Predstavljen je v vsakem vnosu in ima vrednost TRUE, ki ima vnos podrejene vnose.
- numSubordinates. Predstavljen je v vsakem vnosu in vsebuje število vnosov, ki so podrejeni temu vnosu.
- pwdChangedTime, pwdAccountLockedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdReset, pwdHistory. (atributi načel za gesla)
- subschemasubentry - predstavljen je v vsakem vnosu in določa mesto sheme za ta del drevesa. To je uporabno za strežnike z več shemami, če želite najti shemo, ki jo lahko uporabite kot del drevesa.

Krmilni elementi in razširjene operacije

Krmilni elementi

Krmilni elementi nudijo dodatne informacije za strežnik, ki krmili, kako bo interpretirana določena zahteva. Krmilni element za brisanje poddrevesa lahko na primer podate v zahtevi za brisanje LDAP, in kaže, naj strežnik zbriše vnos in vse njegove podrejene vnose in ne samo podanega vnosa. Krmilni element je sestavljen iz treh delov:

- tipa krmilnega elementa, ki je OID, ki določa krmilni element
- indikatorja kritičnosti, ki podaja, kako naj se vede strežnik, če krmilnega elementa ne podpira; to je boolova vrednost; vrednost FALSE kaže, da krmilni element ni kritičnega pomena, zato jo lahko strežnik v primeru, da je ne podpira, zanemari; vrednost TRUE kaže, da je krmilni element kritičnega pomena, zato celotna zahteva ne bo uspela (in vrnila napako zaradi nepodprtega kritičnega dodatka), če strežnik ne more sprejeti krmilnega elementa
- neobvezne vrednosti krmilnega elementa, ki vsebuje druge informacije, specifične za krmilni element; vsebina vrednosti krmilnega elementa je podana z zapisom ASN.1; sama vrednost je kodiranje BER podatkov krmilnega elementa.

Imeniški strežnik podpira naslednje krmilne elemente:

Ime	OID	Najstarejša izdaja OS/400	Najstarejša izdaja strežnika IBM Directory Server	opis
Upravljanje DSA IT	2.16.840.1.1137.30.3.4.2	V4R5	V3.2	Obravnavanje vnosov referenčnih kazalcev kot običajne vnose

Ime	OID	Najstarejša izdaja OS/400	Najstarejša izdaja strežnika IBM Directory Server	opis
Transakcija	1.3.18.0.2.10.5	V4R5	V3.2	Označitev operacije kot dela transakcije
OS/400 DLTUSRPRF OWNOBJOPT	1.3.18.0.2.10.8	V5R2		Možnost brisanja profila uporabnika za lastnika objekta Podrobnosti boste našli v razdelku “Ozadje, določeno z operacijskim sistemom” na strani 64.
OS/400 DLTUSRPRF PGPOPT	1.3.18.0.2.10.9	V5R2		Možnost brisanja profila uporabnika OS/400 za primarno skupino Podrobnosti boste našli v razdelku “Ozadje, določeno z operacijskim sistemom” na strani 64.
Razvrščeno iskanje	1.2.840.113556.1.4.473 (zahteva) in 1.2.840.113556.1.4.474 (odziv)	V5R2 s PTF-jem	V4.1	Razvrstitev rezultatov iskanja pred vrnitvijo rezultatov odjemalcu
Iskanje po straneh	1.2.840.113556.1.4.319	V5R2 s PTF-jem	V4.1	Vrnitev rezultatov iskanja odjemalcu po straneh namesto naenkrat
Krmilni element brisanja drevesa	1.2.840.113556.1.4.805	V5R3	V5.1	Ta krmilni element je pripet zahtevi za brisanje in kaže, da želite zbrisati podan vnos in vse njegove naslednike. Uporabnik mora biti skrbnik imenika. Vnos, ki ga želite zbrisati, ne sme biti kontekst podvajanja.
Načela za gesla	1.3.6.1.4.1.42.2.27.8.5.1	V5R3	V5.1	Vrnitev dodatnih informacij o napaki v načelih za gesla odjemalcu

Ime	OID	Najstarejša izdaja OS/400	Najstarejša izdaja strežnika IBM Directory Server	opis
Upravljanje strežnika	1.3.18.0.2.10.15	V5R3	V5.1	Skrbniku omogoča izvedbo vzdrževalnih operacij, ki bi bile sicer zavrnjene (na primer ažuriranje kopije samo za branje, ažuriranje mirujočega strežnika ali niz določenih operacijskih atributov).

Razširjene operacije

Razširjene operacije se uporabljajo za zagon dodatnih operacij, ki presegajo osnovne operacije LDAP. Razširjene operacije lahko na primer definirajo združitev niza operacij v eno transakcijo. Razširjena operacija je sestavljena iz naslednjega:

- imena zahteve; to je OID, ki določa specifično operacijo
- neobvezne vrednosti zahteve, ki vsebuje druge informacije, specifične za operacijo; vsebina vrednosti zahteve je podana z zapisom ASN.1; sama vrednost je kodiranje BER podatkov zahteve.

Razširjene operacije imajo običajno razširjen odziv, ki je sestavljen iz naslednjega:

- komponent standardnega rezultata LDAP (koda napake, primerjani DN in sporočilo o napaki)
- odzivnega imena; to je OID, ki določa tip odziva
- neobvezne vrednosti, ki vsebuje druge informacije, specifične za odziv; vsebina odzivne vrednosti je podana z zapisom ASN.1; sama vrednost je kodiranje BER podatkov odziva.

Imeniški strežnik podpira naslednje razširjene zahteve:

Ime	OID	Najstarejša izdaja OS/400	Najstarejša izdaja strežnika IBM Directory Server	opis
Register za dogodke	1.3.18.0.2.12.1	V4R5	V3.2	
Odstranitev registra za dogodke	1.3.18.0.2.12.3	V4R5	V3.2	
Začetek transakcije	1.3.18.0.2.12.5	V4R5	V3.2	
Konec transakcije	1.3.18.0.2.12.6	V4R5	V3.2	
Zahteva za normalizacijo DN-ja	1.3.18.0.2.12.30	V5R3	V5.1	

Definirane so tudi dodatne razširjene operacije, ki pa jih ne zažene odjemalec. Uporabljajo se prek pripomočka ldapexop ali operacij, ki jih izvaja orodje za spletno upravljanje. Te operacije in pooblastilo, potrebno za njihov zagon, so navedeni spodaj:

Ime	OID	Najstarejša izdaja OS/400	Najstarejša izdaja strežnika IBM Directory Server	opis
Krmiljenje podvajanja	1.3.18.0.2.12.16	V5R3	V5.1	Ta operacija izvede zahtevano dejanje v strežniku, na katerem je izdana, in prenese klic vsem potrošnikom, ki so v topologiji podvajanja pod njim. Odjemalec mora biti skrbnik imenika ali pa imeti pisalno pooblastilo za objekt ibm-replicagroup=default povezanega konteksta podvajanja.
Čakalna vrsta krmiljenja podvajanja	1.3.18.0.2.12.17	V5R3	V5.1	Ta operacija označi elemente kot že podvojene za določen dogovor. Dovoljena je samo, če ima odjemalec pisalno pooblastilo za dogovor o podvajanju.
Preklopi v mirujoče stanje ali prekini mirujoče stanje	1.3.18.0.2.12.17	V5R3	V5.1	Ta operacija preklopi poddrevo v stanje, v katerem ne more sprejemati popravkov odjemalca (ali to stanje prekine), razen za tiste odjemalce, ki so overjeni kot skrbniki imenika, kjer je prisoten krmilni element za upravljanje strežnika. Odjemalec mora biti overjen kot skrbnik imenika ali imeti pisalno pooblastilo za objekt ibm-replicagroup=default povezanega konteksta podvajanja.
Konec transakcije	1.3.18.0.2.12.19	V5R3	V5.1	

Ime	OID	Najstarejša izdaja OS/400	Najstarejša izdaja strežnika IBM Directory Server	opis
Lestvičeno krmiljenje podvajanja	1.3.18.0.2.12.15	V5R3	V5.1	Ta operacija izvede zahtevano dejanje v strežniku, na katerem je izdana, in prenese klic vsem potrošnikom, ki so v topologiji podvajanja pod njim. Odjemalec mora biti skrbnik imenika ali pa imeti pisalno pooblastilo za objekt ibm-replicagroup=default povezanega konteksta podvajanja.
Ažuriranje konfiguracije	1.3.18.0.2.12.28	V5R3	V5.1	Ta operacija povzroči, da strežnik na novo prebere podane nastavitve iz konfiguracije. Dovoljena je samo, če je odjemalec skrbnik imenika.

Poglavje 5. Prvi koraki z imeniškim strežnikom

Imeniški strežnik se samodejno namesti pri namestitvi sistema i5/OS in vključuje privzeto konfiguracijo. Z imeniškim strežnikom začnete delati takole:

1. Če nameščate V5R3 in ste uporabljali imeniški strežnik že v prejšnji izdaji, preglejte vprašanja, povezana s selitvijo. Dodatne informacije boste našli v razdelku “Problematika selitve”.
2. Izdelajte načrt za imeniški strežnik. Dodatne informacije boste našli v razdelku “Načrtovanje imeniškega strežnika” na strani 79.
3. Za prilagoditev nastavitev imeniškega strežnika zaženite čarovnika za konfiguriranje imeniškega strežnika. Dodatne informacije boste našli v razdelku “Konfiguriranje imeniškega strežnika” na strani 80.
4. Zaženite strežnik. Dodatne informacije boste našli v razdelku “Zagon imeniškega strežnika” na strani 94.
5. Z orodjem za spletno upravljanje izdelajte ali uredite imenike LDAP. Dodatne informacije boste našli v razdelku “Spletno upravljanje” na strani 81.
6. Dodatne informacije o tem, kako izvajati različne naloge imeniškega strežnika, boste našli v razdelku Poglavje 7, “Upravljanje imeniškega strežnika”, na strani 93.

Problematika selitve

Imeniški strežnik se samodejno namesti pri namestitvi sistema i5/OS. Pri prvem zagonu strežnik samodejno preseli obstoječo konfiguracijo in podatke, kar lahko povzroči precejšnjo zakasnitev zagona.

Če izvajate imeniški strežnik pod izdajo V5R2 ali V5R1, preglejte razdelek “Selitev v V5R3 iz V5R2 ali V5R1”.

Če izvajate imeniški strežnik pod izdajo V4R3, V4R4 ali V4R5, lahko preselite podatke v V5R3. Dodatne informacije boste našli v razdelku “Selitev podatkov iz V4R3, V4R4 ali V4R5 v V5R3” na strani 76.

Če uporabljate omrežje strežnikov za podvajanje, boste našli dodatne informacije v razdelku “Selitev omrežja strežnikov za podvajanje” na strani 77.

Če uporabljate Kerberos, preglejte razdelek “Sprememba storitvenega imena Kerberos” na strani 79.

Selitev v V5R3 iz V5R2 ali V5R1

V izdaji OS/400 V5R3 smo vpeljali v imeniški strežnik nove funkcije in zmožnosti. Te spremembe se nanašajo na imeniški strežnik LDAP in na grafični uporabniški vmesnik (GUI) Navigatorja iSeries. Da bi lahko izkoristili prednost novih možnosti GUI, morate namestiti Navigator iSeries v PC, ki lahko prek TCP/IP komunicira s strežnikom iSeries. Navigator iSeries je komponenta iSeries Access za Windows. Če imate nameščeno starejšo različico Navigatorja iSeries, opravite nadgraditev v V5R3.

Izdaja OS/400 V5R3 podpira nadgradnje iz V5R1 in V5R2. Če izvedete nadgradnjo iz izdaje OS/400 V5R3, so imeniški podatki LDAP in datoteke imeniških shem samodejno preseljeni tako, da ustrezajo formatom izdaje V5R3.

Pri selitvi v izdajo OS/400 V5R3 morate upoštevati nekatera vprašanja, povezana s selitvijo:

- Pri selitvi v V5R3 imeniški strežnik samodejno preseli datoteke shem v V5R3 in zbriše stare datoteke shem. Če ste datoteke shem zbrisali ali preimenovali, jih imeniški strežnik ne more preseliti. V tem primeru lahko pride do napake ali pa imeniški strežnik sklepa, da so datoteke že preseljene.
- Imeniški strežnik preseli imeniške podatke v format V5R3 pri prvem zagonu strežnika ali uvozu datoteke LDIF. Za izvedbo preselitve morate omogočiti dovolj časa.

  Po končani nadgraditvi v V5R3 zaženite strežnik, da preselite obstoječe podatke, preden uvozite nove. Če poskušate uvoziti podatke pred zagonom strežnika in nimate zadostnih pooblastil, uvažanje ne bo uspelo.

- Po izvedeni selitvi se bo imeniški strežnik LDAP samodejno zagnal ob zagonu TCP/IP. Če ne želite samodejnega zagona imeniškega strežnika, lahko to nastavitev spremenite s pomočjo Navigatorja iSeries.

Selitev podatkov iz V4R3, V4R4 ali V4R5 v V5R3

Izdaja OS/400 V5R3 ne podpira neposrednih nadgraditev iz izdaj V4R3, V4R4 ali V4R5. Selitev imeniškega strežnika V4R3, V4R4 ali V4R5 v V5R3 lahko opravite z enim od naslednjih postopkov:

- "Nadgraditev OS/400 iz V4R3, V4R4 ali V4R5 v vmesno izdajo"
- "Shranitev knjižnice baze podatkov in namestitev V5R3" na strani 77

Preden začnete, preberite naslednje:

- Pri nadgrajevanju iz V4R3 v katerokoli kasnejšo različico morate upoštevati naslednje:
  - **Preselitev datoteke obroča ključev v bazo podatkov ključev:**

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

    Naslednji tokovni datoteki, ki jih je v V4R3 uporabljal imeniški strežnik, nista več potrebni, in se samodejno odstranita pri namestitvi kasnejše različice:

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

    S temi datotekami vam ni treba storiti ničesar. To je omenjeno samo zato, da vas ne bo skrbelo, ker datotek ni več v sistemu.
- Izdaja V4R4 in starejše izdaje imeniškega strežnika pri izdelavi vnosov časovnega žiga niso upoštevale časovnih pasov. Začenši z različico V4R5 se časovni pas uporablja v vseh dodatkih in popravkih imenika. Če torej nadgradite podatke iz V4R4 ali starejše izdaje, imeniški strežnik prilagodi obstoječa atributa createtimestamp in modifytimestamp, tako da odražata pravilen časovni pas. To naredi tako, da odšteje časovni pas, ki je trenutno definiran v sistemu iSeries od časovnih pasov, ki so shranjeni v imeniku. Če trenutni časovni pas (time) ni tisti časovni pas, ki je bil aktiven pri izvirnem izdelovanju ali spreminjanju, nove vrednosti časovnega pasu ne bodo odražale izvirnega časovnega pasu.
- Če nadgrajujete podatke iz V4R4 ali starejše izdaje, se morate zavedati, da bodo imeniški podatki zahtevali približno dvakrat toliko pomnilniškega prostora kot predhodno. Razlog za to je, da je imeniški strežnik v V4R4 ali starejših izdajah podpiral samo nabor znakov IA5 in je shranil podatke v ccsid 37 (enobajtni format). Imeniški strežnik zdaj podpira celoten nabor znakov ISO 10646. Po končani nadgraditvi zaženite strežnik, da preselite obstoječe podatke, preden uvozite nove. Če poskušate uvoziti podatke pred zagonom strežnika in nimate zadostnih pooblastil, uvažanje ne bo uspelo.
- Upoštevati morate tudi, da je z nadgrajevanjem v trenutno izdajo iz drugih izdaj povezana dodatna problematika.

Nadgraditev OS/400 iz V4R3, V4R4 ali V4R5 v vmesno izdajo

Čeprav nadgradnje iz izdaj OS/400 V4R3, V4R4 in V4R5 v V5R3 niso podprte, so veljajo naslednje izjeme:

- nadgradnja iz V4R3 in V4R4 v V4R5
- nadgradnja iz V4R4 in V4R5 v V5R1
- nadgradnja iz V4R5 in V5R1 v V5R2
- nadgradnja V5R1 in V5R2 v V5R3

Eden od načinov, na katerega lahko preselite imeniški strežnik, je z nadgraditvijo v vmesno izdajo (V5R1 ali V5R2), nato pa v V5R3. Podrobne informacije o namestitvenih postopkih za OS/400 boste našli v priročniku *Software Installation*  . Sledite splošnemu postopku za izvedbo selitve:

1. Zapišite si vse spremembe, ki jih izvedete v datotekah sheme v imeniku /QIBM/UserData/OS400/DirSrv. Datoteke sheme se preselijo samodejno.
2. Za V5R3 namestite V4R5.
3. Za V4R4 ali V4R5 namestite V5R1 ali V5R2.

4. Opravite namestitev v V5R3.
5. Če imeniški strežnik še ni zagnan, ga zaženite.
6. Z orodjem za spletno upravljanje popravite datoteke shem za vse uporabniške spremembe, ki ste si jih zapisali v koraku 1 na strani 76.
7. Znova zaženite imeniški strežnik.

Shranitev knjižnice baze podatkov in namestitev V5R3

Imeniški strežnik lahko preselite tako, da shranite bazo podatkov, ki jo uporablja, v V4R3, V4R4 ali V4R5, nato pa jo po namestitvi V5R3 obnovite. S tem si prihranite korak namestitve vmesne izdaje. Toda nastavitev strežnika ne preselite, zato jih morate na novo konfigurirati. Podrobne informacije o namestitvenih postopkih OS/400 boste našli v priročniku *Software Installation*  . Sledite splošnemu postopku za izvedbo selitve:

1. Zapišite si vse spremembe, ki jih izvedete v datotekah sheme v imeniku /QIBM/UserData/OS400/DirSrv. Datoteke sheme se ne preselijo samodejno. Če želite ohraniti spremembe, jih boste morali znova izvesti ročno.
2. Zapišite si različne konfiguracijske nastavitve v lastnostih imeniškega strežnika, vključno z imenom knjižnice baze podatkov.
3. Shranite knjižnico baze podatkov, ki je podana v konfiguraciji imeniškega strežnika. Če ste konfigurirali dnevnik sprememb, morate shraniti tudi knjižnico QUSRDIRCL.
4. Zapišite si konfiguracijo objavljanja.
5. V sistem namestite izdajo imeniškega strežnika V5R3.
6. Za konfiguriranje imeniškega strežnika uporabite čarovnika EZ-Setup.
7. Obnovite knjižnico baz podatkov, ki ste jo shranili v koraku 3. Če ste v koraku 3 shranili knjižnico QUSRDIRCL, jo obnovite.
8. Z orodjem za spletno upravljanje popravite datoteke shem za vse uporabniške spremembe, ki ste si jih zapisali v koraku 1.
9. Z Navigatorjem iSeries na novo konfigurirajte imeniški strežnik. Podajte knjižnico baze podatkov, ki ste jo predhodno konfigurirali ter shranili in obnovili v prejšnjih korakih.
10. Z Navigatorjem iSeries znova konfigurirajte objavljanje.
11. Znova zaženite imeniški strežnik.

Selitev omrežja strežnikov za podvajanje

Ko prvič zaženete glavni strežnik, le-ta preseli informacije v imeniku, ki krmilijo podvajanje. Vnosi z objektnim razredom replicaObject pod cn=localhost so nadomeščeni z vnosi, ki jih uporablja nov model podvajanja (dodatne informacije boste našli v razdelku “Podvajanje” na strani 34). Glavni strežnik je konfiguriran tako, da podvoji vse pripone v imeniku. Vnosi dogovora so izdelani z atributom ibm-replicationOnHold, ki je nastavljen na true. S tem je omogočeno, da se popravki, ki jih opravite v glavnem strežniku, nabirajo, dokler strežnik za podvajanje ni pripravljen.

Te vnose imenujemo topologija podvajanja. Novi glavni strežnik lahko uporabite s strežniki za podvajanje, v katerih se izvajajo starejše različice; podatki, ki so povezani z novimi funkcijami, ne bodo podvojeni v strežnike nižjih ravni. Vnose topologije podvajanje morate izvoziti iz glavnega strežnika in jih po selitvi strežnika za podvajanje dodati v vsak dvojnik. Za izvoz vnosov uporabite orodje ukazne vrstice Qshell “ldapsearch” na strani 169 in shranite izhodne podatke v datoteko. Ukaz za iskanje je podoben naslednjemu:

```
ldapsearch -h gostiteljsko-ime-glavnega-strežnika -p vrata-glavnega-strežnika \
 -D upravni-DN-glavnega-strežnika -w
 upravno-geslo-glavnega-strežnika \
 -b ibm-replicagroup=default,DN-vnosa-pripone \
 -L "(|(objectclass=ibm-replicaSubEntry)(objectclass=ibm-replicationAgreement))" \
     > replication.topology.ldif
```

S tem ukazom izdelate v trenutnem delovnem imeniku izhodno datoteko LDIF, imenovano replication.topology.ldif. Datoteka vsebuje samo nove vnose.

Opomba: Naslednjih pripon ne vključite:

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

Vključite samo uporabniško izdelane pripone.

Ponovite ukaz za vsak vnos pripone v glavnem strežniku, vendar nadomestite “>” z “>>”, da pripnete podatke izhodni datoteki za nadaljnja iskanja. Ko je datoteka končana, jo prekopirajte v strežnike za podvajanje.

Ko so strežniki za podvajanje uspešno preseljeni, jim dodajte datoteko; datoteke ne dodajte v strežnike, v katerih se izvajajo starejše različice imeniškega strežnika. Preden dodate datoteko, morate strežnik zagnati in zaustaviti.

Strežnik zaženite z možnostjo **Start** v Navigatorju iSeries. Če želite več informacij, poglejte “Zagon imeniškega strežnika” na strani 94.

Strežnik zaustavite z možnostjo **Ustavi** v Navigatorju iSeries. Dodatne informacije boste našli v “Zaustavitev imeniškega strežnika” na strani 94.

Ko dodate datoteko v strežnik za podvajanje, ta ne sme biti zagnan. Podatke dodajte z možnostjo **Uvozi datoteko** Navigatorja iSeries.

Ko naložite vnose topologije podvajanja, zaženite strežnik za podvajanje in obnovite podvajanje. Podvajanje lahko z enim od naslednjih načinov:

- V glavnem strežniku uporabite možnost orodja za spletno upravljanje **Upravljaj čakalne vrste v upravljanju podvajanja**.
- Uporabite pripomoček ukazne vrstice **ldapexop**, Na primer:

```
ldapexop -h gostiteljsko-ime-glavnega-strežnika
-p  vrata-glavnega-strežnika \
 -D upravni-DN-glavnega-strežnika -w
 upravno-geslo-glavnega-strežnika \
 -op controlrepl -action resume -ra DN-dogovora-podvajanja
```

  Ta ukaz obnovi podvajanje za strežnik, ki je definiran v vnosu s podanim DN-jem.

Če želite določiti, kateri DN dogovora o podvajanju ustreza strežniku za podvajanje, preglejte datoteko replication.topology.ldif. Glavni strežnik bo zabeležil sporočilo, ki ga je zagnalo podvajanje za ta strežnik za podvajanje in opozorilo, da se ID glavnega strežnika v dogovoru ne ujema z ID-jem strežnika za podvajanje. Če želite ažurirati dogovor o podvajanju tako, da bo uporabljal pravilni ID strežnika, uporabite funkcijo **upravljanja podvajanja** v orodju za spletno upravljanje ali pa orodje ukazne vrstice **ldapmodify**, Na primer:

```
ldapmodify -c -h gostiteljsko-ime-glavnega-strežnika -p vrata-glavnega-strežnika \
 -D upravni-DN-glavnega-strežnika -w
 upravno-geslo-glavnega-strežnika
dn: DN-dogovora-podvajanja
changetype: modify
replace: ibm-replicaConsumerID
ibm-replicaConsumerID: ID-strežnika-za-podvajanje
```

Te ukaze lahko vnesete neposredno v ukazno vrstico ali pa jih shranite v datoteko LDIF in jih podate za ukaz z možnostjo **-i** *datoteka*. Ukaz zaustavite z možnostjo **Zaključi prejšnjo zahtevo**.

Selitev za ta strežnik za podvajanje je končana.

Če želite še naprej uporabljati strežnik za podvajanje, v katerem se izvaja prejšnja različica, morate obnoviti podvajanje z orodjem ukazne vrstice **ldapexop** ali s funkcijo **upravljanja podvajanja** v orodju za spletno upravljanje tega

strežnika za podvajanje. Če preselite strežnik za podvajanje, v katerem se izvaja starejša različica, kasneje, z orodjem ukazne vrstice **ldapdiff** uskladite imeniške podatke. S tem zagotovite, da bodo vnosi ali atributi, ki niso bili podvojeni, v strežniku za podvajanje ažurirani.

Sprememba storitvenega imena Kerberos

V izdaji V5R3 smo spremenili storitveno ime, ki ga uporablja imeniški strežnik, in odjemalske API-je za overjanje GSSAPI (Kerberos). Ta sprememba ni združljiva s storitvenim imenom, ki smo ga uporabljali pred izdajo V5R3 (V5R2M0 PTF 5722SS1-SI08487 vključuje enako spremembo).

Pred to izdajo so uporabljali imeniški strežnik i5/OS in odjemalski API-ji storitveno ime v obliki LDAP/gostiteljsko-ime-dns@področje-Kerberos, če je bil za overjanje uporabljen mehanizem GSSAPI (Kerberos). To ime ne ustreza standardom, ki definirajo overjanje GSSAPI, ki določajo, da se mora začeti ime principala z ″ldap″, izpisan z malimi črkami. Zaradi tega imeniški strežnik i5/OS in odjemalski API-ji ne morejo delovati z izdelki drugih proizvajalcev. To še posebej velja, če uporablja razdelilni center ključev (KDC) Kerberos imena principalov, ki upoštevajo velike in male črke. Zgled odjemalca, vključenega v i5/OS, je ponudnik storitev LDAP za JNDI, splošno uporabljan odjemalski API Java, ki uporablja pravilno storitveno ime.

V5R3M0 spremeni storitveno ime tako, da ustreza standardom, vendar s tem povzroči lastne težave v združljivosti.

- Imeniški strežnik, ki je konfiguriran za uporabo overjanja GSSAPI, ne bo začel z nameščanjem te izdaje. Razlog za to je, da vsebuje datoteka keytab, ki jo uporablja strežnik, poverilnice s starim storitvenim imenom (LDAP/mysys.ibm.com@IBM.COM), strežnik pa išče poverilnice z novim storitvenim imenom (ldap/mysys.ibm.com@IBM.COM).
- Imeniški strežnik ali aplikacija LDAP, ki uporabljata API-je LDAP na ravni V5R3M0, se morda ne bosta uspela overiti s starejšimi strežniki ali odjemalci i5/OS. To težavo odpravite takole:
  1. Če uporablja KDC imena principalov, ki upoštevajo velike in male črke, izdelajte šifro, ki uporablja pravilno storitveno ime (ldap/mysys.ibm.com@IBM.COM).
  2. Datoteko keytab, ki jo uporablja imeniški strežnik i5/OS, ažurirajte tako, da bo vsebovala poverilnice za novo storitveno ime. Če želite, lahko stare poverilnice tudi zbrišete. Datoteko keytab lahko ažurirate tudi s pripomočkom Qshell keytab. Po privzetku uporablja imeniški strežnik datoteko /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab. Čarovnik za storitev omrežnega overjanja V5R3M0 (Kerberos) v Navigatorju iSeries izdela datoteko keytab z novim storitvenim imenom.
  3. Ažurirajte sisteme V5R2M0 i5/OS, v katerih je uporabljen GSSAPI, tako da uveljavite PTF 5722SS1-SI08487.

Če želite, pa lahko tudi pustite, da imeniški strežnik in odjemalski API-ji še naprej uporabljajo staro storitveno ime. To lahko naredite, če uporabljate overjanje Kerberos v mešanem omrežju sistemov, ki se izvajajo s PTF-ji in brez njih. V ta namen nastavite spremenljivko okolja LDAP_KRB_SERVICE_NAME. Za celoten sistem jo lahko nastavite z naslednjim ukazom (potrebno za nastavitev storitvenega imena za strežnik).

```
ADDENVVAR ENVVAR(LDAP_KRB_SERVICE_NAME)
```

ali pa v QSH (za vpliv na pripomočke LDAP, ki se izvajajo iz te seje QSH):

```
export LDAP_KRB_SERVICE_NAME=1
```

Načrtovanje imeniškega strežnika

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

- **Organiziranje imenika**. Načrtujte strukturo imenika in določite, katere pripone in lastnosti bo zahteval vaš strežnik. Dodatne informacije boste našli v razdelkih “Imeniki” na strani 7, “Pripona (kontekst poimenovanja)” na strani 14 in “Atributi” na strani 19.
- **Določitev velikosti imenika**. Nato lahko ocenite, koliko pomnilnika potrebujete. Velikost imenika je odvisna od:
  - števila lastnosti v shemi strežnika
  - števila vnosov v strežniku
  - tipa informacij, ki jih hranite v strežniku.

Prazen imenik, ki uporablja privzeto shemo imeniškega strežnika, zahteva približno 10 Mb pomnilniškega prostora. Imenik, ki uporablja privzeto shemo, in vsebuje 1000 vnosov tipičnih informacij o zaposlenih, zahteva približno 30 MB prostora. To število se spreminja glede na natančno število uporabljenih lastnosti. Zelo se poveča v primeru, če v imeniku hranite velike objekte, kot so slike.

- **Določanje varnostnih ukrepov**.

  Imeniški strežnik omogoča, da uveljavite načelo za gesla, s katerim zagotovite, da uporabniki občasno spremenijo svoja gesla in da le-ta ustrezajo sintaktičnim zahtevam za gesla v podjetju.

  Imeniški strežnik podpira uporabo plasti zaščitenih vtičnic (SSL) in digitalnih potrdil, kot tudi zaščito plasti prenosa (TLS) za varnost komunikacij. Podprto je tudi overjanje Kerberos.

  Imeniški strežnik omogoča, da krmilite dostop do imeniških objektov s seznami za nadzor dostopa (ACL-ji). Za zaščito imenika lahko uporabite tudi beleženje zaščite i5/OS.

  Dodatno se odločite, katero načelo za gesla boste uveljavili.
- **Izberite DN in geslo skrbnika**. Privzeti DN skrbnika je cn=administrator. To je edina identiteta, ki ima pooblastilo za izdelovanje ali spreminjanje imeniških vnosov pri začetni konfiguraciji strežnika. Uporabite lahko privzeti DN skrbnika ali pa izdelate drugega. Za DN skrbnika morate izdelati tudi geslo.
- **Namestite predpogojno programsko opremo za orodje za spletno upravljanje imeniškega strežnika**. Če želite uporabljati orodje za spletno upravljanje imeniškega strežnika, morate namestiti v strežnik iSeries naslednje predpogojne izdelke.
  - IBM HTTP Server za iSeries (5722-DG1)
  - IBM WebSphere Application Server - Express (osnova 5722-IWE in možnost 2)

  V temi IBM HTTP Server boste našli dodatne informacije o strežniku IBM HTTP Server za iSeries in strežniku IBM WebSphere Application Server - Express.

Konfiguriranje imeniškega strežnika

1. Če sistema ne konfigurirate za objavo informacij v drugem strežniku LDAP in strežnik TCP/IP DNS ne pozna nobenega strežnika LDAP, je imeniški strežnik samodejno nameščeno z omejeno privzeto konfiguracijo. Za dodatne informacije glejte “Privzeta konfiguracija za imeniški strežnik” na strani 81. Imeniški strežnik vsebuje čarovnika, ki vam bo pomagal pri konfiguriranju imeniškega strežnika za vaše specifične potrebe. Ta čarovnik lahko izvedete kot del programa EZ-Setup, oziroma ga izvedete pozneje iz Navigatorja iSeries. Tega čarovnika uporabite, ko prvikrat konfigurirate imeniški strežnik. Uporabite ga lahko tudi pri vnovični konfiguraciji imeniškega strežnika.

   Opomba: Če čarovnika uporabljate za vnovično konfiguriranje imeniškega strežnika, začenjate konfigurirati od začetka. Izvirno konfiguracijo raje zbrišite, kot pa da jo spremenite. Pri tem imeniških podatkov ne zbrišete, saj ostanejo shranjeni v knjižnici, ki ste jo izbrali za namestitev (po privzetku je to QUSRDIRDB). Dnevnik sprememb bo prav tako ostal nedotaknjen in bo po privzetku shranjen v knjižnici QUSRDIRCL.

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

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

   Za konfiguriranje strežnika morate imeti posebna pooblastila *ALLOBJ in *IOSYSCFG. Če želite konfigurirati beleženje zaščite OS/400, morate imeti tudi posebno pooblastilo *AUDIT.
2. Če želite zagnati čarovnika za konfiguracijo imeniški strežnik, storite naslednje:
   a. V Navigatorju iSeries razširite **Omrežje**.
   b. Razširite **Strežniki**.
   c. Kliknite **TCP/IP**.
   d. Z desnim gumbom miške kliknite **Imenik** in izberite **Konfiguriraj**.

   Opomba: Če ste imeniški strežnik že konfigurirali, raje kliknite **Znova konfiguriraj** kot pa **Konfiguriraj**.
3. Za konfiguriranje imeniškega strežnika sledite navodilom v čarovniku za konfiguriranje imeniškega strežnika.

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

4. Ko se čarovnik konča, je imeniški strežnik nastavljen z osnovno konfiguracijo. Če izvajate v sistemu Lotus Domino, lahko vrata 389 (privzeta vrata za strežnik LDAP) že uporablja funkcija LDAP Domino. Narediti morate eno od naslednjega:
   - Spremenite vrata, ki jih uporablja Lotus Domino. Dodatne informacije poiščite v razdelku " Gostovanje Domino LDAP in imeniškega strežnika na istem iSeries" v temi Elektronska pošta.
   - Spremenite vrata, ki jih uporablja imeniški strežnik. Za dodatne informacije glejte "Spreminjanje vrat ali naslova IP" na strani 96.
   - Uporabite specifične naslove IP. Za dodatne informacije glejte "Spreminjanje vrat ali naslova IP" na strani 96.
5. Izdelajte vnose, ki ustrezajo izdelani priponi ali priponam. Če želite več informacij, poglejte "Dodajanje in odstranjevanje pripon imeniškega strežnika" na strani 98.

Preden nadaljujete, lahko izvedete vse naslednje postopke ali pa samo nekatere med njimi:
- Uvozite podatke v strežnik; glejte "Uvažanje datoteke LDIF" na strani 97.
- Omogočite plast zaščitenih vtičnic (SSL); glejte "Omogočanje SSL v imeniškem strežniku" na strani 117.
- Omogočite overjanje Kerberos; glejte "Omogočanje overjanja Kerberos v imeniškem strežniku" na strani 119.
- Nastavite referenčni kazalec; glejte "Podajanje strežnika za referenčne kazalce imenika" na strani 97.

Privzeta konfiguracija za imeniški strežnik

Imeniški strežnik se samodejno namesti pri namestitvi OS/400. Ta namestitev vključuje privzeto konfiguracijo. Imeniški strežnik uporablja privzeto konfiguracijo, če velja vse od naslednjega:
- Skrbniki niso zagnali čarovnika za konfiguriranje imeniškega strežnika ali spremenili imeniških nastavitev s stranmi lastnosti.
- Objavljanje imeniškega strežnika ni konfigurirano.
- Imeniški strežnik ne more najti nobenih informacij o LDAP DNS.

Če uporablja imeniški strežnik privzeto konfiguracijo, se zgodi naslednje:
- Imeniški strežnik se zažene samodejno pri zagonu TCP/IP.
- Sistem izdela privzetega skrbnika, cn=Administrator. Ustvari tudi geslo, ki se uporablja interno. Če morate uporabiti geslo skrbnika kasneje, lahko nastavite novega na strani z lastnostmi imeniškega strežnika.
- Izdelana je privzeta pripona, ki temelji na imenu IP sistema. Na osnovi imena sistema se izdela tudi pripona sistemskih objektov. Če je na primer ime IP sistema mary.acme.com, je pripona dc=mary,dc=acme,dc=com.
- Imeniški strežnik uporablja privzeto podatkovno knjižnico QUSRDIRDB. Sistem jo izdela v sistemskem ASP.
- Za nezaščitene komunikacije uporablja strežnik vrata 389. Če je bilo digitalno potrdilo konfigurirano za LDAP, je plast zaščitenih vtičnic omogočena, za zaščitene komunikacije pa se uporabijo vrata 636.

Spletno upravljanje

Prek ukazne mize za spletno upravljanje lahko upravljate enega ali več imeniških strežnikov. Na ukazni mizi za spletno upravljanje lahko naredite naslednje:
- dodate ali spremenite seznam imeniških strežnikov za upravljanje
- upravljate imeniški strežnik z orodjem za spletno upravljanje
- spremenite atribute ukazne mize za spletno upravljanje.

Za uporabo ukazne mize za spletno upravljanje naredite naslednje:
1. Če gre za prvo uporabo spletnega upravljanja imeniškega strežnika, morate najprej nastaviti spletno upravljanje (glejte "Prva nastavitev spletnega upravljanja" na strani 82) in nato nadaljevati z naslednjim korakom.
2. Prijavite se v spletno upravljanje imeniškega strežnika:

- V Navigatorju iSeries izberite strežnik in kliknite **Omrežje > Strežniki > TCP/IP**, z desno tipko miške kliknite **Imenik**, nato pa **Upravljanje strežnika**.
- Na strani Naloge iSeries (http://*vaš_strežnik*:2001) kliknite **IBM Directory Server**.

3. Za upravljanje imeniškega strežnika naredite naslednje:
   a. V polju **Gostiteljsko ime LDAP** izberite imeniški strežnik, ki ga želite upravljati.
   b. Vnesite prijavni DN skrbnika, ki ga uporabljate za povezovanje z imeniškim strežnikom.
   c. Vnesite geslo skrbnika.
   d. Kliknite **Prijava**. Prikaže se stran za spletno upravljanje strežnika IBM Directory Server. Dodatne informacije o strani za spletno upravljanje strežnika IBM Directory Server boste našli v razdelku “Orodje za spletno upravljanje” na strani 84.
4. Če želite dodati ali spremeniti seznam imeniških strežnikov za upravljanje ali spremeniti atribute ukazne miza za spletno upravljanje, naredite naslednje:
   a. V polju **Gostiteljsko ime LDAP** izberite **Upravljanje ukazne mize**.
   b. Vnesite prijavni ID skrbnika ukazne mize.
   c. Vnesite geslo skrbnika ukazne mize.
   d. Kliknite **Prijava**. Prikaže se stran za spletno upravljanje strežnika IBM Directory Server. Dodatne informacije o strani za spletno upravljanje strežnika IBM Directory Server boste našli v razdelku “Orodje za spletno upravljanje” na strani 84.
   e. Kliknite **Upravljanje ukazne mize** in izberite nekaj od naslednjega:
      - **Spremeni prijavo skrbnika ukazne mize**, da spremenite prijavno ime skrbnika ukazne mize.
      - **Spremeni geslo skrbnika ukazne mize**, da spremenite geslo skrbnika ukazne mize.
      - **Upravljanje strežnikov ukazne mize**, da spremenite, katere strežnike je mogoče upravljati z ukazno mizo za spletno upravljanje.
      - **Upravljanje lastnosti ukazne mize**, da spremenite lastnosti ukazne mize za spletno upravljanje.

Prva nastavitev spletnega upravljanja

Za prvo nastavitev orodja za spletno upravljanje imeniškega strežnika izvedite naslednje postopke.

1. Namestite strežnik IBM WebSphere Application Server - Express (osnova 5722-IWE in možnost 2) in povezano predpogojno programsko opremo (če še ni nameščena). Dodatne informacije boste našli v temi Strežnik IBM HTTP Server.
2. V primerku strežnika HTTP ADMIN omogočite primerek sistemskega strežnika aplikacij.
   a. Zaženite rimerek strežnika HTTP ADMIN, tako da naredite eno od naslednjega.
      - V Navigatorju iSeries kliknite **Omrežje -> Strežniki -> TCP/IP** in z desnim gumbom kliknite **HTTP Administration**. Nato kliknite **Zaženi** .
      - V ukazno vrstico i5/OS vpišite STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).
   b. Prijavite se v funkcijo IBM Web Administration za iSeries. Z uporabniškim profilom i5/OS in geslom se prijavite na stran Naloge iSeries (http:// *vaš_strežnik*:2001) in kliknite **IBM Web Administration for iSeries**.
   c. Na strani Upravljanje strežnika HTTP *vaš_strežnik* kliknite jeziček **Upravljanje** in nato kliknite jeziček **Strežniki HTTP**. Preverite, ali je na spustnem seznamu Strežniki izbran **ADMIN – Apache**. Izmed možnosti v levem oknu na strani izberite **Splošna konfiguracija strežnika**.

      Opomba: Morda boste morali razširiti razdelek **Lastnosti strežnika**, da boste videli možnost **Splošna konfiguracija strežnika**.
   d. Nastavite možnost **Zaženi primerek sistemskega strežnika aplikacij, ko je zagnana strežnik 'Admin'** na **Da**.
   e. Kliknite **Potrdi**.
3. Nastavite WebSphere Application Server, da bo uporabljal SYSINST.
   a. Izmed možnosti v levem podoknu izberite **WebSphere Application Server**.

b. Izberite **WebSphere Application Server – Express 5.0**.
c. S spustnega seznama **Primerki WebSphere** izberite **SYSINST**.

   Opomba: Če možnosti SYSINST ni na spustnem seznamu, znova zaženite strežnik ADMIN.
d. Na spustnem seznamu **Zaženi vse strežnike aplikacij WebSphere...** izberite **Da**.
e. S spustnega seznama **Zaustavi vse strežnike aplikacij WebSphere ...** izberite **Da**.
f. Kliknite **Potrdi**.

4. Znova zaženite primerek strežnika HTTP ADMIN, tako da kliknete gumb za vnovični zagon (drugi gumb po jezičkom **Strežniki HTTP**). Primerek strežnika HTTP ADMIn lahko zaustavite in zaženete tudi z Navigatorjem iSeries ali ukazno vrstico i5/OS.

   Primerek strežnika HTTP ADMIN lahko zaustavite tako, da naredite eno od naslednjega:
   - V Navigatorju iSeries kliknite **Omrežje -> Strežniki -> TCP/IP** in z desno tipko miške kliknite **Upravljanje HTTP**. Nato kliknite **Zaustavi**.
   - V ukazno vrstico vpišite i5/OS ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN) .

   Primerek strežnika HTTP ADMIN lahko zaženete tako, da naredite eno od naslednjega:
   - V Navigatorju iSeries kliknite **Omrežje -> Strežniki -> TCP/IP** in z desno tipko miške kliknite **Upravljanje HTTP**. Nato kliknite **Zaženi** .
   - V ukazno vrstico i5/OS vpišite STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).

   Dodatne informacije boste našli v temi Strežnik IBM HTTP Server.
5. Prijavite se v orodje za spletno upravljanje imeniškega strežnika.
   a. Odprite **prijavno stran**, tako da naredite eno od naslednjega.
      - V Navigatorju iSeries izberite vaš strežnik in kliknite **Omrežje -> Strežniki -> TCP/IP**, z desnim gumbom kliknite **IBM Directory Server** in kliknite **Upravljanje strežnika**.
      - Na strani Naloge iSeries (http:// *vaš_strežnik*:2001) kliknite **IBM Directory Server for iSeries**.
   b. V polju **Gostiteljsko ime LDAP** izberite **Upravljanje ukazne mize**.
   c. V polje **Ime uporabnika** vnesite superadmin.
   d. V polje **Geslo** vnesite secret.
   e. Kliknite **Prijava**. Prikaže se stran za spletno upravljanje strežnika IBM Directory Server.
6. Spremenite prijavno ime za upravljanje ukazne mize.
   a. V levem oknu kliknite **Upravljanje z ukazno mizo**, da razširite razdelek in nato kliknite **Spremeni prijavo skrbnika ukazne mize**.
   b. V polje **Prijava skrbnika ukazne mize** vpišite novo prijavno ime skrbnika ukazne mize.
   c. V polje **Trenutno geslo** vpišite trenutno geslo (secret).
   d. Kliknite **Potrdi**.
7. Spremenite geslo ukazne mize. V levem oknu kliknite **Spremeni geslo skrbnika ukazne mize**.
8. Dodajte imeniški strežnik, ki ga želite upravljati. V levem oknu kliknite **Upravljanje strežnikov ukazne mize**.

   Opomba: Pri dodajanju imeniškega strežnika i5/OS **vrata za upravljanje** niso uporabljena in so zanemarjena.
9. Če želite, spremenite lastnosti ukazne mize. V levem oknu kliknite **Upravljanje lastnosti ukazne mize**.
10. Kliknite **Odjava**. Ko se prikaže zaslon o uspešni odjavi, kliknite povezavo **tukaj**, da se vrnete na prijavno stran spletnega upravljanja.

Po prvem konfiguriranju ukazne mize se lahko kadarkoli vrnete na ukazno mizo in naredite naslednje:
- spremenite prijavno ime in geslo skrbnika ukazne mize
- spremenite, katere imeniške strežnike je mogoče upravljati z orodjem za spletno upravljanje
- spremenite lastnosti ukazne mize.

Orodje za spletno upravljanje

Po prijavi v orodje za spletno upravljanje se odpre aplikacijsko okno, sestavljeno iz petih delov:

Področje traku
Področje traku je na vrhu okna in vsebuje ime aplikacije in IBM-ov logotip.

Področje za usmerjanje
V področju za usmerjanje, ki je na levi strani okna, so prikazane razširljive kategorije za različne vsebinske naloge strežnika, kot so naslednje:

Lastnosti uporabnika
S to nalogo lahko spremenite trenutno geslo uporabnika.

Upravljanje sheme
Ta naloga omogoča delo z objektnimi razredi, atributi, primerjalnimi pravili in skladnjo.

Upravljanje imenika
Ta naloga omogoča delo z imeniškimi vnosi.

Upravljanje podvajanja
Ta naloga omogoča delo s poverilnicami, topologijo, načrti in čakalnimi vrstami.

Področja in predloge
Ta naloga omogoča delo z uporabniškimi predlogami in področji.

Uporabniki in skupine
Ta naloga omogoča delo z uporabniki in skupinami v definiranih področjih. Če želite na primer izdelati novega spletnega uporabnika, omogoča naloga **Uporabniki in skupine** delo z enim objektnim razredom skupine groupOfNames. Podporo za skupine lahko prilagodite.

Delovno področje
V delovnem področju so prikazane naloge, ki so povezane z izbrano nalogo v področju za usmerjanje. Če na primer izberete v področju za usmerjanje nalogo Upravljanje zaščite strežnika, je v delovnem področju prikazana stran Zaščita strežnika in jezički, ki vsebujejo naloge za nastavitev zaščite strežnika.

Statusno področje strežnika
Statusno področje strežnika, prikazano na vrhu delovnega področja. Ikona na levi strani statusnega področja kaže trenutni status strežnika. Poleg ikone je ime strežnika, ki ga upravljate. Ikona na desni strani statusnega področja omogoča povezavo z zaslonsko pomočjo.

Statusno področje naloge
V področju naloge, ki je pod delovnim področjem, je prikazan status trenutne naloge.

Poglavje 6. Scenarij: nastavitev imeniškega strežnika v podjetju MyCo, Inc.

Situacija

Kot skrbnik računalniških sistemov v podjetju želite shraniti informacije o uslužbencih, kot so telefonske številke in naslovi elektronske pošte, v osrednje odlagališče LDAP.

Cilji

V tem scenariju želijo v podjetju MyCo, Inc. konfigurirati imeniški strežnik in izdelati imeniško bazo podatkov, ki bo vsebovala informacije o uslužbencih, kot so ime, naslov elektronske pošte in telefonska številka.

Cilji tega scenarija so naslednji:

- Omogočiti razpoložljivost informacij o uslužbencih kjerkoli v omrežju podjetja za uslužbence, ki uporabljajo Lotus Notes ali poštnega odjemalca Microsoft Outlook Express.
- Upravnikom omogočiti spreminjanje podatkov o uslužbencih v imeniški bazi podatkov, neupravnikom pa to preprečiti.
- Strežniku iSeries omogočiti objavljanje podatkov o uslužbencih v imeniški bazi podatkov.

Podrobnosti

Imeniški strežnik se bo izvajal v strežniku iSeries, imenovanem myiSeries.

Naslednji zgled kaže informacije, ki jih želijo v podjetju MyCo, Inc. vključiti v svojo imeniško bazo podatkov za vsakega uslužbenca.

```
Ime: Jose Alvirez
Oddelek: DEPTA
Telefonska številka: 999 999 9999
Naslov elektronske pošte: jalvirez@my_co.com
```

Imeniška struktura za ta scenarij je lahko podobna naslednji:

```
/
|
+- 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
.
.
.
```

Vsi uslužbenci (upravniki in neupravniki) obstajajo v imeniškem drevesu uslužbencev. Upravniki spadajo tudi v skupino upravnikov. Člani skupine upravnikov imajo pooblastilo za spreminjanje podatkov o uslužbencih.

Strežnik iSeries (myiSeries) potrebuje tudi pooblastilo za spreminjanje podatkov o uslužbencih. V tem scenariju je strežnik iSeries postavljen v imeniško drevo uslužbencev in je član skupine upravnikov.

Če želite ločiti vnose uslužbencev od vnosa strežnika iSeries, lahko izdelate drugo imeniško drevo (na primer računalniki) in dodate strežnik iSeries vanj. Strežnik iSeries mora imeti enako pooblastilo kot upravniki.

Predpogoji in predpostavke

Orodje za spletno upravljanje je pravilno konfigurirano in se izvaja. Za dodatne informacije glejte “Spletno upravljanje” na strani 81.

Nastavitveni koraki

Opravite naslednje naloge.
1. “Podrobnosti scenarija: nastavitev imeniškega strežnika”.
2. “Podrobnosti scenarija: izdelava imeniške baze podatkov” na strani 87
3. “Podrobnosti scenarija: objava podatkov iSeries v imeniški bazi podatkov” na strani 89
4. “Podrobnosti scenarija: vnos informacij v imeniško bazo podatkov” na strani 90
5. “Podrobnosti scenarija: preskus imeniške baze podatkov” na strani 91

Podrobnosti scenarija: nastavitev imeniškega strežnika

1. korak: konfiguriranje imeniškega strežnika

Opomba: Za konfiguriranje strežnika morate imeti posebna pooblastila *ALLOBJ in *IOSYSCFG.

1. V Navigatorju iSeries kliknite **Omrežje —> Strežniki —> TCP/IP**.
2. V oknu **Konfiguracijske naloge strežnika** na spodnji desni strani Navigatorja iSeries kliknite **Konfiguriraj sistem kot imeniški strežnik**.
3. Prikaže se **čarovnik za konfiguriranje imeniškega strežnika**.
4. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - dobrodošli** kliknite **Konfiguriraj lokalni imeniški strežnik LDAP**.
5. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - dobrodošli** kliknite **Naprej**.
6. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - podajanje nastavitev** izberite **Ne**. Na ta način boste konfigurirali strežnik LDAP brez privzetih nastavitev.
7. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - podajanje nastavitev** kliknite **Naprej**.
8. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - podajanje DN-ja skrbnika** odstranite označitev možnosti **Sistemsko izdelan** in vnesite naslednje:

DN skrbnika	cn=administrator
Geslo	secret
Potrditev gesla	secret

   Opomba: Vsa gesla iz tega scenarija so zgolj ilustrativna. Da ne bi ogrozili zaščite svojega sistema ali omrežja, teh gesel nikoli ne uporabite kot del konfiguracije.
9. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - podajanje DN-ja skrbnika** kliknite **Naprej**.
10. V polje **Pripona** v oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - podajanje pripon** vpišite dc=my_co,dc=com.
11. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - podajanje pripon** kliknite **Dodaj**.

12. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - podajanje pripon** kliknite **Naprej**.
13. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - izbira naslovov IP** izberite **Da, uporabi vse naslove IP**.
14. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - izbira naslovov IP** kliknite **Naprej**.
15. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - podajanje nastavitev TCP/IP** izberite **Da**.
16. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - podajanje nastavitev TCP/IP** kliknite **Naprej**.
17. V oknu Čarovnik za konfiguriranje **IBM-ovega imeniškega strežnika - povzetek** kliknite **Dokončaj**.
18. Z desno tipko miške kliknite **IBM-ov imeniški strežnik** in izberite **Start**.

2. korak: konfiguriranje orodja za spletno upravljanje imeniškega strežnika

1. Pregledovalnik nastavite na naslov *myiSeries.my_co.com*:9080/IDSWebApp/IDSjsp/Login.jsp, kjer je *myiSeries.my_co.com* vaš strežnik iSeries.
2. Prikaže se prijavna stran. Kliknite seznam **Gostiteljsko ime LDAP** in izberite **Upravljanje ukazne mize**. Za ime uporabnika vpišite superadmin, za geslo pa secret. Kliknite **Prijava**.
3. Orodje za spletno upravljanje konfigurirajte za povezavo s strežnikom LDAP v strežniku iSeries. V levem oknu za usmerjanje izberite **Upravljanje ukazne mize —> Upravljanje strežnikov ukazne mize**.
4. Kliknite **Dodaj**.
5. V polje **Dodaj strežnik** vpišite myiSeries.my_co.com.
6. Kliknite **Dodaj**. Na seznamu **Upravljanje strežnikov ukazne mize** se prikaže nov strežnik.
7. V levem oknu za upravljanje kliknite **Odjava**.
8. Na prijavni strani orodja za spletno upravljanje kliknite seznam **Gostiteljsko ime LDAP** in izberite pravkar konfigurirani strežnik (**myiSeries.my_co.com**).
9. V polje **Ime uporabnika** vpišite cn=administrator, v polje **Geslo** pa secret. Kliknite **Prijava**. Prikaže se glavna stran orodja za spletno upravljanje IBM-ovega imeniškega strežnika.

Podrobnosti scenarija: izdelava imeniške baze podatkov

Preden lahko začnete z vnašanjem podatkov, morate izdelati prostor, kamor boste podatki shranjevali.

1. korak: izdelava objekta osnovnega DN

1. Kliknite **Upravljanje imenika —> Upravljanje vnosov**. Prikaže se izpis objektov na osnovni ravni imenika. Ker je strežnik nov, se prikažejo samo strukturalni objekti, ki vsebujejo konfiguracijske informacije.
2. Dodati želite nov objekt, ki bo vseboval podatke o MyCo, Inc. Najprej kliknite **Dodaj...** na desni strani okna. V naslednjem oknu se pomaknite po seznamu **Objektni razredi** in izberite **domeno**, nato pa kliknite **Naprej**.
3. Ker ne želite dodati nobenih pomožnih objektnih razredov, kliknite **Naprej**.
4. V oknu **Vnos atributov** vnesite podatke, ki ustrezajo priponi, ki ste jo predhodno izdelali v čarovniku. Spustni seznam **Objektni razred** pustite nastavljen na **domeno**. V polje **Relativni DN** vpišite dc=my_co. V polje **Nadrejeni DN** vpišite dc=com. V polje **dc** vpišite my_co.
5. Na dnu okna kliknite **Dokončaj**. Če se vrnete na osnovno raven, se prikaže nov osnovni DN.

2. korak: izdelava uporabniške predloge

Uporabniško predlogo lahko izdelate kot pomoč pri dodajanju podatkov o uslužbencih podjetja MyCo, Inc.

1. Kliknite **Področja in predloge —> Dodaj uporabniško predlogo**.
2. V polje **Ime uporabniške predloge** vpišite Uslužbenec.
3. Kliknite gumb **Preglej...** poleg polja **Nadrejeni DN**. Kliknite osnovni DN, ki ste ga izdelali v prejšnjem razdelku **dc=my_co,dc=com**, nato pa v desnem oknu kliknite **Izberi**.
4. Kliknite **Naprej.**

5. Na spustnem seznamu **Strukturalni objektni razredi**
6. izberite **inetOrgPerson** in kliknite **Naprej**.
7. Na spustnem seznamu **Atribut poimenovanja** izberite **cn**.
8. Na seznamu **Jezički** izberite **Obvezni** in kliknite **Urejanje**.
9. V oknu **Urejanje jezičkov** lahko izberete polja, ki jih želite vključiti v uporabniško predlogo. **sn** in **cn** sta obvezna.
10. Na seznamu **Atributi** izberite **departmentNumber** in kliknite **Dodaj >>>**.
11. Izberite **telephoneNumber** in kliknite **Dodaj >>>**.
12. Izberite **mail** in kliknite **Dodaj >>>**.
13. Izberite **userPassword** in kliknite **Dodaj >>>**.
14. Kliknite **Potrdi**, nato pa **Dokončaj**, da izdelate uporabniško predlogo.

3. korak: izdelava področja

1. V orodju za spletno upravljanje kliknite **Področja in predloge—> Dodaj predlogo**.
2. V polje **Ime predloge** vpišite employees.
3. Kliknite **Preglej...** na desni strani polja **Nadrejeni DN**.
4. Izberite izdelani nadrejeni DN **dc=my_co,dc=com** in kliknite **Izberi** na desni strani okna.
5. Kliknite **Naprej**.
6. V naslednjem oknu morate spremeniti samo spustni seznam **Uporabniška predloga**. Izberite izdelano uporabniško predlogo **cn=employees,dc=my_co,dc=com**.
7. Kliknite **Dokončaj**.

4. korak: izdelava skupine upraviteljev

1. Izdelajte skupino upraviteljev.
   a. Kliknite **Uporabniki in skupine —> Dodaj skupino**.
   b. V polje **Ime skupine** vpišite managers.
   c. Na spustnem seznamu **Področje** mora biti izbrana možnost **employees**.
   d. Kliknite **Dokončaj**.
2. Konfigurirajte skrbnika skupine upraviteljev za področje **employees**.
   a. Kliknite **Področja in predloge —> Upravljanje predlog**.
   b. Izberite izdelano področje **cn=employees,dc=my_co,dc=com** in kliknite **Urejanje**.
   c. Na desni strani polja **Skupina skrbnikov** kliknite **Preglej...**.
   d. Izberite **dc=my_co,dc=com** in kliknite **Razširi**.
   e. Izberite **cn=employees** in kliknite **Razširi**.
   f. Izberite **cn=managers** in kliknite **Izberi**.
   g. V oknu **Urejanje področja** kliknite **Potrdi**.
3. Skupini upraviteljev dodelite pooblastilo za pripono **dc=my_co,dc=com**.
   a. Kliknite **Upravljanje imenika —> Upravljanje vnosov**.
   b. Izberite **dc=my_co,dc=com** in kliknite **Uredi ACL...**.
   c. V oknu **Urejanje ACL** kliknite jeziček **Lastniki**.
   d. Izberite potrditveno polje **Razširi lastnika**. Vsi, ki so člani skupine upraviteljev, bodo postali lastniki podatkovnega drevesa **dc=my_co,dc=com**.
   e. Na spustnem seznamu **Tip** izberite **Skupina**.
   f. V polje **DN (razločevalno ime)** vpišite cn=managers,cn=employees,dc=my_co,dc=com.
   g. Kliknite **Dodaj**.
   h. Kliknite **Potrdi**.

5. korak: dodajanje uporabnika kot upravitelja

1. V orodju za spletno upravljanje kliknite **Uporabniki in skupine—> Dodaj uporabnika**.
2. Na spustnem seznamu **Področje** izberite izdelano področje **employees** in kliknite **Naprej**.
3. V polje **cn** vpišite Jose Alvirez.
4. V polje ***sn** (priimek) vpišite Alvirez.
5. V polje ***cn** (celotno ime) vpišite Jose Alvirez. cn se uporablja za izdelavo DN-ja vnosa. *cn je atribut objekta.
6. V polje **telephoneNumber** vpišite 999 555 1234.
7. V polje **departmentNumber** vpišite DEPTA.
8. V polje **mail** vpišite jalvirez@my_co.com.
9. V polje **userPassword** vpišite secret.
10. Kliknite jeziček **Skupine uporabnikov**.
11. Na seznamu **Razpoložljive skupine** izberite **managers** in kliknite **Dodaj —>**.
12. Na dnu okna kliknite **Dokončaj**.
13. S klikom gumba **Odjava** na levi strani usmerjevalnega okna se odjavite iz orodja za spletno upravljanje.

Podrobnosti scenarija: objava podatkov iSeries v imeniški bazi podatkov

Konfigurirajte objavljanje, da strežniku iSeries omogočite samodejno vnašanje uporabniških informacij v imenik LDAP. V imeniku LDAP so objavljene uporabniške informacije iz sistemskega razdeljevalnega imenika.

Opomba: Uporabniki, ki ste jih izdelali z Navigatorjem iSeries, imajo uporabniški vnos za profil uporabnika in sistemski razdeljevalni imenik. Če uporabite za izdelavo uporabnikov ukaze CL, morate izdelati uporabniški vnos za profil uporabnika (**CRTUSRPRF**) in sistemski razdeljevalni imenik (**WRKDIRE**). Če obstajajo uporabniki samo kot profili uporabnikov in jih želite objaviti v imeniku LDAP, morate zanje izdelati uporabniške vnose sistemskega razdeljevalnega imenika.

1. korak: izdelava strežnika iSeries kot uporabnika imeniškega strežnika

1. V orodje za spletno upravljanje (**myiSeries.my_co.com**:9080/IDSWebApp/IDSjsp/Login.jsp) se prijavite kot skrbnik.
   a. Na seznamu **Gostiteljsko ime LDAP** izberite **myiSeries.my_co.com**.
   b. V polje **Ime uporabnika** vpišite cn=administrator.
   c. V polje **Geslo** vpišite secret.
   d. Kliknite **Prijava**.
2. Izberite **Uporabniki in skupine —> Dodaj uporabnika**.
3. Na seznamu **Področje** izberite **employees**.
4. Kliknite **Naprej**.
5. V polje **cn** vpišite myiSeries.my_co.com.
6. V polje ***sn** vpišite myiSeries.my_co.com.
7. V polje ***cn** vpišite myiSeries.my_co.com.
8. V polje **userPassword** vpišite secret.
9. Kliknite jeziček **Skupine uporabnikov**.
10. Izberite skupino **managers**.
11. Kliknite **Dodaj —>**.
12. Kliknite **Dokončaj**.

2. korak: konfiguriranje strežnika iSeries za objavljanje podatkov

1. V Navigatorju iSeries z desno tipko miške kliknite strežnik iSeries v levem oknu za usmerjanje in izberite **Lastnosti**.
2. V pogovornem oknu **Lastnosti** izberite jeziček **Imeniški strežnik**.
3. Izberite **Uporabniki** in kliknite **Podrobnosti**.
4. Izberite potrditveno polje **Objavi informacije o uporabniku**.
5. V razdelku **Kje objaviti** kliknite gumb **Urejanje**. Prikaže se okno.
6. Vpišite myiSeries.my_co.com.
7. V polje **Pod DN** vpišite cn=employees,dc=my_co,dc=com.
8. V razdelku **Povezava strežnika** zagotovite, da je v polje **Vrata** vnesena privzeta številka vrat **389**. Na spustnem seznamu **Način overjanja** izberite **razločevalno ime** in v polje **Razločevalno ime** vnesite cn=myiSeries,cn=employees,dc=my_co,dc=com.
9. Kliknite **Geslo**.
10. V polje **Geslo** vpišite secret.
11. V polje **Potrditev gesla** vpišite secret.
12. Kliknite **Potrdi**.
13. Kliknite gumb **Preveri**. S tem zagotovite, da so vse informacije pravilno vnesene in da se strežnik iSeries lahko poveže z imenikom LDAP.
14. Kliknite **Potrdi**.
15. Kliknite **Potrdi**.

Podrobnosti scenarija: vnos informacij v imeniško bazo podatkov

Jose Alvirez kot upravitelj zdaj doda in ažurira podatke za posameznike v svojem oddelku. Dodati mora še nekaj dodatnih informacij o Jane Doe. Jane Doe je uporabnica v strežniku iSeries in njene informacije so bile že objavljene. Jose Alvirez mora dodati tudi informacije o Johnu Smithu, ki ni uporabnik v strežniku iSeries. Jose Alvirez naredi naslednje:

1. korak: prijava v orodje za spletno upravljanje

Prijavite se v orodje za spletno upravljanje (http://**myiSeries.my_co.com**:9080/IDSWebApp/IDSjsp/Login.), tako da naredite naslednje:

1. Na seznamu **Gostiteljsko ime LDAP** izberite **myiSeries.my_co.com**.
2. V polje Ime uporabnika vpišite cn=Jose Alvirez,cn=myco employees,dc=my_co,dc=com.
3. V polje Geslo vpišite secret.
4. Kliknite **Prijava**.

2. korak: spreminjanje podatkov o uslužbencih

1. Kliknite **Uporabniki in skupine —> Upravljanje uporabnikov**.
2. Na seznamu **Področje** izberite **employees** in kliknite **Prikaži uporabnike**.
3. Na seznamu uporabnikov izberite **Jane Doe** in kliknite **Urejanje**.
4. V polje **departmentNumber** vpišite DEPTA,
5. Kliknite **Potrdi**.
6. Kliknite **Zapri**.

3. korak: dodajanje podatkov o uslužbencu

1. Kliknite **Uporabniki in skupine —> Dodaj uporabnika**.
2. Na spustnem seznamu **Področje** izberite **employees** in kliknite **Naprej**.
3. V polje **cn** vpišite John Smith.
4. V polje ***sn** vpišite Smith.

5. V polje ***cn** vpišite John Smith.
6. V polje **telephoneNumber** vpišite 999 555 1235.
7. V polje **departmentNumber** vpišite DEPTA.
8. V polje **mail** vpišite jsmith@my_co.com.
9. Na dnu okna kliknite **Dokončaj**.

Podrobnosti scenarija: preskus imeniške baze podatkov

Ko vnesete podatke o uslužbencih v imeniško bazo podatkov, z naslednjimi postopki preskusite imeniško bazo podatkov in imeniški strežnik:

Preiščite imeniško bazo podatkov z osebnim imenikom za elektronsko pošto

Informacije v imeniku LDAP lahko preprosto preiščete s programi, ki so omogočeni za LDAP. Številni odjemalci elektronske pošte lahko preiščejo imeniške strežnike LDAP kot del svoje funkcije osebnega imenika. Sledita vzorčna postopka za konfiguriranje Lotus Notes 6 in Microsoft Outlook Express 6. Postopki za večino drugih odjemalcev elektronske pošte bodo podobni.

Lotus Notes

1. Odprite osebni imenik.
2. Kliknite **Actions —> New —> Account**.
3. V polje **Account name** vpišite myiSeries.
4. V polje **Account server name** vpišite myiSeries.my_co.com,
5. V polje **Protocol** vpišite **LDAP**.
6. Kliknite jeziček **Protocol Configuration**.
7. V polje **Search base** vpišite dc=my_co,dc=com.
8. Kliknite **Save and close**.
9. Kliknite **Create —> Mail —> Memo**.
10. Kliknite **Address...**.
11. V polju **Choose address book** izberite myiSeries.
12. V polje **Search for** vpišite Alvirez.
13. Kliknite **Search**. Prikažejo se podatki za Josea Alvireza.

Microsoft Outlook Express

1. Kliknite **Tools —> Accounts**.
2. Kliknite **Add —> Directory Service**.
3. V polje **Internet Directory (LDAP) server** (myiSeries.my_co.com) vpišite spletni naslov iSeries.
4. Odstranite kljukico iz potrditvenega polja **My LDAP server requires me to log on**.
5. Kliknite **Naprej**.
6. Kliknite **Naprej**.
7. Kliknite **Dokončaj**.
8. Izberite myiSeries.my_co.com (pravkar konfigurirana imeniška storitev) in kliknite **Properties**.
9. Kliknite **Advanced**.
10. V polje **Search base** vpišite dc=my_co,dc=com.
11. Kliknite **Dodaj**.
12. Kliknite **Zapri**.
13. Vpišite Ctrl+E, da odprete okno **Find People**.
14. Na seznamu **Look in** izberite myiSeries.my_co.com.

15. V polje **Name** vpišite Alvirez.
16. Kliknite **Find now**. Prikažejo se podatki za Josea Alvireza.

Pregled imeniške baze podatkov z ukazom ukazne vrstice ldapsearch

1. V vmesnik, temelječ na znakih, vnesite ukaz CL **QSH**, da odprete sejo Qshell.
2. Z naslednjim ukazom prikažete seznam vseh vnosov LDAP v bazi podatkov.

   ```
   ldapsearch –h myiSeries.my_co.com –b dc=my_co,dc=com objectclass=*
   ```

   Pri tem velja naslednje:

   –h je ime gostiteljskega računalnika, na katerem se izvaja strežnik LDAP,

   –b je osnovni DN, pod katerim se izvaja iskanje,

   objectclass=*
   vrne vse vnose v imeniku.

   Ta ukaz vrne izpis, podoben naslednjemu:

   ```
   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 vrstica vsakega vnosa se imenuje razločevalno ime (DN). DN-ji so podobni celotnemu datotečnemu imenu vsakega vnosa. Nekateri vnosi ne vsebujejo podatkov in so samo strukturalni. Tisti z vrstico **objectclass=inetOrgPerson**, ustrezajo vnosom, ki ste jih izdelali za osebe. DN za Joseja Alvireza je **cn=Jose Alvirez,cn=MyCo Employees,dc=my_co,dc=com**.

Poglavje 7. Upravljanje imeniškega strežnika

Za upravljanje imeniškega strežnika potrebujete naslednje skupine pooblastil:

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

Če želite upravljati objekte imenika (vključno s seznami za nadzor dostopa, lastništvom objektov in kopijami), se povežite v imenik kot skrbnik DN ali kot drugi DN, ki ima ustrezna pooblastila LDAP. Če uporabljate integracijo pooblastil, je lahko skrbnik tudi projicirani uporabnik (glejte “Ozadje, določeno z operacijskim sistemom” na strani 64), ki ima pooblastilo za ID funkcije skrbnika imeniškega strežnika (glejte “Delo z upravnim dostopom za pooblaščene uporabnike” na strani 99).

Splošne upravne naloge

Vsebinske naloge imenika

- “Upravljanje seznamov za nadzor dostopa (ACL-jev)” na strani 145

Naloge objavljanja
- “Objavljanje informacij v imeniškem strežniku” na strani 149

Zagon imeniškega strežnika

Imeniški strežnik zaženete z naslednjim postopkom:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom miške kliknite **Imenik** in izberite **Zaženi**.

   Zagon imeniškega strežnika lahko traja nekaj časa in je odvisen od hitrosti strežnika in količine razpoložljivega pomnilnika. Prvi zagon imeniškega strežnika bo morda trajal nekoliko dlje, ker mora strežnik izdelati nove datoteke. Podobno velja tudi za prvi zagon imeniškega strežnika po nadgraditvi iz starejše različice, ker mora strežnik preseliti datoteke. Status strežnika lahko občasno preverite (glejte “Preverjanje statusa imeniškega strežnika” na strani 95), da vidite, ali se je že zagnal.

Imeniški strežnik lahko zaženete tudi iz vmesnika, temelječega na znakih, tako da vnesete ukaz STRTCPSVR *DIRSRV. Če ste imeniški strežnik konfigurirali tako, da se zažene ob zagonu TCP/IP, ga lahko zaženete tudi z vnosom ukaza STRTCP.

Način samo za konfiguriranje

Imeniški strežnik lahko zaženete v načinu samo za konfiguriranje iz vmesnika, temelječega na znakih, tako da vnesete ukaz TRCTCPAPP APP(*DIRSRV) ARGLIST(SAFEMODE).

Način samo za konfiguriranje zažene strežnik tako, da je aktivna samo pripona cn=configuration, in ni odvisen od uspešne inicializacije ozadja baze podatkov.

Zaustavitev imeniškega strežnika

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

Imeniški strežnik zaustavite z naslednjim postopkom:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom miške kliknite **Imenik** in izberite **Zaustavi**.

   Zaustavitev imeniškega strežnika lahko traja nekaj časa in je odvisna od hitrosti sistema, količine aktivnosti strežnika in količine razpoložljivega pomnilnika. Status strežnika lahko občasno preverite (glejte “Preverjanje statusa imeniškega strežnika” na strani 95), da vidite, ali se je že zagnal.

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

Preverjanje statusa imeniškega strežnika

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

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

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

Preverjanje opravil v imeniškem strežniku

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

Omogočanje obveščanja o dogodkih

Imeniški strežnik podpira obveščanje o dogodkih, ki omogoča, da so odjemalci, ki so registrirani s strežnikom LDAP, obveščeni o določenem dogodku, kot je na primer dodajanje v imenik.

Če želite v strežniku omogočiti obveščanje o dogodkih, storite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite **Dogodki**.
6. Izberite **Odjemalcem omogoči prijavo za obveščanje o dogodkih**.

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

Dodatne informacije o obveščanju o dogodkih boste našli v razdelku Event notification priročnika IBM Directory Server Version 5.1 Programming Reference.

Določitev nastavitev za transakcije

imeniški strežnik podpirajo transakcije, ki omogočajo, da je skupina operacij imenika LDAP obravnavana kot ena enota. Če želite več informacij, poglejte “Transakcije” na strani 39.

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

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

Spreminjanje vrat ali naslova IP

Imeniški strežnik uporablja naslednja privzeta vrata:
- 389 za nezaščitene povezave
- 636 za zaščitene povezave (če ste z Upravljalnikom digitalnih potrdil omogočili imeniški strežnik kot aplikacijo, ki lahko uporablja zaščitena vrata).

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

Če ta vrata že uporabljate za drugo aplikacijo, lahko dodelite imeniškemu strežniku druga vrata ali pa uporabite za dva strežnika različna naslova IP, če aplikaciji podpirata povezovanje z določenim naslovom IP.

Zgled strežnika Domino LDAP, ki je v navzkrižju z imeniškim strežnikom, boste našli v temi Gostovanje Domino LDAP in imeniškega strežnika v istem iSeries.

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

Če želite spremeniti naslov IP, na katerem imeniški strežnik sprejema povezave, naredite naslednje:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Omrežje**.
6. Kliknite gumb **Naslovi IP...**.
7. Izberite **Uporabi izbrane naslove IP** in izberite naslove IP za strežnik, ki ga želite uporabiti pri sprejemanju povezav.

Nastavitev načela za gesla

Načelo za gesla nastavite takole:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Geslo**.
6. Vnesite informacije o načelih za gesla. Če želite, lahko kliknete **Preverjanje in zaklepanje gesla**, da podate dodatne informacij o načelu za gesla, nato pa kliknite **Potrdi**.
7. Kliknite **Potrdi**.

Opomba: Za nastavitev načela za gesla lahko uporabite tudi pomožni program ldapmodify (glejte “ldapmodify in ldapadd” na strani 157).

Dodatne informacije o načelu za gesla boste našli v razdelku “Načelo gesel” na strani 58.

Uvažanje datoteke LDIF

Informacije med imeniškimi strežniki lahko prenesete z datotekami LDIF (format za izmenjavo podatkov LDAP). Za dodatne informacije glejte “Format za izmenjavo podatkov LDAP (LDIF)” na strani 182. Preden začnete s tem postopkom, prenesite datoteko LDIF v vaš strežnik iSeries kot tokovno datoteko.

Datoteko LDIF uvozite v imeniški strežnik z naslednjim postopkom:
1. Če je imeniški strežnik zagnan, ga zaustavite. Informacije o zaustavitvi imeniškega strežnika boste našli v razdelku “Zaustavitev imeniškega strežnika” na strani 94.
2. V Navigatorju iSeries razširite **Omrežje**.
3. Razširite **Strežniki**.
4. Kliknite **TCP/IP**.
5. Z desnim gumbom miške kliknite **Imenik** in izberite **Orodja** in nato **Uvozi datoteko**.

   Če izberete možnost **Podvoji uvožene podatke**, lahko strežnik podvoji na novo uvožene podatke pri naslednjem zagonu. To je uporabno, če dodajate nove vnose v obstoječe imeniško drevo v glavnem strežniku. Če uvažate podatke za inicializiranje strežnika za podvajanje (ali enakovrednega strežnika), podatkov običajno ne boste želeli podvojiti, saj lahko že obstajajo v strežnikih, za katere je ta strežnik oskrbnik.

Opomba: Za uvažanje datotek LDIF lahko uporabite tudi pomožni program ldapadd (glejte “ldapmodify in ldapadd” na strani 157).

Izvažanje datoteke LDIF

Informacije med imeniškimi strežniki lahko prenesete z datotekami LDIF (format za izmenjavo podatkov LDAP) (glejte “Format za izmenjavo podatkov LDAP (LDIF)” na strani 182). V datoteko LDIF lahko izvozite celoten ali samo del imenika LDAP.

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

   Opomba: Če ne podate celotne poti do datoteke LDIF, v katero želite izvoziti podatke, bo datoteka izdelana v domačem imeniku, ki je podan v profilu uporabnika i5/OS.

Opombe:
1. Za datoteko LDIF nastavite pooblastila in s tem preprečite nepooblaščen dostop do podatkov imenika. V ta namen z desnim gumbom miške kliknite datoteko v Navigatorju iSeries in nato izberite **Pooblastila**.
2. S pomočjo pomožnega programa LDIF lahko izdelate popolno ali delno datoteko LDIF. Preglejte “ldapsearch” na strani 169. Uporabite možnost -L in preusmerite izhodne podatke v datoteko.

Podajanje strežnika za referenčne kazalce imenika

Za dodelitev referenčnih strežnikov za imeniški strežnik opravite naslednji postopek:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom miške kliknite **Imenik** in nato izberite **Lastnosti**.
5. Izberite stran lastnosti **Splošno**.
6. V polju **Novi referenčni kazalec** podajte URL referenčnega strežnika.
7. V pozivu podajte ime strežnika referenčnih kazalcev v obliki URL. Sprejemljivi URL-ji LDAP:
   - ldap://test.server.com
   - ldap://test.server.com:400
   - ldap://9.9.99.255

Opomba: Če referenčni strežnik ne uporablja privzetih vrat, podajte pravilno številko vrat kot del URL-ja, tako kot so vrata 400 podana v drugem zgledu zgoraj.

8. Kliknite **Dodaj**.
9. Kliknite **Potrdi**.

Dodajanje in odstranjevanje pripon imeniškega strežnika

Z dodajanjem pripone v imeniški strežnik strežniku omogočite upravljanje tega dela imeniškega drevesa.

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

Če želite dodati pripono v imeniški strežnik, storite naslednje:

1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Baza podatkov/Pripone**.
6. V polje **Nova pripona** vpišite ime nove pripone.
7. Kliknite **Dodaj**.
8. Kliknite **Potrdi**.

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

Pripono odstranite iz imeniškega strežnika z naslednjim postopkom:

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

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

Shranjevanje in obnavljanje informacij imeniškega strežnika

imeniški strežnik shrani informacije na naslednja nahajališča:

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

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

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

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

Dodatne informacije o shranjevanju in obnavljanju podatkov OS/400 boste našli v priročniku Backup and Recovery, SC41-5304 .

Delo z upravnim dostopom za pooblaščene uporabnike

Uporabniškim profilom, ki imajo dostop do identifikatorja (ID-ja) funkcije skrbnika imeniškega strežnika (QIBM_DIRSRV_ADMIN) lahko podelite skrbniški dostop.

Če je na primer uporabniškemu profilu JOHNSMITH podeljen dostop do ID-ja funkcije skrbnika imeniškega strežnika in izberete v pogovornem oknu Lastnosti imenika možnost Podeli skrbniški dostop pooblaščenim uporabnikom, ima profil JOHNSMITH pooblastilo skrbnika LDAP. Če se ta profil uporablja za povezovanje imeniškega strežnika z uporabo naslednjega DN, os400-profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com, ima uporabnik pooblastilo skrbnika. Pripona objektov sistema je v tem primeru os400-sys=systemA.acme.com. Dodatne informacije o projiciranih uporabnikih boste našli v razdelku “Ozadje, določeno z operacijskim sistemom” na strani 64.

Če želite izbrati to možnost, naredite naslednje:

1. V Navigator iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
4. Na jezičku **Splošno** pod **Informacije o skrbniku** izberite možnost **Dodeli skrbniški dostop pooblaščenim uporabnikom**.

ID funkcije za pooblastilo skrbnika imeniškega strežnika v uporabniškem profilu nastavite z naslednjim postopkom:

1. V Navigatorju iSeries z desno tipko kliknite ime sistema in izberite **Upravljanje aplikacije**.
2. Kliknite jeziček **Gostiteljske aplikacije**.
3. Razširite možnost **Operating System/400**.
4. Kliknite **Skrbnik imeniškega strežnika**, da označite možnost.
5. Kliknite gumb **Prilagodi**.
6. Razširite **Uporabniki**, **Skupine** ali **Uporabniki niso v skupini**, kar je ustrezno za želenega uporabnika.
7. Izberite uporabnika ali skupino, ki ju želite dodati na seznam **Dostop dovoljen**.
8. Kliknite gumb **Dodaj**.
9. Kliknite **Potrdi,** da shranite spremembe.
10. Kliknite **Potrdi** v pogovornem oknu **Upravljanje aplikacije**.

Sledenje dostopu in spremembam v imeniku LDAP

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

Če želite omogočiti dnevnik sprememb, naredite naslednje:

1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Dnevnik sprememb**.
6. Izberite **Beleži spremembe imenika**.
7. (neobvezno) V polju **Največje število vnosov** podajte največje število vnosov, ki jih bo hranil dnevnik sprememb. V polju **Največja starost** podajte, kako dolgo želite hraniti vnose dnevnika sprememb.

   Opomba: Čeprav sta ta parametra neobvezna, priporočamo, da podate največje število vnosov ali največjo starost. Če ne podate nobenega, bo dnevnik sprememb hranil vse vnose, zato se lahko zelo poveča.

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

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

Primer:

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

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

Omogočanje beleženja objektov za imeniški strežnik

Imeniški strežnik podpira beleženje zaščite OS/400. Če za sistemsko vrednost QAUDCTL podate *OBJAUD, lahko beleženje objektov omogočite prek Navigatorja iSeries.

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

Spremembe nastavitev beleženje bodo uveljavljene takoj, ko kliknete **Potrdi**. Imeniškega strežnika ni potrebno znova zagnati. Če želite več informacij, poglejte “Zaščita imeniškega strežnika” na strani 40.

Prilagoditev iskalnih nastavitev

Iskalne parametre lahko nastavite tako, da nadzorujejo uporabnikove iskalne zmožnosti, kot sta na primer iskanje po straneh ali razvrščeno iskanje.

Rezultati na več straneh omogočajo lažje delo z večjo količino podatkov, ki jih vrne iskalna zahteva. Namesto da prejmete vse rezultate naenkrat, lahko zahtevate podniz postavk (stran). Nadaljnje iskalne zahteve prikazujejo naslednjo stran rezultatov, dokler ni operacija preklicana ali dokler ni vrnjen zadnji rezultat.

Razvrščeno iskanje odjemalcu omogoča, da prejme rezultate iskanja, ki so razvrščeni s seznamom kriterijev, kjer vsak kriterij predstavlja ključ razvrščanja. Naloga razvrščanja se tako prenese iz odjemalske aplikacije v strežnik.

Iskalne vrednosti imeniškega strežnika prilagodite z naslednjim postopkom:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Iskanje**.

Prilagoditev nastavitev zmogljivosti

Nastavitve zmogljivosti imeniškega strežnika lahko prilagodite tako, da spremenite karkoli od naslednjega:
- velikost predpomnilnika ACL, velikost predpomnilnika vnosa, največje število iskanj, ki bodo shranjena v predpomnilniku filtra in največje iskanje, ki bo shranjeno v predpomnilniku filtra
- nastavitve transakcij strežnika

- število povezav baze podatkov in niti strežnika.

Vrednosti predpomnilnika imeniškega strežnika prilagodite z naslednjim postopkom:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Zmogljivost**.

Vrednosti transakcij imeniškega strežnika prilagodite z naslednjim postopkom:
1. V Navigatorju iSeries razširite **Omrežje**.
2. Razširite **Strežniki**.
3. Kliknite **TCP/IP**.
4. Z desnim gumbom kliknite **Imenik** in izberite **Lastnosti**.
5. Kliknite jeziček **Transakcije**.

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

Upravljanje podvajanja

Za upravljanje podvajanje razširite kategorijo orodja za spletno upravljanje, imenovano **Upravljanje podvajanja**. Dodatne informacije o konceptih podvajanja boste našli v razdelku “Podvajanje” na strani 34.

Dodatne informacije boste našli v naslednjih temah:
- “Izdelava topologije glavnega strežnika-strežnika za podvajanje”
- “Izdelava topologije glavni strežnik-strežnik za odpošiljanje-strežnik za podvajanje” na strani 106
- “Pregled izdelave kompleksne topologije podvajanja” na strani 108
- “Izdelava kompleksne topologije s podvajanjem enakovrednih strežnikov” na strani 108
- “Upravljanje topologij” na strani 111
- “Spreminjanje lastnosti podvajanja” na strani 114
- “Izdelava urnikov podvajanja” na strani 115
- “Upravljanje čakalnih vrst” na strani 116

Izdelava topologije glavnega strežnika-strežnika za podvajanje

Če želite definirati osnovno topologijo glavnega strežnika-strežnika za podvajanje, morate narediti naslednje:
1. Izdelati glavni strežnik in definirati, kaj vsebuje. Izberite poddrevo, ki ga želite podvojiti in podajte strežnik kot glavni. Glejte “Izdelava glavnega strežnika (podvojenega poddrevesa)” na strani 102.
2. Izdelajte poverilnice, ki jih bo uporabljal oskrbnik. Glejte “Izdelava poverilnic” na strani 102.
3. Izdelajte strežnik za podvajanje. Glejte “Izdelava strežnika za podvajanje” na strani 104.
4. Izvozite topologijo iz glavnega strežnika v strežnik za podvajanje. Glejte “Kopiranje podatkov v strežnik za podvajanje” na strani 105.
5. Spremenite konfiguracijo strežnika za podvajanje, tako da bo določala, kdo je pooblaščen za podvajanje sprememb, in glavnemu strežniku dodajte referenčni kazalec. Glejte “Dodajanje informacij o oskrbniku v strežnik za podvajanje” na strani 106.

Opomba:

Če vnos v korenu poddrevesa, ki ga želite podvojiti, ni pripona v strežniku, morate pred uporabo funkcije **Dodaj poddrevo** zagotoviti, da je njegov ACL definiran takole:

Za nefiltrirane ACL-je:

```
ownersource: <enako kot DN vnosa>
ownerpropagate: TRUE

aclsource: <enako kot DN vnosa>
aclpropagate: TRUE
```

Za filtrirane ACL-je:

```
ibm-filteraclinherit: FALSE
```

Če vnos ni pripona v strežniku, morate za zadovoljitev zahtev ACL urediti ACL za ta vnos v oknu **Upravljanje vnosov**. Izberite vnos in kliknite **Uredi ACL**. Če želite dodati nefiltrirane ACL-je, izberite ta jeziček in potrditveno polje, ki podaja, ali so ACL-ji eksplicitni ali ne za ACL-je in lastnike. Možnosti **Razširi ACL-je** in **Razširi lastnika** morata biti označeni. Če želite dodati filtrirane ACL-je, izberite ta jeziček in dodajte vnos **cn=this** z vlogo **access-id** tako za ACL-je, kot tudi za lastnike. Možnost **Nakopiči filtrirane ACL-je** ne sme biti označena, možnost **Razširi lastnika** pa mora biti označena. Podrobnejše informacije boste našli v razdelku “Upravljanje seznamov za nadzor dostopa (ACL-jev)” na strani 145.

V začetku prevzame objekt **ibm-replicagroup**, izdelan s tem postopkom, ACL korenskega vnosa za podvojeno poddrevo. Ti ACL-ji morda ne bodo primerni za krmiljenje dostopa do informacij o podvajanju v imeniku.

Izdelava glavnega strežnika (podvojenega poddrevesa)

Opomba: Za izvedbo te naloge se mora strežnik izvajati.

Ta naloga označi vnos kot koren neodvisno podvojenega poddrevesa in izdela **ibm-replicasubentry**, ki predstavlja ta strežnik kot glavni strežnik za poddrevo. Za izdelavo podvojenega poddrevesa morate določiti poddrevo, ki ga naj strežnik podvoji.

V področju za usmerjanje razširite kategorijo Upravljanje podvajanja in kliknite **Upravljanje topologije**.

1. Kliknite **Dodaj poddrevo**.
2. Vnesite DN korenskega vnosa poddrevesa, ki ga želite podvojiti, ali pa kliknite **Preglej**, da razširite vnose in izberete vnos, ki bo koren poddrevesa.
3. URL referenčnega kazalca glavnega strežnika je prikazan v obliki LDAP URL, kot je naslednja:
   `ldap://<ime-mojega-strežnika>.<moje-mesto>.<moje-podjetje>.com`

   Opomba: URL referenčnega kazalca glavnega strežnika ni obvezen in se uporablja samo v naslednjih primerih:
   - če strežnik vsebuje (ali bo vseboval) poddrevesa, ki so samo za branje
   - za definiranje URL-ja referenčnega kazalca, ki je vrnjen za popravke v drevesu samo za branje v strežniku.
4. Kliknite **Potrdi**.
5. Nov strežnik je prikazan v oknu Upravljanje topologije pod naslovom **Podvojena poddrevesa**.

Izdelava poverilnic

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo Upravljanje podvajanja in kliknite **Upravljanje poverilnic**.

1. S seznama poddreves izberite mesto, ki ga želite uporabiti za shranjevanje poverilnic. Orodje za spletno upravljanje omogoča, da definirate poverilnice na naslednjih mestih:
   - **cn=replication,cn=localhost**, ki hrani poverilnice samo v trenutnem strežniku.

Opomba: V večini primerov je hranjenje poverilnic v cn=replication,cn=localhost zaželeno, saj nudi večjo zaščito od podvojenih poverilnic v poddrevesu. Toda obstajajo tudi primeri, ko poverilnice, shranjene v cn=replication,cn=localhost, niso na voljo.

Če poskušate dodati dvojnik pod strežnik, kot je na primer strežnikA in ste z orodjem za spletno upravljanje povezani z drugim strežnikom - strežnikB - v polju **Izbira poverilnic** ni prikazana možnost **cn=replication,cn=localhost**. Razlog za to je, da informacij pod **cn=localhost** strežnikaA ne morete brati ali ažurirati, če ste povezani s strežnikomB.

Možnost cn=replication,cn=localhost je na voljo samo, če je strežnik, pod katerega poskušate dodati dvojnik, tisti strežnik, s katerim ste povezani prek orodja za spletno upravljanje.

- V podvojenem poddrevesu, ko so poverilnice podvojene z preostalim delom poddrevesa. Poverilnice, shranjene v podvojenem poddrevesu, so izdelane pod vnosom **ibm-replicagroup=default** za to poddrevo.

Opomba: Če ni prikazano nobeno poddrevo, pojdite v "Izdelava glavnega strežnika (podvojenega poddrevesa)" na strani 102, kjer boste našli navodila za izdelavo poddrevesa, ki ga želite podvojiti.

2. Kliknite **Dodaj**.
3. Vnesite ime za poverilnice, ki jih izdelujete, kot je na primer **mojepov**; cn= je že vnesen v polje.
4. Izberite način overjanja, ki ga želite uporabiti, in kliknite **Naprej**.
   - Če izberite preprosto overjanje pri povezovanju, naredite naslednje:
     a. Vnesite DN, ki ga uporablja strežnik za povezovanje s strežnikom za podvajanje, kot je na primer cn=any.
     b. Vnesite geslo, ki ga uporablja strežnik pri povezovanju s strežnikom za podvajanje, kot je na primer secret.
     c. Z vnovičnim vnosom gesla potrdite, da ni tipografskih napak.
     d. Če želite, vnesite kratek opis poverilnic.
     e. Kliknite **Dokončaj**.

     Opomba: Povezovalni DN poverilnic in geslo si lahko tudi zapišete, da ju ne boste pozabili. Geslo boste namreč potrebovali pri izdelavi dogovora o podvajanju.
   - Če izberete overjanje Kerberos, naredite naslednje:
     a. Vnesite povezovalni DN Kerberos.
     b. Vnesite povezovalno geslo.
     c. Znova vnesite povezovalno geslo, da ga potrdite.
     d. Če želite, vnesite kratek opis poverilnic. Druge informacije niso potrebne. Dodatne informacije boste našli v razdelku "Omogočanje overjanja Kerberos v imeniškem strežniku" na strani 119.
     e. Kliknite **Dokončaj**.

     Po privzetku uporablja oskrbnik za povezavo s potrošnikom lastni storitveni principal. Če se na primer oskrbnik imenuje master.our.org.com, področje pa je SOME.REALM, je DN **ibm-Kn=ldap/master.our.org.com@SOME.REALM**. Vrednost področja ne upošteva velikih in malih črk. Če obstaja več oskrbnikov, morate podati principala in geslo, ki ju bodo uporabljali vsi oskrbniki.

     V strežniku, kjer ste izdelali poverilnice, naredite naslednje:

     a. Razširite **Upravljanje imenika** in kliknite **Upravljanje vnosov**.
     b. Izberite poddrevo, v katerega ste shranili poverilnice, kot je na primer **cn=localhost**, in kliknite **Razširi**.
     c. Izberite **cn=replication** in kliknite **Razširi**.
     d. Izberite poverilnice kerberos (ibm-replicationCredentialsKerberos) in kliknite **Urejanje atributov**.
     e. Kliknite jeziček **Drugi atributi**.
     f. Vnesite **replicaBindDN**, kot je na primer **ibm-kn=myprincipal@SOME.REALM**.
     g. Vnesite **replicaCredentials**. To je geslo KDC, uporabljeno za **myprincipal**.

Opomba: Ta principal in geslo morata biti enaka kot tista, ki ste ju uporabili za zagon pripomočka **kinit** iz ukazne vrstice.

V strežniku za podvajanje naredite naslednje:

a. V področju za usmerjanje kliknite **Upravljanje lastnosti podvajanja**.
b. V spustnem meniju **Informacije o oskrbniku** izberite oskrbnika ali vnesite ime podvojenega poddrevesa, za katerega želite konfigurirati poverilnice oskrbnika.
c. Kliknite **Urejanje**.
d. Vnesite povezovalni DN podvajanja. V tem primeru je to **ibm-kn=myprincipal@SOME.REALM**.
e. Vnesite in potrdite **povezovalno geslo podvajanja**. To je geslo KDC, uporabljeno za **myprincipal**.

- Če ste izbrali z overjanjem potrdil SSL, dodatnih informacij ni potrebno podati, če uporabljate potrdilo strežnika. Če izberete potrdilo, ki ni strežnikovo, naredite naslednje:
  a. Vnesite ime datoteke ključev.
  b. Vnesite geslo datoteke ključev.
  c. Z vnovičnim vnosom gesla datoteke ključev le-tega potrdite.
  d. Vnesite oznako ključa.
  e. Če želite, vnesite kratek opis.
  f. Kliknite **Dokončaj**.

  Dodatne informacije boste našli v razdelku “Omogočanje SSL v imeniškem strežniku” na strani 117.

5. V strežniku, kjer ste izdelali poverilnice, nastavite sistemsko vrednost QRETSVRSEC (Allow server security information to be retained - Omogoči ohranitev informacij o zaščiti strežnika) na 1 (ohrani podatke). Ker so poverilnice podvajanja shranjene na seznamu za preverjanje veljavnosti, jih lahko strežnik pridobi s tega seznama, ko se poveže s strežnikom za podvajanje.

Izdelava strežnika za podvajanje

Opomba: Za izvedbo te naloge se mora strežnik izvajati.

V področju za usmerjanje razširite kategorijo **Upravljanje podvajanja** in kliknite **Upravljanje topologije**.

1. Izberite poddrevo, ki ga želite podvojiti, in kliknite **Prikaži topologijo**.
2. S puščico poleg izbire **Topologija podvajanja** razširite seznam oskrbniških strežnikov.
3. Izberite oskrbniški strežnik in kliknite **Dodaj strežnik za podvajanje**.

Na jezičku **Strežnik** okna **Dodajanje strežnika za podvajanje** naredite naslednje:

- Vnesite gostiteljsko ime in številko vrat za strežnik podvajanja, ki ga izdelujete. Privzeta številka za vrata brez zaščite SSL so 389, za vrata z zaščito SSL pa 636. Ti polji sta obvezni.
- Izberite, ali želite omogočiti komunikacije SSL.
- Vnesite ime strežnika za podvajanje ali pa pustite to polje prazno za uporabo gostiteljskega imena.
- Vnesite ID strežnika za podvajanje. Če se strežnik, v katerem izdelujete strežnik za podvajanje, izvaja, kliknite **Poišči ID strežnika za podvajanje**, da omogočite samodejno izpolnitev tega polja. To polje je obvezno, če bo strežnik, ki ga dodajate, enakovredni strežnik ali strežnik za razpošiljanje. Priporočamo, da uporabljajo vsi strežniki enako izdajo.
- Vnesite opis strežnika za podvajanje.

Na jezičku **Dodatno** naredite naslednje:

1. Podajte poverilnice, ki jih uporablja strežnik za podvajanje za komuniciranje z glavnim strežnikom.

Opomba: Orodje za spletno upravljanje omogoča, da definirate poverilnice na naslednjih mestih:

- **cn=replication,cn=localhost**, ki hrani poverilnice samo v strežniku, ki jih uporablja.

- V podvojenem poddrevesu, ko so poverilnice podvojene z preostalim delom poddrevesa. Poverilnice, shranjene v podvojenem poddrevesu, so izdelane pod vnosom **ibm-replicagroup=default** za to poddrevo.

Shranitev poverilnic v cn=replication,cn=localhost je varnejša.

a. Kliknite **Izbiranje**.
b. Izberite želeno mesto za poverilnice. Priporočamo, da uporabite cn=replication,cn=localhost.
c. Kliknite **Prikaži poverilnice**.
d. Razširite seznam poverilnic in izberite tisto, ki jo želite uporabiti.
e. Kliknite **Potrdi**.

Dodatne informacije o poverilnicah dogovorov boste našli v razdelku “Izdelava poverilnic” na strani 102.

2. Urnik podvajanja izberite s spustnega seznama ali pa ga s klikom gumba **Dodaj** izdelajte. Glejte “Izdelava urnikov podvajanja” na strani 115
3. S seznama zmožnosti oskrbnika lahko odstranite tiste zmožnosti, ki jih ne želite podvojiti v potrošniku.

   Če uporabljate v omrežju strežnike različnih izdaj, so za novejše izdaje na voljo zmožnosti, ki jih starejše ne nudijo. Nekatere zmožnosti, kot so filtrirani ACL-ji in načelo za gesla, uporabljajo operacijske atribute, ki so podvojeni z drugimi spremembami. Če izberete te zmožnosti, boste v večini primerov želeli, da jih podpirajo vsi strežniki. Če zmožnosti ne podpirajo vsi strežniki, je najbrž ne boste uporabili. Tako najbrž ne boste želeli, da bodo na vsakem strežniku uporabljeni različni ACL-ji, toda obstajajo tudi primeri, ko boste uporabili zmožnost v strežnikih, ki jo podpirajo, sprememb pa ne boste povezali z zmožnostjo, podvojeno v strežnikih, ki je ne podpirajo. V takšnih primerih lahko s seznamom zmožnosti označite tiste zmožnosti, ki jih ne želite podvojiti.
4. S klikom gumba **Potrdi** izdelajte strežnik za podvajanje.
5. Prikaže se sporočilo, ki vas obvesti, da morate opraviti dodatna dejanja. Kliknite **Potrdi**.

Opomba: Če dodajate več strežnikov kot dodatnih strežnikov za podvajanje ali izdelujete zapleteno topologijo, ne nadaljujte z razdelkom “Kopiranje podatkov v strežnik za podvajanje” ali “Dodajanje informacij o oskrbniku v strežnik za podvajanje” na strani 106, dokler ne končate z definiranjem topologije v glavnem strežniku. Če izdelate datoteko *masterfile.ldif* po dokončanju topologije, bo vsebovala imeniške vnose glavnega strežnika in celotno kopijo dogovorov iz topologije. Če naložite to datoteko v vse strežnike, bodo vsi strežniki vsebovali enake informacije.

Kopiranje podatkov v strežnik za podvajanje

Po izdelavi strežnika za podvajanje morate izvoziti topologijo iz glavnega strežnika v strežnik za podvajanje.

1. V glavnem strežniku izdelajte datoteko LDIF za podatke. Z naslednjim postopkom prekopirajte vse podatke, vsebovane v glavnem strežniku:
   a. V Navigatorju iSeries razširite **Omrežje**.
   b. Razširite **Strežniki**.
   c. Kliknite **TCP/IP**.
   d. Z desnim gumbom miške kliknite **Imenik** in izberite **Orodja** in nato **Izvozi datoteko**.
   e. Podajte izhodno ime datoteke LDIF (na primer masterfile.ldif), in po želji podajte še poddrevo za izvoz (na primer subtreeDN), in kliknite **Potrdi**.
2. Na računalniku, kjer izdelujete strežnik za podvajanje, naredite naslednje:
   a. Preverite, ali so podvojene pripone definirane v konfiguraciji strežnika za podvajanje.
   b. Zaustavite strežnik za podvajanje.
   c. Datoteko LDIF prekopirajte v strežnik za podvajanje in naredite naslednje:
      1) V Navigatorju iSeries razširite **Omrežje**.
      2) Razširite **Strežniki**.
      3) Kliknite **TCP/IP**.
      4) Z desnim gumbom miške kliknite **Imenik** in izberite **Orodja** in nato **Uvozi datoteko**.
      5) Podajte vhodno ime datoteke LDIF (na primer masterfile.ldif), in želji podajte, ali želite podvojiti podatke, nato pa kliknite **Potrdi**.

Izvede se nalaganje dogovorov o podvajanju, urnikov, poverilnic (če so shranjene v podvojenem poddrevesu) in podatkov vnosov v strežnik za podvajanje.

d. Zaženite strežnik.

Dodajanje informacij o oskrbniku v strežnik za podvajanje

Spremeniti morate konfiguracijo strežnika za podvajanje, da bo določala, kdo lahko podvaja spremembe, in dodati referenčni kazalec v glavni strežnik.

Na računalniku, kjer izdelujete strežnik za podvajanje, naredite naslednje:

1. V področju za usmerjanje razširite **Upravljanje podvajanja** in kliknite **Upravljanje lastnosti podvajanja**.
2. Kliknite **Dodaj**.
3. V spustnem meniju **Podvojeno poddrevo** izberite oskrbnika ali vnesite ime podvojenega poddrevesa, za katerega želite konfigurirati poverilnice oskrbnika. Urejanje poverilnic v tem polju ni mogoče.
4. Vnesite povezovalni DN podvajanja. V tem primeru je to cn=any.

   Opomba: Glede na vaš primer lahko uporabite eno od naslednjih možnosti.

   - Nastavite povezovalni DN podvajanja (in geslo) ter privzeti referenčni kazalec za vsa poddrevesa, podvojena v strežniku s 'privzetimi poverilnicami in referenčnim kazalcem'. To možnost lahko uporabite, če podvojite vsa poddrevesa istega oskrbnika.
   - Nastavite povezovalni DN podvajanja in geslo neodvisno za vsako podvojeno poddrevo, tako da dodate informacije o oskrbniku za vsako poddrevo. To možnost lahko uporabite, če ima vsako poddrevo drugega oskrbnika (to je drug glavni strežnik za vsako poddrevo).
5. Glede na vrsto poverilnic vnesite in potrdite geslo poverilnic. (Geslo ste si predhodno zapisali.)
   - **Preprosta povezava** - podajte DN in geslo
   - **Kerberos** - če poverilnice oskrbnika ne določajo principala in gesla in je potrebno uporabiti lastnega storitvenega principala strežnika, je ta povezovalni DN ibm-kn=ldap/<*ime-vašega-strežnika@vaše-področje*>. Če imajo poverilnice ime principala, kot je <*mojprincipal@mojepodročje*>, ga uporabite kot DN. Geslo v nobenem primeru ni potrebno.
   - **Povezava SSL w/ EXTERNAL** - podajte DN subjekta za potrdilo brez gesla.

   Glejte "Izdelava poverilnic" na strani 102.
6. Kliknite **Potrdi**.
7. Za uveljavitev sprememb morate znova zagnati strežnik za podvajanje.

Dodatne informacije boste našli v razdelku "Spreminjanje lastnosti podvajanja" na strani 114.

Strežnik za podvajanje je v stanju začasne ustavitve in podvajanje se ne izvaja. Ko končate z nastavljanjem topologije podvajanja, morate klikniti **Upravljanje čakalnih vrst**, izbrati strežnik za podvajanje in s klikom možnosti **Začasno ustavi/obnovi** zagnati podvajanje. Podrobnejše informacije boste našli v razdelku "Upravljanje čakalnih vrst" na strani 116. Strežnik za podvajanje zdaj prejme popravke iz glavnega strežnika.

Izdelava topologije glavni strežnik-strežnik za odpošiljanje-strežnik za podvajanje

Če želite definirati topologijo glavni strežnik-strežnik za odpošiljanje-strežnik za podvajanje, morate narediti naslednje:

1. Izdelajte glavni strežnik in strežnik za podvajanje. Glejte "Izdelava topologije glavnega strežnika-strežnika za podvajanje" na strani 101.
2. Izdelajte nov strežnik za podvajanje za izvirni strežnik za podvajanje. Glejte "Izdelava novega strežnika za podvajanje" na strani 107.
3. Prekopirajte podatke v strežnike za podvajanje. Glejte "Kopiranje podatkov v strežnik za podvajanje" na strani 105.

Izdelava novega strežnika za podvajanje

Če ste nastavili topologijo podvajanja (glejte "Izdelava glavnega strežnika (podvojenega poddrevesa)" na strani 102) z glavnim strežnikom (strežnik1) in strežnikom za podvajanje (strežnik2), lahko vlogo strežnika2 spremenite tako, da postane strežnik za odpošiljanje. V ta namen morate pod strežnikom2 izdelati nov strežnik za podvajanje (strežnik3).

1. Orodje za spletno upravljanje povežite z glavnim strežnikom (strežnikom1).
2. V področju za usmerjanje razširite kategorijo Upravljanje podvajanja in kliknite **Upravljanje topologije**.
3. Izberite poddrevo, ki ga želite podvojiti, in kliknite **Prikaži topologijo**.
4. S puščico poleg izbire **Topologija podvajanja** razširite seznam oskrbniških strežnikov.
5. Kliknite puščico poleg izbire **strežnik1**, da razširite seznam strežnikov.
6. Izberite strežnik2 in kliknite **Dodaj strežnik za podvajanje**.
7. Na jezičku **Strežnik** okna **Dodajanje strežnika za podvajanje** naredite naslednje:
   - Vnesite gostiteljsko ime in številko vrat strežnika za podvajanje (strežnika3), ki ga izdelujete. Privzeta številka za vrata brez zaščite SSL so 389, za vrata z zaščito SSL pa 636. Ti polji sta obvezni.
   - Izberite, ali želite omogočiti komunikacije SSL.
   - Vnesite ime strežnika za podvajanje ali pa pustite to polje prazno za uporabo gostiteljskega imena.
   - Vnesite ID strežnika za podvajanje. Če se strežnik, v katerem izdelujete strežnik za podvajanje, izvaja, kliknite **Poišči ID strežnika za podvajanje**, da omogočite samodejno izpolnitev tega polja. To polje je obvezno, če bo strežnik, ki ga dodajate, enakovredni strežnik ali strežnik za razpošiljanje. Priporočamo, da uporabljajo vsi strežniki enako izdajo.
   - Vnesite opis strežnika za podvajanje.

   Na jezičku **Dodatno** naredite naslednje:

   a. Podajte poverilnice, ki jih uporablja strežnik za podvajanje za komuniciranje z glavnim strežnikom.

      Opomba: Orodje za spletno upravljanje omogoča, da definirate poverilnice na dveh mestih:
      - **cn=replication,cn=localhost**, ki hrani poverilnice samo v strežniku, ki jih uporablja.
      - V podvojenem poddrevesu, ko so poverilnice podvojene z preostalim delom poddrevesa.

      Shranitev poverilnic v cn=replication,cn=localhost je varnejša. Poverilnice, shranjene v podvojenem poddrevesu, so izdelane pod vnosom **ibm-replicagroup=default** za to poddrevo.

      1) Kliknite **Izbiranje**.
      2) Izberite želeno mesto za poverilnice. Priporočamo, da uporabite cn=replication,cn=localhost.
      3) Kliknite **Prikaži poverilnice**.
      4) Razširite seznam poverilnic in izberite tisto, ki jo želite uporabiti.
      5) Kliknite **Potrdi**.

      Dodatne informacije o poverilnicah dogovorov boste našli v razdelku "Izdelava poverilnic" na strani 102.

   b. Urnik podvajanja izberite s spustnega seznama ali pa ga s klikom gumba **Dodaj** izdelajte. Glejte "Izdelava urnikov podvajanja" na strani 115.

   c. S seznama zmožnosti oskrbnika lahko odstranite tiste zmožnosti, ki jih ne želite podvojiti v potrošniku.

      Če uporabljate v omrežju strežnike različnih izdaj, so za novejše izdaje na voljo zmožnosti, ki jih starejše ne nudijo. Nekatere zmožnosti, kot so filtrirani ACL-ji in načelo za gesla, uporabljajo operacijske atribute, ki so podvojeni z drugimi spremembami. Če izberete te zmožnosti, boste v večini primerov želeli, da jih podpirajo vsi strežniki. Če zmožnosti ne podpirajo vsi strežniki, je najbrž ne boste uporabili. Tako najbrž ne boste želeli, da bodo na vsakem strežniku uporabljeni različni ACL-ji, toda obstajajo tudi primeri, ko boste uporabili zmožnost v strežnikih, ki jo podpirajo, sprememb pa ne boste povezali z zmožnostjo, podvojeno v strežnikih, ki je ne podpirajo. V takšnih primerih lahko s seznamom zmožnosti označite tiste zmožnosti, ki jih ne želite podvojiti.

   d. S klikom gumba **Potrdi** izdelajte strežnik za podvajanje.

8. Podatke iz strežnika2 prekopirajte v nov strežnik3 za podvajanje. Informacije o tem postopku boste našli v razdelku "Kopiranje podatkov v strežnik za podvajanje" na strani 105.

9. V strežnik3 dodajte dogovor oskrbnika, s čimer postane strežnik2 oskrbnik za strežnik3, strežnik3 pa potrošnik strežnika2. Informacije o tem postopku boste našli v razdelku “Dodajanje informacij o oskrbniku v strežnik za podvajanje” na strani 106.

Vloge strežnika so predstavljene z ikonami v orodju za spletno upravljanje. Topologija je zdaj takšna:

- strežnik1 (glavni strežnik)
  - strežnik2 (strežnik za odpošiljanje)
    - strežnik3 (strežnik za podvajanje)

Pregled izdelave kompleksne topologije podvajanja

Naslednji pregled visoke ravni uporabite kot vodilo pri nastavljanju kompleksne topologije podvajanja.

1. Zaženite vse enakovredne strežnike ali bodoče strežnike za podvajanje. To je potrebno, da lahko orodje za spletno upravljanje zbere informacije iz strežnikov.
2. Zaženite ’prvi’ glavni strežnik in ga konfigurirajte kot glavnega za kontekst.
3. V ’prvi’ glavni strežnik naložite podatke za poddrevo, ki ga želite podvojiti (če podatki še niso naloženi).
4. Izberite poddrevo za podvajanje.
5. Vse potencialne enakovredne glavne strežnike dodajte kot strežnike za podvajanje ’prvega’ glavnega strežnika.
6. Dodajte vse druge strežnike za podvajanje.
7. Druge glavne enakovredne strežnike premaknite, da jih povišate.
8. Vsakemu od glavnih enakovrednih strežnikov dodajte dogovore o podvajanju za strežnike za podvajanje.

   Opomba: Če boste izdelali poverilnice v **cn=replication,cn=localhost**, jih morate izdelati na vsakem strežniku po njihovem vnovičnem zagonu. Podvajanje z enakovrednimi strežniki ne bo uspelo, dokler ne izdelate objektov poverilnic.
9. Vsakemu od glavnih enakovrednih strežnikov dodajte dogovore podvajanja za druge glavne strežnike. ’Prvi’ glavni strežnik te informacije že vsebuje.
10. Podvojeno poddrevo preklopite v mirujoče stanje. S tem preprečite izvajanje popravkov med kopiranjem podatkov v druge strežnike.
11. Za preskok za vsako čakalno vrsto uporabite Upravljanje čakalnih vrst.
12. Izvozite podatke za podvojeno poddrevo iz ’prvega’ glavnega strežnika.
13. Prekinite stanje mirovanja poddrevesa.
14. Zaustavite strežnike za podvajanje in uvozite podatke za podvojeno poddrevo v vsak strežnik za podvajanje in enakovredni glavni strežnik. Nato strežnike znova zaženite.
15. Z upravljanjem lastnosti podvajanja v vsakem strežniku za podvajanje in enakovrednem strežniku nastavite poverilnice, ki jih bodo uporabljali oskrbniki.

Izdelava kompleksne topologije s podvajanjem enakovrednih strežnikov

Podvajanje enakovrednih strežnikov je topologija podvajanja, v kateri je glavnih več strežnikov, vendar za razliko od okolja z več glavnimi strežniki tu ne prihaja do razreševanja navzkrižij med enakovrednimi strežniki. Strežniki LDAP sprejmejo popravke, ki jih posredujejo enakovredni strežniki, in ažurirajo lastne kopije podatkov. Vrstnemu redu popravkov ali možnemu navzkrižju med več popravki ni namenjena nobena pozornost.

Če želite dodati druge glavne strežnike (enakovredne strežnike), najprej dodate strežnik kot dvojnik obstoječih glavnih strežnikov, ki je samo za branje (glejte “Izdelava strežnika za podvajanje” na strani 104), inicializirate imeniške podatke, nato pa povišate strežnik v glavnega (glejte “Prenos ali povišanje strežnika” na strani 112).

V začetku prevzame objekt **ibm-replicagroup**, izdelan s tem postopkom, ACL korenskega vnosa za podvojeno poddrevo. Ti ACL-ji morda ne bodo primerni za krmiljenje dostopa do informacij o podvajanju v imeniku.

Da bi operacija dodajanja poddrevesa uspela, mora DN vnosa, ki ga dodajate, uporabljati pravilne ACL-je, če ni pripona v strežniku.

Za nefiltrirane ACL-je:

- ownersource : <*DN vnosa*>
- ownerpropagate : TRUE
- aclsource : <*DN vnosa*>
- aclpropagate: TRUE

Filtrirani ACL-ji:

- ownersource : <*DN vnosa*>
- ownerpropagate : TRUE
- ibm-filteraclinherit : FALSE
- ibm-filteraclentry : <*katerakoli vrednost*>

S funkcijo **Urejanje ACL-jev** orodja za spletno upravljanje nastavite ACL-je za informacije o podvajanju, povezane z na novo izdelanim podvojenim poddrevesom (glejte “Urejanje seznamov za nadzor dostopa” na strani 113).

Strežnik za podvajanje je v stanju začasne ustavitve in podvajanje se ne izvaja. Ko končate z nastavljanjem topologije podvajanja, morate klikniti **Upravljanje čakalnih vrst**, izbrati strežnik za podvajanje in s klikom možnosti **Začasno ustavi/obnovi** zagnati podvajanje. Podrobnejše informacije boste našli v razdelku “Upravljanje čakalnih vrst” na strani 116. Strežnik za podvajanje zdaj prejme popravke iz glavnega strežnika.

Podvajanje enakovrednih strežnikov uporabite samo v okoljih, kjer je vzorec imeniških popravkov dobro znan. Popravke v določenih objektih znotraj imenika mora opraviti samo en enakovredni strežnik. S tem preprečite scenarij, v katerem en strežnik zbriše objekt, temu pa sledi strežnik, ki objekt spremeni. V tem scenariju je mogoče, da enakovredni strežnik prejme ukaz za brisanje, ki mu sledi ukaz za spreminjanje, kar vodi v navzkrižje.

Če želite definirati topologijo enakovredni strežnik-odpremnik-strežnik za podvajanje, ki je sestavljena iz dveh enakovrednih glavnih strežnikov, dveh strežnikov za odpošiljanje in štirih strežnikov za podvajanje, morate narediti naslednje:

1. Izdelajte glavni strežnik in strežnik za podvajanje. Glejte “Izdelava topologije glavnega strežnika-strežnika za podvajanje” na strani 101.
2. Za glavni strežnik izdelati dva dodatna strežnika za podvajanje. Glejte “Izdelava strežnika za podvajanje” na strani 104.
3. Pod vsakim na novo izdelanim strežnikom za podvajanje izdelati dva strežnika za podvajanje.
4. Povišati izvirni strežnik za podvajanje v glavni strežnik. Glejte “Povišanje strežnika v enakovredni strežnik”.

   Opomba: Strežnik, ki ga želite povišati v glavni strežnik, ne sme imeti nobenih podrejenih strežnikov za podvajanje.
5. Prekopirajte podatke iz glavnega strežnika v nov glavni strežnik in strežnike za podvajanje. Glejte “Kopiranje podatkov v strežnik za podvajanje” na strani 105.

Povišanje strežnika v enakovredni strežnik

S topologijo odpošiljanja, ki ste jo izdelali v razdelku “Izdelava topologije glavni strežnik-strežnik za odpošiljanje-strežnik za podvajanje” na strani 106, lahko povišate strežnik tako, da je enakovreden. V tem zgledu bomo povišali strežnik za podvajanje (strežnik3) v enakovredni strežnik glavnega strežnika (strežnika1).

1. Orodje za spletno upravljanje povežite z glavnim strežnikom (strežnikom1).
2. V področju za usmerjanje razširite kategorijo Upravljanje podvajanja in kliknite **Upravljanje topologije**.
3. Izberite poddrevo, ki ga želite podvojiti, in kliknite **Prikaži topologijo**.
4. S puščico poleg izbire **Topologija podvajanja** razširite seznam strežnikov.
5. Kliknite puščico poleg izbire **strežnik1**, da razširite seznam strežnikov.
6. Kliknite puščico poleg izbire **strežnik1**, da razširite seznam strežnikov.

7. Kliknite **strežnik1** in **Dodaj strežnik za podvajanje**. Izdelajte strežnik4. Glejte “Izdelava strežnika za podvajanje” na strani 104. Z enakim postopkom izdelajte še strežnik5. Vloge strežnika so predstavljene z ikonami v orodju za spletno upravljanje. Topologija je zdaj takšna:
   - strežnik1 (glavni strežnik)
     - strežnik2 (strežnik za odpošiljanje)
       - strežnik3 (strežnik za podvajanje)
     - strežnik4 (strežnik za podvajanje)
     - strežnik5 (strežnik za podvajanje)
8. Kliknite **strežnik2** in **Dodaj strežnik za podvajanje**, da izdelate strežnik6.
9. Kliknite **strežnik4** in **Dodaj strežnik za podvajanje**, da izdelate strežnik7. Z enakim postopkom izdelajte še strežnik8. Topologija je zdaj takšna:
   - strežnik1 (glavni strežnik)
     - strežnik2 (strežnik za odpošiljanje)
       - strežnik3 (strežnik za podvajanje)
       - strežnik6 (strežnik za podvajanje)
     - strežnik4 (strežnik za odpošiljanje)
       - strežnik7 (strežnik za podvajanje)
       - strežnik8 (strežnik za podvajanje
     - strežnik5 (strežnik za podvajanje)
10. Izberite **strežnik5** in kliknite **Prenesi**.

    Opomba: Strežnik, ki ga želite prenesti, ne sme imeti nobenih podrejenih strežnikov za podvajanje.
11. Izberite **Topologija podvajanja**, da povišate strežnik za podvajanje v glavni strežnik. Kliknite **Prenesi**.
12. Prikaže se okno **Izdelava dodatnih dogovorov oskrbnikov**. Podvajanje enakovrednih strežnikov zahteva, da je vsak glavni strežnik oskrbnik in potrošnik drugih glavnih strežnikov v topologiji in vsake od prvih ravni strežnikov za podvajanje, to sta strežnik2 in strežnik4. Strežnik5 je že potrošnik strežnika1, vendar mora zdaj postati oskrbnik za strežnik1, strežnik2 in strežnik4. V okencih za dogovore oskrbnika morajo biti označene naslednje možnosti:

Tabela 3.

	Oskrbnik	Potrošnik
✓	strežnik5	strežnik1
✓	strežnik5	strežnik2
✓	strežnik5	strežnik4

Kliknite **Nadaljuj**.

Opomba: Včasih se prikaže okno Izbira poverilnic, ki zahteva vnos tistih poverilnic, ki niso shranjene v cn=replication,cn=localhost. V tem primeru morate podati objekt poverilnice, ki ni shranjen v cn=replication,cn=localhost. V obstoječem nizu poverilnic izberite poverilnice, ki jih bo uporabilo poddrevo, ali pa izdelajte nove. Glejte “Izdelava poverilnic” na strani 102

.

13. Kliknite **Potrdi**. Topologija je zdaj takšna:
   - strežnik1 (glavni strežnik)
     - strežnik2 (strežnik za odpošiljanje)
       - strežnik3 (strežnik za podvajanje)
       - strežnik6 (strežnik za podvajanje)
     - strežnik4 (strežnik za odpošiljanje)
       - strežnik7 (strežnik za podvajanje)

- strežnik8 (strežnik za podvajanje
  - strežnik5 (glavni strežnik)
- strežnik5 (glavni strežnik)
  - strežnik1 (glavni strežnik)
  - strežnik2 (strežnik za odpošiljanje)
  - strežnik4 (strežnik za odpošiljanje)

14. Podatke iz strežnika1 prekopirajte v vse druge strežnike. Informacije o tem postopku boste našli v razdelku “Kopiranje podatkov v strežnik za podvajanje” na strani 105.

Upravljanje topologij

Topologije so specifične za podvojena poddrevesa.

Prikaz topologije

Opomba: Za izvedbo te naloge se mora strežnik izvajati.

V področju za usmerjanje razširite kategorijo **Upravljanje podvajanja** in kliknite **Upravljanje topologije**.

1. Izberite poddrevo, ki si ga želite ogledati, in kliknite **Prikaži topologijo**.

Topologija se prikaže na seznamu Topologija podvajanja. S klikom modrih trikotnikov razširite topologije. Na tem seznamu lahko naredite naslednje:

- dodate strežnik za podvajanje
- uredite informacije obstoječega strežnika za podvajanje
- preklopite v drug oskrbniški strežnik za strežnik podvajanja ali povišate strežnik za podvajanje v glavni strežnik
- zbrišete strežnik za podvajanje.

Dodajanje strežnika za podvajanje

Glejte “Izdelava strežnika za podvajanje” na strani 104.

Urejanje dogovora

Za strežnik podvajanja lahko spremenite naslednje informacije:

Na jezičku **Strežnik** lahko spremenite samo naslednje:

- gostiteljsko ime
- vrata
- omogočanje SSL
- opis

Na jezičku **Dodatno** lahko spremenite naslednje:

- poverilnice - glejte “Izdelava poverilnic” na strani 102.

- urnike podvajanja - glejte “Izdelava urnikov podvajanja” na strani 115.
- spremenite zmožnosti, ki so podvojene v potrošniški strežnik za podvajanje; S seznama zmožnosti oskrbnika lahko odstranite tiste zmožnosti, ki jih ne želite podvojiti v potrošniku.
- Ko končate, kliknite **Potrdi**.

Prenos ali povišanje strežnika

1. Izberite želeni strežnik in kliknite **Prenesi**.
2. Izberite strežnik, v katerega želite prenesti strežnik za podvajanje, za povišanje strežnika za podvajanje v glavni strežnik pa izberite **Topologija podvajanja**. Kliknite **Prenesi**.
3. Včasih se prikaže okno Izbira poverilnic, ki zahteva vnos tistih poverilnic, ki niso shranjene v cn=replication,cn=localhost. V tem primeru morate podati objekt poverilnice, ki ni shranjen v cn=replication,cn=localhost. V obstoječem nizu poverilnic izberite poverilnice, ki jih bo uporabilo poddrevo, ali pa izdelajte nove. Glejte “Izdelava poverilnic” na strani 102.
4. Prikaže se okno **Izdelava dodatnih dogovorov oskrbnikov**. Izberite dogovore oskrbnika, ki ustrezajo vlogi strežnika. Če boste na primer strežnik za podvajanje povišali v enakovredni strežnik, morate izbrati izdelavo dogovorov oskrbnika z vsemi drugimi strežniki in njihovimi strežniki za podvajanje prve ravni. Ti dogovori omogočajo, da deluje povišani strežnik kot oskrbnik za druge strežnike in njihove strežnike za podvajanje. Obstoječi dogovori oskrbnika iz drugih strežnikov v na novo izdelani povišani strežnik še vedno delujejo, zato jih ni potrebno na novo izdelati.
5. Kliknite **Potrdi**.

Sprememba v drevesu topologije odraža prenos strežnika.

Za dodatne informacije glejte “Izdelava kompleksne topologije s podvajanjem enakovrednih strežnikov” na strani 108.

Znižanje glavnega strežnika

Z naslednjim postopkom spremenite vlogo glavnega strežnika v strežnik za podvajanje:

1. Orodje za spletno upravljanje povežite s strežnikom, ki ga želite znižati.
2. Kliknite **Upravljanje topologije**.
3. Izberite poddrevo in kliknite **Prikaži topologijo**.
4. Zbrišite vse dogovore za strežnik, ki ga želite znižati.
5. Izberite strežnik, ki ga znižujete, in kliknite **Prenesi**.
6. Izberite strežnik, pod katerega boste shranili znižani strežnik, in kliknite **Prenesi**.
7. Podobno kot za novi strežnik za podvajanje izdelajte nove dogovore oskrbnika med znižanim strežnikom in njegovim oskrbnikom. Navodila boste našli v razdelku “Izdelava strežnika za podvajanje” na strani 104.

Podvajanje poddrevesa

Opomba: Za izvedbo te naloge se mora strežnik izvajati.

V področju za usmerjanje razširite kategorijo **Upravljanje podvajanja** in kliknite **Upravljanje topologije**.

- Kliknite **Dodaj poddrevo**.
- Vnesite DN poddrevesa, ki ga želite podvojiti, ali pa z gumbom **Preglej** razširite vnose in izberite vnos, ki bo koren poddrevesa.
- Vnesite URL referenčnega kazalca glavnega strežnika. Ta mora imeti obliko URL-ja LDAP, kot je naslednja:
  `ldap://<ime-mojega-strežnika>.<moje-mesto>.<moje-podjetje>.com`
- Kliknite **Potrdi**.
- Nov strežnik je prikazan v oknu Upravljanje topologije pod naslovom **Podvojena poddrevesa**.

Urejanje poddrevesa

S to možnostjo spremenite URL glavnega strežnika, v katerega pošiljajo popravke to poddrevo in njegovi strežniki za podvajanje. To morate narediti, če spremenite številko vrat ali gostiteljsko ime glavnega strežnika ali spremenite glavni strežnik v kakšen drug strežnik.

1. Izberite poddrevo, ki ga želite urediti.
2. Kliknite **Urejanje poddrevesa**.
3. Vnesite URL referenčnega kazalca glavnega strežnika. Ta mora imeti obliko URL-ja LDAP, kot je naslednja:
   `ldap://<ime-mojega-novega-strežnika>.<moje-mesto>.<moje-podjetje>.com`

Glede na vlogo, ki jo ima strežnik v tem poddrevesu (glavni strežnik, strežnik za podvajanje ali strežnik za odpošiljanje), se v oknu prikažejo različne oznake in gumbi.

- Če ima poddrevo vlogo strežnika za podvajanje, je poleg gumba **Strežnik spremeni v glavnega** prikazana še oznaka, ki kaže, da strežnik deluje kot strežnik za podvajanje ali strežnik za odpošiljanje. Če kliknete ta gumb, postane strežnik, s katerim je povezano orodje za spletno upravljanje, glavni strežnik.
- Če z dodajanjem pomožnega razreda konfigurirate poddrevo samo za podvajanje (privzeta skupina ali podvnos nista prisotna), je poleg gumba **Podvoji poddrevo** prikazana oznaka **To poddrevo ni podvojeno**. Če kliknete ta gumb, dodate privzeto skupino in podvnos, tako da postane strežnik, s katerim je povezano orodje za spletno upravljanje, glavni strežnik.
- Če ni najden noben podvnos za glavne strežnike, je poleg gumb **Strežnik spremeni v glavnega** prikazana oznaka **Za to poddrevo ni definiran noben glavni strežnik**. Če kliknete ta gumb, je dodan manjkajoči podvnos, tako da postane strežnik, s katerim je povezano orodje za spletno upravljanje, glavni strežnik.

Odstranjevanje poddrevesa

1. Izberite poddrevo, ki ga želite odstraniti.
2. Kliknite **Zbriši poddrevo**.
3. Za poziv na potrditev brisanja kliknite **Potrdi**.

Poddrevo je odstranjeno s seznama **Podvojeno poddrevo**.

Opomba: Ta operacija uspe samo, če je vnos ibm-replicaGroup=default prazen.

Preklop poddrevesa v mirujoče stanje

Ta funkcija je uporabna, če želite opraviti vzdrževanje v topologijo ali le-to spremeniti. Z njo zmanjšate število popravkov, ki jih je mogoče opraviti v strežniku. Mirujoči strežnik ne sprejema odjemalskih zahtev, pač pa samo zahteve skrbnika, ki uporablja krmilni element Upravljanje strežnika.

Ta funkcija je Boolova.

1. Za preklop poddrevesa v mirujoče stanje kliknite **Mirujoče stanje/Prekini mirujoče stanje**.
2. Za poziv na potrditev dejanja kliknite **Potrdi**.
3. Za prekinitev mirujočega stanja poddrevesa kliknite **Mirujoče stanje/Prekini mirujoče stanje**.
4. Za poziv na potrditev dejanja kliknite **Potrdi**.

Urejanje seznamov za nadzor dostopa

Informacije o podvajanju (podvnosi podvajanja, dogovori o podvajanju, urniki, poverilnice) so shranjene pod posebnim objektom **ibm-replicagroup=default**. Objekt ibm-replicagroup se nahaja neposredno pod korenskim vnosom podvojenega poddrevesa. Po privzetku nasledi to poddrevo ACL od korenskega vnosa podvojenega poddrevesa. Ta ACL morda ne bo primeren za krmljenje dostopa do informacij o podvajanju.

Potrebna pooblastila:

- krmiljenje podvajanja - potrebujete pisalni dostop za objekt ibm-replicagroup=default (ali pa morate biti lastnik/skrbnik)

- kaskadno krmiljenje podvajanja - potrebujete pisalni dostop za objekt ibm-replicagroup=default (ali pa morate biti lastnik/skrbnik)
- krmiljenje čakalne vrste - potrebujete pisalni dostop za dogovor o podvajanju.

Za prikaz lastnosti ACL-jev z orodjem za spletno upravljanje in za delo z ACL-ji preglejte razdelek “Upravljanje seznamov za nadzor dostopa (ACL-jev)” na strani 145.

Dodatne informacije boste našli v razdelku “Seznami za nadzor dostopa” na strani 47.

Spreminjanje lastnosti podvajanja

V področju za usmerjanje razširite kategorijo **Upravljanje podvajanja** in kliknite **Upravljanje lastnosti podvajanja**. Za prikaz upravljanja lastnosti podvajanja se morate prijaviti v orodje za spletno upravljanje kot projicirani uporabnik i5/OS s posebnima pooblastiloma *ALLOBJ in *IOSYSCFG.

V tem oknu lahko naredite naslednje:

- Spremenite največje število sprememb v teku, ki jih bodo vrnile poizvedbe o statusu podvajanja. Privzeta vrednost je 200.
- Dodate, uredite ali zbrišete informacije o oskrbniku.

  Opomba: DN oskrbnika je lahko DN projiciranega profila uporabnika i5/OS. Projicirani profil uporabnika i5/OS ne sme imeti upravnega pooblastila LDAP. Uporabnik ne sme imeti posebnih pooblastil *ALLOBJ in *IOSYSCFG in mu ne sme biti dodeljeno upravno pooblastilo prek ID-ja aplikacije skrbnika imeniškega strežnika.

Dodatne informacije boste našli v naslednjih temah:

- “Dodajanje informacij oskrbnika”
- “Urejanje informacij oskrbnika” na strani 115
- “Odstranjevanje informacij oskrbnika” na strani 115

Dodajanje informacij oskrbnika

1. Kliknite **Dodaj**.
2. Oskrbnika izberite s spustnega seznama ali pa vnesite ime podvojenega poddrevesa, ki ga želite dodati kot oskrbnika.
3. Vnesite povezovalni DN podvajanja za poverilnice.

   Opomba: Glede na vaš primer lahko uporabite eno od naslednjih možnosti.
   - Nastavite povezovalni DN podvajanja (in geslo) ter privzeti referenčni kazalec za vsa poddrevesa, podvojena v strežniku s ’privzetimi poverilnicami in referenčnim kazalcem’. To možnost lahko uporabite, če podvojite vsa poddrevesa istega oskrbnika.
   - Nastavite povezovalni DN podvajanja in geslo neodvisno za vsako podvojeno poddrevo, tako da dodate informacije o oskrbniku za vsako poddrevo. To možnost lahko uporabite, če ima vsako poddrevo drugega oskrbnika (to je drug glavni strežnik za vsako poddrevo).
4. Glede na vrsto poverilnic vnesite in potrdite geslo poverilnic. (Geslo ste si predhodno zapisali.)
   - **Preprosta povezava** - podajte DN in geslo
   - **Kerberos** - podajte navidezni DN v obliki ’ibm-kn=storitveno-ime-LDAP@področje’ brez gesla
   - **Povezava SSL w/ EXTERNAL** - podajte DN subjekta za potrdilo brez gesla.

   Glejte “Izdelava poverilnic” na strani 102.
5. Kliknite **Potrdi**.

Poddrevo oskrbnika je dodano na seznam Informacije oskrbnika.

Urejanje informacij oskrbnika

1. Izberite poddrevo oskrbnika, ki ga želite urejati.
2. Kliknite **Urejanje**.
3. Če urejate **privzete poverilnice in referenčni kazalec**, ki se uporabljata za izdelavo vnosa cn=Master Server pod cn=configuration, vnesite v polje URL LDAP privzetega oskrbnika URL strežnika, iz katerega bo odjemalec prejemal popravke strežnika za podvajanje. To mora biti veljaven LDAP URL (ldap://). V nasprotnem primeru skočite na četrti korak.
4. Vnesite povezovalni DN podvajanja za nove poverilnice, ki jih želite uporabiti.
5. Vnesite in potrdite geslo poverilnic.
6. Kliknite **Potrdi**.

Odstranjevanje informacij oskrbnika

1. Izberite poddrevo oskrbnika, ki ga želite odstraniti.
2. Kliknite **Zbriši**.
3. Za poziv na potrditev brisanja kliknite **Potrdi**.

Poddrevo je odstranjeno s seznama Informacije oskrbnika.

Izdelava urnikov podvajanja

Če želite, lahko definirate urnike podvajanja, s katerimi načrtujete izvedbo podvajanja ob določenih urah. Če urnika ne uporabite, strežnik načrtuje podvajanje pri vsaki opravljeni spremembi. Ta možnost je enakovredna urniku, v katerem podate takojšnje podvajanje, ki se začne vse dni ob 12.00.

V področju za usmerjanje razširite kategorijo **Upravljanje podvajanja** in kliknite **Upravljanje urnikov**.

Na jezičku **Tedenski urnik** izberite poddrevo, za katerega želite izdelati urnik, in kliknite **Prikaži urnike**. Če obstaja kakšen urnik, je prikazan v okencu **Tedenski urniki**. Nov urnik izdelate ali dodate takole:

1. Kliknite **Dodaj**.
2. Vnesite ime urnika, kot je na primer **urnik1**.
3. Za vse dni od nedelje do sobote je dnevni urnik podan kot **Nič**, kar pomeni, da ni načrtovan noben dogodek podvajanja. V veljavi je še zadnji dogodek podvajanja, če obstaja. Ker gre za nov strežnik za podvajanje, prejšnji dogodki podvajanja ne obstajajo, zato je urnik po privzetku nastavljen na takojšnje podvajanje.
4. Če želite za dan izdelati dnevni urnik podvajanja, lahko dan izberete in kliknete **Dodaj dnevni urnik**. Izdelan dnevni urnik postane privzeti urnik za vse dni v tednu. Naredite lahko naslednje:
   - Ohranite dnevni urnik kot privzetek za vse dni ali izberete določen dan in spremenite urnik nazaj v vrednost Nič. Ne pozabite, da je za dan, za katerega ni načrtovan noben dogodek podvajanja, še vedno v veljavi zadnji dogodek podvajanja.
   - Spremenite dnevni urnik, tako da izberete dan in kliknete **Urejanje dnevnega urnika**. Ne pozabite, da vplivajo spremembe v dnevnem urniku na vse dni, ki uporabljajo ta urnik, in ne samo na izbran dan.
   - Izdelate drug dnevni urnik, tako da izberete dan in kliknete **Dodaj dnevni urnik**. Po končani izdelavi je ta urnik dodan v spustni meni **Dnevni urnik**. Ta urnik morate izbrati za vsak dan, za katerega ga želite uporabiti.

   Dodatne informacije o nastavitvi dnevnih urnikov boste našli v razdelku “Izdelava dnevnega urnika”.
5. Ko končate, kliknite **Potrdi**.

Izdelava dnevnega urnika

V področju za usmerjanje razširite kategorijo **Upravljanje podvajanja** in kliknite **Upravljanje urnikov**.

Na jezičku **Dnevni urnik** izberite poddrevo, za katerega želite izdelati urnik, in kliknite **Prikaži urnike**. Če obstaja kakšen urnik, je prikazan v okencu **Dnevni urniki**. Nov urnik izdelate ali dodate takole:

1. Kliknite **Dodaj**.
2. Vnesite ime urnika, kot je na primer **ponedeljek1**.

3. Za nastavitev časovnega pasu izberite UTC ali lokalni pas.
4. S spustnega menija izberite tip podvajanja:

   Takoj Izvede vse čakajoče popravke vnosov od zadnjega dogodka podvajanja, nato pa vnose ažurira nepretrgano, dokler ne doseže naslednjega načrtovanega dogodka ažuriranja.

   Enkrat
   Pred začetnim časom izvede vse čakajoče popravke. Vsi popravki, ki so izvedeni po začetnem času, bodo počakali do naslednjega načrtovanega dogodka podvajanja.
5. Izberite začetni čas za dogodek podvajanja.
6. Kliknite **Dodaj**. Prikažeta se tip dogodka podvajanja in ura.
7. Z dodajanjem ali odstranjevanjem dogodkov dokončajte urnik. Seznam dogodkov je osvežen v kronološkem vrstnem redu.
8. Ko končate, kliknite **Potrdi**.

Na primer:

Tabela 4.

Tip podvajanja	Začetni čas
Takoj	12.00
Enkrat	10.00
Enkrat	14.00
Takoj	16.00
Enkrat	20.00

V tem urniku se zgodi prvi dogodek podvajanja ob polnoči in ažurira vse čakajoče spremembe pred tem časom. Popravki podvajanja se opravljajo med izvajanjem do 10.00. Popravki, izvedeni med 10.00 in 14.00, bodo podvojeni ob 14.00. Popravki, izvedeni med 14.00 in 16.00 počakajo na dogodek podvajanja, ki je načrtovan ob 16.00, kasneje pa se popravki podvajanja nadaljujejo do naslednjega načrtovanega dogodka podvajanja ob 20.00. Popravki, izvedeni po 20.00, počakajo do naslednjega načrtovanega dogodka podvajanja.

Opomba: Če so dogodki podvajanja načrtovani preblizu skupaj, je dogodek podvajanja lahko izpuščen, če so popravki iz prejšnjega dogodka še vedno v teku, ko je že načrtovan naslednji dogodek.

Upravljanje čakalnih vrst

S to nalogo lahko nadzorujete status podvajanja za vsak dogovor o podvajanju (čakalno vrsto), ki ga uporablja ta strežnik.

V področju za usmerjanje razširite kategorijo **Upravljanje podvajanja** in kliknite **Upravljanje čakalnih vrst**.

Izberite strežnik za podvajanje, za katerega želite upravljati čakalno vrsto.

- Glede na status strežnika za podvajanje lahko kliknete **Začasno ustavi/obnovi**, da podvajanje zaustavite ali zaženete.
- Kliknite **Uveljavi podvajanje**, da podvojite vse čakajoče spremembe ne glede na to, kjer je načrtovano naslednje podvajanje.
- Za dodatne informacije o čakalni vrsti strežnika za podvajanje kliknite **Podrobnosti čakalne vrste**. Iz te izbire lahko tudi upravljate čakalno vrsto.
- Če želite ažurirati čakalne vrste in počistiti sporočila strežnika, kliknite **Osveži**.

Podrobnosti čakalne vrste

Če ste kliknili izbiro **Podrobnosti čakalne vrste**, se prikažejo trije jezički:

- Status

- Podrobnosti zadnjega poskusa
- Čakajoče spremembe

Na jezičku **Status** so prikazani ime strežnika za podvajanje, njegovo poddrevo, status in zapis časov podvajanja. V tem oknu lahko s klikom gumba **Nadaljuj** začasno ustavite podvajanje ali ga nadaljujete. Za ažuriranje informacij o čakalni vrsti kliknite **Osveži**.

Jeziček **Podrobnosti zadnjega poskusa** podaja informacije o zadnjem poskusu ažuriranja. Če vnosa ni mogoče naložiti, pritisnite **Preskoči blokiran vnos**, da nadaljujete podvajanje z naslednjim čakajočim vnosom. Za ažuriranje informacij o čakalni vrsti kliknite **Osveži**.

Na jezičku **Čakajoče spremembe** so prikazane vse čakajoče spremembe za strežnik podvajanja. Če je podvajanje blokirano, lahko s klikom gumba **Preskoči vse** zbrišete vse čakajoče spremembe. Za ažuriranje seznama čakajočih sprememb, tako da bo odražal vsak novi popravek ali obdelane popravke, kliknite **Osveži**.

Opomba: Če se odločite, da boste blokirne spremembe preskočili, morate potrošniški strežnik na koncu ažurirati. Za dodatne informacije glejte “ldapdiff” na strani 178.

Omogočanje SSL v imeniškem strežniku

Če imate v sistemu nameščen Upravljalnik digitalnih potrdil, lahko s plastjo zaščitenih vtičnic (SSL) zaščitite dostop do imeniškega strežnika. Preden v imeniškem strežniku omogočite SSL, priporočamo, da preberete razdelek “Plast zaščitenih vtičnic (SSL) in zaščita plasti prenosa z imeniškim strežnikom” na strani 40.

Za uporabo povezave SSL pri upravljanju imeniškega strežnika iz Navigatorja iSeries ali za uporabo SSL z odjemalcem Windows LDAP morate imeti na PC-ju nameščenega enega od izdelkov za šifriranje odjemalcev (5722CE2 ali 5722CE3).

SSL v strežniku LDAP omogočite takole:

1. **Povezava potrdila z imeniškim strežnikom**
   a. Če želite upravljati imeniški strežnik prek povezave SSL iz Navigatorja iSeries, preberite Navodila uporabniku iSeries Access za Windows (po izbiri ga lahko namestite na PC pri namestitvi Navigatorja iSeries). Če boste za imeniški strežnik izbrali povezave s SSL in brez SSL, lahko ta korak preskočite.
   b. Zaženite IBM-ov Upravljalnik digitalnih potrdil. Dodatne informacije boste našli v razdelku Zagon Upravljalnika digitalnih potrdil teme Upravljalnik digitalnih potrdil.
   c. Če morate potrdila pridobiti ali izdelati ali kako drugače nastaviti ali spremeniti sistem potrdil, to naredite zdaj. Informacije o nastavljanju sistema potrdil boste našli v temi Upravljalnik digitalnih potrdil. Z imeniškim strežnikom sta povezani dve strežniški aplikaciji in ena odjemalska aplikacija, in sicer:

      Aplikacija imeniškega strežnika
      Aplikacija imeniškega strežnika je sam strežnik.

      Objavna aplikacija imeniškega strežnika
      Objavna aplikacija imeniškega strežnika določa potrdilo, uporabljeno pri objavljanju.

      Odjemalska aplikacija imeniškega strežnika
      Odjemalska aplikacija imeniškega strežnika določa privzeto potrdilo, ki ga uporabljajo aplikacije, ki uporabljajo odjemalske API-je ILE LDAP.

   d. Kliknite gumb **Izberi prostor za potrdila**.
   e. Izberite ***SYSTEM**. Kliknite **Nadaljuj**.
   f. Vnesite ustrezno geslo prostora za potrdila *SYSTEM. Kliknite **Nadaljuj**.
   g. Ko se levi meni za usmerjanje na novo naloži, razširite možnost **Upravljanje aplikacij**.
   h. Kliknite **Ažuriraj dodelitve potrdil**.
   i. Na naslednjem zaslonu izberite aplikacijo **Strežnik**. Kliknite **Nadaljuj**.

j. Izberite **Strežnik imeniškega strežnika**.

k. Kliknite **Ažuriraj dodelitev potrdil**, da dodelite imeniškemu strežniku potrdilo, s katerim bo vzpostavil svojo identiteto za odjemalce iSeries Access za Windows.

Opomba: Če izberete potrdilo službe za potrdila, katere potrdilo ni v bazi podatkov ključev odjemalca iSeries Access za Windows, ga morate za uporabo zaščite SSL dodati. Ta postopek dokončajte, preden začnete zgornjega.

l. S seznama izberite potrdilo, ki ga boste dodelili strežniku.

m. Kliknite **Dodeli novo potrdilo**.

n. DCM na novo naloži stran **Ažuriraj dodelitev potrdil** s potrditvenim sporočilom. Ko končate z nastavljanjem potrdil za imeniški strežnik, kliknite **Opravljeno**.

2. **Povežite potrdilo za objavljanje imeniškega strežnika**. (neobvezen korak) Če želite omogočiti objavljanje iz sistema v imeniškem strežniku prek povezave SSL, lahko povežete potrdilo z objavljanjem imeniškega strežnika. S tem določite privzeto potrdilo in overjene službe za potrdila za aplikacije, ki uporabljajo API-je ILE LDAP, ki ne podajajo lastnega ID-ja aplikacije ali nadomestne baze podatkov ključev.

a. Zaženite IBM-ov Upravljalnik digitalnih potrdil.

b. Kliknite gumb **Izberi prostor za potrdila**.

c. Izberite ***SYSTEM**. Kliknite **Nadaljuj**.

d. Vnesite ustrezno geslo prostora za potrdila *SYSTEM. Kliknite **Nadaljuj**.

e. Ko se levi meni za usmerjanje na novo naloži, razširite možnost **Upravljanje aplikacij**.

f. Kliknite **Ažuriraj dodelitve potrdil**.

g. Na naslednjem zaslonu izberite aplikacijo **Odjemalec**. Kliknite **Nadaljuj**.

h. Izberite **Objavljanje imeniškega strežnika**.

i. Kliknite **Ažuriraj dodelitev potrdila**, da dodelite potrdilo za objavljanje imeniškega strežnika, ki bo določalo njegovo identiteto.

j. S seznama izberite potrdilo, ki ga boste dodelili strežniku.

k. Kliknite **Dodeli novo potrdilo**.

l. DCM na novo naloži stran **Ažuriraj dodelitev potrdil** s potrditvenim sporočilom.

Opomba: Tej koraki so napisani na predpostavki, da informacije v imeniškem strežniku že objavljate s povezavo, ki ne uporablja SSL. Celotne informacije o nastavitvi objavljanja boste našli v razdelku “Objavljanje informacij v imeniškem strežniku” na strani 149.

3. **Povezava potrdila za odjemalca imeniškega strežnika**. (neobvezen korak) Če imate druge aplikacije, ki uporabljajo povezave SSL z imeniškim strežnikom, morate potrdilo povezati z odjemalcem imeniškega strežnika.

a. Zaženite IBM-ov Upravljalnik digitalnih potrdil.

b. Kliknite gumb **Izberi prostor za potrdila**.

c. Izberite ***SYSTEM**. Kliknite **Nadaljuj**.

d. Vnesite ustrezno geslo prostora za potrdila *SYSTEM. Kliknite **Nadaljuj**.

e. Ko se levi meni za usmerjanje na novo naloži, razširite možnost **Upravljanje aplikacij**.

f. Kliknite **Ažuriraj dodelitve potrdil**.

g. Na naslednjem zaslonu izberite aplikacijo **Odjemalec**. Kliknite **Nadaljuj**.

h. Izberite **Odjemalec imeniškega strežnika**.

i. Kliknite **Ažuriraj dodelitev potrdila**, da dodelite potrdilo za odjemalcu imeniškega strežnika, ki bo določalo njegovo identiteto.

j. S seznama izberite potrdilo, ki ga boste dodelili strežniku.

k. Kliknite **Dodeli novo potrdilo**.

l. DCM na novo naloži stran **Ažuriraj dodelitev potrdil** s potrditvenim sporočilom.

Ko omogočite SSL, lahko spremenite vrata, ki jih uporablja imeniški strežnik za zaščitene povezave.

Omogočanje overjanja Kerberos v imeniškem strežniku

Če imate v sistemu konfigurirano storitev za omrežno overjanje, lahko nastavite imeniški strežnik za uporabo overjanja Kerberos. Overjanje Kerberos velja za uporabnike in skrbnika. Preden omogočite v imeniškem strežniku Kerberos, lahko preberete pregled uporabe overjanja Kerberos z imeniškim strežnikom.

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

Upravljanje sheme

Dodatne informacije o shemi boste našli v razdelku “Shema” na strani 15.

Shemo lahko upravljate z orodjem za spletno upravljanje ali z aplikacijo LDAP, kot je ldapmodify, v kombinaciji z datotekami LDIF. Pri prvem definiranju objektnih razredov ali atributov bo uporaba orodja za spletno upravljanje najbrž najbolj priročna. Če morate prekopirati novo shemo v druge strežnike (morda kot del izdelka ali orodja, ki ju razvijate), bo pripomoček ldapmodify morda bolj uporaben; dodatne informacije boste našli v razdelku “Kopiranje sheme v druge strežnike” na strani 128.

Dodatne informacije boste našli v naslednjih temah:
- “Prikaz objektnih razredov”
- “Dodajanje objektnega razreda” na strani 120
- “Urejanje objektnega razreda” na strani 121
- “Kopiranje objektnega razreda” na strani 122
- “Brisanje objektnega razreda” na strani 123
- “Prikaz atributov” na strani 124
- “Dodajanje atributa” na strani 124
- “Urejanje atributa” na strani 125
- “Kopiranje atributa” na strani 127
- “Brisanje atributa” na strani 128

Prikaz objektnih razredov

Objektne razrede v shemi si lahko ogledate z orodjem za spletno upravljanje, izbrani način ali z ukazno vrstico.

Spletno upravljanje

V področju za usmerjanje razširite **Upravljanje shem** in kliknite **Upravljanje objektnih razredov**. Prikaže se okno samo za branje, v katerem si lahko ogledate objektne razrede v shemi in njihove značilnosti. Objektni razredi so prikazani v abecednem vrstnem redu. S klikom gumbov Nazaj ali Naprej se lahko premaknete za eno stran nazaj ali naprej. Polje poleg teh gumbov določa stran, na kateri ste. Za skok na določeno stran lahko uporabite tudi spustni meni tega polja. Prvi objektni razred, naveden na stran, je prikazan s številko strani, ki vam pomaga najti objektni razred, ki si ga želite ogledati. Če na primer iščete objektni razred **person**, razširite spustni meni in se pomaknete do **strani 14 od 16 nsLiServer** in **stran 15 od 16 printerLPR**. Ker je objektni razred person po abecednem vrstnem redu med nsLiServer in printerLPR, izberite stran 14 in kliknite **Pojdi**.

Objektne razrede lahko prikažete tudi razvrščene po tipu. Izberite **Tip** in kliknite **Razvrsti**. Objektni razredi so razvrščeni v abecednem vrstnem redu po tipu, in sicer abstraktni, pomožni ali strukturalni. Vrstni red na seznamu lahko obrnete, tako da izberete **Padajoče** in kliknete **Razvrsti**.

Ko najdete želeni objektni razred, si lahko ogledate njegov tip, nasledstvo, obvezne atribute in neobvezne atribute. Razširite spustne menije za nasledstvo, obvezne atribute in neobvezne atribute, da prikažete celoten izpis za vsako značilnost.

V orodjarni na desni strani lahko izberete operacije, ki jih želite izvesti v objektnem razred:

- dodajanje
- urejanje
- kopiranje
- brisanje.

Ko končate, kliknite **Zapri**, da se vrnete v **uvodno** okno strežnika IBM Directory Server.

Ukazna vrstica

Za prikaz objektnih razredov, vsebovanih v shemi, izdajte naslednji ukaz:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Dodajanje objektnega razreda

Spletno upravljanje

Če v področju za upravljanje še niste razširili možnosti **Upravljanje shem**, to naredite zdaj, nato pa kliknite **Upravljanje objektnih razredov**. Nov objektni razred izdelate z naslednjim postopkom:

1. Kliknite **Dodaj**.

   Opomba: Do tega okna lahko dostopite tudi tako, da v področju za upravljanje razširite možnost **Upravljanje shem** in kliknete **Dodaj objektni razred**.
2. Na jezičku **Splošne lastnosti** naredite naslednje:
   - Vnesite **ime objektnega razreda**. To polje je obvezno je je opisno za funkcijo objektnega razreda, kot je na primer **tempEmployee** za objektni razred, uporabljen za sledenje začasnih uslužbencev.
   - Vnesite **opis** objektnega razreda, kot je na primer **Objektni razred, uporabljen za začasne uslužbence**.
   - Vnesite **OID** za objektni razred. To polje je obvezno. Glejte “Identifikator objekta (OID)” na strani 25. Če OID-ja nimate, lahko uporabite **ime objektnega razreda**, ki mu dodate **-oid**. Če je ime objektnega razreda na primer **tempEmployee**, uporabite OID **tempEmployee-oid**. Vrednost tega polja lahko spremenite.
   - S spustnega seznama izberite **nadrejeni objektni razred**. S tem določite objektni razred, iz katerega bodo podedovani drugi atributi. Običajno je **nadrejeni objektni razred zgornji**, vendar ni nujno. Nadrejeni objektni razred za **tempEmployee** je lahko na primer **ePerson**.
   - Izberite **tip objektnega razreda**. Dodatne informacije o tipih objektnih razredov boste našli v razdelku “Objektni razredi” na strani 17.
   - Kliknite jeziček Atributi in podajte obvezne in neobvezne atribute za objektni razred in si oglejte podedovane atribute, ali pa kliknite **Potrdi** in dodajte nov objektni razred, ali pa kliknite **Prekliči** in se vrnite v **upravljanje objektnih razredov**, ne da bi opravili kakšno spremembo.
3. Na jezičku **Atributi** naredite naslednje:
   - Iz abecednega seznama **Razpoložljivi atributi** izberite atribut in kliknite **Dodaj med obvezne**, da spremenite atribut v obveznega, ali pa kliknite **Dodaj med neobvezne**, da bo atribut za objektni razred neobvezen. Atribut je prikazan na ustreznem seznamu izbranih atributov.
   - Ta postopek ponovite za vse atribute, ki jih želite izbrati.

- Atribut lahko prenesete z enega seznama na drugega ali ga zbrišete z izbranih seznamov, tako da ga izberete in kliknete ustrezen gumb **Prenesi na** ali **Zbriši**.
- Seznam obveznih in neobveznih podedovanih atributov si lahko ogledate. Podedovani atributi temeljijo na **nadrejenem objektnem razredu**, ki ste ga izbrali na jezičku **Splošno**. Podedovanih atributov ne morete spremeniti, toda če spremenite **nadrejeni objektni razred** na jezičku **Splošno**, se prikaže drug niz podedovanih atributov.

4. Za dodajanje novega objektnega razreda kliknite **Potrdi**, za vrnitev v okno **Upravljanje objektnih razredov**, ne da bi opravili kakšno spremembo, pa **Prekliči**.

Opomba: Če ste na jezičku **Splošno** kliknili **Potrdi**, ne da bi dodali kakšen atribut, jih lahko dodate tako, da uredite nov objektni razred.

Ukazna vrstica

Za dodajanje objektnega razreda z ukazno vrstico izdajte naslednji ukaz:

```
ldapmodify -D <adminDN> -w <adminPW> -i <ime-datoteke>
```

kjer <*ime-datoteke*>vsebuje:

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: ( <myobjectClass-oid> NAME
'<mojObjektniRazred>'
DESC '<Objektni razred,
                definiran za mojo aplikacijo LDAP>'
SUP '< objectclassinheritance>'
                <objectclasstype> MAY (<attribute1> $ <attribute2>))
```

Urejanje objektnega razreda

Vse spremembe v shemi niso dovoljene. Omejitve spreminjanja boste našli v razdelku “Nedovoljene spremembe sheme” na strani 27.

Spletno upravljanje

Če v področju za upravljanje še niste razširili možnosti **Upravljanje shem**, to naredite zdaj, nato pa kliknite **Upravljanje objektnih razredov**. Objektni razred uredite z naslednjim postopkom:

1. Kliknite izbirni gumb poleg objektnega razreda, ki ga želite urediti.
2. Kliknite **Urejanje**.
3. Izberite jeziček:
   - Jeziček **Splošno** izberite, če želite narediti naslednje:
     - Spremeniti **opis**.
     - Spremeniti **nadrejeni objektni razred**, ki ga izberite s spustnega seznama Nadrejeni objektni razred. S tem določite objektni razred, iz katerega bodo podedovani drugi atributi. Običajno je **nadrejeni objektni razred zgornji**, vendar ni nujno. Nadrejeni objektni razred za **tempEmployee** je lahko na primer **ePerson**.
     - Spremeniti **tip objektnega razreda**. Izberite tip objektnega razreda. Dodatne informacije o tipih objektnih razredov boste našli v razdelku “Objektni razredi” na strani 17.
     - Klikniti jeziček Atributi, da spremenite obvezne in neobvezne atribute objektnega razreda in si ogledati podedovane atribute, ali klikniti **Potrdi**, da uveljavite spremembe ali pa klikniti **Prekliči**, da se vrnete v okno **Upravljanje objektnih razredov**, ne da bi opravili kakšno spremembo.
   - Jeziček **Atributi** izberite, če želite narediti naslednje:

     Iz abecednega seznama **Razpoložljivi atributi** izberite atribut in kliknite **Dodaj med obvezne**, da spremenite atribut v obveznega, ali pa kliknite **Dodaj med neobvezne**, da bo atribut za objektni razred neobvezen. Atribut je prikazan na ustreznem seznamu izbranih atributov.

Ta postopek ponovite za vse atribute, ki jih želite izbrati.

Atribut lahko prenesete z enega seznama na drugega ali ga zbrišete z izbranih seznamov, tako da ga izberete in kliknete ustrezen gumb **Prenesi na** ali **Zbriši**.

Seznam obveznih in neobveznih podedovanih atributov si lahko ogledate. Podedovani atributi temeljijo na **nadrejenem objektnem razredu**, ki ste ga izbrali na jezičku **Splošno**. Podedovanih atributov ne morete spremeniti, toda če spremenite **nadrejeni objektni razred** na jezičku **Splošno**, se prikaže drug niz podedovanih atributov.

4. Kliknite **Potrdi**, da uveljavite spremembe ali kliknite **Prekliči**, da se vrnete v okno **Upravljanje objektnih razredov**, ne da bi opravili kakšno spremembo.

Ukazna vrstica

Če si želite ogledati objektne razrede, vsebovane v shemi, izdajte naslednji ukaz:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Za urejanje objektnega razreda z ukazno vrstico, izdajte naslednji ukaz:

```
ldapmodify -D <adminDN> -w <adminPW> -i <ime-datoteke>
```

kjer <*ime-datoteke*>vsebuje:

```
dn: cn=schema
changetype: modify
replace: objectclasses
objectclasses: ( <myobjectClass-oid> NAME
'<mojObjektniRazred>'
DESC '<Objektni razred,
                 definiran za mojo aplikacijo LDAP>' SUP  '< newsuperiorclassobject>'
                 <newobjectclasstype> MAY (attribute1> $ <attribute2>
                  $ <newattribute3>) )
```

Kopiranje objektnega razreda

Spletno upravljanje

Če v področju za upravljanje še niste razširili možnosti **Upravljanje shem**, to naredite zdaj, nato pa kliknite **Upravljanje objektnih razredov**. Objektni razred prekopirate z naslednjim postopkom:

1. Kliknite izbirni gumb poleg objektnega razreda, ki ga želite prekopirati.
2. Kliknite **Prekopiraj**.
3. Izberite jeziček:
   - Jeziček **Splošno** izberite, če želite narediti naslednje:
     - Spremeniti **ime objektnega razreda**. Privzeto ime je ime prekopiranega objektnega razreda, ki mu je dodana besedica COPY, kot je na primer **tempPerson**, ki je prekopiran kot **tempPersonCOPY**.
     - Spremeniti **opis**.
     - Spremeniti **OID**. Privzeti OID je OID prekopiranega objektnega razreda, ki mu je dodana besedica COPY, kot je na primer **tempPerson-oid**, ki je prekopiran kot **tempPerson-oidCOPY**.
     - Spremeniti **nadrejeni objektni razred**, ki ga izberite s spustnega seznama. S tem določite objektni razred, iz katerega bodo podedovani drugi atributi. Običajno je **nadrejeni objektni razred zgornji**, vendar ni nujno. Nadrejeni objektni razred za **tempEmployeeCOPY** je lahko na primer **ePerson**.
     - Spremeniti **tip objektnega razreda**. Izberite tip objektnega razreda. Dodatne informacije o tipih objektnih razredov boste našli v razdelku “Objektni razredi” na strani 17.
     - Kliknite jeziček **Atributi**, da spremenite obvezne in neobvezne atribute za objektni razred in si ogledate podedovane atribute ali kliknite **Potrdi**, da uveljavite spremembe ali pa kliknite **Prekliči**, da se vrnete v okno **Upravljanje objektnih razredov**, ne da bi opravili kakšno spremembo.
   - Jeziček **Atributi** izberite, če želite narediti naslednje:

Iz abecednega seznama **Razpoložljivi atributi** izberite atribut in kliknite **Dodaj med obvezne**, da spremenite atribut v obveznega, ali pa kliknite **Dodaj med neobvezne**, da bo atribut za objektni razred neobvezen. Atribut je prikazan na ustreznem seznamu izbranih atributov.

Ta postopek ponovite za vse atribute, ki jih želite izbrati.

Atribut lahko prenesete z enega seznama na drugega ali ga zbrišete z izbranih seznamov, tako da ga izberete in kliknete ustrezen gumb **Prenesi na** ali **Zbriši**.

Seznam obveznih in neobveznih podedovanih atributov si lahko ogledate. Podedovani atributi temeljijo na **nadrejenem objektnem razredu**, ki ste ga izbrali na jezičku **Splošno**. Podedovanih atributov ne morete spremeniti, toda če spremenite **nadrejeni objektni razred** na jezičku **Splošno**, se prikaže drug niz podedovanih atributov.

4. Kliknite **Potrdi**, da uveljavite spremembe ali kliknite **Prekliči**, da se vrnete v okno **Upravljanje objektnih razredov**, ne da bi opravili kakšno spremembo.

Ukazna vrstica

Če si želite ogledati objektne razrede, vsebovane v shemi, izdajte naslednji ukaz:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Izberite objektni razred, ki ga želite prekopirati. Z urejevalnikom spremenite ustrezne informacije in shranite spremembe v <*ime-datoteke*>. Nato izdajte naslednji ukaz:

```
ldapmodify -D <adminDN> -w <adminPW> -i <ime-datoteke>
```

kjer <*ime-datoteke*>vsebuje:

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( <oid-mojeganovegaObjektnegaRazreda>
NAME '<mojnoviObjektniRazred>'
                DESC '<Nov objektni razred,
                  prekopiran za aplikacijo LDAP>'
               SUP '<nadrejeniObjektniRazred>'<tipObjektnegaRazreda> MAY
(attribute1>
               $ <attribute2> $ <attribute3>) )
```

Brisanje objektnega razreda

Vse spremembe v shemi niso dovoljene. Omejitve spreminjanja boste našli v razdelku “Nedovoljene spremembe sheme” na strani 27.

Spletno upravljanje

Če v področju za upravljanje še niste razširili možnosti **Upravljanje shem**, to naredite zdaj, nato pa kliknite **Upravljanje objektnih razredov**. Objektni razred zbrišete z naslednjim postopkom:

1. Kliknite izbirni gumb poleg objektnega razreda, ki ga želite zbrisati.
2. Kliknite **Zbriši**.
3. Program vas pozove, da potrdite brisanje objektnega razreda. S klikom gumba **Potrdi** objektni razred zbrišete, s klikom gumba **Prekliči** pa se vrnete v okno **Upravljanje objektnih razredov**, ne da bi opravili kakšno spremembo.

Ukazna vrstica

Če si želite ogledati objektne razrede, vsebovane v shemi, izdajte naslednji ukaz:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Izberite objektni razred, ki ga želite zbrisati, in izdajte naslednji ukaz:

```
ldapmodify -D <adminDN> -w <adminPW> -i <ime-datoteke>
```

kjer <*ime-datoteke*>vsebuje:

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: (<oid-mojegaObjektnegaRazreda>)
```

Prikaz atributov

Atribute v shemi si lahko ogledate z orodjem za spletno upravljanje, izbrani način ali z ukazno vrstico.

Spletno upravljanje

V področju za usmerjanje razširite možnost **Upravljanje sheme** in kliknite **Upravljanje atributov**. Prikaže se okno samo za branje, v katerem si lahko ogledate atribute v shemi in njihove značilnosti. Atributi so prikazani v abecednem vrstnem redu. S klikom gumbov Nazaj ali Naprej se lahko premaknete za eno stran nazaj ali naprej. Polje poleg teh gumbov določa stran, na kateri ste. Za skok na določeno stran lahko uporabite tudi spustni meni tega polja. Prvi objektni razred, naveden na stran, je prikazan s številko strani, ki vam pomaga najti objektni razred, ki si ga želite ogledati. Če ste na primer iskali atribut **authenticationUserID**, razširite spustni seznam in se pomaknete, da se prikaže **stran 3 od 62 applSystemHint** in **stran 4 od 62 authorityRevocatonList**. Ker je authenticationUserID po abecednem vrstnem redu med applSystemHint in authorityRevocatonList, izberite stran 3 in kliknite **Pojdi**.

Atribute lahko prikažete tudi razvrščene po skladnji. Izberite **Skladnja** in kliknite **Razvrsti**. Atributi bodo razvrščeni v abecednem vrstnem redu znotraj njihove skladnje. Izpis tipov skladnje boste našli v razdelku “Skladnja atributa” na strani 24. Vrstni red na seznamu lahko obrnete, tako da izberete **Padajoče** in kliknete **Razvrsti**.

Ko najdete želeni atribut, si lahko ogledate njegovo skladnjo, ali vsebuje več vrednosti in objektne razrede, ki jih vsebuje. Razširite spustni meni za objektne razrede in si oglejte seznam objektnih razredov za atribut.

Ko končate, kliknite **Zapri**, da se vrnete v **uvodno** okno strežnika IBM Directory Server.

Ukazna vrstica

Za prikaz atributov, vsebovanih v shemi, izdajte naslednji ukaz:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Dodajanje atributa

Uporabite enega od načinov za izdelavo novega atributa. Priporočeni način je orodje za spletno upravljanje.

Spletno upravljanje

Če v področju za upravljanje še niste razširili možnosti **Upravljanje shem**, to naredite zdaj, nato pa kliknite **Upravljanje atributov**. Nov atribut izdelate takole:

1. Kliknite **Dodaj**.

   Opomba: Do tega okna lahko dostopite tudi tako, da v področju za upravljanje razširite možnost **Upravljanje shem** in kliknete **Dodaj atribut**.
2. Vnesite **ime atributa**, kot je na primer **tempId**. To polje je obvezno in se mora začeti z abecednim znakom.
3. Vnesite **opis** atributa, kot je na primer **Identifikacijska številka, dodeljena začasnemu uslužbencu**.
4. Vnesite **OID** za atribut. To polje je obvezno. Glejte “Identifikator objekta (OID)” na strani 25. Če OID-ja nimate, lahko uporabite ime atributa, ki mu dodate -oid, kot na primer v primeru, če je ime atributa **tempID**, ko bo privzeti OID **tempID-oid**. Vrednost tega polja lahko spremenite.
5. S spustnega seznama izberite **nadrejeni atribut**. Le-ta določa atribut, iz katerega so podedovane lastnosti.

6. S spustnega seznama izberite **skladnjo**. Dodatne informacije o skladnji boste našli v razdelku “Skladnja atributa” na strani 24.
7. Vnesite **dolžino atributa**, ki podaja največjo dolžino tega atributa. Dolžina je izražena s številom bajtov.
8. Če želite omogočiti, da bo atribut vseboval več vrednosti, izberite potrditveno polje **Omogoči več vrednosti**.
9. Z vsakega spustnega menija izberite pravilo primerjanja za enakost, ureditev in podniz. Celoten seznam pravil primerjanja boste našli v razdelku “Pravila za primerjanje” na strani 22.
10. Kliknite jeziček **IBM-ove pripone** in podajte dodatne pripone za atribut ali kliknite **Potrdi**, da dodate nov atribut ali pa kliknite **Prekliči**, da se vrnete v okno **Upravljanje atributov**, ne da bi opravili kakšno spremembo.
11. Na jezičku **IBM-ove pripone** naredite naslednje:
    - Spremenite ime tabele **DB2**. Če pustite to polje prazno, ustvari ime tabele DB2 strežnik. Če vnesete ime tabele DB2, morate vnesti tudi ime stolpca DB2.
    - Spremenite ime stolpca **DB2**. Če pustite to polje prazno, ustvari ime stolpca strežnik DB2. Če vnesete ime stolpca DB2, morate vnesti tudi ime tabele DB2.
    - Nastavite **razred zaščite**, tako da s spustnega seznama izberete **normalna**, **občutljiva** ali **kritična**.
    - Z izbiro enega ali več pravil za indeksiranje nastavite **pravila za indeksiranje**. Dodatne informacije o pravilih za indeksiranje boste našli v razdelku “Pravila indeksiranja” na strani 24.

      Opomba: Priporočamo, da podate v atributih, ki bodo uporabljeni v iskalnih filtrih, vsaj indeksiranje po enakosti.
12. S klikom gumba **Potrdi** dodajte nov atribut, s klikom gumba **Prekliči** pa se vrnite v okno **Upravljanje atributov**, ne da bi opravili kakšno spremembo.

Opomba: Če ste na jezičku Splošno kliknili Potrdi, ne da bi dodali kakšno pripono, lahko le-te dodate z ureditvijo novega atributa.

Ukazna vrstica

V naslednjem primeru bomo dodali definicijo tipa za atribut, imenovan ″myAttribute″, s skladnjo imeniškega niza (glejte “Skladnja atributa” na strani 24) in primerjavo enakosti brez upoštevanja velikih in malih črk (glejte “Pravila za primerjanje” na strani 22). IBM-ov specifičen del definicije pravi, da so podatki atributa shranjeni v stolpcu ″myAttrColumn″ tabele ″myAttrTable″. Če teh imen niste podali, bo za ime stolpca in tabele po privzetku uporabljeno ime ″myAttribute″. Atribut je dodeljen ″normalnemu″ dostopnemu razredu, vrednosti pa imajo največjo dovoljeno dolžino 200 bajtov.

```
ldapmodify -D <admindn> -w <adminpw> -i myschema.ldif
```

kjer datoteka **myschema.ldif** vsebuje naslednje:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' )
                 DESC 'Atribut, definiran za aplikacijo LDAP'
                 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 )
```

Dodatne informacije o tem ukazu boste našli v razdelku “ldapmodify in ldapadd” na strani 157.

Urejanje atributa

Vse spremembe v shemi niso dovoljene. Omejitve spreminjanja boste našli v razdelku “Nedovoljene spremembe sheme” na strani 27.

Preden dodate vnose, ki uporabljajo atribut, lahko spremenite katerikoli del definicije. Za urejanje atributa uporabite enega od naslednjih načinov. Priporočeni način je orodje za spletno upravljanje.

Spletno upravljanje

Če v področju za upravljanje še niste razširili možnosti **Upravljanje shem**, to naredite zdaj, nato pa kliknite **Upravljanje atributov**. Atribut lahko uredite z naslednjim postopkom:

1. Kliknite izbirni gumb poleg atributa, ki ga želite urediti.
2. Kliknite **Urejanje**.
3. Izberite jeziček:
   - Jeziček **Splošno** izberite, če želite narediti naslednje:
     – Izberite jeziček, in sicer
       - **Splošno**, da naredite naslednje:
         - spremenite **opis**
         - spremenite **skladnjo**
         - nastavite **dolžino atributa**
         - spremenite nastavitve za **več vrednosti**
         - izberete **pravilo primerjanja**
         - spremenite **nadrejeni atribut**.
       - Kliknite jeziček **IBM-ove pripone**, da uredite pripone za atribut ali kliknite **Potrdi**, da uveljavite spremembe ali pa kliknite **Prekliči**, da se vrnete v okno **Upravljanje atributov**, ne da bi opravili kakšno spremembo.
       - **IBM-ove pripone**, če uporabljate strežnik IBM, da naredite naslednje:
         - spremenite **razred zaščite**
         - spremenite **pravilo indeksiranja**.
     – Kliknite **Potrdi**, da uveljavite spremembe ali pa **Prekliči**, da se vrnete v okno **Upravljanje atributov**, ne da bi opravili kakšno spremembo.
4. Kliknite **Potrdi**, da uveljavite spremembe ali pa **Prekliči**, da se vrnete v okno **Upravljanje atributov**, ne da bi opravili kakšno spremembo.

Ukazna vrstica

V tem zgledu bomo atributu dodali indeksiranje, tako da bo njegovo iskanje potekalo hitreje. Za spremembo definicije uporabite ukaz ldapmodify in datoteko LDIF:

```
ldapmodify -D <admindn> -w <adminpw> -i myschemachange.ldif
```

kjer datoteka **myschemachange.ldif** vsebuje naslednje:

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' ) DESC 'Atribut,
                 definiran za mojo aplikacijo LDAP' 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 )
```

Opomba: V operacijo zamenjave morate vključiti oba dela definicije (**attributetypes** in **ibmattributetypes**), čeprav boste spremenili samo razdelek **ibmattributetypes**. Edina sprememba je dodajanje niza ″EQUALITY SUBSTR″ na konec definicije za zahtevanje indeksov za primerjavo enakosti in podniza.

Dodatne informacije o tem ukazu boste našli v razdelku “ldapmodify in ldapadd” na strani 157.

Kopiranje atributa

Za kopiranje atributa uporabite enega od naslednjih načinov. Priporočeni način je orodje za spletno upravljanje.

Spletno upravljanje

Če v področju za upravljanje še niste razširili možnosti **Upravljanje shem**, to naredite zdaj, nato pa kliknite **Upravljanje atributov**. Atribut prekopirate takole:

1. Kliknite izbirni gumb poleg atributa, ki ga želite prekopirati.
2. Kliknite **Prekopiraj**.
3. Spremenite **ime atributa**. Privzeto ime je prekopirano ime atributa, ki mu je dodana besedica COPY, kot je na primer **tempID**, ki je prekopiran kot **tempIDCOPY**.
4. Spremenite **opis** atributa, kot je na primer **Identifikacijska številka, dodeljena začasnemu uslužbencu**.
5. Spremeniti **OID**. Privzeti OID je OID prekopiranega atributa, ki mu je dodana besedica COPYOID, kot je na primer **tempID-oid**, ki je prekopiran kot **tempID-oidCOPYOID**.
6. S spustnega seznama izberite **nadrejeni atribut**. Le-ta določa atribut, iz katerega so podedovane lastnosti.
7. S spustnega seznama izberite **skladnjo**. Dodatne informacije o skladnji boste našli v razdelku “Skladnja atributa” na strani 24.
8. Vnesite **dolžino atributa**, ki podaja največjo dolžino tega atributa. Dolžina je izražena s številom bajtov.
9. Če želite omogočiti, da bo atribut vseboval več vrednosti, izberite potrditveno polje **Omogoči več vrednosti**.
10. Z vsakega spustnega menija izberite pravilo primerjanja za enakost, ureditev in podniz. Celoten seznam pravil primerjanja boste našli v razdelku “Pravila za primerjanje” na strani 22.
11. Kliknite jeziček **IBM-ove pripone**, da spremenite dodatne pripone za atribut ali kliknite **Potrdi**, da uveljavite spremembe ali pa kliknite **Prekliči**, da se vrnete v okno **Upravljanje atributov**, ne da bi opravili kakšno spremembo.
12. Na jezičku **IBM-ove pripone** naredite naslednje:
    - Spremenite ime tabele **DB2**. Če pustite to polje prazno, ustvari ime tabele DB2 strežnik. Če vnesete ime tabele DB2, morate vnesti tudi ime stolpca DB2.
    - Spremenite ime stolpca **DB2**. Če pustite to polje prazno, ustvari ime stolpca strežnik DB2. Če vnesete ime stolpca DB2, morate vnesti tudi ime tabele DB2.
    - Spremenite **razred zaščite**, tako da s spustnega seznama izberete **normalna**, **občutljiva** ali **kritična**.
    - Z izbiro enega ali več pravil za indeksiranje nastavite **pravila za indeksiranje**. Dodatne informacije o pravilih za indeksiranje boste našli v razdelku “Pravila indeksiranja” na strani 24.

      Opomba: Priporočamo, da podate v atributih, ki bodo uporabljeni v iskalnih filtrih, vsaj indeksiranje po enakosti.
13. Kliknite **Potrdi**, da uveljavite spremembe ali pa **Prekliči**, da se vrnete v okno **Upravljanje atributov**, ne da bi opravili kakšno spremembo.

Opomba: Če ste na jezičku **Splošno** kliknili **Potrdi**, ne da bi dodali kakšno pripono, lahko le-te dodate ali spremenite tako, da uredite novi atribut.

Ukazna vrstica

Če si želite ogledati atribute, vsebovane v shemi, izdajte naslednji ukaz:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Izberite atribut, ki ga želite prekopirati. Z urejevalnikom spremenite ustrezne informacije in shranite spremembe v <*ime-datoteke*>. Nato izdajte naslednji ukaz:

```
ldapmodify -D <adminDN> -w <adminPW> -i <ime-datoteke>
```

kjer <*ime-datoteke*>vsebuje:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( <oid-mojegaNovegaAtributa> NAME
'<mojNoviAtribut>' DESC '<Novi
                atribut, prekopiran za aplikacijo LDAP> 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

Vse spremembe v shemi niso dovoljene. Omejitve spreminjanja boste našli v razdelku “Nedovoljene spremembe sheme” na strani 27.

Za brisanje atributa uporabite enega od naslednjih načinov. Priporočeni način je orodje za spletno upravljanje.

Spletno upravljanje

Če v področju za upravljanje še niste razširili možnosti **Upravljanje shem**, to naredite zdaj, nato pa kliknite **Upravljanje atributov**. Atribut zbrišete z naslednjim postopkom:

1. Kliknite izbirni gumb poleg atributa, ki ga želite zbrisati.
2. Kliknite **Zbriši**.
3. Program vas pozove, da potrdite brisanje atributa. S klikom gumba **Potrdi** atribut zbrišete, s klikom gumba **Prekliči** pa se vrnete v okno **Upravljanje atributov**, ne da bi opravili kakšno spremembo.

Ukazna vrstica

```
ldapmodify -D <admindn> -w <adminpw> -i myschemadelete.ldif
```

kjer datoteka **myschemadelete.ldif** vključuje naslednje:

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

Dodatne informacije o tem ukazu boste našli v razdelku “ldapmodify in ldapadd” na strani 157.

Kopiranje sheme v druge strežnike

Shemo prekopirate v druge strežnike z naslednjim postopkom:

1. S pripomočkom ldapsearch prekopirajte shemo v datoteko:

   ```
   ldapsearch -b cn=schema -L "(objectclass=*)" > schema.ldif
   ```

2. Datoteka sheme bo vsebovala vse objektne razrede in atribute. Uredite datoteko LIDF, tako da bo vključevala samo želene elemente sheme, z uporabo orodja, kot je grep, pa lahko tudi prefiltrirate izhodne podatke pripomočka ldapsearch. Atributi morajo biti pred objektnimi razredi, ki se sklicujejo na njih. Končna datoteka je lahko na primer takšna (ne spreglejte, da ima vsaka nadaljujoča se vrstica na koncu presledek, nadaljevalna vrstica pa vsaj en presledek na začetku vrstice).

   ```
   attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Del
     informacij.' 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 'Del
     informacij.' 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
  nekaj.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

3. Pred vsako vrstico objectclasses ali attributetype vstavite vrstice, da izdelate smernice LDIF za dodajanje teh vrednosti v vnos cn=schema. Vsak objektni razred in atribut morate dodati kot posamezen popravek.

```
dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Del
  informacij.' 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 'Del
  informacij.' 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
  nekaj.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

4. To shemo naložite v druge strežnike s pripomočkom ldapmodify:

```
ldapmodify -D cn=administrator -w <password> -f schema.ldif
```

Upravljanje imeniških vnosov

Za upravljanje imeniških vnosov v področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Upravljanje imenika**.

Dodatne informacije boste našli v naslednjih temah:

Pregled drevesa

Če v področju za usmerjanje še niste razširili kategorije **Upravljanje imenika**, to naredite zdaj, nato pa kliknite izbiro **Upravljanje vnosov**. Razširite lahko različna poddrevesa in izberete vnos, s katerim želite delati. Operacijo, ki jo želite izvesti, lahko izberete iz orodjarne na desni strani.

Dodajanje vnosa

Če v področju za usmerjanje še niste razširili kategorije **Upravljanje imenika**, to naredite zdaj.

1. Kliknite **Dodaj vnos**.
2. S spustnega seznama izberite **strukturalni objektni razred**.
3. Kliknite **Naprej**.
4. V okencu Razpoložljivo izberite katerikoli **pomožni objektni razred** in kliknite **Dodaj**. Ta postopek ponovite za vsak pomožni objektni razred, ki ga želite dodati. Pomožni objektni razred lahko tudi zbrišete iz okenca Izbrano, tako da ga izberete in kliknete **Odstrani**.
5. Kliknite **Naprej**.
6. V polje **Relativni DN** vnesite relativno razločevalno ime (RDN) vnosa, ki ga dodajate, kot je na primer cn=John Doe.
7. V polje **Nadrejeni DN** vnesite razločevalno ime izbranega imeniškega vnosa, kot je na primer ou=Austin, o=IBM. Za izbiro nadrejenega DN-ja s seznama lahko tudi kliknete **Preglej**. Za prikaz drugih izbir nižje v poddrevesu lahko razširite izbiro. Podajte izbiro in kliknite **Izberi**, da podate želeni nadrejeni DN. Za **nadrejeni DN** je po privzetku uporabljen vnos, izbran v drevesu.

   Opomba: Če ste začeli izvajanje te naloge v oknu **Upravljanje vnosov**, bo to polje vnaprej izpolnjeno. **Nadrejeni** vnos ste izbrali, preden ste kliknili **Dodaj** za začetek dodajanja vnosa.
8. Na jezičku **Obvezni atributi** vnesite vrednosti za obvezne atribute. Če želite dodati za določen atribut več vrednosti, kliknite **Več vrednosti** in nato dodajte posamezne vrednosti.
9. Kliknite **Izbirni atributi**.
10. Na jezičku **Izbirni atributi** vnesite vrednosti, ki so ustrezne za neobvezne atribute. Informacije o dodajanju dvojiških vrednosti boste našli v razdelku “Spreminjanje dvojiških atributov” na strani 134. Če želite dodati za določen atribut več vrednosti, kliknite **Več vrednosti** in nato dodajte posamezne vrednosti.
11. Za izdelavo vnosa kliknite Potrdi.
12. Če želite za ta vnos spremeniti seznam za nadzor dostopa, kliknite **ACL**. Informacije o ACL-jih boste našli v razdelku “Seznami za nadzor dostopa” na strani 47.
13. Ko izpolnite vsaj obvezna polja, kliknite **Dodaj**, da dodate nov vnos, ali pa **Prekliči**, da se vrnete v okno **Pregledovanje drevesa**, ne da bi opravili kakšno spremembo v imeniku.

Brisanje vnosa

Če v področju za usmerjanje še niste razširili kategorije **Upravljanje imenika**, to naredite zdaj, nato pa kliknite izbiro **Upravljanje vnosov**. Razširite lahko različna poddrevesa in izberete poddrevo, pripono ali vnos, s katerim želite delati. Iz orodjarne na desni strani izberite **Zbriši**.

- Brisanje morate potrditi. Kliknite **Potrdi**.
- Vnos je zbrisan, vi pa se vrnete na seznam vnosov.

Urejanje vnosa

Če v področju za usmerjanje še niste razširili kategorije **Upravljanje imenika**, to naredite zdaj, nato pa kliknite izbiro **Upravljanje vnosov**. Razširite lahko različna poddrevesa in izberete vnos, s katerim želite delati. V orodjarni na desni strani izberite **Urejanje atributov**.

1. Na jezičku **Obvezni atributi** vnesite vrednosti za obvezne atribute. Informacije o dodajanju dvojiških vrednosti boste našli v razdelku “Spreminjanje dvojiških atributov” na strani 134. Če želite dodati za določen atribut več vrednosti, kliknite **Več vrednosti** in nato dodajte posamezne vrednosti.
2. Kliknite **Izbirni atributi**.
3. Na jezičku **Izbirni atributi** vnesite vrednosti, ki so ustrezne za neobvezne atribute. Če želite dodati za določen atribut več vrednosti, kliknite **Več vrednosti** in nato dodajte posamezne vrednosti.
4. Kliknite **Članstva**.
5. Če ste izdelali kakšno skupino, naredite na jezičku **Članstva** naslednje:

- Na seznamu **Razpoložljive skupine** izberite skupino in kliknite **Dodaj**, da bo vnos postal član izbranega **članstva v statični skupini**.
- Na seznamu **Članstva v statični skupini** izberite skupino in s klikom gumba **Odstrani** odstranite vnos iz izbrane skupine.

6. Če gre za vnos skupine, je na voljo jeziček **Člani**. Na jezičku **Člani** so prikazani člani izbrane skupine. Člane lahko dodate v skupino ali jih odstranite.
   - Člana dodate v skupino z naslednjim postopkom:
     a. Z jezičkom **Člani** kliknite **Več vrednosti** ali pa na jezičku **Člani** kliknite **Člani**.
     b. V polje Član vnesite DN vnosa, ki ga želite dodati.
     c. Kliknite **Dodaj**.
     d. Kliknite **Potrdi**.
   - Član odstranite iz skupine z naslednjim postopkom:
     a. Z jezičkom **Člani** kliknite **Več vrednosti** ali pa na jezičku **Člani** kliknite **Člani**.
     b. Izberite vnos, ki ga želite odstraniti.
     c. Kliknite **Odstrani**.
     d. Kliknite **Potrdi**.
   - Za osvežitev seznama članov kliknite **Ažuriraj**.
7. Za spremembo vnosa kliknite **Potrdi**.

Kopiranje vnosa

Ta funkcija je uporabna, če izdelujete podobne vnose, saj kopija prevzame vse atributa izvirnika. Spremeniti morate samo ime novega vnosa.

Če v področju za usmerjanje še niste razširili kategorije **Upravljanje imenika**, to naredite zdaj, nato pa kliknite izbiro **Upravljanje vnosov**. Razširite lahko različna poddrevesa in izberete vnos, kot je na primer John Doe, s katerim želite delati. Iz orodjarne na desni strani izberite **Prekopiraj**.

- Spremenite vnos RDN v polju DN. cn=John Doe na primer spremenite v cn=Jim Smith.
- Na jezičku Obvezni atributi spremenite vnos cn v nov RDN. V tem primeru je to Jim Smith.
- Spremenite tudi druge obvezne atribute. V tem primeru spremenite atribut sn iz Doe v Smith.
- Ko opravite potrebne spremembe, kliknite **Potrdi**, da izdelate nov vnos.
- Nov vnos Jim Smith je dodan na dno seznama vnosov.

Opomba: Ta postopek prekopira samo atribute vnosa. Članstva v skupini izvirnega vnosa niso prekopirana v nov vnos. Za dodajanje članstva uporabite funkcijo Urejanje atributov.

Urejanje seznamov za nadzor dostopa

Za prikaz lastnosti ACL-jev z orodjem za spletno upravljanje in za delo z ACL-ji preglejte razdelek “Upravljanje seznamov za nadzor dostopa (ACL-jev)” na strani 145.

Dodatne informacije boste našli v razdelku “Seznami za nadzor dostopa” na strani 47.

Dodajanje pomožnega objektnega razreda

Z gumbom orodjarne **Dodaj pomožne razrede** dodajte obstoječemu vnosu imeniškega drevesa pomožni objektni razred. Pomožni objektni razred podaja dodatne atribute za vnos, ki mu je dodan.

Če v področju za usmerjanje še niste razširili kategorije **Upravljanje imenika**, to naredite zdaj, nato pa kliknite izbiro **Upravljanje vnosov**. Razširite lahko različna poddrevesa in izberete vnos, kot je na primer John Doe, s katerim želite delati. V orodjarni na desni strani izberite **Dodaj pomožni razred**.

1. V okencu Razpoložljivo izberite katerikoli **pomožni objektni razred** in kliknite **Dodaj**. Ta postopek ponovite za vsak pomožni objektni razred, ki ga želite dodati. Pomožni objektni razred lahko tudi zbrišete iz okenca Izbrano, tako da ga izberete in kliknete **Odstrani**.
2. Na jezičku **Obvezni atributi** vnesite vrednosti za obvezne atribute. Če želite dodati za določen atribut več vrednosti, kliknite **Več vrednosti** in nato dodajte posamezne vrednosti.
3. Kliknite **Izbirni atributi**.
4. Na jezičku **Izbirni atributi** vnesite vrednosti, ki so ustrezne za neobvezne atribute. Če želite dodati za določen atribut več vrednosti, kliknite **Več vrednosti** in nato dodajte posamezne vrednosti.
5. Kliknite **Članstva**.
6. Če ste izdelali kakšno skupino, naredite na jezičku **Članstva** naslednje:
   - Na seznamu **Razpoložljive skupine** izberite skupino in kliknite **Dodaj**, da bo vnos postal član izbranega **članstva v statični skupini**.
   - Na seznamu **Članstva v statični skupini** izberite skupino in s klikom gumba **Odstrani** odstranite vnos iz izbrane skupine.
7. Za spremembo vnosa kliknite **Potrdi**.

Brisanje pomožnega razreda

Čeprav lahko pomožni razred zbrišete med postopkom dodajanja pomožnega razreda, je uporaba funkcije za brisanje pomožnega razreda preprostejša, če boste iz vnosa zbrisali samo en pomožni razred. Če boste iz vnosa zbrisali več pomožnih razredov, pa bo uporaba postopka za dodajanje pomožnega razreda najbrž bolj priročna.

1. Če v področju za usmerjanje še niste razširili kategorije **Upravljanje imenika**, to naredite zdaj, nato pa kliknite izbiro **Upravljanje vnosov**. Razširite lahko različna poddrevesa in izberete vnos, kot je na primer John Doe, s katerim želite delati. V orodjarni na desni strani izberite **Zbriši pomožni razred**.
2. Na seznamu pomožnih razredov izberite tistega, ki ga želite zbrisati, nato pa kliknite **Potrdi**.
3. Program zahteva, da brisanje potrdite, zato kliknite **Potrdi**.
4. Pomožni razred je zbrisan iz vnosa, vi pa se vrnete na seznam vnosov.

Te korake ponovite za vse pomožne razrede, ki jih želite zbrisati.

Spreminjanje članstva v skupini

Če v področju za usmerjanje še niste razširili kategorije **Upravljanje imenika**, to naredite zdaj.

1. Kliknite **Upravljanje vnosov**.
2. Iz imeniškega drevesa izberite uporabnika, nato pa v orodjarni kliknite ikono **Urejanje atributov**.
3. Kliknite jeziček **Članstva**.
4. Spremenite članstva za uporabnika. V oknu **Spreminjanje članstev** so prikazane **razpoložljive skupine**, v katere lahko dodate uporabnika, kot tudi **članstva v statični skupini** za vnos.
   - Na seznamu **Razpoložljive skupine** izberite skupino in kliknite **Dodaj**, da bo vnos postal član izbrane skupine.
   - Na seznamu **Članstva v statični skupini** izberite skupino in s klikom gumba **Odstrani** odstranite vnos iz izbrane skupine.
5. S klikom gumba **Potrdi** shranite spremembe, s klikom gumba **Prekliči** pa se vrnete v prejšnje okno, ne da bi shranili spremembe.

Iskanje imeniških vnosov

Za pregled imeniškega drevesa obstajajo tri možnosti:

- preprosto iskanje z vnaprej definiranim nizom iskalnih kriterijev
- zahtevnejše iskanje z uporabniško definiranim nizom iskalnih kriterijev
- ročno iskanje

Do teh iskalnih možnosti dostopite tako, da v področju za usmerjanje razširite kategorijo **Upravljanje imenika** in kliknete **Iskanje vnosov**. Izberite jeziček **Iskalni filtri** ali **Možnosti**.

Opomba: Dvojiških vnosov, kot so na primer gesla, ni mogoče iskati.

Iskalni filtri

Izberite eno od naslednjih vrst iskanja:

Preprosto iskanje

Privzeto iskanje uporablja privzeti iskalni kriterij:

- Osnovni DN je **Vse pripone**
- Iskalno območje je **Poddrevo**
- Velikost iskanja je **Neomejena**
- Časovna omejitev je **Neomejeno**
- Odstranitev krmilnih podatkov za vzdevek je **Nikoli**
- Možnost iskanja referenčnih kazalcev ni izbrana (je izključena)

Preprosto iskanje izvedete takole:

1. Na jezičku **Iskalni filter** kliknite **Preprosto iskanje**.
2. S spustnega seznama izberite objektne razrede.
3. Izberite določen atribut za izbran tip vnosa. Če izberete iskanje po določenem atributu, le-tega izberite s spustnega seznama in vnesite vrednost atributa v polje **Enak kot**. Če atributa ne podate, vrne iskanje vse imeniške vnose izbranega tipa vnosa.

Zahtevnejše iskanje

Zahtevnejše iskanje omogoča, da podate iskalne omejitve in omogočite iskalne filtre. Preprosto iskanje izberite, če želite uporabiti privzeti iskalni kriterij.

- Zahtevnejše iskanje izvedete takole:
  1. Na jezičku **Iskalni filter** kliknite **Zahtevnejše iskanje**.
  2. S spustnega seznama izberite **Atribut**.
  3. Izberite **primerjalni** operator.
     - = Atribut je enak vrednosti.
     - ! Atribut ni enak vrednosti.
     - < Atribut je manjši ali enak kot vrednost.
     - > Atribut je večji ali enak kot vrednost.
     - ~ Atribut je približno enak kot vrednost.
  4. Vnesite **vrednost** za primerjavo.
  5. Za kompleksne poizvedbe uporabite gumbe iskalnih operatorjev.
     - Če ste že dodali vsaj en iskalni filter, podajte dodatni kriterij in kliknite **AND**. Ukaz **AND** vrne vnose, ki ustrezajo obema nizoma iskalnih kriterijev.
     - Če ste že dodali vsaj en iskalni filter, podajte dodatni kriterij in kliknite **OR**. Ukaz **OR** vrne vnose, ki ustrezajo enemu ali drugemu nizu iskalnih kriterijev.
  6.
     - Kliknite **Dodaj**, da odstranite kriterij iskalnega filtra v zahtevnejše iskanje.
     - Kliknite **Zbriši**, da odstranite kriterij iskalnega filtra iz zahtevnejšega iskanja.
     - S klikom gumba **Nastavi na novo** počistite vse iskalne filtre.

Ročno iskanje

Ta način uporabite, če želite izdelati iskalni filter. Če želite na primer izvesti iskanje po priimkih, vnesite v polje vrednost sn=*. Če izvajate iskanje po več atributih, morate uporabiti skladnjo iskalnega filtra. Če želite na primer izvesti iskanje priimkov v določenem oddelku, vnesite naslednje:

```
(&(sn=*)(dept=<departmentname>))
```

Možnosti

Na jezičku **Možnosti** naredite naslednje:

- **Poišči osnovni DN** - s spustnega seznama izberite pripono, če želite izvesti iskanje samo znotraj te pripone.

  Opomba: Če ste začeli izvajanje te naloge v oknu **Upravljanje vnosov**, bo to polje vnaprej izpolnjeno. **Nadrejeni** vnos ste izbrali, preden ste kliknili **Dodaj** za začetek dodajanja vnosa.

  Če želite preiskati celotno drevo, lahko izberete možnost **Vse pripone**.
- **Območje iskanja**
  - Če želite izvesti iskanje samo znotraj izbranega objekta, izberite **Objekt**.
  - Če želite izvesti iskanje samo znotraj takojšnjega podrejenega objekta izbranega objekta, izberite **Ena raven**.
  - Če želite preiskati vse naslednike izbranega vnosa, izberite **Poddrevo**.
- **Omejitev velikosti iskanja** - vnesite največje število vnosov za iskanje ali pa izberite možnost **Neomejeno**.
- **Časovna omejitev iskanja** - vnesite največje število sekund za izvajanje iskanja ali pa izberite možnost **Neomejeno**.
- S spustnega seznama izberite vrsto **odstranitve krmilnih podatkov za vzdevek**.
  - **Nikoli** - če je izbrani vnos vzdevek, v iskanju krmilni elementi zanj ne bodo odstranjeni, kar pomeni, da bo iskanje zanemarilo reference na vzdevek.
  - **Iskanje** - če je izbrani vnos vzdevek, bodo v iskanju odstranjeni krmilni elementi zanj, iskanje pa se izvede od mesta vzdevka.
  - **Pregledovanje** - krmilni elementi za izbrani vnos niso odstranjeni, odstranjeni pa so krmilni elementi za vse najdene vnose v pregledovanju.
  - **Vedno** - krmilni elementi za vse vzdevke, najdene v iskanju, bodo odstranjeni.
- Izberite potrditveno polje **Sledi referenčnim kazalcem**, če želite slediti referenčnim kazalcem na drug strežnik, če je referenčni kazalec vrnjen v iskanju. Če referenčni strežnik usmeri iskanje na drug strežnik, povezava s strežnikom uporabi trenutne poverilnice. Če ste prijavljeni kot anonimni uporabnik, se boste morda morali prijaviti v strežnik z overjenim DN-jem.

Dodatne informacije o iskanjih boste našli v razdelku “Prilagoditev iskalnih nastavitev” na strani 100.

Spreminjanje dvojiških atributov

Če zahteva atribut dvojiške podatke, je poleg polja atributa prikazan gumb **Dvojiški podatki**. Če atribut nima podatkov, je polje prazno. Ker dvojiških atributov ni mogoče prikazati, je v polju v primeru, da atribut vsebuje dvojiške podatke, prikazana vrednost **Dvojiški podatki - 1**. Če vsebuje atribut več vrednosti, je polje prikazano kot spustni seznam.

Za delo z dvojiškimi atributi kliknite gumb **Dvojiški podati**.

Dvojiške podatke lahko uvozite, izvozite ali zbrišete.

Dvojiške podatke dodate atributu z naslednjim postopkom:

1. Kliknite gumb **Dvojiški podatki**.
2. Kliknite **Uvozi**.
3. Pot do želene datoteke lahko vnesete ali pa kliknete gumb **Preglej**, da dvojiško datoteko poiščete in izberete.
4. Kliknite **Predloži datoteko**. Prikaže se sporočilo Datoteka je odložena na oddaljeni računalnik.
5. Kliknite **Zapri**. Pod možnostjo **Vnosi dvojiških podatkov** se zdaj prikaže izbira **Dvojiški podatki - 1**.

6. Postopek uvažanja ponovite za vse dvojiške datoteke, ki jih želite dodati. Nadaljnji vnosi so navedeni kot **Dvojiški podatki - 2**, **Dvojiški podatki -3** itd.
7. Ko končate z dodajanjem dvojiških podatkov, kliknite **Potrdi**.

Dvojiške podatke izvozite takole:
1. Kliknite gumb **Dvojiški podatki**.
2. Kliknite **Izvozi**.
3. Kliknite povezavo **Dvojiški podatki za snemanje iz oddaljenega računalnika**.
4. Sledite navodilom čarovnika za prikaz dvojiške datoteke ali za njeno shranitev na novo mesto.
5. Kliknite **Zapri**.
6. Postopek uvažanja ponovite za vse dvojiške datoteke, ki jih želite izvoziti.
7. Ko končate z izvažanjem podatkov, kliknite **Potrdi**.

Dvojiške podatke zbrišete takole:
1. Kliknite gumb **Dvojiški podatki**.
2. Kliknite datoteko dvojiških podatkov, ki jo želite zbrisati. Izberete lahko več datotek.
3. Kliknite **Zbriši**.
4. Ko vas program pozove na potrditev brisanja, kliknite **Potrdi**. Dvojiški podatki, označeni za brisanje, so odstranjeni s seznama.
5. Ko končate z brisanjem podatkov, kliknite **Potrdi**.

Opomba: Iskanja v dvojiških atributih ni mogoče izvajati.

Upravljanje uporabnikov in skupin

Za upravljanje uporabnikov in skupin razširite v področju za usmerjanje orodja za spletno upravljanje kategorijo **Uporabniki in skupine**.

Dodatne informacije boste našli v naslednjih temah:
- “Upravljanje uporabnikov”
- “Upravljanje skupin” na strani 136

Upravljanje uporabnikov

Ko nastavite področja in predloge, jih lahko poselite z uporabniki. Preglejte naslednje teme:
- “Dodajanje uporabnikov”
- “Iskanje uporabnikov v področju” na strani 136
- “Urejanje uporabniških informacij” na strani 136
- “Kopiranje uporabnika” na strani 136
- “Odstranitev uporabnika” na strani 136

Dodajanje uporabnikov

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Uporabniki in skupine**.
1. Kliknite **Dodaj uporabnika** ali **Upravljanje uporabnikov**, nato pa **Dodaj**.
2. S spustnega seznama izberite področje, v katero želite dodati uporabnika.
3. Kliknite **Naprej**. Prikaže se predloga, ki je povezana s tem področjem. Izpolnite obvezna polja, označena z zvezdico (*), in vsa druga polja na jezičkih. Če ste v področju že izdelali skupine, lahko v eno ali več skupin dodate uporabnika.
4. Ko končate, kliknite **Dokončaj**.

Iskanje uporabnikov v področju

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Uporabniki in skupine**.

1. Kliknite **Najdi uporabnika** ali **Upravljanje uporabnikov**, nato pa **Poišči**.
2. V polju **Izbira področja** izberite področje, ki ga želite preiskati.
3. V polje **Atribut poimenovanja** vnesite iskalni niz. Univerzalni znaki so podprti; če vpišete ***smoje**, se prikažejo vsi vnosi z atributom poimenovanja, ki se konča s smoje.
4. Za izbranega uporabnika lahko izvedete naslednje operacije:
   - **Urejanje** - glejte “Urejanje uporabniških informacij”.
   - **Kopiranje** - glejte “Kopiranje uporabnika”.
   - **Brisanje** - glejte “Odstranitev uporabnika”.
5. Ko končate, kliknite **Potrdi**.

Urejanje uporabniških informacij

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Uporabniki in skupine**.

1. Kliknite **Upravljanje uporabnikov**.
2. S spustnega menija izberite področje. Če uporabniki niso prikazani v okencu **Uporabniki**, kliknite **Prikaži uporabnike**.
3. Izberite uporabnike, ki ga želite urejati, in kliknite **Urejanje**.
4. Spremenite informacije na jezičkih in članstvo v skupini.
5. Ko končate, kliknite **Potrdi**.

Kopiranje uporabnika

Če morate izdelati več uporabnikov, katerih informacije so v glavnem identične, to lahko naredite tako, da prekopirate začetnega uporabnika in spremenite informacije.

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Uporabniki in skupine**.

1. Kliknite **Upravljanje uporabnikov**.
2. S spustnega menija izberite področje. Če uporabniki niso prikazani v okencu **Uporabniki**, kliknite **Prikaži uporabnike**.
3. Izberite uporabnika, ki ga želite prekopirati, in kliknite **Prekopiraj**.
4. Spremenite ustrezne informacije za novega uporabnika, kot so na primer obvezne informacije, ki specifičnega uporabnika določajo, kot je na primer sn ali cn. Informacij, ki so skupne obema uporabnikoma, ni potrebno spremeniti.
5. Ko končate, kliknite **Potrdi**.

Odstranitev uporabnika

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Uporabniki in skupine**.

1. Kliknite **Upravljanje uporabnikov**.
2. S spustnega menija izberite področje. Če uporabniki niso prikazani v okencu **Uporabniki**, kliknite **Prikaži uporabnike**.
3. Izberite uporabnika, ki ga želite odstraniti, in kliknite **Zbriši**.
4. Ko vas program pozove na potrditev brisanja, kliknite **Potrdi**.
5. Uporabnik je odstranjen s seznama uporabnikov.

Upravljanje skupin

Ko nastavite področja in predloge, lahko izdelate skupine. Preglejte naslednje teme:

- “Dodajanje skupine” na strani 137
- “Iskanje skupin v področju” na strani 137
- “Urejanje informacij skupine” na strani 137

- “Kopiranje skupine”
- “Odstranitev skupine” na strani 138

Dodajanje skupine

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Uporabniki in skupine**.

1. Kliknite **Dodaj skupino** ali **Upravljanje skupin**, nato pa **Dodaj**.
2. Vnesite ime skupine, ki jo želite izdelati.
3. S spustnega seznama izberite področje, v katero želite dodati uporabnika.
4. Za izdelavo skupine kliknite **Dokončaj**. Če v področju že imate uporabnike, lahko kliknete **Naprej** in izberete uporabnike za dodajanje v skupino. Nato kliknite **Dokončaj**.

Dodatne informacije boste našli v razdelku “Skupine in vloge” na strani 41.

Iskanje skupin v področju

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Uporabniki in skupine**.

1. Kliknite **Najdi skupino** ali **Upravljanje skupin**, nato pa **Poišči**.
2. V polju **Izbira področja** izberite področje, ki ga želite preiskati.
3. V polje **Atribut poimenovanja** vnesite iskalni niz. Univerzalni znaki so podprti; če na primer vpišete ***klub**, bodo vrnjene vse skupine z atributom poimenovanja klub, kot so na primer knjižni klub, šahovski klub, smučarski klub itd.
4. Za izbrano skupino lahko izvedete naslednje operacije:
   - **Urejanje** - glejte “Urejanje informacij skupine”.
   - **Kopiranje** - glejte “Kopiranje skupine”.
   - **Brisanje** - glejte “Odstranitev skupine” na strani 138.
5. Ko končate, kliknite **Zapri**.

Urejanje informacij skupine

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Uporabniki in skupine**.

1. Kliknite **Upravljanje skupin**.
2. S spustnega menija izberite področje. Če skupine še niso prikazane v okencu **Skupine**, kliknite **Prikaži skupine**.
3. Izberite skupino, ki jo želite urejati, in kliknite **Urejanje**.
4. Če želite omejiti število **razpoložljivih uporabnikov**, lahko kliknete **Filter**. Če na primer vnesete v polje priimka *smoje, omejite razpoložljive uporabnike na tiste, katerih ime se konča s smoje, kot so na primer Miha Smoje, Bine Smoje, Alenka Smoje in tako naprej.
5. Uporabnike lahko v skupino dodate ali jih odstranite iz nje.
6. Ko končate, kliknite **Potrdi**.

Kopiranje skupine

Če morate izdelati več skupin, ki v glavnem vsebujejo enake člane, lahko to naredite tako, da prekopirate začetno skupino in spremenite informacije.

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Uporabniki in skupine**.

1. Kliknite **Upravljanje skupin**.
2. S spustnega menija izberite področje. Če v okencu **Skupine** niso prikazani uporabniki, kliknite **Prikaži skupine**.
3. Izberite skupino, ki jo želite prekopirati, in kliknite **Prekopiraj**.
4. V polju **Ime skupine** spremenite ime skupine. Nova skupina ima enake člane kot izvorna.
5. Člane skupine lahko spremenite.
6. Ko končate, kliknite **Potrdi**. Izdelana je nova skupina, ki vsebuje enake člane kot izvorna skupina, ter popravke zaradi dodajanja ali odstranjevanja, ki ste jih opravili med postopkom kopiranja.

Odstranitev skupine

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Uporabniki in skupine**.

1. Kliknite **Upravljanje skupin**.
2. S spustnega menija izberite področje. Če skupine še niso prikazane v okencu **Skupine**, kliknite **Prikaži skupine**.
3. Izberite skupino, ki jo želite odstraniti, in kliknite **Zbriši**.
4. Ko vas program pozove na potrditev brisanja, kliknite **Potrdi**.
5. Skupina je odstranjena s seznama skupin.

Upravljanje področij in uporabniških predlog

Za upravljanje področij in uporabniških predlog kliknite v področju za usmerjanje orodja za spletno upravljanje možnost **Področja in predloge**. S področji in uporabniškimi predlogami drugim uporabnikom poenostavite vnašanje podatkov v imenik. Dodatne informacije o konceptih področij in uporabniških predlog boste našli v temi “Področja in uporabniške predloge” na strani 38.

Dodatne informacije boste našli v naslednjih temah:

- “Izdelava področja”
- “Izdelava skrbnika področja”
- “Izdelava predloge” na strani 139
- “Dodajanje predloge v področje” na strani 141
- “Izdelava skupin” na strani 141
- “Dodajanje uporabnika v področje” na strani 141
- “Upravljanje področij” na strani 141
- “Upravljanje predlog” na strani 142

Izdelava področja

Dodatne informacije o konceptih področij in uporabniških predlog boste našli v temi “Področja in uporabniške predloge” na strani 38.

Področje izdelate z naslednjim postopkom:

1. V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Področja in predloge**.
2. Kliknite **Dodaj področje**.
   - Vnesite ime področja, kot je na primer **področje1**.
   - Vnesite nadrejeni DN, ki določa mesto področja. Ta vnos ima obliko pripone, kot je na primer o=ibm,c=us. Ta vnos je lahko pripona ali vnos kjerkoli drugje v imeniku. Za izbiro mesta želenega poddrevesa lahko tudi kliknete **Preglej**.
3. Za nadaljevanje kliknite **Naprej** ali pa kliknite **Dokončaj**.
4. Če ste kliknili **Naprej**, preglejte informacije. Področje na tej točki dejansko še ni izdelano, zato lahko polji **Uporabniška predloga** in **Uporabniški iskalni filter** zanemarite.
5. Za izdelavo področja kliknite **Dokončaj**.

Izdelava skrbnika področja

Za izdelavo skrbnika področja morate za to področje najprej izdelati skupino za upravljanje:

1. Izdelajte upravno skupino področja.
   a. V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Upravljanje imenika**.
   b. Kliknite **Upravljanje vnosov**.
   c. Razširite drevo in izberite pravkar izdelano področje **cn=realm1,o=ibm,c=us**.
   d. Kliknite **Urejanje ACL-ja**.

e. Kliknite jeziček **Lastniki**.
f. Polje **Razširi lastnika** mora biti označeno.
g. vnesite DN področja **cn=realm1,o=ibm,c=us**.
h. Spremenite **tip** na skupino.
i. Kliknite **Dodaj**.

2. Izdelajte vnos skrbnika. Če uporabniškega vnosa za skrbnika še nimate, ga morate izdelati.
   a. V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Upravljanje imenika**.
   b. Kliknite **Upravljanje vnosov**.
   c. Drevo razširite na mestu, kamor želite shraniti vnos skrbnika.

      Opomba: Če shranite vnos skrbnika izven področja, preprečite, da bi skrbnik po nesreči zbrisal svoj vnos. V tem primeru je mesto lahko **o=ibm,c=us**.

   d. Kliknite **Dodaj**.
   e. Izberite **Strukturalni objektni razred**, kot je na primer **inetOrgPerson**.
   f. Kliknite **Naprej**.
   g. Izberite pomožni objektni razred, ki ga želite dodati.
   h. Kliknite **Naprej**.
   i. Vnesite obvezne atribute za vnos, kot so na primer
      - **RDN** cn=JohnDoe
      - **DN** o=ibm,c=us
      - **cn** John Doe
      - **sn** Doe
   j. Na jezičku **Drugi atributi** ne pozabite dodeliti gesla.
   k. Ko končate, kliknite **Dokončaj**.
3. Skrbnika dodajte v upravno skupino.
   a. V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Upravljanje imenika**.
   b. Kliknite **Upravljanje vnosov**.
   c. Razširite drevo in izberite pravkar izdelano področje **cn=realm1,o=ibm,c=us**.
   d. Kliknite **Urejanje atributov**.
   e. Kliknite jeziček **Člani**.
   f. Kliknite **Člani**.
   g. V polje **Člani** vnesite DN skrbnika; v tem primeru je to **cn=John Doe,o=ibm,c=us**.
   h. Kliknite **Dodaj**. DN se prikaže na seznamu **Člani**.
   i. Kliknite **Potrdi**.
   j. Kliknite **Ažuriraj**. DN se prikaže na seznamu **Trenutni člani**.
   k. Kliknite **Potrdi**.
4. Izdelali ste skrbnika, ki lahko upravlja vnose znotraj področja.

Izdelava predloge

Po izdelavi področja sledi izdelava uporabniške predloge. Predloga vam bo pomagala pri ureditvi informacij, ki jih želite vnesti. V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Področja in predloge**.

1. Kliknite **Dodaj uporabniško predlogo**.
   - Vnesite ime predloge, kot je na primer **predloga1**.
   - Vnesite mesto, kjer bo predloga shranjena. Zaradi podvajanja jo shranite v poddrevesu področja, ki bo uporabljalo to predlogo, kot je na primer področje, izdelano v prejšnjih operacijah **cn=realm1,o=ibm,c=us**. Če želite za mesto predloge poiskati drugo poddrevo, lahko tudi kliknete gumb **Preglej**.

2. Kliknite **Naprej**. Za izdelavo prazne predloge lahko kliknete **Dokončaj**. Informacije lahko predlogi dodate kasneje; glejte “Urejanje predloge” na strani 144.
3. Če ste kliknili **Naprej**, izberite za predlogo strukturalni objektni razred, kot je na primer **inetOrgPerson**. Dodate lahko tudi želene pomožne objektne razrede.
4. Kliknite **Naprej**.
5. V predlogi je bil izdelan jeziček **Obvezno**. Informacije na tem jezičku lahko spremenite.
   a. Na meniju jezička izberite **Obvezno** in kliknite **Urejanje**. Prikaže se okno **Urejanje jezička**. Prikaže se ime jezička **Obvezno** in izbrani atributi, ki jih zahteva objektni razred **inetOrgPerson**:
      - *sn - priimek
      - *cn - splošno ime

      Opomba: * označuje obvezne informacije.
   b. Če želite na ta jeziček vnesti dodatne informacije, izberite atribut z menija **Atributi**. Izberete lahko na primer **departmentNumber** in kliknete **Dodaj** ali **employeeNumber** in kliknete **Dodaj** ali **title** in kliknete **Dodaj**. Meni **Izbrani atributi** je zdaj takšen:
      - title
      - employeeNumber
      - departmentNumber
      - *sn
      - *cn
   c. Če označite izbran atribut in kliknete **Premakni gor** ali **Premakni dol**, lahko spremenite način prikaza teh polj na predlogi. S tem spremenite mesto atributa za en položaj. Postopek ponavljajte, dokler atributi niso urejeni tako, kot želite, kot na primer v naslednjem primeru:
      - *sn
      - *cn
      - title
      - employeeNumber
      - departmentNumber
   d. Vsakega od izbranih atributov lahko tudi spremenite.
      1) Atribut označite v okencu **Izbrani atributi** in kliknite **Urejanje**.
      2) Spremenite lahko ime polja za prikaz, ki bo uporabljeno na predlogi. Če želite na primer prikazati **departmentNumber** kot **Department number**, vnesite to ime v polje **Ime za prikaz**.
      3) Podate lahko tudi privzeto vrednost, ki bo vnaprej vnesena v polje atributa na predlogi. Če bo na primer večina uporabnikov, ki jih boste vnesli, članov oddelka 789, lahko vnesete 789 kot privzeto vrednost. Polje na predlogi bo vnaprej izpolnjeno z vrednostjo 789. Vrednost lahko spremenite, ko dodate dejanske informacije o uporabniku.
      4) Kliknite **Potrdi**.
   e. Kliknite **Potrdi**.
6. Če želite izdelati drugo kategorijo jezička za dodatne informacije, kliknite **Dodaj**.
   - Vnesite ime novega jezička, kot so na primer Informacije o naslovu.
   - Za ta jeziček izberite atribute z menija **Atributi**. Izberete lahko na primer **homePostalAddress** in kliknete **Dodaj** ali **postOfficeBox** in kliknete **Dodaj** ali **telephoneNumber** in kliknete **Dodaj** ali **homePhone** in kliknete **Dodaj** ali **facsimileTelephoneNumber** in kliknete **Dodaj**. Meni **Izbrani atributi** je zdaj takšen:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone
     – facsimileTelephoneNumber

- Če označite izbran atribut in kliknete **Premakni gor** ali **Premakni dol**, lahko spremenite način prikaza teh polj na predlogi. S tem spremenite mesto atributa za en položaj. Postopek ponavljajte, dokler atributi niso urejeni tako, kot želite, kot na primer v naslednjem primeru:
  - homePostalAddress
  - postOfficeBox
  - telephoneNumber
  - facsimileTelephoneNumber
  - homePhone
- Kliknite **Potrdi**.

7. Ta postopek ponovite za vse jezičke, ki jih želite izdelati. Ko končate, kliknite **Dokončaj**, da izdelate predlogo.

Dodajanje predloge v področje

Ko izdelate področje in predlogo, morate predlogo dodati v področje. V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Področja in predloge**.

1. Kliknite **Upravljanje področij**.
2. Izberite področje, v katero želite dodati predlogo - v tem primeru je to **cn=realm1,o=ibm,c=us** - in kliknite **Urejanje**.
3. Pomaknite se do izbire **Uporabniška predloga** in razširite spustni meni.
4. Izberite predlogo, ki je v tem primeru **cn=template1,cn=realm1,o=ibm,c=us**.
5. Kliknite **Potrdi**.
6. Kliknite **Zapri**.

Izdelava skupin

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Uporabniki in skupine**.

1. Kliknite **Dodaj skupino**.
2. Vnesite ime skupine, ki jo želite izdelati. kot je na primer **skupina1**.
3. S spustnega seznama izberite področje, v katero želite dodati uporabnika. V tem primeru izberite **področje1**.
4. Za izdelavo skupine kliknite **Dokončaj**. Če v področju že imate uporabnike, lahko kliknete **Naprej** in izberete uporabnike za dodajanje v skupino1. Nato kliknite **Dokončaj**.

Dodatne informacije boste našli v razdelku “Skupine in vloge” na strani 41.

Dodajanje uporabnika v področje

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Uporabniki in skupine**.

1. Kliknite **Dodaj uporabnika**.
2. S spustnega seznama izberite področje, v katero želite dodati uporabnika. V tem primeru izberite **področje1**.
3. Kliknite **Naprej**. Prikaže se pravkar izdelana predloga, to je predloga1. Izpolnite obvezna polja, označena z zvezdico (*), in vsa druga polja na jezičkih. Če ste v področju že izdelali skupine, lahko v eno ali več skupin dodate uporabnika.
4. Ko končate, kliknite **Dokončaj**.

Upravljanje področij

Ko nastavite in poselite začetno področje, lahko dodate več področij ali spremenite obstoječa.

V področju za usmerjanje razširite kategorijo **Področja in predloge** in kliknite **Upravljanje področij**. Prikaže se seznam obstoječih področij. V tem oknu lahko področje, dodate, uredite, odstranite ali uredite sezname za nadzor dostopa (ACL-je) področja. Dodatne informacije boste našli v naslednjih temah:

- “Dodajanje področja” na strani 142
- “Urejanje področja” na strani 142

- “Odstranitev področja”
- “Urejanje ACL-jev v področju”

Dodajanje področja

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Področja in predloge**.

1. Kliknite **Dodaj področje**.
   - Vnesite ime področja, kot je na primer **področje2**.
   - Če kakšno področje že obstaja, kot je na primer **področje1**, lahko prekopirate njegove nastavitve v področje, ki ga izdelujete.
   - Vnesite nadrejeni DN, ki določa mesto področja. Ta vnos ima obliko pripone, kot je na primer **o=ibm,c=us**. Za izbiro mesta želenega poddrevesa lahko tudi kliknete **Preglej**.
2. Za nadaljevanje kliknite **Naprej** ali pa kliknite **Dokončaj**.
3. Če ste kliknili **Naprej**, preglejte informacije.
4. S spustnega seznama izberite **Uporabniška predloga**. Če ste prekopirali nastavitve iz že obstoječega področja, je to polje vnaprej izpolnjeno.
5. Vnesite **Iskalni filter uporabnika**.
6. Za izdelavo področja kliknite **Dokončaj**.

Urejanje področja

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Področja in predloge**.

- Kliknite **Upravljanje področij**.
- S seznama področij izberite področje, ki ga želite urediti.
- Kliknite **Urejanje**.
  - Z gumbi **Preglej** lahko tudi spremenite
    - skupino skrbnikov
    - vsebnik skupine
    - vsebnik uporabnika.
  - S spustnega menija lahko izberete drugo predlogo.
  - Kliknite **Urejanje**, da spremenite **iskalni filter uporabnika**.
- Ko končate, kliknite **Potrdi**.

Odstranitev področja

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Področja in predloge**.

1. Kliknite **Upravljanje področij**.
2. Izberite področje, ki ga želite odstraniti.
3. Kliknite **Zbriši**.
4. Ko vas program pozove na potrditev brisanja, kliknite **Potrdi**.
5. Področje je odstranjeno s seznama področij.

Urejanje ACL-jev v področju

Za prikaz lastnosti ACL-jev z orodjem za spletno upravljanje in za delo z ACL-ji preglejte razdelek “Upravljanje seznamov za nadzor dostopa (ACL-jev)” na strani 145.

Dodatne informacije boste našli v razdelku “Seznami za nadzor dostopa” na strani 47.

Upravljanje predlog

Ko izdelate začetno predlogo, lahko dodate druge predloge ali spremenite obstoječe.

V področju za usmerjanje razširite kategorijo **Področja in predloge** in kliknite **Upravljanje uporabniških predlog**. Prikaže se seznam obstoječih predlog. V tem oknu lahko predlogo dodate, jo uredite, odstranite ali uredite sezname za nadzor dostopa (ACL-je) predloge. Dodatne informacije boste našli v naslednjih temah:

- “Dodajanje uporabniške predloge”
- “Urejanje predloge” na strani 144
- “Odstranitev predloge” na strani 144
- “Urejanje ACL-jev na predlogi” na strani 145

Dodajanje uporabniške predloge

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Področja in predloge**.

1. Kliknite **Dodaj uporabniško predlogo** ali **Upravljanje uporabniških predlog**, nato pa **Dodaj**.
   - Vnesite ime nove predloge, kot je na primer **predloga2**.
   - Če kakšna predloga že obstaja, kot je na primer **predloga1**, lahko prekopirate njene nastavitve v predlogo, ki jo izdelujete.
   - Vnesite nadrejeni DN, ki določa mesto predloge. Ta vnos ima obliko DN-ja, kot je na primer **cn=realm1,o=ibm,c=us**. Za izbiro mesta želenega poddrevesa lahko tudi kliknete **Preglej**.
2. Kliknite **Naprej**. Za izdelavo prazne predloge lahko kliknete **Dokončaj**. Informacije lahko predlogi dodate kasneje; glejte “Urejanje predloge” na strani 144.
3. Če ste kliknili **Naprej**, izberite za predlogo strukturalni objektni razred, kot je na primer **inetOrgPerson**. Dodate lahko tudi želene pomožne objektne razrede.
4. Kliknite **Naprej**.
5. V predlogi je bil izdelan jeziček **Obvezno**. Informacije na tem jezičku lahko spremenite.
   a. Na meniju jezička izberite **Obvezno** in kliknite **Urejanje**. Prikaže se okno **Urejanje jezička**. Prikaže se ime jezička **Obvezno** in izbrani atributi, ki jih zahteva objektni razred **inetOrgPerson**:
      - *sn - priimek
      - *cn - splošno ime

      Opomba: * označuje obvezne informacije.
   b. Če želite na ta jeziček vnesti dodatne informacije, izberite atribut z menija **Atributi**. Izberete lahko na primer **departmentNumber** in kliknete **Dodaj** ali **employeeNumber** in kliknete **Dodaj** ali **title** in kliknete **Dodaj**. Meni **Izbrani atributi** je zdaj takšen:
      - title
      - employeeNumber
      - departmentNumber
      - *sn
      - *cn
   c. Če označite izbran atribut in kliknete **Premakni gor** ali **Premakni dol**, lahko spremenite način prikaza teh polj na predlogi. S tem spremenite mesto atributa za en položaj. Postopek ponavljajte, dokler atributi niso urejeni tako, kot želite, kot na primer v naslednjem primeru:
      - *sn
      - *cn
      - title
      - employeeNumber
      - departmentNumber
   d. Vsakega od izbranih atributov lahko tudi spremenite.
      1) Atribut označite v okencu **Izbrani atributi** in kliknite **Urejanje**.
      2) Spremenite lahko ime polja za prikaz, ki bo uporabljeno na predlogi. Če želite na primer prikazati **departmentNumber** kot **Department number**, vnesite to ime v polje **Ime za prikaz**.

3) Podate lahko tudi privzeto vrednost, ki bo vnaprej vnesena v polje atributa na predlogi. Če bo na primer večina uporabnikov, ki jih boste vnesli, članov oddelka 789, lahko vnesete 789 kot privzeto vrednost. Polje na predlogi bo vnaprej izpolnjeno z vrednostjo 789. Vrednost lahko spremenite, ko dodate dejanske informacije o uporabniku.

4) Kliknite **Potrdi**.

e. Kliknite **Potrdi**.

6. Če želite izdelati drugo kategorijo jezička za dodatne informacije, kliknite **Dodaj**.
   - Vnesite ime novega jezička, kot so na primer Informacije o naslovu.
   - Za ta jeziček izberite atribut z menija **Atributi**. Izberete lahko na primer **homePostalAddress** in kliknete **Dodaj** ali **postOfficeBox** in kliknete **Dodaj** ali **telephoneNumber** in kliknete **Dodaj** ali **homePhone** in kliknete **Dodaj** ali **facsimileTelephoneNumber** in kliknete **Dodaj**. Meni **Izbrani atributi** je zdaj takšen:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone
     – facsimileTelephoneNumber
   - Če označite izbran atribut in kliknete **Premakni gor** ali **Premakni dol**, lahko spremenite način prikaza teh polj na predlogi. S tem spremenite mesto atributa za en položaj. Postopek ponavljajte, dokler atributi niso urejeni tako, kot želite, kot na primer v naslednjem primeru:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – facsimileTelephoneNumber
     – homePhone
   - Kliknite **Potrdi**.
7. Ta postopek ponovite za vse jezičke, ki jih želite izdelati. Ko končate, kliknite **Dokončaj**, da izdelate predlogo.

Urejanje predloge

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Področja in predloge**.

- Kliknite **Urejanje uporabniških predlog**.
- S seznama področij izberite področje, ki ga želite urediti.
- Kliknite **Urejanje**.
- Če že imate kakšno predlogo, kot je na primer predloga1, lahko prekopirate njene nastavitve v predlogo, ki jo urejate.
- Kliknite **Naprej**.
  – S spustnim menijem lahko spremenite strukturalni objektni razred predloge.
  – Pomožne objekte razrede lahko dodate ali odstranite.
- Kliknite **Naprej**.
- Jezičke in atribute, vsebovane v predlogi, lahko spremenite. Informacije o spreminjanju jezičkov boste našli v razdelku 5 na strani 143.
- Ko končate, kliknite **Dokončaj**.

Odstranitev predloge

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Področja in predloge**.

1. Kliknite **Urejanje uporabniških predlog**.
2. Izberite predlogo, ki jo želite odstraniti.
3. Kliknite **Zbriši**.
4. Ko vas program pozove na potrditev brisanja, kliknite **Potrdi**.

5. Predloga je odstranjena s seznama predlog

Urejanje ACL-jev na predlogi

V področju za usmerjanje orodja za spletno upravljanje razširite kategorijo **Področja in predloge**.

1. Kliknite **Urejanje uporabniških predlog**.
2. Izberite predlogo, za katero želite urediti ACL-je.
3. Kliknite **Urejanje ACL-ja**.

Za prikaz lastnosti ACL-jev z orodjem za spletno upravljanje in za delo z ACL-ji preglejte razdelek “Upravljanje seznamov za nadzor dostopa (ACL-jev)”.

Dodatne informacije boste našli v razdelku “Seznami za nadzor dostopa” na strani 47.

Upravljanje seznamov za nadzor dostopa (ACL-jev)

Dodatne informacije o seznamih za nadzor dostopa boste našli v razdelku “Seznami za nadzor dostopa” na strani 47.

Za prikaz lastnosti ACL-jev z orodjem za spletno upravljanje in delo z njimi naredite naslednje:

1. Izberite imeniški vnos, kot je na primer cn=John Doe,ou=Advertising,o=ibm,c=US.
2. Kliknite **Urejanje ACL-ja**. Prikaže se okno Urejanje ACL-ja z vnaprej izbranim jezičkom **Razpoložljivi ACL-ji**.

To okno vsebuje pet jezičkov:

- “Razpoložljivi ACL-ji”
- “Razpoložljivi lastniki” na strani 146
- “Nefiltrirani ACL-ji” na strani 146
- “Filtrirani ACL-ji” na strani 147
- “Lastniki” na strani 148

Jezička **Razpoložljivi ACL-ji** in **Razpoložljivi lastniki** vsebujeta bralne informacije o ACL-jih.

Razpoložljivi ACL-ji

Razpoložljivi ACL-ji so eksplicitni in podedovani ACL-ji izbranega vnosa. Dostopne pravice za določen razpoložljiv ACL si lahko ogledate tako, da ga izberete in kliknete gumb **Prikaži**. Odpre se okno **Prikaz pravic za dostop**.

Prikaz pravic za dostop

- V razdelku **Pravice** so prikazane subjektove pravice za dodajanje in brisanje.
  - **Dodaj otroka** subjektu dodeli ali zavrne pravico za dodajanje imeniškega vnosa pod izbran vnos.
  - **Zbriši vnos** subjektu dodeli ali zavrne pravico za brisanje izbranega vnosa.
- Razdelek razreda **Zaščita** definira dovoljenja za razrede zaščite. Atributi so razdeljeni v razrede zaščite:
  - **Normalni** - razredi normalnih atributov zahtevajo najmanjšo zaščito, kot je na primer atribut commonName.
  - **Občutljivi** - razredi občutljivih atributov zahtevajo srednjo raven zaščite, kot je na primer homePhone.
  - **kritični** - razredi kritičnih atributov zahtevajo najvišjo raven zaščite, kot je na primer atribut userpassword.

  Z vsakim razredom zaščite so povezana dovoljenja.
  - **Branje** - subjekt lahko atribute bere.
  - **Pisanje** - subjekt lahko atribute spreminja.
  - **Iskanje** - subjekt lahko atribute išče.
  - **Primerjava** - subjekt lahko atribute primerja.

Za vrnitev na jeziček Razpoložljivi ACL-ji kliknite **Potrdi**.

Za vrnitev v okno Urejanje ACL-jev kliknite **Prekliči**.

Razpoložljivi lastniki

Razpoložljivi lastniki so eksplicitni in podedovani lastniki izbranega vnosa.

Nefiltrirani ACL-ji

Vnosu lahko dodate nove nefiltrirane ACL-je ali uredite obstoječe nefiltrirane ACL-je.

Nefiltrirane ACL-je lahko razširite. To pomeni, da lahko informacije o nadzoru dostopa, ki so definirane za en vnos, uveljavite v vseh njegovih podrejenih vnosih. Izvor ACL-ja je izvor trenutnega ACL-ja za izbran vnos. Če vnos nima ACL-ja, ga podeduje iz nadrejenih objektov glede na nastavitve ACL-ja nadrejenih objektov.

Na jeziček **Nefiltrirani** ACL-ji vnesite naslednje informacije:

- Razširi ACL-je - potrditveno polje **Razširi** izberite, da naslednikom brez eksplicitno definiranega ACL-ja omogočite dedovanje iz tega vnosa. Če je potrditveno polje izbrano, naslednik podeduje ACL-je iz tega vnosa; če je ACL eksplicitno definiran za otroški vnos, je ACL, ki je bil podedovan od starša, nadomeščen z novim ACL-jem, ki je bil dodan. Če potrditveno polje ni izbrano, bodo nasledniški vnosi brez eksplicitno definiranega ACL-ja podedovali ACL-je iz starša tega vnosa, v katerem je omogočena ta možnost.
- DN (razločevalno ime) - vnesite **(DN) razločevalno ime** vnosa, ki zahteva dostop za izvedbo operacij v izbranem vnosu, kot je na primer cn=Marketing Group.
- Tip - vnesite **tip** DN-ja. Izberete lahko na primer access-id, če je DN uporabnik.

Dodajanje in urejanje pravic za dostop

Kliknite **Dodaj**, da dodate DN v polje DN (razločevalno ime) na seznamu ACL-jev ali gumb Urejanje, da spremenite ACL-je obstoječega DN-ja.

V oknih **Dodajanje pravic za dostop** in **Urejanje pravic za dostop** lahko nastavite pravice za dostop za nove ali obstoječe sezname za nadzor dostopa (ACL-je). Vrednost v polju **Tip** je po privzetku nastavljena na tip, ki ga izberete v oknu **Urejanje ACL-jev**. Če ACL dodajate, so vsa druga polja po privzetku prazna. Če ACL urejate, polja vsebujejo vrednosti, ki ste jih nastavili pri zadnji spremembi ACL-ja.

Naredite lahko naslednje:

- spremenite tip ACL-ja
- nastavite pravice za dodajanje in brisanje
- nastavite dovoljenja za razrede zaščite.

Pravice za dostop nastavite takole:

1. Izberite **tip** vnosa za ACL. Izberete lahko na primer access-id, če je DN uporabnik.
2. V razdelku **Pravice** so prikazane subjektove pravice za dodajanje in brisanje.
   - **Dodaj otroka** subjektu dodeli ali zavrne pravico za dodajanje imeniškega vnosa pod izbran vnos.
   - **Zbriši vnos** subjektu dodeli ali zavrne pravico za brisanje izbranega vnosa.
3. Razdelek **Razred zaščite** definira dovoljenja za razrede atributov. Atributi so razdeljeni v razrede zaščite:
   - Normalna - razredi normalnih atributov zahtevajo najmanjšo zaščito, kot je na primer atribut commonName.
   - Občutljiva - razredi občutljivih atributov zahtevajo srednjo raven zaščite, kot je na primer homePhone.
   - Kritična - razredi kritičnih atributov zahtevajo najvišjo raven zaščite, kot je na primer atribut userpassword.

   Z vsakim razredom zaščite so povezana dovoljenja.
   - Branje - subjekt lahko atribute bere.
   - Pisanje - subjekt lahko atribute spreminja.
   - Iskanje - subjekt lahko atribute išče.
   - Primerjava - subjekt lahko atribute primerja.

Poleg tega lahko podate dovoljenja na osnovi atributa namesto na osnovi razreda zaščite, v katerega spada atribut. Razdelek atributa je naveden spodaj pod izbiro **Kritični razred zaščite**.

- Izberite atribut s spustnega seznama **Definiranje atributa**.
- Kliknite **Definiraj**. Atribut se prikaže se tabelo dovoljenj.
- Podajte, ali želite vsako od štirih dovoljenj za razred zaščite, povezanih z atributom, dodeliti ali zavrniti.
- Ta postopek lahko ponovite za več atributov.
- Če želite atribut odstraniti, ga preprosto izberite in kliknite **Zbriši**.
- Ko končate, kliknite **Potrdi**.

Odstranitev ACL-jev

ACL-je lahko odstranite na dva načina:

- Izberite izbirni gumb poleg ACL-ja, ki ga želite zbrisati in kliknite **Odstrani**.
- Kliknite **Odstrani vse**, da zbrišete vse DN-je s seznama.

Filtrirani ACL-ji

Vnosu lahko dodate nove filtrirane ACL-je ali uredite obstoječe filtrirane ACL-je.

ACL-ji, ki temeljijo na filtrih, uporabljajo primerjavo, temelječo na filtrih s podanim objektnim filtrom, s katerim primerjajo ciljne objekte z razpoložljivim dostopom, ki velja za njih.

Privzeto vedenje ACL-jev, temelječih na filtrih, je kopičenje od najnižjega vnosa, ki vsebuje, do verige vnosov prednika, pa vse do najvišjega vnosa v DIT, ki vsebuje. Razpoložljiv dostop je izračunan kot zveza dostopnih pravic, ki jih odobrijo ali zavrnejo sestavni vnosi prednika. Vendar obstaja v tem vedenju izjema. Zaradi združljivosti s funkcijo podvajanja poddrevesa in da bi se omogočil večji nadzor nad upravljanjem, se uporablja atribut zgornje meje kot sredstvo za zaustavitev kopičenja v vnosu, v katerem je vsebovan.

Na jeziček Filtrirani ACL-ji vnesite naslednje informacije:

- Nakopiči filtrirane ACLs -
  - Izbirni gumb **Nepodan** izberite, da odstranite atribut ibm-filterACLInherit iz izbranega vnosa.
  - Izbirni gumb **True** izberite, kopičenje ACL-jev za izbran vnos od tega vnosa in navzgor vzdolž verige vnosov prednika, pa vse do najvišjega filtriranega ACL-ja, ki vsebuje vnos v DIT.
  - Izbirni gumb **False** izberite, da zaustavite kopičenje filtriranih ACL-jev v izbranem vnosu.
- DN (razločevalno ime) - vnesite **(DN) razločevalno ime** enote, ki zahteva dostop za izvedbo operacij v izbranem vnosu, kot je na primer cn=Marketing Group.
- Tip - vnesite **tip** DN-ja. Izberete lahko na primer access-id, če je DN uporabnik.

Dodajanje in urejanje pravic za dostop

Kliknite **Dodaj**, da dodate DN v polje DN (razločevalno ime) na seznamu ACL-jev ali gumb Urejanje, da spremenite ACL-je obstoječega DN-ja.

V oknih **Dodajanje pravic za dostop** in **Urejanje pravic za dostop** lahko nastavite pravice za dostop za nove ali obstoječe sezname za nadzor dostopa (ACL-je). Privzeta vrednost za polje Tip je tip, ki ste ga izbrali v oknu Urejanje ACL-jev. Če ACL dodajate, so vsa druga polja po privzetku prazna. Če ACL urejate, polja vsebujejo vrednosti, ki ste jih nastavili pri zadnji spremembi ACL-ja.

Naredite lahko naslednje:

- spremenite tip ACL-ja
- nastavite pravice za dodajanje in brisanje
- nastavite objektni filter za filtrirane ACL-je

- nastavite dovoljenja za razrede zaščite.

Pravice za dostop nastavite takole:

1. Izberite **tip** vnosa za ACL. Izberete lahko na primer access-id, če je DN uporabnik.
2. V razdelku **Pravice** so prikazane subjektove pravice za dodajanje in brisanje.
   - **Dodaj otroka** subjektu dodeli ali zavrne pravico za dodajanje imeniškega vnosa pod izbran vnos.
   - **Zbriši vnos** subjektu dodeli ali zavrne pravico za brisanje izbranega vnosa.
3. Nastavite objektni filter za primerjavo, temelječo na filtrih. V polje **Objektni filter** vnesite želeni objektni filter za izbran ACL. Če potrebujete pomoč pri sestavljanju niza iskalnega filtra, kliknite **Urejanje filtra**. Trenutni filtrirani ACL se razširi v vse naslednjiške objekte v povezanem poddrevesu, ki ustreza filtru v tem polju.
4. Razdelek **Razred zaščite** definira dovoljenja za razrede atributov. Atributi so razdeljeni v razrede zaščite:
   - Normalna - razredi normalnih atributov zahtevajo najmanjšo zaščito, kot je na primer atribut commonName.
   - Občutljiva - razredi občutljivih atributov zahtevajo srednjo raven zaščite, kot je na primer homePhone.
   - Kritična - razredi kritičnih atributov zahtevajo najvišjo raven zaščite, kot je na primer atribut userpassword.

   Z vsakim razredom zaščite so povezana dovoljenja.
   - Branje - subjekt lahko atribute bere.
   - Pisanje - subjekt lahko atribute spreminja.
   - Iskanje - subjekt lahko atribute išče.
   - Primerjava - subjekt lahko atribute primerja.

   Poleg tega lahko podate dovoljenja na osnovi atributa namesto na osnovi razreda zaščite, v katerega spada atribut. Razdelek atributa je naveden spodaj pod izbiro **Kritični razred zaščite**.
   - Izberite atribut s spustnega seznama **Definiranje atributa**.
   - Kliknite **Definiraj**. Atribut se prikaže se tabelo dovoljenj.
   - Podajte, ali želite vsako od štirih dovoljenj za razred zaščite, povezanih z atributom, dodeliti ali zavrniti.
   - Ta postopek lahko ponovite za več atributov.
   - Če želite atribut odstraniti, ga preprosto izberite in kliknite **Zbriši**.
   - Ko končate, kliknite **Potrdi**.

Odstranitev ACL-jev

ACL-je lahko odstranite na dva načina:

- Izberite izbirni gumb poleg ACL-ja, ki ga želite zbrisati in kliknite **Odstrani**.
- Kliknite **Odstrani vse**, da zbrišete vse DN-je s seznama.

Lastniki

Lastniki vnosov imajo dovoljenja za izvajanje katerihkoli operacij v objektu. Lastniki vnosov so lahko eksplicitni ali razširjeni (podedovani).

Na jeziček **Lastniki** vnesite naslednje informacije:

- Potrditveno polje **Razširi lastnike** izberite, da omogočite naslednikom brez eksplicitno definiranega vnosa dedovanje iz tega vnosa. Če potrditveno polje ni izbrano, bodo naslednjiški vnosi brez eksplicitno definiranega lastnika podedovali lastnika iz starša tega vnosa, v katerem je omogočena ta možnost.
- DN (razločevalno ime) - vnesite **(DN) razločevalno ime** entitete, ki zahteva dostop za izvedbo operacij v izbranem vnosu, kot je na primer cn=Marketing Group.

  Če uporabite cn=this z objekti, ki razširijo svoje lastništvo na druge objekte, boste poenostavili izdelavo imeniškega poddrevesa, v katerem je vsak objekt sam svoj lastnik.
- Tip - vnesite **tip** DN-ja. Izberete lahko na primer access-id, če je DN uporabnik.

Dodajanje lastnika

Kliknite **Dodaj**, da dodate DN v polju **DN (razločevalno ime)** na seznam.

Odstranitev lastnika

Lastnika lahko odstranite na dva načina:

- Izberite izbirni gumb poleg DN-ja lastnika, ki ga želite zbrisati in kliknite **Odstrani**.
- Kliknite **Odstrani vse**, da zbrišete vse DN-je lastnikov s seznama.

Objavljanje informacij v imeniškem strežniku

Sistem lahko konfigurirate tako, da objavi določene informacije v imeniškem strežniku v istem ali v drugem sistemu; to velja tudi za uporabniško definirane informacije. OS/400 samodejno objavi te informacije v imeniškem strežniku, če z Navigatorjem iSeries spremenite te informacije v OS/400. Informacije, ki jih lahko objavite, vključujejo sistemske informacije (sistemi in tiskalniki), tiskalnike v skupni rabi, uporabniške informacije in načela kakovosti storitve TCP/IP (dodatne informacije boste našli v razdelku “Objavljanje” na strani 33).

Če nadrejeni DN, v katerega objavljate podatke, ne obstaja, ga imeniški strežnik samodejno izdela. Namestite lahko tudi druge aplikacije OS/400, ki objavljajo informacije v imeniku LDAP. Poleg tega lahko iz lastnih programov pokličete vmesnike uporabniških programov (API-je), ki objavijo v imenik LDAP druge vrste informacij.

Opomba: Informacije OS/400 lahko objavite tudi v imeniškem strežniku, ki se ne izvaja v OS/400, če ta strežnik konfigurirate za uporabo IBM-ove sheme.

Sistem konfigurirate za objavo informacij OS/400 v imeniškem strežniku z naslednjimi koraki:

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

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

   Opomba: Če želite objaviti informacije OS/400 na imeniškem strežniku z uporabo SSL ali Kerberos, morate imeniški strežnik najprej konfigurirati za uporabo ustreznega protokola. Dodatne informacije o zaščiti SSL in Kerberos boste našli v razdelku “Overjanje Kerberos z imeniškim strežnikom” na strani 41.
10. Če imeniški strežnik ne uporablja privzetih vrat, vnesite pravilno številko vrat v polje **Vrata**.
11. Kliknite **Preveri**, s čimer zagotovite, da nadrejeno RN obstaja v sistemu in da so informacije o povezavi pravilne. Če pot imenika ne obstaja, se bo prikazalo pogovorno okno, ki vas bo pozvalo k izdelavi imenika.

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

Opomba: Informacije i5/OS lahko objavite tudi v imeniškem na drugi platformi. Uporabniške in sistemske informacije morate objaviti v imeniški strežnik, ki uporablja shemo, združljivo s shemo IBM-ovega imeniškega strežnika. Dodatne informacije o IBM-ovi imeniški shemi boste našli v razdelku “IBM Directory Server” na strani 16.

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

Imeniški strežnik vsebuje vgrajeno podporo za objavljanje uporabniških in sistemskih informacij. Te postavke so navedene na strani **Imeniški strežnik** pogovornega okna s sistemskimi **lastnostmi**. Konfiguracijo strežnika LDAP in API-je za objavljanje lahko uporabite za omogočanje programov OS/400, ki ste jih napisali za objavljanje drugih tipov informacij. Te informacije so ravno tako prikazane na strani **Imeniški strežnik**. Tako kot uporabniške in sistemske informacije so v začetku onemogočene, konfigurirate pa ju z enakim postopkom. Program, ki doda podatke v imenik LDAP, se imenuje posrednik za objavljanje. Tip objavljenih informacij, kot so prikazane na strani **Imeniški strežnik**, se imenuje ime posrednika.

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

QgldChgDirSvrA
Aplikacija uporablja format CSVR0500 za začetno dodajanje imena posrednika, ki je označen kot onemogočena postavka. Navodila za uporabnike aplikacije morajo poudariti, naj z Navigatorjem iSeries odprejo stran lastnosti imeniškega strežnika, kjer naj konfigurirajo posrednika za objavljanje. Zgledi imen posrednikov so sistemska in uporabniška imena posrednikov, ki so na voljo na strani **Imeniški strežnik**.

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

QgldPubDirObj
Ta API uporabite za dejansko objavljanje informacij.

Podrobne informacije o teh API-jih boste našli v temi Lightweight Directory Access Protocol (LDAP) razdelka Programiranje v Informacijskem centru iSeries.

Poglavje 8. Odpravljanje težav v imeniškem strežniku

Na žalost prihaja tudi v zanesljivih strežnikih, kot je imeniški strežnik, včasih do težav. V primeru težav vam bodo naslednje informacije pomagale ugotoviti, kaj je narobe in kako težavo odpraviti.

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

“Nadzorovanje napak in dostopa z dnevnikom opravil imeniškega strežnika” na strani 152
Če pride v imeniškem strežniku do napake, o kateri potrebujete več podrobnosti, si lahko ogledate dnevnik opravila QDIRSRV.

“Uporaba TRCTCPAPP za pomoč pri iskanju težav” na strani 152
Za napake, ki jih je mogoče poustvariti, lahko z ukazom TRCTCPAPP APP(*DIRSRV) (Trace TCP/IP Application - Sledi aplikaciji TCP/IP) zaženete sledenje napakam.

“Uporaba možnosti LDAP_OPT_DEBUG za sledenje napak” na strani 153
Sledite težavam z odjemalci, ki uporabljajo API-je C LDAP.

“Splošne napake odjemalca LDAP” na strani 153
Poznavanje vzrokov splošnih napak odjemalca LDAP vam lahko pomaga pri reševanju težav s strežnikom.

Dodatne informacije o splošnih težavah v imeniškem strežniku boste našli na domači strani imeniškega strežnika (www.iseries.ibm.com/ldap).

Imeniški strežnik uporablja več strežnikov SQL (Structured Query Language), ki so opravila QSQSRVR iSeries. Če pride do napake SQL, bo dnevnik opravil QDIRSRV običajno vseboval naslednje sporočilo:

```
Prišlo je do napake SQL -1
```

V teh primerih vas dnevnik opravil QDIRSRV napoti na dnevnike opravil strežnika SQL. V nekaterih primerih QDIRSRV morda ne bo vseboval tega sporočila in referenčnega kazalca, čeprav je strežnik SQL vzrok težave. V teh primerih bo pomagalo, če boste vedeli, katera strežniška opravila SQL so bila zagnana, tako da boste vedeli, v katerih dnevnikih opravil QSQSRVR iskati dodatne napake.

Če se imeniški strežnik normalno zažene, ustvari sporočila, podobna naslednjim:

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

  >> CALL PGM(QSYS/QGLDSVR)
     Opr 057448/QUSER/QSQSRVR upor. za obd. načina strežnika SQL.
     Opr 057340/QUSER/QSQSRVR upor. za obd. načina strežnika SQL.
     Opr 057448/QUSER/QSQSRVR upor. za obd. načina strežnika SQL.
     Opr 057166/QUSER/QSQSRVR upor. za obd. načina strežnika SQL.
     Opr 057279/QUSER/QSQSRVR upor. za obd. načina strežnika SQL.
     Opr 057288/QUSER/QSQSRVR upor. za obd. načina strežnika SQL.
     Imeniški strežnik je bil uspešno zagnan.
```

Sporočila se nanašajo na opravila QSQSRVR, ki so bila zagnana za strežnik. Število opravil na strežniku se lahko razlikuje glede na konfiguracijo in število opravil QSQSRVR, potrebnih za izvedbo zagona strežnika.

Na strani Navigatorja iSeries podate na strani lastnosti **Baza podatkov/pripone** imeniških strežnikov skupno število strežnikov SQL, ki jih uporablja imeniški strežnik za imeniške operacije po zagonu strežnika. Za podvajanje so zagnani dodati strežniki SQL.

Nadzorovanje napak in dostopa z dnevnikom opravil imeniškega strežnika

Pregled dnevnika opravil za imeniški strežnik vas bo opozoril na napake in vam pomagal pri nadzorovanju dostopa do strežnika. Dnevnik opravila vsebuje naslednje:

- Sporočila o delovanju strežnika in vse težave na strežniku, kot so težave v opravilih strežnika SQL in težave pri podvajanju.
- Z zaščito povezana sporočila, ki kažejo operacije odjemalcev, kot so na primer napačna gesla.
- Sporočila, ki podajajo podrobnosti o napakah odjemalcev, kot so na primer manjkajoči atributi.

Napake odjemalcev boste morda beležili samo v primeru, da razhroščujete odjemalske težave. Beleženje odjemalskih napak lahko nadzorujete na strani **Splošno** imeniškega strežnika v Navigatorju iSeries.

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

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

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

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

Uporaba TRCTCPAPP za pomoč pri iskanju težav

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

Ukaz TRCTCPAPP (Trace TCP/IP Application - Sledi aplikaciji TCP/IP) z možnostjo *DIRSRV lahko uporabite v imeniškem strežniku kot pomoč pri iskanju težav z odjemalci ali aplikacijami.

Podrobnejše informacije o uporabi ukaza TRCTCPAPP z LDAP, kot tudi o omejitvah obveznih atributov, boste našli v opisu ukaza TRCTCPAPP (Trace TCP/IP Application - Sledi aplikaciji TCP/IP).

Splošne informacije o uporabi komunikacijskega sledenja boste našli v razdelku Komunikacijska sled.

Uporaba možnosti LDAP_OPT_DEBUG za sledenje napak

Možnost LDAP_OPT_DEBUG API-ja **ldap_set_option()** lahko uporabite za sledenje težavam odjemalcev, ki uporabljajo API-j C LDAP. Možnost razhroščevanja ima več nastavitev ravni razhroščevanja, ki so vam lahko v pomoč pri odpravljanju težav s temi aplikacijami.

Primer omogočanja možnosti razhroščevanja sledenja odjemalca:

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

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

Zgled omogočanja sledenja odjemalca z uporabo spremenljivke okolja LDAP_DEBUG:

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

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

```
DMPUSRTRC    ClientJobNumber
```

kjer ClientJobNumber podaja številko opravila odjemalca.

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

```
DSPPFM  QAPOZDMP  QP0Znnnnnn
```

kjer vsebuje QAP0ZDMP nič, nnnnnn pa je številka opravila.

Če želite te informacije shraniti, da bi jih poslali servisu, naredite naslednje:

1. Izdelajte datoteko SAVF z uporabo ukaza za izdelavo SAVF (CRTSAVF).
2. V ukazni poziv na iSeries vnesite naslednje:

   ```
   SAVOBJ  OBJ(QAP0ZDMP  LIB(QTEMP)  DEV(*SAVF)  SAVF(xxx)
   ```

   kjer vsebuje QAP0ZDMP nič, *xxx* pa je ime, ki ste ga določili za datoteko SAVF.

Splošne napake odjemalca LDAP

Poznavanje vzrokov splošnih napak odjemalca LDAP vam lahko pomaga pri reševanju težav s strežnikom. Celoten seznam stanj napak v odjemalcu LDAP boste našli v temi “API-ji imeniškega strežnika” pod razdelkom Programiranje v Informacijskem centru iSeries.

Sporočila o napakah odjemalca imajo naslednji format:

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

Opomba: Razlaga teh napak predpostavlja, da odjemalec komunicira s strežnikom LDAP v i5/OS. Odjemalec, ki komunicira s strežnikom na drugi platformi, lahko dobi podobna sporočila, vzroki in rešitve pa so lahko drugačni.

Splošna sporočila vključujejo naslednje:

- “ldap_search: Presežena je časovna omejitev” na strani 154
- “[Neuspela operacija LDAP]: Napaka v operaciji” na strani 154

- “ldap_bind: Takega objekta ni”
- “ldap_bind: Neustrezno overjanje”
- “[Napačna operacija LDAP]: Nezadosten dostop”
- “[Neuspela operacija LDAP]: Ne morem komunicirati s strežnikom LDAP”
- “[neuspela operacija LDAP]: povezava s strežnikom SSL ni uspela” na strani 155

ldap_search: Presežena je časovna omejitev

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

- Povečajte omejitev iskalnega časa za imeniški strežnik. Informacije o tem postopku boste našli v razdelku “Prilagoditev nastavitev zmogljivosti” na strani 100.
- Zmanjšajte delovanje vašega sistema. Zmanjšate lahko tudi število aktivnih opravil odjemalcev LDAP, ki se izvajajo.

[Neuspela operacija LDAP]: Napaka v operaciji

To napako lahko povzroči več stvari. Informacije o vzroku te napake za določen primerek boste našli v dnevnikih opravil QDIRSRV (kot opisuje “Nadzorovanje napak in dostopa z dnevnikom opravil imeniškega strežnika” na strani 152) in v dnevnikih strežnikih opravil SQL (Structured Query Language) (kot opisuje Poglavje 8, “Odpravljanje težav v imeniškem strežniku”, na strani 151).

ldap_bind: Takega objekta ni

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

Podrobnosti o napaki boste našli v dnevniku opravila QDIRSRV, kot opisuje razdelek “Nadzorovanje napak in dostopa z dnevnikom opravil imeniškega strežnika” na strani 152.

ldap_bind: Neustrezno overjanje

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

- Postavka, ki nima lastnosti uporabniškega gesla
- Postavka, ki predstavlja uporabnika i5/OS, ki ima lastnost UID in ne lastnosti uporabniškega gesla. To povzroči, da se izvede primerjava med podanim geslom in geslom uporabnika i5/OS, ki se je ujemata.
- Postavka, ki predstavlja projektiranega uporabnika, zahtevana pa je bila povezovalna metoda, ki ni preprosta.

Do te napake običajno pride, ko se odjemalec poskuša povezati z geslom, ki ni veljavno. Če potrebujete podrobnosti o napaki, preglejte dnevnik opravila QDIRSRV kot to opisuje “Nadzorovanje napak in dostopa z dnevnikom opravil imeniškega strežnika” na strani 152.

[Napačna operacija LDAP]: Nezadosten dostop

Do te napake običajno pride, če povezovalni DN nima pooblastila za izvajanje operacije (kot je dodajanje ali brisanje), ki jo zahteva odjemalec. Za podrobnejše informacije o tej napaki preglejte dnevnik opravil QDIRSRV, kot je opisano v razdelku “Nadzorovanje napak in dostopa z dnevnikom opravil imeniškega strežnika” na strani 152.

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

Najpogostejši vzroki te napake so naslednji:

- Odjemalec LDAP izda zahtevo, še preden strežnik LDAP v podanem sistemu začne delovati in je v stanju izbirnega čakanja.
- Uporabnik poda številko vrat, ki ni veljavna. Strežnik na primer posluša na vratih 386, zahteva odjemalca pa poskuša uporabiti vrata 387.

Za podrobnejše informacije o tej napaki preglejte dnevnik opravil QDIRSRV, kot je opisano v razdelku “Nadzorovanje napak in dostopa z dnevnikom opravil imeniškega strežnika” na strani 152. Če je bil imeniški strežnik uspešno zagnan, bo dnevnik opravila QDIRSRV vseboval sporočilo o njegovem uspešnem zagonu.

[neuspela operacija LDAP]: povezava s strežnikom SSL ni uspela

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

- Podpora za upravljanje potrdil je zavrnila poskus odjemalca, da bi vzpostavil povezavo s strežnikom. Z Upravljalnikom digitalnih potrdil preverite, ali so potrdila pravilno nastavljena, nato pa strežnik znova zaženite in ponovite povezavo.
- Uporabnik morda nima bralnega dostopa do prostora za potrdila *SYSTEM (po privzetku /QIBM/userdata/ICSS/Cert/Server/default.kdb).

V aplikacijah C i5/OS so na voljo tudi dodatne informacije o napaki SSL. Podrobnosti boste našli v razdelku “API-ji imeniškega strežnika” v temi Programiranje.

Poglavje 9. Referenčne informacije

Dodatne referenčne informacije boste našli v naslednjih temah:

- “Pripomočki ukazne vrstice”
- “Format za izmenjavo podatkov LDAP (LDIF)” na strani 182
- “Konfiguracijska shema imeniškega strežnika” na strani 184

Pripomočki ukazne vrstice

Ta razdelek opisuje pripomočke, ki jih lahko zaženete iz ukaznega okolja Qshell v sistemu i5/OS. Dodatne informacije boste našli v naslednjih ukazih:

- “ldapmodify in ldapadd”
- “ldapdelete” na strani 160
- “ldapexop” na strani 162
- “ldapmodrdn” na strani 166
- “ldapsearch” na strani 169
- “ldapchangepwd” na strani 177
- “ldapdiff” na strani 178
- “Opombe o uporabi SSL s pripomočki ukazne vrstice LDAP” na strani 181

Da bi bili nekateri nizi pravilno obdelani v ukaznem okolju Qshell, morajo biti vključeni v narekovaje. To se običajno nanaša na nize, ki so DN-ji, iskalni filtri in seznam atributov, ki jih vrne ldapsearch. Primere boste našli na naslednjem seznamu.

- Nizi, ki vsebujejo presledke: "cn=John Smith,cn=users"
- Nizi, ki vsebujejo univerzalne znake: "*"
- Nizi, ki vsebujejo oklepaje: "(objectclass=person)"

Dodatne informacije o ukaznem okolju Qshell boste našli v temi “Qshell”.

ldapmodify in ldapadd

Orodje za spreminjanje vnosa LDAP in dodajanje vnosa LDAP

Oris

```
ldapmodify [-a] [-b] [-c] [-C nabor-znakov] [-d raven-razhroščevanja][-D povezovalni-dn][-i datoteka]
[-h gostitelj-ldap] [-k] [-K datoteka-ključev] [-m mehanizem] [-M] [-N ime-potrdila]
[-O največ-preskokov] [-p vrata-ldap] [-P geslo-datoteke-ključev] [-r] [-R] [-v] [-V]
[-w geslo | ?] [-Z]
```

```
ldapadd [-a] [-b] [-c] [-C nabor-znakov] [-d raven-razhroščevanja][-D povezovalni-dn][-i datoteka]
[-h gostitelj-ldap] [-k] [-K datoteka-ključev] [-m mehanizem] [-M] [-N ime-potrdila]
[-O največ-preskokov] [-p vrata-ldap] [-P geslo-datoteke-ključev] [-r] [-R] [-v] [-V] [-w geslo | ?]
[-Z]
```

Opis

ldapmodify je vmesnik ukazne vrstice za vmesnike uporabniških programov (API-je) ldap_modify, ldap_add, ldap_delete in ldap_modrdn. **ldapadd** se izvaja kot preimenovana različica ldapmodify. Če ga pokličete kot ldapadd, je oznaka **-a** (dodaj nov vnos) vključena samodejno.

ldapmodify odpre povezavo s strežnikom LDAP in se s strežnikom poveže. **ldapmodify** lahko uporabljate za spreminjanje ali dodajanje vnosov. Informacije o vnosu so prebrane iz standardnega vhoda ali iz datoteke z možnostjo **-i**.

Če želite prikazati skladenjsko pomoč za **ldapmodify** ali **ldapadd**, vpišite

```
ldapmodify -?
```

ali

```
ldapadd -?.
```

Možnosti

-a Doda nove vnose. Privzeto dejanje za **ldapmodify** je spreminjanje obstoječih vnosov. Če ga pokličete kot **ldapadd**, je ta oznaka vedno nastavljena.

-b Sklep, da so vse vrednosti, ki se začno z znakom `/', dvojiške vrednosti, in da je dejanska vrednost v datoteki, katere pot je podana namesto vrednosti.

-c Način nepretrganega delovanja. Napake so sporočene, toda **ldapmodify** se nadaljuje s popravki. Privzeto dejanje je sicer izhod po pošiljanju napake.

-C *nabor-znakov*
Podaja, da so nizi, ki so podani kot vhodni podatki za pripomočka **ldapmodify** in **ldapadd**, predstavljani v lokalnem naboru znakov, ki ga podaja nabor-znakov, in da morajo biti pretvorjeni v UTF-8. Možnost **-C** *nabor-znakov* uporabite, če se kodna stran vhodnega niza razlikuje od vrednosti kodne strani opravila. Podprte vrednosti za nabor znakov boste našli v API-ju ldap_set_iconv_local_charset().

-d *raven-razhroščevanja*
Raven razhroščevanja LDAP nastavi na raven-razhroščevanja.

-D*povezovalni-dni*
Možnost ***povezovalni-dn*** uporabite za povezovanje z imenikom LDAP. ***povezovalni-dn*** je DN, predstavljen z nizom.

-h*gostitelj-ldap*
Podajte nadomestnega gostitelja, na katerem se izvaja strežnik ldap.

-i *datoteka*
S to možnostjo preberete informacije o popravkih postavke iz datoteke LDIF namesto iz standardnega vhoda. Če datoteka LDIF ni podana, morate z uporabo standardnega vhoda podati zapise za ažuriranje v formatu LDIF.

-k Podaja uporabo nadzora za upravljanje strežnika.

-K*datoteka-ključev*
Podaja ime datoteke baze podatkov ključev SSL s privzeto pripono **kdb**. Če datoteka baze podatkov ključev ni v trenutnem imeniku, podajte celotno ime datoteke baze podatkov ključev. Če imena datoteke baze podatkov ključev ne podate, ta pripomoček najprej pregleda, ali obstaja spremenljivka okolja SSL_KEYRING s povezanim imenom datoteke. Če spremenljivka okolja SSL_KEYRING ni definirana, bo uporabljena sistemska datoteka obroča ključev (če obstaja).

Ta parameter učinkovito omogoča stikalo **-Z**. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-m*mehanizem*
Z ***mehanizmom*** podajte mehanizem SASL, ki bo uporabljen za povezavo s strežnikom. Uporabljen je API ldap_sasl_bind_s(). Parameter **-m** je zanemarjen, če podate **-V 2**. Če **-m** ne podate, se uporabi preprosto overjanje. Veljavni mehanizmi so naslednji:

- CRAM-MD5 - ščiti geslo, poslano strežniku
- EXTERNAL - uporabi potrdilo SSL; zahteva možnost -Z
- GSSAPI - uporabi uporabnikove poverilnice Kerberos

-M Referenčne objekte upravlja kot navadne vnose.

-N*ime-potrdila*
S to možnostjo podate oznako, ki je povezava s potrdilom odjemalca v datoteki baze podatkov ključev. Če je strežnik LDAP konfiguriran, da izvaja samo overjanje strežnika, potrdilo odjemalca ni potrebno. Če je strežnik LDAP konfiguriran za overjanje odjemalca in strežnika, bo najbrž potrebno potrdilo odjemalca. ***ime-potrdila*** ni potrebno, če je par potrdila/zasebnega ključa določen kot privzetek za datoteko baze podatkov ključev. Prav tako ***ime-potrdila*** ni potrebno, če v določeni datoteki baze podatkov obstaja posamezni par potrdila in zasebnega ključa. Ta parameter je zanemarjen, če ne podate niti **-Z** niti **-K**. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-O *največ-preskokov*
Možnost ***največ-preskokov*** podaja največje dovoljeno število preskokov, prek katerih gre knjižnica odjemalca pri sledenju referenčnim kazalcem. Privzeta vrednost za števec preskokov je 10.

-p *vrata-ldap*
Podajte nadomestna vrata TCP, na katerih posluša strežnik ldap. Privzeta vrata LDAP so 389. Če ne podate možnosti **-p** in podate možnost **-Z**, bodo uporabljena privzeta vrata SSL LDAP 636.

-P*geslo-datoteke-ključev*
Podaja geslo baze podatkov ključev. To geslo je potrebno za dostopanje do šifriranih informacij v datoteki baze podatkov ključev, ki lahko vsebuje enega ali več zasebnih ključev. Če je z datoteko baze podatkov ključev povezano skrita datoteka gesel, je geslo pridobljeno iz nje, parameter **-P** pa ni potreben. Ta parameter je zanemarjen, če ne podate niti **-Z** niti **-K**.

-r S to možnostjo po privzetku zamenjate obstoječe vrednosti.

-R Ta možnost podaja, da se referenčnim kazalcem ne sme slediti samodejno.

-v Uporabite način z razlago, z veliko diagnostičnimi podatki, ki se zapišejo v standardni izhod.

-V Podaja različico LDAP, ki jo bo uporabil **ldapmodify** pri povezovanju s strežnikom LDAP. Po privzetku je vzpostavljena povezava LDAP V3. Če želite izrecno izbrati LDAP V3, podajte **-V 3**. Za izvajanje kot aplikacija LDAP V2 podajte **-V 2**.

-w *geslo* **| ?**
Za overjanje uporabite ***geslo*** kot geslo. ? uporabite za tvorbo poziva za geslo.

-Z To možnost uporabite, če povezava SSL komunicira s strežnikom LDAP. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

Vhodni format

Vsebina datoteke (ali standardni vhod, če v ukazni vrstici ni podana oznaka **-i**), mora ustrezati formatu LDIF. Dodatne informacije o formatu LDIF boste našli v razdelku “Format za izmenjavo podatkov LDAP (LDIF)” na strani 182.

Primeri

Denimo, da datoteka /tmp/entrymods obstaja in ima naslednjo vsebino:

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

```
jpegPhoto: /tmp/modme.jpeg
-
delete: description
-
```

ukaz

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

nadomesti vsebino atributa mail za vnos Modify Me z vrednostjo modme@student.of.life.edu, doda naslov Grand Poobah, pretvori vsebino datoteke /tmp/modme.jpeg v jpegPhoto in v celoti odstrani atribut description. Enake spremembe lahko opravite s starejšim vhodnim formatom ldapmodify:

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

in ukazom

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

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

```
dn: cn=John Doe, o=University of Higher Learning, c=US
objectClass: person
cn: John Doe
cn: Johnny
sn: Doe
title: the world's most famous mythical person
mail: johndoe@student.of.life.edu
uid: jdoe
```

ukaz

```
 ldapadd -i /tmp/entrymods
```

doda nov vnos za Johna Doa, pri čemer uporabi vrednosti iz datoteke /tmp/newentry.

Opombe

Če informacije o vnosu niso posredovane iz datoteke z uporabo možnosti **-i**, bo ukaz **ldapmodify** počakal, da bo prebral vnose iz standardnega vhoda.

Diagnosticiranje

Če se ne zgodi nobena napaka, je izhodni status 0. Napake povzročijo izhodni status, ki ni nič, in zapis diagnostičnega sporočila v standardno napako.

ldapdelete

Orodje za brisanje vnosa LDAP

Oris

```
ldapdelete [-c] [-C nabor-znakov] [-d raven-razhroščevanja][-D povezovalni-dn][-i datoteka]
[-h gostitelj-ldap] [-k] [-K datoteka-ključev] [-m mehanizem] [-M] [-n] [-N ime-potrdila]
[-O največ-preskokov] [-p vrata-ldap] [-P geslo-datoteke-ključev] [-R] [-s][-v] [-V različica]
[-w geslo | ?] [-Z] [dn]...
```

Opis

ldapdelete je vmesnik ukazne vrstice za aplikacijski programerski vmesnik (API) ldap_delete.

ldapdelete odpre povezavo s strežnikom LDAP, se poveže ter zbriše enega ali več vnosov. Če podate enega ali več argumentov razločevalnega imena (DN), so vnosi s temi DN-ji zbrisani. Vsak DN je DN, predstavljen z nizom. Če ne podate nobenega argumenta DN, je seznam DN-jev prebran iz standardnega vhoda ali iz datoteke, če uporabite oznako **-i**.

Če želite prikazati skladenjsko pomoč za **ldapdelete**, vpišite naslednje:

```
ldapdelete -?
```

Možnosti

-c Način nepretrganega delovanja. Napake so sporočene, toda **ldapdelete** se nadaljuje s popravki. Privzeto dejanje je sicer izhod po pošiljanju napake.

-C *nabor-znakov*
Podaja, da so DN-ji, ki so posredovani kot vhod za pripomoček **ldapdelete**, predstavljeni z lokalnim naborom znakov, ki ga podaja nabor-znakov. Možnost **-C** *nabor-znakov* uporabite, če se kodna stran vhodnega niza razlikuje od vrednosti kodne strani opravila. Podprte vrednosti za nabor znakov boste našli v API-ju ldap_set_iconv_local_charset().

-d *raven-razhroščevanja*
Raven razhroščevanja LDAP nastavi na raven-razhroščevanja.

-D*povezovalni-dni*
Možnost ***povezovalni-dn*** uporabite za povezovanje z imenikom LDAP. ***povezovalni-dn*** je DN, predstavljen z nizom.

-h*gostitelj-ldap*
Podajte nadomestnega gostitelja, na katerem se izvaja strežnik LDAP.

-i *datoteka*
Branje niza vrstic iz datoteke in izvedba enega brisanja LDAP za vsako vrstico v datoteki. Vsaka vrstica v datoteki mora vsebovati eno razločevalno ime.

-k Podaja uporabo nadzora za upravljanje strežnika.

-K*datoteka-ključev*
S to možnostjo podate datoteko baze podatkov ključev SSL. Če datoteka baze podatkov ključev ni v trenutnem imeniku, podajte celotno ime datoteke baze podatkov ključev.

Če pomožni program ne more določiti položaja baze podatkov ključev, bo uporabil programsko določen niz privzetih overjenih skrbnikov služb za pooblastila. Datoteka baze podatkov ključev vsebuje običajno enega ali več potrdil služb za pooblastila (CA), ki jim zaupajo odjemalci. Ti tipi potrdil X.509 so običajno poznani kot overjena potrdila.

Ta parameter učinkovito omogoča stikalo **-Z**. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-m*mehanizem*
Z ***mehanizmom*** podajte mehanizem SASL, ki bo uporabljen za povezavo s strežnikom. Parameter **-m** je zanemarjen, če podate **-V 2**. Če možnosti **-m** ne podate, bo uporabljeno preprosto overjanje.

-M Referenčne objekte upravlja kot navadne vnose.

-n Prikaže, kaj bi se zgodilo, vendar vnosov dejansko ne spremeni. Koristno pri razhroščevanju v povezavi z **-v**.

-N*ime-potrdila*
S to možnostjo podate oznako, ki je povezava s potrdilom odjemalca v datoteki baze podatkov ključev. Če je strežnik LDAP konfiguriran, da izvaja samo overjanje strežnika, potrdilo odjemalca ni potrebno. Če je strežnik LDAP konfiguriran za overjanje odjemalca in strežnika, bo najbrž potrebno potrdilo odjemalca. Parameter ***ime-potrdila*** ni obvezen, če ste kot privzetek določili par potrdilo/zasebni ključ. Prav tako ***ime-potrdila*** ni potrebno, če v določeni datoteki baze podatkov obstaja posamezni par potrdila in zasebnega ključa. Ta parameter je zanemarjen, če ne podate niti **-Z** niti **-K**. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-O *največ-preskokov*
Možnost ***največ-preskokov*** podaja največje dovoljeno število preskokov, prek katerih gre knjižnica odjemalca pri sledenju referenčnim kazalcem. Privzeta vrednost za števec preskokov je 10.

-p *vrata-ldap*
Podajte nadomestna vrata TCP, na katerih posluša strežnik LDAP. Privzeta vrata LDAP so 389. Če ne podate možnosti **-p** in podate možnost **-Z**, bodo uporabljena privzeta vrata SSL LDAP 636.

-P*geslo-datoteke-ključev*
Podaja geslo baze podatkov ključev. To geslo je potrebno za dostopanje do šifriranih informacij v datoteki baze podatkov ključev, ki lahko vsebuje enega ali več zasebnih ključev. Če je z datoteko baze podatkov ključev povezano skrita datoteka gesel, je geslo pridobljeno iz nje, parameter **-P** pa ni potreben. Ta parameter je zanemarjen, če ne podate niti **-Z** niti **-K**.

-R Ta možnost podaja, da se referenčnim kazalcem ne sme slediti samodejno.

-s To možnost uporabite za brisanje poddrevesa s korenom v podanem vnosu.

-v Uporabite način z razlago, z veliko diagnostičnimi podatki, ki se zapišejo v standardni izhod.

-V Podaja različico LDAP, ki jo bo uporabil **ldapdelete** pri povezovanju s strežnikom LDAP. Po privzetku je vzpostavljena povezava LDAP V3. Če želite izrecno izbrati LDAP V3, podajte **-V 3**. Za izvajanje kot aplikacija LDAP V2 podajte **-V 2**.

-w *geslo* **| ?**
Za overjanje uporabite ***geslo*** kot geslo. ? uporabite za tvorbo poziva za geslo.

-Z To možnost uporabite, če povezava SSL komunicira s strežnikom LDAP. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

dn Podaja enega ali več argumentov DN. Vsak DN mora biti DN, predstavljen z nizom.

Primeri

Ukaz

```
ldapdelete -D cn=administrator -w secret "cn=Delete Me, o=University of Life, c=US"
```

poskusi zbrisati vnos, poimenovan s splošnim imenom ″Delete Me″ neposredno pod vnosom University of Life.

Opombe

Če ne podate nobenega argumenta DN, ukaz **ldapdelete** počaka in prebere seznam DN-jev iz standardnega vhoda.

Diagnosticiranje

Če se ne zgodi nobena napaka, je izhodni status 0. Napake povzročijo izhodni status, ki ni nič, in zapis diagnostičnega sporočila v standardno napako.

ldapexop

Orodje za razširjeno operacijo LDAP

Oris

```
ldapexop [-C nabor-znakov] [-d raven-razhroščevanja][-D povezovalni-dn][-e] [-h gostitelj-ldap]
[-help][-K datoteka-ključev] [-m mehanizem] [-N ime-potrdila]
[-p vrata-ldap] [-P geslo-datoteke-ključev] [-?] [-v] [-w geslo | ?] [-Z]
-op {cascrepl | controlqueue | controlrepl |
quiesce | readconfig}
```

Opis

Pripomoček **ldapexop** je vmesnik ukazne vrstice, ki omogoča povezovanje z imeniškim strežnikom in izdajanje ene razširjene operacije z vsemi podatki, ki tvorijo vrednost razširjene operacije.

Pripomoček **ldapexop** podpira možnosti za standardnega gostitelja, vrata, SSL in overjanje, ki jih uporabljajo vsi odjemalski pripomočki LDAP. Poleg tega je definiran niz možnosti, ki podajajo operacijo za izvedbo, in argumente za vsako razširjeno operacijo.

Če želite prikazati skladenjsko pomoč za **ldapexop**, vpišite naslednje:

```
ldapexop -?
```

ali

```
ldapexop -help
```

Možnosti

Možnosti za ukaz ldapexop so razdeljene v dve kategoriji:

1. Splošne možnosti, ki določajo povezavo z imeniškim strežnikom. Podati jih morate pred možnostmi, specifičnimi za operacije.
2. Možnost razširjene operacije, ki določa razširjeno operacijo za izvedbo.

Splošne možnosti

Te možnosti podajajo načine za povezovanje s strežnikom, in jih morate podati pred možnostjo **-op**.

-C *nabor-znakov*
: Podaja, da so DN-ji, ki so posredovani kot vhod za pripomoček **ldapexop**, predstavljeni z lokalnim naborom znakov, ki ga podaja nabor-znakov. Možnost **-C** *nabor-znakov* uporabite, če se kodna stran vhodnega niza razlikuje od vrednosti kodne strani opravila. Podprte vrednosti za nabor znakov boste našli v API-ju ldap_set_iconv_local_charset().

-d *raven-razhroščevanja*
: Raven razhroščevanja LDAP nastavi na raven-razhroščevanja.

-D*povezovalni-dni*
: Možnost ***povezovalni-dn*** uporabite za povezovanje z imenikom LDAP. ***povezovalni-dn*** je DN, predstavljen z nizom.

-e Prikaže informacije o različici knjižnice LDAP, nato pa se zapre.

-h*gostitelj-ldap*
: Podajte nadomestnega gostitelja, na katerem se izvaja strežnik LDAP.

-help Prikaže skladnjo ukaza in informacije o uporabi.

-K*datoteka-ključev*
: S to možnostjo podate datoteko baze podatkov ključev SSL. Če datoteka baze podatkov ključev ni v trenutnem imeniku, podajte celotno ime datoteke baze podatkov ključev.

  Če pripomoček ne more najti baze podatkov ključev, je uporabljena sistemska baza podatkov ključev. Datoteka baze podatkov ključev vsebuje običajno enega ali več potrdil služb za pooblastila (CA), ki jim zaupajo odjemalci. Ti tipi potrdil X.509 so običajno poznani kot overjena potrdila.

  Ta parameter učinkovito omogoča stikalo **-Z**. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-m*mehanizem*
: Z ***mehanizmom*** podajte mehanizem SASL, ki bo uporabljen za povezavo s strežnikom. Uporabljen bo API ldap_sasl_bind_s(). Parameter **-m** bo zanemarjen, če nastavite **-V 2**. Če **-m** ne podate, se uporabi preprosto overjanje.

-N*ime-potrdila*

S to možnostjo podate oznako, ki je povezava s potrdilom odjemalca v datoteki baze podatkov ključev. Če je strežnik LDAP konfiguriran, da izvaja samo overjanje strežnika, potrdilo odjemalca ni potrebno. Če je strežnik LDAP konfiguriran za overjanje odjemalca in strežnika, bo najbrž potrebno potrdilo odjemalca. Parameter ***ime-potrdila*** ni obvezen, če ste kot privzetek določili par potrdilo/zasebni ključ. Prav tako ***ime-potrdila*** ni potrebno, če v določeni datoteki baze podatkov obstaja posamezni par potrdila in zasebnega ključa. Ta parameter je zanemarjen, če ne podate niti **-Z** niti **-K**. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-p *vrata-ldap*

Podajte nadomestna vrata TCP, na katerih posluša strežnik LDAP. Privzeta vrata LDAP so 389. Če ne podate možnosti **-p** in podate možnost **-Z**, bodo uporabljena privzeta vrata SSL LDAP 636.

-P*geslo-datoteke-ključev*

Podaja geslo baze podatkov ključev. To geslo je potrebno za dostopanje do šifriranih informacij v datoteki baze podatkov ključev, ki lahko vsebuje enega ali več zasebnih ključev. Če je z datoteko baze podatkov ključev povezano skrita datoteka gesel, je geslo pridobljeno iz nje, parameter **-P** pa ni potreben. Ta parameter je zanemarjen, če ne podate niti **-Z** niti **-K**.

-? Prikaže skladnjo ukaza in informacije o uporabi.

-v Uporabite način z razlago, z veliko diagnostičnimi podatki, ki se zapišejo v standardni izhod.

-w *geslo* **| ?**

Za overjanje uporabite ***geslo*** kot geslo. ? uporabite za tvorbo poziva za geslo.

-Z To možnost uporabite, če povezava SSL komunicira s strežnikom LDAP. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

Možnost razširjenih operacij

Možnost razširjenih operacij **-op** določa razširjeno operacijo za izvedbo. Vrednost za razširjeno operacijo je lahko nekaj od naslednjega:

- **cascrepl**: razširjena operacija kaskadnega nadzornega podvajanja. Zahtevano dejanje je uveljavljeno v podanem strežniku in posredovano tudi vsem strežnikom za podvajanje podanega poddrevesa. Če je kateri od teh strežnikov za podvajanje strežnik za posredovanje, je razširjena operacija poslana tudi njihovim strežnikom za podvajanje. Operacija se prenese na celotno topologijo podvajanja.

  -action quiesce | unquiesce | replnow | wait

  To je obvezni atribut, ki podaja dejanje za izvedbo.

  quiesce

  Nadaljnji popravki niso dovoljeni, z izjemo podvajanja.

  unquiesce

  Normalno delovanje se nadaljuje, popravki odjemalca so sprejeti.

  replnow

  Čim hitrejša podvojitev vseh čakajočih sprememb v vseh strežnikih za podvajanje ne glede na urnik.

  wait Čakanje, da bodo vsi popravki podvojeni v vseh strežnikih za podvajanje.

  -rc *kontekstni-dn*

  To je obvezni atribut, ki podaja koren poddrevesa.

  -timeout *sekund*

  To je neobvezni atribut, ki v primeru, da je prisoten, podaja čakalni čas v sekundah. Če ni prisoten ali če je njegova vrednost 0, operacija čaka neskončno.

  Primer:

```
ldapexop -op cascrepl -action -quiesce -rc "o=acme,c=us" -timeout 60
```

- **controlqueue**: razširjena operacija podvajanja nadzorne čakalne vrste. Ta operacija omogoča, da zbrišete ali odstranite čakajoče spremembe s seznama sprememb podvajanja, ki so se nakopičile, vendar zaradi napak v podvajanju niso bile izvedene. Uporabna je, če podatke strežnika za podvajanje popravljate ročno. S to operacijo boste preskočili nekaj nakopičenih napak.

  -skip all | id-spremembe
  To je obvezni atribut.
  - **all** kaže, da želite preskočiti vse čakajoče spremembe za ta dogovor.
  - **id-spremembe** določa eno spremembo, ki jo želite preskočiti. Če strežnik te spremembe trenutno ne podvaja, zahteva ne uspe.

  -ra *dn-dogovora*
  To je obvezni atribut, ki podaja DN dogovora o podvajanju.

  Primeri:

```
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**: razširjena operacija nadzornega podvajanja

  -action suspend | resume | replnow
  To je obvezni atribut, ki podaja dejanje za izvedbo.

  -rc *kontekstni-dn* **| -ra** *dn-dogovora*
  -rc *kontekstni-dn* je DN konteksta podvajanja. Dejanje se izvede za vse dogovore za ta kontekst. **-ra** *dn-dogovora* je DN dogovora o podvajanju. Dejanje se izvede za podan dogovor o podvajanju.

  Primer:

```
ldapexop -op controlrepl -action suspend -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"
```

- **quiesce**: mirovanje ali prekinitev mirovanja razširjene operacije podvajanja poddrevesa

  -rc *kontekstni-dn*
  To je obvezni atribut, ki podaja DN konteksta podvajanja (poddrevesa), ki ga želite preklopiti v stanje mirovanja ali to stanje prekiniti.

  -end To je neobvezni atribut, ki v primeru, da je prisoten, podaja prekinitev mirovanja poddrevesa. Če ga ne podate, bo poddrevo po privzetku v stanju mirovanja.

  Primeri:

```
ldapexop -op quiesce -rc "o=acme,c=us"

ldapexop -op quiesce -end -rc "o=ibm,c=us"
```

- **readconfig**: razširjena operacija vnovičnega branja konfiguracijske datoteke

  -scope entire | single<*DN vnosa***><***atribut***>**
  To je obvezni atribut.
  - **entire** kaže, da želite znova prebrati celo konfiguracijsko datoteko.
  - **single** kaže, da želite prebrati en vnos in podan atribut.

  Primeri:

```
ldapexop -op readconfig -scope entire

ldapexop -op readconfig -scope single "cn=configuration" ibm-slapdAdminPW
```

Opomba: Naslednji vnosi, ki so označeni z:

- [1] stopijo v veljavo takoj
- [2] delujejo za nove operacije
- [3] začnejo delovati takoj, ko spremenite geslo (readconfig ni potreben)
- [4], so podprti v pripomočku ukazne vrstice v sistemu i5/OS, ne pa tudi v imeniškem strežniku v 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]
```

Diagnosticiranje

Če se ne zgodi nobena napaka, je izhodni status 0. Napake povzročijo izhodni status, ki ni nič, in zapis diagnostičnega sporočila v standardno napako.

ldapmodrdn

Orodje RDN za spreminjanje vnosa LDAP

Oris

```
ldapmodrdn [-c] [-C nabor-znakov] [-d raven-razhroščevanja][-D povezovalni-dn] [-h gostitelj-ldap]
[-i datoteka] [-k] [-K datoteka-ključev] [-m mehanizem] [-M] [-n]
[-N ime-potrdila] [-O številec-preskokov] [-p vrata-ldap] [-P geslo-datoteke-ključev]
[-r] [-R] [-v] [-V] [-w geslo | ?] [-Z] [dn novi-rdn | [-i datoteka]]
```

Opis

ldapmodrdn je vmesnik ukazne vrstice za aplikacijski programerski vmesnik (API) ldap_modrdn.

ldapmodrdn odpre povezavo s strežnikom LDAP, se poveže z njim in spremeni vnose RDN. Informacije o vnosu so prebrane iz standardnega vhoda, iz datoteke z uporabo možnosti **- f** ali iz para ukazne vrstice dn in rdn.

Informacije o RDN-jih (relativnih razločevalnih imenih) in DN-jih (razločevalnih imenih) boste našli v razdelku “Razločevalna imena (DN-ji)” na strani 11.

Če želite prikazati skladenjsko pomoč za **ldapmodrdn**, vpišite naslednje:

```
ldapmodrdn -?
```

Možnosti

-c Način nepretrganega delovanja. Napake so sporočene, toda **ldapmodrdn** se nadaljuje s popravki. Privzeto dejanje je sicer izhod po pošiljanju napake.

-C *nabor-znakov*
Podaja, da so DN-ji, ki so posredovani kot vhod za pripomoček **ldapmodrdn**, predstavljeni z lokalnim naborom znakov, ki ga podaja nabor-znakov. Možnost **-C** *nabor-znakov* uporabite, če se kodna stran vhodnega niza razlikuje od vrednosti kodne strani opravila. Podprte vrednosti nabora znakov boste našli v API-ju ldap_set_iconv_local_charset(). Podprte vrednosti za nabor znakov so tiste, ki so podprte za oznako nabor-znakov, ki jo lahko po izbiri definirate v datotekah LDIF različice 1.

-d *raven-razhroščevanja*
Raven razhroščevanja LDAP nastavi na raven-razhroščevanja.

-D*povezovalni-dni*
Možnost ***povezovalni-dn*** uporabite za povezovanje z imenikom LDAP. povezovalni-dn mora biti DN, predstavljen z nizom.

-h*gostitelj-ldap*
Podajte nadomestnega gostitelja, na katerem se izvaja strežnik ldap.

-i *datoteka*
Informacije o popravkih vnosa preberite namesto iz standardnega vhoda ali iz ukazne vrstice iz datoteke (tako da podate rdn ali novi-rdn). Standardni vhod je lahko posredovan iz datoteke kot tudi iz (″< datoteka″).

-k Podaja uporabo nadzora za upravljanje strežnika.

-K*datoteka-ključev*
S to možnostjo podate datoteko baze podatkov ključev SSL. Če datoteka baze podatkov ključev ni v trenutnem imeniku, podajte celotno ime datoteke baze podatkov ključev.

Če pomožni program ne more določiti položaja baze podatkov ključev, bo uporabil programsko določen niz privzetih overjenih skrbnikov služb za pooblastila. Datoteka baze podatkov ključev vsebuje običajno enega ali več potrdil služb za pooblastila (CA), ki jim zaupajo odjemalci. Ti tipi potrdil X.509 so običajno poznani kot overjena potrdila.

Ta parameter učinkovito omogoča stikalo **-Z**. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-m*mehanizem*
Z ***mehanizmom*** podajte mehanizem SASL, ki bo uporabljen za povezavo s strežnikom. Uporabljen je API ldap_sasl_bind_s() API. Parameter **-m** bo zanemarjen, če nastavite **-V 2**. Če **-m** ne podate, se uporabi preprosto overjanje.

-M Referenčne objekte upravlja kot navadne vnose.

-n Prikaže, kaj bi se zgodilo, vendar vnosov dejansko ne spremeni. Koristno pri razhroščevanju v povezavi z **-v**.

-N*ime-potrdila*
S to možnostjo podate oznako, ki je povezava s potrdilom odjemalca v datoteki baze podatkov ključev. Če je strežnik LDAP konfiguriran samo za izvajanje overjanja strežnika, potrdilo odjemalca ni potrebno. Če je strežnik LDAP konfiguriran za overjanje odjemalca in strežnika, bo najbrž potrebno potrdilo odjemalca. Parameter ***ime-potrdila*** ni obvezen, če ste kot privzetek določili par potrdilo/zasebni ključ. Prav tako

ime-potrdila ni potrebno, če v določeni datoteki baze podatkov obstaja posamezni par potrdila in zasebnega ključa. Ta parameter je zanemarjen, če ne podate niti **-Z** niti **-K**. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-O*število-preskokov*
Podaja ***število-preskokov*** za nastavitev največjega števila preskokov, prek katerih gre knjižnica odjemalca pri sledenju referenčnim kazalcem. Privzeta vrednost za število preskokov je 10.

-p *vrata-ldap*
Podajte nadomestna vrata TCP, na katerih posluša strežnik ldap. Privzeta vrata LDAP so 389. Če te možnosti ne podate, podate pa -Z, bodo uporabljena privzeta vrata SSL LDAP 636.

-P*geslo-datoteke-ključev*
Podaja geslo baze podatkov ključev. To geslo je potrebno za dostopanje do šifriranih informacij v datoteki baze podatkov ključev (ki lahko vsebuje enega ali več zasebnih ključev). Če je z datoteko baze podatkov ključev povezano skrita datoteka gesel, je geslo pridobljeno iz nje, parameter **-P** pa ni potreben. Ta parameter je zanemarjen, če ne podate niti **-Z** niti **-K**.

-r Iz vnosa odstrani stare vrednosti RDN. Privzeto dejanje je ohranitev starih vrednosti.

-R Ta možnost podaja, da se referenčnim kazalcem ne sme slediti samodejno.

-v Uporabite način z razlago, z veliko diagnostičnimi podatki, ki se zapišejo v standardni izhod.

-V Podaja različico LDAP, ki jo bo uporabil **ldapmodrdn** pri povezovanju s strežnikom LDAP. Po privzetku je vzpostavljena povezava LDAP V3. Če želite izrecno izbrati LDAP V3, podajte **-V 3**. Za izvajanje kot aplikacija LDAP V2 podajte **-V 2**. Aplikacija, kot je **ldapmodrdn**, izbere LDAP V3 kot želeni protokol, tako da namesto ldap_open uporabi ldap_init.

-w *geslo* **| ?**
Za overjanje uporabite ***geslo*** kot geslo. ? uporabite za tvorbo poziva za geslo.

-Z To možnost uporabite, če povezava SSL komunicira s strežnikom LDAP. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

dn novi-rdn
Dodatne informacije boste našli v naslednjem razdelku “Vhodni format za dn novi-rdn”.

Vhodni format za dn novi-rdn

Če podate argumenta ukazne vrstice *dn* in *novi-rdn*, *novi-rdn* zamenja RDN vnosa, podanega z DN-jem *dn*. V nasprotnem primeru je vsebina datoteke (ali standardni vhod, če oznaka **- i** ni podana) sestavljena iz enega ali več vnosov:

```
Razločevalno ime (DN)

Relativno razločevalno ime (RDN)
```

Za ločitev vsakega para DN in RDN lahko uporabite eno ali več praznih vrstic.

Primeri

Denimo, da datoteka /tmp/entrymods obstaja in ima naslednjo vsebino:

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

ukaz

```
ldapmodrdn -r -i /tmp/entrymods
```

spremeni RDN vnosa Modify Me iz Modify Me v The New Me, stari cn Modify Me pa je odstranjen.

Opombe

Če informacij o vnosu ne podate iz datoteke z možnostjo **-i** (ali iz para ukazne vrstice *dn* in *rdn*), ukaz **ldapmodrdn** počaka, da prebere vnose iz standardnega vhoda.

Diagnosticiranje

Če se ne zgodi nobena napaka, je izhodni status 0. Napake povzročijo izhodni status, ki ni nič, in zapis diagnostičnega sporočila v standardno napako.

ldapsearch

Iskalno orodje in vzorčni program LDAP

Oris

```
ldapsearch [-a deref] [-A] [-b iskalna-baza] [-B] [-C nabor-znakov] [-d raven-razhroščevanja]
[-D povezovalni-dn] [-F ločilo] [-h gostitelj-ldap] [-i datoteka] [-K datoteka-ključev] [-l časovna-omejitev] [-L]
[-m mehanizem] [-M] [-n] [-N ime-potrdila][-o tip_atr] [-O največ-preskokov]
[-p vrata-ldap] [-P geslo-datoteke-ključev] [-q velikost-strani]  [-R] [-s območje ] [-t] [-T sekund]
[-v] [-V različica] [-w geslo | ?] [-z omejitev-velikosti] [-Z] filter [atr...]
```

Opis

ldapsearch je vmesnik ukazne vrstice za aplikacijski programerski vmesnik (API) ldap_search.

ldapsearch odpre povezavo s strežnikom LDAP, se poveže in izvede iskanje s filtrom. Filter mora ustrezati predstavitvi nizov za filtre LDAP (dodatne informacije o filtrih boste našli v razdelku ldap_search teme API-ji imeniškega strežnika).

Če najde **ldapsearch** enega ali več vnosov, so atributi, ki jih podajajo atr prebrani, vnosi in vrednosti pa so natisnjeni v standardni izhod. Če ni naveden noben atr, so vrnjeni vsi atributi.

Če želite prikazati skladenjsko pomoč za **ldapsearch**, vpišite ldapsearch -?.

Možnosti

-a deref
: S to možnostjo podate, kako se opravi dereferenciranje vzdevkov. Vrednost za deref je never, always, search ali find, s katerimi podate, da vzdevki ne bodo nikoli dereferencirani, vedno dereferencirani, dereferencirani pri iskanju ali dereferencirani samo pri iskanju osnovnega objekta za iskanje. Privzeta vrednost je, da se vzdevki nikoli (never) ne dereferencirajo.

-A
: Poiščete samo lastnosti (brez vrednosti). Ta možnost je koristna, če želite videti samo, ali lastnost obstaja v vnosu, in vas ne zanimajo posamezne vrednosti.

-b osnova-iskanja
: osnovno-iskanja uporabite kot začetno točko za iskanje namesto privzete vrednosti. Če ne podate možnosti **-b**, bo ta pripomoček iskal definicijo osnove-iskanja v spremenljivki okolja LDAP_BASEDN. Če ni nastavljena nobena, bo privzeta osnova nastavljena na ″″.

-B
: Prikaz vrednosti, ki niso ASCII, ne bo zadržan. To je koristno pri obravnavanju vrednosti iz nadomestnega nabora znakov, kot je ISO-8859.1. Ta možnost je uveljavljena z možnostjo **-L**.

-C nabor-znakov
: Podaja, da bodo nizi, ki so podani kot vhod za pripomoček ldapsearch, predstavljeni z lokalnim naborom znakov (kot ga podaja nabor-znakov). Vnos niza vključuje filter, povezovalni DN in osnovni DN. Podobno je pri prikazu podatkov, ko **ldapsearch** pretvori prejete podatke iz strežnika LDAP v podan nabor znakov.

Možnost **-C** *nabor-znakov* uporabite, če se kodna stran vhodnega niza razlikuje od vrednosti kodne strani opravila. Podprte vrednosti za nabor znakov boste našli v API-ju ldap_set_iconv_local_charset(). Če podate možnost **-C** in **-L**, se domneva, da so vhodni podatki v podanem naboru znakov, toda izhodni podatki iz **ldapsearch** so vedno ohranjeni v svoji predstavitvi UTF-8 ali v predstavitvi podatkov, kodirani v osnovi-64, če so odkriti znaki, ki jih ni mogoče natisniti. Razlog za to je, da vsebujejo standardne datoteke LDIF samo predstavitve nizovnih podatkov UTF-8 (ali v UTF-8, kodiranem z osnovo-64). Podprte vrednosti za nabor znakov so tiste, ki so podprte za oznako nabor-znakov, ki jo lahko po izbiri definirate v datotekah LDIF različice 1.

-d raven-razhroščevanja
Raven razhroščevanja LDAP nastavi na raven-razhroščevanja.

-D povezovalni-dn
povezovalni-dn uporabite za povezovanje z imenikom LDAP. povezovalni-dn mora biti DN, predstavljen z nizom (glejte razločevalna imena LDAP).

-e Prikaže informacije o različici knjižnice LDAP in se zapre.

-F ločilo
ločilo uporabite kot ločilo polja med imeni atributov in vrednostmi. Privzeto ločilo je `=', razen če podate oznako **-L**, ko je ta možnost zanemarjena.

-h gostitelj-ldap
Podajte nadomestnega gostitelja, na katerem se izvaja strežnik ldap.

-i datoteka
Prebere niz vrstic iz datoteke in izvede iskanje LDAP za vsako vrstico. V tem primeru je filter, ki je podan v ukazni vrstici, obravnavan kot vzorec, kjer je prva pojavitev za % nadomeščena z vrstico iz datoteke. Če je datoteka en znak ″-″, so vrstice prebrane iz standardnega vhoda.

-K datoteka-ključev
S to možnostjo podate datoteko baze podatkov ključev SSL. Če datoteka baze podatkov ključev ni v trenutnem imeniku, podajte celotno ime datoteke baze podatkov ključev.

Če pomožni program ne more določiti položaja baze podatkov ključev, bo uporabil programsko določen niz privzetih overjenih skrbnikov služb za pooblastila. Datoteka baze podatkov ključev vsebuje običajno enega ali več potrdil služb za pooblastila (CA), ki jim zaupajo odjemalci. Ti tipi potrdil X.509 so običajno poznani kot overjena potrdila.

Ta parameter učinkovito omogoča stikalo **-Z**. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-l časovna-omejitev
Čakanje na dokončanje iskanja, ki ga določa največja časovna omejitev v sekundah.

-L S to možnostjo prikažete rezultate iskanja v formatu LDIF. Ta možnost vključi tudi možnost **-B** in povzroči, da je možnost **-F** zanemarjena.

-m mehanizem
S to možnostjo podajte mehanizem SASL, uporabljen za povezovanje s strežnikom. Uporabljen bo API ldap_sasl_bind_s(). Parameter **-m** bo zanemarjen, če nastavite **-V 2**. Če **-m** ne podate, se uporabi preprosto overjanje.

-M Referenčne objekte upravlja kot navadne vnose.

-n Prikaže, kaj bi se zgodilo, vendar vnosov dejansko ne spremeni. Koristno pri razhroščevanju v povezavi z **-v**.

-N ime-potrdila
S to možnostjo podate oznako, ki je povezava s potrdilom odjemalca v datoteki baze podatkov ključev.

Opomba: Če je strežnik LDAP konfiguriran, da izvaja samo overjanje strežnika, potrdilo odjemalca ni potrebno. Če je strežnik LDAP konfiguriran za overjanje odjemalca in strežnika, bo najbrž potrebno potrdilo odjemalca. Parameter *ime-potrdila* ni obvezen, če ste kot privzetek določili par

potrdilo/zasebni ključ. Prav tako *ime-potrdila* ni potrebno, če v določeni datoteki baze podatkov obstaja posamezni par potrdila in zasebnega ključa. Ta parameter je zanemarjen, če ne podate niti **-Z** niti **-K**.

Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-o *tip-atr*

Za podajanje atributa, ki bo uporabljen za kriterij razvrščanja iskalnih rezultatov lahko uporabite parameter -o (order). Za nadaljnje definiranje sortirnega urejanja lahko uporabite več parametrov -o. V naslednjem primeru so rezultati iskanja razvrščani najprej po priimku (sn), nato pa po danem imenu, ki je razvrščeno v obratnem (padajočem) vrstnem redu, kot ga podaja predznak minus (-):

```
-o sn -o -givenname
```

Skladnja parametra za razvrščanje je torej takšna:

```
[-]<ime atributa>[:<OID pravila za primerjanje>]
```

kjer je

- ime atributa ime atributa, po katerem želite razvrščati
- OID pravila za primerjanje je neobvezni OID pravila za primerjanje, ki ga želite uporabiti za razvrščanje. Imeniški strežnik ne podpira atributa OID pravila za primerjanje, drugi strežniki LDAP pa ga lahko.
- Znak minus (-) kaže, da morajo biti rezultati razvrščeni v obratnem vrstnem redu.
- Kritičnost je vedno nastavljena na kritično.

Privzeta operacija ldapsearch je, da se razvrščanje vrnjenih rezultatov ne izvede.

-O največ-preskokov

Podaja največ preskokov, prek katerih gre knjižnica odjemalca pri sledenju referenčnim kazalcem. Privzeta vrednost za števec preskokov je 10.

-p vrata-ldap

Podajte nadomestna vrata TCP, na katerih posluša strežnik ldap. Privzeta vrata LDAP so 389. Če te možnosti ne podate, podate pa -Z, bodo uporabljena privzeta vrata SSL LDAP 636.

-P geslo-datoteke-ključev

Podaja geslo baze podatkov ključev. To geslo je potrebno za dostopanje do šifriranih informacij v datoteki baze podatkov ključev (ki lahko vsebuje enega ali več zasebnih ključev). Če je z datoteko baze podatkov ključev povezano skrita datoteka gesel, je geslo pridobljeno iz nje, parameter **-P** pa ni potreben. Ta parameter je zanemarjen, če ne podate niti **-Z** niti **-K**.

-q *velikost-strani*

Za podajanje razdelitve rezultatov iskanja na strani lahko uporabite dva parametra: -q (velikost strani poizvedbe) in -T (čas med iskanji v sekundah). V naslednjem primeru vrnejo rezultati iskanja naenkrat stran (25 vnosov) vsakih 15 sekund, dokler niso vrnjeni vsi rezultati za to iskanje. Odjemalec ldapsearch obravnava vsa nadaljevanja povezave za vsako zahtevo rezultatov na strani za čas trajanja iskalne operacije.

Ta parametra sta uporabna, če ima odjemalec omejena sredstva ali če je povezan prek povezave z nizko pasovno širino. Na splošno omogoča, da nadzorujete hitrost, s katero so vrnjeni podatki iz iskalne zahteve. Namesto da prejmete vse rezultate naenkrat, jih lahko prejmete na več straneh. Poleg tega lahko nadzorujete trajanje zamika med vsako zahtevo za stran, ki da odjemalcu dovolj časa za obdelavo rezultatov.

```
 -q 25  -T 15
```

Če podate parameter -v (verbose), ldapsearch izpiše, koliko vnosov je bilo vrnjenih po vsaki vrnitvi rezultatov iz strežnika, kot je na primer **Skupaj je bilo vrnjenih 30 vnosov**

Omogočenih je več parametrov -q, tako da lahko v času trajanja ene iskalne operacije podate različne velikosti strani. V naslednjem primeru vsebuje prva stran 15 vnosov, druga 20, tretji parameter pa konča operacijo vrnjenih rezultatov po straneh/iskanja:

```
-q 15 -q 20 -q 0
```

V naslednjem primeru vsebuje prva stran 15 vnosov, vse druge strani pa 20 vnosov in se nadaljujejo z zadnjo podano vrednostjo **-q**, dokler se operacija iskanja ne konča:

```
-q 15 -q 20
```

Privzeta operacija ldapsearch je vrnitev vseh vnosov v eni zahtevi. Za privzeto operacijo ldapsearch se ne izvede razdelitev na strani.

-R Ta možnost podaja, da se referenčnim kazalcem ne sme slediti samodejno.

-s območje
S to možnostjo podajte območje iskanja. območje je base, one ali sub, ki podajajo osnovni objekt, eno raven ali iskanje v poddrevesu. Privzeta vrednost je sub.

-t Poiskane vrednosti zapišete v niz začasnih datotek. Ta možnost je uporabna za delo z vrednostmi, ki niso ASCII, kot sta jpegPhoto ali zvok.

-T *sekund*
Čas med iskanji (v sekundah). Možnost **-T** je podprta samo, če podate možnost **-q**.

-v Uporabite način z razlago, z veliko diagnostičnimi podatki, ki se zapišejo v standardni izhod.

-V Podaja različico LDAP, ki jo bo uporabil pripomoček ldapmodify pri povezovanju s strežnikom LDAP. Po privzetku je vzpostavljena povezava LDAP V3. Če želite izrecno izbrati LDAP V3, podajte ″-V 3″. Za izvajanje kot aplikacija LDAP V2 podajte ″-V 2″. Aplikacija, kot je ldapmodify, izbere LDAP V3 kot želeni protokol, tako da namesto ldap_open uporabi ldap_init.

-w *geslo* **| ?**
Za overjanje uporabite ***geslo*** kot geslo. ? uporabite za tvorbo poziva za geslo. .

-z omejitev-velikosti
Omejitev rezultatov iskanja na največ vnosov. S tem lahko postavite zgornjo mejo števila vnosov, ki jih vrne operacija iskanja.

-Z To možnost uporabite, če povezava SSL komunicira s strežnikom LDAP. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

filter Podaja nizovno predstavitev filtra, ki bo uporabljen v iskanju. Preproste filtre lahko podate kot attributetype=attributevalue. Bolj kompleksne filtre uporabite kot zapis predpone v skladu z naslednjim zapisom BNF (Backus Naur Form):

```
<filter> ::='('<filtercomp>')'
<filtercomp> ::= <and>|<or>|<not>|<simple>
<and> ::= '&' <filterlist>
<or> ::= '|' <filterlist>
<not> ::= '!' <filter>
<filterlist> ::= <filter>|<filter><filterlist>
<simple> ::= <attributetype><filtertype>
<attributevalue>
<filtertype> ::= '='|'~='|'<='|'>='
```

Sestavek '~=' se uporablja za podajanje približne primerjave. Predstavitev <*attributetype*> in <*attributevalue*> mora biti v skladu z opisom ″RFC 2252, LDAP V3 Attribute Syntax Definitions″ . Če uporabite tip filtra is '=', je lahko <*attributevalue*> ena *, da sprejme preskus obstoja atributa ali pa lahko vsebuje besedilo in vmesne zvezdice (*) za primerjavo podnizov.

Filter ″mail=*″ na primer najde vse vnose z atributom mail. Filter ″mail=*@student.of.life.edu″ najde vse vnose, katerih atribut mail se konča s podanim nizom. Če želite v filter vključiti oklepaje, uporabite znak za poševnico nazaj (\).

Opomba: Filter, kot je "cn=Bob *", kjer je med Bob in zvezdico (*) presledek, primerja v IBM-ovem imeniku ime ″Bob Carter″, ne pa tudi ″Bobby Carter″. Presledek med ″Bob″ in univerzalnim znakom (*) vpliva na rezultat iskanja z uporabo filtrov.

Podrobnejše opis dovoljenih filtrov boste našli v temi ″RFC 2254, A String Representation of LDAP Search Filters″  .

Izhodni format

Če je najdenih eden ali več vnosov, je vsak med njimi zapisan v standardni izhod v naslednji obliki:

```
Razločevalno ime (DN)

ime_atributa=vrednost

ime_atributa=vrednost

ime_atributa=vrednost

...
```

Postavke se med seboj ločene z eno prazno vrstico. Če z možnostjo **-F** podate znak za ločilo, bo uporabljen namesto znaka `=’. Če uporabite možnost **-t**, je namesto dejanske vrednosti uporabljeno ime začasne datoteke. Če podate možnost **-A**, je zapisan samo del ″ime_atributa″.

Primeri

Ukaz:

```
ldapsearch "cn=john doe" cn telephoneNumber
```

izvede iskanje v poddrevesu (s privzeto iskalno osnovo) za vnose s commonName ″john doe″. Vrednosti za commonName in telephoneNumber sta prebrani in zapisani v standardnem izhodu. Če sta najdena dva vnosa, je izpis lahko podoben naslednjemu:

```
  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
```

Ukaz

```
ldapsearch -t "uid=jed" jpegPhoto audio
```

izvede iskanje v poddrevesu s privzeto iskalno osnovo za vnose z ID-jem uporabnika ″jed″. Vrednosti za jpegPhoto in zvok sta prebrani in zapisani v začasne datoteke. Če je najden en vnos z eno vrednostjo za vsakega od zahtevanih atributov, je izpis lahko podoben naslednjemu:

```
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
```

Ukaz

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

izvede enoravensko iskanje na ravni c=US za vse organizacije, katerih organizationName se začne z university. Rezultati iskanja bodo prikazani v formatu LDIF (glejte format za izmenjavo podatkov LDAP). Vrednosti atributov za organizationName in description bosta prebrani in natisnjeni v standardnem izhodu, ki je podoben naslednjemu:

```
dn: o=University of Alaska Fairbanks, c=US

  o: University of Alaska Fairbanks

  description: Preparing Alaska for a brave new tomorrow

  description: leaf node only


  dn: o=University of Colorado at Boulder, c=US

  o: University of Colorado at Boulder

  description: No personnel information

  description: Institution of education and research


  dn: o=University of Colorado at Denver, c=US

  o: University of Colorado at Denver

  o: UCD

  o: CU/Denver

  o: CU-Denver

  description: Institute for Higher Learning and Research


  dn: o=University of Florida, c=US

  o: University of Florida

  o: UFl

  description: Shaper of young minds
```

...

Ukaz

```
ldapsearch -b "c=US" -o ibm-slapdDN "objectclass=person" ibm-slapdDN
```

izvede iskanje v poddrevesu na ravni c=US za vse osebe. Če uporabite ta posebni atribut (ibm-slapdDN) za razvrščena iskanja, razvrsti rezultate iskanja po nizovni predstavitvi razločevalnega imena (DN-ja). Izhod je lahko podoben naslednjemu:

```
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
```

Ukaz

```
ldapsearch –h ime-gostitelja –o sn –b "o=ibm,c=us" "title=engineer"
```

vrne vse vnose v imeniku IBM-ovih uslužbencev, katerih naziv je ″engineer″, in razvrsti rezultate po priimku.

Ukaz

```
ldapsearch –h ime-gostitelja –o -sn –o cn –b "o=ibm,c=us" "title=engineer"
```

vrne vse vnose v imeniku IBM-ovih uslužbencev, katerih naziv je ″engineer″, in razvrsti rezultate po priimku (v padajočem vrstnem redu) in splošnem imenu (v rastočem vrstnem redu).

Ukaz

```
ldapsearch –h ime-gostitelja –q 5 –T 3 –b o=ibm,c=us "title=engineer"
```

vrne pet vnosov na stran z zakasnitvijo 3 sekund med vsemi stranmi za vse vnose v imeniku IBM-ovih uslužbencev, katerih naziv je ″engineer″.

Ta zgled prikazuje iskanja, kjer je vključen objekt referenčnega kazalca. Kot smo razložili v razdelku “Referenčni kazalci imenika LDAP” na strani 39, lahko vsebujejo imeniki LDAP imeniškega strežnika referenčne objekte, ki pa lahko vsebujejo samo naslednje:

- razločevalno ime (dn).
- objektni razred (objectClass).
- atribut referenčnih kazalcev (ref).

Denimo, da je v sistemu ’System_A’ shranjen naslednji vnos referenčnega kazalca:

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

Vsi atributi, povezani z vnosom, morajo biti v sistemu ’System_B’.

System_B vsebuje naslednji vnos:

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

Ko izda odjemalec zahtevo za ’System_A’, se strežnik LDAP v System_A odzove odjemalcu z URL-jem:

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

Odjemalec uporabi te informacije za izdajo zahteve za System_B. Če vsebuje vnos v System_A atribute poleg dn, objectclass in ref, jih strežnik zanemari (razen če podate oznako **-R**, ki kaže, da se sledenje referenčnim kazalcem ne bo izvajalo).

Če odjemalec iz strežnika sprejme odziv referenčnega kazalca, znova izda zahtevo, tokrat strežniku, na katerega se nanaša vrnjeni URL. Nova zahteva ima enako območje kot izvirna. Rezultati tega iskanja se spreminjajo glede na vrednost, ki jo podate za območje iskanja (**-b**).

Če podate -s base, kot kaže naslednji primer:

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

vrne iskanje vse atribute za vse vnose s ’sn=Jensen’, ki so v ’ou=Rochester, o=Big Company, c=US’ v System_A in System_B.

Če podate -s sub, kot je prikazano tukaj:

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

vrne iskanje vse atribute za vse vnose s ’sn=Jensen’, ki so v ali pod ’ou=Rochester, o=Big Company, c=US’ v System_A in System_B.

Če podate -s one, kot je prikazano tukaj:

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

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

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

Odjemalec, ki je na vrsti, predloži zahtevo:

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

Tudi to ne vrne nobenih rezultatov, ker je vnos

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
```

v

```
ou=Rochester, o=Big Company, c=US
```

Iskanje s -s one poskusi najti vse vnose na ravni pod

```
ou=Rochester, o=Big Company, c=US
```

Diagnosticiranje

Če se ne zgodi nobena napaka, je izhodni status 0. Napake povzročijo izhodni status, ki ni nič, in zapis diagnostičnega sporočila v standardno napako.

ldapchangepwd

Orodje za spreminjanje gesla LDAP.

Oris

```
ldapchangepwd -D povezovalni-dn -w geslo | ? -n novo-geslo | ?
[-C nabor-znakov] [-d raven-razhroščevanja][-h gostitelj-ldap] [-K datoteka-ključev]
[-m mehanizem] [-M]  [-N ime-potrdila] [-O največ-preskokov]
[-p vrata-ldap] [-P geslo-datoteke-ključev]  [-R] [-v] [-V različica]
[-Z] [-?]
```

Opis

Strežniku LDAP pošlje zahtevo za spreminjanje gesla. Omogoča spremembo gesla za imeniški vnos.

Možnosti

-C *nabor-znakov*
: Podaja, da so DN-ji, ki so posredovani kot vhod za pripomoček **ldapdelete**, predstavljeni z lokalnim naborom znakov, ki ga podaja nabor-znakov. Možnost **-C** *nabor-znakov* uporabite, če se kodna stran vhodnega niza razlikuje od vrednosti kodne strani opravila. Podprte vrednosti za nabor znakov boste našli v API-ju ldap_set_iconv_local_charset().

-d *raven-razhroščevanja*
: Raven razhroščevanja LDAP nastavi na raven-razhroščevanja.

-D*povezovalni-dni*
: Možnost ***povezovalni-dn*** uporabite za povezovanje z imenikom LDAP. ***povezovalni-dn*** je DN, predstavljen z nizom.

-h*gostitelj-ldap*
: Podajte nadomestnega gostitelja, na katerem se izvaja strežnik ldap.

-K*datoteka-ključev*
: S to možnostjo podate datoteko baze podatkov ključev SSL. Če datoteka baze podatkov ključev ni v trenutnem imeniku, podajte celotno ime datoteke baze podatkov ključev.

  Če pomožni program ne more določiti položaja baze podatkov ključev, bo uporabil programsko določen niz privzetih overjenih skrbnikov služb za pooblastila. Datoteka baze podatkov ključev vsebuje običajno enega ali več potrdil služb za pooblastila (CA), ki jim zaupajo odjemalci. Ti tipi potrdil X.509 so običajno poznani kot overjena potrdila.

  Ta parameter učinkovito omogoča stikalo **-Z**. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-m*mehanizem*
: Z ***mehanizmom*** podajte mehanizem SASL, ki bo uporabljen za povezavo s strežnikom. Uporabljen bo API ldap_sasl_bind_s(). Parameter **-m** bo zanemarjen, če nastavite **-V 2**. Če **-m** ne podate, se uporabi preprosto overjanje.

-M
: Referenčne objekte upravlja kot navadne vnose.

-n *novo-geslo* **| ?**
: Podaja novo geslo. ? uporabite za tvorbo poziva za geslo.

-N*ime-potrdila*
: S to možnostjo podate oznako, ki je povezava s potrdilom odjemalca v datoteki baze podatkov ključev. Če je strežnik LDAP konfiguriran, da izvaja samo overjanje strežnika, potrdilo odjemalca ni potrebno. Če je strežnik

LDAP konfiguriran za overjanje odjemalca in strežnika, bo najbrž potrebno potrdilo odjemalca. Parameter ***ime-potrdila*** ni obvezen, če ste kot privzetek določili par potrdilo/zasebni ključ. Prav tako ***ime-potrdila*** ni potrebno, če v določeni datoteki baze podatkov obstaja posamezni par potrdila in zasebnega ključa. Ta parameter je zanemarjen, če ne podate niti **-Z** niti **-K**. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-O *največ-preskokov*
Možnost ***največ-preskokov*** podaja največje dovoljeno število preskokov, prek katerih gre knjižnica odjemalca pri sledenju referenčnim kazalcem. Privzeta vrednost za števec preskokov je 10.

-p *vrata-ldap*
Podajte nadomestna vrata TCP, na katerih posluša strežnik ldap. Privzeta vrata LDAP so 389. Če ne podate možnosti **-p** in podate možnost **-Z**, bodo uporabljena privzeta vrata SSL LDAP 636.

-P*geslo-datoteke-ključev*
Podaja geslo baze podatkov ključev. To geslo je potrebno za dostopanje do šifriranih informacij v datoteki baze podatkov ključev, ki lahko vsebuje enega ali več zasebnih ključev. Če je z datoteko baze podatkov ključev povezano skrita datoteka gesel, je geslo pridobljeno iz nje, parameter **-P** pa ni potreben. Ta parameter je zanemarjen, če ne podate niti **-Z** niti **-K**.

-R Ta možnost podaja, da se referenčnim kazalcem ne sme slediti samodejno.

-v Uporabite način z razlago, z veliko diagnostičnimi podatki, ki se zapišejo v standardni izhod.

-V *različica*
Podaja različico LDAP, ki jo bo uporabil **ldapdchangepwd** pri povezovanju s strežnikom LDAP. Po privzetku je vzpostavljena povezava LDAP V3. Če želite izrecno izbrati LDAP V3, podajte **-V 3**. Za izvajanje kot aplikacija LDAP V2 podajte **-V 2**. Aplikacija, kot je **ldapdchangepwd**, izbere LDAP V3 kot želeni protokol, tako da namesto ldap_open uporabi ldap_init.

-w *geslo* **| ?**
Za overjanje uporabite ***geslo*** kot geslo. ? uporabite za tvorbo poziva za geslo.

-Z To možnost uporabite, če povezava SSL komunicira s strežnikom LDAP. Če uporabite za imeniški strežnik v i5/OS možnost -Z in ne -K ali -N, bo uporabljeno potrdilo, povezano z ID-jem odjemalske aplikacije imeniških storitev.

-? Prikaže skladenjsko pomoč za ldapchangepwd.

Primeri

Ukaz

```
ldapchangepwd -D cn=John Doe -w a1b2c3d4 -n wxyz9876
```

spremeni geslo za poimenovan vnos s commonName ″John Doe″ iz a1b2c3d4 v wxyz9876

Diagnosticiranje

Če se ne zgodi nobena napaka, je izhodni status 0. Napake povzročijo izhodni status, ki ni nič, in zapis diagnostičnega sporočila v standardno napako.

ldapdiff

Orodje za uskladitev strežnika za podvajanje LDAP.

Opomba: Ta ukaz se lahko zelo dolgo izvaja, če je potrebno podvojiti veliko število vnosov (in atributov za te vnose).

Oris

(Primerja in uskladi podatkovne vnose med dvema strežnikoma v okolju podvajanja.)

```
ldapdiff -b osnovni-DN -sh gostitelj -ch gostitelj [-a] [-C števec]
 [-cD dn] [-cK prostor-ključev] [-cw geslo] -[cN oznaka-ključa]
 [-cp vrata] [-cP geslo-prostora-ključev]  [-cZ] [-F] [-L ime-datoteke] [-sD dn] [-sK prostor-ključev]
 [-sw geslo] -[sN oznaka-ključa] [-sp vrata] [-sP geslo-prostora-ključev]
 [-sZ] [-v]
```

ali

(Primerja shemo med dvema strežnikoma.)

```
 ldapdiff -S -sh gostitelj -ch gostitelj [-a] [-C števec][-cD dn]
 [-cK prostor-ključev] [-cw geslo] -[cN oznaka-ključa] [-cp vrata]
 [-cP geslo-prostora-ključev] [-cZ] [-L ime-datoteke] [-sD dn]
 [-sK prostor-ključev] [-sw geslo] [-sN oznaka-ključa] [-sp vrata]
 [-sP geslo-prostora-ključev] [-sZ] [-v]
```

Opis

To orodje uskladi strežnik za podvajanje z njegovim glavnim strežnikom. Če želite prikazati skladenjsko pomoč za **ldapdiff**, vpišite naslednje:

```
ldapdiff -?
```

Možnosti

Za ukaz **ldapdiff** se uporabljajo naslednje možnosti. Obstajata dve podskupini, ki se nanašata posebej na oskrbniški ali potrošniški strežnik.

-a Podaja uporabo krmilnega elementa za upravljanje strežnika za pisanja v strežnik za podvajanje, ki je samo za branje.

-b *osnovni-DN*
osnovno-iskanja uporabite kot začetno točko za iskanje namesto privzete vrednosti. Če ne podate možnosti **-b**, bo ta pripomoček iskal definicijo osnove-iskanja v spremenljivki okolja LDAP_BASEDN.

-C *števec*
Šteje število vnosov, ki jih je potrebno popraviti. Če je najdeno več neujemanj, kot podaja števec, orodje obstaja.

-F To je možnost za popravilo. Če jo podate, bo vsebina potrošniškega strežnika za podvajanje spremenjena tako, da bo ustrezala vsebini oskrbniškega strežnika. Možnosti ne morete uporabiti, če podate tudi **-S**.

-L Če ne podate možnosti **-F**, uporabite to možnost za tvorbo datoteke LDIF za izhodne podatke. S to datoteko LDIF lahko ažurirate potrošnika in odstranite razlike.

-S Podaja primerjavo sheme na obeh strežnikih.

-v Uporabite način z razlago, z veliko diagnostičnimi podatki, ki se zapišejo v standardni izhod.

Možnosti za oskrbnika podvajanja

Naslednje možnosti se uporabljajo za potrošniški strežnik in so v imenu možnosti z začetnico ’s’.

-sD *dn* ***dn*** za povezovanje z imenikom LDAP. ***dn*** je DN, predstavljen z nizom.

-sh *gostitelj*
Podaja ime gostitelja.

-sK *prostor-ključev*
Podaja ime datoteke baze podatkov ključev SSL s privzeto pripono **kdb**. Če tega parametra ne podate ali če je vrednost prazen niz (-sK″″), je uporabljen sistemski prostor ključev. Če datoteka baze podatkov ključev ni v trenutnem imeniku, podajte celotno ime datoteke baze podatkov ključev.

-sN *oznaka-ključa*
S to možnostjo podate oznako, ki je povezava s potrdilom odjemalca v datoteki baze podatkov ključev. Če

podate oznako, ne da bi podali prostor ključev, je oznaka identifikator aplikacije v Upravljalniku digitalnih potrdil (DCM-ju). Privzeta oznaka (id aplikacije) je QIBM_GLD_DIRSRV_CLIENT. Če je strežnik LDAP konfiguriran, da izvaja samo overjanje strežnika, potrdilo odjemalca ni potrebno. Če je strežnik LDAP konfiguriran za overjanje odjemalca in strežnika, je potrdilo odjemalca potrebno. ***oznaka-ključa*** ni potrebno, če določite par privzeto potrdilo/zasebni ključ. ***oznaka-ključa*** tudi ni potrebna, če obstaja v določeni datoteki baze podatkov ključev en par potrdila/zasebnega ključa. Ta parameter je zanemarjen, če ne podate niti **-sZ** niti **-sK**.

-sp *vrata-ldap*
Podajte nadomestna vrata TCP, na katerih posluša strežnik ldap. Privzeta vrata LDAP so 389. Če ne podate možnosti **-sp** in podate možnost **-sZ**, bodo uporabljena privzeta vrata SSL LDAP 636.

-sP *geslo-prostora-ključev*
Podaja geslo baze podatkov ključev. To geslo je potrebno za dostopanje do šifriranih informacij v datoteki baze podatkov ključev, ki lahko vsebuje enega ali več zasebnih ključev. Če je z datoteko baze podatkov ključev povezana skrita datoteka gesel, je geslo pridobljeno iz nje, in parameter **-sP** ni potreben. Ta parameter je zanemarjen, če ne podate niti **-sZ** niti **-sK**. Geslo ne bo uporabljeno, če obstaja skrita datoteka za prostor ključev, ki ga uporabljate.

-st *tip-overjenega-prostora*
Podajte oznako, povezano s potrdilom odjemalca v overjeni datoteki baze podatkov. Če je strežnik LDAP konfiguriran, da izvaja samo overjanje strežnika, potrdilo odjemalca ni potrebno. Če je strežnik LDAP konfiguriran za overjanje odjemalca in strežnika, bo najbrž potrebno potrdilo odjemalca. ***tip-overjenega-prostora*** ni potreben, če kot privzetek določite par potrdilo/zasebni ključ. ***tip-overjenega-prostora*** prav tako ni potreben, če obstaja v določeni datoteki baze podatkov ključev en par potrdila/zasebnega ključa. Ta parameter je zanemarjen, če ne podate niti **-sZ** niti **-sT**.

-sZ To možnost uporabite, če povezava SSL komunicira s strežnikom LDAP.

Možnosti za potrošnika podvajanja

Naslednje možnosti se uporabljajo za potrošniški strežnik in so v imenu možnosti z začetnico 'c'. Če podate -cZ, ne da bi podali vrednosti za -cK, -cN ali -cP, zaradi priročnosti uporabljajo te možnosti enako vrednost, kot je podana za možnosti SSL oskrbnika. Če želite nadomestiti možnosti oskrbnika in uporabiti privzete nastavitve, podate -cK ″″ -cN ″″ -cP ″″.

-cD *dn* ***dn*** za povezovanje z imenikom LDAP. ***dn*** je DN, predstavljen z nizom.

-ch *gostitelj*
Podaja ime gostitelja.

-cK *prostor-ključev*
Podajte ime datoteke baze podatkov ključev SSL s privzeto pripono kdb. Če je vrednost prazen niz (-sK″″), je uporabljen sistemski prostor ključev. Če datoteka baze podatkov ključev ni v trenutnem imeniku, podajte celotno ime datoteke baze podatkov ključev.

-cN *oznaka-ključa*
S to možnostjo podate oznako, ki je povezava s potrdilom odjemalca v datoteki baze podatkov ključev. Če je strežnik LDAP konfiguriran, da izvaja samo overjanje strežnika, potrdilo odjemalca ni potrebno. Če podate oznako, ne da bi podali prostor ključev, je oznaka identifikator aplikacije v Upravljalniku digitalnih potrdil (DCM-ju). Privzeta oznaka (id aplikacije) je QIBM_GLD_DIRSRV_CLIENT. Če je strežnik LDAP konfiguriran za overjanje odjemalca in strežnika, je potrdilo odjemalca potrebno. ***oznaka-ključa*** ni potrebna, če določite par privzeto potrdilo/zasebni ključ. ***oznaka-ključa*** tudi ni potrebna, če obstaja v določeni datoteki baze podatkov ključev en par potrdila/zasebnega ključa. Ta parameter je zanemarjen, če ne podate niti **-cZ** niti **-cK**.

-cp *vrata-ldap*
Podajte nadomestna vrata TCP, na katerih posluša strežnik ldap. Privzeta vrata LDAP so 389. Če ne podate možnosti **-cp** in podate možnost **-cZ**, bodo uporabljena privzeta vrata SSL LDAP 636.

-cP *geslo-prostora-ključev*

Podaja geslo baze podatkov ključev. To geslo je potrebno za dostopanje do šifriranih informacij v datoteki baze podatkov ključev, ki lahko vsebuje enega ali več zasebnih ključev. Če je z datoteko baze podatkov ključev povezano skrita datoteka gesel, je geslo pridobljeno iz nje, parameter **-cP** pa ni potreben. Ta parameter je zanemarjen, če ne podate niti **-cZ** niti **-cK**.

-cw *geslo* **| ?**

geslo uporabite kot geslo za overjanje. ? uporabite za tvorbo poziva za geslo.

-cZ To možnost uporabite, če povezava SSL komunicira s strežnikom LDAP.

Primeri

```
ldapdiff -b <osnovni-DN> -sh <gostiteljsko-ime-oskrbnika> -ch
<gostiteljsko-ime-potrošnika> [options]
```

ali

```
ldapdiff -S  -sh <gostiteljsko-ime-oskrbnika> -ch
<gostiteljsko-ime-potrošnika> [options]
```

Diagnosticiranje

Če se ne zgodi nobena napaka, je izhodni status 0. Napake povzročijo izhodni status, ki ni nič, in zapis diagnostičnega sporočila v standardno napako.

Opombe o uporabi SSL s pripomočki ukazne vrstice LDAP

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

Razdelek “Plast zaščitenih vtičnic (SSL) in zaščita plasti prenosa z imeniškim strežnikom” na strani 40 razlaga uporabo SSL s strežnikom LDAP imeniškega strežnika. Te informacije zajemajo upravljanje in izdelovanje overjenih služb za pooblastila z upravljalnikom digitalnih potrdil.

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

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

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

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

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

Format za izmenjavo podatkov LDAP (LDIF)

V tej dokumentaciji opisujemo format za izmenjavo podatkov LDAP (LDIF), kot ga uporabljajo pripomočki ldapmodify, ldapsearch in ldapadd. Format LDIF, ki ga podajamo tu, podpirajo tudi strežniški pripomočki, ki jih nudi IBM-ov imenik.

LDIF se uporablja za predstavitev vnosov LDAP v besedilni obliki. Osnovna oblika vnosa LDIF je naslednja:

```
dn: <razločevalno-ime>
<tip-atributa> : <vrednost-atributa>
<tip-atributa> : <vrednost-atributa>
...
```

Vrstico lahko nadaljujete tako, da začnete naslednjo vrstico z enim znakom za presledek ali tabulatorjem, kot v naslednjem primeru:

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

Več vrednosti atributov je podanih v ločenih vrsticah:

```
cn: John E Doe
cn: John Doe
```

Če vsebuje <*vrednost-atributa*> znak, ki ni US-ASCII ali se začne s presledkom ali dvopičjem ':', sledi <*tipu-atributa*> dvojno dvopičje, vrednost pa je kodirana v zapisu osnove-64. Vrednost ″ se začne s presledkom″ je na primer kodirana takole:

```
cn:: IGJlZ2lucyB3aXRoIGEgc3BhY2U=
```

Več vnosov v isti datoteki LDIF je ločenih s prazno vrstico. Več praznih vrstic se smatra za logičen konec datoteke.

Dodatne informacije boste našli v naslednjih temah:

- "Primer datoteke LDIF"
- "Podpora za LDIF različice 1" na strani 183
- "Primeri za LDIF različice 1" na strani 183

Primer datoteke LDIF

Sledi primer datoteke LDIF, ki vsebuje tri vnose.

```
dn: cn=John E Doe, o=University of High
 er Learning, c=US
cn: John E Doe
cn: John Doe
objectclass: person
sn: Doe

dn: cn=Bjorn L Doe, o=University of High
 er Learning, c=US
cn: Bjorn L Doe
cn: Bjorn Doe
objectclass: person
sn: Doe

dn: cn=Jennifer K. Doe, o=University of High
 er Learning, c=US
cn: Jennifer K. Doe
cn: Jennifer Doe
objectclass: person
sn: Doe
```

```
jpegPhoto:: /9j/4AAQSkZJRgABAAAAAQABAAD/2wBDABALD
 A4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQ
 ERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARESEhgVG
...
```

jpegPhoto v vnosu Jennifer Jensen je kodiran z osnovo-64. Tudi besedilne vrednosti atributov lahko podate v formatu osnove-64, toda v tem primeru mora biti kodiranje osnove-64 v kodni strani žičnega formata za protokol (to je nabor znakov IA5 za LDAP V2 in kodiranje UTF-8 za LDAP V3).

Podpora za LDIF različice 1

Odjemalske pripomočke (ldapmodify in ldapadd) smo izboljšali tako, da prepoznajo najnovejšo različico datoteke LDIF, ki je določena s prisotnostjo oznake ″različica: 1″ v oglavju datoteke. Za razliko od izvirnih različic datoteke LDIF novejše različice podpirajo vrednosti atributov, ki so predstavljene v formatu UTF-8 (namesto v zelo omejenem US-ASCII).

Toda ročna izdelava datoteke LDIF, ki vsebuje vrednosti UTF-8, je lahko dokaj težka. Zaradi poenostavitve tega postopka je podprta razširitev nabora znakov za format LDIF. Ta razširitev omogoča, da podate ime nabora znakov IANA v oglavju datoteke LDIF (skupaj s številko različice). Podprt je tudi omejen niz naborov znakov IANA.

Format LDIF različice 1 podpira tudi datotečne URL-je. To nudi prožnejši način za definiranje specifikacije datoteke. Datotečni URL-ji imajo naslednjo obliko:

```
atribut:< file:///pot          (skladnja poti je odvisna od platforme)
```

Tole sta na primer veljavna datotečna spletna naslova:

```
jpegphoto:< file:///d:\temp\photos\myphoto.jpg    (poti v slogu DOS/Windows)
jpegphoto:< file:///etc/temp/photos/myphoto.jpg   (poti v slogu Unix)
```

Opomba: Pripomočki IBM-ovega imenika podpirajo novo specifikacijo datotečnega URL-ja, kot tudi star slog (″jpegphoto: /etc/temp/myphoto″), ne glede na specifikacijo različice. To pomeni, da lahko uporabite novi format datotečnega URL-ja, ne da bi dodali v datoteke LDIF oznako različice.

Primeri za LDIF različice 1

Uporabite lahko neobvezno oznako charset, da bodo pripomočki samodejno opravili pretvorbo iz podanega nabora znakov v UTF-8, kot v naslednjem primeru:

```
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
```

V tem primeru so vse vrednosti, ki sledijo imenu atributa in enojno dvopičje, prevedeni iz nabora znakov ISO-8859-1 v UTF-8. Vrednosti, ki sledijo imenu atributa in dvojnemu dvopičju (kot je description:: V2hhdCBhIGNhcm...), morajo biti kodirane z osnovo-64, in morajo biti dvojiški ali znakovni nizi UTF-8. Tudi vrednosti, ki so prebrane iz datoteke, kot je na primer atribut jpegPhoto, ki je v prejšnjem primeru podan s spletnim naslovom, morajo biti dvojiške ali UTF-8. Za te vrednosti se ne opravi noben prevod iz podanega ″charset″ v UTF-8.

V tem primeru datoteke LDIF brez oznake charset se pričakuje, da bo vsebina v UTF-8 ali v UTF-8, kodiranem z osnovo-64 ali dvojiški podatki, kodirani z osnovo-64:

```
# Datoteka LDIF IBM Directorysample
 #
 # Pripono "o=IBM, c=US" definirajte, preden poskusite naložiti
 # te podatke.
```

```
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
```

To datoteko lahko uporabite tudi brez informacij v glavi version: 1, kot je bilo to v prejšnjih izdajah IBM-ovega imenika:

```
# Datoteka LDIF IBM Directorysample
#
# Pripono "o=IBM, c=US" definirajte, preden poskusite naložiti
# te podatke.

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
```

Opomba: Besedilne vrednosti atributov lahko podate v formatu osnove-64.

Konfiguracijska shema imeniškega strežnika

Te informacije opisujejo imeniško informacijsko drevo (DIT) in atribute, uporabljene za konfiguriranje datoteke ibmslapd.conf. V prejšnjih izdajah so bile konfiguracijske nastavitve imenika shranjene v lastniškem formatu v konfiguracijski datoteki, zdaj pa so v konfiguracijski datoteki shranjene s formatom LDIF.

Konfiguracijska datoteka se imenuje ibmslapd.conf. Zdaj je na voljo tudi shema, ki jo uporablja konfiguracijska datoteka. Tipe atributov boste našli v datoteki v3.config.at, objektne razrede pa v datoteki v3.config.oc. Atribute lahko spremenite z ukazom ldapmodify. Dodatne informacije o ukazu ldapmodify boste našli v razdelku “ldapmodify in ldapadd” na strani 157.

- “Imeniško informacijsko drevo”
- “Atributi” na strani 193

Imeniško informacijsko drevo

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 vnos zgornje ravni v DIT konfiguracije, in hrani podatke, ki so za strežnik globalno zanimivi, čeprav v praksi vsebuje tudi raznotere podatke. Vsak atribut iz tega vnosa prihaja iz prvega razdelka (globalna stanca) ibmslapd.conf.

Število 1 (obvezno)

Objektni razred
ibm-slapdTop

Obvezni atributi

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

Izbirni atributi

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (zastarel)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion

cn=Admin

DN cn=Admin, cn=Configuration

Opis Globalne konfiguracijske nastavitve za IBM Admin Daemon

Število 1 (obvezno)

Objektni razred
ibm-slapdAdmin

Obvezni atributi

- cn
- ibm-slapdErrorLog
- ibm-slapdPort

Izbirni atributi

- ibm-slapdSecurePort

cn=Event Notification

DN cn=Event Notification, cn=Configuration

Opis Globalne nastavitve obveščanja o dogodkih za imeniški strežnik.

Število 0 ali 1 (neobvezno in potrebno samo, če želite omogočiti obveščanje o dogodkih)

Objektni razred
ibm-slapdEventNotification

Obvezni atributi

- cn
- ibm-slapdEnableEventNotification
- objectClass

Izbirni atributi

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

cn=Front End

DN cn=Front End, cn=Configuration

Opis Globalne nastavitve okolja, ki jih uporabi strežnik pri zagonu.

Število 0 ali 1 (neobvezno)

Objektni razred
ibm-slapdFrontEnd

Obvezni atributi

- cn
- objectClass

Izbirni 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 nastavitve overjanja Kerberos za imeniški strežnik.

Število 0 ali 1 (neobvezno)

Objektni razred
ibm-slapdKerberos

Obvezni atributi

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

Izbirni atributi

- None

cn=Master Server

DN cn=Master Server, cn=Configuration

Opis Pri konfiguriranju strežnika za podvajanje ta vnos hrani povezovalne poverilnice in URL referenčnega kazalca glavnega strežnika.

Število 0 ali 1 (neobvezno)

Objektni razred
ibm-slapdReplication

Obvezni atributi

- cn
- ibm-slapdMasterPW (obvezno, če ne uporabljate overjanja Kerberos)

Izbirni atributi

- ibm-slapdMasterDN
- ibm-slapdMasterPW (neobvezno, če uporabljate overjanje Kerberos)
- ibm-slapdMasterReferral
- objectClass

cn=Referral

DN cn=Referral, cn=Configuration

Opis Ta vnos vsebuje vse vnose referenčnega kazalca iz prvega razdelka (globalna stanca) ibmslapd.conf. Če referenčni kazalci ne obstajajo (ni jih po privzetku), je ta vnos neobvezen.

Število 0 ali 1 (neobvezno)

Objektni razred
ibm-slapdReferral

Obvezni atributi

- cn
- ibm-slapdReferral
- objectClass

Izbirni atributi

- None

cn=Schemas

DN cn=Schemas, cn=Configuration

Opis Ta vnos služi kot vsebnik za sheme. Dejansko ni potreben, saj lahko sheme ločite z objektnim razredom ibm-slapdSchema, vključen pa je zaradi izboljšanja berljivosti DIT.

Trenutno je dovoljen samo en vnos sheme: cn=IBM Directory.

Število 1 (obvezno)

Objektni razred
Container

Obvezni atributi

- cn
- objectClass

Izbirni atributi

- None

cn=IBM Directory

DN cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Ta vnos vsebuje vse konfiguracijske podatke sheme iz prvega razdelka (globalna stanca) ibmslapd.conf. Služi tudi kot vsebnik za vsa ozadja, ki uporabljajo shemo. Več shem trenutno ni podprtih, toda če bi bile, bi obstajal en vnos ibm-slapdSchema na shemo. Predvideva se, da več shem ni združljivih, zato lahko povežete ozadje samo z eno shemo.

Število 1 (obvezno)

Objektni razred
ibm-slapdSchema

Obvezni atributi

- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

Izbirni atributi

- ibm-slapdSchemaAdditions

cn=Config Backends

DN cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Ta vnos služi kot vsebnik za Config backends.

Število 1 (obvezno)

Objektni razred
Container

Obvezni atributi

- cn
- objectClass

Izbirni atributi
None

cn=ConfigDB

DN cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Konfiguracijsko ozadje z konfiguracijo strežnika IBM Directory server.

Število 0 - n (neobvezno)

Objektni razred
ibm-slapdConfigBackend

Obvezni atributi

- ibm-slapdSuffix
- ibm-slapdPlugin

Izbirni atributi

- ibm-slapdReadOnly

cn=RDBM Backends

DN cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Ta vnos služi kot vsebnik za ozadja RDBM in učinkovito nadomešča vrstico database rdbm iz ibmslapd.conf, saj določi vse podvnose kot ozadja DB2. Ta vnos dejansko ni potreben, saj lahko ločite ozadja RDBM z objektnim razredom ibm-slapdRdbmBackend, vključen pa je zaradi izboljšanja berljivosti DIT.

Število 0 ali 1 (neobvezno)

Objektni razred
Container

Obvezni atributi

- cn
- objectClass

Izbirni atributi

- None

cn=Directory

DN cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Ta vnos vsebuje vse konfiguracijske nastavitve baze podatkov za ozadje privzete baze podatkov RDBM.

Čeprav lahko izdelate več ozadij s poljubnimi imeni, funkcija upravljanja strežnika sklepa, da je ″cn=Directory″ glavno imeniško ozadje, ″cn=Change Log″ pa neobvezno ozadje za spremembo dnevnika. Prek funkcije za upravljanje strežnika lahko konfigurirate samo pripone, ki so prikazane v ″cn=Directory″ (razen pripone changelog, ki jo nastavite transparentno, tako da omogočite changelog).

Število 0 - n (neobvezno)

Objektni razred
ibm-slapdRdbmBackend

Obvezni atributi

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Izbirni 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

Opomba: Če uporabljate **ibm-slapdUseProcessIdPw**, morate spremeniti shemo, tako da bo **ibm-slapdDbUserPW** neobvezen.

cn=Change Log

DN cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Ta vnos vsebuje vse konfiguracijske nastavitve baze podatkov za ozadje spreminjanja dnevnika.

Število 0 - n (neobvezno)

Objektni razred
ibm-slapdRdbmBackend

Obvezni atributi

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Izbirni 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

Opomba: Če uporabljate **ibm-slapdUseProcessIdPw**, morate spremeniti shemo, tako da bo **ibm-slapdDbUserPW** neobvezen.

cn=LDCF Backends

DN cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Ta vnos služi kot vsebnik za ozadja LDCF, in učinkovito nadomešča vrstico database ldcf iz ibmslapd.conf, tako da določi vse podvnose kot ozadja LDCF. Dejansko ni potreben, saj lahko ozadja LDCF ločite z objektnim razredom ibm-slapdLdcfBackend, vključen pa je zaradi izboljšanja berljivosti DIT.

Število 1 (obvezno)

Objektni razred
Container

Obvezni atributi

- cn
- objectClass

Izbirni atributi

- ibm-slapdPlugin

cn=SchemaDB

DN cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Ta vnos vsebuje vse konfiguracijske podatke baze podatkov iz razdelka baze podatkov ldcf iz ibmslapd.conf.

Število 1 (obvezno)

Objektni razred
ibm-slapdLdcfBackend

Obvezni atributi

- cn
- objectClass

Izbirni atributi

- ibm-slapdPlugin
- ibm-slapdSuffix

cn=SSL

DN cn=SSL, cn=Configuration

Opis Globalne povezovalne nastavitve SSL za imeniški strežnik.

Število 0 ali 1 (neobvezno)

Objektni razred
ibm-slapdSSL

Obvezni atributi

- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

Izbirni atributi

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

  Opomba: **ibm-slapdSslCipherSpecs** je zdaj opuščen. Namesto njega uporabite **ibm-slapdSslCipherSpec**. Če uporabite **ibm-slapdSslCipherSpecs**, bo strežnik pretvoril podprti atribut.
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW

cn=CRL

DN cn=CRL, cn=SSL, cn=Configuration

Opis Ta vnos vsebuje podatke seznama za preklic potrdil iz prvega razdelka (globalna stanca) ibmslapd.conf. Potreben je samo, če je ″ibm-slapdSslAuth = serverclientauth″ v vnosu cn=SSL in so bila odjemalska potrdila izdana za preverjanje CRL.

Število 0 ali 1 (neobvezno)

Objektni razred
ibm-slapdCRL

Obvezni atributi

- cn
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPort
- objectClass

Izbirni atributi

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword

cn=Transaction

DN cn = Transaction, cn = Configuration

Opis Podaja podporne nastavitve za globalne transakcije. Podpora za transakcije je omogočena z dodatkom:

```
extendedop /QSYS.LIB/QGLDTRANEX.SRVPGM tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

Strežnik (**slapd**) naloži ta dodatek samodejno pri zagonu, če je **ibm-slapdTransactionEnable = TRUE**. Dodatka ni potrebno izrecno dodati v **ibmslapd.conf**.

Število 0 ali 1 (neobvezno in potrebno samo, če želite uporabljati transakcije)

Objektni razred
ibm-slapdTransaction

Obvezni atributi

- cn

- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

Izbirni atributi

- None

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 To je atribut splošnega imena X.500, ki vsebuje ime objekta.

Skladnja
Imeniški niz

Največja dolžina
256

Vrednost
Več vrednosti

ibm-slapdACIMechanism

Opis Določa, kateri model ACL bo uporabljal strežnik. (podprt samo v i5/OS od različice 3.2 naprej, v drugih platformah pa zanemarjen)

- Model ACL 1.3.18.0.2.26.1 = IBM SecureWay v3.1
- Model ACL 1.3.18.0.2.26.2 = IBM SecureWay v3.2

Privzetek
Model ACL 1.3.18.0.2.26.2 = IBM SecureWay v3.2

Skladnja
Imeniški niz

Največja dolžina
256

Vrednost
Več vrednosti

ibm-slapdACLAccess

Opis Krmili, ali je dostop do ACL-jev omogočen. Če je nastavljen na TRUE, je dostop do ACL-jev omogočen, če pa je nastavljen na FALSE, je onemogočen.

Privzetek
TRUE

Skladnja
Boolova vrednost

Največja dolžina
5

Vrednost
Ena vrednost

ibm-slapdACLCache

Opis Krmili, ali strežnik shrani informacije o ACL-jih v predpomnilnik ali ne.

- Če je vrednost TRUE, strežnik shrani informacije o ACL-jih v predpomnilnik.
- Če je vrednost FALSE, strežnik informacij o ACL-jih ne shrani v predpomnilnik.

Privzetek
TRUE

Skladnja
Boolova vrednost

Največja dolžina
5

Vrednost
Ena vrednost

ibm-slapdACLCacheSize

Opis Največje število vnosov, ki bodo shranjeni v predpomnilniku ACL.

Privzetek
25000

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdAdminDN

Opis Povezovalni DN skrbnika za imeniški strežnik.

Privzetek
cn=root

Skladnja
DN

Največja dolžina
Neomejeno

Vrednost
Ena vrednost

ibm-slapdAdminPW

Opis Povezovalno geslo skrbnika za imeniški strežnik.

Privzetek
secret

Skladnja
Dvojiško število

Največja dolžina
128

Vrednost
Ena vrednost

ibm-slapdBulkloadErrors

Opis Datotečna pot ali naprava na gostiteljskem računalniku ibmslapd, kamor bodo zapisana sporočila o napaki pri preveliki obremenitvi.

Privzetek
/var/bulkload.log

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
1024

Vrednost
Ena vrednost

ibm-slapdChangeLogMaxEntries

Opis Ta atribut uporablja dodatek changelog za podajanje največjega števila vnosov spreminjanja dnevnika, dovoljenega v bazi podatkov RDBM. Vsak changelog ima lasten atribut changeLogMaxEntries.

```
Minimum = 0 (neomejeno)
Maksimum = 2,147,483,647 (32-bitno celo število s predznakom)
```

Privzetek
0

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdCLIErrors

Opis Datotečna pot ali naprava na gostiteljskem računalniku ibmslapd, kamor bodo zapisana sporočila o napaki CLI.

Privzetek
/var/db2cli.log

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
1024

Vrednost
Ena vrednost

ibm-slapdConcurrentRW

Opis Če izberete nastavitev TRUE, omogočite sočasno izvajanje iskanj z ažuriranji. Omogočite tudi ’umazana branja’, kar pomeni, da rezultati morda ne bodo skladni s potrjenim stanjem baze podatkov.

Opozorilo: Ta atribut je opuščen.

Privzetek
FALSE

Skladnja
Boolova vrednost

Največja dolžina
5

Vrednost
Ena vrednost

ibm-slapdDB2CP

Opis Podaja kodno stran imeniške baze podatkov. Kodna stran za baze podatkov UTF-8 je 1208.

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdDBAlias

Opis Vzdevek baze podatkov DB2.

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
8

Vrednost
Ena vrednost

ibm-slapdDbConnections

Opis Podajte število povezav DB2, ki jih bo strežnik namenil ozadju DB2. Vrednost mora biti med 5 in 50 (vključno).

Opomba: Nad vrednostjo te smernice prevlada spremenljivka okolja ODBCCONS.
Če je vrednost za ibm-slapdDbConnections (ali ODBCCONS) manj kot 5 ali več kot 50, bo strežnik uporabil vrednost 5 oziroma 50. Za podvajanje bo izdelana ena dodatna povezava (tudi če podvajanje ni definirano), za spreminjanje dnevnika pa dve dodatni povezavi (če je spreminjanje dnevnika omogočeno).

Privzetek
15

Skladnja
Celo število

Največja dolžina
50

Vrednost
Ena vrednost

ibm-slapdDbInstance

Opis Podaja primerek baze podatkov DB2 za to ozadje.

Privzetek
ldapdb2

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
8

Vrednost
Ena vrednost

Opomba: Vsi objekti ibm-slapdRdbmBackend morajo uporabljati enak ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW in nabor znakov DB2.

ibm-slapdDbLocation

Opis Pot datotečnega sistema, kjer je shranjena baza podatkov ozadja.

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
1024

Vrednost
Ena vrednost

ibm-slapdDbName

Opis Podaja ime baze podatkov DB2 za to ozadje.

Privzetek
ldapdb2

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
8

Vrednost
Ena vrednost

ibm-slapdDbUserID

Opis Podaja ime uporabnika, s katerim bo izvedena povezava z bazo podatkov DB2 za to ozadje.

Privzetek
ldapdb2

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
8

Vrednost
Ena vrednost

Opomba: Vsi objekti ibm-slapdRdbmBackend morajo uporabljati enak ibm-slapdDbInstance ibm-slapdDbUserID, ibm-slapdDbUserPW in nabor znakov DB2.

ibm-slapdDbUserPW

Opis Podaja geslo uporabnika, s katerim bo izvedena povezava z bazo podatkov DB2 za to ozadje. Geslo je lahko v čistem besedilu ali šifrirano z imask.

Privzetek
ldapdb2

Skladnja
Dvojiško število

Največja dolžina
128

Vrednost
Ena vrednost

Opomba: Vsi objekti ibm-slapdRdbmBackend morajo uporabljati enak ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW in nabor znakov DB2.

ibm-slapdEnableEventNotification

Opis Podaja, ali bo obveščanje o dogodkih omogočeno. Izbrati morate vrednost TRUE ali FALSE.

Če uporabite FALSE, strežnik zavrne vse odjemalske zahteve za registriranje obveščanja o dogodkih z razširjenim rezultatom LDAP_UNWILLING_TO_PERFORM.

Privzetek
TRUE

Skladnja
Boolova vrednost

Največja dolžina
5

Vrednost
Ena vrednost

ibm-slapdEntryCacheSize

Opis Največje število vnosov, ki bodo shranjeni v predpomnilniku vnosov.

Privzetek
25000

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdErrorLog

Opis Podaja datotečno pot ali napravo na računalniku imeniškega strežnika, kamor bodo zapisana sporočila o napakah.

Privzetek
/var/ibmslapd.log

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
1024

Vrednost
Ena vrednost

ibm-slapdFilterCacheBypassLimit

Opis Iskalni filtri, ki primerjajo več vnosov, kot podaja to število, ne bodo dodani v predpomnilnik iskalnih filtrov. Ker je v ta predpomnilnik vključen seznam ID-jev vnosov, ki so ustrezali filtru, ta nastavitev pomaga omejiti uporabo pomnilnika. Vrednost 0 kaže, da omejitve ni.

Privzetek
100

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdFilterCacheSize

Opis Podaja največje število vnosov, ki bodo shranjeni v predpomnilniku iskalnih filtrov.

Privzetek
25000

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdIdleTimeOut

Opis Najdaljši čas, ko povezava LDAP ostane odprta, če ni dejavna. Čas mirovanja za povezavo LDAP je čas (v sekundah) med zadnjo dejavnostjo povezave in trenutnim časom. Če povezava poteče na osnovi časa mirovanja, ki je večji od vrednosti tega atributa, strežnik LDAP počisti in konča povezavo LDAP, tako da je na voljo za druge vhodne zahteve.

Privzetek
300

Skladnja
Celo število

Dolžina
11

Števec Eden

Uporaba
Imeniška operacija

Uporabniško spreminjanje
Da

Razred dostopa
Kritičen

Obvezen
Ne

ibm-slapdIncludeSchema

Opis Podaja datotečno pot na strežniškem računalniku imeniškega strežnika, ki vsebuje definicije shem.

Privzetek

/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

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
1024

Vrednost
Več vrednosti

ibm-slapdKrbAdminDN

Opis Podaja ID Kerberos za skrbnika LDAP (kot je na primer ibm-kn=admin1@realm1). Uporablja se, če uporabite overjanje Kerberos za overjanje skrbnika pri prijavi v vmesnik strežnika za upravljanje. To možnost lahko podate namesto ali poleg adminDN in adminPW.

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
128

Vrednost
Ena vrednost

ibm-slapdKrbEnable

Opis Podaja, ali strežnik podpira overjanje Kerberos. Vrednost mora biti TRUE ali FALSE.

Privzetek
TRUE

Skladnja
Boolova vrednost

Največja dolžina
5

Vrednost
Ena vrednost

ibm-slapdKrbIdentityMap

Opis Podaja, ali bo uporabljena preslikava identitet Kerberos. Izbrati morate vrednost TRUE ali FALSE. Če uporabite vrednost TRUE, bo strežnik pri overjanju odjemalca z ID-jem Kerberos poiskal vse lokalne uporabnike z ujemajočimi se poverilnicami Kerberos in dodal te uporabniške DN-je v povezovalne poverilnice povezave. S tem omogočite uporabnost ACL-jev, ki temeljijo na DN-jih uporabnikov, pri overjanju Kerberos.

Privzetek
FALSE

Skladnja
Boolova vrednost

Največja dolžina
5

Vrednost
Ena vrednost

ibm-slapdKrbKeyTab

Opis Podaja datoteko tabulatorskih ključev Kerberos strežnika LDAP. Ta datoteka vsebuje zasebni ključ strežnika LDAP, ki je povezan z njegovo šifro Kerberos. Datoteka mora biti zaščitena (kot strežniška datoteka baze podatkov ključev SSL).

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
1024

Vrednost
Ena vrednost

ibm-slapdKrbRealm

Opis Podaja področje Kerberos strežnika LDAP. Uporablja se za objavljanje atributa ldapservicename v korenskem DSE. Strežnik LDAP lahko služi kot odložišče za informacije o šifrah za več KDC-jev (in področij), toda strežnik LDAP je lahko član enega samega področja.

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
Imeniški niz s primerjanjem, ki ne upošteva velikih in malih črk

Največja dolžina
256

Vrednost
Ena vrednost

ibm-slapdLdapCrlHost

Opis Podaja gostiteljsko ime strežnika LDAP, ki vsebuje sezname za preklic potrdil (CRL-je) za preverjanje potrdil x.509v3 odjemalcev. Ta parameter je potreben, če izdate ibm-slapdSslAuth=serverclientauth in odjemalska potrdila za preverjanje CRL.

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
Imeniški niz s primerjanjem, ki ne upošteva velikih in malih črk

Največja dolžina
256

Vrednost
Ena vrednost

ibm-slapdLdapCrlPassword

Opis Podaja geslo, ki ga uporablja strežniški SSL za povezovanje s strežnikom LDAP, ki vsebuje sezname za preklic potrdil (CRL-je) za preverjanje potrdil x.509v3 odjemalcev. Ta parameter je lahko potreben, če izdate ibm-slapdSslAuth=serverclientauth in odjemalska potrdila za preverjanje CRL.

Opomba: Če strežnik LDAP, ki hrani CRL-je, omogoča neoverjen dostop do CRL-jev (to je anonimni dostop), ibm-slapdLdapCrlPassword ni potreben.

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
Dvojiško število

Največja dolžina
128

Vrednost
Ena vrednost

ibm-slapdLdapCrlPort

Opis Podaja vrata, uporabljena za povezovanje s strežnikom LDAP, ki vsebuje sezname za preklic potrdil (CRL-je) za preverjanje potrdil x.509v3 odjemalcev. Ta parameter je potreben, če izdate ibm-slapdSslAuth=serverclientauth in odjemalska potrdila za preverjanje CRL. (vrata IP so nepodpisana, 16-bitna cela števila v območju od 1 do 65535)

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdLdapCrlUser

Opis Podaja povezovalni DN, ki ga uporablja strežniški SSL za povezovanje s strežnikom LDAP, ki vsebuje sezname za preklic potrdil (CRL-je) za preverjanje potrdil x.509v3 odjemalcev. Ta parameter je lahko potreben, če izdate ibm-slapdSslAuth=serverclientauth in odjemalska potrdila za preverjanje CRL.

Opomba: Če strežnik LDAP, ki hrani CRL-je, omogoča neoverjen dostop do CRL-jev (to je anonimni dostop), ibm-slapdLdapCrlUser ni potreben.

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
DN

Največja dolžina
1000

Vrednost
Ena vrednost

ibm-slapdMasterDN

Opis Podaja povezovalni DN glavnega strežnika. Vrednost se mora ujemati z replicaBindDN v replicaObject, ki je definiran za glavni strežnik. Če uporabite za overjanje strežnika za podvajanje Kerberos, mora ibm-slapdMasterDN podajati predstavitev DN za ID Kerberos (na primer ibm-kn=freddy@realm1). Če uporabite overjanje Kerberos, je MasterServerPW zanemarjen.

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
DN

Največja dolžina
1000

Vrednost
Ena vrednost

ibm-slapdMasterPW

Opis Podaja povezovalno geslo glavnega strežnika za podvajanje. Vrednost se mora ujemati z replicaBindDN v replicaObject, ki je definiran za glavni strežnik. Če uporabite za overjanje strežnika za podvajanje Kerberos, mora ibm-slapdMasterDN podajati predstavitev DN za ID Kerberos (na primer ibm-kn=freddy@realm1). Če uporabite overjanje Kerberos, je MasterServerPW zanemarjen.

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
Dvojiško število

Največja dolžina
128

Vrednost
Ena vrednost

ibm-slapdMasterReferral

Opis Podaja URL glavnega strežnika za podvajanje, kot je na primer

```
ldap://master.us.ibm.com
```

Za zaščito, ki je nastavljena samo na SSL:

```
ldaps://master.us.ibm.com:636
```

Za zaščito, ki je nastavljena na nič in uporabo nestandardnih vrat:

```
ldap://master.us.ibm.com:1389
```

Privzetek
none

Skladnja
Imeniški niz s primerjanjem, ki ne upošteva velikih in malih črk

Največja dolžina
256

Vrednost
Ena vrednost

ibm-slapdMaxEventsPerConnection

Opis Podaja največje število obvestil o dogodkih, ki jih lahko registrirate na povezavo.

```
Minimum = 0 (neomejeno)
Maksimum = 2,147,483,647
```

Privzetek
100

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdMaxEventsTotal

Opis Podaja največje skupno število obvestil o dogodkih, ki jih lahko registrirate za vse povezave.

```
Minimum = 0 (neomejeno)
Maksimum = 2,147,483,647
```

Privzetek
0

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdMaxNumOfTransactions

Opis Podaja največje število transakcij na strežnik.

```
Minimum = 0 (neomejeno)
Maksimum = 2,147,483,647
```

Privzetek
20

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdMaxOpPerTransaction

Opis Podaja največje število operacij na transakcijo.

```
Minimum = 0 (neomejeno)
Maksimum = 2,147,483,647
```

Privzetek
5

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdMaxPendingChangesDisplayed

Opis Največje število sprememb v teku, ki bodo prikazane.

Privzetek
200

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdMaxTimeLimitOfTransactions

Opis Podaja največjo vrednost čakalnega časa v sekundah za transakcijo v teku.

```
Minimum = 0 (neomejeno)
Maksimum = 2,147,483,647
```

Privzetek
300

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdPagedResAllowNonAdmin

Opis Ali bo strežnik omogočil povezavo neskrbnika za zahteve po rezultatih, ki so vrnjeni na več straneh. Če je vrednost, prebrana iz datoteke ibmslapd.conf, FALSE, bo strežnik obdelal samo tiste odjemalske zahteve, ki jih predloži uporabnik s pooblastilom skrbnika. Če odjemalec, ki zahteva za iskalno operacijo rezultate na več straneh, nima pooblastila skrbnika in je vrednost, ki je za ta atribut prebrana iz datoteke ibmslapd.conf FALSE, bo strežnik vrnil odjemalcu povratno kodo insufficientAccessRights, iskanje ali razdelitev na strani pa se ne bosta izvedla.

Privzetek
FALSE

Skladnja
Boolova vrednost

Dolžina
5

Števec Eden

Uporaba
directoryOperation

Uporabniško spreminjanje
Da

Razred dostopa
Kritičen

Objectclass
ibm-slapdRdbmBackend

Obvezen
Ne

ibm-slapdPagedResLmt

Opis Največje število sočasno aktivnih čakajočih iskalnih zahtev na več straneh. Območje = 0.... Če zahteva odjemalec operacijo z rezultati na več straneh in je trenutno aktivno največje dovoljeno število čakajočih

rezultatov, ki so vrnjeni na več straneh, bo strežnik vrnil odjemalcu povratno kodo, ki kaže, da je zaposlen, iskanje ali razdelitev na strani pa se ne bosta izvedla.

Privzetek
3

Skladnja
Celo število

Dolžina
11

Števec Eden

Uporaba
directoryOperation

Uporabniško spreminjanje
Da

Razred dostopa
Kritičen

Obvezen
Ne

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPageSizeLmt

Opis Največje število vnosov, ki jih bo vrnilo iskanje za posamezno stran, če podate krmilni element za rezultate, ki so vrnjeni na več straneh, ne glede na velikost strani, ki je lahko podana v iskalni zahtevi odjemalca. Območje = 0.... Če je odjemalec posredoval velikost strani, bo uporabljena tista od odjemalske vrednosti in vrednosti, prebrane iz datoteke ibmslapd.conf, ki je manjša.

Privzetek
50

Skladnja
Celo število

Dolžina
11

Števec Eden

Uporaba
directoryOperation

Uporabniško spreminjanje
Da

Razred dostopa
Kritičen

Obvezen
Ne

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPlugin

Opis Dodatek je dinamično naložena knjižnica, ki razširja zmožnosti strežnika. Atribut ibm-slapdPlugin podaja za strežnik, kako naj naloži in inicializira knjižnico dodatka. Skladnja je takšna:

ključna-beseda ime-datoteke init_function [*argumenti...*]

Skladnja se zaradi pravil knjižnice o poimenovanju nekoliko razlikuje za vsako platformo.

Večina dodatkov je neobveznih, toda ozadje dodatka RDBM je potrebno za vsa ozadja RDBM.

Privzetek
baza-podatkov /bin/libback-rdbm.dll rdbm_backend_init

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
2000

Vrednost
Več vrednosti

ibm-slapdPort

Opis Podaja vrata TCP/IP, uporabljena za povezave, ki ne uporabljajo zaščite SSL. Vrednost ne sme biti enaka kot za ibm-slapdSecurePort. (vrata IP so nepodpisana, 16-bitna cela števila v območju od 1 do 65535)

Privzetek
389

Skladnja
Celo število

Največja dolžina
5

Vrednost
Ena vrednost

ibm-slapdPWEncryption

Opis Podaja mehanizem kodiranja za uporabniška gesla, preden so shranjena v imenik. Vrednost mora biti none, imask, crypt ali sha (za uporabo kodiranja SHA-1 morate uporabiti ključno besedo **sha**). Da bi povezave SASL cram-md5 uspele, mora biti vrednost nastavljena na none.

Privzetek
none

Skladnja
Imeniški niz s primerjanjem, ki ne upošteva velikih in malih črk

Največja dolžina
5

Vrednost
Ena vrednost

ibm-slapdReadOnly

Opis Ta atribut se običajno uporablja samo za ozadje imenika, in podaja, ali je v ozadje mogoče pisati. Uporabiti morate vrednost TRUE ali FALSE. Če vrednosti ne podate, je uporabljen privzetek FALSE. Če uporabite vrednost TRUE, vrne strežnik v odziv na vse odjemalske zahteve, ki spremenijo podatke v bazi podatkov, ki je samo za branje, LDAP_UNWILLING_TO_PERFORM (0x35).

Privzetek
FALSE

Skladnja
Boolova vrednost

Največja dolžina
5

Vrednost
Ena vrednost

ibm-slapdReferral

Opis Podaja URL LDAP referenčnega kazalca, ki bo vrnjen, če se lokalne pripone ne ujemajo z zahtevo. Uporablja se za nadrejeni referenčni kazalec (to pomeni, da pripona ni v poimenovalnem kontekstu strežnika).

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
32700

Vrednost
Več vrednosti

ibm-slapdReplDbConns

Opis Največje število povezav baze podatkov, ki bodo uporabljene pri podvajanju.

Privzetek
4

Skladnja
Celo število

Največja dolžina
11

Vrednost
Ena vrednost

ibm-slapdReplicaSubtree

Opis Določa DN podvojenega poddrevesa.

Skladnja
DN

Največja dolžina
1000

Vrednost
Ena vrednost

ibm-slapdSchemaAdditions

Opis Atribut ibm-slapdSchemaAdditions izrecno določa, katera shema bo hranila nove vnose sheme. Po privzetku je nastavljen na /etc/V3.modifiedschema. Če tega atributa ne definirate, strežnik uporabi zadnjo datoteko ibm-slapdIncludeSchema kot v prejšnjih izdajah.

Pred različico 3.2 je bil zadnji vnos includeSchema v **slapd.conf** datoteka, v katero je dodajal strežnik vse nove vnose sheme, če je od odjemalca prejel zahtevo za dodajanje. Običajno je zadnji includeSchema datoteka V3.modifiedschema, ki je prazna in je nameščena samo za ta namen.

Opomba: Uporabljeno ime je zavajajoče, saj hrani samo nove vnose. Spremembe v obstoječih vnosih sheme so opravljene v njihovih izvirnih datotekah.

Privzetek
/etc/V3.modifiedschema

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
1024

Vrednost
Ena vrednost

ibm-slapdSchemaCheck

Opis Podaja mehanizem preverjanja sheme za operacijo dodajanja/spreminjanja/brisanja. Uporabiti morate vrednost V2, V3 ali V3_lenient.

- V2 - ohrani preverjanje v2 in v2.1; priporočamo za selitvene namene
- V3 - izvedba preverjanja v3
- V3_lenient - vsi nadrejeni objektni razredi niso potrebni; pri dodajanju vnosov je potreben samo najbližji objektni razred.

Privzetek
V3_lenient

Skladnja
Imeniški niz s primerjanjem, ki ne upošteva velikih in malih črk

Največja dolžina
10

Vrednost
Ena vrednost

ibm-slapdSecurePort

Opis Podaja vrata TCP/IP, uporabljena za povezave SSL. Vrednost ne sme biti enaka kot za ibm-slapdPort. (vrata IP so nepodpisana, 16-bitna cela števila v območju od 1 do 65535)

Privzetek
636

Skladnja
Celo število

Največja dolžina
5

Vrednost
Ena vrednost

ibm-slapdSecurity

Opis Omogoča povezave SSL. Vrednost mora biti none, SSL ali SSLOnly.

- none - strežnik posluša samo na vratih brez zaščite ssl
- SSL - strežnik posluša na vratih z zaščito ssl in brez nje
- SSLOnly - strežnik posluša samo na vratih ssl.

Privzetek
none

Skladnja
Imeniški niz s primerjanjem, ki ne upošteva velikih in malih črk

Največja dolžina
7

Vrednost
Ena vrednost

ibm-slapdServerId

Opis Določa strežnik, ki bo uporabljen za podvajanje.

Skladnja
Niz IA5 s primerjanjem, ki upošteva velike in male črke

Največja dolžina
240

Vrednost
Ena vrednost

ibm-slapdSetenv

Opis Strežnik izvede pri zagonu **putenv()** za vse vrednosti ibm-slapdSetenv, da spremeni izvajalno okolje strežnika. Spremenljivke lupine (kot sta %PATH% ali $LANG) niso razširjene.

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
2000

Vrednost
Več vrednosti

ibm-slapdSizeLimit

Opis Podaja največje število vnosov, ki bodo vrnjeni pri iskanju, ne glede na katerokoli omejitev velikosti, ki je lahko podana v iskalni zahtevi odjemalca (Območje = 0...). Če odjemalec posreduje omejitev, bo uporabljena tista odjemalska vrednost ali vrednost, prebrana iz datoteke **ibmslapd.conf**, ki je manjša. Če odjemalec ne posreduje omejitve in se je povezal s skrbniškim DN-jem, omejitev nima omejitve. Če odjemalec ne posreduje omejitve in se ne poveže s skrbniškim DN-jem, je uporabljena omejitev, ki je prebrana iz datoteke **ibmslapd.conf**. 0 = neomejeno

Privzetek
500

Skladnja
Celo število

Največja dolžina
12

Vrednost
Ena vrednost

ibm-slapdSortKeyLimit

Opis Največje število pogojev razvrščanja (ključev), ki jih lahko podate v eni iskalni zahtevi. Območje = 0.... Če posreduje odjemalec iskalno zahtevo z več ključi razvrščanja, kot dovoljuje omejitev in je kritičnost

krmilnega elementa za razvrščeno iskanje nastavljena na vrednost FALSE, bo strežnik sprejel vrednost, prebrano iz datoteke ibmslapd.conf in zanemaril vse ključe razvrščanja, na katere naleti po dosegi omejitve; iskanje in razvrščanje se izvedeta. Če posreduje odjemalec iskalno zahtevo z več ključi, kot dovoljuje omejitev in je kritičnost krmilnega elementa za razvrščeno iskanje TRUE, bo vrnil strežnik odjemalcu povratno kodo **adminLimitExceeded**, iskanje ali razvrščanje pa se ne izvedeta.

Privzetek
3

Skladnja
cis

Dolžina
11

Števec Eden

Uporaba
directoryOperation

Uporabniško spreminjanje
Da

Razred dostopa
Kritičen

Objectclass
ibm-slapdRdbmBackend

Obvezen
Ne

ibm-slapdSortSrchAllowNonAdmin

Opis Ali bo strežnik omogočil povezavo neskrbnika za razvrščanje v iskalni zahtevi ali ne. Če je vrednost, prebrana iz datoteke ibmslapd.conf, FALSE, bo strežnik obdelal samo tiste odjemalske zahteve, ki jih predloži uporabnik s pooblastilom skrbnika. Če odjemalec, ki zahteva za iskalno operacijo razvrščanje, nima pooblastila skrbnika in je vrednost, ki je za ta atribut prebrana iz datoteke ibmslapd.conf FALSE, bo strežnik vrnil odjemalcu povratno kodo insufficientAccessRights, iskanje ali razvrščanje pa se ne bosta izvedla.

Privzetek
FALSE

Skladnja
Boolova vrednost

Dolžina
5

Števec Eden

Uporaba
directoryOperation

Uporabniško spreminjanje
Da

Razred dostopa
Kritičen

Objectclass
ibm-slapdRdbmBackend

Obvezen
Ne

ibm-slapdSslAuth

Opis Podaja tip overjanja za povezavo ssl, in sicer serverauth ali serverclientauth.

- serverauth - podpira overjanje strežnika na odjemalcu; to je privzeta vrednost
- serverclientauth - podpira overjanje strežnika in odjemalca

Privzetek
serverauth

Skladnja
Imeniški niz s primerjanjem, ki ne upošteva velikih in malih črk

Največja dolžina
16

Vrednost
Ena vrednost

ibm-slapdSslCertificate

Opis Podaja oznako, ki določa osebno potrdilo strežnika v datoteki baze podatkov ključev. Ta oznaka je podana, ko z aplikacijo **gsk4ikm** izdelate zasebni ključ in potrdilo strežnika. Če ibm-slapdSslCertificate ne definirate, uporabi strežnik LDAP za povezave SSL privzeti zasebni ključ, kot je definiran v datoteki baze podatkov ključev.

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
128

Vrednost
Ena vrednost

ibm-slapdSslCipherSpec

Podaja način šifriranja SSL za odjemalce, ki dostopajo do strežnika. Uporabiti morate eno od naslednjih vrednosti:

Tabela 5. Načini šifriranja SSL

Atribut	Raven šifriranja
TripleDES-168	Šifriranje Triple DES s 168-bitni ključem in SHA-1 MAC
DES-56	Šifriranje DES s 56-bitnim ključem in SHA-1 MAC
RC4-128-SHA	Šifriranje RC4 s 128-bitnim ključem in SHA-1 MAC
RC4-128-MD5	Šifriranje RC4 s 128-bitnim ključem in MD5 MAC
RC2-40-MD5	Šifriranje RC4 s 40-bitnim ključem in MD5 MAC
RC4-40-MD5	Šifriranje RC4 s 40-bitnim ključem in MD5 MAC
AES	Šifriranje AES

Skladnja
Niz IA5

Največja dolžina
30

ibm-slapdSslKeyDatabase

Opis Podaja pot do datoteke baze podatkov ključev SSL strežnika LDAP. Ta datoteka baze podatkov ključev se uporablja za obravnavanje zahtev SSL iz odjemalcev LDAP, kot tudi za izdelovanje zaščitenih povezav SSL s strežniki za podvajanje LDAP.

Privzetek
/etc/key.kdb

Skladnja
Imeniški niz z natančnim ujemanjem velikosti črk

Največja dolžina
1024

Vrednost
Ena vrednost

ibm-slapdSslKeyDatabasePW

Opis Podaja geslo, povezano z datoteko baze podatkov ključev SSL strežnika LDAP, kot je podano v parametru ibm-slapdSslKeyDatabase. Če je z datoteko baze podatkov ključev strežnika LDAP povezana skrita datoteka gesel, lahko parameter ibm-slapdSslKeyDatabasePW izpustite ali nastavite na vrednost none.

Opomba: Skrita datoteka gesel mora biti v istem imeniku kot datoteka baze podatkov ključev in mora uporabljati enako ime kot datoteka baze podatkov ključev, toda njena pripona mora biti .sth in ne .kdb.

Privzetek
none

Skladnja
Dvojiško število

Največja dolžina
128

Vrednost
Ena vrednost

ibm-slapdSslKeyRingFile

Opis Pot do datoteke baze podatkov ključev SSL strežnika LDAP. Ta datoteka baze podatkov ključev se uporablja za obravnavanje zahtev SSL iz odjemalcev LDAP, kot tudi za izdelovanje zaščitenih povezav SSL s strežniki za podvajanje LDAP.

Privzetek
key.kdb

Skladnja
Imeniški niz s primerjavo, ki upošteva velike in male črke

Največja dolžina
1024

Vrednost
Ena vrednost

ibm-slapdSuffix

Opis Podaja kontekst poimenovanja, ki bo shranjen v tem ozadju.

Opomba: To ime je enako kot za objektni razred.

Privzetek
Vnaprej nastavljen privzetek ni definiran

Skladnja
DN

Največja dolžina
1000

Vrednost
Več vrednosti

ibm-slapdSupportedWebAdmVersion

Opis Ta atribut definira najstarejšo različico orodja za spletno upravljanje, ki podpira ta strežnik cn=configuration.

Privzetek

Skladnja
Imeniški niz

Največja dolžina

Vrednost
Ena vrednost

ibm-slapdSysLogLevel

Opis Podaja raven, pri kateri so statistični podatki o razhroščevanju in delovanju zabeleženi v datoteki slapd.errors. Uporabiti morate vrednost l, m ali h.

- h - high (visoka - nudi največ informacij)
- m - medium (srednja - privzetek)
- l - low (nizka - nudi najmanj informacij)

Privzetek
m

Skladnja
Imeniški niz s primerjanjem, ki ne upošteva velikih in malih črk

Največja dolžina
1

Vrednost
Ena vrednost

ibm-slapdTimeLimit

Opis Podaja največje število sekund za iskalno zahtevo, ne glede na druge časovne omejitve, ki so lahko podane v odjemalski zahtevi. Če odjemalec posreduje omejitev, bo uporabljena tista odjemalska vrednost ali vrednost, prebrana iz datoteke **ibmslapd.conf**, ki je manjša. Če odjemalec ne posreduje omejitve in se je povezal s skrbniškim DN-jem, omejitev nima omejitve. Če odjemalec ne posreduje omejitve in se ne poveže s skrbniškim DN-jem, je uporabljena omejitev, ki je prebrana iz datoteke **ibmslapd.conf**. 0 = neomejeno

Privzetek
900

Skladnja
Celo število

Največja dolžina

Vrednost
Ena vrednost

ibm-slapdTransactionEnable

Opis Če je dodatek transakcij naložen in je ibm-slapdTransactionEnable nastavljen na vrednost FALSE, strežnik zavrne vse zahteve StartTransaction in vrne odziv LDAP_UNWILLING_TO_PERFORM.

Privzetek
TRUE

Skladnja
Boolova vrednost

Največja dolžina
5

Vrednost
Ena vrednost

ibm-slapdUseProcessIdPw

Opis Če uporabite vrednost TRUE, strežnik zanemari atributa ibm-slapdDbUserID in ibm-slapdDbUserPW in uporabi za overjanje v DB2 lastne poverilnice.

Privzetek
FALSE

Skladnja
Boolova vrednost

Največja dolžina
5

Vrednost
Ena vrednost

ibm-slapdVersion

Opis Številka različice IBM Slapd.

Privzetek

Skladnja
Imeniški niz s primerjavo, ki upošteva velike in male črke

Največja dolžina

Vrednost
Ena vrednost

objectClass

Opis Vrednosti atributa objectClass opisujejo vrsto objekta, ki ga predstavlja vnos.

Skladnja
Imeniški niz

Največja dolžina
128

Vrednost
Več vrednosti

Poglavje 10. S tem povezane informacije

Spodaj so navedene IBM-ove rdeče knjige (v formatu PDF), spletne strani in teme Informacijskega centra, ki so povezane s temo imeniškega strežnika. Te datoteke PDF si lahko ogledate ali jih natisnete.

Rdeče knjige (www.redbooks.ibm.com)

- *Understanding LDAP*, SG24-4986  .
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino*, SG24-6163  .
- *Implementation and Practical Use of LDAP on the iSeries Server*, SG24-6193  .

Spletne strani

- Spletna stran IBM Directory Server for iSeries (www.ibm.com/servers/eserver/iseries/ldap) 
- Spletna stran Java Naming and Directory Interface (JNDI) Tutorial (java.sun.com/products/jndi/tutorial/) 

Druge informacije

“API-ji imeniškega strežnika” v temi Programiranje.

Dodatek. Opombe

Te informacije smo razvili za izdelke in storitve, ki jih nudimo v Združenih državah Amerike.

IBM morda izdelkov, storitev ali funkcij, opisanih v tem dokumentu, ne bo nudil v drugih državah. Informacije o izdelkih in storitvah, ki so trenutno na voljo pri vas, boste dobili pri lokalnem IBM-ovem predstavniku. Nobena referenca na IBM-ov izdelek, program ali storitev ne pomeni, da lahko uporabite samo ta IBM-ov izdelek, program ali storitev. Namesto njih lahko uporabite katerikoli funkcionalno enakovreden izdelek, program ali storitev, ki ne krši IBM-ovih pravic do intelektualne lastnine, vendar pa je uporabnik sam odgovoren za preverjanje in ocenitev delovanja vseh izdelkov, programov ali storitev drugih proizvajalcev.

IBM ima morda patentirane ali vloge za patente, ki pokrivajo predmet tega dokumenta. Posedovanje tega dokumenta vam ne daje licence za te patente. Pisna vprašanja o licencah lahko pošljete na naslednji naslov:

| IBM Director of Licensing
| IBM Corporation
| North Castle Drive
| Armonk, NY 10504-1785
| U.S.A.

Če imate vprašanja v zvezi z licencami za dvobajtne (DBCS) informacije, se obrnite na IBM-ov oddelek za intelektualno lastnino v svoji državi ali pa pošljite pisna vprašanja na naslednji naslov:

| IBM World Trade Asia Corporation
| Licensing
| 2-31 Roppongi 3-chome, Minato-ku
| Tokyo 106-0032, Japan

Naslednji odstavek ne velja za Veliko Britanijo ali za druge države, kjer takšni predpisi niso v skladu z lokalnim zakonom: INTERNATIONAL BUSINESS MACHINES CORPORATION NUDI TO PUBLIKACIJO "TAKŠNO KOT JE", BREZ JAMSTEV KAKRŠNEKOLI VRSTE, PA NAJ BODO IZRECNA ALI POSREDNA, KAR BREZ OMEJITVE VKLJUČUJE TUDI POSREDNA JAMSTVA ZA NEKRŠITEV, TRŽNOST ALI PRIMERNOST ZA DOLOČEN NAMEN. V nekaterih državah ni dovoljena zavrnitev odgovornosti za izrecna ali posredna jamstva v določenih transakcijah, zato ta izjava morda za vas ne velja.

Te informacije lahko vsebujejo tehnične netočnosti ali tipografske napake. Informacije v tem dokumentu občasno spremenimo, spremembe pa vključimo v nove izdaje publikacije. IBM lahko kadarkoli in brez vsakega obvestila izboljša in/ali spremeni izdelek(ke) in/ali programe(e), opisane v tej publikaciji.

Vse reference v teh informacijah na spletne strani, ki niso IBM-ove, so podane zgolj zaradi priročnosti, in na noben način ne pomenijo, da te spletne strani potrjujemo. Gradivo na teh spletnih straneh ni del gradiva za ta IBM-ov izdelek, in te spletne strani uporabljate na lastno odgovornost.

IBM lahko uporablja ali razpečuje informacije, ki nam jih pošljete, na kakršenkoli način, ki se nam zdi primeren, ne da bi imeli do vas kakršnokoli obveznost.

Imetniki licenc za ta program, ki potrebujejo informacije, da bi omogočili: (i) izmenjavo informacij med neodvisno izdelanimi programi in drugimi programi (vključno s tem) in (ii) medsebojno uporabo izmenjanih informacij, naj pišejo na naslednji naslov:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Te informacije so na voljo pod določenimi pogoji in določbami, ki v nekaterih primerih zahtevajo tudi plačilo.

Licenčni program, opisan v teh informacijah, in vse licenčno gradivo, ki je na voljo zanj, nudi IBM v skladu s pogoji IBM-ove pogodbe s strankami, IBM-ove mednarodne licenčne pogodbe za programe, IBM-ove licenčne pogodbe za strojno kodo ali katerekoli enakovredne pogodbe med nami.

Vse podatke o zmogljivosti, vsebovane v tem dokumentu, smo ugotovili v nadzorovanem okolju, zato se lahko rezultati, ki jih boste dobili v operacijskih okoljih, precej razlikujejo. Nekatere meritve smo opravili v sistemih na razvojni ravni, zato ne dajemo nobenega jamstva, da bodo v splošno razpoložljivih sistemih enake. Nekatere meritve smo opravili tudi z ekstrapolacijo. Dejanski rezultati se lahko razlikujejo. Uporabniki tega dokumenta naj preverijo ustrezne podatke za svoje specifično okolje.

Informacije o izdelkih drugih proizvajalcev smo dobili pri njihovih dobaviteljih, iz njihovih objav ali drugih javno razpoložljivih virov. IBM teh izdelkov ni preveril in ne more potrditi natančnosti podatkov o zmogljivosti, združljivosti ali drugih zahtev v zvezi z izdelki drugih proizvajalcev. Vprašanja v zvezi z zmožnostmi izdelkov drugih proizvajalcev naslovite na njihove dobavitelje.

Vse izjave v zvezi z IBM-ovo bodočo usmeritvijo ali načrti lahko spremenimo ali umaknemo brez vsakega obvestila, in predstavljajo zgolj cilje in namene.

Vse prikazane IBM-ove cene so IBM-ove predlagane maloprodajne cene, so trenutne in se lahko spremenijo brez obvestila. Cene za zastopnike se razlikujejo.

Te informacije so namenjene samo načrtovanju. Tukaj prikazane informacije se lahko spremenijo še preden so opisani izdelki na voljo.

Informacije vsebujejo primere podatkov in poročil iz vsakodnevnih poslovnih operacij. Da bi bili primeri čim bolj nazorni, vsebujejo imena posameznikov, podjetij, znamk in izdelkov. Vsa imena so izmišljena in vsakršna podobnost z imeni in naslovi dejanskih podjetij je zgolj naključna.

LICENCA ZA AVTORSKE PRAVICE:

Te informacije vsebujejo vzorčne uporabniške programe, napisane v izvornem jeziku, ki kažejo programerske tehnike na različnih operacijskih platformah. Te vzorčne programe lahko kopirate, spreminjate in razpečujete v kakršnikoli obliki brez plačila IBM-u, če gre za razvijanje, uporabo, trženje ali razpečevanje uporabniških programov, ki ustrezajo vmesniku uporabniškega programa za operacijsko platformo, za katero so vzorčni programi napisani. Ti zgledi niso bili natančno preizkušeni v vseh pogojih, zato pri IBM-u ne zagotavljamo zanesljivosti, uporabnosti ali delovanja teh programov.

RAZEN ZA MOREBITNA ZAKONSKA JAMSTVA, KI JIH NI MOGOČE IZKLJUČITI, IBM, NJEGOVI RAZVIJALCI PROGRAMA IN DOBAVITELJI NE DAJEJO JAMSTEV ALI POGOJEV, BODISI IZRECNO ALI POSREDNO, VKLJUČUJOČ, TODA NE OMEJENO NA, POSREDNA JAMSTVA ALI POGOJE ZA TRŽNOST, PRIMERNOST ZA DOLOČEN NAMEN IN NEKRŠITEV V ZVEZI S PROGRAMOM ALI TEHNIČNO PODPORO, ČE TA OBSTAJA.

IBM, NJEGOVI RAZVIJALCI PROGRAMOV ALI ZASTOPNIKI NISO POD NOBENIM POGOJEM ODGOVORNI ZA NASLEDNJE, TUDI ČE SO OBVEŠČENI O MOŽNOSTI:

1. IZGUBO ALI POŠKODOVANJE PODATKOV
2. POSEBNO, SLUČAJNO ALI POSREDNO ŠKODO ALI ZA KATEROKOLI EKONOMSKO POSLEDIČNO ŠKODO ALI
3. IZGUBO DOBIČKA, POSLA, DOHODKA, DOBREGA IMENA ALI PRIČAKOVANIH PRIHRANKOV.

NEKATERE ZAKONODAJE NE DOPUŠČAJO IZVZETJA ALI OMEJITVE POSLEDIČNIH ŠKOD ALI SLUČAJNE ŠKODE, ZATO NEKATERE ALI VSE ZGORNJE OMEJITVE ALI IZVZETJA MORDA ZA VAS NE VELJAJO.

Vsaka kopija ali katerikoli del teh vzorčnih programov ali iz njih izpeljanih izdelkov mora vsebovati obvestilo o avtorskih pravicah v naslednji obliki:

© (ime vašega podjetja) (leto). Deli te kode so izpeljani iz vzorčnih programov IBM Corp. . © Copyright IBM Corp. _vnesite leto ali leta_. Vse pravice so pridržane.

Če si ogledujete te informacije v zaslonski obliki, morda ne boste videli fotografij in barvnih ilustracij.

Blagovne znamke

Naslednji izrazi so blagovne znamke International Business Machines Corporation v Združenih državah Amerike, v drugih državah ali v obojih:

| AIX
| AIX 5L
| e(logo)server
| eServer
| i5/OS
| IBM
| iSeries
| pSeries
| xSeries
| zSeries

| Intel, Intel Inside (logotipi), MMX in Pentium so blagovne znamke Intel Corporation v Združenih državah Amerike,
| ostalih državah ali povsod.

Microsoft, Windows, Windows NT in logotip Windows so blagovne znamke Microsoft Corporation v Združenih državah Amerike, v drugih državah ali v obojih.

Java in vse na Javi temelječe blagovne znamke so blagovne znamke Sun Microsystems, Inc. v Združenih državah Amerike, v drugih državah ali v obojih.

| Linux je blagovna znamka Linusa Torvaldsa v Združenih državah Amerike, ostalih državah ali obojih.

UNIX je registrirana blagovna znamka The Open Group v Združenih državah Amerike in ostalih državah.

Ostala imena podjetij, izdelkov ali storitev so lahko prodajne ali storitvene znamke drugih.

| Določbe in pogoji za snemanje in tiskanje informacij

| Pravice za uporabo informacij, ki ste jih izbrali za presnetje z oddaljenega računalnika, so predmet naslednjih določb in
| pogojev in vaše navedbe, da jih sprejmete.

| **Osebna uporaba:** te informacije lahko ponatisnete za svojo osebno in nekomercialno uporabo, pod pogojem, da
| ohranite vse oznake o lastništvu. Izpeljanih delov teh informacij ali kateregakoli njihovega dela ne smete razdeljevati,
| prikazovati ali izdelovati brez izrecne privolitve IBM-a.

| **Komercialna uporaba:** te informacije lahko ponatisnete, razdelite in prikazujete izključno znotraj podjetja in pod
| pogojem, da ohranite vse oznake o lastništvu. Izdelava izpeljanih del teh informacij ni dovoljena, ponatis, razdeljevanje
| ali prikazovanje teh informacij ali kateregakoli njihovega dela izven podjetja pa ni dovoljeno brez izrecne privolitve
| IBM-a.

| Razen kot je izrecno odobreno v tem dovoljenju, niso dodeljene nobene druge pravice, licence ali pravice, pa naj bodo
| izrecne ali posredne, za informacije ali katerekoli podatke, programsko opremo ali drugo intelektualno lastnino,
| vsebovano v njih.

IBM si pridržuje pravico umakniti dovoljenja, vsebovana v tem dokumentu, če presodi, da mu uporaba informacij škodi ali če določi, da zgornja navodila niso pravilno upoštevana.

Te informacije lahko presnamete z oddaljenega računalnika, jih izvozite ali na novo izvozite samo s popolnim upoštevanjem vseh ustreznih zakonov in predpisov, vključno z vsemi zakoni in predpisi Združenih držav Amerike o izvozu. IBM NE DAJE NOBENEGA JAMSTVA ZA VSEBINO TEH INFORMACIJ. INFORMACIJE SO NA VOLJO ″TAKŠNE KOT SO″ BREZ JAMSTVA KAKRŠNEKOLI VRSTE, IZRECNEGA ALI POSREDNEGA, KAR VKLJUČUJE, VENDAR NI OMEJENO NA POSREDNA JAMSTVA TRŽNOSTI, NE-KRŠENJE IN PRIMERNOSTI ZA DOLOČEN NAMEN.

S presnetjem ali natisom informacij s te spletne strani soglašate s temi pogoji in določbami.

Natisnjeno na Danskem