System i

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

Verzija 6 Izdanje 1

System i

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

Verzija 6 Izdanje 1

Napomena

Prije upotrebe ovih informacija i proizvoda koji one podržavaju pročitajte informacije u “Napomene”, na stranici 301.

Ovo izdanje se primjenjuje na verziju 6, izdanje 1, modifikaciju 0 od IBM i5/OS (broj proizvoda 5761-SS1) i na sva sljedeća izdanja i modifikacije, dok se drukčije ne označi u novim izdanjima. Ova verzija ne radi na svim računalima sa smanjenim skupom instrukcija (RISC), niti ne radi na CISC modelima.

Sadržaj

IBM Tivoli Directory Server za i5/OS (LDAP)

IBM Tivoli Directory Server za i5/OS (u daljnjem tekstu Directory Server) je funkcija i5/OS koji osigurava poslužitelj Protokola pristupa bazi podataka (LDAP). LDAP se izvodi preko Transmission Control Protocol/Internet Protocol (TCP/IP) i popularan je kao usluga direktorija i za Internet i ne-Internet aplikacije.

Sljedeća poglavlja daju informacije koje vam pomažu da razumijete i koristite Directory Server.

Što je novo za V6R1

Pročitajte o novim ili značajno promijenjenim informacijama za IBM Tivoli Directory Server za i5/OS (LDAP) zbirku poglavlja.

Rezolucija sukoba replikacije

U mreži s višestrukim glavnim poslužiteljima, IBM Tivoli® Directory Server ima sposobnost automatski otkriti i riješiti promjene sukoba tako da direktoriji na svim poslužiteljima ostanu dosljedni. Kad se otkriju sukobi replikacije, oni izvještavaju se u dnevnik poslužitelja i zapisuju u datoteku dnevnika ″izgubljeno i nađeno″ tako da administrator može obnoviti podatke.

- Pregled replikacije
- Modificiranje postavki dnevnika izgubljeno i nađeno
- Pregledavanje datoteke dnevnika izgubljeno i nađeno

Naredba ldapmodify

Opcija -e errorfile dodana naredbi ldapmodify za specificiranje datoteke u koju se upisuju odbijeni unosi. Opcija -n se dodaje tako da promjenama koje bi se napravile prethodi uskličnik i ispisuje se na standardnom izlazu.

- ldapmodify i ldapadd
- LDAP format razmjene podataka (LDIF)

Višenitna replikacija

Možete replicirati pomoću višestrukih niti, poboljšavajući ukupni protok replikacije.

- Višenitna replikacija
- Ugovori replikacije

Šifriranje lozinke

IBM Tivoli Directory Server osigurava opciju konfiguracije za šifriranje podataka korisničke lozinke prije memorije u direktoriju. Ova opcija šifriranja može se koristiti da se spriječi da pristup podacima lozinke čistog teksta imaju redoviti korisnici direktorija kao i administrativni korisnici direktorija.

- Šifriranje lozinke
- Postavljanje svojstva politike lozinke

Atributi IBMAttributeTypes

IBM Tivoli Directory Server 6.0 dozvoljava da se prvih 128 znakova atributa koristi za kreiranje imena tablice.

- Atributi IBMAttributeTypes

Nedozvoljene promjene sheme

Možete povećati veličinu stupca putem modifikacije sheme. To omogućava povećanje maksimuma dužine atributa kroz modifikaciju sheme pomoću Web administracije ili pomoćnog programa ldapmodify.

- Nedozvoljene promjene sheme

Distribuirani direktorij

IBM Tivoli Directory Server zamišljen je kao distribuirani direktorij. Povezan s proxy poslužiteljem, funkcija distribuiranog direktorija dozvoljava klasteru direktorija da izgleda kao jedan. Funkcija distribuiranog direktorija zajedno s funkcijom proxy poslužitelja omogućit će razvoj direktorija za zadržavanje milijuna unosa.

- Distribuirani direktoriji

ldapmodrdn

IBM Tivoli Directory Server podržava modifyDN s novim superiornim atributom na završnom čvoru.

- ldapmodrdn

Upotreba TRCTCPAPP za pronalaženje problema

Možete koristiti naredbu TRCTCPAPP za praćenje instance aktivnog poslužitelja.

- Upotreba TRCTCPAPP za pronalaženje problema

Pristup čitanja za projicirane korisnike

Možete zabraniti sve operacije pretraživanja usmjerene prema korisnički projiciranoj pozadini.

- LDAP operacije
- Pristup čitanja za projicirane korisnike

Instance višestrukog poslužitelja

Možete imate višestruke directory server-e na svom sistemu i5/OS®. Svaki poslužitelj poznat je kao instanca. Ako koristite directory server na prethodnom izdanju i5/OS-a, migrirat će u instancu s imenom QUSRDIR. Možete kreirati višestruke instance directory servera za servisiranje vaših aplikacija.

- Upravljanje instancama
- Konfiguriranje Directory Servera

Razmatranja migriranja

IBM Tivoli Directory Server je nadograđen na novije verzije prvi puta kada se vrijeme pokrene.

- Migriranje u V6R1 iz V5R4 ili V5R3

Politika lozinke

Administrativni računi mogu se zaključati u slučaju pretjeranih grešaka u provjeri autentičnosti. Ova se funkcija primjenjuje jedino na povezivanja na udaljeni klijent. Račun se ponovo postavlja kod pokretanja poslužitelja. Novi atribut se definira za dozvoljavanje administrativnog zaključavanja računa.

- Postavljanje administrativne lozinke i politike zaključavanja
- Postavljanje svojstva politike lozinke

Proširena operacija, zahtjev statusa računa, osigurava se za dohvaćanje statusa određenog računa: otvoreno (omogućeno), zaključano ili isteklo.

- ldapexop

Ostalo

Jednakost **IBM® Tivoli® Directory Server:** V6R1 Directory Server je ekvivalentan verziji 6.0 IBM Tivoli Directory Servera.

- Tivoli softverski informacijski centar

Kako vidjeti što ima novo ili je promijenjeno

Za pomoć da se vidi gdje su bile izvršene tehničke promjene ova informacija koristi:

- Sliku » da označi gdje nova ili promijenjena informacija počinje.
- Sliku « da označi gdje nova ili promijenjena informacija završava.

U PDF datotekama mogli biste vidjeti crtice revizije (|) u lijevoj margini nove i promijenjene informacije.

Za ostale informacije o tome što je novo ili promijenjeno u ovom izdanju, pogledajte Memorandum za korisnike.

PDF datoteka za IBM Tivoli Directory Server za i5/OS (LDAP)

Možete gledati i ispisivati PDF datoteku IBM Tivoli Directory Servera za i5/OS (LDAP).

Za gledanje ili učitavanje PDF verzije ovog dokumenta, izaberite IBM Tivoli Directory Server za i5/OS (LDAP (oko 2700 KB).

Ostale informacije

Za gledanje ili ispisivanje PDF-ova odgovarajućih priručnika i IBM Redbooks publikacija, pogledajte “Povezane informacije” na stranici 299.

Spremanja PDF datoteka

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

1. Desno kliknite PDF vezu u svom pretražitelju.
2. Kliknite opciju koja sprema lokalno PDF.
3. Izaberite direktorij u koji želite spremiti PDF datoteku.
4. Kliknite **Spremanje**.

Spuštanje Adobe Acrobat Reader-a

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

Koncepti poslužitelja direktorija

Informacije o konceptima Poslužitelja direktorija.

Poslužitelj direktorija implementira specifikacije Internet Engineering Task Force (IETF) LDAP V3. Uključuje također poboljšanja koje IBM dodaje u funkcionalna i izvedbena područja. Ova verzija koristi IBM DB2 Universal Database za iSeries kao rezervnu pohranu kako bi se osigurala cjelovitost transakcije LDAP operacije, operacije najbolje izvedbe, te on-line sigurnosno kopiranje i vraćanje sposobnosti. Međudjeluje s klijentima zasnovanim na IETF LDAP V3.

Direktorije

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

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

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

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

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

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

Primjer direktorija u Slika 1 na stranici 5 prikazuje unos za Tim Jones koji uključuje atribute mail i telephoneNumber. Neki od drugih mogućih atributa mogu biti fax, title, sn (za prezime) i jpegPhoto.

Svaki direktorij ima shemu koja predstavlja skup pravila koja određuju strukturu i sadržaje direktorija. Shemu možete pregledati korištenjem Web administracijskog alata.

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

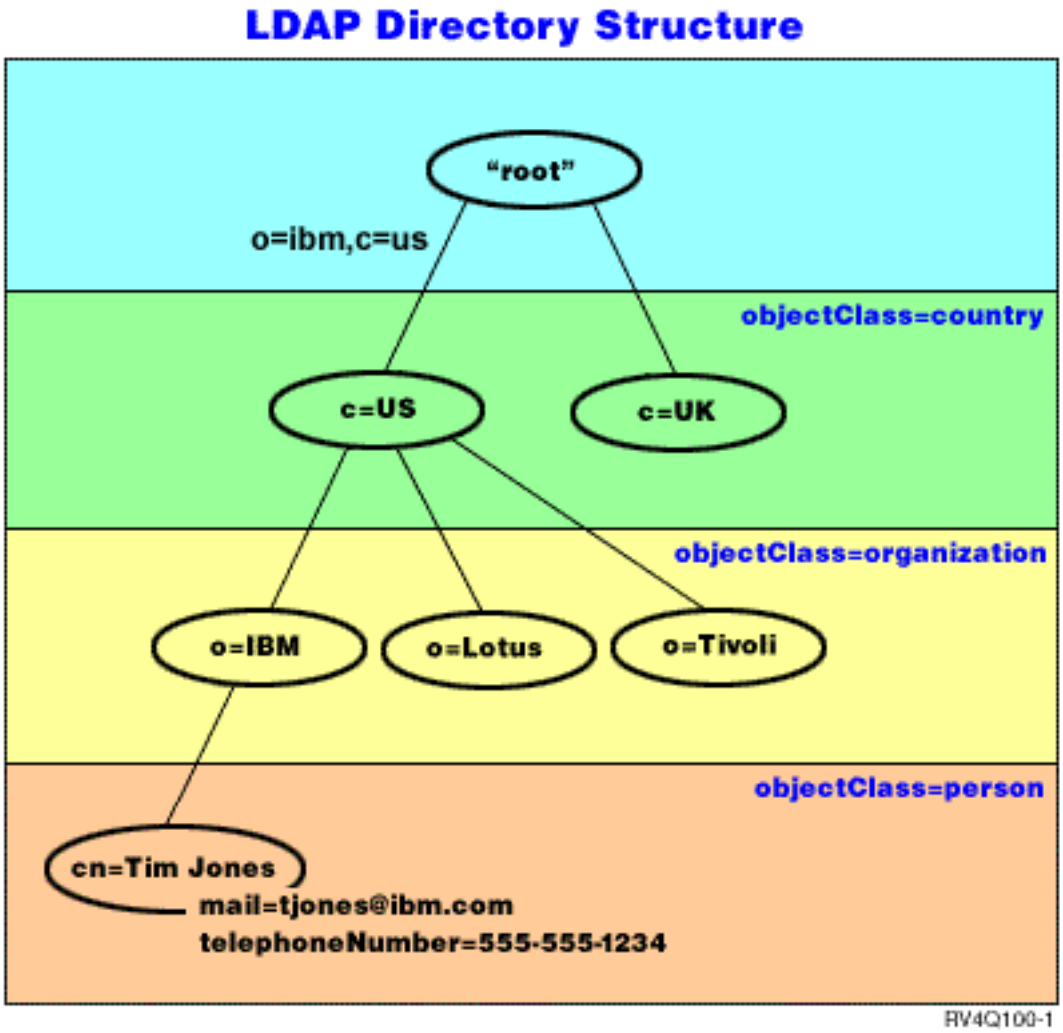
Osim atributa koje je definirala shema, unosi imaju i skup atributa koje održava poslužitelj. Ti atributi koji se nazivaju operativnim atributima, uključuju stvari kao što je vrijeme kada je unos bio kreiran i informacije kontrole pristupa.

Tradicionalno, slogovi u LDAP direktoriju su raspoređeni u hijerarhijskoj strukturi koja odražava političke, zemljopisne ili organizacijske granice (vidjeti Slika 1 na stranici 5). Na vrhu hijerarhije se nalaze unosi koji predstavljaju zemlje ili regije. Upisi koji predstavljaju države ili nacionalne udruge zauzimaju drugu razinu na dolje u hijerarhiji. Slogovi koji se potom nalaze ispod toga predstavljaju ljude, organizacijske jedinice, pisače, dokumente ili druge stvari.

LDAP se odnosi na unose s Razlikovnim imenima (DN-ovi). Ta prepoznatljiva razlikovna imena se sastoje od imena samog upisa kao i od imena, u poretku od dna prema vrhu, objekata iznad njega u direktoriju. Na primjer, potpuno DN za unos u donjem lijevom kutu od Slika 1 na stranici 5 je cn=Tim Jones, o=IBM, c=US. Svaki unos ima barem jedan atribut koji se koristi za imenovanje unosa. Taj atribut imenovanja se naziva Relativno razlikovno ime (RDN) unosa. Unos iznad danog RDN se zove njegovo roditeljsko Razlikovno ime. U gornjem primjeru, cn=Tim Jones imenuje unos tako da je to RDN. o=IBM, c=US je nadređeno DN za cn=Tim Jones.

Ako želite dati LDAP poslužitelju mogućnost održavanja i upravljanja dijelom LDAP direktorija, trebate navesti viša razlikovna imena najviše razine u konfiguraciji poslužitelja. Ta razlikovna imena se nazivaju sufiksima. Poslužitelj može pristupiti svim objektima u direktoriju koji se nalaze ispod navedenog sufiksa u hijerarhiji direktorija. Na primjer,

ako LDAP poslužitelj sadrži direktorij koji je prikazan u Slika 1, on treba imati sufiks o=ibm, c=us specificiran u svojoj konfiguraciji kako bi mogao odgovoriti na upite klijenta koji se odnose na Tim Jones.



Slika 1. Struktura LDAP direktorija

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

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

```
/
|
+- ibm.com
   |
   +- employees
      |
      +- Tim Jones
      |  555-555-1234
      |  tjones@ibm.com
```

```
      |
      +- John Smith
         555-555-1235
         jsmith@ibm.com
```

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

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

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

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

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

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

Klijenti i poslužitelji direktorija

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

API definira sučelje programiranja koje određeni programski jezik koristi za pristupanje usluzi. Format i sadržaj poruka koje su razmijenjene između klijenta i poslužitelja moraju odgovarati onom što je dogovoreno na protokolu. LDAP definira protokol poruke kojeg koriste klijenti direktorija i poslužitelji direktorija. Postoji i pridruženi LDAP API za C

jezik i načini pristupa direktoriju iz Java aplikacije upotrebom Java imenovanja i Sučelja direktorija (JNDI).

Sigurnost direktorija

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

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

Srodni koncepti

“Shema” na stranici 14
Shema je skup pravila koji upravlja načinom na koji se podaci mogu pohraniti u direktorij. Shema definira dozvoljeni tip unosa, njihovu strukturu atributa i sintaksu atributa.

“Operativni atributi” na stranici 88
Postoji nekoliko atributa koji imaju posebno značenje na Poslužitelju direktorija, a koji se nazivaju operativnim atributima. To su atributi koje održava poslužitelj i oni odražavaju informacije o unosu kojima rukuje poslužitelj ili utječu na operaciju poslužitelja.

“Razlikovna imena (DN-ovi)” na stranici 9
Svaki unos u direktorij ima razlikovno ime (DN). DN je ime koje jednoznačno identificira unos u direktorij. Prva komponenta DN-a se naziva Relativno razlikovno ime (RDN).

Lightweight Directory Access Protocol (LDAP) API-ji
Pogledajte Lightweight Directory Access Protocol (LDAP) API-je za više informacija o API-jima Directory Servera.

“Sigurnost Poslužitelja direktorija” na stranici 50
Saznajte kako se raznolikost funkcija može koristiti da učini vaš Directory Server sigurnim.

Srodne informacije

Web stranica Java Naming and Directory Interface (JNDI) priručnik

Distribuirani direktoriji

Distribuirani direktorij je okolina direktorija u kojoj se podaci raspodjeljuju preko višestrukih directory servera. Kako bi distribuirani direktorij izgledao kao jednostruki direktorij aplikacijama klijenta, osiguran je jedan ili više proxy poslužitelja koji imaju znanje svih poslužitelja i podataka koje sadržavaju.

Proxy poslužitelji distribuiraju dolazne zahtjeve pravim poslužiteljima i skupljaju rezultate za povrat združenog odgovora klijentu. Skup pozadinskih poslužitelja sadržavaju svoje dijelove distribuiranog direktorija. Ti pozadinski poslužitelji su načelno standardni LDAP poslužitelji s dodatnom podrškom za proxy poslužitelj za izdavanje zahtjeva u ime korisnika koji može biti definiran u različitom poslužitelju ili pripadati grupama koje su definirane na različitim poslužiteljima.

IBM Tivoli Directory Server v6.0 i kasnije (distribuirane platforme) sadržavaju takav distribuirani direktorij s proxy poslužiteljima, pozadinskim poslužiteljima i alatima za postavljanje takvog direktorija. Takav direktorij sposoban je skalirati do nekoliko milijuna unosa.

IBM Directory Server za i5/OS podršku za Distribuirane direktorije

IBM Directory Server za i5/OS sposoban je djelovati kao pozadinski poslužitelj unutar distribuiranog poslužitelja IBM Tivoli Directory Server. i5/OS directory server ne može djelovati kao proxy poslužitelj niti uključuje alate potrebne za

postavljanje distribuiranog direktorija. Proxy poslužitelj bi tada mogao raditi na drugoj platformi dok se stvarni podaci nalaze na jednom ili više i5/OS directory servera ili mješavini i5/OS i Tivoli-platform directory servera.

Kako bi se raspodijelili postojeći podaci iz i5/OS directory servera za upotrebu u topologiji distribuiranog direktorija, podaci se trebaju eksportirati u LDIF datoteku iz i5/OS direktorija, alat za postavljanje distribuiranog direktorija Tivoli na Tivoli platformama treba se izvoditi pomoću LDIF datoteke i podaci se trebaju ponovno napuniti na i5/OS i Tivoli directory servere koji sudjeluju kao pozadinski poslužitelji za distribuirani direktorij. Ta obrada nije različita za i5/OS poslužitelje ili poslužitelje Tivoli platforme i korisnici već imaju alat za postavljanje distribuiranog direktorija jer posjeduju proxy poslužitelj na Tivoli platformi.

Kontrole i proširene operacije za podršku Distribuiranim direktorijima

Budući da korisnici i grupe kojima pripadaju mogu biti distribuirani preko višestrukih poslužitelja, IBM Tivoli Directory Server definirao je skup kontrola i proširenih operacija za podršku grupnom članstvu i kontroli pristupa u distribuiranom direktoriju, osiguran je i mehanizam za osiguravanje ″staze revizije″ natrag do prvobitnog klijenta.

Bilješka: Unos direktorij drži se na jednom poslužitelju i njegovim replikama. Međutim, u distribuiranom direktoriju, korisnik može pripadati jednoj ili više grupa na jednom poslužitelju, te pripadati drugim grupama koje su definirane na drugom poslužitelju. Slično tome, samo korisnik ne mora biti definiran na pozadinskom poslužitelju koji obrađuje određeni zahtjev.

Revizijska kontrola

Revizijska kontrola je mehanizam koji proxy poslužitelj koristi za slanje jedinstvenog identifikatora zahtjeva klijenta koji je započeo proxy poslužitelj do pozadinskog poslužitelja. Osim jedinstvenog identifikatora, IP prvobitnog klijenta šalje se također u Revizijsku kontrolu. Taj jedinstven identifikator je ono što se koristi za podudaranje unosa revizije na proxy poslužitelju s unosima revizije na pozadinskim poslužitelja. Ako zahtjev prolazi kroz višestruke poslužitelje, pridodaje se IP informacija za svaki poslužitelj, što osigurava stazu kroz svaki poslužitelj natrag do originalnog klijenta.

Proširena operacija procjene grupnog članstva

Ova proširena operacija dozvoljava ovlaštenom klijentu (proxy poslužitelju) slanje informacija o korisniku do pozadinskog poslužitelja i zahtijevanje liste grupa (statičkih, ugniježđenih ili dinamičkih) da je korisnik član na pozadinskom poslužitelju.

Kontrola grupnog članstva

Ova kontrola dozvoljava ovlaštenom klijentu (proxy poslužitelju) slanje liste grupa koje će se koristiti za kontrolu pristupa. Kontrola pristupa se procjenjuje pomoću te liste grupa umjesto liste grupa koju bi radije poslužitelj normalno odredio, što se temelji na informaciji grupe pohranjenoj na poslužitelju. Kod tipične upotrebe, ta lista grupa je lista grupa koju proxy poslužitelj skuplja sa svakog pozadinskog poslužitelja pomoću proširene operacije Procjena grupnog članstva.

Revizijska podrška za distribuirane direktorije

i5/OS Sigurnosno revidiranje poboljšano je da bi se dala podrška distribuiranim direktorijima.

- **Kontrola revizije**: Korisna je nakon zahtjeva natrag do prvobitnog klijenta. I5/OS revidira ″kontrolu revizije″ dodavanjem polja “usmjeravanja” postojećem DI unosu dnevnika sigurnosnog revidiranja. Dok se sadržaji ne mogu dokazati, oni dolaze s klijenta koji je ovlašten za korištenje proxy autorizacije i morao bi biti pouzdan klijent.
- **Kontrola grupnog članstva**: Prisutnost kontrole grupe se revidira u dva dijela: Polje pojedinačnog znaka “izjava grupnog članstva” dodano je u DI unos dnevnika sigurnosnog revidiranja. Poslužitelj može biti konfiguriran za opcijsku reviziju liste grupa koje klijent osigura. Kad se ta opcija konfigurira, poslužitelj također revidira polje ″XD unakrsna referenca″ u DI unosu dnevnika i kreira jedan ili više XD unosa dnevnika sigurnosnog revidiranja s odgovarajućim poljem ″XD unakrsna referenca″ i listu grupa (do 5 grupa po unosu dnevnika)

Pogledajte poglavlje Sigurnosna referenca naniže navedenim odgovarajućim vezama za više detalja o i5/OS Sigurnosno revidiranje. Možete pogledati i web stranicu Inženjerska radna skupina Interneta i potražiti *rfc4648* da biste doznali više o konfiguriranju revidiranja za directory server.

Za više informacija o distribuiranim direktorijima i postavljanju distribuiranih direktorija, pogledajte poglavlje Distribuirani direktoriji u Tivoli softverskom informacijskom centru.

Srodni koncepti

"Revizija" na stranici 51
Revidiranje vam dozvoljava praćenje detalja određenih transakcija Directory Servera.

Srodne informacije

Revizije sigurnosti
Za više informacija o reviziji pogledajte poglavlje Revizije sigurnosti.

Identifikatori objekta (OID) za proširene operacije i kontrole

Razlikovna imena (DN-ovi)

Svaki unos u direktorij ima razlikovno ime (DN). DN je ime koje jednoznačno identificira unos u direktorij. Prva komponenta DN-a se naziva Relativno razlikovno ime (RDN).

DN se sastoji od attribute=value parova koji su odvojeni zarezima, na primjer:

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

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

Slijedite sljedeći primjer kako bi kreirali unos za osobu:

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

DN izlazna pravila

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

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

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

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

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

```
CN=L. Eagle,O=Sue\2C Grabbit and Runn,C=GB
```

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

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

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

Pseudo DN-ovi

Pseudo DN-ovi se koriste kod definicije i procjene kontrole pristupa. LDAP direktorij podržava nekoliko pseudo DN-ova (na primjer, ″group:CN=THIS″ i ″access-id:CN=ANYBODY″), koji se koriste kako bi se označio prevelik broj DN-ova koji dijele zajedničke karakteristike, u odnosu na operaciju koja se izvodi ili na objekt u kojem se izvodi operacija.

Poslužitelj direktorija podržava tri pseudo DN-ova:

- access-id: CN=THIS

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

- group: CN=ANYBODY

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

- group: CN=AUTHENTICATED

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

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

Neki primjeri pseudo DN-ova:

Primjer 1

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

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

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

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

Primjer 2

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

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

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

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

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

Poboljšana DN obrada

Sastavljen RDN od DN se može sastojati od višestrukih komponenta povezanih pomoću '+' operatora. Poslužitelj poboljšava podršku za pretraživanje na unosima koji imaju takav DN. Sastavljen RDN se može specificirati u bilo kojem poretku kao baza za operaciju pretraživanja.

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

Poslužitelj podržava proširene operacije DN normalizacije. Proširene operacije DN normalizacije normaliziraju DN-ove korištenjem sheme poslužitelja. Ta proširena operacija može biti korisna za aplikacije koje koriste DN-ove.

Sintaksa razlikovnog imena

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

```
<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> ::= slova, brojevi i razmak

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

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

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

<pair> ::= "\" ( <special> | "\" | '"')
<stringchar> ::= svaki znak osim <special> ili "\" ili '"'


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

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

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

Dodatno, znakovi praznog mjesta (' ' ASCII 32) mogu biti prisutni ili prije ili nakon '+' ili '='. Ti znakovi za razmak se zanemaruju kod raščlambe.

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

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

Srodni koncepti

"Direktorije" na stranici 3
Directory Server dozvoljava pristup tipu baze podataka koja pohranjuje informacije u hijerarhijsku strukturu sličnu načinu na koji je i5/OS integrirani sistem datoteka organiziran.

"Sigurnost Poslužitelja direktorija" na stranici 50
Saznajte kako se raznolikost funkcija može koristiti da učini vaš Directory Server sigurnim.

"Kontrole i proširene operacije" na stranici 90
Kontrole i proširene operacije dozvoljavaju LDAP protokolu da bude proširen bez promjene samog protokola.

Sufiks (kontekst imenovanja)

Sufiks (poznat i kao kontekst imenovanja) je DN koji identificira najviši unos u lokalno zadržanoj hijerarhiji direktorija.

Budući se u LDAP-u koristi relativna shema imenovanja, taj DN je isto tako sufiks bilo kojeg drugog unosa unutar hijerarhije tog direktorija. Poslužitelj direktorija može imati više sufiksa, a svaki od njih identificira lokalno zadržanu hijerarhiju direktorija, na primjer o=ibm,c=us.

Direktoriju mora biti dodan specifičan unos koji se podudara sa sufiksom. Unos kojeg kreirate mora koristiti klasu objekta koja sadrži korišteni atribut imenovanja. Možete koristiti alat Web administracije ili pomoćni program Qshell ldapadd kako bi kreirali odgovarajući unos za taj sufiks.

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

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

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

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

- cn=schema sadrži LDAP dohvatljiv prikaz sheme
- cn=changelog sadrži dnevnik promjena poslužitelja, ako je omogućen
- cn=localhost sadrži ne-replicirane informacije koje kontroliraju neke aspekte operacija poslužitelja, na primjer, objekte konfiguracije replikacije
- cn=IBMpolicies sadrži informacije o operaciji poslužitelja koja *se* replicira
- cn=pwdpolicy sadrži poslužitelj-široku politiku lozinke
- ″os400-sys=system-name.mydomain.com″ sufiks osigurava LDAP dostupnost i5/OS objektima, trenutno ograničena na korisničke profile i grupe

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

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

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

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

Klasa objekta domena ima i neke neobvezne atribute koje ćete možda željeti koristiti. Pregledajte shemu ili uredite unos kojeg ste kreirali korištenjem alata Web administracije kako bi vidjeli dodatne atribute koje možete koristiti.

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

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

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

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

Aplikacije koje vi koristite mogu zahtijevati da određeni nastavci budu definirani ili da bude korištena određena konvencija imenovanja. Na primjer, ako se vaš direktorij koristi za upravljanje digitalnim certifikatima, od vas će se možda tražiti dio strukture vašeg direktorija tako da imena unosa odgovaraju podložnim DN-ima certifikata koje sadržava.

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

Srodni koncepti

"Zadaci unosa direktorija" na stranici 184
Koristite ovu informaciju za upravljanje unosima direktorija.

"Zadaci sheme" na stranici 174
Koristite ovu informaciju za upravljanje shemom.

Srodni zadaci

"Dodavanje i uklanjanje sufiksa Directory Servera" na stranici 118
Koristite ovu informaciju za dodavanje ili uklanjanje sufiksa Directory Servera.

Srodne reference

"ldapmodify i ldapadd" na stranici 205
Pomoćni programi reda za naredbe LDAP modificiraj-unos i LDAP dodaj-unos.

Shema

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

Podaci su pohranjeni u direktoriju korištenjem unosa direktorija. Unos se sastoji od klase objekta, koja je potrebna i njezinih atributa. Atributi mogu biti obvezni ili neobvezni. Klasa objekta specificira vrstu informacija koju unos opisuje i definira skup atributa koje sadrži. Svaki atribut ima jednu ili više pridruženih vrijednosti.

Za više informacija koje se odnose na shemu, pogledajte:

Srodni koncepti

"Direktorije" na stranici 3
Directory Server dozvoljava pristup tipu baze podataka koja pohranjuje informacije u hijerarhijsku strukturu sličnu načinu na koji je i5/OS integrirani sistem datoteka organiziran.

"Zadaci unosa direktorija" na stranici 184
Koristite ovu informaciju za upravljanje unosima direktorija.

"Zadaci sheme" na stranici 174
Koristite ovu informaciju za upravljanje shemom.

Shema Directory Servera

Shema za poslužitelj direktorija je preddefinirana, međutim možete promijeniti shemu, ako imate dodatne zahtjeve.

Poslužitelj direktorija sadrži podršku dinamičke sheme. Shema je objavljena kao dio informacije o direktoriju i dostupna je u Subschema unosu (DN=″cn=schema″). Možete slati upite na shemu koristeći ldap_search() API i promijeniti je koristeći ldap_modify().

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

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

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

Shema sadrži vrijednosti za sljedeće tipove atributa:

- objectClasses
- attributeTypes
- IBMAttributeTypes
- matching rules

- ldap syntaxes

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

Primjer unosa sheme bi mogao sadržavati:

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

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

attributeTypes=( 2.5.18.10
                 NAME 'subschemaSubentry'
                 EQUALITY distinguishedNameMatch
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
                 NO-USER-MODIFICATION
                 SINGLE-VALUE USAGE directoryOperation )
attributeTypes=( 2.5.21.5 NAME 'attributeTypes'
                 EQUALITY objectIdentifierFirstComponentMatch
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.3
                 USAGE directoryOperation )
attributeTypes=( 2.5.21.6 NAME 'objectClasses'
                 EQUALITY objectIdentifierFirstComponentMatch
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.37
                 USAGE directoryOperation
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
                 USAGE directoryOperation )

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

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

Informacije o shemi se mogu preinačiti pomoću ldap_modify API-ja. S DN ″cn=schema″ možete dodati, obrisati ili zamijeniti tip atributa ili klasu objekta. Možete osigurati i potpuni opis. Možete dodavati ili zamijeniti unos sheme s definicijom LDAP verzija 3 ili s definicijom IBM proširenjem atributa ili s obje definicije.

Srodni koncepti

"Zadaci sheme" na stranici 174
Koristite ovu informaciju za upravljanje shemom.

Lightweight Directory Access Protocol (LDAP) API-ji
Pogledajte Lightweight Directory Access Protocol (LDAP) API-je za više informacija o API-jima Directory Servera.

"Klase objekta"
Klasa objekta specificira skup atributa koji se koriste za opisivanje objekta.

"Atributi" na stranici 17
Svaki unos direktorija ima skup atributa povezanih s njim kroz svoju klasu objekta.

Srodne reference

"Atributi IBMAttributeTypes" na stranici 20
IBMAttributeTypes atribut se može koristiti za definiranje informacije o shemi koju ne pokriva standard LDAP Verzija 3 za atribute.

"Pravila podudaranja" na stranici 21
Pravilo podudaranja osigurava upute za usporedbu niza za vrijeme operacije traženja.

"Sintaksa atributa" na stranici 23
Sintaksa atributa definira dopustive vrijednosti za atribut.

"Dinamička shema" na stranici 26
Moguće je dinamički promijeniti shemu.

Podrška uobičajene sheme

IBM direktorij podržava standardnu shemu direktorija.

IBM direktorij podržava standardnu shemu direktorija kako je definirano na sljedeći način.

- Internet Engineering Task Force (IETF) LDAP verzija 3 RFC-i, poput RFC 2252 i 2256.
- Common Information Model (CIM) iz Desktop Management Task Force (DMTF).
- Lightweight Internet Person Schema (LIPS) iz Network Application Consortium.

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

IBM također osigurava skup proširenih zajedničkih shematskih definicija koje drugi IBM proizvodi dijele kad iskorištavaju LDAP direktorij. One uključuju:

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

Srodne informacije

Internet Engineering Task Force (IETF)

Desktop Management Task Force (DMTF)

Network Application Consortium

Klase objekta

Klasa objekta specificira skup atributa koji se koriste za opisivanje objekta.

Na primjer, ako ste kreirali klasu objekta **tempEmployee**, ona bi mogla sadržavati atribute koji su pridruženi trenutnom zaposleniku kao što je **idNumber**, **dateOfHire** ili **assignmentLength**. Može dodati prilagođene klase objekta koje odgovaraju potrebama vaše organizacije. IBM shema poslužitelja direktorija omogućava neke osnovne tipove klasa nit Opasnosti, uključujući:

- Grupe

- Lokacije
- Organizacije
- Ljudi

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

Klase objekta su definirane karakteristikama tipa, nasljeđa i atributa.

Tip klase objekta

Klasa objekta može biti jednog od tri tipa:

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

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

Pomoćna:
Taj tip označava dodatne atribute koji mogu biti pridruženi unosu koji pripada određenoj strukturalnoj klasi objekta. Iako unos može pripadati samo pojedinačnim strukturalnim objektima klase, može pripadati višestrukim pomoćnim objektima klase.

Nasljeđivanje klase objekta

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

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

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

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

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

Atributi

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

Atributi

Svaki unos direktorija ima skup atributa povezanih s njim kroz svoju klasu objekta.

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

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

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

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

Za više informacija, pogledajte sljedeće:

Uobičajeni elementi podsheme:

Elementi se koriste za definiranje temeljnih pravila vrijednosti atributa podsheme.

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

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

Atribut objectclass:

Atribut objectclasses ispisuje klase objekta koje podržava poslužitelj.

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

```
ObjectClassDescription = "(" whsp
        numericoid whsp ; Objectclass identifikator
        [ "NAME" qdescrs ]
        [ "DESC" qdstring ]
        [ "OBSOLETE" whsp ]
        [ "SUP" oids ] ; Superiorne klase objekata
```

```
        [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ] ; default je structural
        [ "MUST" oids ] ; AttributeTypes
        [ "MAY" oids ] ; AttributeTypes
        whsp ")"
```

Na primjer, definicija person objectclass je:

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

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

Srodni koncepti

"Zadaci sheme" na stranici 174
Koristite ovu informaciju za upravljanje shemom.

Atribut attributetypes:

Atribut attributetypes ispisuje atribute koje podržava poslužitelj.

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

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

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

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

- "Pravila podudaranja" na stranici 21
- "Sintaksa atributa" na stranici 23

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

Na primjer, atribut ″description″ ima sljedeće definicije:

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

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

Srodni koncepti

“Zadaci sheme” na stranici 174
Koristite ovu informaciju za upravljanje shemom.

Atributi IBMAttributeTypes:

IBMAttributeTypes atribut se može koristiti za definiranje informacije o shemi koju ne pokriva standard LDAP Verzija 3 za atribute.

Vrijednosti IBMAttributeTypes moraju biti u skladu sa sljedećim temeljnim pravilima:

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

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

   IBMwlen = whsp len
```

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

DBNAME
Možete dobaviti najviše 2 imena, ako je potrebno, 2 imena su dana. Prvo je ime tablice koje se koristi za taj atribut. Drugo je ime stupca koje je korišteno za potpuno normaliziranu vrijednost atributa u tablici. Ako dobavite samo jedno ime, ono se koristi kao ime tablice kao i ime stupca. Ako ne osigurate nijedan DBNAME, tada se koristi ime bazirano na prvih 128 znakova imena atributa (koje mora biti jedinstveno). Imena tablice baze podataka su skraćena na 128 znakova. Imena stupaca su skraćena na 30 znakova.

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

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

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

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

EQUALITY, ORDERING, APPROX, SUBSTR, REVERSE
Ako se koristi bilo koji od tih atributa, indeks se kreira za odgovarajuće pravilo podudaranja. Neobvezna

dužina specificira širinu indeksiranog stupca. Jedan indeks se koristi za implementiranje više pravila podudaranja. Poslužitelj direktorija dodjeljuje dužinu 500 ako ju nije osigurao korisnik. Poslužitelj može koristiti i kraću dužinu od one koju je tražio korisnik ako to ima smisla. Na primjer, kada dužina indeksa premašuje maksimalnu dužinu atributa, dužina indeksa se zanemaruje.

Pravila podudaranja:

Pravilo podudaranja osigurava upute za usporedbu niza za vrijeme operacije traženja.

Podudarajuća pravila podijeljena su u tri kategorije:

- Jednakost
- Poredak
- Podniz

Poslužitelj direktorija podržava ekvivalentna podudaranja za sve sintakse osim binarne. Za atribute definirane koristeći binarnu sintaksu, poslužitelj podržava sam pretraživanja postojanja, ne primjer ″(jpegphoto=*)″. Za IA5 Znakovne i Direktorij znakovne sintakse, definicija atributa može biti dodatno definirana kao točan slovnik ili ignoriranje slovnika. Na primjer, cn atribut koristi caseIgnoreMatch pravilo uparivanja čineći vrijednosti ″John Doe″ i ″john doe″ jednakima. Za pravila ignoriranja velikih slova, usporedba je dana nakon pretvaranja vrijednosti u velika slova. Algoritam velikih slova nije lokalno-osjetljiv i ne mora biti ispravan za sve lokalizacije.

Poslužitelj direktorija podržava podudaranje podniza za Direktorij niz, IA5 Niz i atribute sintakse razlikovnog imena. Filteri pretraživanja za podudaranja podniza koriste ″*″ znak da upare nula ili više znakova u nizu znakova. Na primjer, filter pretraživanja ″(cn=*smith)″ podudara sve cn vrijednosti koje završavaju sa znakom ″smith″.

Podudaranja poretka su podržana za Integer, Direktorij niz znakova, IA5 Niz znakova i Razlikovno ime sintakse. Za znakovne sintakse, poredak je baziran na jednostavnom bajtnom poretku UTF-8 znakovnih vrijednosti. Ako je atribut definiran s pravilom ignoriraj velika slova, poredak je napravljan koristeći velika slova. Kao što je napomenuto prije, algoritam velikih slova ne mora biti ispravan za sve lokalizacije.

U IBM poslužitelju direktorija, podniz i ponašanje uparivanja poretka je uključeno pomoću pravila uparivanja: sve sintakse koje podržavaju podudaranje podniza imaju implicirano pravilo uparivanja podniza i sve sintakse koje podržavaju poredak imaju uključeno pravilo poretka. Za atribute definirane koristeći pravilo zanemarivanja velikih slova, uključena pravila podniza i uparivanja poretka također zanemaruju velika slova.

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

Pravila podudaranja jednakosti		
Pravilo podudaranja	**OID**	**Sintaksa**
objectIdentifierMatch	2.5.13.0	Niz za sadržavanje OID-ova. OID je niz koji sadržava znamenke (0-9) i decimalne točke (.)
octetStringMatch	2.5.13.17	Sintaksa Niza direktorija
telephoneNumberMatch	2.5.13.20	Sintaksa telefonskog broja
uTCTimeMatch	2.5.13.25	Sintaksa UTC vremena

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

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

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

Srodne reference

“Općenito i UTC vrijeme” na stranici 32
Directory Server podržava generalizirano vrijeme i sintakse (UTC) univerzalnog vremena.

Pravila indeksiranja:

Pravila indeksa koja su pripojena atributima omogućuju brže vraćanje informacija.

Ako je dan samo atribut, ne održavaju se nikakvi indeksi. Poslužitelj direktorija sadrži sljedeća pravila indeksiranja:

- Jednakost
- Poredak
- Procijenjeno
- Podniz
- Obrnuto

Specifikacije pravila indeksiranja za atribute:

Specificiranje pravila indeksiranja za atribut kontrolira kreiranje i održavanje posebnih indeksa na vrijednostima atributa. To umnogome poboljšava vrijeme odgovora za pretraživanja s filterima koji uključuju te atribute.

Pet mogućih tipova pravila indeksiranja se odnose na operacije koje su primijenjene u filteru pretraživanja.

Jednakost

Primjenjuje se na sljedeće operacije pretraživanja:

- equalityMatch '='

Na primjer:

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

Poredak

Primjenjuje se na sljedeće operacije pretraživanja:

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

Na primjer:

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

Procijenjeno

Primjenjuje se na sljedeće operacije pretraživanja:

- approxMatch '~='

Na primjer:

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

Podniz Odnosi se na operacije pretraživanja korištenjem sintakse podniza:

- podniz '*'

Na primjer:

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

Obrnuto

Primjenjuje se na sljedeće operacije pretraživanja:

- '*' podniz

Na primjer:

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

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

Sintaksa atributa:

Sintaksa atributa definira dopustive vrijednosti za atribut.

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

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

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

Ili razmotrite uključivanje informacije o poretku u vrijednost:

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

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

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

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

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

Booleovi atributi sadrže nizove TRUE ili FALSE.

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

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

Atributi Općenitog vremena sadržavaju znakovni prikaz datuma i vremena 2000 godine korištenjem GMT vremena s neobveznim pomakom GMT vremenske zone.

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

Atributi Integer sadrže prikaz tekstovnog niza vrijednosti. Na primjer, 0 ili 1000. Vrijednosti za atribute Integer sintakse moraju biti u rasponu od -2147483648 do 2147483647.

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

UTC Time atributi koriste raniji format niza prije 2000 godine za prikazivanje datuma i vremena.

U shemi direktorija, sintaksa atributa je navedena koristeći Identifikatore Objekta (OIDs) pridružene svakoj sintaksi. Sljedeća tablica ispisuje sintakse podržane od strane poslužitelja direktorija i njihovih OID-a.

Sintaksa	OID
Sintaksa atributa Type Description	1.3.6.1.4.1.1466.115.121.1.3
Binarno - niz okteta	1.3.6.1.4.1.1466.115.121.1.5
Boolean - TRUE/FALSE	1.3.6.1.4.1.1466.115.121.1.7
Sintaksa Niza direktorija	1.3.6.1.4.1.1466.115.121.1.15
Sintaksa Opisa pravila DIT Sadržaja	1.3.6.1.4.1.1466.115.121.1.16
Sintaksa Opisa pravila DITStructure	1.3.6.1.4.1.1466.115.121.1.17
DN - razlikovno ime	1.3.6.1.4.1.1466.115.121.1.12
Sintaksa Općenitog vremena	1.3.6.1.4.1.1466.115.121.1.24
IA5 Sintaksa niza	1.3.6.1.4.1.1466.115.121.1.26
IBM Opis tipa atributa	1.3.18.0.2.8.1
Sintaksa cijelog broja - integralni broj	1.3.6.1.4.1.1466.115.121.1.27
Sintaksa Opisa LDAP sintakse	1.3.6.1.4.1.1466.115.121.1.54

Sintaksa	OID
Opis pravila podudaranja	1.3.6.1.4.1.1466.115.121.1.30
Opis Koristi pravilo podudaranja	1.3.6.1.4.1.1466.115.121.1.31
Opis Oblika imena	1.3.6.1.4.1.1466.115.121.1.35
Sintaksa Opisa klase objekta	1.3.6.1.4.1.1466.115.121.1.37
Niz za sadržavanje OID-ova. OID je niz koji sadržava znamenke (0-9) i decimalne točke (.).	1.3.6.1.4.1.1466.115.121.1.38
Sintaksa telefonskog broja	1.3.6.1.4.1.1466.115.121.1.50
Sintaksa UTC Vremena. UTC-vrijeme je format vremenskog niza definiran s ASN.1 standardima. Pogledajte ISO 8601 i X680. Koristite tu sintaksu za pohranjivanje vrijednosti vremena u UTC formatu vremena.	1.3.6.1.4.1.1466.115.121.1.53

Srodni koncepti

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

Srodne reference

"Općenito i UTC vrijeme" na stranici 32
Directory Server podržava generalizirano vrijeme i sintakse (UTC) univerzalnog vremena.

Identifikator objekta (OID)

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

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

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

- Registrirajte objekte s ovlaštenjem. Ta strategija može biti prikladna ako, na primjer, trebate malo OID-ova.
- Dobavite luk (luk je pojedinačno podstablo OID stabla) iz ovlaštenja i dodijelite svoje vlastite OID-ove kako je to potrebno. Ova strategija može biti preferirana ako je potrebno mnogo OID-a ili OID dodjeljivanje nije stabilno.

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

U većini zemalja ili regija, udruženje nacionalnih standarda održava OID registar. Kao i kod ANSI luka, to su općeniti lukovi dodijeljeni pod OID 2.16. Možda će trebati određeno istraživanje za pronalazak OID ovlaštenja za određenu zemlju ili regiju. Nacionalna organizacija za standarde za vašu zemlju može biti ISO član. Imena i kontakt informacije ISO članova možete pronaći na ISO Web stranici (www.iso.ch).

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

Jednom kada se organizaciji dodijeli OID, možete definirati svoje vlastite OID-ove pridodavanjem na kraj OID-a. Na primjer, pretpostavimo da je vašoj organizaciji dodijeljen izmišljen OID 1.1.1. Nijednoj drugoj organizaciji se neće

dodijeliti OID koji počinje s ″1.1.1″. Možete kreirati čitav raspon za LDAP dodavanjem ″.1″ kako bi oblikovali 1.1.1.1. To možete dalje podijeliti u lance za klase objekata (1.1.1.1.1), tipove atributa (1.1.1.1.2) itd. i dodijeliti OID 1.1.1.1.2.34 atributu ″foo″.

Srodne informacije

ANSI Web stranica

ISO Web stranica

IANA Web stranica

Unosi podsheme

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

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

IBMsubschema klasa objekta

Klasa objekta IBMsubschema je određena klasa objekta koja pohranjuje sve atribute i klase objekta za određeni directory server.

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

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

Ispitivanja sheme

ldap_search() API se može koristiti za slanje upita unosu podsheme.

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

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

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

Srodni koncepti

Lightweight Directory Access Protocol (LDAP) API-ji
Pogledajte Lightweight Directory Access Protocol (LDAP) API-je za više informacija o API-jima Directory Servera.

Dinamička shema

Moguće je dinamički promijeniti shemu.

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

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

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

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

Da bi dodali ili zamijenili cjelinu sheme, vi MORATE omogućiti LDAP Verziju 3 definiciju i MOŽETE omogućiti IBM definiciju. U svakom slučaju morate osigurati samo definiciju ili definicije entiteta sheme na koju želite utjecati.

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

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

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

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

LDIF verzija gore navedenog bi bila:

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

Kontrole pristupa

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

Replikacija

Kada se izvodi dinamička promjene sheme, ona se replicira.

Nedozvoljene promjene sheme

Nisu dozvoljene sve promjene sheme.

U ograničenja promjene spada sljedeće:

- Sve promjene na shemi moraju ostaviti shemu u konzistentnom stanju.
- Tip atributa koji je supertip od drugog tipa atributa ne može biti obrisan. Tip atributa koji je ″MOŽE″ ili ″MORA″ tip atributa klase objekta ne može biti obrisan.
- Klasa objekta koja je nadklasa drugog ne može biti obrisana.

- Ne mogu se dodati tipovi atributa ili klase objekta koje se odnose na nepostojeće entitete (na primjer, sintakse ili klase objekta).
- Tipovi atributa ili klase objekta se ne mogu modificirati na način da oni nakon modifikacije referenciraju nepostojeće entitete (na primjer, sintakse ili klase objekta).
- Novi atributi ne mogu koristiti postojeće tablice baze podataka u njihovoj IBMattributestype definiciji.
- Atributi koji su korišteni u postojećim unosima direktorija ne mogu biti obrisani.
- Dužina i sintaksa atributa ne može biti promijenjena.
- Tablica baze podataka ili stupac povezan s atributom ne može biti promijenjen.
- Atributi korišteni u definiciji postojećih objekata klase ne mogu biti obrisani.
- Klase objekata koje su korištene u postojećim unosima direktorija ne mogu biti obrisane.

Možete povećati veličinu stupca putem modifikacije sheme. To omogućava povećanje maksimuma dužine atributa kroz modifikaciju sheme pomoću Web administracije ili pomoćnog programa ldapmodify.

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

Klase objekta:

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

Atributi:

- aclEntry
- aclPropagate
- aclSource
- aliasedObjectName, aliasedentryName
- businessCategory
- cn, commonName
- createTimestamp
- creatorsName
- opis
- 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
- vlasnik
- ownerPropagate
- ownerSource
- ref
- replicaBindDN
- replicaBindMethod
- replicaCredentials, replicaBindCredentials
- replicaHost
- replicaPort
- replicaUpdateTimeInterval
- replicaUseSSL
- seeAlso

Sintakse:
All

Pravila podudaranja:
All

Provjera sheme

Kada se inicijalizira poslužitelj, čitaju se datoteke sheme i provjerava se njihova konzistentnost i ispravnost.

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

Sljedeće stavke se provjeravaju kod tipova atributa:

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

Sljedeće stavke se provjeravaju kod klasa objekta:

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

Provjera unosa na shemi

Kada se unos doda ili preinači putem LDAP operacije, unos se provjerava na shemi. Po defaultu se izvode sve provjere koje su ispisane u ovom odlomku. No, vi možete selektivno onemogućiti neka od provjeravanja sheme mijenjanjem razine provjeravanja sheme. To se radi kroz System i Navigator promjenom vrijednosti polja **Provjera sheme** na stranici **Baza podataka/Sufiksi** svojstava Directory Servera.

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

S obzirom na klase objekta:

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

Valjanost tipova atributa za unos se određuje kako slijedi:

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

Valjanost vrijednosti tipa atributa za unos se određuje kako slijedi:

- Za svaki tip atributa kojeg sadržava unos, ako tip atributa ima jednu vrijednost, a unos ima više od jedne vrijednosti, unos se odbacuje.
- Za svaku vrijednost atributa svakog tipa atributa kojeg sadržava unos, ako sintaksa nije u skladu s rutinom provjeravanja sintakse za sintaksu tog atributa, unos se odbacuje.

- Za svaku vrijednost atributa svakog tipa atributa koji je sadržan u unosu, ako je njegova dužina veća od maksimalne dužine koja je dodijeljena tom tipu atributa, unos se odbacuje.

Valjanost DN-a se provjerava kako slijedi:

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

Srodni koncepti

"Shema konfiguracije Poslužitelja direktorija" na stranici 242
Ove informacije opisuju Stablo informacija direktorija (DIT) i atribute koji se koriste za konfiguriranje ibmslapd.conf datoteke.

iPlanet kompatibilnost

Sintaktički analizator kojeg koristi Poslužitelj direktorija dopušta da se vrijednosti atributa tipova atributa sheme (objectClasses i attributeTypes) specificiraju korištenjem temeljnih pravila za iPlanet.

Na primjer, descrs i numeric-oids se mogu specificirati okruženi jednostrukim navodnicima (kao da su qdescrs). Međutim, informacije o shemi su uvijek dostupne preko ldap_search. Odmah nakon što se izvede jedna dinamička promjena (korištenjem ldap_modify) na vrijednosti atributa u datoteci, cijela datoteka se zamjenjuje onom u kojoj sve vrijednosti atributa slijede specifikacije Poslužitelja direktorija. Budući da se isti sintaktički analizator koristi na datotekama i ldap_modify zahtjevima, ispravno se rukuje i s ldap_modify koji koristi iPlanet gramatiku za vrijednosti atributa.

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

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

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

Poslužitelj direktorija to ovako opisuje:

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

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

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

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

Općenito i UTC vrijeme

Directory Server podržava generalizirano vrijeme i sintakse (UTC) univerzalnog vremena.

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

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

i na još mnogo drugih načina bilježenja.

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

- Sintaksa Općenitog vremena u obliku:

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

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

  `"19991106210627.3"`

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

  `"19991106210627.3Z"`

  što označava koordinirano univerzalno vrijeme.

  `"19991106210627.3-0500"`

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

  Ako označavate i neobvezan djelić sekunde, potrebna je točka ili zarez. Za lokalni vremenski diferencijal, '+' ili '-' mora prethoditi vrijednost sat-minuta.

- Sintaksa Univerzalnog vremena u obliku:

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

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

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

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

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

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

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

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

Nisu valjani sljedeći filteri:

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

Preporučene prakse za strukturu direktorija

Poslužitelj direktorija je često korišten kao spremište za korisnike i grupe. Ovaj odlomak opisuje neke preporučene prakse za postavljanje strukture koja je optimizirana za upravljanje korisnicima i grupama. Ta struktura i pridruženi model sigurnosti mogu biti prošireni na druge upotrebe direktorija.

Korisnici su tipično pohranjeni u jednoj ili nekoliko lokacija. Možda ćete imati jedan spremnik, cn=users, koji je nadređeni unos za sve korisnike ili odijeljeni spremnici za zasebne skupove korisnika koji su administrirani posebno. Na primjer, zaposlenici, prodavači i samo-registrirani Internet korisnici mogu biti locirani pod objektima koji se zovu cn=employees, cn=vendors i cn=Internet users. Netko može biti u iskušenju da smjeste ljude pod organizacije kojima pripadaju; međutim, to može kreirati probleme kada se premjeste na druge organizacije zato što unos direktorija onda također treba biti premješten i grupe ili drugi izvori podataka (interni i eksterni u direktoriju)možda trebaju biti ažurirani da odraze novi DN. Odnos korisnika prema organizacijskoj strukturi može biti uhvaćen unutar korisničkog unosa koristeći atribute direktorija kao što je ″o″ (ime organizacije), ″ou″ (ime organizacijske jedinice) i departmentNumber koji su dijelovi standardne sheme za organizationalPerson iinetOrgPerson.

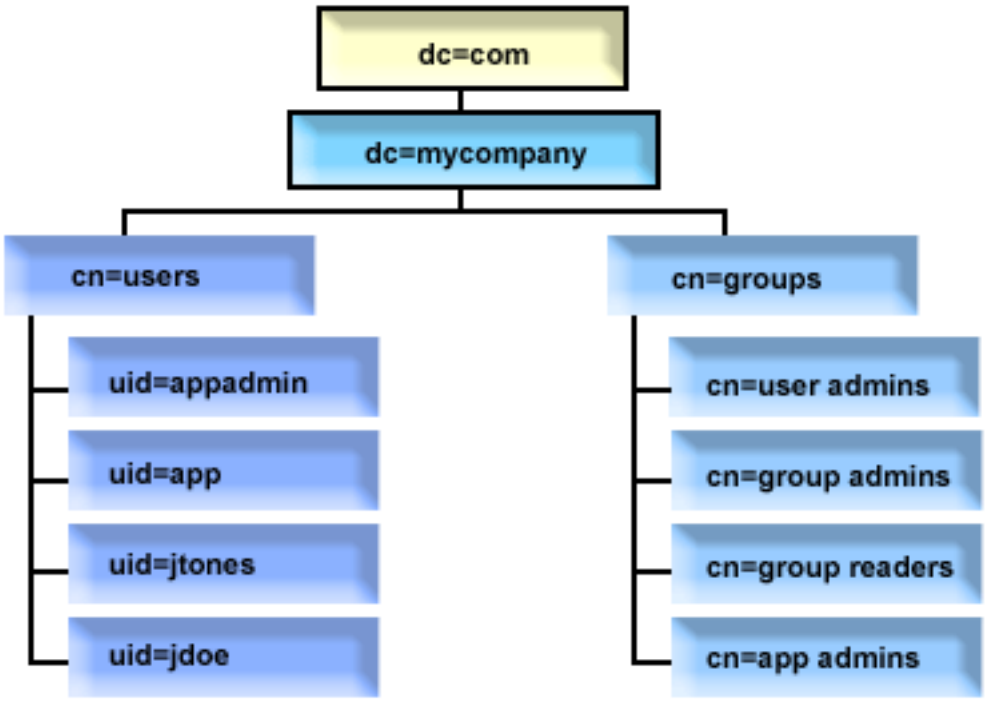
Slično, grupe su tipično smještene u posebne spremnike, na primjer spremnik koji se zove ″cn=groups″.

Organiziranjem korisnika i grupa na ovaj način, postoji samo nekoliko mjesta gdje liste kontrole pristupa (ACL) trebaju biti postavljene.

Ovisno o tome kako je poslužitelj direktorija korišten i kako su korisnici i grupe upravljane, možda ćete koristiti jedan od sljedećih obrazaca kontrole pristupa:

- Ako je direktorij korišten za aplikacije kao što je adresar, možda ćete htjeti dodijeliti posebnoj grupi cn=anybody dozvole čitanja i pretraživanja za ″normalne″ atribute u cn=users spremniku i njegovim nadređenim objektima.
- Često, samo DN-ovi korišteni od strane određenih aplikacija i administratora grupa trebaju pristup na cn=groups spremnik. Možda ćete htjeti kreirati grupu koja drži DN-ove administratora grupa i učiniti tu grupu vlasnikom cn=groups i njenih podređenih. Možda ćete kreirati drugu grupu koja drži DN-ove korištene od strane aplikacija za čitanje grupnih informacija i dodijeliti dozvole čitanja i pretraživanja na cn=groups.
- Ako su korisnički objekti ažurirani direktno od strane korisnika, vi ćete htjeti dodijeliti poseban pristupni-id cn=this odgovarajuće dozvole čitanja, pisanja i pretraživanja.
- Ako su korisnici ažurirani kroz aplikacije, često se te aplikacije izvode pod svojim vlastitim identitetom i samo te aplikacije trebaju ovlaštenje da ažuriraju korisničke objekte. Još jednom, prikladno je da se dodaju ti DN-ovi grupi, na primjer, cn=user administrators i da se toj grupi dodijeli potrebne dozvole za cn=users.

Primjenjivanje ovog tipa strukture i kontrole pristupa, vaš inicijalni direktorij može izgledati ovako:



Slika 2. Primjer strukture direktorija

- c=mycompany, dc=com je u vlasništvu administratora direktorija ili drugog korisnika ili grupe s ovlaštenjem za upravljanje na vrhu razine direktorija. Dodatni ACL unosi dodjeljuju pristup čitanja na normalnim atributima za jedan od cn=anybody ili cn=authenticated ili moguće neke druge grupe ako su potrebni višeograničavajući ACL-ovi.
- cn=users ima ACL unose preko onih opisanih ispod da dozvoli odgovarajući pristup korisnicima. ACL-ovi mogu uključivati:
  - pristup čitanja i pretraživanja na normalnim atributima za cn=anybody ili cn=authenticated
  - pristup čitanja i pretraživanja za normalne i osjetljive atribute za upravitelje
  - druge ACL unose po želji, možda dozvoljavajući pristup pisanja za pojedince za njihov vlastiti unos.

Napomene:

- Da bi poboljšali čitljivost, RDN-ovi unosa su bili korišteni umjesto punih DN-ova. Na primjer, ″user admins″ grupa bi imala puni DN uid=app,cn=users,dc=mycompany,dc=com kao član umjesto kraćeg uid=app.
- Neki korisnici i grupe mogu biti kombinirane. Na primjer, ako administrator aplikacije treba imati ovlaštenje da upravlja korisnicima, aplikacija se može izvoditi pod DN-om administratora aplikacije. Međutim, možda ćete htjeti ograničiti mogućnost, na primjer, promjene aplikacijske administratorske lozinke bez rekonfiguriranja nove lozinke u aplikaciji.
- Dok to predstavlja najbolju praksu za direktorije korištene od strane samo jedne aplikacije, možda će biti brže imati sva ažuriranja napravljena provjerom autentičnosti kao administratora direktorija. Ova praksa se izbjegava radi razloga raspravljenih ranije.

Objavljivanje

Directory Server osigurava sposobnost da sistem može objaviti određene vrste informacija LDAP direktoriju. To znači, sistem će kreirati i ažurirati LDAP unose koji predstavljaju različite tipove podataka.

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

Korisnici

Kada konfigurirate operativni sistem radi objavljivanja informacija o tipu korisnika na poslužitelj direktorija, on automatski eksportira unose iz sistemskog distribucijskog direktorija u poslužitelj direktorija. Da bi to napravio, on koristi QGLDSSDD_modrdn aplikativno programsko sučelje (API). Time i LDAP direktorij ostaje sinkroniziran s promjenama napravljenim u sistemskom distribucijskom direktoriju.

Objavljivanje korisnika je korisno za osiguravanje LDAP pristupa pretraživanja informacijama iz direktorija sistemske raspodjele (na primjer za osiguravanje LDAP pristupa adresara za LDAP-aktivirane POP3 mail klijente poput Netscape Communicator-a ili Microsoft Outlook Express-a).

Objavljeni korisnici mogu također biti korišteni da daju podršku LDAP provjeri autentičnosti s nekim korisnicima koji su objavljeni iz sistemskog distribucijskog direktorija i drugih korisnika dodanih direktoriju na druge načine. Objavljeni korisnik ima uid atribut koji imenuje profil korisnika i nema userPassword atribut. Kada je vezani zahtjev primljen za unos poput ovog, poslužitelj poziva sigurnost operativnog sistema da provjeri valjanost uid-a i lozinke kao valjanog korisničkog profila i lozinku za taj profil. Ako želite koristiti LDAP provjeru autentičnosti, te biste željeli da postojeći korisnici mogu provjeriti autentičnost lozinke svog operativnog sistema, dok se ne-i5/OS korisnici dodaju ručno u direktorij, trebali biste razmotriti ovu funkciju.

Drugi način za objavljivanje korisnika je da uzmete unose iz postojeće HTTP validacijske liste i kreirate odgovarajuće LDAP unose u poslužitelju direktorija. To se radi putem QGLDPUBVL sučelja aplikativnog programa (API). Taj API kreira inetOrgPerson unose direktorija s lozinkama koje su povezane s originalnim unosima validacijske liste. API može biti pokrenut jednom ili raspoređen da se periodički izvodi radi provjere novih unosa za dodavanje u poslužitelj direktorija.

Bilješka: Samo unosi validacijske liste kreirani za korištenje s HTTP poslužiteljem (podržan s Apache) su podržani s ovim API-jem. Postojeći unosi u poslužitelju direktorija neće biti ažurirani. Korisnici koji su obrisani iz validacijske liste nisu otkriveni.

Jednom kad su korisnici dodani u direktorij oni se mogu autentizirati aplikacijama koje koriste provjeru valjanosti kao i aplikacijama koje podržavaju LDAP provjeru autentičnosti.

Sistemske informacije

Kada konfigurirate operativni sistem da objavi informacije o tipu sistema na poslužitelj direktorija, sljedeći tipovi informacija su objavljeni:

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

U informacije pisača koje se mogu objaviti spadaju:

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

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

Podjele pisača

Kada konfigurirate operativni sistem za objavljivanje podjela pisača, informacije o izabranim iSeries NetServer podjelama pisača se izdaju na konfigurirani poslužitelj Aktivni direktorij. Objavljivanje podjela pisača u Aktivni dozvoljava korisnicima da dodaju System i pisače na svoj Windows 2000 desktop pomoću čarobnjaka Dodavanje pisača Windowsa 2000. Kako bi se to napravilo u čarobnjaku Dodavanje pisača, specificirajte da želite pronaći pisač u Windows 2000 aktivnom direktoriju. Podjele pisača morate objaviti na poslužitelju direktorija koji podržava Microsoft shemu Aktivnog direktorija.

TCP/IP kvaliteta usluga

Poslužitelj TCP/IP kvaliteta usluga (QOS) se može konfigurirati za upotrebu dijeljene QOS politike definirane u LDAP direktoriju pomoću IBM definirane sheme. TCP/IP QOS agenta objavljivanja koristi QOS poslužitelj kako bi pročitao informacije o politici; on definira poslužitelja, informacije o provjeri autentičnosti i gdje su na direktoriju pohranjene informacije o politici.

Možete kreirati i aplikaciju koja će objavljivati ili tražiti druge tipove informacija u LDAP direktoriju korištenjem ove okosnice definiranjem dodatnih agenta objavljivanja i korištenjem API-ja objavljivanja direktorija.

Srodni koncepti

Lightweight Directory Access Protocol (LDAP) API-ji
Pogledajte Lightweight Directory Access Protocol (LDAP) API-je za više informacija o API-jima Directory Servera.

Srodni zadaci

"Objavljivanje informacija Directory Server-u" na stranici 123
Koristite ovu informaciju za objavljivanje informacija Directory Server-u.

Replikacija

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

Radi više informacija o repliciranju, pogledajte sljedeće:

Srodni koncepti

"Zadaci replikacije" na stranici 139
Koristite ovu informaciju za upravljanje replikacijom.

"Migracija mreže poslužitelja repliciranja" na stranici 94
Koristite ovu informaciju ako imate mrežu replicirajućih poslužitelja.

Pregled replikacije

Preko replikacije se promjene koje su učinjene na jednom direktoriju šire na još jedan ili više dodatnih direktorija. U stvari, promjena na jednom direktoriju se pojavljuje na više različitih direktorija.

Replikacija ima dvije glavne koristi:

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

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

IBM direktorij podržava prošireni model glavne-podređene replikacije. Topologije replikacije su proširene tako da uključuju:

- Replikaciju podstabla Stabla informacije direktorija (DIT) na određenim poslužiteljima
- Višerazinsku topologiju koja se naziva kaskadna replikacija
- Dodjeljivanje uloge poslužitelja (glavnog ili replike) od strane podstabla
- Višestruke glavne poslužitelje koji se smatraju ravnopravnom zamjenom
- Gateway replikacija preko mreža

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

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

Tipovi poslužitelja definirani pomoću funkcije su *glavni/podređeni*, *kaskadni*, *gateway* i *replika*.

Tablica 1. Uloge poslužitelja

Direktorij	Opis
Glavni/ravnopravni	Glavni/ravnopravni poslužitelj sadrži informacije glavnog direktorija iz kojeg se ažuriranja šire na replike. Sve promjene se rade i pojavljuju na glavnom poslužitelju i glavni poslužitelj je odgovoran za širenje tih promjena na replike. Nekoliko poslužitelja se može ponašati kao glavni poslužitelj za informacije o direktoriju, s tim da je svaki glavni poslužitelj odgovoran za ažuriranje drugih glavnih poslužitelja i replika poslužitelja. To se naziva ravnopravnom replikacijom. Ravnopravna replikacija može poboljšati izvedbu i pouzdanost. Izvedba je poboljšana omogućavanjem lokalnom poslužitelju da rukuje ažuriranjima u široko distribuiranoj mreži. Pouzdanost se poboljšava omogućavanjem da backup glavni poslužitelj bude spreman za trenutno preuzimanje ako dođe do kvara na primarnom glavnom poslužitelju. **Napomene:** 1. Glavni poslužitelji repliciraju sva ažuriranja klijenta, ali ne repliciraju ažuriranja koja su primljena iz drugih glavnih poslužitelja. 2. Ažuriranja na istom unosu koje izvodi više poslužitelja mogu uzrokovati nekonzistentnosti u podacima direktorija jer nema rješenja sukoba.
Kaskadni (prosljeđivanje)	Kaskadni poslužitelj je replika poslužitelj koji replicira sve promjene koje su poslane na njega. Razlika u odnosi na glavni/ravnopravni poslužitelj je u tome da glavni/ravnopravni poslužitelj replicira samo promjene koje čini klijent koji je povezan na tog poslužitelja. Kaskadni poslužitelj može smanjiti radno opterećenje replikacije sa glavnih poslužitelja u mreži koja sadrži široko raspoređene replike.
Gateway	Gateway replikacija koristi gateway poslužitelje da sakupi i distribuira informacije o replikaciji efikasno preko replicirajuće mreže. Glavna dobit gateway replikacije je smanjivanje mrežnog prometa.
Replika (samo za čitanje)	Replika je dodatni poslužitelj koji sadrži kopiju informacija o direktoriju. Replike su kopije glavnih poslužitelja (ili podstabla). Replika osigurava backup repliciranog podstabla.

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

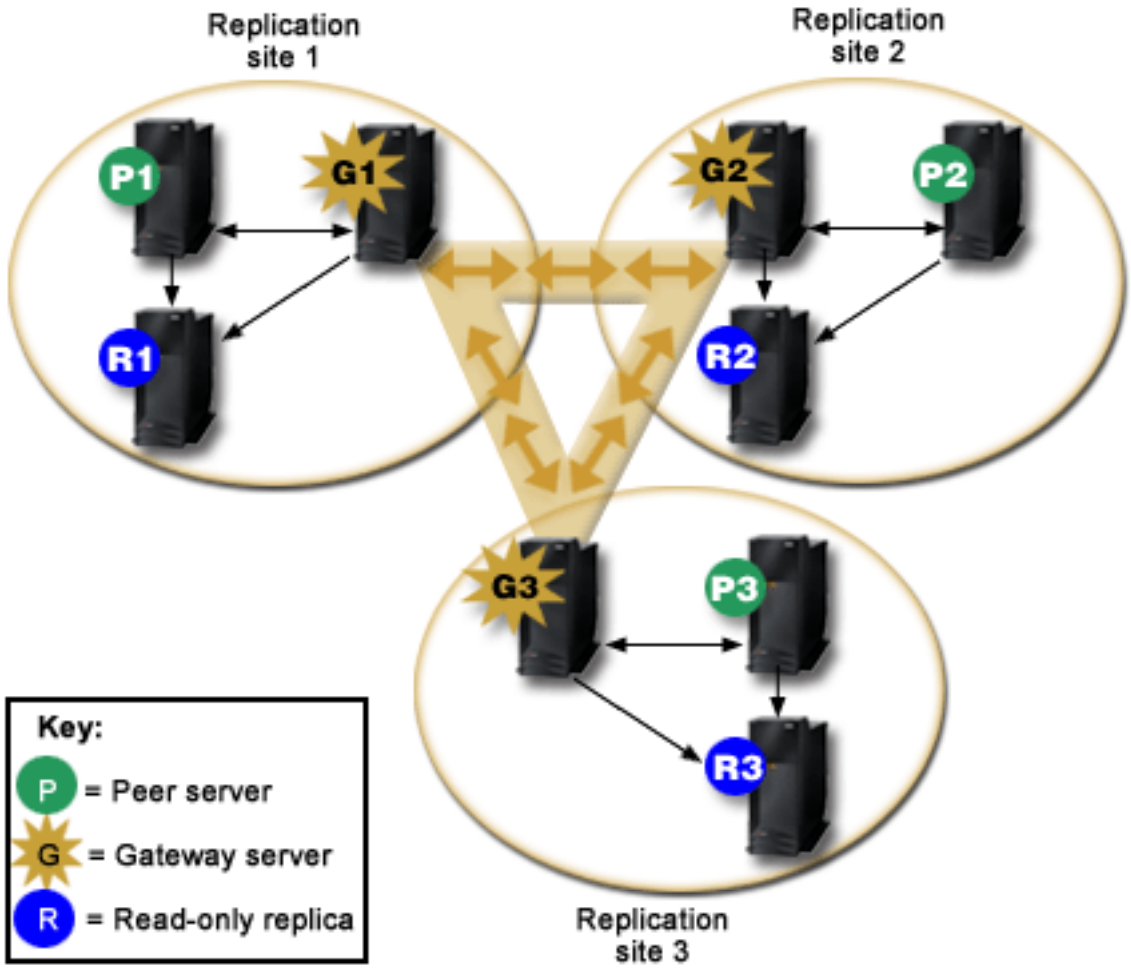
Možete tražiti ažuriranja na replika poslužitelju, no ažuriranje se u stvari prosljeđuje na glavni poslužitelj upućivanjem natrag na klijenta. Ako je ažuriranje uspješno, glavni poslužitelj onda šalje ažuriranje na replike. Tako dugo dok glavni poslužitelj ne dovrši replikaciju ažuriranja, promjena se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

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

Gateway replikacija

Gateway replikacija koristi gateway poslužitelje da sakupi i distribuira informacije o replikaciji efikasno preko replicirajuće mreže. Glavna korist gateway replikacije je smanjivanje mrežnog prometa. Gateway poslužitelji moraju biti glavni (na njih se može pisati).

Sljedeća slika ilustrira kako replikacija gatewaya radi:



Slika 3. Replicirajuća mreža s gateway poslužiteljima

Replicirajuća mreža na prethodnoj slici sadrži tri replikativna mjesta, a svaki sadrži gateway poslužitelj. Gateway poslužitelj sakuplja ažuriranja repliciranja iz ravnopravni/glavni poslužitelja u replikativnom mjestu gdje se nalazi i šalje ažuriranja na sve druge gateway poslužitelje unutar replikativne mreže. Također skuplja replikativna ažuriranja s drugih gateway poslužitelja u replikativnoj mreži i šalje ta ažuriranja na ravnopravne/glavne i replike u replikativnom mjestu gdje se nalazi.

Gateway poslužitelji koriste poslužiteljske ID-ove i korisničke ID-ove da odrede koja ažuriranja su poslana na druge gateway poslužitelje u replicirajućoj mreži i koja ažuriranja su poslana na lokalne poslužitelje unutar stranice repliciranja.

Da bi postavili repliciranje gatewaya, morate kreirati barem dva gateway poslužitelja. Kreiranje gateway poslužitelja postavlja replikativnu stranicu. Tada morate kreirati replikacijske ugovore između gatewaya i bilo kojeg glavni/ravnopravni i replika koje želite uključiti u replikativnu stranicu tog gatewaya.

Gateway poslužitelji moraju biti glavni (na njih se mora pisati). Ako pokušate dodati objekt klase gatewaya, ibm-replicaGateway, u podunos koji nije glavni, vraća se poruka pogreške.

Postoje dvije metode za kreiranje gateway poslužitelja. Možete:

- Kreirati novi gateway poslužitelj
- Pretvoriti postojeći ravnopravan poslužitelj u gateway poslužitelj

Bilješka: Vrlo je bitno da dodijelite samo jedan gateway poslužitelj po replikativnoj stranici.

Rezolucija sukoba replikacije

U mreži s višestrukim glavnim poslužiteljima, moguće je napraviti promjene sukoba u unosu koji bi mogao uzrokovati da poslužitelji imaju različite podatke za unos nakon repliciranja promjene. Promjene sukoba su neuobičajene budući da zahtijevaju promjene na različitim glavnim poslužiteljima što je više moguće u isto vrijeme. Neki primjeri promjena sukoba uključuju:

- Dodavanje istog unosa s različitim atributima na dva poslužitelja.
- Resetiranje lozinke za unos pomoću različitih lozinki na dva poslužitelja.
- Preimenovanje unosa na jednom poslužitelju dok se modificira unos na drugom poslužitelju.

IBM Tivoli Directory Server ima sposobnost automatski otkriti i riješiti promjene sukoba tako da direktoriji na svim poslužiteljima ostanu konzistentni. Kada se uoče sukobi replikacije, promjena sukoba se izvještava u dnevniku poslužitelja i zapisuje se u datoteku dnevnika ″izgubljeno i nađeno″, tako da administrator može obnoviti sve izgubljene podatke.

Rezolucija sukoba za operacije dodaj i modificiraj u replikaciji za razmjenu podataka bazira se na vremenskim oznakama unosa i promjene. Ažuriranje najnovijom vremenskom oznakom na bilo kojem poslužitelju u višestruko-glavnoj okolini replikacije je ono koje ima prednost. Kad se otkrije sukob replikacije zamijenjen unos se arhivira u svrhu obnavljanja u dnevnik Izgubljeno i nađeno.

Replicirani zahtjevi obriši i preimenuj su prihvaćeni redoslijedom primljenim bez rezolucije sukoba. Ako se dese sukobi replikacije koji uključuju operacije briši ili modifyDN (preimenuj ili premjesti), mogu se pojaviti greške koje zahtijevaju ljudsku intervenciju. Na primjer, ako je unos preimenovan na jednom poslužitelju dok se modificira na drugom poslužitelju, operacija preimenuj modifyDN bi mogla doći kod replike prije operacije modificiraj. Tada, kada dođe operacija modificiraj, ne uspije. U tom slučaju administrator treba odgovoriti na grešku primjenom modifikacija na unosu pomoću novog DN-a. Sve informacije potrebne za ponovno modificiranje s ispravnim imenom su sačuvane u dnevnicima replikacije i grešaka. Takve greške replikacije su rijetke u ispravno konfiguriranoj topologiji replikacije, ali nije sigurno pretpostaviti da se nikad ne dešavaju.

Ažuriranja istog unosa od strane poslužitelja mogu uzrokovati nedosljednost kod podataka direktorija jer se rezolucija sukoba bazira na vremenskoj oznaci unosa. Najnovije vremenska oznaka modificiraj ima prednost. Ako su podaci na poslužitelju postali nekonzistentni, pogledajte ldapdiff poglavlje u niže navedenim odgovarajućim vezama za informacije o resinkronizirajućim poslužiteljima.

Rezolucija sukoba replikacije zahtijeva da dobavljač osigura vremensku oznaku unosa prije nego što se unos ažurira na dobavljaču. IBM Tivoli Directory Server za i5/OS u V5R4 ranijim verzijama nemaju sposobnost dobaviti tu vrstu informacije. Dakle, rezolucija sukoba replikacije nije primjenjiva na slučajeve u kojima dobavljač nije poslužitelj niže razine. U V6R1, IBM Tivoli Directory Server za i5/OS poslužitelj potrošača, u ovom slučaju, uzima repliciranu vremensku oznaku i ažurira i primjenjuje je bez provjere sukoba.

Bilješka: Ranije verzije IBM Tivoli Directory Servera za i5/OS ne podržavaju rezoluciju sukoba vremenske oznake. Ako vaša topologija sadrži ranije verzije IBM Tivoli Directory Servera za i5/OS, konzistentnost podataka nije osigurana za mrežu.

Promjene sukob mogu se izbjeći pomoću ravnoteže učitavanja, virtualnog preuzimanja IP adrese ili drugim metodama kako bi se osiguralo da su promjene direktorija napravljene na jednom poslužitelju, dok se osigurava automatsko nadilaženje greške na druge poslužitelje ako preferirani poslužitelj nije dostupan.

Ravnoteža učitavanja, kao što je IBM WebSphere Edge Server, ima virtualno host ime koje aplikacije koriste kad šalju ažuriranja u direktorij. Ravnoteža učitavanja je konfigurirana za slanje tih ažuriranja na samo jedan poslužitelj. Ako je

| taj poslužitelj onesposobljen ili nedostupan zbog kvara mreže, ravnoteža učitavanja šalje ažuriranja sljedećem
| dostupnom ravnopravnom poslužitelju dok se prvi poslužitelj ponovno ne uključi i postane dostupan. Pogledajte
| dokumentaciju proizvoda ravnoteže učitavanja za informacije kako instalirati i konfigurirati poslužitelj ravnoteže
| učitavanja.

Srodni zadaci

"Modificiranje postavki dnevnika izgubljeno i nađeno" na stranici 156
Dnevnik izgubljeno i nađeno (LostAndFound.log je default ime datoteke) zapisuje greške koje se dešavaju kao rezultat sukoba replikacije. Postoje postavke koje kontroliraju dnevnik izgubljeno i nađeno uključujući lokaciju i maksimum veličine datoteke i arhiviranje starih datoteka dnevnika.

"Kreiranje jednostavne topologije s ravnopravnom replikacijom" na stranici 146
Ravnopravna replikacija je topologija replikacije u kojoj ima više glavnih poslužitelja. Koristite ravnopravnu replikaciju jedino u okolinama u kojima su vektori ažuriranja dobro poznati.

Srodne reference

"ldapdiff" na stranici 232
Pomoćni programi reda za naredbe LDAP sinkronizacije replike.

Terminologija replikacije

Definicije nekih terminologija korištenih u opisivanju replikacije.

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

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

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

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

Gateway poslužitelj
Poslužitelj koji preusmjeruje sav replikativni promet iz lokalne replikativne stranice gdje se nalazi na druge gateway poslužitelje u replikativnoj mreži. Gateway poslužitelj prima replikativni promet od drugih gateway poslužitelja unutar replikativne mreže, koji onda preusmjeruje na sve poslužitelje na svom lokalnom replikativnom mjestu. Gateway poslužitelji moraju biti glavni (na njih se može pisati).

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

Ugniježđeno podstablo
Podstablo unutar repliciranog podstabla direktorija.

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

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

Podstablo replike
Ispod replika unosa grupe, jedan ili više unosa s objectclass ibm-replicaSubentry mogu biti kreirani; jedan za

svaki poslužitelj koji sudjeluje u replikaciji kao dobavljač. Podstablo replike identificira ulogu koju poslužitelj ima u replikaciji: glavni ili samo za čitanje. Poslužitelj samo za čitanje bi mogao imati ugovore replikacije koji podržavaju kaskadnu replikaciju.

Replicirano podstablo
Dio DIT-a koje je bilo replicirano iz jednog poslužitelja na drugi. Pod ovim oblikovanjem, dano podstablo se može replicirati na neke poslužitelje, a ne može se na druge. Na podstablo se može pisati na danom poslužitelju, dok se s drugih podstabala može samo čitati.

Replikativna mreža
Mreža koja sadrži povezane replikativne stranice.

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

Kontekst replikacije
Identificira korijen podstabla replikacije. ibm-replicationContext pomoćna klasa objekta može biti dodana u unos da ga označi kao korijen replikativnog područja. Informacije koje se odnose na topologiju replikacije se održavaju u skupu unosa kreiranih pod kontekstom replikacije.

Replikativna stranica
Gateway poslužitelj i bilo koji glavni, ravnopravni ili replika poslužitelji konfigurirani da repliciraju zajedno.

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

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

Višenitna replikacija

Pomoću višenitne (asinkrone) replikacije, administratori mogu replicirati pomoću višestrukih niti, poboljšavajući ukupni protok replikacije.

Kod upotrebe jednonitne (sinkrone) replikacije, moguće je da klijenti dosljedno ažuriraju brže nego što replikacija može slati promjene na druge poslužitelje. To je zato što standardni model replikacije koristi jednostruku nit za repliciranje svih promjena redom kojim ih zaprima.

Standardni model replikacije također blokira kada se dese određeni tipovi grešaka, na primjer, ako replicirani zahtjev modificiraj ne uspije jer ciljni unos ne postoji na poslužitelju potrošača. Dok takvo ponašanje ukazuje na neslaganja između poslužitelja koja bi se trebala ispraviti, to može dovesti i do sve većeg zaostatka promjena koje su još u toku. U nekim aplikacijama, tak zaostatak nerepliciranih promjena može biti nepoželjan.

Kako bi se to riješilo, višenitna replikacija također osigurava sposobnost zapisivati informacija o neuspjelim promjenama u dnevnik grešaka, te zatim nastavlja s preostalim promjenama. Dnevnik osigurava dovoljno informacija da se odredi koji unosi imaju neslaganja i koje su promjene preskočene, zajedno s alatima za ponovno pokušavanje promjena nakon ispravljanja grešaka. Kako bi se spriječilo preskakanje velikog broja promjena zbog glavnih neslaganja, osiguran je podesiv prag greške; kad se dosegne, replikacija će blokirati dok se greške ne isprave, a dnevnik grešaka replikacije ne obriše.

- Može biti teško upravljati višenitnom (asinkronom) replikacijom ako poslužitelji mreža nisu pouzdani, što uzrokuje da mnoge replicirane promjene budu preskočene.

Kada se greške dogode, one se zapisuju i administrator ih može ponoviti, ali se dnevnici grešaka moraju pažljivo nadgledati. Slijedi pretraživanje koje prikazuje zaostatak za sve ugovore koje je dobavio jedan poslužitelj:

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

Ako je stanje replikacije aktivno, a brojanje u toku još raste, postoji zaostatak koji se neće smanjiti osim ako se ne smanji brzina ažuriranja ili ako se način replikacije ne promijeni iz sinkronog u asinkroni (višenitni).

Replikacija također ima utjecaja na radno opterećenje na glavnom poslužitelju gdje se ažuriranja najprije primjenjuju. Osim ažuriranja svoje kopije podataka direktorija, glavni poslužitelj mora slati promjene na sve replika poslužitelje. Ako vaša aplikacija ili korisnici ne ovise o izravnoj replikaciji, tada će pažljivo raspoređivanje replikacije za izbjegavanje vršnog vremena aktivnosti pomoći smanjiti utjecaj na protok glavnog poslužitelja.

Za višenitnu replikaciju, kad se desi greška replikacije, dešava se sljedeće:

- ibm-slapdReplMaxErrors: 0 znači da se nijedna greška ne smije zapisati u dnevnik grešaka replikacije, ali se te greške zapisuju u dnevnik poslužitelja, a replikacija je odgođena dok se sve greške ne obrišu.
- Ako broj grešaka za granica premaši granicu, replikacija se odgađa dok se barem jedna greška ne obriše ili dok se broj grešaka za granicu ugovora ne poveća.
- Status za ugovor replikacije jest:

```
ibm-replicationStatus: dnevnik grešaka pun
```

Tablica grešaka replikacije

Tablica grešaka replikacije zapisuje neuspjela ažuriranja za kasnije obnavljanje. Kad se replikacija pokrene, broj kvarova prijavljenih za svaki ugovor replikacija se broji. To se brojanje povećava ako ažuriranje rezultira kvarom, a novi se unos dodaje u tablicu.

Svaki unos u tablici grešaka replikacije sadrži sljedeće:

- ID ugovora replikacije.
- ID promjene replikacije.
- Vremensku oznaku za kad je ažuriranje pokušavano.
- Broj pokušaja (ova vrijednost je po defaultu 1 i povećava se nakon svakog pokušaja).
- Kod rezultata od potrošača.
- Sve informacije od operacije replikacije koje pripadaju ažuriranju, na primjer, DN, stvarni podaci, kontrole, oznake i tako dalje.

Ako vrijednost koju je specificirao atribut ibm-slapdReplMaxErrors u konfiguraciji poslužitelja iznosi 0, replikacija nastavlja ažuriranje obrade. Atribut ibm-slapdReplMaxErrors je atribut u unosu konfiguracije replikacije i može mijenjati dinamički.

Ako vrijednost koju je specificirao atribut ibm-slapdReplMaxErrors veća od 0, tada brojanje grešaka za ugovor replikacije premašuje tu vrijednost, replikacija čini jednu od sljedećih stvari:

- **Jednonitni**: Replikacija odlazi u petlju pokušavajući replicirati ažuriranje neuspjeha.
- **Višenitni**: Replikacija je odgođena.

Ako je poslužitelj konfiguriran za upotrebu pojedinačne veze, replikacija pokušava slati isto ažuriranje nakon čekanja 60 sekundi i dalje pokušava dok replikacija ne uspije ili administrator ne preskoči ažuriranje.

Za poslužitelj konfiguriran za upotrebu višestrukih veza, replikacija je odgođena za taj ugovor. Niti primaoci nastavljaju izbor za status iz bilo kojeg ažuriranja koje je poslano, ali se više ne replicira nijedno ažuriranje. Za nastavak replikacije, administrator direktorija mora očistiti najmanje jednu grešku za taj ugovor ili povećati granicu s dinamičkom modifikacijom konfiguracije poslužitelja.

Za više informacija, pogledajte poglavlje Upravljanje redovima replikacije u niže navedenim odgovarajućim vezama. Također pogledajte -op controlreplerr opciju u ldapexop poglavlju u niže navedenim odgovarajućim vezama.

Srodni zadaci

"Upravljanje redovima replikacije" na stranici 155
Koristite ovu informaciju za nadgledanje statusa replikacije za svaki ugovor (red) replikacije koji koristi ovaj poslužitelj.

Srodne reference

"ldapexop" na stranici 212
Pomoćni program reda za naredbe LDAP proširene operacije.

Ugovori replikacije

Ugovor replikacije je unos u direktorij s klasom objekta **ibm-replicationAgreement** koja je kreirana ispod podunosa replike za definiranje replikacije iz poslužitelja kojeg predstavlja podunos na drugi poslužitelj.

Ti objekti su slični unosima replicaObject koji koriste prethodne verzije Poslužitelja direktorija. Ugovor replikacije se sastoji od sljedećih stavki:

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

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

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

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

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

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

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

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

Za ugovor replikacije koji koristi jednonitne metode replikacije, broj povezivanja potrošača uvijek je jedan, vrijednost atributa se zanemaruje. Za ugovor koji koristi višenitnu replikaciju, broj povezivanja može se konfigurirati od 1 do 32. Ako nikakva vrijednost nije specificirana na ugovoru, broj povezivanja potrošača je postavljen na jedan.

Bilješka: Za cn=ibmpolicies podstablo, svi ugovori replikacije će koristiti jednonitnu metodu replikacije i jedno povezivanje potrošača, zanemarujući vrijednosti atributa.

Kako se informacije replikacije pohranjuju u poslužitelju

Informacije o replikaciji pohranjuju se u direktorij na nekoliko mjesta.

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

Sigurnosna razmatranja o informacijama replikacije

Pregled sigurnosnih razmatranja za određene objekte.

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

Replikacija u visoko dostupnom okruženju

Poslužitelj direktorija je često korišten u jedinstvena prijava rješenjima, što može rezultirati u jednom mjestu neuspjeha.

Directory Server se može učiniti visoko dostupnim upotrebom replikacije na dva načina: pomoću preuzimanja IBM ravnoteže učitavanja ili IP adrese. Više informacija o tom poglavlju možete pronaći u poglavlju 13.2 IBM Redbooks publikacije *IBM WebSphere V5.1 izvedba, skalabilnost i visoka dostupnost*.

Srodne informacije

IBM WebSphere V5.1 Performanse, skalabilnost i visoka dostupnost

Područja i predlošci korisnika

Područje i objekti predloška korisnika nađeni u Web administration tool koriste se kako bi se korisniku olakšala obveza da razumije neka temeljna LDAP pitanja.

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

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

Kada dodate novo područje, vi kreirate objekt ibm-područja u direktoriju. Objekt ibm-područja prati svojstva područja kao što su podaci o tome gdje su definirani korisnici i grupe i koji će se predložak koristiti. Objekt ibm-područja može ukazivati na postojeći unos direktorija koji je nadređeni korisnicima ili može ukazivati na samog sebe (default) čineći se tako spremnikom za nove korisnike. Na primjer, možete imati postojeći cn=users,o=acme,c=us spremnik i kreirati područje pod imenom korisnici drugdje u direktoriju (možda u objektu spremnika pod nazivom cn=realms,cn=admin stuff,o=acme,c=us) koji identificira cn=users,o=acme,c=us kao lokaciju za korisnike i grupe. Time se kreira objekt ibm-područja:

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

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

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

Srodni koncepti

“Zadaci područja i predložaka korisnika” na stranici 193
Koristite ovu informaciju za upravljanje područjima i predlošcima korisnika.

Srodni zadaci

“Kreiranje područja” na stranici 194
Koristite ovu informaciju za kreiranje područja.

Parametri pretraživanja

Da bi ograničili broj resursa korištenih od strane poslužitelja, administrator može postaviti parametre pretraživanja da ograniči korisničke mogućnosti pretraživanja. Mogućnosti pretraživanja se također mogu proširiti za posebne korisnika.

Korisnička pretraživanja mogu biti ograničena ili proširena koristeći ove metode:

Ograničeno pretraživanje

- Pretraživanje na stranici
- Sortirano pretraživanje
- Onemogući alias dereferenciranje

Prošireno pretraživanje

- Pretraživanje grupa ograničenja

Pretraživanje na stranici

Stranični rezultati dozvoljavaju klijentu da upravlja količinom podataka vraćenih iz zahtjeva pretraživanja. Klijent može zahtijevati podskup unosa (stranicu) umjesto primanja svih rezultata od poslužitelja odjednom. Sljedeći zahtjevi za pretraživanje vraćaju sljedeću stranicu rezultata dok operacija nije opozvana ili je vraćen zadnji rezultat.

Administrator može ograničiti njegovo korištenje samo dozvoljavajući administratorima da ga koriste.

Sortirano pretraživanje

Sortirano pretraživanje dozvoljava klijentu da primi rezultate pretraživanja sortirane po listi kriterija, gdje svaki kriterij predstavlja ključ sortiranja. Time se premješta odgovornost za sortiranje iz aplikacije klijenta na poslužitelja. Administrator može ograničiti njegovo korištenje samo dozvoljavajući administratorima da ga koriste.

Onemogući alias dereferenciranje

Unos direktorija s objectclass aliasa ili aliasObject sadrži atribut aliasedObjectName, koji je korišten kao referenca na drugi unos u direktoriju. Samo zahtjevi za pretraživanje mogu navesti da li se aliasi koriste. *Dereferenciranje* znači da se traži trag aliasa natrag do originalnog unosa. Odzivno vrijeme IBM Poslužitelja direktorija za pretraživanja s opcijom alias dereferenciranja postavljenom na **uvijek** ili **pretraži** može biti bitno duži nego pretraživanje s opcijom dereferenciranja postavljenom na **nikada**, čak i ako unosi aliasa ne postoje u direktoriju. Dvije postavke određuju dereferencirajuće ponašanje aliasa poslužitelja: opcija dereferenciranja navedena u klijentovom zahtjevu za pretraživanje i opcija dereferenciranja kao što je konfigurirana u poslužitelju od strane administratora. Ako je tako konfiguriran, poslužitelj može automatski zaobići alias dereferenciranje ako u direktoriju ne postoje alias objekti kao i nadjačati opcije dereferenciranja navedene u zahtjevima za pretraživanje klijenta. Sljedeća tablica opisuje kako je alias dereferenciranje raspršeno između klijenta i poslužitelja.

Tablica 2. Stvarno alias dereferenciranje bazirano na postavkama klijenta i poslužitelja

Poslužitelj	Klijent	Stvaran
nikada	bilo koja postavka	nikada
uvijek	bilo koja postavka	postavka klijenta
bilo koja postavka	uvijek	postavlja poslužitelja
traženje	naći	nikada
naći	traženje	nikada

Pretraživanje grupa ograničenja

Administrator može kreirati grupe ograničavanja pretraživanja koje mogu imati fleksibilnije granice pretraživanja od običnih korisnika. Individualnim članovima ili grupama sadržanim u grupi ograničavanja pretraživanja je dana manje ograničavajuća granica pretraživanja nego što je postavljena za obične korisnike.

Kada korisnik započinje pretraživanje, ograničenja zahtjeva za pretraživanje su prvo provjerena. Ako je korisnik član grupe ograničavanje pretraživanja, ograničenja se uspoređuju. Ako su ograničenja grupe ograničavanja pretraživanja veća od onih zahtjeva pretraživanja, korištena su ograničenja zahtjeva za pretraživanje. Ako su ograničenja zahtjeva za pretraživanje veća oda onih grupe ograničavanja pretraživanja, korištena su ona od grupe ograničavanja pretraživanja. Ako nisu pronađeni unosi grupe ograničavanja pretraživanja, ista usporedba je napravljena na ograničenje pretraživanja poslužitelja. Ako ograničenja pretraživanja poslužitelja nisu postavljena, usporedba je napravljena na osnovu default postavki poslužitelja. Korištena ograničenja su uvijek najniže postavke u usporedbi.

Ako korisnik pripada u više grupa ograničavanja pretraživanja, korisniku je dozvoljeno do najveće razine mogućnosti pretraživanja. Na primjer, korisnik pripada grupi pretraživanja 1, koja daje veličinu pretraživanja ograničenu na 2000 unosa i vrijeme pretraživanja od 4000 sekundi i grupi pretraživanja 2, koja dozvoljava granicu pretraživanja neograničene veličine i vrijeme pretraživanja od 3000 sekundi. Korisnik ima ograničenje pretraživanja neograničene veličine i vrijeme pretraživanja od 4000 sekundi.

Grupe ograničavanja pretraživanja mogu biti pohranjene pod localhost ili IBMpolicies. Grupe ograničavanja pretraživanja pod IBMpolicies su replicirane; one pod localhost nisu. Možete pohraniti istu grupu ograničavanja pretraživanja pod localhost i IBMpolicies. Ako grupa ograničavanja pretraživanja nije pohranjena pod jedan od ovih DN-a, poslužitelj ignorira dio ograničavanja pretraživanja grupe i tretira gakao normalnu grupu.

Kada korisnik započinje pretraživanje, unosi grupe ograničavanje pretraživanja pod localhost su prvi provjereni. Ako nisu pronađeni unosi za korisnika, unosi grupe ograničavanja pretraživanja pod IBMpolicies su onda pretraženi. Ako su unosi pronađeni pod localhost, unosi grupe ograničavanja pretraživanja pod IBMpolicies nisu provjereni. Unosi grupe ograničavanja pretraživanja pod localhost imaju prioritet nad onima pod IBMpolicies.

Srodni koncepti

"Zadaci grupe ograničavanja pretraživanja" na stranici 129
Koristite ovu informaciju za upravljanje grupama ograničavanja pretraživanja.

Srodni zadaci

"Prilagođavanje postavki pretraživanja" na stranici 122
Koristite ovu informaciju za kontroliranje korisničkih sposobnosti pretraživanja.

"Pretraživanje unosa direktorija" na stranici 188
Koristite ovu informaciju za pretraživanje unosa direktorija.

Pitanja podrške nacionalnim jezicima (NLS)

NLS razmatranja uključuju formate podataka, znakove, metode mapiranja i slučaj niza.

Vodite računa o sljedećim NLS razmatranjima:

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

Srodne informacije

i5/OS globalizacija
Pogledajte i5/OS globalizaciju za više informacija o NLS razmatranjima.

Oznake jezika

Termin *oznake jezika* definira mehanizam koji omogućuje Directory Serveru da pridruži kodove prirodnog jezika s vrijednostima koje se nalaze u direktoriju i omogućava klijentima da direktoriju šalju upite za vrijednosti koje odgovaraju određenim zahtjevima prirodnog jezika.

Oznaka jezika je komponenta opisa atributa. Oznaka jezika je niz znakova s prefiksom lang-, primarna podoznaka abecednih znakova i, opcijski, sljedeće podoznake povezane s crticom (-). Sljedeće podoznake mogu biti bilo koja kombinacija abecednih znakova; samo primarna podoznaka treba biti abecedna. Podoznake mogu biti bilo koje dužine; jedino ograničenje je da ukupna veličina ne može premašiti 240 znakova. Oznake jezika nisu osjetljive na veličinu slova; en-us i en-US i EN-US su identični. Oznake jezika nisu dozvoljene u komponentama DN ili RDN. Dozvoljena je samo jedna oznaka jezika po opisu atributa.

Bilješka: Po atributnoj bazi, oznake jezika su međusobno isključive s jedinstvenim atributima. Ako ste odredili određeni atribut da bude jedinstveni atribut, on ne može imati oznake jezika povezane sa sobom.

Ako su oznake jezika uključene kada su podaci dodani u direktorij, one mogu biti korištene kod operacija pretraživanja da selektivno dohvate vrijednosti atributa u određenim jezicima. Ako je oznaka jezika dana u opisu atributa unutar zahtijevane liste pretraživanja, onda samo vrijednosti atributa u unosu direktorija koje imaju istu oznaku jezika kao i dana oznaka trebaju biti vraćene. Tako za pretraživanje poput:

```
ldapsearch -b "o=ibm,c=us" (objectclass=organization) description;lang-en
```

poslužitelj vraća vrijednosti atributa ″description;lang-en″, ali ne vraća vrijednosti atributa ″description″ ili″description;lang-fr″.

Ako je zahtjev napravljen navođenjem atributa bez davanja oznake jezika, onda su vraćene sve vrijednosti atributa bez obzira na njihov jezik.

Tip atributa i oznaka jezika su odvojene sa znakom točka-zarez (;).

Bilješka: Znak točka-zarez je dozvoljen za korištenje u ″NAME″ dijelu AttributeType. Međutim, zato što je taj znak korišten za odvajanje AttributeType od oznake jezika, njegovo korištenje u ″NAME″ dijelu AttributeType nije dozvoljeno.

Na primjer, ako klijent zahtjeva ″description″ atribut i podudarajući unos sadrži:

```
objectclass: top
objectclass: organization
o: Software GmbH
description: software
description;lang-en: software products
description;lang-de: Softwareprodukte
postalAddress: Berlin 8001 Germany
postalAddress;lang-de: Berlin 8001 Deutschland
```

poslužitelj vraća:

```
description: software
description;lang-en: software products
description;lang-de: Softwareprodukte
```

Ako pretraživanje zahtijeva ″description;lang-de″ atribut, onda poslužitelj vraća:

```
description;lang-de: Softwareprodukte
```

Korištenje oznaka jezika dozvoljava više-jezične podatke u direktorijima koji mogu podržati klijente koji operiraju s više jezika. Korištenjem oznaka jezika, aplikacija može biti napisana tako da Njemački klijent vidi samo podatke unesene za lang-de atribut i Francuski klijent vidi samo podatke unesene za lang-fr atribut.

Da bi odredili da li je funkcija oznake jezika omogućena, izdajte korijensko DSE pretraživanje navođenjem atributa ″ibm-enabledCapabilities″.

```
ldapsearch -b "" -s base objectclass=* ibm-enabledCapabilities
```

Ako je OID ″1.3.6.1.4.1.4203.1.5.4″ vraćen, funkcija je omogućena.

Ako podrška oznaka jezika nije omogućena, bilo koja LDAP operacija koja pridružuje oznaku jezika s atributom je odbijena s porukom greške.

Neki atributi mogu imati oznake jezika pridružene s njima, dok neki ne mogu. Da bi odredili da li atribut dozvoljava oznake jezika, upotrijebite ldapexop naredbu:

- Za atribute koji dozvoljavaju oznake jezika: ldapexop -op getattributes -attrType language_tag -matches true
- Za atribute koji ne dozvoljavaju oznake jezika: ldapexop -op getattributes -attrType language_tag -matches false

Srodni zadaci

“Dodavanje unosa koji sadrži atribute s oznakama jezika” na stranici 185
Koristite ovu informaciju za kreiranje unosa koji sadrži atribute s oznakama jezika.

Referali LDAP direktorija

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

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

Bilješka: S Directory Serverom, referalni objekti moraju sadržavati samo razlikovno ime (dn), objectClass (objectClass) i referalni (ref) atribut. Pogledajte ldapsearch naredbu za primjer koji ilustrira to ograničenje.

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

Srodni zadaci

"Specificiranje poslužitelja za upućivanja direktorija" na stranici 118
Koristite ovu informaciju za specificiranje referalnih poslužitelja.

Srodne reference

"ldapsearch" na stranici 222
Pomoćni programi reda za naredbe LDAP pretraživanja.

Transakcije

Možete konfigurirati Poslužitelj direktorija kako bi omogućili klijentima da koriste transakcije. Transakcija je grupa operacija LDAP direktorija koje se tretiraju kao jedna jedinica.

Nijedna od pojedinačnih LDAP operacija koje čine transakciju nisu trajne dok se sve operacije u transakciji ne dovrše uspješno i transakcija je predana. Ako bilo koja operacija ne uspije ili je transakcija opozvana, ostale operacije se poništavaju. Ova sposobnost može pomoći korisnicima da LDAP operacije budu organizirane. Na primjer, korisnik može postaviti transakciju na klijenta koji će obrisati nekoliko unosa u direktorij. Ako klijent izgubi vezu s poslužiteljem u toku transakcije, niti jedan unos nije obrisan. Tako korisnik može jednostavno započeti transakciju ponovno, a ne provjeravati koji su unosi uspješno obrisani.

Sljedeće LDAP operacije mogu biti dio transakcije:

- dodavanje
- promjena
- promjena RDN
- brisanje

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

Srodni zadaci

"Specificiranje postavki transakcije" na stranici 116
Koristite ovu informaciju za konfiguriranje postavki transakcije Directory Servera.

Sigurnost Poslužitelja direktorija

Saznajte kako se raznolikost funkcija može koristiti da učini vaš Directory Server sigurnim.

Pogledajte sljedeće poglavlje za više informacija o sigurnosti Poslužitelja direktorija:

Srodni koncepti

"Direktorije" na stranici 3
Directory Server dozvoljava pristup tipu baze podataka koja pohranjuje informacije u hijerarhijsku strukturu sličnu načinu na koji je i5/OS integrirani sistem datoteka organiziran.

"Razlikovna imena (DN-ovi)" na stranici 9
Svaki unos u direktorij ima razlikovno ime (DN). DN je ime koje jednoznačno identificira unos u direktorij. Prva komponenta DN-a se naziva Relativno razlikovno ime (RDN).

"Zadaci svojstava sigurnosti" na stranici 166
Koristite ovu informaciju za upravljanje zadacima sigurnosti.

Srodni zadaci

"Omogućavanje revizije objekta na Directory Server-u" na stranici 121
Koristite ovu informaciju za omogućavanje revizije objekta za Directory Server.

Revizija

Revidiranje vam dozvoljava praćenje detalja određenih transakcija Directory Servera.

Directory Server podržava i5/OS sigurnosno revidiranje. Stavke podložne reviziji uključuju sljedeće:

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

Možda ćete trebati napraviti promjene na postavkama revizije prije nego što će revizija unosa direktorija raditi. Ako sistemska vrijednost QAUDCTL ima specificirano *OBJAUD, možete omogućiti reviziju objekta kroz System i Navigator.

Grupna imena mogu se specificirati za revidiranje. Ovlašteni klijenti mogu zahtijevati da se operacija izvodi pomoću ovlaštenja grupa koje je specificirao klijent umjesto grupa koje poslužitelj pridružuje identitetu klijenta. Ova postavka kontrolira pokazuje li revidiranje tih zahtjeva jedino da je klijent specificirao grupe koje se moraju koristiti ili također uključuje listu specificiranih grupa. Revidiranje liste grupa kreira dodatne unose revizije koji sadržavaju listu grupa za svaki zahtjev.

Za specificiranje trebaju li se grupna imena revidirati, učinite sljedeće:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM poslužitelj direktorija** i izaberite **Svojstva**.
5. Na kartici **Revidiranje**, označite kontrolnu kućicu **Uključi grupna imena kod revidiranja upotrebe specificiranih grupa pozivatelja**.

Srodni koncepti

"Distribuirani direktoriji" na stranici 7
Distribuirani direktorij je okolina direktorija u kojoj se podaci raspodjeljuju preko višestrukih directory servera. Kako bi distribuirani direktorij izgledao kao jednostruki direktorij aplikacijama klijenta, osiguran je jedan ili više proxy poslužitelja koji imaju znanje svih poslužitelja i podataka koje sadržavaju.

Srodni zadaci

"Omogućavanje revizije objekta na Directory Server-u" na stranici 121
Koristite ovu informaciju za omogućavanje revizije objekta za Directory Server.

Srodne informacije

Upute za sigurnost

Revizije sigurnosti
Za više informacija o reviziji pogledajte poglavlje Revizije sigurnosti.

Sloj sigurnih utičnica (SSL) i Sigurnost razine prijenosa (TLS) s Poslužiteljem direktorija

Da bi komunikacija s Directory Server-om bila još sigurnija, Directory Server mora koristiti sigurnost Sloja sigurnih utičnica (SSL) i Sigurnost sloja transporta (TLS).

SSL je standard za Internet zaštitu. SSL možete koristiti za komunikaciju s LDAP klijentima kao i s replikama LDAP poslužitelja. Možete klijentsku provjeru autentičnosti kao dodatak poslužiteljskoj provjeri autentičnosti da date dodatnu sigurnost vašim SSL vezama. Provjera autentičnosti klijenta zahtjeva da LDAP klijent preda digitalni certifikat koji potvrđuje identitet klijenta poslužitelju prije nego što je veza ostvarena.

Za upotrebu SSL-a, morate imati Upravitelj digitalnih certifikata (DCM), opcija 34 od i5/OS, instaliran na sistem. DCM pruža sučelje preko kojega možete kreirati i upravljati digitalnim certifikatima i spremištima certifikata.

TLS je dizajniran kao nasljednik za SSL i koristi iste kriptografske metode, ali podržava više kriptografskih algoritama. TLS omogućava poslužitelj da prima sigurne ili nesigurne komunikacije iz klijenta preko default porta, 389. Radi sigurnih komunikacija klijent mora koristiti StartTLS proširenu operaciju.

Da bi klijent mogao koristiti TLS:

1. Poslužitelj direktorija mora biti konfiguriran da koristi TLS ili SSLTLS.
2. Opcija -Y treba biti navedena na uslužnim programima reda za naredbe klijenta.

Bilješka: TLS i SSL nisu međuoperativni. Izdavanjem pokreni TLS zahtjeva (-Y opcija) preko SSL porta uzrokuje greške u operacijama.

Klijent se može povezati na sigurni port (636) koristeći TLS ili SSL. StartTLS je LDAP značajka koja omogućava sigurnu komunikaciju preko postojeće nesigurne veze (npr. port 389). Kao takav, možete koristiti samo StartTLS (ili uslužni program reda za naredbe -Y opcija) sa standardnim nesigurnim portom (389); ne možete koristiti StartTLS sa sigurnom vezom.

Srodni zadaci

“Omogućavanje SSL-a i sigurnosti sloja prijenosa na Directory Server-u” na stranici 171
Koristite ovu informaciju za omogućavanje SSL-a i sigurnosti sloja prijenosa na Directory Server-u.

“Omogućavanje SSL-a i sigurnosti sloja prijenosa na Directory Server-u” na stranici 171
Koristite ovu informaciju za omogućavanje SSL-a i sigurnosti sloja prijenosa na Directory Server-u.

“Upotreba SSL-a s pomoćnim programima LDAP reda za naredbe” na stranici 235
Koristite ovu informaciju kako biste razumjeli kako koristiti SSL s pomoćnim programima LDAP reda za naredbe.

Srodne informacije

Upravitelj digitalnih certifikata

Sloj sigurnih utičnica (SSL)

Podržani SSL i Transport Layer Security (TLS) protokoli

Kerberos provjera autentičnosti s Poslužiteljem direktorija

Directory Server dozvoljava korištenje Kerberos provjere autentičnosti. Kerberos je protokol provjere autentičnosti mreže koji koristi tajnu kriptografiju ključa kako bi se osigurala vrlo dobra provjera autentičnosti za aplikacije klijenta i poslužitelja.

Da omogućite Kerberos provjeru autentičnosti, morate imati konfiguriran mrežni servis provjere autentičnosti.

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

Kerberos osnovno ime koje poslužitelj koristi ima sljedeći oblik:

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

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

Na primjer, kod sistema pod imenom my-as400 u acme.com TCP/IP domeni s default Kerberos područjem ACME.COM, Kerberos ime principala LDAP poslužitelja bi bilo ldap/my-as400.acme.com@ACME.COM. Default

Kerberos područje je specificirano u Kerberos konfiguracijskoj datoteci (po defaultu, /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) s default_realm direktivom (default_realm = ACME.COM). Poslužitelj direktorija ne može biti konfiguriran da koristi Kerberos provjeru autentičnosti ako default područje nije konfigurirano.

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

- Poslužitelj može kreirati DN na osnovi Kerberos ID-a. Kad izaberete ovu opciju, Kerberos identitet oblika principal@realm generira DN oblika ibm-kn=principal@realm. ibm-kn= je ekvivalent za ibm-kerberosName=.
- Poslužitelj može pretražiti direktorij za razlikovno ime (DN) koje sadrži unos za Kerberos osnovu i područje. Kada izaberete tu opciju, poslužitelj traži u direktoriju unos koji specificira taj Kerberos identitet.

Morate imati datoteku tablice ključeva (keytab) koja sadržava ključ za osnove LDAP usluge.

Srodne informacije

Usluge mrežne provjere autentičnosti
Pogledajte poglavlje Usluge mrežne provjere autentičnosti za više informacija o Kerberosu.

Konfiguriranje usluga mrežne provjere autentičnosti
Pogledajte poglavlje Konfiguriranje usluga mrežne provjere autentičnosti za više informacija o dodavanju informacija u datoteke tablica ključeva (keytab).

Šifriranje lozinke

IBM Tivoli Directory Server omogućuje sprječavanje neovlaštenog pristupa korisničkim lozinkama. Administrator može konfigurirati poslužitelj da šifrira userPassword vrijednosti atributa u jednosmjerni format šifriranja ili u dvosmjerni format šifriranja. Šifrirane lozinke su označene s imenom algoritma šifriranja tako da lozinke šifrirane u različitim formatima mogu istodobno postojati u direktoriju. Kad je konfiguracija šifriranja promijenjena, postojeće šifrirane lozinke ostaju nepromijenjene i nastavljaju rad.

Upotrebom jednosmjernih formata šifriranja, korisničke lozinke se mogu šifrirati i pohraniti u direktorij, što sprečava da čistim lozinkama pristupa bilo koji korisnik uključujući administratore. Pomoću dvosmjernih formata šifriranja, lozinke se šifriraju dok se pohranjuju u bazu podataka i dešifriraju se kod vraćanja ovlaštenom klijentu. Upotreba dvosmjernog šifriranja štiti lozinku koja je pohranjena u bazi podataka, dok podržava upotrebu metoda provjere autentičnosti poput DIGEST-MD5, koje zahtijevaju da poslužitelj ima pristup čistim tekstualnim lozinkama i podražava aplikacije koje mogu trebati čistu tekstualnu lozinku.

Jednosmjerno šifrirane lozinke se mogu koristiti za podudaranje lozinki, ali se ne mogu dešifrirati. Za vrijeme korisničke prijave, lozinka prijave se šifrira i uspoređuje s pohranjenom verzijom za provjeru podudaranja.

Čak i ako je poslužitelj konfiguriran za pohranu novih lozinki u posebni format, prihvatit će lozinke prethodno šifrirane pomoću druge metode. Na primjer, poslužitelj bi mogao biti konfiguriran za upotrebu AES256 šifriranja lozinke, ali i dalje dozvoliti administratoru da učitava podatke s drugog poslužitelja koji sadržava SHA-1 šifrirane lozinke. Oba skupa lozinki mogu se koristiti za provjeru autentičnost do poslužitelja pomoću jednostavne provjere autentičnosti lozinke, ali će se SHA-1 lozinke vratiti kao šifrirani nizovi i ne mogu se koristiti s DIGEST-MD5 provjerom autentičnosti.

Jednosmjerni formati šifriranja su :

- SHA-1
- MD5
- šifriranje

Nakon konfiguriranja poslužitelja, sve nove lozinke (za nove korisnike) ili modificirane lozinke(za postojeće korisnike) se šifriraju prije nego što se pohranjuju u bazu podataka direktorija. Sljedeća LDAP pretraživanje će vratiti označenu i šifriranu vrijednost.

Za aplikacije koje trebaju dohvat čistih lozinki, kao što su srednje vezni agenti provjere autentičnosti, administrator direktorija treba konfigurirati poslužitelj za izvođenje dvosmjerno šifrirajuće šifriranje na korisničkim lozinkama. U toj instanci, čiste lozinke koje poslužitelj vatrozaštićene su ACL mehanizmom direktorija.

Dvosmjerni formati šifriranja su :

- nijedan
- AES

Dvosmjerna opcija šifriranja, AES, osigurana je kako bi se vrijednostima userPassword atributa dozvolilo šifriranje u direktorij i dohvaćanje kao dio unosa u originalnom čistom formatu. Može se konfigurirati za upotrebu 128, 192 i 256-bitnih dužina tipki. Neke aplikacije poput srednje veznih poslužitelj provjere autentičnosti zahtijevaju da se lozinke dohvaćaju u čistom tekstualnom formatu; međutim, korporativne politika sigurnosti mogu zabraniti pohranjivanje čistih lozinku u sekundarnu trajnu memoriju. Ova opcija zadovoljava oba zahtjeva.

Usto, kad se koristi AES šifriranje lozinki u repliciranoj mreži, ako su svi poslužitelj konfigurirani s istom AES prolaznom frazom i salt-om, podaci lozinke će se replicirati u svoj šifrirani oblik, što će bolje zaštititi podatke lozinke. Ako poslužitelj ne podržava AES ili je konfiguriran s različitim AES informacijama, lozinke će se dešifrirati i replicirati kao čisti tekst.

Bilješka:

1. AES nije podržan na pred-V6R1 LDAP poslužiteljima. Specifično, replikacija AES šifriranih podataka nije podržana na pred-V6R1 LDAP poslužitelju.
2. Na drugim platformama, kad je izabrano 'Nijedan', čiste tekstualne lozinke se pohranjuju u bazu podataka. Ako taj poslužitelj sudjeluje u mreži koja uključuje IBM Tivoli Directory Server na drugim platformama, preporuča se upotreba jedne od AES opcija šifriranja.

Jednostavno vezanje će uspjeti ako se dana lozinka u veznom zahtjevu podudara s bilo kojom višestrukom vrijednosti userPassword atributa.

Kad konfigurirate poslužitelj pomoću Web administracija, možete izabrati jednu od sljedećih opcija šifriranja:

nijedan
Lozinke se pohranjuju dvosmjerno šifrirane u validacijskoj listi i dohvaćaju se kao dio unosa u originalnom čistom tekstualnom formatu. Vrijednost QRETSVRSEC sistema mora biti postavljena na 1 za upotrebu ove postavke.

šifriranje
Lozinke kodira UNIX algoritam za kodiranje prije nego što se pohranjuju u direktorij. Kad se koristi šifra, samo se prvih 8 znakova lozinke koristi. Lozinke dulje od 8 znakova se skraćuju.

MD5 Lozinke kodira MD5 algoritam raspršivanja prije nego što se pohranjuju u direktorij.

SHA-1 Lozinke kodira SHA-1 algoritam za kodiranje prije nego što se pohranjuju u direktorij.

AES128
Lozinke šifrira AES128 algoritam prije nego što se pohranjuju u direktorij i dohvaćaju se kao dio unosa u originalnom čistom formatu.

AES192
Lozinke šifrira AES192 algoritam prije nego što se pohranjuju u direktorij i dohvaćaju se kao dio unosa u originalnom čistom formatu.

AES256
Lozinke šifrira AES256 algoritam prije nego što se pohranjuju u direktorij i dohvaćaju se kao dio unosa u originalnom čistom formatu.

Bilješka: Format imask koji je bio dostupan u ranijim izdanjima više nije opcija šifriranja. Međutim, još uvijek vrijede sve postojeće imask šifrirane vrijednosti.

| Default opcija za Tivoli Directory Server za i5/OS je SHA-1, koja je kompatibilna s ranijim izdanjima i ne zahtijeva
| postavljanje AES lozinke i salt.

| Osim userPassword, vrijednosti secretKey atributa su uvijek AES256 šifrirani u direktorij. Za razliku
| userPassword, to se šifriranje provodi za vrijednosti secretKey. Nije osigurana nijedna druga opcija. Atribut
| secretKey IBM definirana shema. Aplikacije mogu koristiti taj atribut za pohranjivanje osjetljivih podataka koji se
| uvijek trebaju šifrirati u direktorij i dohvaćati podatke u čistom tekstualnom formatu pomoću kontrole pristupa
| direktoriju.

| Za promjenu tipa šifriranja pomoću reda za naredbe, na primjer promjena u **crypt**, izdajte sljedeću naredbu:

| ldapmodify -D <adminDN> -w <adminPW> -i <filename>

| where <filename> contains:

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

| Kako bi ažurirane postavke dinamički utjecale, izdajte sljedeću ldapexop naredbu:

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

| **Bilješka:** Za promjenu konfiguracije, morate provjeriti autentičnost pomoću projiciranog korisničkog DN-a i lozinke
| za i5/OS korisnički profil koji ima *ALLOBJ i *IOSYSCFG posebno ovlaštenje. To je istp ovlaštenje
| potrebno za promjenu konfiguracije poslužitelja kroz druga sučelja.

| **Srodni zadaci**

| “Postavljanje svojstva politike lozinke” na stranici 166
| Koristite ovu informaciju za postavljanje svojstva politike lozinke.

Grupe i uloge

Koristite grupe i uloge za organiziranje i kontroliranje pristupa ili dozvola članova.

Grupa je popis, zbirka imena. Grupa se može koristiti u **aclentry**, **ibm-filterAclEntry** i **entryowner** atributima za kontroliranje pristupa ili kod upotreba specifičnih za aplikaciju kao što je lista slanja pošte. Grupe se mogu definirati kao statičke, dinamičke ili ugniježđene.

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

Pogledajte sljedeće za više informacija:

Srodni koncepti

“Lista kontrole pristupa” na stranici 62
Liste kontrole pristupa (ACL-ovi) sadrže sredstvo za zaštitu informacija pohranjenih u LDAP direktoriju. Administratori koriste ACL-ove kako bi ograničili pristup različitim dijelovima direktorija ili određenim unosima direktorija.

“Zadaci korisnika i grupe” na stranici 190
Koristite ovu informaciju za upravljanje korisnicima i grupama.

Srodni zadaci

“Dodavanje grupa” na stranici 192
Koristite ovu informaciju za dodavanje grupa.

“Kreiranje grupa” na stranici 197
Koristite ovu informaciju za kreiranje grupa.

Statičke grupe:

Statička grupa definira svoje članove tako da ih izlistava pojedinačno.

Statička grupa definira pojedinačno svakog člana korištenjem strukturalne klase objekata **groupOfNames**, **groupOfUniqueNames**, **accessGroup** ili **accessRole**; ili pomoćne klase objekata **ibm-staticgroup**. Statička grupa koja koristi **groupOfNames** ili **groupOfUniqueNames** strukturalne klase objekta mora imati barem jednog člana. Grupa koja koristi **accessGroup** ili **accessRole** strukturalnu klasu objekta može biti prazna. Statička grupa može također biti definirana koristeći pomoćnu klasu objekta: **ibm-staticGroup**, što ne zahtijeva **member** atribut i stoga može biti prazno.

Tipičan unos grupe je:

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

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

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

Dinamičke grupe:

Dinamička grupa definira svoje članove pomoću LDAP pretraživanja.

Dinamička grupa koristi strukturalnu klasu objekta **groupOfURLs** (ili pomoćnu klasu objekta **ibm-dynamicGroup**) i atribut, **memberURL** kako bi se definiralo pretraživanje pojednostavljene LDAP URL sintakse.

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

Bilješka: Kako to primjer prikazuje, ime hosta ne smije biti prisutno u sintaksi. Preostali parametri su poput normalne ldap URL sintakse. Svako polje parametra mora biti odijeljeno s ?, čak i kada nije specificiran parametar. Normalno je popis atributa koji se vraća uključen između baznog DN-a i opsega pretraživanja. Ovaj parametar također nije korišten od strane poslužitelja kod određivanja dinamičkog članstva i može se izostaviti, međutim, separator **?** mora svejedno biti prisutan.

gdje je :

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

opseg pretraživanja
Specificira raspon pretraživanja. Default opseg je bazni.

- **base** Vraća informacije samo o baznom DN-u specificiranom u URL-u
- **jedan** Vraća informacije o unosima jednu razinu ispod baznog DN-a specificiranog u URL-u. Ne uključuje bazni unos.
- **sub** Vraća informacije o unosima na svim donjim razinama i uključuje bazni DN.

filter_pretraživanja
Da li je filter koji želite primijeniti na svim unosima unutar opsega pretraživanja. Pogledajte opciju ldapsearch filtera za informacije o sintaksi filtera pretraživanja. Default je objectclass=*

Traženje dinamičkih članova je uvijek interno u poslužitelju, pa za razliku od potpunog ldap URL-a, ime hosta i broj porta nisu nikad specificirani, a protokol je uvijek **ldap** (nikad **ldaps**). **memberURL** atribut može sadržavati bilo koji tip URL-a, ali poslužitelj koristi samo **memberURL** koji počinju s **ldap:///** da odredi dinamičko članstvo.

Primjeri

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

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

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

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

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

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

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

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

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

Slijedi primjer člana cn=GROUP1,ou=Austin:

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

Ugniježđene grupe:

Ugniježđavanje grupa omogućuje kreiranje hijerarhijskog odnosa koji se može koristiti kako bi se definirala naslijeđena članstva grupe.

Ugniježđena grupa je definirana kao unos podređene grupe čiji je DN referenciran atributom sadržanim unutar unosa nadređene grupe. Nadređena grupa je kreirana proširivanjem jedne od klasa objekata strukturalne grupe (**groupOfNames**, **groupOfUniqueNames**, **accessGroup**, **accessRole** ili **groupOfURLs**) s dodavanjem **ibm-nestedGroup** pomoćne klase objekta. Nakon ugniježđenih proširenja grupe, nula ili više **ibm-memberGroup** atribute može biti dodano, s njihovim vrijednostima postavljenim na DN od ugniježđenih grupa djece. Na primjer:

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

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

Hibridne grupe:

Članstvo hibridne grupe opisano je kombinacijom statičkih, dinamičkih i ugniježđenih tipova članova.

Na primjer:

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

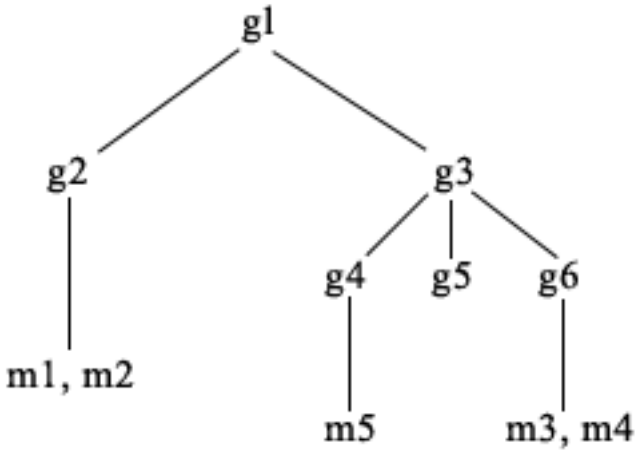
Određivanje članstva grupe:

Dva operativna atributa se mogu koristiti kako bi se ispitalo nakupljeno članstvo grupe.

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

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

Primjeri hijerarhije



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

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

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

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

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

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

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

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

Primjer 1:

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

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


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

Primjer 2:

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

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


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

Primjer 3:

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

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


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

Primjer 4:

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

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


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

Klase objekta grupe za ugniježđene i dinamičke grupe:

Lista klasa objekta grupe za ugniježđene i dinamičke grupe.

ibm-dynamicGroup

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

ibm-dynamicMember

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

ibm-nestedGroup

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

ibm-staticGroup

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

Bilješka: **ibm-staticGroup** je jedina klasa za koju je **član** *opcijski*, sve ostale klase koje uzimaju **član** trebaju najmanje 1 člana.

Tipovi atributa grupe:

Lista tipova atributa grupe.

ibm-allGroups

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

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

ibm-allMembers

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

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

ibm-group

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

ibm-memberGroup

je atribut kojeg uzima pomoćna klasa **ibm-nestedGroup**. Identificira podgrupe unosa nadređene grupe.

Članovi svih takvih podgrupa se smatraju članovima nadređene grupe kada se obrađuju ACL-ovi ili **ibm-allMembers** i **ibm-allGroups** operativni atributi. Sami unosi podgrupe *nisu* članovi. Ugniježđeno članstvo je rekurzivno.

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

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

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

Uloge:

Autorizacija bazirana na ulozi je konceptualna dopuna autorizaciji baziranoj na grupi.

Kao član uloge, imate ovlaštenje da napravite ono što je potrebno za ulogu kako bi se obavio posao. Za razliku od grupe, uloga dolazi s uključenim skupom dozvola. Postoji ugrađena pretpostavka o tome koje se dozvole dobivaju (ili gube) članstvom u grupi.

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

Na primjer, ako postoje skupovi DN-a kao što je 'sys admin', vaša prva reakcija može biti da se o njima razmišlja kao o 'sys admin group' (pošto su grupe najpoznatiji tipovi atributa privilegija). Međutim, pošto postoji skup dozvola koje bi očekivali da primate kao član 'sys admin' skup DN-a može biti preciznije definiran kao 'sys admin role'.

Administrativni pristup

Koristite administrativni pristup za kontrolu pristupa specifičnim administrativnim zadacima.

IBM poslužitelj direktorija dozvoljava sljedeće tipove administrativnog pristupa:

- **Projektirani i5/OS administrator:** Klijent provjerene autentičnosti kao projektirani korisnik (LDAP unos koji predstavlja korisnički profil operativnog sistema) s *ALLOBJ i *IOSYSCFG posebnim ovlaštenjima ima ovlaštenje promijeniti konfiguraciju direktorija pomoću LDAP sučelja (cn=konfiguracijsko podstablo ili zadatak Web administration tool ″Administracija poslužitelja″) i djelovati kao LDAP administrator za ostale unose u direktorij (unosi pohranjeni u jedan od DB2 sufiksa ili shemu). Jedino projicirani i5/OS administratori mogu promijeniti konfiguraciju poslužitelja.
- **LDAP administrator:** Directory Server dozvoljava pojedinačnom korisničkom ID-u (DN) da bude primarni LDAP administrator poslužitelja. Directory Server također dozvoljava da projicirani korisnički profili operativnog sistema budu LDAP administratori. LDAP administratori poslužitelja mogu izvoditi dugačku listu administrativnih zadataka kao što su upravljanje replikacijom, shema i unosi direktorija.
- **Grupa administrativnih korisnika:** Projicirani i5/OS administrator može imenovati nekoliko korisnika da budu u administrativnoj grupi. Članovi te grupe mogu izvoditi mnoge zadatke zato što imaju isti administrativni pristup kao LDAP administrator poslužitelja.

  Bilješka: Kod korištenja Web administracije, zadaci koji nisu dodijeljeni članovima administrativne grupe su onemogućeni.

LDAP administrator ili član administrativne grupe može izvesti sljedeće zadatke administracije poslužitelja:

- Promijeniti vlastitu lozinku.

- Završiti povezivanja.
- Omogućiti i promijeniti politiku lozinke, osim šifriranja lozinke, koju može mijenjati jedino projicirani i5/OS administrator.
- Upravljati jedinstvenim atributima.
- Upravljati shemama poslužitelja.
- Upravljati replikacijom, osim zadatkom replikacijskih svojstava (uključujući bind DN i lozinku glavnog poslužitelja i default upućivanje), što može obaviti jedino projicirani i5/OS administrator.

Srodni koncepti

"Zadaci administrativne grupe" na stranici 127
Koristite ovu informaciju za upravljanje administrativnim grupama.

"DN-ovi povezivanja administratora i kopije" na stranici 86
Možete specificirati projicirani korisnički profil kao DN povezivanja konfiguriranog administratora ili replike. Koristi se lozinka korisničkog profila.

Srodni zadaci

"Dodjeljivanje administratorskog pristupa projiciranim korisnicima" na stranici 119
Koristite ovu informaciju za dodjeljivanje administratorskog pristupa korisničkim profilima.

Proxy autorizacija

Proxy autorizacija je poseban oblik provjere autentičnosti. Korištenjem ovog mehanizma proxy autorizacije, aplikacija klijenta se može vezati na direktorij s vlastitim identitetom, ali joj je dozvoljeno izvođenje operacija u ime drugog korisnika za pristup ciljnom direktoriju. Skup pouzdanih aplikacija ili korisnika može pristupati Poslužitelju direktorija u ime višestrukih korisnika.

Članovi proxy autorizacijske grupe mogu preuzeti bilo koji ovlašteni identitet osim administratora ili članova administratorske grupe.

Grupa proxy autorizacije može biti pohranjena pod localhost ili IBMpolicies. Proxy autorizacijska grupa pod IBMpolicies je replicirana; proxy autorizacijska grupa pod localhost nije. Možete pohraniti proxy autorizacijsku grupu pod localhost i IBMpolicies. Ako proxy grupa nije pohranjena pod jedan od ovih DN-a, poslužitelj ignorira proxy dio grupe i tretira je kao normalnu grupu.

Kao primjer, klijent aplikacija, kllijent1, može se vezati na Poslužitelj direktorija s visokom razinom dopuštenja pristupa. KorisnikA s ograničenim dopuštenjima pošalje zahtjev na klijent aplikaciju. Ako je klijent član proxy autorizacijske grupe, umjesto predavanja zahtjeva na Poslužitelj direktorija kao klijent1, on može poslati zahtjev kao KorisnikA koristeći više ograničavajuće razine dozvola. To znači da umjesto izvođenja zahtjeva kao klijent1, poslužitelj aplikacija može pristupiti samo toj informaciji ili izvesti samo one informacije kojima korisnikA može pristupiti ili izvesti. On izvodi zahtjev u ime ili kao proxy korisnikaA.

Bilješka: Član atributa mora imati svoju vrijednost u obliku DN. Inače je vraćena nevažeća DN sintaksa. Grupnom DN nije dozvoljeno da bude član proxy autorizacijske grupe.

Administratori i članovi administratorske grupe ne mogu biti članovi proxy autorizacijske grupe. Dnevnik revizije zapisuje DN vezivanja i proxy DN za svaku akciju koju izvodi proxy autorizacija.

Srodni koncepti

"Zadaci proxy autorizacijske grupe" na stranici 131
Koristite ovu informaciju za upravljanje proxy autorizacijskim grupama.

Lista kontrole pristupa

Liste kontrole pristupa (ACL-ovi) sadrže sredstvo za zaštitu informacija pohranjenih u LDAP direktoriju. Administratori koriste ACL-ove kako bi ograničili pristup različitim dijelovima direktorija ili određenim unosima direktorija.

Promjene na svakom unosu i atributu u direktoriju se mogu kontrolirati korištenjem ACL-ova. ACL za dani unos ili atribut se može naslijediti iz svojeg nadređenog unosa ili se može izričito definirati.

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

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

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

Postoje dvije vrste lista kontrole pristupa koje možete izabrati: filter-zasnovani ACL-ovi i ne-filtrirani ACL-ovi. Nefiltrirani ACL-ovi se izričito primjenjuju na unos direktorija koji ih sadrži, ali se mogu proširiti na nijedan ili na sve unose koji ih nasljeđuju. ACL-ovi bazirani na filteru se razlikuju po tome što oni koriste usporedbu baziranu na filteru upotrebom specificiranog filtera objekta, za usporedbu ciljnih objekata s učinkovitim pristupom koji se na njih odnosi.

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

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

Za dodatne informacije pogledajte sljedeće:

Srodni koncepti

“Grupe i uloge” na stranici 55
Koristite grupe i uloge za organiziranje i kontroliranje pristupa ili dozvola članova.

“Zadaci Liste kontrole pristupa (ACL)” na stranici 201
Koristite ovu informaciju za upravljanje lista kontrole pristupa (ACL-a).

“Operativni atributi” na stranici 88
Postoji nekoliko atributa koji imaju posebno značenje na Poslužitelju direktorija, a koji se nazivaju operativnim atributima. To su atributi koje održava poslužitelj i oni odražavaju informacije o unosu kojima rukuje poslužitelj ili utječu na operaciju poslužitelja.

“Uređivanje lista kontrole pristupa” na stranici 186
Koristite ovu informaciju za upravljanje lista kontrole pristupa (ACL-a).

“Uređivanje ACL-ova na području” na stranici 198
Koristite ovu informaciju za uređivanje ACL-ova na području.

Srodni zadaci

“Uređivanje ACL-ova na predlošku” na stranici 201
Koristite ovu informaciju za uređivanje ACL-ova na predlošku.

Filtrirane liste kontrole pristupa:

ACL (liste kontrole pristupa) baziran na filtriranju koriste usporedbu baziranu na filtriranju, pomoću specificiranog filtera objekta za podudaranje ciljnih objekata s učinkovitim pristupom koji se na njih odnosi.

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

Default ponašanje filter-zasnovanih ACL-ova je da prikuplja od najniže sadržanog unosa, preko lanca unosa prethodnika, do unosa koji je sadržan na vrhu DIT-a. Učinkovit pristup se izračunava kao unija dodijeljenih ili odbijenih prava pristupa od strane sastavnih unosa prethodnika. Postoji iznimka od tog ponašanja. Radi kompatibilnosti s funkcijom replikacije podstabla i da bi dozvolili veću administrativnu kontrolu, atribut stropa je korišten kao način zaustavljanja skupljanja na unosu na kojem je sadržan.

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

- ibm-filterAclEntry
- ibm-filterAclInherit

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

Srodni koncepti

“Širenje” na stranici 67
Kada unos nema aclEntry ili entryOwner izričito definirano, nasljeđuje se iz prethodnika ili se širi niz stablo.

Sintaksa atributa kontrole pristupa:

Atributima Liste kontrole pristupa (ACL) može se upravljati pomoću sistema označavanja LDAP format izmjenjivanja podataka (LDIF). Sintaksa za nove atribute filter-zasnovanog ACL-a je modificirana verzija trenutnih atributa ne-filter-zasnovanog ACL-a.

Sljedeće definira sintaksu za informacije o kontroli pristupa (ACI) i atribute entryOwner pomoću baccus naur obrasca(BNF).

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

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

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

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

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

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

<subjectDn> ::= <DN>

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

<pseudoDn> ::= "group:cn=anybody" | "group:cn=authenticated" |
                       "access-id:cn=this"
<object filter> ::= niz za pretragu filtera kako je definirano u RFC 2254, odlomak 4
                                (prošireno podudaranje nije podržano).
```

```
<rights> ::= <accessList> [":" <rights> ]

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

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

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

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

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

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

<attributeName> ::= attributeType name as described in RFC 2251, section 4.1.4.
                       (dozvoljeno je OID ili alfanumerički niz s izvornom
                        abecedom, "-" i ";")

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

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

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

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

Subjekt

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

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

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

Sve grupe direktorija se mogu koristiti u kontroli pristupa.

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

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

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

Pseudo DN

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

Trenutno su definirana tri pseudo DN-a:

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

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

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

Filter objekta

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

Prava

Prava pristupa se mogu odnositi na cijeli objekt ili na atribute objekta. LDAP prava pristupa su diskretna. Jedno pravo ne implicira drugo pravo. Prava mogu biti kombinirana da omoguće željenu listu prava prateći skup pravila o kojima ćemo kasnije raspravljati. Prava se mogu sastojati od nespecificirane vrijednosti, a to označava da nisu dodijeljena prava pristupa subjektu na ciljnom objektu. Prava se sastoje od tri dijela:

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

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

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

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

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

Bilješka: Za operacije pretraživanja, subjekt mora imati pristup pretraživanja na sve atribute u filteru pretraživanja ili nisu vraćeni unosi. Za vraćene unose iz pretraživanja, subjekt treba imati pristup pretraživanja i čitanja na sve atribute u RDN-u vraćenih unosa ili ti unosi nisu vraćeni.

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

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

IBM definira tri klase atributa koje su korištene u procjeni pristupa korisničkim atributima: **normalna**, **osjetljiva** i **kritična**. Na primjer, atribut **commonName** spada u normalnu klasu, a atribut userpassword spada u kritičnu klasu. Korisnički definirani atributi pripadaju normalnoj klasi pristupa ako nije drugačije specificirano.

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

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

To su atributi koje održava LDAP poslužitelj i njih mogu korisnici direktorija samo čitati. **OwnerSource** i **aclSource** su opisani u poglavlju Širenje.

Ograničena klasa atributa koji definiraju kontrolu pristupa su:

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

Svi korisnici imaju pravo čitanja ograničenih atributa, ali samo **entryOwners** mogu kreirati, mijenjati i brisati te atribute.

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

Srodni koncepti

"Širenje"
Kada unos nema aclEntry ili entryOwner izričito definirano, nasljeđuje se iz prethodnika ili se širi niz stablo.

EntryOwner:

Vlasnici unosa imaju potpunu dozvolu da izvode bilo koje operacije na objektu bez obzira na aclEntry.

Osim toga, jedino vlasnici unosa smiju rukovati s aclEntry-jima za taj objekt. Vlasnik unosa je subjekt kontrole pristupa, on se može definirati kao pojedinci, grupe ili uloge.

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

Širenje:

Kada unos nema aclEntry ili entryOwner izričito definirano, nasljeđuje se iz prethodnika ili se širi niz stablo.

Za unose na kojima je bio smješten aclEntry se smatra da imaju izričiti **aclEntry**. Slično tome, ako je **vlasnik unosa** bio postavljen na određenom unosu, taj unos ima izričitog vlasnika. To dvoje se ne isprepliće, unos s izričitim

vlasnikom može, ali ne mora, imati izričiti **aclEntry**, a unos s izričitim **aclEntry** može imati izričitog vlasnika. Ako bilo koja od tih vrijednosti nije izričito prisutna na unosu, nedostajuća vrijednost se nasljeđuje iz čvora prethodnika u stablu direktorija.

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

Bilješka: Filter-zasnovani ACL-ovi se ne šire na način na koji se šire ne-filter-zasnovani ACL-ovi. Oni se šire do svih objekata uparenih uspoređivanjem u pridruženom podstablu.

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

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

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

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

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

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

Srodni koncepti

“Filtrirane liste kontrole pristupa” na stranici 63
ACL (liste kontrole pristupa) baziran na filtriranju koriste usporedbu baziranu na filtriranju, pomoću specificiranog filtera objekta za podudaranje ciljnih objekata s učinkovitim pristupom koji se na njih odnosi.

Procjena pristupa:

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

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

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

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

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

Da bi ograničili prikupljanje filter-baziranih ACL-a u računanju učinkovitog pristupa, **ibm-filterAclInherit** atribut postavljen na vrijednost ″false″ može biti smješten u bilo koji unos između najvećeg i najmanjeg pojavljivanja **ibm-filterAclEntry** u danom podstablu. To uzrokuje zanemarivanje podskupa **ibm-filterAclEntry** atributa iznad njega u lancu prethodnika ciljnog objekta.

U filter-zasnovanom ACL načinu, ako se ne primjenjuje filter-zasnovani ACL, primjenjuje se default ACL (cn=anybody - svatko ima dozvolu čitanja, pretraživanja i uspoređivanja atributa u normalnoj klasi pristupa). Ta se situacija može dogoditi kada se unos kojem se pristupa ne podudara s bilo kojim filterom specificiranim u **ibm-filterAclEntry** vrijednostima. Možda ćete htjeti navesti default filter ACL kao sljedeći ako ne želite da se ova default kontrola pristupa primjeni:

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

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

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

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

Pravilo specificiranja

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

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

Pravilo kombiniranja

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

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

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

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

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

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

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

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

Taj korisnik dobiva:

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

Kod drugog primjera sa sljedećim aclEntry-ima:

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

Korisnik:

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

Razmatranja replikacije podstabla:

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

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

Primjer definiranja ACI-a i vlasnika unosa:

Sljedeća dva primjera pokazuju postavljanje administrativne poddomene pomoću pomoćnih programa reda za naredbe.

Prvi primjer prikazuje jednog korisnika koji se dodjeljuje kao entryOwner za cijelu domenu. Drugi primjer prikazuje grupu koja je dodijeljena kao entryOwner.

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

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

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

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

ibm-filterAclInherit: false
```

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

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

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

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

Primjer promjene vrijednosti ACI-a i vlasnika unosa:

Nekoliko primjera promjene vrijednosti ACI-a i vlasnika unos pomoću pomoćnih programa reda za naredbe.

Modificiranje-zamjena

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

Dani sljedeći ACI-ji za unos:

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

izvode sljedeće promjene:

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

Rezultirajući ACI je:

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

ACI vrijednosti za Dept ABC su izgubljene zamjenjivanjem.

Dani sljedeći ACI-ji za unos:

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

izvode sljedeće promjene:

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

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

Rezultirajući ACI je:

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

ACI vrijednosti za Dept ABC su izgubljene zamjenjivanjem.

Modificiraj-dodaj

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

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

s preinakom:

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

bi proizveo aclEntry s više vrijednosti:

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

Na primjer, dani ACI:

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

s preinakom:

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

bi proizveo aclEntry s više vrijednosti:

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

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

Na primjer, ako je dan sljedeći ACI:

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

s preinakom:

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

proizvest će se aclEntry:

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

Na primjer, ako je dan sljedeći ACI:

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

s preinakom:

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

proizvest će se aclEntry:

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

Modificiraj-obriši

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

Dani ACI:

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

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

proizvodi preostali ACI na poslužitelju :

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

Dani ACI:

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

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

proizvodi preostali ACI na poslužitelju :

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

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

Primjer brisanja vrijednosti ACI-a i vlasnika unosa:

Primjer brisanja vrijednosti ACI-a i vlasnika unosa pomoću pomoćnih programa reda za naredbe

S ldapmodify-obriši operacijom, entryOwner se može obrisati specificiranjem

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

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

Isto se može napraviti kako bi se aclEntry sasvim obrisao:

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

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

Primjer dohvaćanja vrijednosti ACI-a i vlasnika unosa:

Primjer dohvaćanja vrijednosti ACI-a i vlasnika unosa pomoću pomoćnih programa reda za naredbe

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

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

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

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

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

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

Vlasništva objekata LDAP direktorija

Svaki objekt u LDAP direktoriju ima najmanje jednog vlasnika. Vlasnici objekata imaju tu moć da mogu brisati objekte. Vlasnici i administrator poslužitelja su jedini korisnici koji mogu mijenjati vlasnička svojstva i listu kontrole pristupa (ACL) objekta. Vlasništvo nad objektom može biti naslijeđeno ili eksplicitno.

Za dodjelu vlasništva možete izaberite jednu od sljedećih opcija:

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

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

Srodni koncepti

“Zadaci unosa direktorija” na stranici 184
Koristite ovu informaciju za upravljanje unosima direktorija.

Politika lozinke

Kada se koriste LDAP poslužitelji za provjeru autentičnosti, važno je da LDAP poslužitelj podržava politike koje se odnose na istek dozvole, neuspjeli pokušaj prijave i pravila lozinke. Poslužitelj direktorija osigurava konfigurabilnu podršku za sve tri vrste politika.

Politika lozinka primjenjuje se na sve unose direktorija koji imaju userPassword atribut. Ne možete definirati jednu politiku za jedan skup korisnika, a druge politike za druge skupove korisnika. Poslužitelj direktorija osigurava i mehanizam kojim će se klijenti obavijestiti o stanjima koja se odnose na lozinku (lozinka ističe kroz tri dana) i skup operativnih atributa koje administrator može koristiti za traženje takvih stvari kao što su korisnici s lozinkama koje su istekle ili korisnici sa zaključanim računima.

Konfiguracija

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

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

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

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

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

```
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 svjesne politike lozinka

Podrška politike lozinka Directory Servera uključuje skup LDAP lozinka koje može koristiti aplikacija svjesna politike lozinka za primanje obavijesti uvjeta vezanih uz dodatnu politiku lozinka.

Aplikacija se može informirati o sljedećim stanjima upozorenja:

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

Aplikacija se isto tako može informirati o sljedećim stanjima greške:

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

- Nova lozinka je u povijesti

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

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

- ldap_parse_pwdpolicy_response
- ldap_pwdpolicy_err2string

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

Kontrola zahtjeva politike lozinka

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

Kontrola odgovora politike lozinka

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

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

Operativni atributi politike lozinka

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

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

- pwdReset - Booleov atribut koji sadrži vrijednost TRUE ako je lozinka bila resetirana pa ju korisnik mora promijeniti.
- ibm-pwdAccountLocked - Booleov atribut koji označuje da je račun administrativno zaključan.

Replikacija politike lozinka

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

Srodni koncepti

"Zadaci lozinki" na stranici 166
Koristite ovu informaciju za upravljanje zadacima lozinki.

"Operativni atributi" na stranici 88
Postoji nekoliko atributa koji imaju posebno značenje na Poslužitelju direktorija, a koji se nazivaju operativnim atributima. To su atributi koje održava poslužitelj i oni odražavaju informacije o unosu kojima rukuje poslužitelj ili utječu na operaciju poslužitelja.

Savjeti za politike lozinki

Politika lozinka neće se uvijek ponašati kako se i očekuje.

Postoje dva područja gdje se implementacija politike lozinke možda neće ponašati prema očekivanju:

1. Ako pwdReset atribut nije postavljen za unos, klijent se može vezati neograničeno koristeći uneseni DN i lozinku resetiranja. S prisutnim zahtjevom kontrole politike lozinke, ovo rezultira u uspješnom vezivanju s upozorenjem u odgovoru kontrole. Ali ako klijent ne navede kontrolu zahtjeva, ovaj klijent ″ne svjestan politike lozinke″ vidi uspješno vezivanje bez indikacije da lozinka mora biti promijenjena. Sljedeće operacije pod tim DN će i dalje biti neuspješne s greškom ″ne želi izvoditi″; samo početni rezultat vezivanja može izgledati krivo. To može biti pitanje ako je vezivanje napravljeno samo za provjeru autentičnosti, kao što može biti slučaj s web aplikacijama koje koriste direktorij za provjeru autentičnosti.
2. pwdSafeModify i pwdMustChange politike se ne ponašaju kako možete očekivati s aplikacijom koja mijenja lozinke pod identitetom osim DN unosa za kojeg je lozinka mijenjana. U tom scenariju, sigurna promjena lozinke je napravljena pod administrativnim identitetom, na primjer, rezultirat će u postavljanju pwdReset atributa. Aplikacija koja mijenja lozinku može koristiti administratorski račun i ukloniti pwdReset atribut kao što je opisano ranije.

Provjera autentičnosti

Koristite metodu provjere autentičnosti za kontroliranje pristupa unutar Directory Servera.

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

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

- Anoniman
- Administrator direktorija (cn=administrator po defaultu)
- Projicirani i5/OS korisnički profil

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

Iz LDAP perspektiva, okosnice za autorizaciju na LDAP slijede:

- Jednostavno vezanje u kojem aplikacija osigurava DN i lozinku jasnog teksta za taj DN.

- Jednostavna autorizacija i Sloj sigurnosti (SASL), koji omogućuje nekoliko dodatnih metoda autorizacije uključujući CRAM-MD5, DIGEST-MD5, EXTERNAL, GSSAPI i OS400-PRFTKN.

Jednostavno vezanje, DIGEST-MD5 i CRAM-MD5

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

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

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

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

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

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

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

CRAM-MD5 metoda zahtjeva da poslužitelj ima pristup na lozinku jasnog teksta (zaštita lozinke je postavljena na ništa, što ustvari znači da je lozinka pohranjena u dešifriranom obliku i vraćena prilikom pretraživanja kao jasan tekst) i QRETSVRSEC (Zadrži sigurnosne podatke poslužitelja) sistemska vrijednost mora biti 1 (Zadrži podatke). Klijent šalje DN na poslužitelja. Poslužitelj dohvaća vrijednost lozinke korisnika za unos i generira slučajan niz znakova. Slučajan niz znakova se šalje na klijenta. Klijent i poslužitelj raspršuju slučajan niz korištenjem lozinke kao ključa, a klijent šalje rezultat na poslužitelja. Ako se podudaraju dva raspršena niza, zahtjev za vezivanjem je uspješan, a lozinka nije nikad bila poslana na poslužitelja.

DIGEST-MD5 metoda je slična CRAM-MD5. Poslužitelj treba imati pristup lozinci jasnog teksta (zaštita lozinke je postavljena na nulu), a sistemska vrijednost QRETSVRSEC postavljena na 1. Umjesto slanja DN-a na poslužitelj, DIGEST-MD5 zahtijeva da klijent pošalje vrijednost imena korisnika na poslužitelj. Da bi bili sposobni koristiti DIGEST-MD5 za redovitog korisnika (ne administratora) zahtjeva da niti jedan drugi unos u direktoriju nema istu vrijednost za atribut korisničkog imena. Druge razlike s DIGGEST-MD5 uključuju više opcija konfiguracije: područje poslužitelja, atribut korisničkog imena i administratorsku lozinku. Directory Server dozvoljava korisnicima da se povezuju kao projicirani ili objavljeni korisnici, kada poslužitelj provjerava dobavljenu lozinku prema lozinci korisničkog profila na sistemu. S obzirom na to da lozinka jasnog teksta za korisničke profile nije dostupna za poslužitelj, DIGEST-MD5 se ne može koristiti s projiciranim ili objavljenim korisnicima.

Vezivanje objavljenog korisnika

Poslužitelj direktorija omogućava način postojanja LDAP unosa čija lozinka je ista kao korisnički profil operativnog sistema na istom sistemu. Da se to ostvari, unos mora:

- Imati UID atribut, čija vrijednost je ime korisničkog profila operativnog sistema
- Nemati userPassword atribut

Kada poslužitelj primi zahtjev vezivanja za unos koji ima UID vrijednost, ali nema userPassword, poslužitelj poziva sigurnost operativnog sistema da provjeri da je UID valjano ime korisničkog profila i da je navedena lozinka ispravna lozinka za taj korisnički profil. Takav unos se naziva objavljeni korisnik zbog toga jer se objavljuje direktorij distribucije sistema (SDD) na LDAP-u koji kreira takve unose.

Vezivanje projiciranog korisnika

LDAP unos koji predstavlja korisnički profil operativnog sistema se naziva projicirani korisnik. Možete koristiti DN projiciranog korisnika zajedno s ispravnom lozinkom za taj profil korisnika u jednostavnom vezanju. Na primjer, DN za korisnika JSMITH na sistemu my-system.acme.com bi bio:

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

SASL EXTERNAL vezanje

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

Na primjer, dani certifikat je dodijeljen na:

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

DN subjekta bi bio:

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

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

SASL GSSAPI vezanje

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

- Generirati pseudo DN oblika ibm-kn=jsmith@acme.com.
- Tražiti unos koji ima ibm-securityidentities pomoćnu klasu i altsecurityidenties vrijednost oblika KERBEROS:<principal>@<realm>.

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

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

OS400-PRFTKN vezanje

OS400-PRFTKN SASL mehanizam vezanja se koristi kako bi se ovlastilo korisnika na poslužitelja korištenjem oznake profila (pogledajte API Generiranje oznake profila). Kada se koristi taj mehanizam, poslužitelj provjerava valjanost te oznake profila i pridružuje ju DN-u projiciranog profila korisnika s vezom (na primjer, os400-

profile=JSMITH,cn=accounts,os400-system=my-as400.mycompany.com). Ako aplikacija već ima oznaku profila, tim mehanizmom se izbjegava potreba za dohvaćanjem imena profila korisnika i lozinke korisnika kako bi se izvodilo jednostavno vezanje. Za upotrebu ovog mehanizma koristite ldap_sasl_bind_s API, specificirajući nulti DN, OS400-PRFTKN za mehanizam i berval (binarni podaci koji su kodirani pomoću pojednostavljenih osnovnih pravila kodiranja) koji sadrži 32-bitnu oznaku profila za vjerodajnicu. Kod upotrebe LDAP API-a u i5/OS ili pomoću QSH komandnih pomoćnih programa (kao što je ldapsearch) za pristup lokalnom directory server-u, možete izostaviti lozinku, a API-i klijenta će provjeriti autentičnost poslužitelju kao trenutni korisnički profil za posao. Na primjer:

```
> ldapsearch -m OS400-PRFTKN -b "o=ibm,c=us" "(uid=johndoe)"
```

će izvesti pretraživanje pod ovlaštenjem trenutnog korisničkog profila kao da ste koristili:

```
> ldapsearch -D os400-profile=myprofile,cn=accounts,os400-sys=mysystem -w mypassword -b
"o=ibm,c=us" "(uid=johndoe)"
```

LDAP kao usluga provjere autentičnosti

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

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

Web poslužitelj također može pratiti DN koji je bio korišten tako da dana aplikacija može koristiti taj DN, možda pohranjujući podatke prilagodbe u tom unosu, drugi unos povezan s njim ili u posebnoj bazi podataka koristeći DN kao ključ za pronalaženje informacija.

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

Srodni koncepti

"Projicirana pozadina operativnog sistema" na stranici 82
Sistemski projicirana pozadina ima sposobnost mapiratii5/OS objekte kao unose unutar LDAP-pristupnog stabla direktorija. Projicirani objekti su LDAP prikazi objekata operativnog sistema umjesto stvarnih unosa pohranjenih u LDAP bazi podataka poslužitelja.

"Zadaci korisnika" na stranici 190
Koristite ovu informaciju za upravljanje korisnicima.

Lightweight Directory Access Protocol (LDAP) API-ji
Pogledajte Lightweight Directory Access Protocol (LDAP) API-je za više informacija o API-jima Directory Servera.

Srodni zadaci

"Konfiguriranje provjere autentičnosti DIGEST-MD5 na Directory Server-u" na stranici 174
Koristite ovu informaciju za konfiguriranje provjere autentičnosti DIGEST-MD5 na Directory Server-u.

"Omogućavanje provjere autentičnosti Kerberos na Directory Server-u" na stranici 173
Koristite ovu informaciju za omogućavanje provjere autentičnosti Kerberos na Directory Server-u.

Odbijanje usluga

Upotrijebite opciju konfiguriranja odbijanje usluge da biste se zaštitili od napada odbijanjem usluge.

Poslužitelj direktorija štiti od sljedećih tipova napada odbijanjem usluge:

- Klijenti koji šalju podatke sporo, šalju parcijalne podatke ili ne pošalju podatke
- Klijenti koji ne čitaju podatke rezultata ili koji čitaju rezultate sporo
- Klijenti koji se ne odspajaju
- Klijenti koji rade zahtjeve koji proizvode dugotrajne zahtjeve na bazi podataka
- Klijenti koji se vežu anonimno
- Opterećenje poslužitelja koje sprječava administratora da administrira poslužitelj

Poslužitelj direktorija daje administratoru nekoliko metoda sprječavanja napada odbijanjem usluge. Administrator uvijek ima pristup na poslužitelj preko korištenja niti opasnosti čak i ako je poslužitelj zauzet s operacijama koje se dugo izvode. Dodatno, administrator ima kontrolu na poslužitelju preko adrese pristupa poslužitelju uključujući sposobnost da odspoji klijente s određenim vezivajućim DN ili IP adresom i konfigurira poslužitelj da ne dozvoli anonimni pristup. Druge opcije konfiguracije mogu biti aktivirane da dozvole poslužitelju aktivno sprječavanje napada odbijanjem usluge.

Srodni zadaci

"Upravljanje vezama poslužitelja" na stranici 113
Koristite ovu informaciju za gledanje svih veza na poslužitelj i operacija koje te veze izvode.

"Upravljanje svojstvima veze" na stranici 114
Koristite ovu informaciju za postavljanje svojstava veze kao što su one koje sprječavaju da klijenti zaključaju poslužitelj.

Projicirana pozadina operativnog sistema

Sistemski projicirana pozadina ima sposobnost mapiratii5/OS objekte kao unose unutar LDAP-pristupnog stabla direktorija. Projicirani objekti su LDAP prikazi objekata operativnog sistema umjesto stvarnih unosa pohranjenih u LDAP bazi podataka poslužitelja.

Korisnički profili su jedini objekti koji se mapiraju ili projiciraju unutar stabla direktorija. Mapiranje objekata korisničkih profila se referencira kao projicirana pozadina operativnog sistema.

LDAP operacije se mapiraju na podcrtane objekte operativnog sistema i LDAP operacije izvode funkcije operativnog sistema da bi pristupile tim objektima. Sve LDAP operacije izvedene na korisničkim profilima učinjene su pod ovlaštenjem korisničkog profila pridruženog vezi klijenta.

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

Srodni zadaci

"Dodjeljivanje administratorskog pristupa projiciranim korisnicima" na stranici 119
Koristite ovu informaciju za dodjeljivanje administratorskog pristupa korisničkim profilima.

Srodne reference

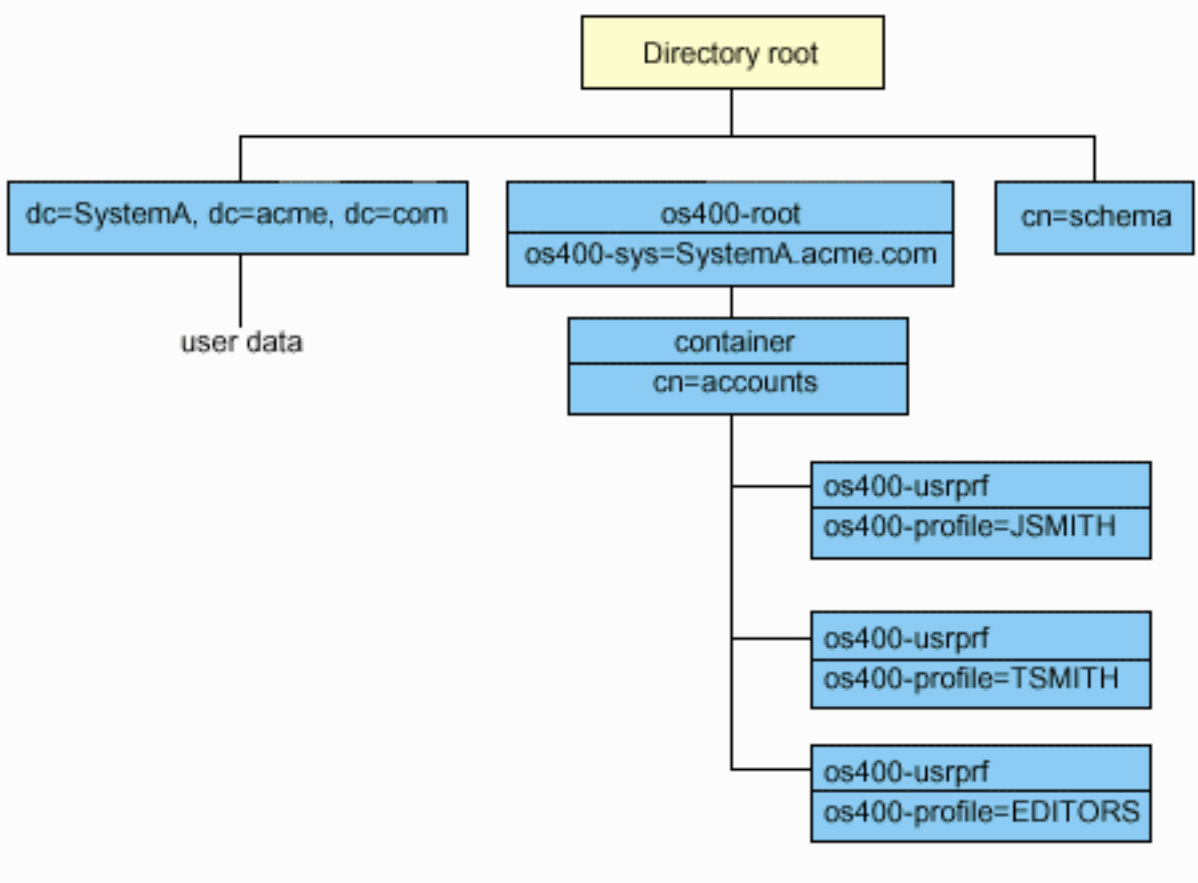
"Provjera autentičnosti" na stranici 78
Koristite metodu provjere autentičnosti za kontroliranje pristupa unutar Directory Servera.

Korisničko projicirano stablo informacija direktorija

Saznajte kako su sufiks i korisnički profili predstavljeni u korisnički projiciranom informacijskom stablu direktorija.

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

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



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

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

LDAP operacije

Spoznajte koje se LDAP operacije mogu izvoditi u projiciranoj pozadini.

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

Vezanje

LDAP klijent se može povezati na (dokazati autentičnost) LDAP poslužitelj koristeći projicirani korisnički profil. To se postiže navođenjem projiciranog razlikovnog imena korisničkog profila (DN) za vezani DN i ispravnu lozinku korisničkog profila za provjeru autentičnosti. Primjer DN korištenog u zahtjevu povezivanja bio bi os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com.

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

Dva dodatna mehanizma su dostupna za provjeru autentičnosti poslužitelja direktorija kao projiciranog korisnika:

- GSSAPI SASL vezanje. Ako je operativni sistem konfiguriran da koristi Mapiranje identiteta u poduzeću (EIM), poslužitelj direktorija šalje upit prema EIM da odredi da li postoji veza između lokalnog korisničkog profila iz inicijalnog Kerberos identiteta. Ako postoji takva asocijacija, poslužitelj će pridružiti profil korisnika vezi i može se koristiti kako bi se pristupilo projiciranoj pozadini sistema.
- OS400-PRFTKN SASL vezanje. Oznaka profila se može koristiti za ovlaštenje na poslužitelj direktorija. Poslužitelj pridružuje vezi oznaku profila korisnika.

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

Traženje

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

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

LDAP administratori mogu zabraniti sve operacije pretraživanja usmjerene prema korisnički projiciranoj pozadini. Za više informacija, pogledajte u poglavlju Pristup čitanju projiciranim korisnicima na niže navedenoj odgovarajućoj vezi.

Sljedeća tablica opisuje ponašanje sistemski projicirane pozadine za operacije traženja.

Tablica 3. Ponašanje sistemske projicirane pozadine za operacije traženja

Traženje zahtijevano	Baza traženja	Opseg traženja	Filter traženja	Komentari
Vrati informacije za os400-sys=SystemA, (opcijski) za spremnike pod njim i (opcijski) za objekte u tim spremnicima.	os400-sys=SystemA.acme.com	baza, pod ili jedan	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	Vrati prikladne atribute i njihove vrijednosti bazirano na specificiranom opsegu i filteru. Hardcoded atributi i njihove vrijednosti se vraćaju za sufiks sistemskog objekta i spremnik pod njim.
Vrati sve korisničke profile.	cn=accounts, os400-sys=SystemA.acme.com	jedan ili pod	os400-gid=0	Samo vrijednosti razlikovnog imena (DN), objectclass i os400-profila se vraćaju za projicirane korisničke profile. Ako je specificiran bilo koji drugi filter, LDAP_UNWILLING_TO_PERFORM se vraća.
Vrati sve grupne profile.	cn=accounts, os400-sys=SystemA.acme.com	jedan ili pod	(!(os400-gid=0))	Samo vrijednosti razlikovnog imena (DN), objectclass i os400-profila se vraćaju za projicirane korisničke profile. Ako je specificiran bilo koji drugi filter, LDAP_UNWILLING_TO_PERFORM se vraća.
Vrati sve korisničke i grupne profile.	cn=accounts, os400-sys=SystemA.acme.com	jedan ili pod	os400-profile=*	Samo vrijednosti razlikovnog imena (DN), objectclass i os400-profila se vraćaju za projicirane korisničke profile. Ako je specificiran bilo koji drugi filter, LDAP_UNWILLING_TO_PERFORM se vraća.
Vrati informacije za specifični korisnički ili grupni profil kao što je korisnički profil JSMITH.	cn=accounts, os400-sys=SystemA.acme.com	jedan ili pod	os400-profile=JSMITH	Ostali atributi koje treba vratiti mogu se specificirati.
Vrati informacije za specifični korisnički ili grupni profil kao što je korisnički profil JSMITH.	os400-profile=JSMITH, cn=accounts, os400-sys=SystemA.acme.com	baza, pod ili jedan	objectclass=os400-usrprf objectclass=* os400-profile=JSMITH	Ostali atributi koje treba vratiti mogu se specificirati. Iako se može specificirati opseg jedne razine, rezultati traženja neće vratiti nijednu vrijednost jer nema ničega ispod korisničkog profila JSMITH u DIT.
Vrati sve korisničke i grupne profile koji počinju s A.	cn=accounts, os400-sys=SystemA.acme.com	jedan ili pod	os400-profile=A*	Samo vrijednosti razlikovnog imena (DN), objectclass i os400-profila se vraćaju za projicirane korisničke profile. Ako je specificiran bilo koji drugi filter, LDAP_UNWILLING_TO_PERFORM se vraća.

Tablica 3. Ponašanje sistemske projicirane pozadine za operacije traženja (nastavak)

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

Usporedba

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

LDAP administratori mogu zabraniti sve operacije usporedbe usmjerene prema korisnički projiciranoj pozadini. Za više informacija, pogledajte u poglavlju Pristup čitanju projiciranim korisnicima na niže navedenoj odgovarajućoj vezi.

Dodavanje i promjena

Možete kreirati korisničke profile koristeći LDAP operaciju dodavanja i možete također promijeniti korisničke profile koristeći LDAP operaciju izmjene.

Brisanje

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

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

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  Kontrolna vrijednost je niz sljedećeg oblika:

  – controlValue ::= ownObjOpt [newOwner]

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

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

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

  Primjeri vrijednosti kontrole su sljedeći:

  – *NODLT: specificira koji se profil ne može brisati ako posjeduje neke objekte.

  – *CHGOWN SMITH: specificira da se vlasništvo nad objektima prenese na korisnički profil SMITH.

- Identifikator objekta (OID) je definiran u ldap.h kao LDAP_OS400_OWNOBJOPT_CONTROL_OID.

  – os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

    Kontrolna vrijednost je definirana kao niz sljedećeg oblika:

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

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

Primjeri vrijednosti kontrole su sljedeći:

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

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

ModRDN

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

API-i za importiranje i eksportiranje

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

Srodni koncepti

Mapiranje identiteta u poduzeću (EIM)

"Pristup čitanja za projicirane korisnike"
Po defaultu, backend projekcije sistema osigurava pristup čitanja informacijama korisničkog profila ovlaštenim korisnicima kroz LDAP operacije pretraživanja i uspoređivanja. Pristup čitanja projiciranim korisnicima može se omogućiti ili onemogućiti pomoću System i Navigator ili postavkom konfiguracije u datoteci /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf (datoteka /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf za instancu default poslužitelja).

DN-ovi povezivanja administratora i kopije

Možete specificirati projicirani korisnički profil kao DN povezivanja konfiguriranog administratora ili replike. Koristi se lozinka korisničkog profila.

Projicirani korisnički profili mogu također postati LDAP administratori ako su ovlašteni za identifikator funkcije Administratora poslužitelja direktorija (QIBM_DIRSRV_ADMIN). Višestrukim korisničkim profilima može se dodijeliti administratorski pristup.

Srodni koncepti

"Administrativni pristup" na stranici 61
Koristite administrativni pristup za kontrolu pristupa specifičnim administrativnim zadacima.

Korisnička projicirana shema

Klase objekata i atributi iz projicirane pozadine mogu se naći u poslužiteljskoj shemi.

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

Pristup čitanja za projicirane korisnike

Po defaultu, backend projekcije sistema osigurava pristup čitanja informacijama korisničkog profila ovlaštenim korisnicima kroz LDAP operacije pretraživanja i uspoređivanja. Pristup čitanja projiciranim korisnicima može se

omogućiti ili onemogućiti pomoću System i Navigator ili postavkom konfiguracije u datoteci /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf (datoteka /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf za instancu default poslužitelja).

Za onemogućavanje pristupa čitanja informacijama korisničkog profila, poduzmite sljedeće korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji>TCP/IP**.
3. Desno kliknite **IBM Tivoli Directory Server** i izaberite **Svojstva**.
4. Izaberite karticu **Baza podataka/Sufiksi**.
5. Maknite oznaku s kontrolne kućice **Dozvoli pristup čitanja informacijama korisnika**.

Sljedeća linija može se promijeniti u stanzi cn=Front End, cn=Configuration datoteke konfiguracije za onemogućavanje operacija pretraživanja i uspoređivanja backendu projiciranog korisnika:

```
ibm-slapdOs400UsrprjRead: TRUE
```

Promijenite vrijednost TRUE ili FALSE za onemogućavanje pristupa čitanja. Ako je vrijednost TRUE ili postavka nije prisutna u datoteci konfiguracije, omogućen je pristup čitanja informacijama projiciranog korisnika.

Srodni zadaci

"Omogućavanje ili onemogućavanje pristupa čitanja projiciranim korisnicima" na stranici 123
Koristite ovu informaciju za zabranu operacija pretraživanja i uspoređivanja backendu projiciranih korisnika.

Srodne reference

"LDAP operacije" na stranici 83
Spoznajte koje se LDAP operacije mogu izvoditi u projiciranoj pozadini.

Directory Server i i5/OS podrška vođenju dnevnika

Directory Server koristi i5/OS podršku baze podataka za pohranjivanje informacija o direktoriju. Directory Server koristi kontrolu predavanja za pohranjivanje unosa direktorija u bazu podataka. To zahtijeva i5/OS podršku vođenju dnevnika.

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

- Dnevnik
- Prijemnik dnevnika
- Tablice baza potrebne za početak

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

Vaše okruženje, veličina i struktura direktorija ili strategija spremanja i obnavljanja može diktirati neke razlike od defaulta, uključujući kako su ti objekti upravljani i korišten prag veličine. Parametre naredbe za vođenje dnevnika možete po potrebi mijenjati. LDAP vođenje dnevnika je postavljeno po defaultu da briše stare primaoce. Ako je dnevnik promjena konfiguriran i želite sačuvati stare primatelje, izvedite sljedeće iz reda za naredbe:

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

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

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

Srodne informacije

Promjena dnevnika (CHGJRN)

Jednoznačni atributi

Funkcija jedinstvenih atributa osigurava da navedeni atributi uvijek imaju jedinstvene vrijednosti unutar direktorija.

Ti atributi mogu biti navedeni u samo dva unosa, cn=uniqueattribute,cn=localhost i cn=uniqueattribute,cn=IBMpolicies. Rezultati pretraživanja za jedinstvene atribute su jedinstveni samo za bazu podataka tog poslužitelja. Rezultati pretraživanja koji uključuju rezultate od preporuka ne moraju biti jedinstveni.

Bilješka: Binarni atributi, operacijski atributi, konfiguracijski atributi i objectclass atributi ne mogu biti dizajnirani kao jedinstveni.

Ne mogu svi atributi biti specificirani kao jedinstveni. Da bi odredili da li atribut može biti naveden kao jedinstven, upotrijebite ldapexop naredbu:

- Za atribute koji mogu biti jedinstveni: ldapexop -op getattributes -attrType unique -matches true
- Za atribute koji ne mogu biti jedinstveni: ldapexop -op getattributes -attrType unique -matches false

Srodni koncepti

"Zadaci jedinstvenog atributa" na stranici 133
Koristite ovu informaciju za upravljanje jedinstvenim atributima.

Operativni atributi

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

Ti atributi imaju posebne karakteristike:

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

Sljedeći skupovi operacijskih atributa su neki od operacijskih atributa podržanih od strane Poslužitelja direktorija:

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

Radi potpune liste operacijskih atributa, upotrijebite sljedeću proširenu operaciju: ldapexop -op getattributes -attrType operational -matches true.

Srodni koncepti

"Direktorije" na stranici 3
Directory Server dozvoljava pristup tipu baze podataka koja pohranjuje informacije u hijerarhijsku strukturu sličnu načinu na koji je i5/OS integrirani sistem datoteka organiziran.

"Lista kontrole pristupa" na stranici 62
Liste kontrole pristupa (ACL-ovi) sadrže sredstvo za zaštitu informacija pohranjenih u LDAP direktoriju. Administratori koriste ACL-ove kako bi ograničili pristup različitim dijelovima direktorija ili određenim unosima direktorija.

"Politika lozinke" na stranici 75
Kada se koriste LDAP poslužitelji za provjeru autentičnosti, važno je da LDAP poslužitelj podržava politike koje se odnose na istek dozvole, neuspjeli pokušaj prijave i pravila lozinke. Poslužitelj direktorija osigurava konfigurabilnu podršku za sve tri vrste politika.

Predmemorije poslužitelja

LDAP predmemorije su brzi međuspremnici za pohranu u memoriji korišteni za pohranjivanje LDAP informacija kao što su upiti, odgovori i korisnička autorizacija za buduće korištenje. Podešavanje LDAP predmemorija je vrlo bitno za poboljšanje performansi.

LDAP pretraživanje koje pristupa LDAP predmemoriji može biti brže nego ono koje treba vezu na DB2, čak i ako se informacije ostavljaju u predmemoriju u DB2. Zbog tog razloga, podešavanje LDAP predmemorija može poboljšati performansu izbjegavanjem poziva prema bazi podataka. LDAP predmemorije su posebno korisne za aplikacije koje često dohvaćaju ponovljene informacije predmemorije.

Sljedeći odlomci raspravljaju o svakom od LDAP predmemorija i demonstriraju kako odrediti i postaviti najbolje postavke predmemorije za vaš sistem.

Srodni koncepti

"Zadaci izvedbe" na stranici 136
Koristite ovu informaciju za prilagodbu postavki izvedbe.

Predmemorija atributa

Predmemorija atributa ima prednost da je sposobna riješiti filtere u memoriji umjesto u bazi podataka. Također ima prednost zato što je ažurirana svaki put kad je izvede LDAP operacija dodavanja, izmjene, brisanja ili modrdn.

U odlučivanju koje atribute želite spremiti u memoriju, trebate razmotriti:

- Količinu dostupne memorije na poslužitelju
- Veličinu direktorija
- Tipove filtera pretraživanja koje aplikacija koristi

Bilješka: Upravitelj predmemorijom atributa može riješiti sljedeće tipove jednostavnih filtera: filteri točnog podudaranja i filteri prisustva. Može riješiti kompleksne filtere koji su konjuktivni ili disjunktivni, a podfilteri moraju biti točno podudaranje, prisutnost, konjuktivni ili disjunktivni.

Ne mogu svi atributi biti dodani u predmemoriju atributa. Da bi odredili da li atribut može biti dodan u predmemoriju, upotrijebite ldapexop naredbu:

- Za atribute koji mogu biti dodani: ldapexop -op getattributes -attrType attribute_cache -matches true
- Za atribute koji ne mogu biti dodani: ldapexop -op getattributes -attrType attribute_cache -matches false

Stavljanje atributa u predmemoriju može biti konfigurirano na dva načina: ručni ili automatski. Da bi ručno konfigurirali predmemoriju atributa, administrator treba izvesti cn=monitor pretraživanja da razumije kako učiniti predmemoriju atributa najefikasnijom. Ta pretraživanja vraćaju trenutne liste informacija o tome koji su atributi stavljeni u predmemoriju, količinu memorije korištene od strane predmemorije svakog atributa, ukupnu količinu memorije korištenu od strane predmemorije atributa, količinu memorije konfiguriranu za predmemoriju atributa i liste atributa najčešće korištenih u filterima predmemorije. Korištenjem ovih informacija, administrator može promijeniti količinu memorije koja je omogućena za korištenje za predmemoriju atributa, kao i koje atribute staviti u predmemoriju gdje god je potrebno bazirano na novim cn=monitor pretraživanjima.

Alternativno, administrator može konfigurirati automatsko stavljanje atributa u predmemoriju. Kada je automatsko stavljanje atributa u predmemoriju omogućeno, Poslužitelj direktorija prati kombinaciju atributa koji bi bili najkorisniji

za predmemoriju unutar memorijskih granica definiranih od administratora. On onda ažurira predmemoriju atributa u vremenskim intervalima definiranim od strane administratora.

Predmemorija filtera

Kada klijent izda upit za podatke i upit ne može biti riješen u memoriji od strane upravitelja predmemorije atributa, upit ide na predmemoriju filtera. Ta predmemorija sadrži unose ID-a stavljene u predmemoriju.

Dvije stvari se mogu dogoditi kada upit stigne do predmemorije filtera:

- **ID-ovi koji odgovaraju postavkama filtera korištenim u upitu su smješteni u predmemoriji filtera.** Ako je to slučaj, lista podudarajućih ID-a je poslana u predmemoriju unosa.
- **ID-ovi koji odgovaraju unosu se ne nalaze u predmemoriji filtera.** U tom slučaju, upit mora pristupati DB″ u pretraživanju željenih podataka.

Da bi odredili koliko mora biti velika predmemorija vašeg filtera, izvedite vaše radno opterećenje s predmemorijom filtera postavljenim na različite vrijednosti i mjerite razlike u operacijama po sekundi.

Konfiguracijska varijabla granice premosnice predmemorije filtera ograničava broj unosa koji mogu biti dodani u predmemoriju filtera. Na primjer, ako je varijabla granice premosnice postavljena na 1,000, filteri pretraživanja koji odgovaraju s više od 1,000 unosa nisu dodani u predmemoriju filtera. To sprječava velika, neuobičajena pretraživanja od prepisivanja korisnih unosa predmemorije. Da bi odredili najbolju granicu premosnice predmemorije filtera za vaše radno opterećenje, izvedite vaše radno opterećenje redovito i mjerite propusnost.

Predmemorija za unos

Predmemorija unosa sadrži podatke unosa u predmemoriji. ID-ovi unosa su poslani u predmemoriju unosa.

Ako su unosi koji odgovaraju ID-ovima unosa u predmemoriji unosa, onda su rezultati vraćeni klijentu. Ako predmemorija unosa ne sadrži unose koji odgovaraju ID-ovima unosa, upit ide na DB2 radi pretraživanja podudarajućih unosa.

Da bi odredili koliko velika treba biti predmemorija unosa, izvedite vaše radno opterećenje s predmemorijom unosa postavljenom na različite veličine i mjerite razlike u operacijama po sekundi.

ACL predmemorija

ACL predmemorija sadrži informacije kontrole pristupa kao što su vlasnik unosa i dozvole unosa za nedavno pristupane informacije. Ta predmemorija je korištena za poboljšanje izvedbe procjene pristupa za dodavanje, brisanje, izmjenu ili pretraživanje unosa.

Ako unos nije nađen u ACL predmemoriji, informacije kontrole pristupa su dobavljene iz baze podataka. Da bi odredili odgovarajuću veličinu ACL predmemorije, izmjerite izvedbu poslužitelja koristeći tipično radno opterećenje s različitim ACL veličinama predmemorije.

Kontrole i proširene operacije

Kontrole i proširene operacije dozvoljavaju LDAP protokolu da bude proširen bez promjene samog protokola.

Kontrole

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

- Tipa kontrole, to je OID koji identificira kontrolu.
- Indikatora kritičnosti koji specificira kako bi se poslužitelj trebao ponašati ako ne podržava kontrolu. To je Booleova vrijednost. FALSE označava da kontrola nije kritična i poslužitelj bi je trebao zanemariti ako je ne podržava. TRUE označava da je kontrola kritična i cijeli zahtjev bi trebao doživjeti neuspjeh (s greškom nepodržano kritično proširenje) ako poslužitelj ne može prihvatiti kontrolu.

- Neobvezna kontrolna vrijednost koja sadrži druge vrijednosti koje su specifične za kontrolu. Sadržaj kontrolne vrijednosti je specificiran korištenjem ASN.1 notacije. Sama vrijednost je BER kodiranje kontrolnih podataka.

Proširene operacije

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

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

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

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

Srodni koncepti

"Razlikovna imena (DN-ovi)" na stranici 9
Svaki unos u direktorij ima razlikovno ime (DN). DN je ime koje jednoznačno identificira unos u direktorij. Prva komponenta DN-a se naziva Relativno razlikovno ime (RDN).

Srodne reference

"Identifikatori objekata (OID-i)" na stranici 282
Ove informacije sadrže identifikatore objekta (OID-i) koji se koriste u Directory Server-u.

Razmatranje spremanja i vraćanja

Directory Server pohranjuje podatke i konfiguracijske informacije na nekoliko lokacija.

Directory Server pohranjuje informacije na sljedeće lokacije:

- Knjižnica baze podataka (QUSRDIRDB po defaultu), koja sadržava sadržaj poslužitelja direktorija.

  Bilješka: Koju knjižnicu baze podataka koristite možete vidjeti na kartici **Baza podataka/Sufiksi** na panelu Svojstva IBM Directory Servera u System i Navigator.
- QDIRSRV2 knjižnica, koja se koristi za pohranu informacija o izdavanju.
- QUSRSYS knjižnica, koja pohranjuje razne stavke u objektima koji počinju s QGLD (specificirajte QUSRSYS/QGLD* da ih spremite).
- Ako konfigurirate poslužitelj direktorija da zapisuje promjene u direktoriju, koristi se knjižnica baza nazvana QUSRDIRCL.

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

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

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

Srodne informacije

Backup i obnavljanje

Kako započeti rad s Directory Server-om

Pokretanje instaliranje, migriranje, planiranje, prilagođavanje i upravljanje Directory Servera.

Directory Server se automatski instalira kad instalirate i5/OS. Poslužitelj direktorija uključuje default konfiguraciju. Za započinjanje rada s Directory Server-om, pogledajte sljedeće:

Razmatranja o migraciji

Ako instalirate V5R4 i koristili ste Poslužitelj direktorija na prijašnjem izdanju, pregledajte razmatranja migracije.

Directory Server se automatski instalira kad instalirate i5/OS. Prvi puta kada se poslužitelj pokrene, on se automatski migrira na bilo koju postojeću konfiguraciju i podatke. To može uzrokovati u dugoj odgodi prije nego što je poslužitelj pokrenut prvi puta.

Bilješka: Migracija konfiguracije i datoteka sheme je napravljena za vrijeme instalacije i prvog pokretanja poslužitelja. Jednom kada je to prvo pokretanje dovršeno, ako su konfiguracija i datoteke sheme u /qibm/userdata/os400/dirsrv vraćene iz sigurnosne kopije prethodnog izdanja, shema i konfiguracija za novo izdanje će biti prekriveni s datotekama prijašnjih izdanja koji neće biti ponovno migrirani. Vraćanje sheme i konfiguracije prethodnih izdanja nakon što se dogodila migracija može uzrokovati da se vaš poslužitelj ne pokreće kao i druge nepredvidive greške. Ako želite napraviti sigurnosnu kopiju konfiguracije i sheme poslužitelja, ovi podaci trebaju biti spremljeni nakon što je poslužitelj uspješno pokrenut.

Migriranje u V6R1 iz V5R4 ili V5R3

Koristite ovu informaciju ako imate Directory Server koji radi pod V5R4 ili V5R3.

i5/OS V6R1 uvodi nove sposobnost i sposobnosti u Directory Server. Te promjene utječu i na LDAP poslužitelj direktorija i na System i Navigator grafičko korisničko sučelje (GUI). Kako biste iskoristili prednost novih GUI funkcija, trebate instalirati System i Navigator na računalo koji može komunicirati preko TCP/IP na vaš iSeries poslužitelj. System i Navigator je komponenta u System i Access za Windows. Ako imate raniju verziju System i Navigator instaliranu, trebali biste nadograditi na V6R1.

i5/OS V6R1 podržava izravne nadogradnje iz V5R4 i V5R3. Directory Server se nadograđuje na V6R1 prvi puta kad se poslužitelj pokreće. LDAP podaci direktorija i datoteke sheme direktorija automatski migriraju kako bi se prilagodile V6R1 formatima.

Kada nadograđujete na i5/OS V6R1, trebali biste biti svjesni nekih pitanja migracije:

- Kada nadograđujete na V6R1 i pokrećete directory server, Directory Server automatski migrira vaše datoteke sheme u V6R1 i briše stare datoteke sheme. Međutim, ako ste obrisali ili preimenovali datoteke sheme, Directory Server ne može ih migrirati. Mogli biste primiti grešku ili bi Directory Server mogao pretpostaviti da su datoteke već migrirale.
- Nakon što nadogradite na V6R1, trebali biste prvo poslužitelj jednom pokrenuti kako bi migrirali postojeći podaci prije importiranja novih podataka. Ako pokušate importirati podatke prije pokretanja poslužitelja jednom i nemate dovoljno ovlaštenja, importiranje možda neće uspjeti. Directory Server migrira podatke direktorija u V6R1 format prvi puta kada pokrenute poslužitelj ili importirate LDIF datoteku. Planirajte tako da ostavite malo vremena da migracija potpuno završi.
- V6R1 uvodi sposobnost za višestrukim instancama directory servera na vašem i5/OS sistemu. Ako koristite directory server prije nadogradnje na V6R1, vaš directory server migrirat će u instancu. To uključuje premještanje konfiguracijskih i shematskih datoteka iz /QIBM/UserData/OS400/DirSrv direktorija u /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR direktorij. To se označava kao default instanca directory servera i nazvat će se QUSRDIR instanca. Također, dva objekta u QUSRSYS knjižnici premještena su u novu knjižnicu, QUSRDIRCF. Ta će se migracija desiti kada se directory server pokrene prvi put nakon nadogradnje na V6R1.
- Sljedeći migraciju, LDAP poslužitelj direktorija će se automatski pokrenuti kada se pokrene TCP/IP. Ako ne želite da se poslužitelj direktorija automatski pokrene, koristite System i Navigator da promijenite postavke.

Migriranje podataka iz V4R4, V4R5, V5R1 ili V5R2 u V6R1

Koristite ovu informaciju ako imate Directory Server koji radi pod V4R4, V4R5 ili V5R1.

i5/OS V5R4 ne podržava izravne nadogradnje iz V4R4, V4R5 ili V5R1.

Bilješka: Kada nadogradite iz V4R4 na bilo koje kasnije izdanje, trebate biti svjesni sljedećih problema:

- V4R4 i ranija izdanja Directory Server nisu uzimala u obzir vremenske zone kod kreiranja unosa vremenske oznake. Počevši s V4R5, vremenska zona se koristi u svim dodacima i promjenama direktorija. Dakle, ako nadograđujete podatke iz V4R4 ili od ranije, Directory Server prilagođava postojeće createtimestamp i modifytimestamp atribute za prikaz ispravne vremenske zone. To čini oduzimanjem vremenske zone koja je trenutno definirana u sistemu iz vremenskih oznaka koje su pohranjene u direktorij. Primijetite da ako trenutna vremenska zona nije ista vremenska zona koja je bila aktivna kad su unosi originalno kreirani ili preinačeni, nove vrijednosti vremenske oznake neće odražavati originalnu vremensku zonu.
- Ako nadograđujete podatke iz V4R4 ili ranijeg, vodite računa o tome da će podaci direktorija trebati približno dvostruko više prostora memorije od onoga koji je ranije bio potreban. To je zato jer je u V4R4 ili ranijim verzijama, Directory Server podržavao jedino IA5 skup znakova i spremljene podatke u ccsid 37 (jednobajtni format). Directory Server podržava puni ISO 10646 skup znakova. Nakon nadogradnje, trebali bi jednom pokrenuti poslužitelja kako bi se migrirali postojeći podaci prije nego se importiraju novi. Ako pokušate importirati podatke prije pokretanja poslužitelja jednom i nemate dovoljno ovlaštenja, importiranje možda neće uspjeti.

Ako želite migrirati ta izdanja u V5R4, možete slijediti bilo koju od sljedećih procedura.

Nadogradnja iz V4R4, V4R5 ili V5R1 u privremeno izdanje:

| Možete migrirati Directory Server za nadogradnju u privremeno izdanje (V5R2 ili V5R3) i zatim u V6R1.

| Preko nadogradnji sa V4R4, V4R5, V5R1 i V5R2 na V6R1nisu podržane, sljedeće nadogradnje su podržane:

- V4R4 i V4R5 nadograđen na V5R1
- V4R5 i V5R1 nadograđen na V5R2
- V5R1 i V5R2 nadograđen na V5R3
- V5R2 i V5R3 nadograđen na V5R4
- | V5R3 i V5R4 nadograđen na V6R1

Za detaljne informacije oi5/OS procedurama instalacije, pogledajte Instaliranje, nadogradnja ili brisanje i5/OS i odgovarajućeg softvera. Pratite sljedeće korake da izvedete migraciju. Promjene sheme trebaju biti izvedene automatski. Nakon svake instalacije, provjerite da su promjene shema još uvijek prisutne.

1. Za V4R4, instalirajte V5R1. Onda, instalirajte V5R3.
2. | Za V4R5, nemojte instalirati V5R1 ili V5R2. Ako instalirate u V5R1, tada morate instalirati u V5R3. Ako
   | instalirate u V5R2, tada morate instalirati u V5R3 ili V5R4.
3. Za V5R1, napravite instalaciju V5R3.
4. | Za V5R2, instalirajte V5R3 ili V5R4.
5. | Kad ste jednom na V5R3 ili V5R4, instalirajte V6R1.
6. Ako već nije pokrenut, pokrenite Poslužitelj direktorija.

Spremanje knjižnice baze podataka i instaliranje V6R1:

Možete migrirati Directory Server spremanjem knjižnice baze podataka koju Directory Server koristi u V4R4 ili V4R5 i zatim ga vratiti nakon instaliranjaV6R1.

Ta vas metoda pošteđuje instaliranja privremenog izdanja. Međutim, postavke poslužitelja se ne migriraju, tako da morate rekonfigurirati postavke poslužitelja. Za detaljne informacije o i5/OS instalacijskim procedurama, pogledajte Instaliranje, nadogradnja ili brisanje i5/OS i odgovarajućeg softvera. Slijedite ove općenite korake za izvođenje migracije:

1. Zabilježite promjene koje ste napravili u datotekama sheme u direktoriju /QIBM/UserData/OS400/DirSrv. Datoteke sheme nisu migrirane automatski, tako da ako želite zadržati promjene trebat ćete ih opet ručno implementirati. Ako je ažuriranje shema napravljeno koristeći LDIF datoteke zajedno s ldapmodify uslužnim

programom, locirajte te datoteke tako da koristite te datoteke nakon pokretanja poslužitelja na novom izdanju. Alat upravljanja direktorijem ili Web administration tool (koji radi na drugom V6R1 sistemu) može se koristiti za pregledavanje pojedinačnog tipa atributa i definicija klase objekta. Ako se vaše promjene sastoje samo od dodavanja novih tipova atributa i objectclasses, napravite kopiju datoteke /qibm/userdata/os400/dirsrv/v3.modifiedschema. Možete koristiti tu datoteku da konstruirate LDIF datoteku koja sadrži ažurirane sheme. Uputite se na “Shema” na stranici 14 za još informacija.

2. Primijetite raznolike konfiguracijske postavke u postavkama Directory Servera, uključujući ime knjižnice baze podataka.
3. Spremite knjižnicu baze podataka koja je specificirana u konfiguraciji Directory Servera. Ako ste konfigurirali dnevnik promjena, onda se treba spremiti QUSRDIRCL knjižnica.
4. Zabilježite konfiguraciju objavljivanja. Konfiguracija objavljivanja, uz izuzetak informacije o lozinci, može se pregledavati pomoću System i Navigator biranjem **Svojstva** za sistem i klikom na karticu **Usluge direktorija**.
5. Instalirajte i5/OS V6R1 na sistem.
6. Koristite čarobnjak u System i Navigator za konfiguraciju Directory Servera.
7. Vratite knjižnicu baze koju ste spremili u koraku 3. Ako ste spremili QUSRDIRCL knjižnicu u koraku 3, sada je vratite.
8. Koristite System i Navigator da rekonfigurirate Poslužitelj direktorija. Specificirajte knjižnicu baze podataka koja je ranije bila konfigurirana i koja je bila spremljena i vraćena u prethodnim koracima.
9. Koristite System i Navigator da rekonfigurirate izdavanje.
10. Ponovno pokrenite Poslužitelj direktorija.
11. Upotrijebite alat Web administracija da promijenite datoteke sheme za bilo koje korisničke promjene koje trebate u koraku 1 na stranici 93.

Migracija mreže poslužitelja repliciranja

Koristite ovu informaciju ako imate mrežu replicirajućih poslužitelja.

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

Ti unosi se nazivaju topologijom replikacije. Novi master može biti korišten s replikama koje izvode prijašnje verzije; podaci povezani s novim funkcijama neće biti replicirani na pozadinske poslužitelje. Potrebno je eksportirati unose topologije replikacije iz glavnog poslužitelja i dodati ih na svaku repliku nakon što je poslužitelj replikacije bio migriran. Kako bi eksportirali unose, koristite alat Qshell red za naredbe “ldapsearch” na stranici 222 i spremite izlaz na datoteku. Naredba pretraživanja je slična sljedećem:

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

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

Bilješka: Nemojte uključiti sljedeće sufikse:

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

Uključite samo korisnički kreirane sufikse.

Ponovite naredbu za svaki unos sufiksa, ali zamijenite “>” s “>>” kako biste pridodali podatke izlaznoj datoteci za naredna pretraživanja. Nakon što se datoteka dovrši, kopirajte je na replika poslužitelje.

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

Za pokretanje poslužitelja, koristite opciju **Pokreni** u System i Navigator.

Za zaustavljanje poslužitelja, koristite opciju **Zaustavi** u System i Navigator.

Kada dodajete datoteku na replika poslužitelja, vodite računa o tome da nije pokrenut replika poslužitelj. Za dodavanje podataka, koristite opciju **Importiraj datoteku** u System i Navigator.

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

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

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

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

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

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

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

Dovršena je migracija za tu repliku.

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

Srodni koncepti

“Replikacija” na stranici 37
Replikacija je tehnika koju koriste poslužitelji direktorija kako bi se poboljšala izvedba i pouzdanost. Proces replikacije zadržava usklađenima podatke u više direktorija.

Srodni zadaci

“Pokretanje Directory Servera” na stranici 111
Koristite ovu informaciju za pokretanje Directory Servera.

Promjena imena Kerberos usluge

Koristite ovu informaciju ako želite koristiti Kerberos prije V5R3.

Počevši u V5R3, ime servisa korišteno od strane poslužitelja direktorija i klijent API-ja za GSSAPI provjeru autentičnosti (Kerberos) su promijenjene. Ta promjena nije kompatibilna s imenom usluga korištenim prije V5R3 (V5R2M0 PTF 5722SS1-SI08487 sadrži istu promjenu).

Prije V5R3, Poslužitelj direktorija i klijent API-ji su koristili ime servisa oblika LDAP/dns-host-name@Kerberos-realm kada je GSSAPI mehanizam (Kerberos) korišten za provjeru autentičnosti. To ime ne odgovara standardima koji definiraju GSSAPI provjeru autentičnosti prema kojoj bi ime principala trebalo započeti s ″ldap″ s malim slovom. Kao rezultat, poslužitelj direktorija i klijent API-ji možda neće raditi s drugim proizvodima prodavača. To je posebno točno ako Kerberos centar distribucije ključa (KDC) ima imena principala osjetljiva na mala i velika slova. LDAP davatelj usluga za JNDI, obično korišten Java LDAP klijent API, je primjer klijenta uključenog s operativnim sistemom koji koristi ispravno ime servisa.

V5R3M0 je promijenio ime servisa da odgovara standardima. No, time uzrokuje vlastite probleme s kompatibilnosti.

- Poslužitelj direktorija koji je konfiguriran da koristi GSSAPI provjeru autentičnosti neće započeti instaliranje tog izdanja. To je posljedica toga što datoteka tablice ključeva ima vjerodajnice koje koriste staro ime usluge (LDAP/mysys.ibm.com@IBM.COM), dok poslužitelj traži vjerodajnice koje koriste novo ime usluge (ldap/mysys.ibm.com@IBM.COM).
- Directory server ili LDAP aplikacija koja koristi LDAP API-a pri V5R3M0 možda neće moći provjeriti autentičnost starijih OS/400 poslužitelja ili klijenata. Kako bi to ispravili, trebali bi napraviti sljedeće:
  1. Ako KDC koristi imena principala osjetljiva na velika i mala slova, kreirajte račun korištenjem ispravnog imena usluge (ldap/mysys.ibm.com@IBM.COM).
  2. Ažurirajte datoteku tablice ključeva korištenu od strane Poslužitelja direktorija da sadrži vjerodajnice za novo ime servisa. Možda bi bilo dobro da obrišete stare vjerodajnice. Možete koristiti Qshell pomoćni program tablice ključeva kako bi ažurirali datoteku tablice ključeva. Po defaultu, directory server koristi/QIBM/UserData/OS/400/NetworkAuthentication/keytab/krb5.keytab datoteku. Čarobnjak Usluge provjere autentičnosti V5R3M0 mreže (Kerberos) u System i Navigator također kreira unose tablice ključeva pomoću imena nove usluge.
  3. Ažurirajte V5R2M0 OS/400 sisteme gdje se GSSAPI koristi primjenom PTF 5722SS1-SI08487.

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

```
ADDENVVAR ENVVAR(LDAP_KRB_SERVICE_NAME)
```

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

```
export LDAP_KRB_SERVICE_NAME=1
```

Planiranje Directory Servera

Prije nego što počnete konfiguriranje Directory Servera i kreiranje strukture LDAP direktorija, trebali biste odvojiti nekoliko minuta za kreiranje plana.

Razmotrite sljedeće prije nego što počnete konfiguriranje Directory Servera i kreiranje strukture LDAP direktorija:

- **Organizirajte direktorij**. Planirajte strukturu vašeg direktorija i odredite koje sufikse i atribute će vaš poslužitelj trebati. Za više informacija, pogledajte poglavlja Preporučene prakse za strukturu direktorija, Direktoriji, Sufiks i Atributi.
- **Odlučite kako velik će biti vaš direktorij**. Onda možete procijeniti koliko memorije vam treba. Veličina direktorija ovisi o sljedećem:
  - Broju atributa u poslužiteljskoj shemi.
  - Broju upisa na poslužitelju.

– Tipu informacija koje pohranjujete na poslužitelju.

Na primjer, prazan direktorij koji koristi default shemu Directory Servera treba približno 10 MB prazne memorije. Direktorij koji koristi default shemu i sadrži 1000 slogova običnih podataka o zaposlenicima zahtijeva oko 30 MB prostora. Ovaj broj će se mijenjati ovisno atributima koje koristite. Također će se jako povećati ako ste pohranili velike objekte, kao što su slike, u direktorij.

- **Odlučite koje sigurnosne mjere ćete poduzeti**.

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

  Directory Server podržava upotrebu Sloja sigurnih utičnica (SSL) i Digitalni certifikata kao i Sigurnost sloja prijenosa (TLS) za komunikacijsku sigurnost. Podržana je i Kerberos provjera autentičnosti.

  Directory Server dozvoljava kontroliranje pristupa objektima direktorija s listama kontrole pristupa (ACL-i). Također možete koristiti reviziju sigurnosti operativnog sistema da bi zaštitili direktorij.

  Osim toga trebate odlučiti koja će se politika lozinke primijeniti.
- **Izaberite DN administratora i lozinku**. Default DN administratora je cn=administrator. To je jedini identitet koji ima ovlaštenje kreiranja ili promjene unosa direktorija kada je poslužitelj inicijalno konfiguriran. Možete koristiti default DN administratora ili izabrati drugačiji DN. Trebate kreirati i lozinku za DN administratora.
- **Instalirajte potrebni softver za Web administracijski alat Poslužitelja direktorija**. Kako biste koristiti Directory Server Web administration tool, moraju biti instalirani sljedeći preduvjetni proizvodi.
  – IBM HTTP Server za i5/OS (5761-DG1)
  – IBM WebSphere Application Server 6.0 (5733-W60 Base ili Express opcije)
- **Planirajte strategiju sigurnosnog kopiranja i obnavljanja**. Planirajte kako ćete spremiti podatke i konfiguracijske informacije.

  Srodni koncepti

  “Preporučene prakse za strukturu direktorija” na stranici 33
  Poslužitelj direktorija je često korišten kao spremište za korisnike i grupe. Ovaj odlomak opisuje neke preporučene prakse za postavljanje strukture koja je optimizirana za upravljanje korisnicima i grupama. Ta struktura i pridruženi model sigurnosti mogu biti prošireni na druge upotrebe direktorija.

  “Direktorije” na stranici 3
  Directory Server dozvoljava pristup tipu baze podataka koja pohranjuje informacije u hijerarhijsku strukturu sličnu načinu na koji je i5/OS integrirani sistem datoteka organiziran.

  “Sufiks (kontekst imenovanja)” na stranici 12
  Sufiks (poznat i kao kontekst imenovanja) je DN koji identificira najviši unos u lokalno zadržanoj hijerarhiji direktorija.

  “Atributi” na stranici 17
  Svaki unos direktorija ima skup atributa povezanih s njim kroz svoju klasu objekta.

  “Razmatranje spremanja i vraćanja” na stranici 91
  Directory Server pohranjuje podatke i konfiguracijske informacije na nekoliko lokacija.

  Srodne informacije

  IBM HTTP Poslužitelj
  Pogledajte poglavlje IBM HTTP Server za više informacija o IBM HTTP Serveru i IBM WebSphere Application Serveru.

Konfiguriranje Directory Servera

Pokrenite čarobnjaka konfiguracije Directory Servera za prilagođavanje postavki Directory Servera.

1. Ako vaš sistem nije konfiguriran za izdavanje informacija drugom LDAP poslužitelju i nijedan LDAP poslužitelj nije poznat TCP/IP DNS poslužitelju, tada se Directory Server automatski instalira s ograničenom default konfiguracijom. Directory Server osigurava čarobnjaka koji vam pomaže u konfiguriranju Directory Servera za vaše određene potrebe. Kasnije možete čarobnjaka pokrenuti iz System i Navigator. Koristite se ovim čarobnjakom kad radite početno konfiguriranje poslužitelja direktorija. Također možete koristiti čarobnjaka da rekonfigurirate poslužitelj direktorija.

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

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

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

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

2. Za pokretanje čarobnjaka konfiguracije Directory Servera, poduzmite ove korake:
   a. U System i Navigator, proširite **Mreža**.
   b. Proširite **Poslužitelji**.
   c. Kliknite **TCP/IP**.
   d. Desno kliknite na **IBM Poslužitelj direktorija** i izaberite **Konfiguriraj**.

   Bilješka: Ako ste već konfigurirali poslužitelj direktorija, kliknite **Rekonfiguriraj**, a ne **Konfiguriraj**.
3. Slijedite upute u čarobnjaku Konfiguriranja Poslužitelja direktorija da konfigurirate vaš Poslužitelj direktorija.

   Bilješka: Također bi možda željeli staviti knjižnicu koja pohranjuje podatke direktorija u korisničko pomoćno memorijsko spremište (ASP) umjesto u sistemski ASP. Međutim, ta knjižnica ne može biti pohranjena u Nezavisnom ASP-u i bilo kakav pokušaj konfiguriranja, rekonfiguriranja ili pokretanja poslužitelja s knjižnicom u Nezavisnom ASP-u neće uspjeti.
4. Kad čarobnjak dovrši, vaš Poslužitelj direktorija ima osnovnu konfiguraciju. Ako izvodite Lotus Domino na vašem sistemu, onda port 389 (default port za LDAP poslužitelj) već može biti korišten od strane Domino LDAP funkcije. Morate napraviti nešto od sljedećeg:
   - Promijenite port koji Lotus Domino koristi. Pogledajte Host Domino LDAP i Directory Server na istom sistemu u poglavlju E-mail za više informacija.
   - Promijenite port koji Directory Server koristi. Za više informacija pogledajte “Promjena porta ili IP adrese” na stranici 117.
   - Koristite određene IP adrese. Za više informacija pogledajte “Promjena porta ili IP adrese” na stranici 117.
5. Kreirajte unose koji odgovaraju sufiksu ili sufiksima koje ste konfigurirali. Za dodatne informacije, pogledajte “Dodavanje i uklanjanje sufiksa Directory Servera” na stranici 118.
6. Možda ćete htjeti napraviti nešto ili sve od sljedećeg prije nego što nastavite:
   - Omogućiti sigurnost Sloja sigurnih utičnica (SSL), pogledajte “Omogućavanje SSL-a i sigurnosti sloja prijenosa na Directory Server-u” na stranici 171.
   - Omogućiti Kerberos provjeru autentičnosti, pogledajte “Omogućavanje provjere autentičnosti Kerberos na Directory Server-u” na stranici 173.
   - Postaviti upućivanje, pogledajte “Specificiranje poslužitelja za upućivanja direktorija” na stranici 118.
7. Pokrenite Directory Server. Za dodatne informacije, pogledajte “Pokretanje Directory Servera” na stranici 111.
8. Postojeća instanca directory servera označava se kao QUSRDIR instanca. Njezine datoteke sheme i konfiguracijska datoteka nalaze se u /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR direktoriju. Instanca poslužitelja može se kreirati automatski ako pokušate pokrenuti default instancu. Automatski se neće kreirati nikakve druge instance.

Srodni koncepti

“Default konfiguracija za Directory Server” na stranici 290
Directory Server se automatski instalira kad instalirate i5/OS. Ta instalacija uključuje default konfiguraciju.

Popunjavanje direktorija

Napunite direktorij s podacima.

Postoji nekoliko načina na napunite direktorij s podacima:

- Izdajte informacije Directory Server-u.
- Importirajte podatke iz LDIF datoteke.
- Kopirajte korisnike iz validacijske liste HTTP poslužitelja u Directory Server.

Srodni zadaci

"Objavljivanje informacija Directory Server-u" na stranici 123
Koristite ovu informaciju za objavljivanje informacija Directory Server-u.

"Importiranje LDIF datoteke" na stranici 125
Koristite ovu informaciju za importiranje datoteke LDAP format izmjenjivanja podataka (LDIF)

"Kopiranje korisnika iz validacijske liste HTTP poslužitelja u Directory Server." na stranici 126
Koristite ovu informaciju za kopiranje korisnika iz validacijske liste HTTP poslužitelja u Directory Server.

Web administracija

Postavite i koristite konzolu Web administracije za upravljanje Directory Server-ima.

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

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

Kako bi koristili Web administracijsku konzolu, napravite sljedeće:

1. Ako je to prvi put da koristite Web administraciju Poslužitelja direktorija, prvo morate postaviti Web administraciju (pogledajte "Postavljanje Web administracije prvi puta" na stranici 100) i onda nastaviti sa sljedećim korakom.
2. Prijavite se U Web administraciju Poslužitelja direktorija radeći jedno od sljedećeg:
   - Iz System i Navigator, izaberite svoj poslužitelj i kliknite **Mrežni → poslužitelji → TCP/IP**, desno kliknite **IBM Directory Server**, te kliknite **Administracija poslužitelja**.
   - Na stranici iSeries Zadaci (http://*your_server*:2001) click **IBM Directory Server**.
3. Ako želite administrirati Poslužitelj direktorija, napravite sljedeće:
   a. Izaberite Poslužitelj direktorija koji želite administrirati u **LDAP Hostname** polju.
   b. Unesite DN prijave administratora koji koristite za povezivanje na poslužitelj direktorija.
   c. Unesite lozinku administratora.
   d. Kliknite **Prijava**. Prikazan je IBM Web administracijski alat Poslužitelja direktorija. Radi više informacija o stranici IBM web administracijskog alata poslužitelja direktorija, pogledajte "Web administracijski alat" na stranici 101.
4. Ako želite dodati ili promijeniti popis Poslužitelja direktorija koji se mogu administrirati ili promijeniti atribute Web administracijske konzole, napravite sljedeće:
   a. Izaberite **Console Admin** u **LDAP Hostname** polju.
   b. Unesite prijavu administratora konzole.
   c. Unesite lozinku administratora konzole.
   d. Kliknite **Prijava**. Prikazan je IBM Web administracijski alat Poslužitelja direktorija. Radi više informacija o stranici IBM web administracijskog alata poslužitelja direktorija, pogledajte "Web administracijski alat" na stranici 101.
   e. Kliknite na **Administracija konzole** i onda izaberite jedno od sljedećeg:
      - **Promjena prijave administratora konzole** kako bi promijenili ime prijave administratora konzole.

- **Promjena lozinke administratora konzole** kako bi promijenili lozinku administratora konzole.
- **Upravljanje poslužiteljima konzole** kako bi promijenili to koje Poslužitelje direktorija može administrirati Web konzola administracije.
- **Upravljanje svojstvima konzole** kako bi promijenili svojstva Web administracijske konzole.

Postavljanje Web administracije prvi puta

Ovo poglavlje daje upute za postavljanje Directory Server Web Administration Tool prvi puta.

1. Instalirajte IBM WebSphere Application Server 6.0 (5733-W60 Base ili Express opcije) i povezani preduvjetni softver ako već nisu instalirani.
2. Omogućite instancu poslužitelja sistemske aplikacije u HTTP ADMIN instanci poslužitelja. Pogledajte poglavlje IBM HTTP Poslužitelj za više informacija.
   a. Pokrenite HTTP ADMIN instancu poslužitelja čineći jedno od sljedećeg.
      - U System i Navigator, kliknite **Mrežni → Poslužitelji → TCP/IP** i desno kliknite **HTTP administracija**. Zatim kliknite **Kreni**.
      - U redu za naredbe upišite STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).
   b. Prijavite se na IBM Webadministraciju za iSeries. Koristite korisnički profil i lozinku operativnog sistema za prijavu na stranicu iSeries Zadaci (http://*your_server*:2001), zatim kliknite **IBM Web administracija za iSeries**.
   c. Na stranici Administracija HTTP poslužitelja *your_server*, kliknite karticu **Upravljanje** i zatim kliknite karticu **HTTP poslužitelji**. Pazite da je izabran **ADMIN ⌂?Apache** na padajućoj listi **Poslužitelj** i da je izabran **Uključi /QIBM/UserData/HTTPA/admin/conf/admin-cust.conf** na padajućoj listi **Područje poslužitelja**.
   d. Iz opcija na lijevom oknu na stranici, kliknite **Općenita konfiguracija poslužitelja**.

      Bilješka: Možda ćete trebati proširiti dio **Svojstva poslužitelja** da bi vidjeli opciju **Općenita konfiguracija poslužitelja**.
   e. Postavite **Pokreni instancu poslužitelja sistemske aplikacije kada je pokrenut 'Admin' poslužitelj** na **Yes**.
   f. Kliknite **OK**.
   g. Ponovno pokrenite instancu HTTP ADMIN poslužitelja klikom na gumb za ponovno pokretanje (drugi gumb na kartici **HTTP Poslužitelji**). Možete također zaustaviti i pokrenuti instancu HTTP ADMIN poslužitelja pomoću System i Navigator ili reda za naredbe.

      Instancu HTTP ADMIN poslužitelja možete zaustaviti čineći jedno od sljedećeg.
      - U System i Navigator, kliknite **Mrežni → poslužitelji → TCP/IP** i desno kliknite **HTTP administracija**. Zatim kliknite **Zaustavi**.
      - U redu za naredbe upišite ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).

      Možete pokrenuti instancu HTTP ADMIN poslužitelja čineći jedno od sljedećeg.
      - U System i Navigator, kliknite **Mrežni → poslužitelji → TCP/IP** i desno kliknite **HTTP administracija**. Zatim kliknite **Kreni**.
      - U redu za naredbe upišite STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).

      Pogledajte poglavlje IBM HTTP Poslužitelj za više informacija.
3. Prijavite se u Web administracijski alat poslužitelja direktorija.
   a. Dovedite naprijed **Stranicu prijave** čineći jedno od sljedećeg.
      - Iz System i Navigator izaberite svoj poslužitelj i kliknite **Mrežni → poslužitelji → TCP/IP**, desno kliknite **IBM Directory Server**, te kliknite **Administracija poslužitelja**.
      - Na stranici iSeries Zadaci (http://*your_server*:2001) kliknite **IBM Directory Server za iSeries**.
   b. Izaberite **Admin konzole** u polju **LDAP Ime hosta**.
   c. Tip superadmin u polju **Ime korisnika**.
   d. Tip secret u polju **Lozinka**.
   e. Kliknite **Prijava**. Prikazuje se stranica IBM Web administracijski alat Poslužitelja direktorija.
4. Promijenite prijavu administracije konzole.

a. Kliknite **Administracija konzole** u lijevom oknu da proširite sekciju i zatim kliknite **Promjena prijave administratora konzole**.
b. Upišite novo ime prijave administracije konzole u polju **Prijava administratora konzole**.
c. Upišite trenutnu lozinku (tajno) u polje **Trenutna lozinka**.
d. Kliknite **OK**.

5. Promjena lozinke administracije konzole. Kliknite **Promjena lozinke administratora konzole** u lijevom oknu.
6. Dodavanje Poslužitelj direktorija kojeg želite administrirati. Kliknite **Upravljanje poslužiteljima konzole** u lijevom oknu.

   Bilješka: Kad dodajete Poslužitelj direktorija, **Administracijski port** nije korišten i bit će zanemaren.
7. Ako želite promijeniti svojstva konzole. Kliknite **Upravljanje svojstvima konzole** u lijevom oknu.
8. Klikni **Odjavi se**. Kada se pojavi ekran Odjava uspješna, kliknite vezu **ovdje** za povratak na stranicu prijave Web administracije.

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

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

Web administracijski alat

Kad se jednom prijavite na Web administration tool, pronaći ćete prozor aplikacije koji se sastoji od pet dijelova.

Područje uvodnika
Područje uvodnika je smješteno na vrhu panela i sadrži ime aplikacije i IBM logo.

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

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

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

Upravljanje direktorijom
Taj zadatak vam omogućava da radite s unosima direktorija.

Upravljanje odgovorima
Taj zadatak vam omogućava da radite s vjerodajnicama, topologijom, rasporedima i redovima.

Područja i predlošci
Taj zadatak vam omogućava da radite s predlošcima korisnika i područjima.

Korisnici i grupe
Taj zadatak vam omogućava da radite s korisnicima i grupama u definiranim područjima. Na primjer, ako želite kreirati novog Web korisnika, zadatak **Korisnici i grupe** radi s jednom klasom objekta grupe, groupOfNames. Vi ne možete oblikovati grupnu podršku.

Administracija poslužitelja
Ovi zadaci vam omogućavaju da promijenite konfiguraciju poslužitelja i sigurnosne postavke.

Radno područje
Radno područje prikazuje zadatke koji su pridruženi izabranim zadacima u području navigacije. Na primjer, ako je izabrana sigurnost Upravljanje poslužiteljem u području navigacije, radno područje prikazuje stranicu Sigurnost poslužitelja i kartice koje sadrže zadatke koji se odnose na postavljanje sigurnosti poslužitelja.

Područje statusa poslužitelja
Područje statusa poslužitelja je locirano na vrhu radnog područja. Ikona na lijevoj strani područja statusa poslužitelja označava trenutni status poslužitelja. Uz ikonu je ime poslužitelja koji se administrira. Ikona na desnoj strani područja statusa poslužitelja osigurava vezu na online pomoć.

Područje status zadatka
Područje zadatka koje je smješteno ispod radnog područja prikazuje status trenutnog zadatka.

Scenariji Directory Servera

Koristite ovu informaciju za pregled scenarija koji ilustriraju primjere tipičnih zadataka Directory Servera.

Scenarij: Postavljanje Directory Servera

Primjer toga kako se postavlja LDAP direktorij na Poslužitelju direktorija.

Situacija

Kao administrator računalnog sistema vašeg poduzeća, vi bi željeli smjestiti informacije o zaposlenicima kao što su brojevi telefona i adrese e-pošte za vašu organizaciju u središnje LDAP spremište.

Ciljevi

U ovom scenariju, MyCo, Inc. želi konfigurirati Poslužitelj direktorija i kreirati bazu podataka koja sadrži informacije o zaposlenicima, kao što su ime, adresa e-pošte i telefonski broj.

Ciljevi ovog scenarija su sljedeći:

- Da bi informacije o zaposlenicima učinili dostupnim bilo gdje na mreži poduzeća zaposlenicima koji koriste Lotus Notes ili Microsoft Outlook Express mail klijent.
- Omogućiti upraviteljima da promijene podatke o zaposlenicima u bazi podataka direktorija, a i istovremeno ne omogućiti ne-upraviteljima da promijene podatke o zaposleniku.
- Kako bi se sistemu dozvolilo objavljivanje podataka o zaposlenicima u bazu podataka direktorija.

Detalji

Directory Server će raditi na sistemu nazvanom mySystem.

Sljedeći primjer prikazuje informacije koje MyCo, Inc. želi uključiti u bazu podataka direktorija za svakog zaposlenika.

```
Ime: Jose Alvirez
Odjel: DEPTA
Broj telefona: 999 999 9999
Adresa e-pošte: jalvirez@my_co.com
```

Struktura direktorija za taj scenarij bi se mogla prikazati kao nešto slično sljedećem:

```
/
|
+- my_co.com
   |
   +- employees
      |
      +- Jose Alvirez
      |  DEPTA
      |  999-555-1234
      |  jalvirez@my_co.com
      |
      +- John Smith
      |  DEPTA
      |  999-555-1235
      |  jsmith@my_co.com
```

```
      |
      +  Managers group
         Jose Alvirez
         mySystem.my_co.com
.
.
.
```

Svi zaposlenici (upravitelji i ne-upravitelji) postoje u stablu direktorija zaposlenika. Upravitelji pripadaju i grupi upravitelja. Članovi grupe upravitelja mogu imati ovlaštenje za promjenom podataka o zaposlenicima.

Sistem (mySystem) također treba imati ovlaštenje da mijenja podatke o zaposlenicima. U ovom scenariju, sistem je smješten u stablo direktorija zaposlenika i pretvoren je u člana grupe upravitelja.

Ako želite zadržati unose o zaposlenicima odijeljene od unosa sistema, možete kreirati drugo stablo direktorija (na primjer: računala) i tamo dodati sistem. Sistem će trebati imati isto ovlaštenje kao upravitelji.

Preduvjeti i pretpostavke

Web administracijski alat je ispravno konfiguriran i izvodi se. Za više informacija pogledajte “Web administracija” na stranici 99.

Koraci za postavljanje

Dovršite sljedeće zadatke:

Detalji scenarija: Postav Poslužitelja direktorija

Korak 1: Konfiguriranje Directory Servera:

Bilješka: Morate imati posebna ovlaštenja *ALLOBJ i *IOSYSCFG kad konfigurirate poslužitelj.

1. U System i Navigator kliknite **Mrežni → poslužitelji → TCP/IP**.
2. Kliknite **Konfiguriraj sistem kao Directory server** u prozoru **Zadaci konfiguracije poslužitelja** na dnu desno od System i Navigator.
3. Pojavit će se **Čarobnjak konfiguracije poslužitelja direktorija**.
4. Kliknite **Konfiguriraj lokalni LDAP poslužitelj direktorija** na **IBM Čarobnjaku konfiguracije poslužitelja direktorija - Dobrodošlica** prozoru.
5. Kliknite **Sljedeće** na **IBM Čarobnjaku konfiguracije poslužitelja direktorija - Dobrodošlica** prozoru.
6. Izaberite **Ne** na **IBM Čarobnjak konfiguracije poslužitelja direktorija - Navedite postavke** prozoru. To vam omogućava da konfigurirate LDAP poslužitelj bez default postavki.
7. Kliknite **Sljedeće** na **IBM Čarobnjak konfiguracije poslužitelja direktorija - Navedite postavke** prozoru.
8. Isključite **Sistemski-generiran** na **IBM Čarobnjak konfiguracije poslužitelja direktorija - Navedite Administratorski DN** prozoru i unesite sljedeće:

DN administrator	cn=administrator
Lozinka	tajna
Potvrda lozinke	tajna

Bilješka: Sve lozinke su specificirane u ovom scenariju samo kao primjeri. Kako bi spriječili kompromitiranje sigurnosti vašeg sistema ili lozinke, nikad ne bi smjeli koristiti ove lozinke kao dio vaše vlastite konfiguracije.

9. Kliknite **Sljedeće** na **IBM Čarobnjaku konfiguracije poslužitelja direktorija - Navedite administratorski DN** prozoru.

10. Upišite dc=my_co,dc=com u **Nastavak** polju na **IBM Čarobnjaku konfiguracije poslužitelja direktorija - Navedite nastavke** prozoru.
11. Kliknite **Dodavanje** na **IBM Čarobnjaku konfiguracije poslužitelja direktorija - Navedite nastavke** prozoru.
12. Kliknite **Sljedeće** na **IBM Čarobnjaku konfiguracije poslužitelja direktorija - Navedite nastavke** prozoru.
13. Izaberite **Da, koristi sve IP adrese** na **IBM Čarobnjaku konfiguracije poslužitelja direktorija - Izaberite IP adrese** prozoru.
14. Kliknite **Sljedeće** na **IBM Čarobnjak konfiguracije poslužitelja direktorija - Izaberite IP adrese** prozoru.
15. Izaberite **Da** na **IBM Čarobnjaku konfiguracije poslužitelja direktorija - Navedite TCP/IP preference** prozoru.
16. Kliknite **Sljedeće** na **IBM Čarobnjak konfiguracije poslužitelja direktorija - Navedite TCP/IP Preference** prozoru.
17. Kliknite **Završetak** na **IBM Čarobnjak konfiguracije poslužitelja direktorija - Sažetak** prozoru.
18. Desno kliknite na **IBM poslužitelj direktorija** i kliknite **Pokreni**.

Korak 2: Konfiguriranje Directory server Web Administration Tool-a:

1. Upišite u svoj pretražitelj http://*mySystem.my_co.com*:9080/IDSWebApp/IDSjsp/Login.jsp, gdje je *mySystem.my_co.com* vaš sistem.
2. Trebala bi se pojaviti stranica prijave. Kliknite na **LDAP Hostname** listu i izaberite **Console Admin**. Upišite superadmin za ime korisnika i tajna za lozinku. Kliknite **Prijava**.
3. Konfigurirajte Web Administration tool za povezivanje na LDAP poslužitelj na vašem sistemu. Izaberite **Administracija konzole → Upravljanje poslužiteljima konzole** na lijevoj navigaciji.
4. Kliknite **Dodavanje**.
5. U polju **Dodavanje poslužitelja**, upišite mySystem.my_co.com.
6. Kliknite **Ok**. U listi se pojavljuje novi poslužitelj pod **Upravljanje poslužiteljima konzole**.
7. Kliknite na **Odjava** u navigaciji s lijeve strane.
8. Na stranici za prijavu Web administration tool-a kliknite listu **LDAP glavno ime** i izaberite poslužitelj koji ste upravo konfigurirali (**mySystem.my_co.com**).
9. U polju **Ime korisnika** upišite cn=administrator, a u polje **Lozinka** upišite tajno. Kliknite **Prijava**. Trebali bi vidjeti glavnu stranicu od IBM Web alata administracije poslužitelja direktorija.

Detalji scenarija: Kreiranje baze podataka direktorija

Prije nego možete početi unositi podatke, morate kreirati prostor za podatke koji će se pohraniti.

Korak 1: Kreiranje objekta baznog DN-a:

1. U Web administration tool-u, kliknite **Upravljanje direktorijem → Upravljanje unosima**. Možete vidjeti popis objekata na osnovnoj razini direktorija. Budući je poslužitelj nov, vidjet ćete samo strukturalne objekte koji sadrže informacije o konfiguraciji.
2. Želite dodati novi objekt koji će sadržavati MyCo, Inc. podatke. Prvo kliknite na **Dodavanje...** na desnoj strani prozora. U sljedećem prozoru, spuštajte se kroz listu **Klasa objekta** kako bi izabrali **domenu** i kliknite na **Sljedeće**.
3. Ne želite dodati pomoćne klase objekta, pa kliknite ponovno na **Sljedeće**.
4. U prozoru **Unos atributa** unesite podatke koji se podudaraju sa sufiksom kojeg ste ranije kreirali u čarobnjaku. Ostavite **Klasa objekta** padajući popis na **domeni**. Upišite dc=my_co u polje **Relativni DN**. Upišite dc=com u polje **Nadređeni DN**. Upišite my_co u polje **dc**.
5. Kliknite na **Završetak** na dnu prozora. Natrag na baznoj razini bi trebali vidjeti novi bazni DN.

korak 2: Kreiranje predloška korisnika:

Kreirat ćete predložak korisnika kao pomoć pri dodavanju MyCo, Inc. podataka o zaposlenicima.

1. U Web administration tool-u, kliknite **Područja i predlošci → Dodavanje predloška korisnika**.
2. U polje **Ime predloška korisnika** upišite Zaposlenik.

3. Kliknite **Pretraživanje...** pokraj polja **Nadređeni DN**. Kliknite na bazni DN koji ste kreirali u prethodnom odlomku, **dc=my_co,dc=com** i kliknite na **Izbor**, s lijeve strane prozora.
4. Kliknite **Sljedeće**.
5. Iz padajuće liste **Strukturalna klasa objekt** izaberite **inetOrgPerson** i kliknite **Dalje**.
6. U padajućoj listi **Atribut imenovanja** izaberite **cn**.
7. U listi **Tabulatori** izaberite **Potrebno** i kliknite na **Uređivanje**.
8. U prozoru **Uređivanje kartice** birate polja koja će biti uključena u predložak korisnika. Potrebno je **sn** i **cn**.
9. Iz liste **Atributi** izaberite **departmentNumber** i kliknite **Dodavanje>>>**.
10. Izaberite **telephoneNumber** i kliknite **Dodavanje >>>**.
11. Izaberite **mail** i kliknite **Dodavanje>>>**.
12. Izaberite **userPassword** i kliknite **Dodavanje >>>**.
13. Kliknite na **OK** i onda **Završetak** da kreirate predložak korisnika.

Korak 3: Kreiranje područja:

1. U Web Administration tool-u, kliknite **Područja i predlošci → Dodavanje područja**.
2. U polje **Ime područja** upišite zaposlenici.
3. Kliknite na **Pregled...** s lijeve strane polja **Nadređeno DN**.
4. Izaberite nadređeno DN koje ste kreirali **dc=my_co,dc=com** i kliknite na **Izbor** na desnoj strani prozora.
5. Kliknite **Sljedeće**.
6. U sljedećem prozoru trebate samo promijeniti padajući popis **Predložak korisnika**. Izaberite predložak korisnika kojeg ste kreirali, **cn=employees,dc=my_co,dc=com**.
7. Kliknite **Završetak**.

Korak 4: Kreiranje grupe upravitelja:

1. Kreirajte grupu upravitelja.
   a. U Web administration tool-u, kliknite **Korisnici i grupe → Dodavanje grupe**.
   b. U polje **Ime grupe** upišite upravitelji.
   c. Provjerite da li su izabrani **zaposlenici** u listi povlačenja **Područje**.
   d. Kliknite **Završetak**.
2. Konfigurirajte administratora grupe upravitelja za područje **zaposlenici**.
   a. Kliknite **Područja i predlošci → Upravljanje područjima**.
   b. Izaberite područje koje ste kreirali, **cn=employees,dc=my_co,dc=com** i kliknite na **Uređivanje**.
   c. S desne strane polja **Grupa administratora** kliknite na **Pregled...**.
   d. Izaberite **dc=my_co,dc=com** i kliknite na **Proširivanje**.
   e. Izaberite **cn=employees** i kliknite na **Proširivanje**.
   f. Izaberite **cn=managers** i kliknite na **Izaberi**.
   g. U prozoru **Uredi područje** kliknite na **OK**.
3. Dajte ovlaštenje upravljanja grupom preko **dc=my_co,dc=com** sufiksa.
   a. Kliknite **Upravljanje direktorijem → Upravljanje unosima**.
   b. Izaberite **dc=my_co,dc=com** i kliknite na **Uređivanje ACL-a...**.
   c. U prozoru **Uredi ACL** kliknite na karticu **Vlasnici**.
   d. Izaberite kućicu provjere**Proširivanje korisnika**. Svatko tko je član grupe upravitelja će postati vlasnikom **dc=my_co,dc=com** stabla podataka.
   e. U **Tip** listi povlačenja izaberite **Grupa**.
   f. U polje **DN (razlikovno ime)**, upišite cn=managers,cn=employees,dc=my_co,dc=com.
   g. Kliknite **Dodavanje**.

h. Kliknite **Ok**.

Korak 5: Dodavanje korisnika kao upravitelja:

1. U Web Administration tool-u, kliknite **Korisnici i grupe → Dodavanje korisnika**.
2. Izaberite područje koje ste kreirali, **zaposlenici**, u padajućem izborniku **Područje** i kliknite **Sljedeće**.
3. U polje **cn** upišite Jose Alvirez.
4. U polje ***sn** (prezime) upišite Alvirez.
5. U polje ***cn** (puno ime) upišite Jose Alvirez. cn se koristi kako bi se kreirao DN unosa. *cn je atribut objekta.
6. U polje **telephoneNumber** upišite 999 555 1234.
7. U polje **departmentNumber** upišite DEPTA.
8. U polje **mail** upišite jalvirez@my_co.com.
9. U polje **userPassword** upišite secret.
10. Kliknite karticu **Grupe korisnika**.
11. Iz liste **Dostupne grupe** izaberite **upravitelji** i kliknite **Dodavanje ->**.
12. Na dnu prozora kliknite na **Završetak**.
13. Odjavite se iz Web administracijskog alata tako da kliknete na **Odjava** u navigaciji s lijeve strane.

Detalji scenarija: Objavite System i5 podatke u bazu podataka direktorija

Konfigurirajte objavljivanje kako biste dozvolili svom sistemu da automatski upisuje informacije o korisniku u LDAP direktorij. Informacije korisnika iz direktorija distribucije sistema se objavljuju u LDAP direktoriju.

Bilješka: Korisnicima kreiranima s System i Navigator dan je korisnički profil i unos korisnika raspodjele sistema. Ako koristite CL naredbe za kreiranje korisnika, morate kreirati i korisnički profil (**CRTUSRPRF**) i korisnički unos sistemskog distribucijskog direktorija (**WRKDIRE**). Ako vaši korisnici postoje samo kao profili korisnika i želite ih objaviti na LDAP direktoriju, morate za njih kreirati unose korisnika direktorija distribucije sistema.

Korak 1: Pretvaranje sistema u korisnika Directory Servera:

1. Prijavite se u Web Administration tool (http://**mySystem.my_co.com**:9080/IDSWebApp/IDSjsp/Login.jsp) kao administrator.
   a. Izaberite **mySystem.my_co.com** iz liste **LDAP glavno ime**.
   b. Upišite cn=administrator u polje **Ime korisnika**
   c. Upišite tajna u polje **Lozinka**.
   d. Kliknite **Prijava**.
2. Izaberite **Korisnici i grupe → Dodavanje korisnika**.
3. Izaberite **zaposlenici** u listi **Područje**.
4. Kliknite **Sljedeće**.
5. Upišite mySystem.my_co.com u polje **cn**.
6. Upišite mySystem.my_co.com u polje ***sn**.
7. Upišite mySystem.my_co.com u polje ***cn**.
8. Upišite tajna u polje **Lozinka_korisnika** .
9. Kliknite na karticu **Grupa korisnika**.
10. Izaberite grupu **upravitelji**.
11. Kliknite **Dodavanje →** .
12. Kliknite **Završetak**.

Korak 2: Konfiguriranje sistema za objavljivanje podataka:

1. U System i Navigator, desno kliknite na iSeries u lijevoj navigaciji i izaberite **Svojstva**.

2. U kućici dijaloga **Svojstva** izaberite karticu **Poslužitelj direktorija**.
3. Izaberite **Korisnici** i kliknite na **Detalji**.
4. Izaberite kućicu provjere **Objavi informacije o korisniku**.
5. U odlomku **Gdje objaviti** kliknite na gumb **Uredi**. Pojavit će se prozor.
6. Upišite mySystem.my_co.com.
7. U polje **Pod DN-om**, upišite cn=employees,dc=my_co,dc=com.
8. U odlomku **Povezivanje poslužitelja** provjerite da li je default broj porta, **389**, unesen u polje **Port**. Iz padajuće liste **Metoda provjere autentičnosti** izaberite **Razlikovno ime** i upišite cn=mySystem,cn=employees,dc=my_co,dc=com u polje **Razlikovno ime**.
9. Kliknite **Lozinka**.
10. Upišite tajna u polje **Lozinka**.
11. Upišite tajna u polje **Potvrda lozinke**.
12. Kliknite **OK**.
13. Kliknite tipku **Provjera**. To osigurava da ste informacije ispravno upisali i da se sistem može povezati na LDAP direktorij.
14. Kliknite **OK**.
15. Kliknite **OK**.

Detalji scenarija: Unos informacija u bazu podataka direktorija

Kao upravitelj, Jose Alvirez sada dodaje i ažurira podatke za pojedince u svojem odjelu. Treba dodati neke dodatne informacije o Jane Doe. Jane Doe je korisnik na sistemu i njezine su informacije objavljene. Jose Alvirez treba dodati informacije i o zaposleniku John Smith. John Smith nije korisnik na sistemu. Jose Alvirez čini sljedeće:

Korak 1: Prijava na Web Administration tool:
Prijavite se na Web administracijski alat (http://**mySystem.my_co.com**:9080/IDSWebApp/IDSjsp/Login.) čineći sljedeće:

1. Izaberite **mySystem.my_co.com**, iz liste **LDAP glavno ime**.
2. Upišite cn=Jose Alvirez,cn=myco employees,dc=my_co,dc=com u polje Ime korisnika.
3. Upišite tajna u polje lozinka.
4. Kliknite **Prijava**.

Korak 2: Promjena podataka o zaposleniku:

1. Kliknite **Korisnici i grupe → Upravljanje korisnicima**.
2. Izaberite **zaposlenici** u listi **Područje** i kliknite na **Pregled korisnika**.
3. Izaberite **Jane Doe** u listi korisnika i kliknite na **Uređivanje**.
4. Upišite DEPTA u polje **departmentNumber**.
5. Kliknite **OK**.
6. Kliknite **Zatvaranje**.

Korak 3: Dodavanje podataka o zaposleniku:

1. Kliknite **Korisnici i grupe → Dodavanje korisnika**.
2. Izaberite **zaposlenici** u izborniku povlačenja **Područje** i kliknite na **Sljedeće**.
3. U polje **cn** upišite John Smith.
4. U polje ***sn** upišite Smith.
5. U polje ***cn** upišite John Smith.
6. U polje **telephoneNumber** upišite 999 555 1235.
7. U polje **departmentNumber** upišite DEPTA Smith.
8. U polje **mail** upišite jsmith@my_co.com.

9. Kliknite na **Završetak** na dnu prozora.

Detalji scenarija: Testiranje baze podataka direktorija

Nakon što ste unijeli podatke o zaposleniku u bazu podataka direktorija, testirajte bazu podataka direktorija i Poslužitelj direktorija čineći jedno od sljedećeg:

Pretražite bazu podataka direktorija pomoću e-mail adresara:
Informacije u LDAP direktoriju mogu lagano potražiti LDAP omogućeni programi. Mnogo klijenata e-pošte može pretraživati LDAP poslužitelje direktorija kao dio funkcije svojeg imenika adresa. Slijede primjeri procedura za konfiguraciju Lotus Notes 6 i Microsoft Outlook Express 6. Procedura za većinu drugih e-mail klijenata bit će slična.

Lotus Notes:

1. otvorite svoj imenik.
2. Kliknite **Akcije → Novi → račun**.
3. Upišite mySystem u polje **Ime računa**.
4. Upišite mySystem.my_co.com u polje **Ime poslužitelja računa**.
5. Izaberite **LDAP** u polju **Protokol**.
6. Kliknite karticu **Konfiguracija protokola**.
7. Upišite dc=my_co,dc=com u polje **Baza traženja**.
8. Kliknite **Spremanje i zatvaranje**.
9. Kliknite **Kreiraj → memorandum → pošte**.
10. Kliknite **Adresa...**.
11. Izaberite mySystem u polju **Izaberi adresar**.
12. Upišite Alvirez u polje **Traži**.
13. Kliknite **Traži**. Pojavit će se podaci za Jose Alvirez.

Microsoft Outlook Express:

1. Kliknite **Alati → Računi**.
2. Kliknite **Dodavanje → Directory Service**.
3. Upišite Web adresu sistema u polje **Poslužitelj Internet direktorija (LDAP)** (mySystem.my_co.com).
4. Odznačite kontrolnu kućicu **Moj LDAP poslužitelj traži da se prijavim**.
5. Kliknite **Sljedeće**.
6. Kliknite **Sljedeće**.
7. Kliknite **Završetak**.
8. Izaberite mySystem.my_co.com (usluga direktorija koju ste upravo konfigurirali) i kliknite **Svojstva**.
9. Kliknite **Napredno**.
10. Upišite dc=my_co,dc=com u polje **Baza traženja**.
11. Kliknite **Ok**.
12. Kliknite **Zatvaranje**.
13. Upišite Ctrl+E kako bi otvorili prozor **Nalaženje ljudi**.
14. Izaberite mySystem.my_co.com iz liste **Pogledaj u** .
15. Upišite Alvirez u polje **Ime**.
16. Kliknite **Nalaženje sada**. Pojavit će se podaci za Jose Alvirez.

Pretražite bazu podataka direktorija upotrebom naredbe ldapsearch reda za naredbe:

1. Na sučelju baziranom na znakovima unesite CL naredbu **QSH** kako bi otvorili Qshell sesiju.
2. Unesite sljedeće kako bi dohvatili popis svih LDAP unosa u bazi podataka.

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

Gdje je:

–h ime glavnog stroja koji izvodi LDAP poslužitelja.

–b je bazni DN pod kojim će se pretraživati.

objectclass=*
vraća sve unose u direktorij.

Ta naredba vraća nešto što je slično sljedećem:

```
dc=my_co,dc=com
dc=my_co
objectclass=domain
objectclass=top

cn=MyCo employee,dc=my_co,dc=com

.
.
.

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

sn=Alvirez
departmentNumber=DEPTA
mail=jalvirez@my_co.com
telephoneNumber=999 999 9999
objectclass=top
objectclass=inetOrgPerson
objectclass=organizationalPerson
objectclass=person
cn=Jose Alvirez

.
.
.
```

Prva linija svakog unosa se naziva razlikovno ime (DN). DN-ovi su poput potpunog imena datoteke svakog unosa. Neki od unosa ne sadrže podatke i oni su samo strukturalni. Oni s linijom **objectclass=inetOrgPerson** odgovaraju unosima koje ste kreirali za ljude. Jose Alvirez DN je **cn=Jose Alvirez,cn=MyCo Employees,dc=my_co,dc=com**.

Scenarij: Kopiranje korisnika iz validacijske liste HTTP poslužitelja u Directory Server

Primjer kako kopirati korisnike iz validacijske liste HTTP poslužitelja u Directory Server.

Situacija i pregled

Trenutno imate aplikaciju koja se izvodi na HTTP poslužitelju (koju pogoni Apache) koristeći Internet korisnike u validacijskoj listi MYLIB/HTTPVLDL. Željeli biste koristiti te iste Internet korisnike s WebSphere Application Serverom (WAS) s LDAP provjerom autentičnosti. Radi izbjegavanja duplog održavanja korisničkih informacija u validacijskoj listi i LDAP-u, također ćete konfigurirati poslužiteljsku HTTP aplikaciju da koristi LDAP provjeru autentičnosti.

Da bi to postigli, ovo su koraci koje trebate napraviti:

1. Kopirajte postojeće korisnike validacijske liste na lokalni poslužitelj direktorija.
2. Konfigurirajte WAS poslužitelj da koristi LDAP provjeru autentičnosti.
3. Rekonfigurirajte HTTP poslužitelj da koristi LDAP provjeru autentičnosti umjesto validacijske liste.

Korak 1: Kopiranje postojećih korisnika validacijske liste u lokalni directory server

Pretpostavlja se da je poslužitelj direktorija prethodno konfiguriran s nastavkom ″o=my company″ i da se izvodi. LDAP korisnici trebaju biti pohranjeni u podstablo direktorija ″cn=users,o=my company″. Administrator poslužitelja direktorija DN je ″cn=administrator″ i administratorska lozinka je ″secret″.

Pozovite API iz komandne linije kako slijedi:

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

Kada je dovršeno, poslužitelj direktorija će sadržavati inetorgperson bazu unosa na unosima validacijske liste. Na primjer, korisnik validacijske liste:

```
Korisničko ime: jsmith
Opis: John Smith
Lozinka: ******
```

će rezultirati sa sljedećim unosom direktorija:

```
dn: uid=jsmith,cn=users,o=my company
objectclass: top
objectclass: osoba
objectclass: organizationalperson
objectclass: inetorgperson
uid: jsmith
sn: jsmith
cn: jsmith
opis: John Smith
userpassword: ******
```

Ovaj unos sada može biti korišten za provjeru autentičnosti na poslužitelj direktorija. Na primjer, izvođenje ovog QSH ldapsearch će pročitati korijenski DSE unos od poslužitelja:

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

Kad su jednom kreirani, možete urediti unose direktorija da sadrže dodatne informacije. Na primjer, možda ćete htjeti promijeniti cn i sn vrijednosti da odraze korisničko puno ime i prezime ili dodati telefonski broj i e-mail adresu.

Korak 2: Konfiguriranje WAS poslužitelj za korištenje LDAP provjere autentičnosti

WAS LDAP sigurnost treba biti konfigurirana da traži unose pod dn ″cn=users,o=my company″, koristeći filter pretraživanja koji mapira uneseno korisničko ime na inetOrgPerson unose koji sadrže tu uid vrijednost atributa. Na primjer, provjera autentičnosti na WAS koristeći korisničkom ime jsmith će rezultirati u pretraživanju unosa koji odgovaraju filteru pretraživanja ″(uid=jsmith)″. Za više informacija, pogledajte Konfiguriraj LDAP filtere pretraživanja u Websphere Application Server za iSeries Informacijski Centar.

Rekonfigurirajte HTTP poslužitelj za LDAP provjere autentičnosti umjesto validacijske liste

Bilješka: Procedura koja je opisana ispod je namijenjena da pomogne ilustrirati primjere u ovom scenariju prikazivanjem pregleda visoke razine konfiguracije HTTP poslužitelja za korištenje LDAP provjere autentičnosti. Možda ćete trebati detaljnije informacije nađene u IBM Redbooks publikaciji Implementacija i praktična upotreba LDAP-a na IBM eServer iSeries poslužitelju, SG24-6193 Odlomak 6.3.2 ″Postavljanje LDAP provjere autentičnosti za one koje pokreće Apache poslužitelj″ kao i Postavljanje zaštite lozinke na HTTP poslužitelju (pokretane preko Apachea).

1. Kliknite **Osnovna provjera autentičnosti** na **Konfiguracija** kartici od vašeg HTTP poslužitelja u HTTP Administracijskom alatu.
2. Pod **Metoda provjere autentičnosti korisnika**, promijenite **Koristite Internet korisnike u validacijskoj listi** da **Upotrijebite korisničke unose u LDAP poslužitelju** i kliknite **OK**.

3. Vratite se na **Konfiguracija** karticu i kliknite **Kontroliraj pristup**. Konfigurirajte to kako je opisano u Redbooks publikaciji za koju je gore navedena veza i kliknite **OK**.
4. Na **Konfiguracija** kartici kliknite **LDAP Provjera autentičnosti**.
   a. Unesite ime hosta LDAP poslužitelja i port. Za **DN Korisničke baze pretraživanja**, unesite cn=users,o=my company.
   b. Pod **Kreiraj jedinstveni LDAP DN za provjeru autentičnosti**, unesite filter (&objectclass=person)(uid=%v1)).
   c. Unesite informacije grupe i kliknite **OK**.
5. Konfigurirajte povezivanje na LDAP poslužitelj kako je opisano u Redbooks publikaciji za koju je gore navedena veza.

Administriranje Directory Servera

Koristite ovu informaciju za upravljanje Directory Server-om.

Da bi administrirali Poslužitelj direktorija, korisnički profil koji koristite mora imati sljedeće ovlaštenje:

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

Za upravljanje objektima direktorija (uključujući i liste kontrole pristupa, vlasništvo nad objektima i replike) trebate se spojiti na direktorij ili s DN administratora ili nekim drugim DN koji ima ispravno LDAP ovlaštenje. Ako je korištena integracija ovlaštenja, administrator može također biti projicirani korisnik (pogledajte “Projicirana pozadina operativnog sistema” na stranici 82) koji ima ovlaštenje na ID funkcije administracije Poslužitelja direktorija. Većina administrativnih zadataka može biti izvedena od strane korisnika u administrativnoj grupi (pogledajte “Administrativni pristup” na stranici 61).

Općeniti administracijski zadaci

Koristite ovu informaciju za upravljanje općenitom administracijom Directory Servera.

Pokretanje Directory Servera

Koristite ovu informaciju za pokretanje Directory Servera.

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM Poslužitelj direktorija** i izaberite **Pokreni**.

   Poslužitelju direktorija će možda trebati nekoliko minuta da se pokrene, ovisno o brzini vašeg poslužitelja i količini dostupne memorije. Kada prvi puta pokrenete poslužitelj direktorija možda će trajati nekoliko minuta duže nego obično zato što vaš poslužitelj mora kreirati nove datoteke. Slično, kad pokrećete directory server prvi put nakon nadogradnje ranije verzije Directory Servera, možda će trajati nekoliko minuta duže nego obično jer poslužitelj mora migrirati datoteke. Povremeno možete provjeravati status poslužitelja (pogledajte “Provjera status Directory Servera” na stranici 112) da bi vidjeli da li je već pokrenut.

Directory Server se također može pokrenuti iz sučelje baziranog na znakovima upisivanjem naredbe STRTCPSVR *DIRSRV. Uz to, ako vam je poslužitelj direktorija konfiguriran da se pokreće kad se pokrene TCP/IP, možete ga također pokretati tako da unesete naredbu STRTCP.

Poslužitelj direktorija se može konfigurirati u načinu samo konfiguracija iz sučelja zasnovanog na znakovima unošenjem naredbe TRCTCPAPP APP(*DIRSRV) ARGLIST(SAFEMODE).

Način samo konfiguracija pokreće poslužitelj s aktivnim samo cn=configuration sufiksom i ne ovisi o uspješnoj inicijalizaciji pozadina baze podataka.

Srodni zadaci

"Zaustavljanje Directory Servera"
Koristite ovu informaciju za zaustavljanje Directory Servera.

"Provjera status Directory Servera"
Koristite ovu informaciju za provjeru statusa Directory Servera.

Zaustavljanje Directory Servera

Koristite ovu informaciju za zaustavljanje Directory Servera.

Bilješka: Zaustavljanje Directory Server utječe na sve aplikacije koje koriste poslužitelj u trenutku njegovog zaustavljanja. Ovo uključuje aplikacije Mapiranja identiteta poduzeća (EIM) koje trenutno koriste poslužitelj direktorija za EIM operacije. Sve aplikacije su odspojene od poslužitelja direktorija, ipak, one nisu spriječene u pokušaju ponovnog spajanja na poslužitelj.

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM poslužitelj direktorija** i izaberite **Zaustavi**.

   Poslužitelj direktorija će možda trebati nekoliko minuta da se zaustavi, ovisno o brzini vašeg sistema, količini poslužiteljske aktivnosti i količini dostupne memorije. Povremeno možete provjeravati status poslužitelja (pogledajte "Provjera status Directory Servera") da bi vidjeli da li je već pokrenut.

Directory Server se također može zaustaviti iz sučelja baziranog na znakovima upisivanjem naredbe ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL ili ENDTCP. ENDTCPSVR *ALL i ENDTCP također utječu na bilo koji TCP/IP poslužitelj koji se izvodi na vašem sistemu. ENDTCP će također zaustaviti i sam TCP/IP.

Srodni zadaci

"Pokretanje Directory Servera" na stranici 111
Koristite ovu informaciju za pokretanje Directory Servera.

Provjera status Directory Servera

Koristite ovu informaciju za provjeru statusa Directory Servera.

Osnovne informacije o statusu nalaze se u System i Navigator. Naprednije i potpunije informacije o statusu se mogu naći koristeći Web administracijski alat.

System i Navigator prikazuje status Directory Servera u stupcu **Status**, u desnom okviru.

Za provjeru statusa Directory Servera u System i Navigator, poduzmite ove korake:

1. Proširite **Mrežu**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**. System i Navigator prikazuje status svih TCP/IP poslužitelja, uključujući poslužitelj direktorija, u stupcu **Status**. Za ažuriranje stanja poslužitelja, kliknite izbornik **Pogled** i izaberite **Osvježi**.
4. Da bi vidjeli više informacija o statusu poslužitelja direktorija, desno kliknite na **IBM Poslužitelj direktorija** i izaberite **Status**. Tako će se prikazati broj aktivnih veza, kao i druge informacije poput prošlih i trenutnih razina aktivnosti.

   Osim što pruža dodatne informacije, gledanje statusa s ovom opcijom može uštedjeti vrijeme. Možete osvježiti status Directory Servera bez dodatnog trošenja vremena koje je potrebno za provjeru statusa drugih TCP/IP poslužitelja.

Da bi vidjeli status poslužitelja direktorija koristeći Web administracijski alat, napravite sljedeće korake:

1. Proširite kategoriju **Administracija poslužitelja** u području navigacije.

   Bilješka: Za promjenu postavki konfiguracije poslužitelja pomoću zadataka u kategoriji Administracija poslužitelja Web Administration tool-a, morate provjeriti autentičnost poslužitelju kao i5/OS korisnički profil koji ima *ALLOBJ i IOSYSCFG posebna ovlaštenja. To može biti napravljeno ovlašćivanjem kao projicirani korisnik s lozinkom za taj profil. Da bi se vezali kao projicirani korisnik iz Web administracijskog alata, unesite korisničko ime oblika os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, gdje su MYUSERNAME i MYSYSTEM.COM nizovi zamijenjeni s vašim imenom korisničkog profila i konfiguriranim projiciranim nastavkom sistema.
2. Kliknite **Pogledaj status poslužitelja**.
3. Na **Pogledaj status poslužitelja** panelu, izaberite različite kartice da pregledate informacije statusa.

Provjera poslova na Directory Server-u

Koristite ovu informaciju za nadgledanje specifičnih poslova na Directory Server-u.

Za provjeru poslova poslužitelja u System i Navigator, poduzmite sljedeće korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM poslužitelj direktorija** i izaberite **Poslovi poslužitelja**.

Upravljanje vezama poslužitelja

Koristite ovu informaciju za gledanje svih veza na poslužitelj i operacija koje te veze izvode.

Administrator može donositi odluke za kontroliranje pristupa i sprječavanje napada odbijanja usluge baziranih na vezama. To se radi kroz Web administracijski alat.

Bilješka: Za promjenu postavki konfiguracije poslužitelja pomoću zadataka u kategoriji Administracija poslužitelja Web Administration tool-a, morate provjeriti autentičnost poslužitelju kao i5/OS korisnički profil koji ima *ALLOBJ i IOSYSCFG posebna ovlaštenja. To može biti napravljeno ovlašćivanjem kao projicirani korisnik s lozinkom za taj profil. Da bi se vezali kao projicirani korisnik iz Web administracijskog alata, unesite korisničko ime oblika os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, gdje su MYUSERNAME i MYSYSTEM.COM nizovi zamijenjeni s vašim imenom korisničkog profila i konfiguriranim projiciranim nastavkom sistema.

1. Proširite kategoriju **Administracija poslužitelja** u području navigacije.
2. Kliknite **Upravljanje vezama poslužitelja**.

   Prikazuje se tablica koja sadrži sljedeće informacije za svaku vezu:

   DN Navodi DN-ove klijentske veze prema poslužitelju.

   IP adresa
   Navodi IP adrese klijenta koji ima vezu na poslužitelj.

   Početno vrijeme
   Navodi datum i vrijeme (u lokalnom vremenu poslužitelja) kada je veza napravljena.

   Stanje Navodi da li je veza aktivna ili u mirovanju. Veza se smatra aktivnom ako ima neke operacije koje se izvode.

   Započete Ops
   Navodi broj operacija koje su zahtijevane od kada je veza ostvarena.

   Dovršene oper
   Navodi broj operacija koji su dovršene za svaku vezu.

Tip Navodi da li je veza osigurana putem SSL ili TLS. Inače, polje je prazno.

Bilješka: Ova tablica prikazuje do 20 veza u isto vrijeme.

Možete navesti da se ta tablica prikazuje po DN ili IP adresama proširivanjem padajućeg izbornika na gornjem panelu i izborom. Default izbor je po DN. Slično možete navesti da li prikazati tablicu u padajućem ili rastućem poretku.

3. Kliknite **Osvježi** da ažurirate trenutne informacije o vezi.
4. Ako ste prijavljeni kao administrator ili član administratorske grupe, imate dodatne izbore za odspajanje veza poslužitelja dostupnih na panelu. Ta mogućnost odspajanja veza poslužitelja omogućava vam da zaustavite napade odbijanjem usluge i kontrolirate napade na poslužitelj. Možete odspojiti vezu proširivanjem padajućih izbornika i izborom DN-a, IP adrese ili oboje i klikom na **Odspoji**. Da bi odspojili sve veze poslužitelja osim one koja radi ovaj zahtjev kliknite **Odspoji sve**. Prikazano je upozorenje o potvrdi. Kliknite **OK** da nastavite s akcijom odspajanja ili kliknite **Opoziv** da prekinete akciju i vratite se na panel **Upravljanje vezama poslužitelja**.

Za više informacija o sprječavanju napada odbijanja usluge, pogledajte Upravljanje svojstvima veze.

Srodni koncepti

"Odbijanje usluga" na stranici 81
Upotrijebite opciju konfiguriranja odbijanje usluge da biste se zaštitili od napada odbijanjem usluge.

Srodni zadaci

"Upravljanje svojstvima veze"
Koristite ovu informaciju za postavljanje svojstava veze kao što su one koje sprječavaju da klijenti zaključaju poslužitelj.

Upravljanje svojstvima veze

Koristite ovu informaciju za postavljanje svojstava veze kao što su one koje sprječavaju da klijenti zaključaju poslužitelj.

Sposobnost upravljanja svojstvima veze vam omogućuje da spriječite klijente od zaključavanja poslužitelja. Također osigurava da administrator uvijek ima pristup na poslužitelj u slučajevima kada je pozadina zauzeta s dugo izvodećim zadacima. Upravljanje svojstvima veze je napravljeno kroz Web administracijski alat.

Bilješka: Ovi izbori se prikazuju samo ako ste prijavljeni kao administrator ili član administratorske grupe na poslužitelju koji podržava tu funkciju.

Da bi postavili svojstva veze, izvedite sljedeće korake:

1. Proširite kategoriju **Administracija poslužitelja** u navigacijskom području i kliknite **Upravljanje svojstvima veze**.

   Bilješka: Za promjenu postavki konfiguracije poslužitelja pomoću zadataka u kategoriji Administracija poslužitelja Web Administration tool-a, morate provjeriti autentičnost poslužitelju kao i5/OS korisnički profil koji ima *ALLOBJ i IOSYSCFG posebna ovlaštenja. To može biti napravljeno ovlašćivanjem kao projicirani korisnik s lozinkom za taj profil. Da bi se vezali kao projicirani korisnik iz Web administracijskog alata, unesite korisničko ime oblika os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, gdje su MYUSERNAME i MYSYSTEM.COM nizovi zamijenjeni s vašim imenom korisničkog profila i konfiguriranim projiciranim nastavkom sistema.
2. Izaberite karticu **Općenito**.
3. Postavite postavku anonimnog povezivanja. **Dozvoli anonimno povezivanje** kontrolna kućica je već izabrana za vas tako da su anonimna vezanja dozvoljena. Ovo je default postavka. Možete kliknuti na kontrolnu kućicu da isključite funkciju **Dozvoli anonimna vezanja**. Ova akcija uzrokuje da poslužitelj prekine sve anonimne veze.

   Bilješka: Neke aplikacije se mogu srušiti ako onemogućite anonimna vezivanja.

4. U polju **Prag čišćenja za anonimne veze**, postavite broj praga da inicirate prekidanje anonimnih veza. Možete navesti broj između 0 i 65535.

   Bilješka: Stvarni maksimalni broj je ograničen s brojem datoteka dozvoljenih po procesu. Na UNIX sistemima vi možete koristiti **ulimit -a** naredbu da odredite granice. Na Windows sistemima to je fiksni broj.

   Default postavka je 0. Kada je taj broj anonimnih veza premašen, veze se čiste na osnovu vremenskog ograničenja mirovanja koji postavljate u polju **Vremensko ograničenje mirovanja**.
5. U polje **Očisti prag za ovlaštene veze** postavite broj praga za započinjanje prekidanja neovlaštenih veza. Možete navesti broj između 0 i 65535.

   Bilješka: Stvarni maksimalni broj je ograničen s brojem datoteka dozvoljenih po procesu. Na UNIX sistemima možete koristiti ulimit -a naredbu da odredite granice. Na Windows sistemima to je fiksni broj.

   Default postavka je 1100. Kada je ovaj broj ovlaštenih veza premašen, veze se čiste bazirano na granici vremenskog prekoračenja mirovanja koju postavljate u polju **Vremensko prekoračenje mirovanja**.
6. U polju **Prag čišćenja za sve veze** postavite broj praga da inicirate odspajanje svih veza. Možete navesti broj između 0 i 65535.

   Bilješka: Stvarni maksimalni broj je ograničen s brojem datoteka dozvoljenih po procesu. Na UNIX sistemima možete koristiti ulimit -a naredbu da odredite granice. Na Windows sistemima to je fiksni broj.

   Default postavka je 1200. Kada je ovaj ukupni broj veza premašen, veze se čiste bazirano na granici vremenskog prekoračenja mirovanja koju postavite u polju **Vremensko prekoračenje mirovanja**.
7. U polju **Granica vremenskog prekoračenja mirovanja** postavite broj sekundi koliko veza može biti u mirovanju prije nego što je zatvorena od strane procesa čišćenja. Možete navesti broj između 0 i 65535.

   Bilješka: Stvarni maksimalni broj je ograničen s brojem datoteka dozvoljenih po procesu. Na UNIX sistemima možete koristiti ulimit -a naredbu da odredite granice. Na Windows sistemima to je fiksni broj.

   Default postavka je 300. Kada je proces čišćenja iniciran, bilo koje veze, podložne procesu, koje premašuju granicu su zatvorene.
8. U polju **Rezultirajuća granica vremenskog prekoračenja** postavite broj sekundi koje su dopuštene između pokušaja pisanja. Možete navesti broj između 0 i 65535. Default postavka je 120. Sve veze koje premašuju ovu granicu su prekinute.

   Bilješka: To se odnosi samo na Windows sisteme. Veza koja premašuje 30 sekundi je automatski odbačena od strane operativnog sistema. Zbog toga se postavka **Rezultirajuća granica vremenskog ograničenja** nadjačava od strane operativnog sistema nakon 30 sekundi.
9. kliknite karticu **Nit opasnosti**.
10. Postavite postavku niti opasnosti. **Omogući nit opasnosti** kontrolna kućica je već izabrana za vas tako da nit opasnosti može biti aktivirana. Ovo je default postavka. Možete kliknuti na kontrolnu kućicu da isključite funkciju **Dozvoli nit opasnosti**. Ova akcija sprečava aktiviranje niti opasnosti.
11. U polju **Prag zahtjeva u čekanju** postavite brojčanu granicu za radne zahtjeve koji aktiviraju nit opasnosti. Navedite broj između 0 i 65535 da postavite granicu radnih zahtjeva koji mogu biti u redu prije aktiviranja niti opasnosti. Default je 50. Kada je navedena granica premašena, nit opasnosti je aktivirana.
12. U polju **Vremenski prag** postavite broj minuta koje će proći od kada je zadnja radna stavka uklonjena iz reda. Ako ima radnih stavki u redu i to je vremensko ograničenje premašeno, nit opasnosti je aktivirana. Možete navesti broj između 0 i 240. Default postavka je 5.
13. Izaberite iz padajućeg izbornika, kriterij za korištenje kod aktivacije niti opasnosti. Možete izabrati:
    - **Samo veličina:** Nit opasnosti se aktivira samo kada red premašuje navedenu količinu radnih stavki u čekanju.
    - **Samo vrijeme:** Nit opasnosti se aktivira samo kada vremenska granica između uklonjenih radnih stavki premašuje navedenu količinu.
    - **Veličina ili vrijeme:** Nit opasnosti se aktivira kada veličina reda ili vremenski prag premašuje navedene količine.
    - **Veličina i vrijeme:** Nit opasnosti se aktivira kada veličina reda i vremenski prag premašuju navedene količine.

Veličina i vrijeme je default postavka.

14. Kliknite **OK**.

Srodni koncepti

“Odbijanje usluga” na stranici 81
Upotrijebite opciju konfiguriranja odbijanje usluge da biste se zaštitili od napada odbijanjem usluge.

Srodni zadaci

“Upravljanje vezama poslužitelja” na stranici 113
Koristite ovu informaciju za gledanje svih veza na poslužitelj i operacija koje te veze izvode.

Omogućavanje obavještavanja o događajima

Koristite ovu informaciju za omogućavanje obavještavanja o događajima Directory Servera.

Obavještavanje o događajima dozvoljava klijentima da se registriraju na Directory Server-u kako bi primali obavijesti kada navedeni događaj, kao nešto što se dodaje direktoriju, odvija.

Za omogućavanje obavještavanja o događajima za vaš poslužitelj, slijedite ove korake:

1. Proširite kategoriju **Upravljanje svojstvima poslužitelja** u području navigacije Web administracijskog alata, izaberite karticu **Obavijest o događaju**.
2. Izaberite kontrolnu kućicu **Omogući obavještavanje o događaju** da omogućite obavještavanje o događaju. Ako je **Omogući obavještavanje o događaju** onemogućeno, poslužitelj zanemaruje sve druge opcije na ovom panelu.
3. Postavite **Maksimalne registracije po vezi**. Kliknite na **Registracije** ili **Neograničeno** radio gumb. Ako izaberete **Registracije**, trebate u polju navesti maksimalni broj registracija dozvoljenih za svaku vezu. Maksimalni broj transakcija je 2,147,483,647. Default postavka je 100 registracija.
4. Postavite **Zbroj maksimalnih registracija**. Ovaj izbor postavlja koliko registracija poslužitelj može imati u jednom trenutku. Kliknite na **Registracije** ili **Neograničeno** radio gumb. Ako izaberete **Registracije**, trebate u polju navesti maksimalni broj registracija dozvoljenih za svaku vezu. Maksimalni broj transakcija je 2,147,483,647. Default broj transakcija je **Neograničeno**.
5. Kada završite kliknite **Primijeni** da spremite vaše izmjene bez izlaska ili kliknite **OK** da primijenite vaše promjene i izađete ili kliknite **Opoziv** da izađete iz ovog panela bez promjena.
6. Ako ste omogućili obavještavanje o događajima, morate ponovno pokrenuti poslužitelj da bi promjene imale učinka. Ako ste mijenjali samo postavke, poslužitelj se ne treba ponovno pokretati.

Bilješka: Da bi onemogućili obavještavanje o događajima, poništite izbor kontrolne kućice **Omogućavanje obavještavanja o događajima** i ponovno pokrenite poslužitelj.

Za dodatne informacije o obavještavanju o događajima, pogledajte odlomak Obavještavanje o događajima reference programiranja IBM Tivoli Directory Server verzije 6.0.

Srodne informacije

IBM Tivoli softver Informacijski centar
Pogledajte IBM Tivoli softver Informacijski centar radi informacija o IBM Tivoli Directory Serveru.

Specificiranje postavki transakcije

Koristite ovu informaciju za konfiguriranje postavki transakcije Directory Servera.

Transakcije Directory Servera dozvoljavaju grupi operacija LDAP direktorija da se tretira kao jedna jedinica.

Da konfigurirate transakcijske postavke vašeg poslužitelja, slijedite ove korake:

1. Proširite kategoriju **Upravljanje svojstvima poslužitelja** u navigacijskom području alata Web administracije, izaberite karticu **Transakcija**.
2. Izaberite **Omogući procesiranje transakcija** da omogućite procesiranje transakcija. Ako je **Omogući procesiranje transakcija** onemogućeno, sve druge opcije na ovom panelu, kao što su **Maksimalni broj operacija po transakciji** i **Vremensko ograničenje čekanja** se zanemaruju od strane poslužitelja.

3. Postavite **Maksimalni broj transakcija**. Kliknite na radio gumb **Transakcije** ili **Neograničeno**. Ako izaberete **Transakcije**, trebate navesti u polju maksimalni broj transakcija. Maksimalni broj transakcija je 2,147,483,647. Default postavka je 20 transakcija.
4. Postavite **Maksimalni broj operacija po transakciji**. Kliknite na radio gumb **Operacije** ili **Neograničeno**. Ako izaberete **Operacije**, trebate navesti u polju maksimalni broj operacija dozvoljenih za svaku transakciju. Maksimalni broj operacija je 2,147,483,647. Što je broj manji, bolje su performanse. Default je 5 operacija.
5. Postavite **Vremensko ograničenje čekanja**. Ovaj izbor postavlja minimalnu vrijednost timeouta za čekajuće transakcije u sekundama. Kliknite na radio gumb **Sekunde** ili **Neograničeno**. Ako izaberete **Sekunde**, trebate navesti u polju maksimalni broj sekundi dozvoljenih za svaku transakciju. Maksimalni broj sekunda je 2,147,483,647. Transakcije koje su nedovršene nakon tog vremena se opozivaju (vraćaju natrag). Default je 300 sekunda.
6. Kada završite kliknite **Primijeni** da spremite vaše izmjene bez izlaska ili kliknite **OK** da primijenite vaše promjene i izađete ili kliknite **Opoziv** da izađete iz ovog panela bez promjena.
7. Ako ste omogućili podršku transakcija, morate ponovno pokrenuti poslužitelj da bi promjene imale učinak. Ako ste mijenjali samo postavke, poslužitelj se ne treba ponovno pokretati.

Bilješka: Da onemogućite obrađivanje transakcija, obrišite kvačicu u kontrolnoj kućici **Omogući obrađivanje transakcija** i ponovno pokrenite poslužitelj.

Srodni koncepti

"Transakcije" na stranici 50
Možete konfigurirati Poslužitelj direktorija kako bi omogućili klijentima da koriste transakcije. Transakcija je grupa operacija LDAP direktorija koje se tretiraju kao jedna jedinica.

Promjena porta ili IP adrese

Koristite ovaj postupak za promjenu portova koje Directory Server koristi ili IP adrese na kojoj Directory Server prihvaća veze.

Poslužitelj direktorija koristi sljedeće default portove:

- 389 za nezaštićene veze.
- 636 za sigurne veze (ako ste koristili Upravitelj digitalnih certifikata koji Directory Server aktivira kao aplikaciju koja koristi sigurni port).

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

Ako već koristite te portove za drugu aplikaciju, možete ili dodijeliti različit port Directory Server-u ili koristiti različite IP adrese za ta dva poslužitelja, ako aplikacije podržavaju vezivanje na određenu IP adresu.

Za promjenu portova koje Directory Server koristi ili IP adrese na kojoj Directory Server prihvaća veze, poduzmite sljedeće korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM poslužitelj direktorija** i izaberite **Svojstva**.
5. Kliknite karticu **Mreža**.
6. Ako želite promijeniti broj porta, upišite odgovarajuće brojeve porta, zatim kliknite **OK**.
7. Ako želite promijeniti IP adresu, kliknite tipku **IP adrese...**. Zatim nastavite sa sljedećim korakom.
8. Izaberite **Koristite izabrane IP adrese** i izaberite IP adrese koje će poslužitelj koristiti za prihvaćanje veza.

Srodne informacije

Host Domino LDAP i Directory Server na istom sistemu

Specificiranje poslužitelja za upućivanja direktorija

Koristite ovu informaciju za specificiranje referalnih poslužitelja.

Za dodjelu referalnih poslužitelja za Directory Server, poduzmite sljedeće korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM Poslužitelj direktorija**, onda izaberite **Svojstva**.
5. Izaberite stranicu svojstva **Općenito**.
6. U polju **Novi referal**, specificirajte URL referalnog poslužitelja.
7. Na upit odredite ime referalnog poslužitelja u URL formatu. U nastavku su primjeri prihvatljivih URL-a za LDAP:
   - ldap://test.server.com
   - ldap://test.server.com:400
   - ldap://9.9.99.255

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

Srodni koncepti

"Referali LDAP direktorija" na stranici 49
Referali omogućuju Poslužiteljima direktorija da rade u timovima. Ako DN koji klijent zahtijeva nije u jednom direktoriju, poslužitelj može automatski poslati (uputiti) zahtjev na neki drugi LDAP poslužitelj.

Dodavanje i uklanjanje sufiksa Directory Servera

Koristite ovu informaciju za dodavanje ili uklanjanje sufiksa Directory Servera.

Dodavanje sufiksa Poslužitelju direktorija omogućava poslužitelju da upravlja tim dijelom stabla direktorija.

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

Ako dodajete sufiks u poslužitelj direktorija, poduzmite ove korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desnim klikom izaberite **IBM Directory Server** i izaberite **Svojstva**.
5. Kliknite karticu **Baze podataka/Sufiksi**.
6. U polju **Novi sufiks** upišite ime novoga sufiksa.
7. Kliknite **Dodavanje**.
8. Kliknite **OK**.

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

Kako bi uklonili sufiks iz Poslužitelja direktorija, poduzmite ove korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.

4. Desnim klikom izaberite **IBM Directory Server** i izaberite **Svojstva**.
5. Kliknite karticu **Baze podataka/Sufiksi**.
6. Kliknite nastavak koji želite ukloniti.
7. Kliknite **Ukloni**.

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

Srodni koncepti

"Sufiks (kontekst imenovanja)" na stranici 12
Sufiks (poznat i kao kontekst imenovanja) je DN koji identificira najviši unos u lokalno zadržanoj hijerarhiji direktorija.

Dodavanje sufiksa na directory server:
Ako dodajete sufiks u poslužitelj direktorija, poduzmite ove korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM poslužitelj direktorija** i izaberite **Svojstva**.
5. Kliknite karticu **Baze podataka/Sufiksi**.
6. U polju **Novi sufiks** upišite ime novoga sufiksa.
7. Kliknite **Dodavanje**.
8. Kliknite **OK**.

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

Uklanjanje sufiksa iz Directory Servera:
Kako bi uklonili sufiks iz Poslužitelja direktorija, poduzmite ove korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM poslužitelj direktorija** i izaberite **Svojstva**.
5. Kliknite karticu **Baze podataka/Sufiksi**.
6. Kliknite nastavak koji želite ukloniti.
7. Kliknite **Ukloni**.

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

Dodjeljivanje administratorskog pristupa projiciranim korisnicima

Koristite ovu informaciju za dodjeljivanje administratorskog pristupa korisničkim profilima.

Administratorski pristup možete dodijeliti profilima korisnika kojima je bio dan pristup identifikatoru funkcije (ID) Administrator poslužitelja direktorija (QIBM_DIRSRV_ADMIN).

Na primjer, ako je profilu korisnika JOHHNSMITH dodijeljen pristup na ID funkcije Administratora poslužitelja direktorija i izabrana je opcija Dodijeli administratorski pristup ovlaštenim korisnicima iz dijaloga Svojstvo direktorija, onda JOHNSMITH profil ima ovlaštenje LDAP administratora. Kad se ovaj profil koristi za povezivanje na poslužitelj

direktorija korištenjem sljedećeg DN-a, os400-profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com, korisnik ima administratorsko ovlaštenje. Sufiks sistemskih objekata u ovom primjeru je os400-sys=systemA.acme.com.

Za izbor opcije Dodijeli administratorski pristup ovlaštenim korisnicima i ID funkcije administratoru Directory Servera, poduzmite sljedeće korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
4. Na kartici **Općenito** pod **Administratorske informacije**, izaberite opciju **Dodijeli administratorski pristup ovlaštenim korisnicima**.
5. U System i Navigator, desno kliknite na ime sistema i izaberite **Administracija aplikacija**.
6. Kliknite karticu **Host aplikacije**.
7. Proširite **Operating System/400**.
8. Kliknite na **Administrator poslužitelja direktorija** da osvijetlite opciju.
9. Kliknite tipku **Prilagodi**.
10. Proširite **Korisnici**, **Grupe** ili **Korisnici koji nisu u grupi**, što odgovara korisniku kojeg želite.
11. Izaberite korisnika ili grupu koji će se dodati na listu **Dozvoljen pristup**.
12. Kliknite tipku **Dodavanje**.
13. Kliknite **OK** za spremanje promjena.
14. Kliknite **OK** na dijalogu **Administracija aplikacija**.

Srodni koncepti

"Administrativni pristup" na stranici 61
Koristite administrativni pristup za kontrolu pristupa specifičnim administrativnim zadacima.

"Projicirana pozadina operativnog sistema" na stranici 82
Sistemski projicirana pozadina ima sposobnost mapiratii5/OS objekte kao unose unutar LDAP-pristupnog stabla direktorija. Projicirani objekti su LDAP prikazi objekata operativnog sistema umjesto stvarnih unosa pohranjenih u LDAP bazi podataka poslužitelja.

Omogućavanje oznaka jezika

Koristite ovu informaciju za omogućavanje oznaka jezika.

Da bi omogućili oznake jezika, napravite sljedeće (one su po defaultu onemogućene):

1. Kliknite **Upravljanje svojstvima poslužitelja** pod kategorijom **Administracija poslužitelja** u navigacijskom području.

   Bilješka: Za promjenu postavki konfiguracije poslužitelja pomoću zadataka u kategoriji Administracija poslužitelja Web Administration tool-a, morate provjeriti autentičnost poslužitelju kao i5/OS korisnički profil koji ima *ALLOBJ i IOSYSCFG posebna ovlaštenja. To može biti napravljeno ovlašćivanjem kao projicirani korisnik s lozinkom za taj profil. Da bi se vezali kao projicirani korisnik iz Web administracijskog alata, unesite korisničko ime oblika os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, gdje su MYUSERNAME i MYSYSTEM.COM nizovi zamijenjeni s vašim imenom korisničkog profila i konfiguriranim projiciranim nastavkom sistema.
2. Kartica Općenito je predizabrana. Kliknite **Omogući podršku oznake jezika** da ju omogućite.

   Bilješka: Nakon omogućavanja funkcije oznake jezika, ako pridružite oznaku jezika s atributima unosa, poslužitelj vraća unos s oznakom jezika. To se događa čak i ako kasnije onemogućite funkciju oznake jezika. Zato što ponašanje poslužitelja možda neće biti ono što aplikacija očekuje i da bi izbjegli potencijalne probleme, nemojte onemogućiti funkciju oznake jezika nakon što ju omogućite.

Praćenje pristupa i promjena do LDAP direktorija

Koristite ovu informaciju za praćenje pristupa i promjena do LDAP direktorija.

Možete koristiti dnevnik promjena LDAP direktorija kako bi mogli pratiti promjene nad direktorijom. Dnevnik promjena se nalazi pod posebnim sufiksom cn=changelog. Pohranjen je u knjižnici QUSRDIRCL.

Da aktivirate dnevnik promjena, slijedite ove korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM poslužitelj direktorija** i izaberite **Svojstva**.
5. Kliknite karticu **Promjena dnevnika**.
6. Izaberite **Zapiši promjene direktorija**.
7. Opcijsko: U polju **Maksimum unosa** specificirajte maksimum broja unosa promjena koje će dnevnik čuvati. U polju **Maksimalna starost** specificirajte koliko dugo se zadržavaju unosi dnevnika promjena.

   Bilješka: Iako su ti parametri opcijski, trebate razmotriti navođenje ili maksimalnog broja unosa ili maksimalne starosti. Ako ne navedete niti jedan, dnevnik promjena će zadržati sve unose i možda će postati prevelik.

Klasa objekta changeLogEntry se koristi za prikaz promjena napravljenih u poslužitelju direktorija. Skup promjena je dan pomoću poredanog skupa svih unosa unutar spremnika dnevnika promjena kao što je definirano pomoću changeNumber. Informacije dnevnika promjena su samo za čitanje.

Bilo koji korisnik koji je na listi kontrole pristupa za cn=changelog nastavak može pretraživati unose u dnevniku promjena. Trebali bi izvoditi samo traženja na sufiksu dnevnika promjena cn=changelog. Nemojte pokušati dodati, promijeniti ili obrisati nastavak dnevnika promjena, čak i ako imate ovlaštenje da to napravite. To može uzrokovati nepredviđene rezultate.

Primjer:

Sljedeći primjer koristi **ldapsearch** pomoćni program reda za naredbe da dohvati sve unose dnevnika promjena zapisane na poslužitelju:

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

Omogućavanje revizije objekta na Directory Server-u

Koristite ovu informaciju za omogućavanje revizije objekta za Directory Server.

Directory Server podržava i5/OS reviziju sigurnosti. Ako sistemska vrijednost QAUDCTL ima specificirano *OBJAUD, možete omogućiti reviziju objekta kroz System i Navigator.

Za omogućavanje revizije objekta za Directory Server, slijedite ove korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM poslužitelj direktorija** i izaberite **Svojstva**.
5. Kliknite karticu **Revizija**.
6. Izaberite postavke revizije koje želite koristiti za vaš poslužitelj.
7. Kliknite **OK**.

Promjene na postavkama revizije će imati utjecaj čim kliknete na **OK**. Nema potrebe za ponovnim pokretanjem Poslužitelja direktorija.

Srodni koncepti

"Revizija" na stranici 51
Revidiranje vam dozvoljava praćenje detalja određenih transakcija Directory Servera.

"Sigurnost Poslužitelja direktorija" na stranici 50
Saznajte kako se raznolikost funkcija može koristiti da učini vaš Directory Server sigurnim.

Prilagođavanje postavki pretraživanja

Koristite ovu informaciju za kontroliranje korisničkih sposobnosti pretraživanja.

Možete postaviti parametre pretraživanja da kontrolirate korisničke sposobnosti pretraživanja, kao što je stranično i sortirano pretraživanje, vremenske i granice veličine i alias dereferencirajuće opcije, koristeći alat Web administracije.

Stranični rezultati dozvoljavaju klijentu da upravlja količinom podataka vraćenih iz zahtjeva pretraživanja. Klijent može zahtijevati podskup unosa (stranicu) umjesto primanja svih rezultata odjednom. Naredni zahtjev za pretraživanjem prikazuje sljedeću stranicu rezultata tako dugo dok se operacija ne opozove ili dok se ne vrati posljednji rezultat.

Sortirano pretraživanje dozvoljava klijentu da primi rezultate pretraživanja sortirane po listi kriterija, gdje svaki kriterij predstavlja ključ sortiranja. Time se premješta odgovornost za sortiranje iz aplikacije klijenta na poslužitelj.

Da bi prilagodili postavke poslužitelja direktorija, pratite ove korake:

1. Proširite **Administracija poslužitelja** u navigacijskom području i kliknite **Upravljanje svojstvima poslužitelja**.

   Bilješka: Za promjenu postavki konfiguracije poslužitelja pomoću zadataka u kategoriji Administracija poslužitelja Web Administration tool-a, morate provjeriti autentičnost poslužitelju kao i5/OS korisnički profil koji ima *ALLOBJ i IOSYSCFG posebna ovlaštenja. To može biti napravljeno ovlašćivanjem kao projicirani korisnik s lozinkom za taj profil. Da bi se vezali kao projicirani korisnik iz Web administracijskog alata, unesite korisničko ime oblika os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, gdje su MYUSERNAME i MYSYSTEM.COM nizovi zamijenjeni s vašim imenom korisničkog profila i konfiguriranim projiciranim nastavkom sistema.
2. Izaberite karticu **Postavke pretraživanja**.
3. Postavite **Granicu pretraživanja**. Kliknite na **Unosi** ili **Neograničeno**. Ako izaberete **Unosi**, trebate navesti u polju maksimalni broj unosa koje pretraživanje vraća. Default postavka je 500. Ako više unosa odgovara kriteriju pretraživanja, oni se ne vraćaju. Ova granica se ne odnosi na administratore ili članove grupe ograničavanja pretraživanja kojima su dodijeljene veće granice veličine pretraživanja.
4. Postavite **Vremensko ograničenje pretraživanja**. Kliknite na radio gumb **Sekunde** ili **Neograničeno**. Ako izaberete **Sekunde**, trebate navesti u polju maksimalnu količinu vremena koju poslužitelj troši na obrađivanje zahtjeva. Default postavka je 900. Ova granica se ne odnosi na administratore ili članove grupe ograničavanja pretraživanja kojima su dodijeljene veće vremenske granice pretraživanja.
5. Da bi ograničili sposobnosti sortiranja pretraživanja na administratore, izaberite **Samo administratori mogu sortirati pretraživanje**.
6. Da bi ograničili sposobnosti podjele u stranice na administratore, izaberite **Samo administratori mogu pretraživati stranice**.
7. Proširite padajući izbornik za **Dereferenciranje zamjenskih imena** i izaberite jedno od sljedećeg. Default postavka je **Uvijek**.

   Nikad Zamjenska imena se nikad ne dereferenciraju.

   Nalaženje
   Zamjenska imena se dereferenciraju kod pronalaženja početne točke pretraživanja, ali ne kod pretraživanja pod tim početnim unosom.

   Traženje
   Zamjenska imena se dereferenciraju kod pretraživanja unosa ispod početne točke pretraživanja, ali ne kod pronalaženja početnih unosa.

Uvijek Zamjenska imena se uvijek dereferenciraju i kod pronalaženja početne točke za pretraživanje i kod pretraživanja unosa ispod početne točke. Uvijek je default postavka.

Srodni zadaci

"Pretraživanje unosa direktorija" na stranici 188
Koristite ovu informaciju za pretraživanje unosa direktorija.

Srodne reference

"Parametri pretraživanja" na stranici 46
Da bi ograničili broj resursa korištenih od strane poslužitelja, administrator može postaviti parametre pretraživanja da ograniči korisničke mogućnosti pretraživanja. Mogućnosti pretraživanja se također mogu proširiti za posebne korisnika.

Omogućavanje ili onemogućavanje pristupa čitanja projiciranim korisnicima

Koristite ovu informaciju za zabranu operacija pretraživanja i uspoređivanja backendu projiciranih korisnika.

Za zabranu operacija pretraživanja i uspoređivanja backendu projiciranih korisnika, učinite sljedeće:

1. Zaustavite directory server. Upišite ENDTCPSVR *DIRSRV.
2. Uredite datoteku /QIBM/UserData/OS400/DirSrv/ibmslapd.conf. Na primjer, upišite EDTF '/QIBM/UserData/OS400/DirSrv/ibmslapd.conf'.
3. Tražite tekst cn=Front End.
4. Umetnite novu liniju s tekstom ibm-slapdSetEnv: IBMSLAPDOS400USRPRJREAD=FALSE odmah nakon linije koja sadrži tekst cn=Front End. U sljedećem primjeru umetnuta je druga linija:

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

5. Spremite datoteku i izađite iz editora. Na primjer, pritisnute F2 za spremanje datoteke i zatim F3 za izlaz iz editora ako koristite EDTF.
6. Ponovno pokrenite directory server. Upišite STRTCPSVR *DIRSRV.

Srodni koncepti

"Pristup čitanja za projicirane korisnike" na stranici 86
Po defaultu, backend projekcije sistema osigurava pristup čitanja informacijama korisničkog profila ovlaštenim korisnicima kroz LDAP operacije pretraživanja i uspoređivanja. Pristup čitanja projiciranim korisnicima može se omogućiti ili onemogućiti pomoću System i Navigator ili postavkom konfiguracije u datoteci /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf (datoteka /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf za instancu default poslužitelja).

Objavljivanje informacija Directory Server-u

Koristite ovu informaciju za objavljivanje informacija Directory Server-u.

Možete konfigurirati vaš sistem da objavi određene informacije u Poslužitelj direktorija na istom sistemu ili na različitim sistemima kao i korisničko definirane informacije. Operativni sistem automatski objavljuje te informacije Directory Server-u kad koristite System i Navigator za promjenu tih informacija na i5/OS. Informacije koje možete objaviti uključuju sistem (sisteme i pisače), dijeljenje pisača, korisničke informacije i politike TCP/IP Kvaliteta usluga.

Ako nadređeni DN kojem se podaci objavljuju ne postoji, Directory Server ga automatski kreira. Možda ste već instalirali drugei5/OS aplikacije koje objavljuju informacije u LDAP direktorij. Osim toga, možete pozvati sučelje aplikativnog programa (API-ji) iz svojih vlastitih programa kako bi objavili druge tipove informacija na LDAP direktoriju.

Bilješka: Možete također objaviti i5/OS informacije directory server-u koji ne radi na i5/OS ako konfigurirate da poslužitelj koristi IBM shemu.

Za konfiguraciju vašeg sistema za objavljivanje i5/OS informacija u directory server, poduzmite sljedeće korake:

1. U System i Navigator, desnom tipkom miša kliknite na vaš sistem i izaberite **Svojstva**.

2. Kliknite na karticu **Poslužitelj direktorija**.
3. Izaberite tipove informacija koje želite objaviti. Izaberite tipove informacija koje želite objaviti.

   Savjet: Ako planirate objavljivati više od jednog tipa podataka u istu lokaciju, možete uštedjeti na vremenu tako da izaberete više tipova podataka i konfigurirate ih istovremeno. Navigator Operacija će potom koristiti vrijednosti koje unesete kad konfigurirate jedan tip podataka kao default vrijednosti kad konfigurirate sve kasnije tipove podataka.
4. Kliknite **Details**.
5. Kliknite **Izdavanje sistemskih informacija** kućicu .
6. Navedite **Metodu provjere ovlaštenja** koju želite da poslužitelj koristi, kao i prikladne informacije o provjeri ovlaštenja.
7. Kliknite gumb **Uredi** pokraj polja**(Aktivan) Poslužitelj direktorija**. U dijalog koji se pojavi, upišite ime directory servera u koji želite objavitii5/OS informacije, zatim kliknite **OK**.
8. U polje **Ispod DN-a** unesite ime nadređenog razlikovnog imena (DN) gdje želite da se dodaju informacije na poslužitelj direktorija.
9. Ispunite polja u okviru **Veza poslužitelja** koja su prikladna vašoj konfiguraciji.

   Bilješka: Za objavljivanje i5/OS informacija u directory server pomoću SSL-a ili Kerberos-a, najprije trebate konfigurirati svoj directory server na upotrebu odgovarajućeg protokola. Pogledajte “Kerberos provjera autentičnosti s Poslužiteljem direktorija” na stranici 52 za više informacija o SSL i Kerberos.
10. Ako vaš poslužitelj ne koristi default port, unesite ispravni broj porta u polju **Port**.
11. Kliknite **Provjera** da osigurate da nadređeno DN postoji na poslužitelju i da je informacija o vezi ispravna. Ako staza direktorija ne postoji, pojavit će se dijalog iz kojega ju možete kreirati.

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

Bilješka: Možete također objaviti i5/OS informacije u directory server koji je na različitoj platformi. Morate objaviti informacije o korisnicima i sistemu u directory server koji koristi shemu koja je kompatibilna s IBM Directory Server shemom. Radi više informacija o IBM shemi direktorija, pogledajte “Shema Directory Servera” na stranici 14.

Možete također koristiti LDAP konfiguraciju poslužitelja i objavljivanje API-eva kako biste omogućili i5/OS da programi koje pišete objavljuju druge tipove informacija. Ti tipovi informacija se onda pojavljuju i na stranici **Poslužitelj direktorija**. Poput korisnika i sistema i oni su početno onemogućeni i možete ih konfigurirati korištenjem iste procedure. Program koji dodaje podatke u LDAP direktorij se naziva izdavački agent. Tip informacije koji je objavljen kada se pojavi na stranici **Poslužitelj direktorija** se naziva ime agenta.

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

QgldChgDirSvrA
Aplikacija koristi CSVR0500 format za inicijalno dodavanje imena agenta koje je označeno kao onemogućeni unos. Upute za korisnike aplikacije bi ih trebale uputiti da koriste System i Navigator kako bi išli na stranicu svojstva Poslužitelja direktorija i kako bi konfigurirali agent objavljivanja. Primjeri imena agenta su imena agenta sistema i korisnika koja su automatski dostupna na stranici **Poslužitelj direktorija**.

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

QgldPubDirObj
Ovaj API upotrijebite za objavljivanje podataka.

Srodni koncepti

"Objavljivanje" na stranici 35
Directory Server osigurava sposobnost da sistem može objaviti određene vrste informacija LDAP direktoriju. To znači, sistem će kreirati i ažurirati LDAP unose koji predstavljaju različite tipove podataka.

Directory Server API-ji

Importiranje LDIF datoteke

Koristite ovu informaciju za importiranje datoteke LDAP format izmjenjivanja podataka (LDIF)

Možete prenositi informacije o različitim Poslužiteljima direktorija korištenjem datoteka LDAP Format razmjene podataka (LDIF). Alat za importiranje (i odgovarajući QgldImportLdif API) koriste se za dodavanje novih unosa u direktorij. Alat za importiranje ne može se koristiti za mijenjanje ili brisanje unosa, a LDIF datoteka mora koristiti stil sadržaja direktorija umjesto LDIF slogova stila sloga promjena. Ako LDIF datoteka unosa sadrži changetype direktive korištene u LDIF slogovima stila sloga promjena, changetype linija se tumači kao još jedan atribut, a unos se neće dodavati u direktorij.

Kod tipičnog korištenja, cijeli direktorij ili podstablo direktorija, eksportira se iz jednog poslužitelja pomoću alata za eksportiranje (ili QgldExportLdif API), te zatim importira na drugi poslužitelj.

Alati za eksportiranje i importiranje nisu ekvivalentni za upotrebu ldapsearch i ldapadd pomoćnih programa reda za naredbe. Alat za eksportiranje uključuje nekoliko operativnih atributa (kao što su informacije o kontroli pristupa i vremenske oznake kreiranja unosa) koje normalno ldapsearch ne vraća, dok alat za importiranje može postaviti atribute koje normalno ne može postaviti aplikacija klijenta kao što je ldapadd. ldapadd pomoćni program može se koristiti s -k opcijom (kontrola administracije poslužitelja) za učitavanje tih datoteka.

Prije pokretanja te procedure, prenesite LDIF datoteku u svoj sistem kao neprekidnu datoteku.

Za import LDIF datoteke na poslužitelj direktorija, poduzmite ove korake:

1. Ako je poslužitelj direktorija pokrenut, zaustavite ga. Pogledajte "Pokretanje Directory Servera" na stranici 111 radi informacija o zaustavljanju poslužitelja direktorija.
2. U System i Navigator, proširite **Mreža**.
3. Proširite **Poslužitelji**.
4. Kliknite **TCP/IP**.
5. Desno kliknite na **IBM Poslužitelj direktorija** i izaberite **Alati**, onda **Importiraj Datoteku**.

   Neobvezno, poslužitelj može replicirati novo importirane podatke kada se sljedeći put pokrene, ako izaberete **Repliciraj importirane podatke**. To je korisno kada dodajete nove unose na postojeće stablo direktorija na glavnom poslužitelju. Ako importirate podatke da bi inicijalizirali replika (ili ravnopravni) poslužitelj, tipično nećete htjeti replicirati podatke, pošto već mogu postojati na poslužiteljima za koje je taj poslužitelj dobavljač.

Bilješka: Možete također koristiti ldapadd pomoćni program za importiranje LDIF datoteke.

Srodne reference

"LDAP format razmjene podataka (LDIF)" na stranici 236
LDAP format razmjene podataka je standardni tekstualni format za prikazivanje LDAP objekata i LDAP ažuriranja (dodaj, modificiraj, obriši, modificiraj DN) u tekstualnom obliku. Datoteke koje sadrže LDIF slogove mogu se koristiti za prijenos podataka između directory servera ili kao ulaz LDAP alatima poput **ldapadd** i **ldapmodify**.

"ldapmodify i ldapadd" na stranici 205
Pomoćni programi reda za naredbe LDAP modificiraj-unos i LDAP dodaj-unos.

Eksportiranje LDIF datoteke

Koristite ovu informaciju za eksportiranje datoteke LDAP format izmjenjivanja podataka (LDIF)

Možete prenositi informacije između različitih LDIF datoteka. U neku LDIF datoteku možete eksportirati sve ili dio svog LDAP direktorija.

Za eksport LDIF datoteke iz poslužitelja direktorija, napravite ove korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM Poslužitelj direktorija** i izaberite **Alati**, onda **Eksportiraj datoteku**.

   Bilješka: Ako želite navesti potpuno kvalificiranu stazu za LDIF datoteke za eksportiranje podataka, datoteka neće biti kreirana u početnom direktoriju navedenom u vašem korisničkom profilu operativnog sistema.
5. Navedite da li treba **Eksportirati cijeli direktorij** ili **Eksportirati izabrano podstablo** kao i da li **Eksportirati operativne atribute**. Operativni atributi koji su eksportirani su creatorsName, createTimestamp, modifiersName i modifyTimestamp.

Napomene:

1. Kod eksportiranja podataka za importiranje u V5R3 ili ranije poslužitelje direktorija, nemojte izabrati **Eksportiraj operativne atribute**. Ti operativni atributi ne mogu biti importirani u V5R3 ili ranije poslužitelje direktorija.
2. Možete također kreirati potpunu ili djelomičnu LDIF datoteku s ldapsearch pomoćnim programom. Koristite -L opciju i preusmjerite izlaz u datoteku.
3. Pazite da odredite ovlaštenje za LDIF datoteku da spriječite neovlašteni pristup podacima u direktoriju. Ako to činite, desnom tipkom kliknite na datoteku u System i Navigator, a zatim izaberite **Dozvole**.

Srodne reference

“LDAP format razmjene podataka (LDIF)” na stranici 236
LDAP format razmjene podataka je standardni tekstualni format za prikazivanje LDAP objekata i LDAP ažuriranja (dodaj, modificiraj, obriši, modificiraj DN) u tekstualnom obliku. Datoteke koje sadrže LDIF slogove mogu se koristiti za prijenos podataka između directory servera ili kao ulaz LDAP alatima poput **ldapadd** i **ldapmodify**.

“ldapsearch” na stranici 222
Pomoćni programi reda za naredbe LDAP pretraživanja.

Kopiranje korisnika iz validacijske liste HTTP poslužitelja u Directory Server.

Koristite ovu informaciju za kopiranje korisnika iz validacijske liste HTTP poslužitelja u Directory Server.

Ako trenutno koristite HTTP poslužitelj ili ste ga koristili u prošlosti, možda ste kreirali validacijske liste radi pohranjivanja Internet korisnika i njihovih lozinki. Kako se pomičete prema WebSphere Aplikacijskom poslužitelju, Portal poslužitelju i drugim aplikacijama koji podržavaju LDAP provjeru autentičnosti, možda ćete htjeti nastaviti koristiti te postojeće Internet korisnike i njihove lozinke. To može biti napravljeno koristeći ″Kopiranje Validacijske Liste u Direktorij″ API, QGLDCPYVL.

QGLDCPYVL čita unose iz validacijske liste i kreira odgovarajuće LDAP objekte u lokalnom directory server-u. Objekti su skeletni inetOrgPerson unosi s userPassword atributom koji sadrži kopiju informacije lozinke iz unosa validacijske liste. Vi možete odlučiti kako i kada je taj API pozvan. Možete ga koristiti kao jedna operacija za validacijsku listu koje se neće mijenjati ili kao raspoređeni posao ažuriranja poslužitelja direktorija radi prikaza novih unosa validacijske liste.

Na primjer:

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

Srodni koncepti

Lightweight Directory Access Protocol (LDAP) API-ji
Pogledajte Lightweight Directory Access Protocol (LDAP) API-je za više informacija o API-jima Directory Servera.

Srodni zadaci

"Scenarij: Kopiranje korisnika iz validacijske liste HTTP poslužitelja u Directory Server" na stranici 109
Primjer kako kopirati korisnike iz validacijske liste HTTP poslužitelja u Directory Server.

Upravljanje instancama

Možete imate višestruke directory server-e na svom i5/OS sistemu. Svaki poslužitelj poznat je kao instanca. Ako koristite directory server na prethodnom izdanju i5/OS, migrirat će u instancu s imenom QUSRDIR. Možete kreirati višestruke instance directory servera za servisiranje vaših aplikacija.

Jedinstvenost među instancama directory servera definira se po tome na koju je IP adresa i/ili port instanca konfigurirana da sluša. Također, svako izvođenje instance directory servera mora imati jedinstvenu bazu podataka, dnevnik promjene i datoteku konfiguracije. Moći ćete kreirati i konfigurirati instance poslužitelja sa sukobima, međutim, ako pokušate pokrenuti instancu poslužitelja koja se sukobljava s drugom aktivnom instancom poslužitelja, druga instanca se neće pokrenuti i izdat će se poruka greške.

Instanca directory servera sastoji se od svih datoteka koje su potrebne kako bi directory server radio na računalu.

Datoteke instance directory servera uključuju:

- ibmslapd.conf datoteka (konfiguracijska datoteka)
- Shematske datoteke
- Datoteke dnevnika
- Datoteke privremenog statusa

Datoteke za instancu directory servera pohranjuju se u direktorij pod imenom idsslapd-*instance_name*, gdje je *instance_name* ime instance directory servera. idsslapd-*instance_name* direktorij nalazi se u /QIBM/UserData/OS400/DirSrv direktoriju.

Svaka instanca directory servera, kod kreiranja, registrira novu aplikaciju u Upravitelj digitalnih certifikata (DCM). Nove instance directory servera imaju ime QIBM_DIRECTORY_SERVER_ <instance-name>. Morate koristiti DCM za pridruživanje digitalnog certifikata s instancom directory servera ako želite koristiti SSL. Kad se instanca svakog directory servera pokrene, registrira se kod System i Navigator kao poslužitelj tako da se može pratiti s System i Navigator.

Posao za instancu directory servera ima svoje ime posla postavljeno na ime instance. Pa, na primjer, QUSRDIR instanca ima potpuno kvalificirano ime posla xxxxxx/QDIRSRV/QUSRDIR. 'xxxxxx' je broj posla koji se određuje kad se posao pokreće. To je razlika za korisnike koji trenutno koriste directory server budući da je njegovo ime posla bilo xxxxxx/QDIRSRV/QDIRSRV.

Za upravljanje instancama, učinite sljedeće:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite **IBM Tivoli Directory Server** i izaberite **Upravljanje instancama**.

Ako povremeno spremate instance, morate spremiti <*instance-name*>CF knjižnicu zajedno s direktorijem baze podataka.

Zadaci administrativne grupe

Koristite ovu informaciju za upravljanje administrativnim grupama.

Administrativna grupa daje sposobnost omogućavanja administrativnih sposobnosti bez potrebe dijeljenja jednog ID-a i lozinke između administratora. Članovi administrativne grupe imaju svoj jedinstveni ID i lozinku. DN-ovi članova administrativne grupe ne smiju se podudarati i ne smiju odgovarati DN-u administratora IBM Poslužitelja direktorija. Također, DN administratora IBM Poslužitelja direktorija ne smije odgovarati DN-u bilo koga člana administrativne grupe.

Ovo pravilo se također primjenjuje na Kerberos ili Digest-MD5 ID-ove od administratora IBM Poslužitelja direktorija i članova administrativne grupe. Ti DN-ovi ne smiju odgovarati bilo kojem od DN-ova dobavljača replikacija IBM poslužitelja direktorija. To također znači da DN-ovi dobavljača replikacije IBM Poslužitelja direktorija ne smiju odgovarati bilo kojem od DN-ova članova administratorske grupe ili DN-u administratora Poslužitelja direktorija.

Bilješka: DN-ovi dobavljača replikacije IBM poslužitelja direktorija mogu se podudarati.

Srodni koncepti

"Administrativni pristup" na stranici 61
Koristite administrativni pristup za kontrolu pristupa specifičnim administrativnim zadacima.

Omogućavanje administrativne grupe

Koristite ovu informaciju za omogućavanje administrativne grupe.

Morate biti administrator IBM Poslužitelja direktorija da izvedete ovu operaciju.

1. Proširite kategoriju **Administracija poslužitelja** u navigacijskom području alata Web administracije i kliknite **Upravljanje administrativnom grupom**.

   Bilješka: Za promjenu postavki konfiguracije poslužitelja pomoću zadataka u kategoriji Administracija poslužitelja Web Administration tool-a, morate provjeriti autentičnost poslužitelju kao i5/OS korisnički profil koji ima *ALLOBJ i IOSYSCFG posebna ovlaštenja. To može biti napravljeno ovlašćivanjem kao projicirani korisnik s lozinkom za taj profil. Da bi se vezali kao projicirani korisnik iz Web administracijskog alata, unesite korisničko ime oblika os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, gdje su MYUSERNAME i MYSYSTEM.COM nizovi zamijenjeni s vašim imenom korisničkog profila i konfiguriranim projiciranim nastavkom sistema.
2. Da bi omogućili ili onemogućili administrativnu grupu, kliknite kontrolnu kućicu pokraj **Omogući administrativnu grupu**. Ako je kućica označena, administrativna grupa je omogućena.
3. Kliknite **OK**.

   Bilješka: Ako onemogućite administrativnu grupu, bilo koji član koji je prijavljen može nastaviti administrativne operacije dok se od korisnika ne zahtijeva ponovno spajanje.

Dodavanje, uređivanje i uklanjanje članova administrativne grupe

Koristite ovu informaciju za dodavanje, uređivanje ili uklanjanje članova administrativne grupe.

Preduvjeti Morate biti administrator IBM Poslužitelja direktorija da izvedete ovu operaciju.

1. Proširite kategoriju **Administracija poslužitelja** u navigacijskom području alata Web administracije i kliknite **Upravljanje administrativnom grupom**.

   Bilješka: Za promjenu postavki konfiguracije poslužitelja pomoću zadataka u kategoriji Administracija poslužitelja Web Administration tool-a, morate provjeriti autentičnost poslužitelju kao i5/OS korisnički profil koji ima *ALLOBJ i IOSYSCFG posebna ovlaštenja. To može biti napravljeno ovlašćivanjem kao projicirani korisnik s lozinkom za taj profil. Da bi se vezali kao projicirani korisnik iz Web administracijskog alata, unesite korisničko ime oblika os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, gdje su MYUSERNAME i MYSYSTEM.COM nizovi zamijenjeni s vašim imenom korisničkog profila i konfiguriranim projiciranim nastavkom sistema.
2. Na panelu **Upravljanje administrativnom grupom** kliknite **Dodavanje**.
3. Na panelu **Dodavanje člana administrativne grupe**:
   a. Unesite DN člana administratora (to mora biti valjana DN sintaksa).
   b. Unesite lozinku člana.
   c. Ponovno unesite lozinku člana da ju potvrdite.

d. Opcijsko: Upišite Kerberos ID člana. Kerberos ID mora biti u ibm-kn ili ibm-KerberosName obliku. Vrijednosti nisu osjetljive na veličinu slova, na primjer, ibm-kn=root@TEST.ROCHESTER.IBM.COM je jednako kao i ibm-kn=ROOT@TEST.ROCHESTER.IBM.COM.

4. Opcijsko: upišite **Digest-MD5 ime korisnika** člana.

   Bilješka: Digest-MD5 korisničko ime je osjetljivo na veličinu slova.

5. Kliknite **OK**.
6. Ponovite ovu proceduru za svakog člana kojeg želite dodati u administrativnu grupu.

DN člana administratora, Digest-MD5 korisničko ime, ako je navedeno i Kerberos ID, ako su navedeni, se prikazuju u kućici s popisom članova Administrativne grupe.

Da bi promijenili ili uklonili članove administrativne grupe, pratite iste procedure kao gore, ali koristite gumbe **Uredi** i **Obriši** na panelu **Upravljanje administrativnom grupom**.

Lozinka za člana administratorske grupe može se također promijeniti pomoću naredbe Promjena atribut Directory Servera (CHGDIRSVRA). Za promjenu lozinke za člana administrativne grupe s veznim DN cn=adminuser1 u novu lozinku, koristite ovu naredbu:

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

Zadaci grupe ograničavanja pretraživanja

Koristite ovu informaciju za upravljanje grupama ograničavanja pretraživanja.

Da bi spriječili da korisnički zahtjevi pretraživanja troše previše resursa i stalno utječu na izvođenje sistema, na te zahtjeve se postavljaju granice pretraživanja za bilo koji dani poslužitelj. Administrator postavlja ove granice pretraživanja na veličinu i trajanje pretraživanja kod konfiguriranja poslužitelja.

Samo su administratori i članovi administratorske grupe isključeni iz ovih granica pretraživanja, koje se primjenjuju na sve ostale korisnike. Međutim, ovisno o potrebama, administrator može kreirati grupe ograničavanja pretraživanja koje mogu imati fleksibilnije granice pretraživanja nego općeniti korisnik. Na taj način, administrator može dati posebne privilegije pretraživanja grupi korisnika.

Alat Web administracije je korišten za upravljanje grupama ograničavanja pretraživanja.

Srodne reference

"Parametri pretraživanja" na stranici 46
Da bi ograničili broj resursa korištenih od strane poslužitelja, administrator može postaviti parametre pretraživanja da ograniči korisničke mogućnosti pretraživanja. Mogućnosti pretraživanja se također mogu proširiti za posebne korisnika.

Kreiranje grupu ograničenja pretraživanja

Koristite ovu informaciju za kreiranje grupe ograničenja pretraživanja.

Da bi kreirali grupu ograničavanja pretraživanja, mora biti kreiran unos grupe koristeći alat Web administracije.

1. Proširite **Upravljanje direktorijem** kategoriju u navigacijskom području i kliknite **Dodavanje unosa** . Ili, kliknite **Upravljanje unosima** i izaberite lokaciju (cn=IBMpolicies ili cn=localhost), onda kliknite **Dodavanje**. Unosi pod cn=IBMpolicies će biti replicirani, a oni pod cn=localhost neće.
2. Izaberite jednu od klasa grupe objekta iz **Klasa strukturiranog objekta** izbornika.
3. Kliknite **Sljedeće**.
4. Izaberite **ibm-searchLimits** pomoćnu klasu objekta iz **Dostupno** izbornika i kliknite **Dodavanje**. Ponovite ovaj proces za svaku dodatnu pomoćnu klasu objekta koja treba biti dodana. Pomoćna klasa objekta iz izbornika **Izabrano** se može ukloniti izborom i klikom na **Ukloni**.
5. Kliknite **Sljedeće**.

6. U polju **Relativni DN**, unesite relativno razlikovno ime (RDN) grupe koja se dodaje. Na primjer, cn=Search Group1.
7. U polju **Nadređeni DN**, unesite razlikovno ime unosa stabla koje je izabrano. Na primjer, cn=localhost. Možete i kliknuti na **Pregled** kako bi izabrali Nadređeno DN iz popisa. Napravite izbor i kliknite **Biranje** da navedete Nadređeni DN. **Nadređeno DN** se postavlja na unos koji je izabran u stablu.

   Bilješka: Ako ste započeli ovaj zadatak iz **Upravljanje unosima** panela, ovo je polje uneseno za vas. **Nadređeni DN** je izabran prije klika na **Dodavanje** radi pokretanja procesa dodavanja unosa.
8. Na kartici **Potrebni atributi**, unesite vrijednosti za potrebne atribute.
   - **cn** je relativni DN koji ste naveli ranije.
   - U polju **ibm-searchSizeLimit** navedite broj unosa s kojim treba ograničiti veličinu pretraživanja. Taj broj može biti u rasponu između 0 i 2,147,483,647. Postavka od 0 je ista kao i **Neograničeno**.
   - U polju **ibm-searchTimeLimit**, navedite broj sekundi s kojim ograničiti trajanje pretraživanja. Taj broj može biti u rasponu između 0 i 2,147,483,647. Postavka od 0 je ista kao i **Neograničeno**.
   - Ovisno o klasi objekta koju izaberete, možda ćete vidjeti **Member** ili **uniqueMember** polje. Ovo su članovi grupe koju kreirate. Unos je u obliku DN, na primjer, cn=Bob Garcia,ou=austin,o=ibm,c=us.
9. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu. Kliknite **OK** kada ste završili dodavanje višestrukih vrijednosti. Vrijednosti su dodane na proširivi izbornik prikazan na atributu.
10. Ako vaš poslužitelj ima omogućene oznake jezika, kliknite **Vrijednost oznake jezika** da bi dodali ili uklonili opise oznaka jezika.
11. Kliknite **Drugi atributi**.
12. Na **Drugi atributi** kartici, unesite vrijednosti kao što je prikladno za atribute. Za više informacija pogledajte “Promjena binarnih atributa” na stranici 189.
13. Kliknite **Završetak** da kreirate unos.

Promjena grupe ograničenja pretraživanja

Koristite ovu informaciju za promjenu grupe ograničenja pretraživanja.

Možete promijeniti veličinu ili vremensko ograničenje atribute od grupe ograničavanja pretraživanja. Možete također dodati i obrisati članove grupe. Upotrijebite alat Web administracije da promijenite grupu ograničavanja pretraživanja.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos na kojem želite raditi. Kliknite na **Uredi atribute** iz desne trake s alatima.
2. Na kartici **Potrebni atributi** unesite vrijednosti za potrebne atribute. Pogledajte “Promjena binarnih atributa” na stranici 189 za informacije o dodavanju binarnih vrijednosti. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
3. Kliknite na **Neobvezni atributi**.
4. Na karticu **Neobvezni atributi** unesite vrijednosti kako je to prikladno za neobvezne atribute. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
5. Kliknite **Memberships**.
6. Ako ste kreirali bilo koje grupe na kartici **Članstvo**:
   - Izaberite grupu iz **Dostupne grupe** i kliknite na **Dodavanje** da napravite unos članom izabranog **Članstva statičke grupe**.
   - Izaberite grupu iz **Članstva statičke grupe** i kliknite na **Ukloni** kako bi uklonili unos iz izabrane grupe.
7. Ako je unos grupni unos, dostupna je kartica **Članovi**. Kartica **Članovi** prikazuje članove izabrane grupe. Možete dodati ili ukloniti članove iz grupe.
   - Kako bi dodali člana grupi:
     a. Kliknite na karticu **Višestruke vrijednosti** uz karticu **Članovi** ili na kartici **Članovi** kliknite na **Članovi**.

b. U polje Član unesite DN unosa kojeg želite dodati.
c. Kliknite **Dodavanje**.
d. Kliknite **OK**.

- Da uklonite član iz grupe:
  a. Kliknite na **Višestruke vrijednosti** uz karticu **Članovi** ili kliknite na karticu **Članovi** i kliknite na **Članovi**.
  b. Izaberite unos koji želite ukloniti.
  c. Kliknite **Ukloni**.
  d. Kliknite **OK**.
- Da osvježite listu članova, kliknite na **Ažuriraj**.

8. Kliknite **OK** za promjenu unosa.

Kopiranje grupe ograničenja pretraživanja

Koristite ovu informaciju za kopiranje grupe ograničenja pretraživanja.

Korisno je kopirati grupu ograničenja pretraživanja ako želite imati istu grupu ograničenja pretraživanja pod localhost i IBMpolicies. Također je korisno ako želite kreirati novu grupu koja ima slične informacije u postojeću grupu, ali s manjim razlikama.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos, kao što je John Doe, na kojem želite raditi. Kliknite na **Kopiranje** iz desne trake s alatima.
2. Promijenite RDN unos u DN polje. Na primjer, promijenite cn=John Doe u cn=Jim Smith.
3. Na potrebnoj kartici s atributima promijenite unos na novi RDN. U ovom primjeru Jim Smith.
4. Promijenite druge potrebne atribute na odgovarajući način. U ovom primjeru promijenite sn iz Doe u Smith.
5. Kada ste dovršili potrebne promjene, kliknite na **OK** kako bi kreirali novi unos. Novi unos Jim Smith se dodajte na dno liste unosa.

Uklanjanje grupe ograničenja pretraživanja

Koristite ovu informaciju za uklanjanje grupe ograničenja pretraživanja.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla, sufiks ili unos na kojem želite raditi. Kliknite na **Obriši** iz desne trake s alatima.
2. Od vas se traži da potvrdite brisanje. Kliknite **OK**. Unos je obrisan iz direktorija i vraćeni ste na listu unosa.

Zadaci proxy autorizacijske grupe

Koristite ovu informaciju za upravljanje proxy autorizacijskim grupama.

Članovi proxy autorizacijske grupe mogu pristupati Poslužitelju direktorija i izvoditi mnoge zadatke u ime više korisnika bez potrebe ponovnog vezivanja za svakog korisnika. Članovi proxy autorizacijske grupe mogu preuzeti bilo koji ovlašteni identitet osim administratora ili članova administratorske grupe.

Alat Web administracije je korišten za upravljanje proxy autorizacijom.

Srodni koncepti

"Proxy autorizacija" na stranici 62
Proxy autorizacija je poseban oblik provjere autentičnosti. Korištenjem ovog mehanizma proxy autorizacije, aplikacija klijenta se može vezati na direktorij s vlastitim identitetom, ali joj je dozvoljeno izvođenje operacija u ime drugog korisnika za pristup ciljnom direktoriju. Skup pouzdanih aplikacija ili korisnika može pristupati Poslužitelju direktorija u ime višestrukih korisnika.

Kreiranje proxy autorizacijske grupe

Koristite ovu informaciju za kreiranje proxy autorizacijske grupe.

1. Proširite **Upravljanje direktorijem** kategoriju u navigacijskom području i kliknite **Dodavanje unosa**. Ili, kliknite **Upravljanje unosima** i izaberite mjesto (cn=ibmPolicies ili cn=localhost) i onda kliknite **Dodavanje**.
2. Izaberite **groupof Names** klase objekata iz izbornika **Strukturalne klase nit Opasnosti**.
3. Kliknite **Sljedeće**.
4. Izaberite **ibm-proxyGroup** pomoćna klasa objekta iz **Dostupni** izbornika i kliknite **Dodavanje**. Ponovite ovaj proces za svaki dodatni pomoćni objekt klase koji želite dodati.
5. Kliknite **Sljedeće**.
6. U **Relativni DN** polju, upišite cn=proxyGroup.
7. U polje **Nadređeni DN** unesite razlikovno ime unosa stabla koji birate, na primjer, cn=localhost. Također možete kliknuti **Pretraživanje** da izaberete **Nadređeni DN** iz liste. Napravite izbor i kliknite **Biranje** za specificiranje nadređenog DN-a koji želite. Default za Nadređeni DN je unos izabran u stablu.

   Bilješka: Ako ste pokrenuli ovaj zadatak iz panela Upravljanje unosima, ovo polje je već ispunjeno za vas. Izabrali ste Nadređeni DN prije klika na Dodavanje da pokrenete proces dodavanja unosa.
8. Na kartici **Potrebni atributi** upišite vrijednosti za potrebne atribute.
   - **cn** je proxyGroup.
   - **Član** je u obliku DN-a, na primjer, cn=Bob Garcia,ou=austin,o=ibm,c=us.

   Pogledajte “Promjena binarnih atributa” na stranici 189 radi više informacija o dodavanju binarnih vrijednosti.
9. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.

   Bilješka: Nemojte kreirati višestruke vrijednosti za vrijednost cn. Proxy autorizacijska grupa mora imati poznato ime, proxyGroup.

   Kliknite **OK** kada ste završili dodavanje višestrukih vrijednosti. Vrijednosti su dodane na proširivi izbornik prikazan na atributu.
10. Ako vaš poslužitelj ima omogućene oznake jezika, kliknite **Vrijednost oznake jezika** da bi dodali ili uklonili opise oznaka jezika.
11. Kliknite **Drugi atributi**.
12. Na **Drugi atributi** kartici, unesite vrijednosti kao što je prikladno za atribute. Pogledajte “Promjena binarnih atributa” na stranici 189 radi više informacija o dodavanju binarnih vrijednosti.
13. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu. Kliknite **OK** kada ste završili dodavanje višestrukih vrijednosti. Vrijednosti su dodane na proširivi izbornik prikazan na atributu.
14. Ako vaš poslužitelj ima omogućene oznake jezika, kliknite **Vrijednost oznake jezika** da bi dodali ili uklonili opise oznaka jezika.
15. Kliknite **Završetak** da kreirate unos.

Promjena proxy autorizacijske grupe

Koristite ovu informaciju za promjenu proxy autorizacijske grupe.

Možete promijeniti proxy autorizacijsku grupu, kao što je dodavanje ili brisanje članova grupe, koristeći alat Web administracije.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos na kojem želite raditi. Kliknite na **Uredi atribute** iz desne trake s alatima.
2. Na kartici **Potrebni atributi** unesite vrijednosti za potrebne atribute. Pogledajte “Promjena binarnih atributa” na stranici 189 za informacije o dodavanju binarnih vrijednosti. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
3. Kliknite na **Neobvezni atributi**.

4. Na karticu **Neobvezni atributi** unesite vrijednosti kako je to prikladno za neobvezne atribute. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
5. Kliknite **Memberships**.
6. Ako ste kreirali bilo koje grupe na kartici **Članstvo**:
   - Izaberite grupu iz **Dostupne grupe** i kliknite na **Dodavanje** da napravite unos članom izabranog **Članstva statičke grupe**.
   - Izaberite grupu iz **Članstva statičke grupe** i kliknite na **Ukloni** kako bi uklonili unos iz izabrane grupe.
7. Ako je unos grupni unos, dostupna je kartica **Članovi**. Kartica **Članovi** prikazuje članove izabrane grupe. Možete dodati ili ukloniti članove iz grupe.
   - Kako bi dodali člana grupi:
     a. Kliknite na karticu **Višestruke vrijednosti** uz karticu **Članovi** ili na kartici **Članovi** kliknite na **Članovi**.
     b. U polje Član unesite DN unosa kojeg želite dodati.
     c. Kliknite **Dodavanje**.
     d. Kliknite **OK**.
   - Da uklonite član iz grupe:
     a. Kliknite na **Višestruke vrijednosti** uz karticu **Članovi** ili kliknite na karticu **Članovi** i kliknite na **Članovi**.
     b. Izaberite unos koji želite ukloniti.
     c. Kliknite **Ukloni**.
     d. Kliknite **OK**.
   - Da osvježite listu članova, kliknite na **Ažuriraj**.
8. Kliknite **OK** za promjenu unosa.

Kopiranje proxy autorizacijske grupe

Koristite ovu informaciju za kopiranje proxy autorizacijske grupe.

Korisno je kopirati proxy autorizacijsku grupu ako želite imati istu proxy autorizacijsku grupu pod localhost i IBMpolicies.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos, kao što je John Doe, na kojem želite raditi. Kliknite na **Kopiranje** iz desne trake s alatima.
2. Promijenite RDN unos u DN polje. Na primjer, promijenite cn=John Doe u cn=Jim Smith.
3. Na potrebnoj kartici s atributima promijenite unos na novi RDN. U ovom primjeru Jim Smith.
4. Promijenite druge potrebne atribute na odgovarajući način. U ovom primjeru promijenite sn iz Doe u Smith.
5. Kada ste dovršili potrebne promjene, kliknite na **OK** kako bi kreirali novi unos. Novi unos Jim Smith se dodajte na dno liste unosa.

Uklanjanje proxy autorizacijske grupe

Koristite ovu informaciju za uklanjanje proxy autorizacijske grupe.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla, sufiks ili unos na kojem želite raditi. Kliknite na **Obriši** iz desne trake s alatima.
2. Od vas se traži da potvrdite brisanje. Kliknite **OK**. Unos je obrisan iz direktorija i vraćeni ste na listu unosa.

Zadaci jedinstvenog atributa

Koristite ovu informaciju za upravljanje jedinstvenim atributima.

Upravljanje jedinstvenim atributima je postignuto preko **Administracija poslužitelja** kategorije od alata Web administracije.

Bilješka: Po atributnoj bazi, oznake jezika su međusobno isključive s jedinstvenim atributima. Ako ste odredili određeni atribut da bude jedinstveni atribut, on ne može imati oznake jezika povezane sa sobom.

Bilješka: Za promjenu postavki konfiguracije poslužitelja pomoću zadataka u kategoriji Administracija poslužitelja Web Administration tool-a, morate provjeriti autentičnost poslužitelju kao i5/OS korisnički profil koji ima *ALLOBJ i IOSYSCFG posebna ovlaštenja. To može biti napravljeno ovlašćivanjem kao projicirani korisnik s lozinkom za taj profil. Da bi se vezali kao projicirani korisnik iz Web administracijskog alata, unesite korisničko ime oblika os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, gdje su MYUSERNAME i MYSYSTEM.COM nizovi zamijenjeni s vašim imenom korisničkog profila i konfiguriranim projiciranim nastavkom sistema.

Srodni koncepti

"Jednoznačni atributi" na stranici 87
Funkcija jedinstvenih atributa osigurava da navedeni atributi uvijek imaju jedinstvene vrijednosti unutar direktorija.

Srodni zadaci

"Kreiranje jedinstvene liste atributa"
Koristite ovu informaciju za kreiranje jedinstvene liste atributa.

"Uklanjanje unosa iz jedinstvene liste atributa" na stranici 135
Koristite ovu informaciju za uklanjanje unosa iz jedinstvene liste atributa

Određivanje može li se atribut specificirati kao jedinstven

Koristite ovu informaciju za određivanje može li se atribut specificirati kao jedinstven.

Ne mogu svi atributi biti specificirani kao jedinstveni. Pogledajte sljedeće za listu uvjeta kad se atribut ne može označiti kao jedinstven:

- Binarni atributi, operacijski atributi, konfiguracijski atributi i objectclass atributi ne mogu biti dizajnirani kao jedinstveni.
- Atributi s postojećim vrijednostima sukoba ne mogu postati jedinstveni.
- Po atributnoj bazi, oznake jezika su međusobno isključive s jedinstvenim atributima. Ako označite određeni atribut kao jedinstven atribut, ne može imati oznake jezika koje su mu pridružene.

Zadatak Upravljanje jedinstvenim atributima Web administration tool-a Manage pokazuje jedino one atribute koji zadovoljavaju prvi uvjet. Možete dohvatiti istu listu atributa izvođenjem naredbe ldapexop nakon vezivanja kao administrator. Za dohvaćanje liste atributa koji mogu biti jedinstveni, specificirajte sljedeće:

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

Za dohvaćanje liste atributa koji ne mogu biti jedinstveni, specificirajte sljedeće:

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

Neki atributi ispisani kao dozvoljeni za jedinstvene atribute mogu imati vrijednosti sukoba i stoga ne mogu postati jedinstveni. Za određivanje može li određeni atribut biti specificiran kao jedinstven, upotrijebite naredbu ldapexop. Na primjer, naredba:

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

pokazuje može li atribut uid postati jedinstven. Također ispisuje vrijednosti sukoba, ako postoje, za taj atribut.

Ako naredba ldapexop pokazuje da postoje vrijednosti sukoba, naredba ldapsearch može se koristiti za pronalaženje unosa koji imaju tu vrijednost. Na primjer, sljedeća naredba ispisuje sve unose koji imaju uid=jsmith:

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

Kreiranje jedinstvene liste atributa

Koristite ovu informaciju za kreiranje jedinstvene liste atributa.

1. Proširite kategoriju **Administracija poslužitelja** u području navigacije. Kliknite **Upravljanje jedinstvenim atributima** .

2. Izaberite atribut koji želite dodati kao jedinstveni atribut na izborniku **Dostupni atributi**. Ispisani dostupni atributi su oni koji mogu biti određeni kao jedinstveni; na primjer, sn.
3. Kliknite na **Dodavanje u cn=localhost** ili **Dodavanje u cn=IBMpolicies**. Razlika između ova dva spremnika je da su cn=IBMpolicies unosi replicirani, a cn=localhost nisu. Atribut je prikazan u odgovarajućoj kućici s popisom. Možete ispisati isti atribut u oba spremnika.

   Bilješka: Ako je unos kreiran pod cn=localhost i cn=IBMpolicies, rezultirajuća unija tih dva unosa je jedinstvena lista atributa. Na primjer, ako su atributi cn i employeeNumber označeni kao jedinstveni u cn=localhost i atributi cn i telephoneNumber su označeni kao jedinstveni u cn=IBMploicies, poslužitelj tretira atribute cn, employeeNumber i telephoneNumber kao jedinstvene atribute.
4. Ponovite ovaj proces za svaki atribut koji želite dodati kao jedinstveni atribut.
5. Kliknite **OK** za spremanje promjena.

Kod dodavanja ili izmjene unosa jedinstvenog atributa, ako postavljanje jedinstvenog ograničenja za bilo koji od ispisanih tipova jedinstvenih atributa rezultira u greškama, unos nije dodan ili kreiran u direktoriju. Problem mora biti riješen i naredba dodavanja ili izmjene mora biti ponovno izdana prije nego što unos može biti kreiran ili izmijenjen. Na primjer, prilikom dodavanja jedinstvenog unosa atributa u direktorij, ako postavljanje jedinstvenog ograničenja na tablici za jedan od ispisanih tipova atributa nije uspjelo (odnosno, zbog duplih vrijednosti u bazi podataka), jedinstveni unos atributa nije dodan u direktorij. Izdana je greška.

Kada aplikacija pokušava dodati unos u direktorij s vrijednosti za atribut koja duplicira postojeći unos direktorija, greška s rezultirajućim kodom20 (LDAP: kod greške 20 - Atribut ili vrijednost postoji) je izdana iz LDAP poslužitelja.

Kada se poslužitelj pokrene, provjerava listu jedinstvenih atributa i određuje da liDB2 ograničenja postoje za svaki od njih. Ako ograničenje ne postoji za atribut zato što je uklonjeno od strane bulkload uslužnog programa ili zato što je uklonjeno ručno od strane korisnika, uklonjeno je s liste jedinstvenih atributa i poruka greške je zabilježene u dnevniku grešaka, ibmslapd.log. Na primjer, ako je atribut cn određen kao jedinstveni u cn=uniqueattributes,cn=localhost i ne postoji DB2 ograničenje za njega sljedeća poruka je zapisana:

```
Vrijednosti za atribut CN nisu jedinstvene.
Atribut CN je uklonjen iz jedinstveni atributi
unosa: CN=UNIQUEATTRIBUTES,CN=LOCALHOST
```

Srodni koncepti

"Zadaci jedinstvenog atributa" na stranici 133
Koristite ovu informaciju za upravljanje jedinstvenim atributima.

Uklanjanje unosa iz jedinstvene liste atributa

Koristite ovu informaciju za uklanjanje unosa iz jedinstvene liste atributa

Ako jedinstveni atribut postoji u cn=uniqueattribute,cn=localhost i cn=uniqueattribute,cn=IBMpolicies i uklonjen je iz samo jednog unosa, poslužitelj nastavlja tretirati taj atribut kao jedinstveni atribut. Atribut postaje nejedinstven kada je uklonjen iz oba unosa.

1. Proširite kategoriju **Administracija poslužitelja** u navigacijskom području i kliknite **Upravljanje jedinstvenim atributima**.
2. Izaberite atribut koji želite ukloniti iz liste jedinstvenih atributa klikom na atribut u odgovarajućoj kućici s popisom.
3. Kliknite **Ukloni**.
4. Ponovite ovaj proces za svaki atribut koji želite ukloniti s liste.
5. Kliknite **OK** za spremanje promjena.

Bilješka: Ako uklonite zadnji jedinstveni atribut iz cn=localhost ili cn=IBMpolicies kućica s popisom, unos spremnika za tu kućicu s popisom, cn=uniqueattribute,cn=localhost ili cn=uniqueattribute,cn=IBMpolicies, se automatski briše.

Srodni koncepti

"Zadaci jedinstvenog atributa" na stranici 133
Koristite ovu informaciju za upravljanje jedinstvenim atributima.

Zadaci izvedbe

Koristite ovu informaciju za prilagodbu postavki izvedbe.

Postavke izvedbe vašeg Poslužitelja direktorija možete podesiti mijenjanjem bilo čega od sljedećeg:

- ACL veličine predmemorije, veličine predmemorije unosa, maksimalnog broja unosa koji se spremaju u predmemoriju filtera i najvećeg pretraživanja koje će se staviti u predmemoriju klijenta.
- Broja veza baza podataka i niti poslužitelja
- Postavke predmemorije atributa
- Postavke transakcija poslužitelja

Srodni koncepti

"Predmemorije poslužitelja" na stranici 89
LDAP predmemorije su brzi međuspremnici za pohranu u memoriji korišteni za pohranjivanje LDAP informacija kao što su upiti, odgovori i korisnička autorizacija za buduće korištenje. Podešavanje LDAP predmemorija je vrlo bitno za poboljšanje performansi.

Postavljanje povezivanja baze podataka i postavki predmemorije

Koristite ovu informaciju za postavljanje povezivanja baze podataka i postavki predmemorije.

Da bi postavili veze baze podataka i postavke predmemorije, učinite sljedeće:

1. Proširite kategoriju **Upravljanje svojstvima poslužitelja** u navigacijskom području alata Web administracije i onda kliknite na karticu **Izvedba** u desnom oknu.
2. Navedite **Broj veza baze podataka**. To postavlja broj DB2 veza korištenih od strane poslužitelja. Minimalni broj koji morate navesti je 4. Default postavka je 15. Ako vaš LDAP poslužitelj prima veliku količinu zahtjeva klijenta ili klijenti primaju ″veza odbijena″ greške, možda ćete vidjeti bolje rezultate povećavanjem postavke broja veza napravljenih prema DB2 od strane poslužitelja. Maksimalni broj veza je određen postavkom na vašoj DB2 bazi podataka. Iako ne postoje ograničenja poslužitelja u broju veza koje navedete, svaka veza troši resurse.
3. Navedite **Broj veza baze podataka za replikaciju**. To postavlja broj DB2 veza korištenih od strane poslužitelja za replikaciju. Minimalni broj koji morate navesti je 1. Default postavka je 4.

   Bilješka: Ukupan broj veza navedenih za veze baze podataka, uključujući veze baze podataka za replikaciju, ne može premašiti broj veza postavljenih u vašoj DB2 bazi podataka.
4. Izaberite **Stavljanje ACL informacija u predmemoriju** da koristite sljedeće ACL postavke predmemorije.
5. Navedite **Maksimalni broj elemenata u ACL predmemoriji**. Default je 25 000.
6. Navedite **Maksimalni broj elemenata u predmemoriji unosa**. Default je 25 000.
7. Navedite **Maksimalni broj elemenata u predmemoriji filtera pretraživanja**. Default je 25 000.Predmemorija filtera pretraživanja se sadrži od stvarnih upita na zahtijevanim filterima atributa i rezultirajućim identifikatorima unosa koji odgovaraju. Na operaciji ažuriranja, svi unosi predmemorije filtera su poništeni.
8. Navedite **Maksimalni broj elemenata iz pojedinačnog pretraživanja dodanog u predmemoriju filtera pretraživanja**. Ako izaberete **Elemente**, morate unijeti broj. Default je 100. Inače, izaberite **Neograničeno**. Unosi pretraživanja koji odgovaraju na više od broja ovdje navedenog nisu dodani u predmemoriju filtera pretraživanja.
9. Kada završite, kliknite na **OK**.
10. Ako postavljate broj veza baze podataka, ponovno pokrenite poslužitelj da bi promjene imale utjecaj. Ako ste izmjenjivali samo postavke predmemorije, poslužitelj ne treba biti ponovno pokrenut.

Konfiguriranje predmemorije atributa

Koristite ovu informaciju za postavljanje predmemorije atributa.

Postavke za predmemoriju atributa konfigurirane su i u Web administration tool i System i Navigator.

Za ručno postavljanje predmemorije atributa u Web administration tool, slijedite ove korake:

1. Proširite kategoriju **Administracija poslužitelja** u području navigacije alata Web administracije i onda izaberite karticu **Predmemorija atributa** na desnom oknu.

   Bilješka: Za promjenu postavki konfiguracije poslužitelja pomoću zadataka u kategoriji Administracija poslužitelja Web Administration tool-a, morate provjeriti autentičnost poslužitelju kao i5/OS korisnički profil koji ima *ALLOBJ i IOSYSCFG posebna ovlaštenja. To može biti napravljeno ovlašćivanjem kao projicirani korisnik s lozinkom za taj profil. Da bi se vezali kao projicirani korisnik iz Web administracijskog alata, unesite korisničko ime oblika os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, gdje su MYUSERNAME i MYSYSTEM.COM nizovi zamijenjeni s vašim imenom korisničkog profila i konfiguriranim projiciranim nastavkom sistema.
2. Promijenite količinu dostupne memorije u kilobajtima za predmemoriju direktorija. Default je 16 384 kilobajta (16 MB).
3. Promijenite količinu dostupne memorije u kilobajtima za predmemoriju dnevnika promjena. Default je 16 384 kilobajta (16 MB).

   Bilješka: Ovaj izbor je onemogućen ako dnevnik promjena nije konfiguriran. Predmemorija atributa za dnevnik promjena treba biti postavljena na 0 i atributi ne bi trebali biti konfigurirani osim ako ne radite česta pretraživanja unutar dnevnika promjena i izvedba tih pretraživanja je kritična.
4. Izaberite atribut koji želite staviti u predmemoriju na izborniku **Dostupni atributi**. Samo atributi koji mogu biti stavljeni u predmemoriju su prikazani u ovom izborniku; na primjer, sn.

   Bilješka: Atribut ostaje u listi dostupnih atributa dok se ne smjesti u cn=directory i cn=changelog spremnike.
5. Kliknite na **Dodavanje u cn=directory** ili **Dodavanje u cn=changelog**. Atribut je prikazan u odgovarajućoj kućici s popisom. Možete ispisati isti atribut u oba spremnika.

   Bilješka: **Dodavanje u cn=changelog** je onemogućeno ako dnevnik promjena nije konfiguriran. Predmemorija atributa za dnevnik promjena treba biti postavljena na 0 i atributi ne bi trebali biti konfigurirani osim ako ne radite česta pretraživanja unutar dnevnika promjena i izvedba tih pretraživanja je kritična.
6. Ponovite ovaj proces za svaki atribut koji želite dodati u predmemoriju atributa.
7. Kada završite, kliknite na **OK**.

Za omogućavanje automatske predmemorije atributa u System i Navigator, poduzmite sljedeće korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM poslužitelj direktorija** i izaberite **Svojstva**.
5. Kliknite karticu **Izvedba**.
6. Izaberite **Omogući automatsko stavljanje atributa u predmemoriju** za **Bazu podataka** ili **Dnevnik promjena** ili oboje. Automatsko stavljanje atributa u predmemoriju za dnevnik promjena ne bi trebalo biti omogućeno osim ako ne radite česta pretraživanja unutar dnevnika promjena i izvedba tih pretraživanja je kritična.
7. Navedite **Vrijeme početka** (u lokalnom vremenu poslužitelja) i **Interval** za svaki tip stavljanja u predmemoriju koji odlučite omogućiti. Na primjer, ako omogućite stavljanje u predmemoriju baze podataka i postavite vrijeme početka na 6.00, a interval na šest sati, predmemorija će biti automatski prilagođena u 6, podne, 18 i ponoć bez obzira na to kada je poslužitelj pokrenut ili kada je auto prilagođavanje bilo konfigurirano.

Bilješka: Automatsko stavljanje atributa u predmemoriju će staviti toliko atributa u predmemoriju koliko omogućava maksimalna količina memorije za predmemoriju navedena u alatu Web administracije kao što je opisano iznad.

Tablica 4. Interakcija postavki predmemorije atributa

Aktivnost	Što se događa
Pokretanje poslužitelja	Ako je automatsko stavljanje atributa u predmemoriju trenutno omogućeno i bilo je omogućeno kod zadnjeg zaustavljanja poslužitelja, isti atributi koji su stavljeni u predmemoriju kada je poslužitelj zaustavljen bit će kreirani kada se poslužitelj ponovno pokrene. Ako je dodatna memorija još uvijek dostupna za predmemoriju atributa, atributi koji su ručno konfigurirani će također biti stavljeni u predmemoriju. Ako je automatsko stavljanje atributa u predmemoriju trenutno omogućeno i nije bilo omogućeno kod zadnjeg zaustavljanja poslužitelja, atributi koji su ručno konfigurirani za predmemoriju će biti stavljeni u predmemoriju. U svakom slučaju, poslužitelj će onda automatski prilagoditi predmemoriju atributa bazirano na navedenom vremenu početka i vremenskom intervalu. Ako automatsko stavljanje u predmemoriju nije omogućeno, ručno podešene postavke predmemorije će imati učinak.
Omogućite automatsko stavljanje atributa u predmemoriju nakon pokretanja poslužitelja	Automatsko stavljanje atributa u predmemoriju će se dogoditi kako je opisano za pokretanje poslužitelja. Bilo koje automatsko konfigurirano stavljanje atributa u predmemoriju koje ne odgovara količini memorije konfigurirane za predmemoriju atributa neće biti obrisano.
Onemogućite automatsko stavljanje atributa u predmemoriju nakon pokretanja poslužitelja	Samo atributi koji su ručno konfigurirani bit će stavljeni u predmemoriju.
Izmijenite atribute ručno stavljene u predmemoriju dok je automatsko stavljane u predmemoriju omogućeno nakon pokretanja poslužitelja	Ništa se neće dogoditi. Ručna konfiguracija će imati utjecaj kada je automatsko stavljanje u predmemoriju onemogućeno.
Promijenite količinu dostupne memorije za predmemoriju nakon pokretanja poslužitelja	Ako je automatsko stavljanje atributa u predmemoriju omogućeno, poslužitelj će odmah ponovno staviti atribute u predmemoriju na novu veličinu. Ako je automatsko stavljanje u predmemoriju onemogućeno, poslužitelj će staviti u predmemoriju ručno konfigurirane atribute do nove veličine.
Promijenite vrijeme početka nakon pokretanja poslužitelja	Ako je automatsko stavljanje u predmemoriju omogućeno, nove postavke će imati utjecaj u vrijeme početka ili zadanog intervala. Ako je automatsko stavljanje u predmemoriju onemogućeno, postavke se pohranjuju i imat će utjecaj kad se automatsko stavljanje u predmemoriju omogući.

Konfiguriranje postavki transakcije

Koristite ovu informaciju za postavljanje postavki transakcije.

Da bi postavili postavke transakcije, napravite sljedeće:

1. Proširite **Upravljanje svojstvima poslužitelja** u navigacijskom području alata Web administracije i onda izaberite **Transakcije** u desnom oknu.
2. Izaberite **Omogući procesiranje transakcija** da omogućite procesiranje transakcija. Ako je **Omogući procesiranje transakcija** onemogućeno, sve druge opcije na ovom panelu se zanemaruju od strane poslužitelja.
3. Postavite **Maksimalni broj transakcija**. Kliknite na radio gumb **Transakcije** ili **Neograničeno**. Ako izaberete **Transakcije**, navedite maksimalni broj transakcija. Maksimum broja transakcija je 2 147 483 647. Default postavka je 20 transakcija.
4. Postavite **Maksimalni broj operacija po transakciji**. Kliknite na radio gumb **Operacije** ili **Neograničeno**. Ako izaberete **Operacije**, trebate navesti u polju maksimalni broj operacija dozvoljenih za svaku transakciju. Maksimum broja operacija je 2 147 483 647. Što je broj manji, bolje su performanse. Default je 5 operacija.
5. Postavite **Vremensko ograničenje čekanja**. Ovaj izbor postavlja minimalnu vrijednost timeouta za čekajuće transakcije u sekundama. Kliknite na radio gumb **Sekunde** ili **Neograničeno**. Ako izaberete **Sekunde**, navedite maksimalni broj sekunda dozvoljenih za svaku transakciju. Maksimum broja sekundi je 2 147 483 647. Transakcije koje su nedovršene nakon tog vremena se opozivaju (vraćaju natrag). Default je 300 sekunda.
6. Kada završite, kliknite na **OK**.

7. Ako ste omogućili podršku transakcija, ponovno pokrenite poslužitelj, da bi promjene imale učinka. Ako ste mijenjali samo postavke, poslužitelj se ne treba ponovno pokretati.

Zadaci replikacije

Koristite ovu informaciju za upravljanje replikacijom.

Da bi upravljali replikacijom, proširite kategoriju **Upravljanje replikacijom** Web administracijskog alata.

Srodni koncepti

"Replikacija" na stranici 37
Replikacija je tehnika koju koriste poslužitelji direktorija kako bi se poboljšala izvedba i pouzdanost. Proces replikacije zadržava usklađenima podatke u više direktorija.

Kreiranje topologije glavne-replike

Koristite ovu informaciju za kreiranje topologije glavne-replike.

Da definirate osnovnu topologiju glavne-replike, morate:

1. Kreirati glavni direktorij i definirati njegov sadržaj. Izaberite podstablo koje želite replicirati i specificirajte poslužitelja kao glavnog. Pogledajte "Kreiranje glavnog poslužitelja (replicirano podstablo)" na stranici 140.
2. Kreirati vjerodajnice koje će koristiti dobavljač. Pogledajte "Kreiranje vjerodajnica replikacije" na stranici 141.
3. Kreirati replika poslužitelja. Pogledajte "Kreiranje poslužitelja replike" na stranici 143.
4. Eksportirati topologiju iz glavnog poslužitelja na repliku. Pogledajte "Kopiranje podataka na repliku" na stranici 144.
5. Promijenite konfiguraciju replike kako bi identificirali tko je ovlašten da replicira promjene i doda referal na glavnog poslužitelja. Pogledajte "Dodavanje informacija o dobavljaču na novu repliku" na stranici 145.

Bilješka:

Ako unos na korijenu podstabla za koje želite da bude replicirano nije sufiks u poslužitelju, prije nego možete koristiti funkciju **Dodavanje podstabla**, morate osigurati da su ACL-ovi definirani kako slijedi:

Za nefiltrirane ACL-ove:

```
ownersource: <kao i DN unosa>
ownerpropagate: TRUE

aclsource: <kao i DN unosa>
aclpropagate: TRUE
```

Za filtrirane ACL-ove:

```
ibm-filteraclinherit: FALSE
```

Kako bi zadovoljili ACL zahtjeve, ako unos nije sufiks u poslužitelju, uredite ACL za taj unos u panelu **Upravljanje unosima**. Izaberite unos i kliknite na **Uredi ACL**. Ako želite dodati nefiltrirane ACL-ove, izaberite tu karticu i izaberite kontrolnu kućicu kako bi specificirali da li su ili nisu ACL-ovi izričiti za ACL-ove i vlasnike. Provjerite da li su označeni **Proširivanje ACL-ova** i **Proširivanje vlasnika**. Ako želite dodati Filtrirane ACL-ove izaberite tu karticu i dodajte unos **cn=this** s ulogom **access-id** za ACL-ove i vlasnike. Provjerite da li je poništen izbor za **Prikupi filtrirane ACL-ove** i da je izabrano **Širi korisnika**. Pogledajte "Zadaci Liste kontrole pristupa (ACL)" na stranici 201 za detaljnije informacije.

U početku, **ibm-replicagroup** objekt kreiran ovom obradom nasljeđuje ACL-ove ishodišnog unosa za replicirano podstablo. Ti ACL-ovi bi mogli biti neprikladni za kontroliranje pristupa informacijama o replikaciji u direktoriju.

Kreiranje topologije glavni-prosljeditelj-replika

Koristite ovu informaciju za kreiranje topologije glavni-prosljeditelj-replik.

Za definiranje topologije glavni-prosljeditelj-replika, morate:

1. Kreirati glavni poslužitelj i replika poslužitelj. Pogledajte “Kreiranje topologije glavne-replike” na stranici 139.
2. Kreirati novi poslužitelj replike za originalnu repliku. Pogledajte “Kreiranje novog poslužitelja replike”.
3. Kopirajte podatke na replike. Pogledajte “Kopiranje podataka na repliku” na stranici 144.

Kreiranje glavnog poslužitelja (replicirano podstablo)

Koristite ovu informaciju za kreiranje repliciranog podstabla glavnog poslužitelja.

Bilješka: Poslužitelj mora raditi da bi se mogao izvesti ovaj zadatak.

Taj zadatak označava unos kao korijen nezavisno repliciranog podstabla i kreira **ibm-replicasubentry** koji predstavlja tog poslužitelja kao jednog glavnog poslužitelja za podstablo. Kako bi kreirali replicirano podstablo, morate označiti podstablo kojeg želite da replicira poslužitelj.

Proširite kategoriju Upravljanje replikacijom u području navigacije i kliknite na **Upravljanje topologijom**.

1. Kliknite **Dodavanje podstabla**.
2. Unesite DN unosa korijena podstabla kojeg želite replicirati ili kliknite na **Pregled** kako bi proširili unose i kako bi izabrali unos koji će biti korijen podstabla.
3. URL referal glavnog poslužitelja je prikazan u obliku LDAP URL, na primjer:
   `ldap://<myservername>.<mylocation>.<mycompany>.com`

   Bilješka: URL referal glavnog poslužitelja je neobvezan. On se koristi samo:
   - Ako poslužitelj sadrži (ili će sadržavati) bilo koja podstabla samo za čitanje.
   - Kako bi se definirao URL referal koji je vraćen za ažuriranje i bilo koje podstablo samo za čitanje na poslužitelju.
4. Kliknite **OK**.
5. Novi poslužitelj je prikazan na panelu Upravljanje topologijom pod naslovom **Replicirana podstabla**.

Kreiranje novog poslužitelja replike

Koristite ovu informaciju za kreiranje novog poslužitelja replike.

Ako ste postavili topologiju replikacije (pogledajte Kreiranje glavnog poslužitelja (replicirano podstablo)) s masterom (poslužitelj1) i replikom (poslužitelj2), možete promijeniti ulogu poslužitelja2 u poslužitelj prosljeđivanja. Kako bi to napravili, trebate kreirati novu repliku (server3) pod poslužiteljem server2.

1. Povežite Web administraciju s glavnim poslužiteljem (server1)
2. Proširite kategoriju Upravljanje replikacijom u području navigacije i kliknite na **Upravljanje topologijom**.
3. Izaberite podstablo koje želite replicirati i kliknite na **Pokazivanje topologije**.
4. Kliknite na strelicu uz izbor **Topologija replikacije** kako bi proširili popis poslužitelja dobavljača.
5. Kliknite na strelicu uz izbor poslužitelja **server1** kako bi proširili popis poslužitelja.
6. Izaberite poslužitelj server2 i kliknite na **Dodavanje replike**.
7. Na karticu **Poslužitelj** prozora **Dodavanje replike**:
   - Unesite ime hosta i broj porta za repliku (server3) koju kreirate. Default port je 389 za ne-SSL i 636 za SSL. To su potrebna polja.
   - Izaberite da li ćete omogućiti SSL komunikacije.
   - Unesite ime replike ili ostavite to polje praznim kako bi se koristilo ime hosta.
   - Unesite ID replike. Ako se izvodi poslužitelj na kojem kreirate repliku, kliknite na **Dobavi ID replike** kako bi se automatski popunilo to polje. To je nužno polje ako će poslužitelj kojeg dodajete biti ravnopravan poslužitelj ili poslužitelj prosljeđivanja. Preporuča se da svi poslužitelji budu na istom izdanju.

- Unesite opis replika poslužitelja.

Na kartici **Dodatno**:

- Specificirajte vjerodajnice koje replika koristi za komuniciranje s glavnim poslužiteljem.

  Bilješka: Web administracijski alat vam omogućava da definirate vjerodajnice na dva mjesta:
  - **cn=replication,cn=localhost**, vjerodajnice se čuvaju samo na poslužitelju koji ih koristi.
  - Unutar repliciranog podstabla, u tom slučaju su vjerodajnice replicirane s ostatkom podstabla.

  Smještanje vjerodajnica u cn=replication,cn=localhost se smatra sigurnijim. Vjerodajnice koje su smještene u replicirano podstablo su kreirane ispod **ibm-replicagroup=default** unosa za to podstablo.
- Kliknite **Biranje**.
  - Izaberite lokaciju za vjerodajnice koje želite koristiti. Preferira se da to bude cn=replication,cn=localhost.
  - Kliknite na **Prikaži vjerodajnice**.
  - Proširite popis vjerodajnica i izaberite jednu koju želite koristiti.
  - Kliknite **OK**.

  Pogledajte Kreiranje replikacijskih vjerodajnica za dodatne informacije o vjerodajnicama ugovora.
- Specificirajte raspored replikacije iz padajućeg popisa ili kliknite na **Dodavanje** da kreirate jedan. Pogledajte Kreiranje replikacijskih rasporeda.
- Iz popisa sposobnosti dobavljača možete poništiti izbor bilo kojih sposobnosti za koje ne želite da se repliciraju na potrošača.

  Ako vaša mreža ima različite poslužitelje na različitim izdanjima, na novijim izdanjima su dostupne sposobnosti koje nisu dostupne na ranijim izdanjima. Neke sposobnosti, kao što su ACL-ovi filtera i lozinka politike, koriste operativne atribute koji su replicirani s drugim promjenama. U većini slučajeva, ako su te funkcije korištene, želite da ih svi poslužitelji podržavaju. Ako svi poslužitelji ne podržavaju neku sposobnost, nemojte ga koristiti. Na primjer, ne želite da različiti ACL-ovi budu učinkoviti na svakom poslužitelju. Međutim, postoje neki slučajevi kada ćete možda željeti koristiti sposobnost na poslužiteljima koji ju podržavaju, a da se promjene koje se odnose na sposobnost ne repliciraju na poslužitelj koji ne podržava sposobnost. U takvim slučajevima možete koristiti listu sposobnosti kako bi označili da ne želite da se neke sposobnosti repliciraju.
- Izaberite jednonitni ili višenitni za metodu replikacije. Ako specificirate višenitni, morate specificirati i broj (između 2 i 32) veza koje će se koristiti za replikaciju. Default broj veza je 2.
- Kliknite na **OK** kako bi kreirali repliku.

8. Kopirajte podatke iz poslužitelja server2 na novog replika poslužitelja server3. Pogledajte Kopiranje podataka u repliku za informacije kako to učiniti.
9. Dodajte ugovor dobavljača na poslužitelja server3 koji čini poslužitelja server2 dobavljačem za server3, a server3 potrošačem za server2. Pogledajte Dodavanje supplier informacija o dobavljaču na novu repliku za informacije kako to učiniti.

Uloge poslužitelj su predstavljene ikonama u Web administracijskom alatu. Sada je vaša topologija:

- server1 (glavni)
  - server2 (prosljeditelj)
    - server3 (replika)

Kreiranje vjerodajnica replikacije

Koristite ovu informaciju za kreiranje vjerodajnica replikacije.

Proširite kategoriju Upravljanje replikacijom u području navigacije Web administration tool-a i kliknite **Upravljanje vjerodajnicama**.

1. Izaberite lokaciju koju želite koristiti i pohranite vjerodajnice s popisa podstabla. Web administracijski alat vam omogućava da definirate vjerodajnice na ovim lokacijama:
   - **cn=replication,cn=localhost**, koji čuvaju vjerodajnice samo na trenutnom poslužitelju.

Bilješka: U većini slučajeva replikacije, preferira se smještanje vjerodajnica u cn=replication,cn=localhost jer ono osigurava veću sigurnost od repliciranih vjerodajnica koje su smještene na podstablu. No, postoje neke situacije u kojima nisu dostupne vjerodajnice smještene na cn=replication,cn=localhost.

Ako pokušavate dodati repliku pod poslužitelja, na primjer poslužitelja A, a povezani ste na drugog poslužitelja s Web administracijskim alatom, poslužitelja B, polje **Izabrane vjerodajnice** ne prikazuje opciju **cn=replication,cn=localhost**. To je stoga jer ne možete čitati informacije ili ažurirati bilo koje informacije pod **cn=localhost** poslužiteljem A kada ste povezani na poslužitelja B.

Opcija cn=replication,cn=localhost je dostupna samo kada je poslužitelj pod kojeg pokušavate dodati repliku isti onaj poslužitelj na kojeg ste povezani s Web administracijskim alatom.

- Unutar repliciranog podstabla, u tom slučaju su vjerodajnice replicirane s ostatkom podstabla. Vjerodajnice koje su smještene u replicirano podstablo su kreirane ispod **ibm-replicagroup=default** unosa za to podstablo.

  Bilješka: Ako nije prikazano nijedno podstablo, otiđite na “Kreiranje glavnog poslužitelja (replicirano podstablo)” na stranici 140 radi uputa o kreiranju podstabla koje želite replicirati.

2. Kliknite **Dodavanje**.
3. Unesite ime za vjerodajnice koje kreirate, na primjer, **mycreds**, cn= je već za vas ispunjeno u polju.
4. Izaberite tip metode za provjeru autentičnosti koju želite koristiti i kliknite na **Sljedeće**.
   - Ako ste izabrali jednostavnu provjeru autentičnosti vezanja:
     a. Unesite DN koji poslužitelj koristi za vezanje na repliku, na primjer, cn=any.
     b. Unesite lozinku koju poslužitelj koristi kada se povezuje na repliku, na primjer, tajna.
     c. Ponovno unesite lozinku da potvrdite da nema tiskarskih greški.
     d. Ako želite, unesite kratki opis vjerodajnica.
     e. Kliknite **Završetak**.

     Bilješka: Možda ćete željeti zapisati DN vezanja vjerodajnice i lozinku za buduće korištenje. Ta lozinka će vam biti potrebna kod kreiranja ugovora o replici.
   - Ako ste izabrali Kerberos provjeru autentičnosti:
     a. Unesite DN Kerberos vezanja.
     b. Unesite ime datoteke kartice ključeva.
     c. Ako želite, unesite kratki opis vjerodajnica. Nisu potrebne nikakve druge informacije. Pogledajte “Omogućavanje provjere autentičnosti Kerberos na Directory Server-u” na stranici 173 za dodatne informacije.
     d. Kliknite **Završetak**.

     Dodavanje Kerberos vjerodajnica panel uzima neobvezan DN vezivanja oblika ibm-kn=user@realm i neobveznu datoteku tablice ključeva (koja se zove i datoteka ključeva). Ako je DN vezivanja naveden, poslužitelj koristi navedeno glavno ime radi provjere autorizacije na potrošački poslužitelj. Inače Kerberos ime servisa poslužitelja (ldap/host-name@realm) je korišteno. Ako je korištena datoteka tablice ključeva, poslužitelj ga koristi da dobije vjerodajnice za navedeno glavno ime. Ako je datoteka tablice ključeva navedena, poslužitelj koristi datoteku tablice ključeva navedenu u Kerberos konfiguraciji poslužitelja. Ako postoji više nego jedan dobavljač, morate navesti principal ime i datoteku tablice ključeva za korištenje od strane svih dobavljača.

     Na poslužitelju na kojem ste kreirali vjerodajnice:
     a. Proširite **Upravljanje direktorijem** i kliknite **Upravljanje unosima**.
     b. Izaberite podstablo na kojem ste pohranili vjerodajnice, na primjer **cn=localhost** i kliknite na **Proširivanje**.
     c. Izaberite **cn=replication** i kliknite na **Proširivanje**.
     d. Izaberite kerberos vjerodajnice (ibm-replicationCredentialsKerberos) i kliknite na **Uredi atribute**.
     e. Kliknite karticu **Drugi atributi**.
     f. Unesite **replicaBindDN**, na primjer, **ibm-kn=myprincipal@SOME.REALM**.

g. Unesite **replicaCredentials**. To je ime datoteke ključeva korišteno za **myprincipal**.

Bilješka: Taj principal i lozinka bi trebali biti jednaki onima koje koristite kako bi se izvodio **kinit** iz reda za naredbe.

Na replici

a. Kliknite na **Upravljanje svojstvima replikacije** u području navigacije.
b. Izaberite dobavljača iz padajućeg izbornika **Informacije o dobavljaču** ili unesite ime repliciranog podstabla za koje želite konfigurirati vjerodajnice dobavljača.
c. Kliknite **Uređivanje**.
d. Unesite DN vezanja replikacije. U ovom primjeru, **ibm-kn=myprincipal@SOME.REALM**.
e. Unesite i potvrdite **Lozinku vezanja replikacije**. To je KDC lozinka koja se koristi za **myprincipal**.

- Ako ste izabrali SSL s provjerom autentičnosti certifikata, onda ne trebate osigurati nikakve dodatne informacije ako koristite certifikat poslužitelja. Ako izaberete korištenje certifikata koji nije certifikat poslužitelja:
  a. Unesite ime datoteke ključa.
  b. Unesite lozinku datoteke ključa.
  c. Ponovno unesite lozinku datoteke ključa kako bi je potvrdili.
  d. Unesite oznaku ključa.
  e. Ako želite, unesite kratki opis.
  f. Kliknite **Završetak**.

  Pogledajte “Omogućavanje SSL-a i sigurnosti sloja prijenosa na Directory Server-u” na stranici 171 za dodatne informacije.

5. Na poslužitelju na kojem ste kreirali vjerodajnice postavite sistemsku vrijednost Dozvoli zadržavanje informacija sigurnosti poslužitelja (QRETSVRSEC) na 1 (zadrži podatke). Budući su vjerodajnice replikacije pohranjene u validacijskoj listi, to omogućuje poslužitelju da dohvati vjerodajnice za validacijske liste kada se povezuje na repliku.

Kreiranje poslužitelja replike

Koristite ovu informaciju za kreiranje poslužitelja replike.

Bilješka: Poslužitelj mora raditi da bi se mogao izvesti ovaj zadatak.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje topologijom**.

1. Izaberite podstablo koje želite replicirati i kliknite na **Pokazivanje topologije**.
2. Kliknite na strelicu uz izbor **Topologija replikacije** kako bi proširili popis poslužitelja dobavljača.
3. Izaberite poslužitelj dobavljača i kliknite na **Dodavanje replike**.
4. Na karticu **Poslužitelj** prozora **Dodavanje replike**:
   a. Unesite ime hosta i broj porta za repliku koju kreirate. Default port je 389 za ne-SSL i 636 za SSL. To su potrebna polja.
   b. Izaberite da li ćete omogućiti SSL komunikacije.
   c. Unesite ime replike ili ostavite to polje praznim kako bi se koristilo ime hosta.
   d. Unesite ID replike. Ako se izvodi poslužitelj na kojem kreirate repliku, kliknite na **Dobavi ID replike** kako bi se automatski popunilo to polje. To je nužno polje ako će poslužitelj kojeg dodajete biti ravnopravan poslužitelj ili poslužitelj proslјeđivanja. Preporuča se da svi poslužitelji budu na istom izdanju.
   e. Unesite opis replika poslužitelja.
5. Na kartici **Dodatni**,
   - Specificirajte vjerodajnice koje replika koristi za komuniciranje s glavnim poslužiteljem.

     Bilješka: Web administracijski alat vam omogućava da definirate vjerodajnice u ovim mjestima:

– **cn=replication,cn=localhost**, čuvaju vjerodajnice samo na poslužitelju koji ih koristi.
– Unutar repliciranog podstabla, u tom slučaju su vjerodajnice replicirane s ostatkom podstabla. Vjerodajnice koje su smještene u replicirano podstablo su kreirane ispod **ibm-replicagroup=default** unosa za to podstablo.

Smještanje vjerodajnica u cn=replication,cn=localhost se smatra sigurnijim. Vjerodajnice smještene u replicirano podstablo kreiraju se ispod unosa ibm-replicagroup=default za to podstablo.

- Kliknite **Biranje**.
  – Izaberite lokaciju za vjerodajnice koje želite koristiti. Preferira se da to bude cn=replication,cn=localhost.
  – Kliknite na **Prikaži vjerodajnice**.
  – Proširite popis vjerodajnica i izaberite jednu koju želite koristiti.
  – Kliknite **OK**.

  Pogledajte Kreiranje replikacijskih vjerodajnica za dodatne informacije o vjerodajnicama ugovora.
- Specificirajte raspored replikacije iz padajućeg popisa ili kliknite na **Dodavanje** da kreirate jedan. Pogledajte Kreiranje replikacijskih rasporeda.
- Iz popisa sposobnosti dobavljača možete poništiti izbor bilo kojih sposobnosti za koje ne želite da se repliciraju na potrošača.

  Ako vaša mreža ima različite poslužitelje na različitim izdanjima, na novijim izdanjima su dostupne sposobnosti koje nisu dostupne na ranijim izdanjima. Neke sposobnosti, kao što su ACL-ovi filtera i lozinka politike, koriste operativne atribute koji su replicirani s drugim promjenama. U većini slučajeva, ako su te funkcije korištene, želite da ih svi poslužitelji podržavaju. Ako svi poslužitelji ne podržavaju neku sposobnost, nemojte ga koristiti. Na primjer, ne želite da različiti ACL-ovi budu učinkoviti na svakom poslužitelju. Međutim, postoje neki slučajevi kada ćete možda željeti koristiti sposobnost na poslužiteljima koji ju podržavaju, a da se promjene koje se odnose na sposobnost ne repliciraju na poslužitelj koji ne podržava sposobnost. U takvim slučajevima možete koristiti listu sposobnosti kako bi označili da ne želite da se neke sposobnosti repliciraju.
- Izaberite jednonitni ili višenitni za metodu replikacije. Ako specificirate višenitni, morate specificirati i broj (između 2 i 32) veza koje će se koristiti za replikaciju. Default broj veza je 2.
- Kliknite **OK** za kreiranje replike.

6. Prikazuje se poruka koja označava da se moraju poduzeti dodatne akcije. Kliknite na **OK**.

Bilješka: Ako dodajete više poslužitelja kao dodatne replike ili kreirate kompleksnu topologiju, nemojte nastaviti s Kopiranjem podataka u repliku ili Dodavanjem informacija o dobavljaču u novu repliku dok ne završite definiranje topologije na glavnom poslužitelju. Ako kreirate *masterfile.ldif* nakon što ste dovršili topologiju, ona sadrži unose direktorije glavnog poslužitelja i potpunu kopiju ugovora topologije. Kada učitate tu datoteku na svakog od poslužitelja, svaki poslužitelj ima iste informacije.

Kopiranje podataka na repliku

Koristite ovu informaciju za kopiranje podataka na repliku.

Nakon kreiranja replike morate eksportirati topologiju iz glavnog poslužitelja na repliku.

1. Na glavnom poslužitelju kreirajte LDIF datoteku za podatke. Kako bi kopirali podatke sadržane na glavnom poslužitelju, napravite sljedeće:
   a. U System i Navigator, proširite **Mreža**.
   b. Proširite **Poslužitelji**.
   c. Kliknite **TCP/IP**.
   d. Desno kliknite na **IBM Poslužitelj direktorija** i izaberite **Alati**, onda **Eksportiraj datoteku**.
   e. Specificirajte ime izlazne LDIF datoteke (na primjer masterfile.ldif), neobvezno specificirajte podstablo koje će se eksportirati (na primjer subtreeDN) i kliknite na **OK**.
2. Na stroju na kojem kreirate repliku napravite sljedeće:
   a. Provjerite da li su replicirani sufiksi definirani u konfiguraciji replika poslužitelja.
   b. Zaustavite replika poslužitelj.

c. Kopirajte LDIF datoteku na repliku i napravite sljedeće:
   1) U System i Navigator, proširite **Mreža**.
   2) Proširite **Poslužitelji**.
   3) Kliknite **TCP/IP**.
   4) Desno kliknite na **IBM Poslužitelj direktorija** i izaberite **Alati**, onda **Importiraj Datoteku**.
   5) Specificirajte ime ulazne LDIF datoteke (na primjer masterfile.ldif), neobvezno specificirajte da li želite replicirati podatke i kliknite na **OK**.

   Ugovori replikacije, rasporedi, vjerodajnice (ako su pohranjene u podstablu replikacije) i unosi podataka se učitavaju na repliku.
d. Pokrenite poslužitelj.

Dodavanje informacija o dobavljaču na novu repliku

Koristite ovu informaciju za dodavanje informacija o poslužitelju na novu repliku.

Trebate promijeniti konfiguraciju replike kako bi identificirali tko je ovlašten da replicira promjene i dodati referala na glavnog poslužitelja.

Na stroju na kojem kreirate repliku:

1. Proširite **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje svojstvima replikacije**.

   Bilješka: Morate se prijaviti na Web administration tool kao projicirani OS/400 korisnik s *ALLOBJ i *IOSYSCFG posebnim ovlaštenjima za promjenu postavki u panelima **Upravljanje replikacijskim svojstvima**.
2. Kliknite **Dodavanje**.
3. Izaberite dobavljača iz padajućeg izbornika **Replicirano podstablo** ili unesite ime repliciranog podstabla za koje želite konfigurirati vjerodajnice dobavljača. Ako uređujete vjerodajnice dobavljača, to polje se ne može uređivati.
4. Unesite DN vezanja replikacije. U ovom primjeru, cn=any.

   Bilješka: Možete koristiti bilo koju od te dvije opcije, ovisno o vašoj situaciji.
   - Postavite DN vezanja replikacije (i lozinku) i default referal za sva podstabla replicirana na poslužitelju korištenjem 'default vjerodajnice i referali'. To bi se moglo koristiti kada su sva podstabla replicirana iz istog dobavljača.
   - Postavite DN vezanja replikacije i lozinku neovisno za svako replicirano podstablo dodavanjem informacije o dobavljaču za svako podstablo. To bi se moglo koristiti kada svako podstablo ima drugačijeg dobavljača (odnosno, različiti glavni poslužitelj za svako podstablo).
5. Ovisno o tipu vjerodajnice, unesite i potvrdite lozinku vjerodajnice. (Ranije ste je zapisali za buduće korištenje.)
   - **Jednostavno vezanje** - Specificirajte DN i lozinku.
   - **Kerberos** - Ako vjerodajnice o dobavljaču ne identificiraju principal i lozinku, to jest, ako se treba koristiti vlastiti uslužni principal poslužitelja, tada je bind DN ibm-kn=ldap/<*yourservername@yourrealm*>. Ako vjerodajnica ima ime principala poput <*myprincipal@myrealm*>, koristite ga kao DN. U svakom slučaju, lozinka nije potrebna.
   - **SSL w/ EXTERNAL vezanje** - Specificirajte DN subjekta za certifikat bez lozinke.

   Pogledajte "Kreiranje vjerodajnica replikacije" na stranici 141.
6. Kliknite **OK**.
7. Morate ponovno pokrenuti repliku kako bi primjene imale učinka.

Pogledajte "Promjena svojstava replikacije" na stranici 152 za dodatne informacije.

Replika je u suspendiranom stanju i ne dolazi do replikacije. Nakon što ste dovršili postavljanje vaše topologije replikacije, morate kliknuti na **Upravljanje redovima**, izabrati repliku i kliknuti na **Odgodi/nastavi** kako bi započeli replikaciju. Pogledajte “Upravljanje redovima replikacije” na stranici 155 za detaljnije informacije. Replika sada prima ažuriranja iz glavnog poslužitelja.

Kreiranje jednostavne topologije s ravnopravnom replikacijom

Ravnopravna replikacija je topologija replikacije u kojoj ima više glavnih poslužitelja. Koristite ravnopravnu replikaciju jedino u okolinama u kojima su vektori ažuriranja dobro poznati.

Ažuriranja na određenim objektima unutar direktorija mora izvoditi samo jedan glavni poslužitelj. Namjera je toga da se spriječi scenarij u kojem jedan poslužitelj briše objekt, nakon čega drugi poslužitelj modificira objekt. Taj scenarij kreira mogućnost da ravnopravni poslužitelj primi naredbu za brisanje pa naredbu za modificiranje za isti objekt, čime se kreira sukob. Replicirani zahtjevi za brisanje i preimenovanje prihvatljivi su u primljenom redu bez rezolucije sukoba. Pogledajte niže navedene odgovarajuće veze za više informacija o Rezoluciji sukoba replikacije.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje topologijom**.

1. Izaberite podstablo koje želite replicirati i kliknite na **Pokazivanje topologije**.
2. Kliknite kućicu pored postojećih poslužitelja za proširenje liste poslužitelja dobavljača, ako želite pogledati postojeću topologiju.
3. Kliknite **Dodavanje mastera**.

Na kartici **Poslužitelj** prozora **Dodavanje mastera**:

- Upišite host ime i broj porta za poslužitelj koji kreirate. Default port je 389 za ne-SSL i 636 za SSL. To su potrebna polja.
- Izaberite da li ćete omogućiti SSL komunikacije.
- Izaberite želite li kreirati poslužitelj kao gateway poslužitelj.
- Upišite ime poslužitelja ili ostavite to polje prazno za korištenje host imena.
- Upišite ID poslužitelja. Ako poslužitelj na kojem kreirate peer-master radi, kliknite **Dohvati ID poslužitelja** za automatsko prethodno popunjavanje tog polja. Ako ne znate ID poslužitelja, upišite **nepoznat**.
- Upišite opis poslužitelja.
- Morate specificirati vjerodajnice koje poslužitelj koristi za komunikaciju s drugim glavnim poslužiteljem. Kliknite **Biranje**

  Bilješka: Web Administration Tool dozvoljava definiranje vjerodajnica na sljedećim mjestima:
  - **cn=replication,cn=localhost**, vjerodajnice se čuvaju samo na poslužitelju koji ih koristi. Smještanje vjerodajnica u cn=replication,cn=localhost se smatra sigurnijim.
  - **cn=replication,cn=IBMpolicies**, koji je dostupan čak i kad poslužitelj s kojim pokušavate dodati repliku nije isti poslužitelj na koji ste spojeni s Web Administration Tool. Vjerodajnice smještene na tu lokaciju replicirane su na poslužitelje.

    Bilješka: Lokacija cn=replication,cn=IBMpolicies je dostupna jedino ako je podrška IBMpolicies OID, 1.3.18.0.2.32.18, prisutna pod ibm-supportedcapabilities korijenskog DSE-a.
  - Unutar repliciranog podstabla, u tom slučaju su vjerodajnice replicirane s ostatkom podstabla. Vjerodajnice koje su smještene u replicirano podstablo su kreirane ispod **ibm-replicagroup=default** unosa za to podstablo.

  1. Izaberite lokaciju za vjerodajnice koje želite koristiti. Preferira se da to bude cn=replication,cn=localhost.
  2. Ako ste već kreirali skup vjerodajnica, kliknite Pokaži vjerodajnice.
  3. Proširite popis vjerodajnica i izaberite jednu koju želite koristiti.
  4. Kliknite OK.
  5. Ako nemate postojeće vjerodajnice, kliknite Dodavanje za kreiranje vjerodajnica.

Na kartici **Dodatno**:

1. Specificirajte raspored replikacije iz padajućeg popisa ili kliknite na **Dodavanje** da kreirate jedan. Pogledajte Kreiranje replikacijskih rasporeda.
2. Iz popisa sposobnosti dobavljača možete poništiti izbor bilo kojih sposobnosti za koje ne želite da se repliciraju na potrošača.

   Ako vaša mreža ima različite poslužitelje na različitim izdanjima, na novijim izdanjima su dostupne sposobnosti koje nisu dostupne na ranijim izdanjima. Neke sposobnosti, kao što su ACL-ovi filtera i lozinka politike, koriste operativne atribute koji su replicirani s drugim promjenama. U većini slučajeva, ako se ta svojstva koriste, svi ih poslužitelji trebaju podržavati. Ako svi poslužitelji ne podržavaju neku sposobnost, nemojte ga koristiti. Na primjer, ne želite da različiti ACL-ovi budu učinkoviti na svakom poslužitelju. Međutim, postoje neki slučajevi kada ćete možda željeti koristiti sposobnost na poslužiteljima koji ju podržavaju, a da se promjene koje se odnose na sposobnost ne repliciraju na poslužitelj koji ne podržava sposobnost. U takvim slučajevima možete koristiti listu sposobnosti kako bi označili da ne želite da se neke sposobnosti repliciraju.
3. Označite kontrolnu kućicu **Dodavanje informacije o vjerodajnici potrošača**, ako želite omogućiti dinamičko ažuriranje vjerodajnica dobavljača. Takav izbor automatski ažurira informaciju o dobavljaču u konfiguracijskoj datoteci poslužitelja potrošača. To omogućava da se informacije o topologiji repliciraju na poslužitelj.
   - Upišite Administracijski DN za poslužitelja potrošača. Na primjer, cn=root.

     Bilješka: Ako je administratorski DN koji je kreiran za vrijeme obrade konfiguracije poslužitelja bio cn=root, tada upišite puni administratorski DN. Ne koristite samo root.
   - Upišite Administracijsku lozinku za poslužitelja potrošača. Na primjer, secret.
4. Kliknite na **OK**.
5. Ugovori dobavljača i potrošača ispisani su između novog glavnog poslužitelja i bilo kojeg postojećeg poslužitelja. Maknite oznaku sa svih ugovora koje ne želite kreirati. To je posebno važno ako kreirate gateway poslužitelj.
6. Kliknite **Nastavak**.
7. Moguće je prikazivanje poruka s napomenom da se moraju poduzeti dodatne akcije. Izvedite ili zabilježite odgovarajuće akcije. Kada završite, kliknite na **OK**.
8. Dodavanje odgovarajuće vjerodajnice.

   Bilješka: U nekim slučajevima pojavit će se panel Biranje vjerodajnice i tražiti vjerodajnicu koja je locirana na mjestu različitom od cn=replication,cn=localhost. U takvim situacijama morate dati objekt vjerodajnice koji je smješten na mjestu osim cn=replication,cn=localhost. Izaberite vjerodajnicu koju će podstablo koristiti iz postojećeg skupa vjerodajnica ili kreirajte nove vjerodajnice.
9. Kliknite **OK** za kreiranje peer-mastera.
10. Moguće je prikazivanje poruka s napomenom da se moraju poduzeti dodatne akcije. Izvedite ili zabilježite odgovarajuće akcije. Kada završite, kliknite na **OK**.

Srodne reference

"Pregled replikacije" na stranici 37
Preko replikacije se promjene koje su učinjene na jednom direktoriju šire na još jedan ili više dodatnih direktorija. U stvari, promjena na jednom direktoriju se pojavljuje na više različitih direktorija.

Kreiranje kompleksne topologije replikacije

Koristite ovaj pregled visoke razine kao vodič za postavljanje topologije kompleksne replikacije.

1. Pokrenite sve glavne poslužitelje ili buduće replike. To je potrebno stoga kako bi Web administracijski alat skupio informacije od poslužitelja.
2. Pokrenite 'prvi' glavni poslužitelj i konfigurirajte ga kao glavnog za kontekst.
3. Učitajte podatke za podstablo koji će se replicirati na 'prvom' glavnom poslužitelju, ako ti podaci nisu već učitani.
4. Izaberite podstablo koje će se replicirati.
5. Dodajte sve potencijalne ravnopravne glavne poslužitelje kao replike 'prvog' glavnog poslužitelja.
6. Dodajte sve druge replike.
7. Premjestite ostale ravnopravne glavne poslužitelje kako bi ih promovirali.

8. Dodajte ugovore replike za replike svakog ravnopravnog glavnog poslužitelja.

   Bilješka: Ako bi se trebale kreirati vjerodajnice u **cn=replication,cn=localhost**, vjerodajnice se moraju kreirati na svakom poslužitelju nakon što su bile ponovno pokrenute. Replikacija od strane ravnopravnih poslužitelja neće uspjeti dok se ne kreiraju objekti replikacije.
9. Dodajte ugovore replike za druge glavne poslužitelje na svakog ravnopravnog glavnog poslužitelja. 'Prvi' glavni poslužitelj već ima te informacije.
10. Umirite replicirano podstablo. Time se sprječava ažuriranje dok se kopiraju podaci na druge poslužitelje.
11. Koristite Upravljanje redom kako bi sve preskočili za svaki red.
12. Eksportirajte podatke za replicirano podstablo iz 'prvog' glavnog poslužitelja.
13. Uznemirite podstablo.
14. Zaustavite replika poslužitelje i importirajte podatke za replicirano podstablo na svaku repliku i ravnopravnog glavnog poslužitelja. Nakon toga ponovno pokrenite poslužitelje.
15. Upravljajte svojstvima replikacije na svakom poslužitelju i ravnopravnom glavnom poslužitelju kako bi postavili vjerodajnice koje će koristiti dobavljači.

Kreiranje kompleksne topologije s ravnopravnom replikacijom

Koristite ovu informaciju za kreiranje kompleksne topologije s ravnopravnom replikacijom.

Ravnopravna replikacija je topologija replikacije u kojoj ima više glavnih poslužitelja. No, za razliku od okoline s više glavnih poslužitelja, nema nikakvog sistema za rješavanja sukoba između ravnopravnih poslužitelja. LDAP poslužitelji prihvaćaju ažuriranja koje osiguravaju ravnopravni poslužitelji i ažuriraju svoje vlastite kopije podataka. Ne vodi se računa o poretku u kojem su primljena ažuriranja ili o tome da li su višestruka ažuriranja u sukobu.

Za dodavanje dodatnih glavnih (ravnopravnih) poslužitelja, prvo trebate dodati poslužitelj kao samo za čitanje repliku postojećih glavnih poslužitelja (pogledajte "Kreiranje poslužitelja replike" na stranici 143), inicijalizirati podatke direktorija i onda promovirati poslužitelj tako da bude glavni poslužitelj (pogledajte "Premještanje ili promoviranje poslužitelja" na stranici 164).

U početku, **ibm-replicagroup** objekt kreiran ovom obradom nasljeđuje ACL-ove ishodišnog unosa za replicirano podstablo. Ti ACL-ovi bi mogli biti neprikladni za kontroliranje pristupa informacijama o replikaciji u direktoriju.

Kako bi bila uspješna operacija Dodavanje podstabla, DN unosa kojeg dodajete mora imati ispravne ACL-ove, ako nije sufiks u poslužitelju.

Za nefiltrirane ACL-ove :

- ownersource : <*DN unos*>
- ownerpropagate: TRUE
- aclsource : <*DN unos*>
- aclpropagate: TRUE

Filtrirani ACL-ovi :

- ownersource : <*DN unos*>
- ownerpropagate: TRUE
- ibm-filteraclinherit: FALSE
- ibm-filteraclentry : <*bilo koja vrijednost*>

Koristite funkciju **Uredi ACL-ove** Web administracijskog alata da postavite ACL-ove za informacije o replikaciji koje su pridružene novo kreiranom repliciranom podstablu (pogledajte "Uređivanje lista kontrole pristupa" na stranici 165).

Replika je u suspendiranom stanju i ne dolazi do replikacije. Nakon što ste dovršili postavljanje vaše topologije replikacije, morate kliknuti na **Upravljanje redovima**, izabrati repliku i kliknuti na **Odgodi/nastavi** kako bi započeli replikaciju. Pogledajte “Upravljanje redovima replikacije” na stranici 155 za detaljnije informacije. Replika sada prima ažuriranja iz glavnog poslužitelja.

Ravnopravnu replikaciju koristite samo u okolinama u kojima je dobro poznat obrazac ažuriranja direktorija. Ažuriranja na određenim objektima unutar direktorija mora izvoditi samo jedan glavni poslužitelj. To je zato da se spriječi scenarij u kojem jedan poslužitelj briše objekt, a nakon toga drugi poslužitelj modificira objekt. Taj scenarij bi mogao rezultirati time da glavni poslužitelj primi naredbu brisanja koju slijedi naredba za modificiranje; tako nastaje sukob.

Kako bi definirali ravnopravni-prosljeditelj-replika topologiju koja se sastoji od dva ravnopravno-glavna poslužitelja, dva poslužitelja prosljeđivanja i četiri replike, morate:

1. Kreirati glavni poslužitelj i replika poslužitelj. Pogledajte “Kreiranje topologije glavne-replike” na stranici 139.
2. Kreirati dva dodatna replika poslužitelja za glavnog poslužitelja. Pogledajte “Kreiranje poslužitelja replike” na stranici 143.
3. Kreirati dvije replike ispod svakog od dva novo kreirana replika poslužitelja.
4. Promovirati originalnu repliku na poslužitelja. Pogledajte “Promoviranje poslužitelja da bude ravnopravan”.

   Bilješka: Poslužitelj kojeg želite promovirati na glavnog poslužitelja mora biti replika s listovima bez podložnih replika.
5. Kopirajte podatke iz glavnog poslužitelja na novi glavni poslužitelj i repliku. Pogledajte “Kopiranje podataka na repliku” na stranici 144.

Srodni zadaci

“Premještanje ili promoviranje poslužitelja” na stranici 164
Koristite ovu informaciju za premještanje ili promoviranje poslužitelja.

Promoviranje poslužitelja da bude ravnopravan

Koristite ovu informaciju za promoviranje poslužitelja da bude ravnopravan.

Korištenjem topologije prosljeđivanja kreirane u “Kreiranje topologije glavni-prosljeditelj-replika” na stranici 140, možete promovirati poslužitelja tako da bude ravnopravan. U ovom ćete primjeru promovirati replika poslužitelja (server3) tako da bude ravnopravan na glavnom poslužitelju (server1).

1. Povežite Web administraciju na glavni poslužitelj (server1).
2. Proširite kategoriju Upravljanje replikacijom u području navigacije i kliknite na **Upravljanje topologijom**.
3. Izaberite podstablo koje želite replicirati i kliknite na **Pokazivanje topologije**.
4. Kliknite na strelicu uz izbor **Topologija replikacije** kako bi proširili popis poslužitelja.
5. Kliknite na strelicu uz izbor poslužitelja **server1** kako bi proširili popis poslužitelja.
6. Kliknite na strelicu uz izbor poslužitelja **server2** kako bi proširili popis poslužitelja.
7. Kliknite na **server1** i kliknite na **Dodavanje replike**. Kreiranje poslužitelj server4. Pogledajte “Kreiranje poslužitelja replike” na stranici 143. Slijedite istu proceduru kako bi kreirali poslužitelj server5. Uloge poslužitelj su predstavljene ikonama u Web administracijskom alatu. Sada je vaša topologija:
   - server1 (glavni)
     - server2 (prosljeditelj)
       - server3 (replika)
     - server4 (replika)
     - server5 (replika)
8. Kliknite na **server2** i kliknite na **Dodavanje replike** kako bi kreirali poslužitelj server6.
9. Kliknite na **server4** i kliknite na **Dodavanje replike** kako bi kreirali poslužitelj server7. Slijedite istu proceduru kako bi kreirali poslužitelj server8. Sada je vaša topologija:
   - server1 (glavni)

- server2 (prosljeditelj)
  - server3 (replika)
  - server6 (replika)
- server4 (prosljeditelj)
  - server7 (replika)
  - server8 (replika)
- server5 (replika)

10. Izaberite **server5** i kliknite **Premjesti**.

    Bilješka: Poslužitelj kojeg želite premjestiti mora biti replika s listovima bez podređenih replika.

11. Izaberite **Topologija replikacije** kako bi promovirali repliku na glavnog poslužitelja. Kliknite **Premjesti**.
12. Prikazan je panel **Kreiraj dodatne ugovore dobavljača**. Ravnopravna replikacija traži da svaki glavni poslužitelj bude dobavljač i potrošač svakom od drugih glavnih poslužitelja u topologiji i svakom od replika prve razine, server2 i server4. Server5 je već potrošač od server1, sada treba postati dobavljač za server1, server2 i server4. Provjerite da li je u kućicama ugovora dobavljača označeno:

Tablica 5.

	Dobavljač	Potrošač
✓	server5	server1
✓	server5	server2
✓	server5	server4

Kliknite **Nastavak**.

Bilješka: U nekim će slučajevima iskočiti panel Biranje vjerodajnice koji će od vas tražiti vjerodajnicu koja je smještena negdje drugdje, a ne na cn=replication,cn=localhost. U takvim situacijama morate osigurati objekt vjerodajnice koji se nalazi negdje drugdje, a ne na cn=replication,cn=localhost. Izaberite vjerodajnice koje će koristiti podstablo, oblikujte postojeće skupove vjerodajnica ili kreirajte nove vjerodajnice. Pogledajte “Kreiranje vjerodajnica replikacije” na stranici 141.

13. Kliknite **OK**. Sada je vaša topologija:
    - server1 (glavni)
      - server2 (prosljeditelj)
        - server3 (replika)
        - server6 (replika)
      - server4 (prosljeditelj)
        - server7 (replika)
        - server8 (replika)
      - server5 (glavni)
    - server5 (glavni)
      - server1 (glavni)
      - server2 (prosljeditelj)
      - server4 (prosljeditelj)
14. Kopirajte podatke iz poslužitelja server1 na sve poslužitelje. Pogledajte “Kopiranje podataka na repliku” na stranici 144 za informacije kako da to napravite.

Postavljanje gateway topologije

Koristite ovu informaciju za postavljanje gateway topologije.

Prije pokretanja postavljanja topologije vaše replikacije, napravite sigurnosnu kopiju vaše originalne ibmslapd.conf datoteke. Možete koristiti tu kopiju da obnovite vašu originalnu konfiguraciju ako naiđete na probleme s replikacijom.

Za postavljanje gateway-a pomoću kompleksne topologije s ravnopravnom replikacijom iz postupka u Promoviranje poslužitelja da bude ravnopravan, morate proći sljedeće korake:

- Pretvorite postojeći ravnopravni poslužitelj (peer 1) u gateway poslužitelj da kreirate replikacijsku stranicu 1.
- Kreirajte novi gateway poslužitelj za replikacijsku stranicu 2 i ugovore s peer 1.
- Kreirajte topologiju za replikacijsku stranicu 2 (nije ilustrirano u ovom primjeru).
- Kopirajte podatke iz glavnog stroja u sve strojeve u topologiji.

1. Upotrijebite alat Web administracije da se prijavite u glavni poslužitelj (server1).
2. Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje topologijom**.
3. Izaberite podstablo koje želite replicirati i kliknite na **Pokazivanje topologije**.
4. Za konvertiranje postojećeg poslužitelja u gateway poslužitelj, izaberite **Upravljanje gateway poslužiteljima**. Izaberite **server1** ili njegov ravnopravni **server5**. Za ovaj primjer koristite **server1** i kliknite **Napravi gateway**.
5. Kliknite **OK**.

   Bilješka: Ako poslužitelj koji želite koristiti kao gateway nije već glavno, mora biti list replika bez podređenih replika koje prvo možete promovirati da budu glavne i onda odrediti kao gateway.
6. 6. Za kreiranje novog gateway poslužitelja, kliknite **Dodavanje poslužitelja**.
7. Kreirajte novi poslužitelj, **server9** kao gateway poslužitelj. Pogledajte “Dodavanje peer-master ili gateway poslužitelja” na stranici 159 za informacije o tome kako to napraviti.
8. Prikazan je **Kreiraj dodatne ugovore dobavljača** panel. U tom panelu, osigurajte da su kućice ugovora dobavljača označene samo za poslužitelj1. Deselektirajte ostale ugovore.

	Dobavljač	Potrošač
✓	server1	server9
✓	server9	server1
	server2	server9
	server9	server2
	server4	server9
	server9	server4
	server9	server5
	server5	server9

9. Kliknite **Nastavak**.
10. Kliknite **OK**.
11. Dodajte odgovarajuće vjerodajnice i informacije o potrošačima.

    Bilješka: U nekim slučajevima se panel **Izbor vjerodajnica** prikazuje tražeći vjerodajnicu koja se nalazi na nekom drugom mjestu osim u cn=replication,cn=localhost. U takvim situacijama morate dati objekt vjerodajnice koji je smješten na mjestu osim cn=replication,cn=localhost. Izaberite vjerodajnicu koju će podstablo koristiti iz postojećeg skupa vjerodajnica ili kreirajte nove vjerodajnice. Pogledajte Kreiranje replikacijske vjerodajnice.
12. Kliknite **OK**. Uloge poslužitelj su predstavljene ikonama u Web administracijskom alatu. Sada je vaša topologija:
    - server1 (master-gateway za replikacijski site1)
      - server2 (prosljeditelj)
        - server3 (replika)
        - server6 (replika)

- server4 (prosljeditelj)
  - server7 (replika)
  - server8 (replika)
- server5 (glavni)
- server9 (master-gateway za replikacijski site 2)

• server5 (glavni)
- server1 (glavni)
- server2 (prosljeditelj)
  - server3 (replika)
  - server6 (replika)
- server4 (prosljeditelj)
  - server7 (replika)
  - server8 (replika)

• server9 (glavni-prosljeditelj)
- server1 (glavni-prosljeditelj)

13. Dodajte poslužitelje na **server9** za kreiranje topologije za replikacijsku stranicu 2. Nemojte zaboraviti deselektirati svaki ugovor za nove poslužitelje na bilo kojem poslužitelju izvan replikacijske stranice 2.
14. Ponovite ovaj proces da kreirate dodatne replikacijske stranice. Imajte na umu da kreirate samo jedan prilazni poslužitelj po replicirajućoj stranici. Međutim, svaki gateway poslužitelj mora biti prisutan topologijama s ugovorima na drugim gateway poslužiteljima.
15. Kada ste završili kreiranje topologije, kopirajte podatke iz server1 na sve nove poslužitelje u svim replicirajućim stranicama i dodajte informacije o dobavljaču na sve poslužitelje. Pogledajte Kopiranje podataka na repliku i Dodavanje informacija o dobavljači na novu repliku za informacije o tome kako to učiniti.

Srodni zadaci

"Dodavanje replika poslužitelja" na stranici 158
Koristite ovu informaciju za kreiranje replika poslužitelja.

"Dodavanje peer-master ili gateway poslužitelja" na stranici 159
Ovo poglavlje sadrži informacije o tome kako kreirati novi peer-master ili gateway poslužitelj.

"Upravljanje gateway poslužiteljima" na stranici 162
Ovo poglavlje daje informacije o upravljanju gateway poslužiteljima. Možete odrediti treba li glavni poslužitelj imati ulogu gateway poslužitelja na stranici replikacije.

Promjena svojstava replikacije

Koristite ovu informaciju za promjenu svojstava replikacije.

Morate se prijaviti na Web administracijski alat kao projicirani korisnik s *ALLOBJ i *IOSYSCFG posebnim ovlaštenjima da promijenite postavke u panelu **Upravljanje svojstvima replikacije**.

1. Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite **Upravljanje svojstvima replikacije**
2. Na ovom panelu možete:
   a. Promijeniti maksimalan broj promjena u stanju čekanja koje se vraćaju iz upita o statusu replikacije. Default je 200.
   b. Postavite maksimum broja grešaka replikacije koje će poslužitelj zapisati dok replicira nadogradnju potrošaču. Ako poslužitelj koristi jednonitnu replikaciju, a maksimum je premašen, nadogradnja se povremeno ponovno pokušava dok ne uspije ili dok administrator ne očisti dnevnik tako da se kvar može dodati. Ako poslužitelj koristi višenitnu replikaciju, a maksimum je premašen, svaka greška replikacije koja se desi za vrijeme nadograđivanja se zapisuje, a replikacija čeka dok administrator ne očisti dnevnik. Dnevnik se može očistiti ponovno pokušajem ili uklanjanjem neuspjelih nadogradnji. Odijeljeni dnevnici se održavaju za svakog potrošača. Default je nula u smislu ništa.

Bilješka: Zapisivanje je omogućeno ako je specificirana vrijednost veća od nule.

c. Promijenite veličinu u bajtovima predmemorije konteksta replikacije. Default je 100,000 bajtova.

d. Postavite veličinu maksimalnog unosa sukoba replikacije u bajtovima. Ako ukupna veličina unosa u bajtovima premašuje vrijednost u tom polju, dobavljač ne šalje ponovno unos za rješavanje sukoba replikacije na potrošaču. Default je 0 za neograničeno.

e. Dodati, urediti ili obrisati informacije o dobavljaču.

Bilješka: DN dobavljača može biti DN projiciranogi5/OS korisničkog profila. Projicirani i5/OS korisnički profil ne smije imati LDAP administrativno ovlaštenje. Korisnik ne može biti korisnik s *ALLOBJ i *IOSYSCFG posebnim ovlaštenjima i nije mu se moglo dodijeliti administrativno ovlaštenje preko ID-a aplikacije administratora poslužitelja direktorija.

Za više informacija, pogledajte sljedeće:

- "Dodavanje informacija o dobavljaču"
- "Uređivanje informacija o dobavljaču"
- "Uklanjanje informacija o dobavljaču" na stranici 154

Dodavanje informacija o dobavljaču

Koristite ovu informaciju za dodavanje informacija o poslužitelju.

1. Kliknite **Dodavanje**.
2. Izaberite dobavljača iz padajućeg izbornika ili unesite ime repliciranog podstabla kojeg želite dodati kao dobavljača.
3. Unesite DN vezanja replikacije za vjerodajnice.

Bilješka: Možete koristiti bilo koju od te dvije opcije, ovisno o vašoj situaciji.

- Postavite DN vezanja replikacije (i lozinku) i default referal za sva podstabla replicirana na poslužitelju korištenjem 'default vjerodajnice i referali'. To bi se moglo koristiti kada su sva podstabla replicirana iz istog dobavljača.
- Postavite DN vezanja replikacije i lozinku neovisno za svako replicirano podstablo dodavanjem informacije o dobavljaču za svako podstablo. To bi se moglo koristiti kada svako podstablo ima drugačijeg dobavljača (odnosno, različiti glavni poslužitelj za svako podstablo).

4. Ovisno o tipu vjerodajnice, unesite i potvrdite lozinku vjerodajnice. (Ranije ste je zapisali za buduće korištenje.)
   - **Jednostavno vezanje** - specificirajte DN i lozinku
   - **Kerberos** - specificirajte pseudo DN oblika 'ibm-kn=LDAP-service-name@realm' bez lozinke
   - **SSL w/ EXTERNAL vezanje** - specificirajte DN subjekta za certifikat, bez dozvole

   Pogledajte "Kreiranje vjerodajnica replikacije" na stranici 141.
5. Kliknite **OK**.

Podstablo dobavljača se dodaje na listu informacije dobavljača.

Uređivanje informacija o dobavljaču

Koristite ovu informaciju za uređivanje informacija o poslužitelju.

1. Izaberite podstablo dobavljača koje želite uređivati.
2. Kliknite **Uređivanje**.
3. Ako uređujete **Default vjerodajnice i referal** koji se koriste za kreiranje cn=Glavni poslužitelj unosa pod cn=configuration, unesite URL za poslužitelj iz kojeg klijent želi primiti ažuriranja replike u polju Default LDAP URL dobavljača. To treba biti valjan LDAP URL (ldap://). U suprotnom preskočite na korak 4.
4. Unesite DN vezanja replikacije za nove vjerodajnice koje želite koristiti.
5. Unesite i potvrdite lozinku vjerodajnice.
6. Kliknite **OK**.

Lozinka za DN dobavljača replikacije može se također promijeniti pomoću naredbe atribut Directory Servera (CHGDIRSVRA). Za promjenu lozinke za veznog DN-a replikacije cn=master u novu lozinku, koristite ovu naredbu:

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

Uklanjanje informacija o dobavljaču

Koristite ovu informaciju za uklanjanje informacija o poslužitelju.

1. Izaberite podstablo dobavljača koje želite ukloniti.
2. Kliknite **Brisanje**.
3. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**.

Podstablo se uklanja iz liste informacija o dobavljaču.

Kreiranje rasporeda replikacije

Koristite ovu informaciju za kreiranje rasporeda replikacije.

Možete neobvezno definirati rasporede replikacije kako bi rasporedili replikacije u određenom vremenu ili da nema replikacije u određenom vremenu. Ako ne koristite raspored, poslužitelj raspoređuje replikaciju uvijek kada se napravi promjena. To je ekvivalentno specificiranju rasporeda s trenutnom replikacijom koja počinje u 12:00 svakog dana.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje rasporedima**.

Na kartici **Tjedni raspored** izaberite podstablo za koje želite kreirati raspored i kliknite na **Prikaži rasporede**. Ako postoje rasporedi, oni se prikazuju u kućici **Tjedni rasporedi**. Kako bi kreirali ili dodali novi raspored:

1. Kliknite **Dodavanje**.
2. Unesite ime za raspored. Na primjer **raspored1**.
3. Za svaki dan, od nedjelje do subote, dnevni raspored je specificiran kao **Ništa**. To znači da nisu raspoređeni događaji za ažuriranje replikacije. Još je aktivan zadnji događaj replikacije, ako je postojao. Budući se radi o novoj replici, pa ne postoje prethodni događaji replikacije, raspored se postavlja na neposrednu replikaciju.
4. Možete izabrati bilo koji dan i kliknuti na **Dodavanje dnevnog rasporeda** kako bi za njega kreirali dnevni raspored replikacije. Ako kreirate dnevni raspored, on postaje default raspored za svaki dan u tjednu. Možete:
   - Zadržati dnevni raspored kao default za svaki dan ili izabrati neki dan i promijeniti raspored natrag na ništa. Vodite računa o tome da je zadnji događaj replikacije koji se je dogodio i dalje aktivan za dan kada nije raspoređen nijedan događaj replikacije.
   - Promijenite dnevni raspored izborom dana i klikom na **Uređivanje dnevnog rasporeda**. Vodite računa o tome da se dnevni raspored odnosi na sve dane koji koriste taj raspored, ne samo na dan koji ste izabrali.
   - Kreirajte drukčiji dnevni raspored tako da izaberete dan i kliknete na **Dodavanje dnevnog rasporeda**. Nakon što kreirate taj raspored, on se dodaje na padajući izbornik **Dnevni raspored**. Taj raspored morate izabrati za svaki dan za koji želite da se koristi raspored.

   Pogledajte “Kreiranje dnevnog rasporeda replikacija” za više informacija o postavljanju dnevnih rasporeda.
5. Kada završite, kliknite na **OK**.

Srodni zadaci

“Pregled rasporeda replikacije” na stranici 163
Za pregled rasporeda replikacije pomoću Web Administration tool-a, slijedite ove korake.

Kreiranje dnevnog rasporeda replikacija

Koristite ovu informaciju za kreiranje dnevnog rasporeda replikacija.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje rasporedima**.

Na kartici **Dnevni raspored** izaberite podstablo za koje želite kreirati raspored i kliknite na **Prikaži rasporede**. Ako postoje rasporedi, oni se prikazuju u kućici **Dnevni rasporedi**. Kako bi kreirali ili dodali novi raspored:

1. Kliknite **Dodavanje**.

2. Unesite ime za raspored. Na primjer **ponedjeljak1**.
3. Izaberite postav vremenske zone, UTC ili lokalno.
4. Izaberite tip replikacije iz padajućeg izbornika:

   Odmah
   Izvodi bilo koja ažuriranja unosa u stanju čekanja od zadnjeg replikacijskog događaja i onda neprekidno ažurira raspored dok se ne dođe do sljedećeg raspoređenog događaja ažuriranja.

   Jednom
   Izvodi sva ažuriranja u stanju čekanja prije vremena pokretanja. Sva ažuriranja učinjena nakon vremena pokretanja čekaju do sljedećeg raspoređenog događaja replikacije.
5. Izaberite početno vrijeme (u lokalnom vremenu poslužitelja) za događaj replikacije.
6. Kliknite **Dodavanje**. Prikazuju se tip događaja replikacije i vrijeme.
7. Dodajte ili uklonite događaje kako bi dovršili svoj raspored. Popis događaja se osvježava u kronološkom poretku.
8. Kada završite, kliknite na **OK**.

Na primjer:

Tip replikacije	Početno vrijeme
Odmah	12:00
Jednom	10:00
Jednom	14:00
Odmah	16:00
Jednom	20:00

U ovom rasporedu do prvog događaja replikacije dolazi u ponoć i ažuriraju se sve promjene u stanju čekanja prije tog vremena. Ažuriranja replikacije se rade onako kako se pojavljuju do 10:00. Ažuriranja napravljena između 10:00 i 14:00 čekaju do 14:00 da bi se replicirala. Sva ažuriranja napravljena između 14:00 i 16:00 čekaju na događaj replikacije koji je raspoređen za 16:00, nakon toga se ažuriranja replikacije nastavljaju do sljedećeg raspoređenog događaja replikacije u 20:00. Sva ažuriranja napravljena nakon 20:00 čekaju do sljedećeg raspoređenog događaja replikacije.

Bilješka: Ako su događaji replikacije raspoređeni previše blizu, moglo bi se desiti da se propusti događaj replikacije ako se još uvijek izvode ažuriranja iz prethodnog događaja kada je raspoređen sljedeći događaj.

Upravljanje redovima replikacije

Koristite ovu informaciju za nadgledanje statusa replikacije za svaki ugovor (red) replikacije koji koristi ovaj poslužitelj.

1. Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje redovima**.
2. Izaberite repliku čijim redom želite upravljati.
3. Ovisno o statusu replike, možete kliknuti na **Odgodi/nastavi** kako bi zaustavili ili pokrenuli replikaciju.
4. Kliknite na **Prisili replikaciju** kako bi replicirali sve promjene u stanju čekanja bez obzira na to kada je raspoređena sljedeća replikacija.
5. Kliknite na **Detalji reda** za više informacija o redu replike. Možete upravljati redom i iz ovog izbora.
6. Kliknite **Pogledaj greške** za dobivanje panela upravljanja greškama replikacije. Odavde možete gledati dnevnik grešaka replikacije, ponovno pokušati neuspjele promjene ili ukloniti unose iz dnevnika.
7. Kliknite na **Osvježi** kako bi ažurirali redove i obrisali poruke poslužitelja.

Ako ste kliknuli na **Detalji reda**, prikazuju se tri kartice:

- Stanje
- Detalji o zadnjem pokušaju

- Promjene još u toku

Kartica **Status** prikazuje ime replike, njezino podstablo, njezin status i zapise o vremenima replikacije. S ovog panela možete odgoditi ili nastaviti replikaciju tako da kliknete na **Nastavak**. Kliknite na **Osvježi** da ažurirate informacije o redu.

Kartica **Detalji zadnjeg pokušaja** vam daje informacije o zadnjem pokušaju ažuriranja. Ako se unos ne može učitati, pritisnite na **Preskoči blokiranje unosa** kako bi nastavili replikaciju sa sljedećim unosom u stanju čekanja. Kliknite na **Osvježi** da ažurirate informacije o redu.

Kartica **Promjene u stanju čekanja** prikazuje sve promjene u stanju čekanja na replici. Ako je replikacija blokirana, možete obrisati sve promjene u stanju čekanja tako da kliknete na **Preskoči sve**. Kliknite na **Osvježi** kako bi ažurirali popis promjena u stanju čekanja tako da odražavaju bilo koje novo ažuriranje ili ažuriranja koja su bila obrađena.

Bilješka: Ako izaberete preskakanje promjena blokiranja, morate osigurati da se poslužitelj potrošača jednom ažurira.

Srodni koncepti

"Tablica grešaka replikacije" na stranici 43
Tablica grešaka replikacije zapisuje neuspjela ažuriranja za kasnije obnavljanje. Kad se replikacija pokrene, broj kvarova prijavljenih za svaki ugovor replikacija se broji. To se brojanje povećava ako ažuriranje rezultira kvarom, a novi se unos dodaje u tablicu.

Srodne reference

"ldapdiff" na stranici 232
Pomoćni programi reda za naredbe LDAP sinkronizacije replike.

Modificiranje postavki dnevnika izgubljeno i nađeno

Dnevnik izgubljeno i nađeno (LostAndFound.log je default ime datoteke) zapisuje greške koje se dešavaju kao rezultat sukoba replikacije. Postoje postavke koje kontroliraju dnevnik izgubljeno i nađeno uključujući lokaciju i maksimum veličine datoteke i arhiviranje starih datoteka dnevnika.

Za modificiranje postavki dnevnika izgubljeno i nađeno, učinite sljedeće:

1. U IBM Tivoli Directory Server Web Administration Tool-u, proširite **Administracija poslužitelja** i zatim **Dnevnici** u području navigacije, kliknite **Modificiraj postavke dnevnika**.
2. 2. Kliknite **Dnevnik izgubljeno i nađeno**.
3. 3. Upišite ime staze i datoteke za dnevnik grešaka. Pazite da datoteka postoji na ldap poslužitelju i da je staza važeća. Default staza dnevnika je *<drive>\idsslapd-<instance-name>\logs*, gdje je *pogon* onaj pogon koji ste specificirali kada ste kreirali instancu directory servera, a *ime instance* je ime instance directory servera. Ako specificirate datoteku koja nije prihvatljivo ime datoteke (na primjer, nevažeća sintaksa ili ako poslužitelj nema prava kreirati i/ili modificirati datoteku), pokušaj ne uspijeva sa sljedećom greškom: LDAP poslužitelj ne želi izvesti operaciju.
4. Ispod **Prag veličine dnevnike (MB)** izaberite prvi kružni izbornik i upišite maksimum veličine dnevnika u megabajtima. Ako ne želite ograničiti veličinu dnevnika, izaberite umjesto toga **Neograničen** kružni izbornik.
5. Ispod **Maksimum arhiva dnevnik** , izaberite jednu od sljedećih opcija:
   - Ako želite specificirati maksimum broja arhiviranih dnevnika, izaberite kružni izbornik s prozorom za uređivanje pored njega. Upišite maksimum broja arhiva koji želite spremiti. Arhiviran dnevnik je raniji dnevnik koji je dosegao svoj prag veličine.
   - Ako ne želite arhivirati dnevnike, izaberite Ne arhive.
   - Ako ne želite ograničiti broj arhiviranih dnevnika, izaberite Neograničeno.
6. Ispod **Staza arhive dnevnika**, izaberite jednu od sljedećih opcija:
   - Ako želite specificirati stazu u kojoj se čuvaju arhive, izaberite kružni izbornik s prozorom za uređivanje pored njega i upišite željenu stazu.
   - Ako želite čuvati arhive u direktoriju u kojem se nalazi datoteka dnevnika, izaberite **Isti direktorij kao datoteka dnevnika** kružni izbornik.

7. Kliknite **Primijeni** za primjenu promjena i nastavak rada s dnevnicima ili kliknite **OK** za spremanje promjena i povratak u panel IBM Tivoli Directory Server uvod u Web administraciju. Kliknite **Odustani** za povratak u panel IBM Tivoli Directory Server uvod u Web administraciju bez spremanja promjena.

Srodne reference

"Pregled replikacije" na stranici 37
Preko replikacije se promjene koje su učinjene na jednom direktoriju šire na još jedan ili više dodatnih direktorija. U stvari, promjena na jednom direktoriju se pojavljuje na više različitih direktorija.

Pregledavanje datoteke dnevnika izgubljeno i nađeno

Datoteka dnevnika replikacije izgubljeno i nađeno može se pregledati pomoću IBM Tivoli Directory Server Web Administration Toola, pomoću opcija datoteke dnevnika ldapexop pomoćnog programa ili izravnim pregledavanjem datoteke.

Za pregled datoteke dnevnika izgubljeno i nađeno pomoću web administration tool-a, proširite **Administraciju poslužitelja** u području navigacije Web administracije i zatim **Dnevnici** u proširenoj listi.

1. Klikni **Pregledaj dnevnik**.
2. U panelu **Pregledaj dnevnike**, izaberite **Dnevnik izgubljeno i nađeno** i kliknite tipku **Pregled**.

Napomena: Administrator direktorija i članovi administrativne grupe su jedini korisnici koji mogu pristupiti tom panelu.

Za pregledanje Dnevnika izgubljeno i nađeno pomoću ldapexop pomoćnog programa, učinite sljedeće iz Qshell:

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

Učinite sljedeće za brisanje Dnevnika izgubljeno i nađeno:

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

Bilješka: Ako ste prijavljeni na i5/OS sistem kao korisnik s *ALLOBJ i *IOSYSCFG posebnim ovlaštenjem ili kao korisnik koji je dobio administratorski pristup u directory server, možete koristiti ldapexop pomoćni program pomoću -m OS400-PRFTKN opcije umjesto dobavljanja administratorskog DN-a i lozinke. Na primjer,

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

Srodne reference

"ldapexop" na stranici 212
Pomoćni program reda za naredbe LDAP proširene operacije.

Postavljanje replikacije preko sigurne veze

Koristite ovu informaciju za postavljanje replikacije preko sigurne veze.

Replikacija preko SSL-a treba biti postavljena u stupnjevima tako da možete raditi provjere u toku procesa.

Prije pokušaja konfiguriranja replikacije preko sigurne veze, trebali bi dovršiti sljedeće zadatke (po bilo kojem redu):

- Konfiguriranje replikacije preko nesigurne veze.
- Konfigurirajte poslužitelj potrošača da prihvati sigurne veze preko sigurnog porta. Provjerite da klijent može koristiti sigurnu vezu na poslužitelj potrošača, na primjer, korištenjem ldapsearch uslužnog programa. Ako želite da poslužitelj dobavljača koristi certifikat za provjeru autentičnosti, kao što je SASL eksterno vezivanje preko SSL, trebate prvo postaviti provjeru autentičnosti vašeg poslužitelja i onda klijent i poslužitelj provjeru autentičnosti, gdje je ″poslužitelj potrošački poslužitelj i klijent je dobavljački poslužitelj.

  Bilješka: Kada je poslužitelj konfiguriran da koristi klijentsku i poslužiteljsku provjeru autentičnosti, svi klijenti koji koriste SSL trebaju imat klijentski certifikat.
- Konfigurirajte poslužitelj dobavljača da vjeruje Izdavaču certifikata koji je izdao potrošački certifikat.

1. U alatu Web administracije, kliknite **Upravljanje topologijom** pod **Upravljanje replikacijom** kategorijom.
2. Izaberite jedan od postojećih argumenata koje želite učiniti sigurnim.

3. Izaberite **Uredi ugovor...** i izaberite korištenje SSL pod uvjetom da koristite ispravni broj porta. 636 je standardni broj sigurnosnog porta.
4. Provjerite da replikacija preko ugovora radi ispravno.

Ako samo želite postaviti replikaciju da provjerite ovlaštenje koristeći DN i lozinku preko sigurne veze, prethodni koraci su to napravili za vas. Provjera autentičnosti korištenjem klijentskih certifikata zahtjeva drugačije objekte vjerodajnica za korištenje od strane dobavljača poslužitelja u svom ugovoru, kao i konfiguriranje potrošačkog poslužitelja da prihvati poslužitelja dobavljača.

Zadaci topologije replikacije

Koristite ovu informaciju za upravljanje topologijama repliciranih podstabala.

Topologije su specifične za replicirana podstabla.

Pregled topologije

Koristite ovu informaciju za pregled topologije podstabla.

Bilješka: Poslužitelj mora raditi da bi se mogao izvesti ovaj zadatak.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje topologijom**.

Izaberite podstablo koje želite pregledati i kliknite na **Pokazivanje topologije**.

Topologija se prikazuje u popisu Topologija replikacije. Proširite topologije tako da kliknete na plave trokutiće. Iz tog popisa možete:

- Dodati repliku.
- Uređivati informacije na postojećoj replici.
- Promijeniti na različit poslužitelj dobavljača za repliku ili promovirati repliku u glavni poslužitelj.
- Obrisati repliku.
- Pregled rasporeda replikacije

Dodavanje replika poslužitelja

Koristite ovu informaciju za kreiranje replika poslužitelja.

Bilješka: Ovdje opisani koraci objašnjavaju kako dodati repliku kroz web administracijski zadatak, te su dio ukupne obrade koja uključuje ostale korake potrebne za ispravno inicijaliziranje novog poslužitelja. Pogledajte poglavlje u niže navedenim odgovarajućim vezama.

Bilješka: Poslužitelj mora raditi da bi se mogao izvesti ovaj zadatak.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje topologijom**.

1. Izaberite podstablo koje želite replicirati i kliknite na **Pokazivanje topologije**.
2. Kliknite na strelicu uz izbor **Topologija replikacije** kako bi proširili popis poslužitelja dobavljača.
3. Izaberite poslužitelj dobavljača i kliknite na **Dodavanje replike**.
4. Na karticu **Poslužitelj** prozora **Dodavanje replike**:
   a. Unesite ime hosta i broj porta za repliku koju kreirate. Default port je 389 za ne-SSL i 636 za SSL. To su potrebna polja.
   b. Izaberite da li ćete omogućiti SSL komunikacije.
   c. Unesite ime replike ili ostavite to polje praznim kako bi se koristilo ime hosta.
   d. Unesite ID replike. Ako se izvodi poslužitelj na kojem kreirate repliku, kliknite na **Dobavi ID replike** kako bi se automatski popunilo to polje. To je nužno polje ako će poslužitelj kojeg dodajete biti ravnopravan poslužitelj ili poslužitelj proslјeđivanja. Preporuča se da svi poslužitelji budu na istom izdanju.

e. Unesite opis replika poslužitelja.

5. Na kartici **Dodatni**,
   - Specificirajte vjerodajnice koje replika koristi za komuniciranje s glavnim poslužiteljem.

     Bilješka: Web administracijski alat vam omogućava da definirate vjerodajnice u ovim mjestima:
     - **cn=replication,cn=localhost**, čuvaju vjerodajnice samo na poslužitelju koji ih koristi.
     - Unutar repliciranog podstabla, u tom slučaju su vjerodajnice replicirane s ostatkom podstabla. Vjerodajnice koje su smještene u replicirano podstablo su kreirane ispod **ibm-replicagroup=default** unosa za to podstablo.

     Smještanje vjerodajnica u cn=replication,cn=localhost se smatra sigurnijim. Vjerodajnice smještene u replicirano podstablo kreiraju se ispod unosa ibm-replicagroup=default za to podstablo.
   - Kliknite **Biranje**.
     - Izaberite lokaciju za vjerodajnice koje želite koristiti. Preferira se da to bude cn=replication,cn=localhost.
     - Kliknite na **Prikaži vjerodajnice**.
     - Proširite popis vjerodajnica i izaberite jednu koju želite koristiti.
     - Kliknite **OK**.

       Pogledajte Kreiranje replikacijskih vjerodajnica za dodatne informacije o vjerodajnicama ugovora.
   - Specificirajte raspored replikacije iz padajućeg popisa ili kliknite na **Dodavanje** da kreirate jedan. Pogledajte Kreiranje replikacijskih rasporeda.
   - Iz popisa sposobnosti dobavljača možete poništiti izbor bilo kojih sposobnosti za koje ne želite da se repliciraju na potrošača.

     Ako vaša mreža ima različite poslužitelje na različitim izdanjima, na novijim izdanjima su dostupne sposobnosti koje nisu dostupne na ranijim izdanjima. Neke sposobnosti, kao što su ACL-ovi filtera i lozinka politike, koriste operativne atribute koji su replicirani s drugim promjenama. U većini slučajeva, ako su te funkcije korištene, želite da ih svi poslužitelji podržavaju. Ako svi poslužitelji ne podržavaju neku sposobnost, nemojte ga koristiti. Na primjer, ne želite da različiti ACL-ovi budu učinkoviti na svakom poslužitelju. Međutim, postoje neki slučajevi kada ćete možda željeti koristiti sposobnost na poslužiteljima koji ju podržavaju, a da se promjene koje se odnose na sposobnost ne repliciraju na poslužitelj koji ne podržava sposobnost. U takvim slučajevima možete koristiti listu sposobnosti kako bi označili da ne želite da se neke sposobnosti repliciraju.
   - Izaberite jednonitni ili višenitni za metodu replikacije. Ako specificirate višenitni, morate specificirati i broj (između 2 i 32) veza koje će se koristiti za replikaciju. Default broj veza je 2.
   - Kliknite **OK** za kreiranje replike.

6. Prikazuje se poruka koja označava da se moraju poduzeti dodatne akcije. Kliknite na **OK**.

   Bilješka: Ako dodajete više poslužitelja kao dodatne replike ili kreirate kompleksnu topologiju, nemojte nastaviti s Kopiranjem podataka u repliku ili Dodavanjem informacija o dobavljaču u novu repliku dok ne završite definiranje topologije na glavnom poslužitelju. Ako kreirate *masterfile.ldif* nakon što ste dovršili topologiju, ona sadrži unose direktorije glavnog poslužitelja i potpunu kopiju ugovora topologije. Kada učitate tu datoteku na svakog od poslužitelja, svaki poslužitelj ima iste informacije.

Srodni zadaci

"Postavljanje gateway topologije" na stranici 150
Koristite ovu informaciju za postavljanje gateway topologije.

Dodavanje peer-master ili gateway poslužitelja

Ovo poglavlje sadrži informacije o tome kako kreirati novi peer-master ili gateway poslužitelj.

Bilješka: Ovdje opisani koraci objašnjavaju kako dodati peer-master ili gateway poslužitelj kroz web administracijski zadatak, te su dio ukupne obrade koja uključuje ostale korake potrebne za ispravno inicijaliziranje novog poslužitelja. Pogledajte poglavlje u niže navedenim odgovarajućim vezama.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje topologijom**.

1. Izaberite podstablo koje želite replicirati i kliknite na **Pokazivanje topologije**.
2. Kliknite okvir pored **Replikacijska topologija** za proširenje liste poslužitelja dobavljača, ako želite pogledati postojeću topologiju.
3. Kliknite **Dodavanje mastera**.

Na kartici **Poslužitelj** prozora **Dodavanje mastera**:

- Upišite host ime i broj porta za poslužitelj koji kreirate. Default port je 389 za ne-SSL i 636 za SSL. To su potrebna polja.
- Izaberite da li ćete omogućiti SSL komunikacije.
- Izaberite želite li kreirati poslužitelj kao gateway poslužitelj.
- Upišite ime poslužitelja ili ostavite to polje prazno te koristite host ime.
- Upišite **ID poslužitelja**. Ako poslužitelj na kojem kreirate peer-master radi, kliknite Dohvati ID poslužitelja za automatsko prethodno popunjavanje tog polja.
- Upišite opis poslužitelja.
- Morate specificirati vjerodajnice koje poslužitelj koristi za komunikaciju s drugim glavnim poslužiteljem. Kliknite **Biranje**.

  Bilješka: Web Administration Tool omogućava definiranje vjerodajnica na sljedećim mjestima:
  - **cn=replication,cn=localhost**, vjerodajnice se čuvaju samo na poslužitelju koji ih koristi. Smještanje vjerodajnica u cn=replication,cn=localhost se smatra sigurnijim.
  - **cn=replication,cn=IBMpolicies**, koji je dostupan čak i kad poslužitelj s kojim pokušavate dodati repliku nije isti poslužitelj na koji ste spojeni s Web Administration Tool. Vjerodajnice smještene na tu lokaciju replicirane su na poslužitelje.

    Bilješka: Lokacija cn=replication,cn=IBMpolicies je dostupna jedino ako je podrška IBMpolicies OID, 1.3.18.0.2.32.18, prisutna pod ibm-supportedcapabilities korijenskog DSE-a.
  - Unutar repliciranog podstabla, u tom slučaju su vjerodajnice replicirane s ostatkom podstabla. Vjerodajnice koje su smještene u replicirano podstablo su kreirane ispod **ibm-replicagroup=default** unosa za to podstablo.
    1. Izaberite lokaciju za vjerodajnice koje želite koristiti. Preferira se da to bude cn=replication,cn=localhost.
    2. Ako ste već kreirali skup vjerodajnica, kliknite Pokazivanje vjerodajnica.
    3. Proširite popis vjerodajnica i izaberite jednu koju želite koristiti.
    4. Kliknite OK.
    5. Ako nemate postojeće vjerodajnice, kliknite Dodavanje za kreiranje vjerodajnica.

Na kartici **Dodatno**:

1. Specificirajte raspored replikacije iz padajućeg popisa ili kliknite na **Dodavanje** da kreirate jedan. Pogledajte Kreiranje replikacijskih rasporeda.
2. Iz popisa sposobnosti dobavljača možete poništiti izbor bilo kojih sposobnosti za koje ne želite da se repliciraju na potrošača.

   Ako vaša mreža ima različite poslužitelje na različitim izdanjima, na novijim izdanjima su dostupne sposobnosti koje nisu dostupne na ranijim izdanjima. Neke sposobnosti, poput filterskih ACL-ova (Filtrirane liste kontrole pristupa) i politike lozinka (Postavljanje svojstva politike lozinka), iskoristite operativne atribute koji su replicirani s drugim promjenama. U većini slučajeva, ako se ta svojstva koriste, svi ih poslužitelji trebaju podržavati. Ako svi poslužitelji ne podržavaju neku sposobnost, nemojte ga koristiti. Na primjer, ne želite da različiti ACL-ovi budu učinkoviti na svakom poslužitelju. Međutim, postoje neki slučajevi kada ćete možda željeti koristiti sposobnost na poslužiteljima koji ju podržavaju, a da se promjene koje se odnose na sposobnost ne repliciraju na poslužitelj koji ne podržava sposobnost. U takvim slučajevima možete koristiti listu sposobnosti kako bi označili da ne želite da se neke sposobnosti repliciraju.

3. Označite kontrolnu kućicu **Dodavanje informacije o vjerodajnici potrošača**, ako želite omogućiti dinamičko ažuriranje vjerodajnica dobavljača. Takav izbor automatski ažurira informaciju o dobavljaču u konfiguracijskoj datoteci poslužitelja koji kreirate. To omogućuje repliciranje informacija o topologiji na poslužitelj.
   - Upišite Administracijski DN za to, potrošača, poslužitelja. Na primjer, cn=root.

     Bilješka: Ako je administratorski DN koji je kreiran za vrijeme obrade konfiguracije poslužitelja bio cn=root, tada upišite puni administratorski DN. Ne koristite samo root.
   - Upišite Administracijsku lozinku za to, potrošača, poslužitelja. Na primjer secret.
4. Kliknite **OK**.
5. Ugovori dobavljača i potrošača ispisani su između novog glavnog poslužitelja i bilo kojeg postojećeg poslužitelja. Maknite oznaku sa svih ugovora koje ne želite kreirati. To je posebno važno ako kreirate gateway poslužitelj.
6. Kliknite **Nastavak**.
7. Moguće je prikazivanje poruka s napomenom da se moraju poduzeti dodatne akcije. Izvedite ili zabilježite odgovarajuće akcije. Kada završite, kliknite **OK**.
8. Dodavanje odgovarajućih vjerodajnica.

   Bilješka: U nekim slučajevima pojavit će se panel Biranje vjerodajnice i tražiti vjerodajnicu koja je locirana na mjestu različitom od cn=replication,cn=localhost. U takvim situacijama morate dati objekt vjerodajnice koji je smješten na mjestu osim cn=replication,cn=localhost. Izaberite vjerodajnicu koju će podstablo koristiti iz postojećeg skupa vjerodajnica ili kreirajte nove vjerodajnice.
9. Označite kontrolnu kućicu **Dodavanje informacije o vjerodajnici potrošača**, ako želite omogućiti dinamičko ažuriranje vjerodajnica dobavljača. Takav izbor automatski ažurira informaciju o dobavljaču u konfiguracijskoj datoteci poslužitelja koji kreirate. To omogućuje repliciranje informacija o topologiji na poslužitelj.
   - Upišite Administracijski DN za to, potrošača, poslužitelja. Na primjer cn=root.

     Bilješka: Ako je administratorski DN koji je kreiran za vrijeme obrade konfiguracije poslužitelja bio cn=root, tada upišite puni administratorski DN. Ne koristite samo root.
   - Upišite Administracijsku lozinku za to, potrošača, poslužitelja. Na primjer, secret.
10. Kliknite **OK** za kreiranje peer-mastera.
11. Moguće je prikazivanje poruka s napomenom da se moraju poduzeti dodatne akcije. Izvedite ili zabilježite odgovarajuće akcije. Kada završite, kliknite **OK**.

Bilješka: Ako se izabere vanjski objekt vjerodajnice dok dodajete vjerodajnice o potrošačima za vrijeme operacije Dodavanje mastera pomoću Web Administracijskih alata, tada se trebaju konfigurirati sljedeće postavke na stroju gdje radi IBM WebSphere Application Server:

- WAS_HOME\java\jre\lib\ext\ sadrži sljedeće jar datoteke:
  - ibmjceprovider.jar
  - ibmpkcs.jar
  - ibmjcefw.jar
  - local_policy.jar
  - US_export_policy.jar
  - ibmjlog.jar
  - gsk7cls.jar
- WAS_HOME\java\jre\lib\security\java.security datoteka mora imati sljedeće svije linije za registraciju CMS dobavljača i JCE dobavljača:

  ```
  security.provider.2=com.ibm.spi.IBMCMSProvider
  security.provider.3=com.ibm.crypto.provider.IBMJCE
  ```
- Ponovno pokrenite IBM WebSphere Application Server.
- Gskit mora biti instaliran i gsk7\lib mora biti u sistemskoj stazi.

- Kako bi Web Administration Tool mogao čitati glavnu datoteku koja sadrži informacije o vjerodajnicama koje glavni poslužitelj koristi za povezivanje na repliku i kreiranje vjerodajnica na repliku, glavna datoteka mora biti prisutna u C:\temp za Windows platforme i u /tmp za UNIX.

Srodni zadaci

"Postavljanje gateway topologije" na stranici 150
Koristite ovu informaciju za postavljanje gateway topologije.

Upravljanje gateway poslužiteljima

Ovo poglavlje daje informacije o upravljanju gateway poslužiteljima. Možete odrediti treba li glavni poslužitelj imati ulogu gateway poslužitelja na stranici replikacije.

Za označavanje glavnog poslužitelja kao gateway poslužitelja, proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite **Upravljanje topologijom**.

1. Izaberite podstablo koje želite pregledati i kliknite na **Pokazivanje topologije**.
2. Kliknite **Upravljanje gateway poslužiteljima**.
3. Izaberite poslužitelj iz kućice **Glavni poslužitelji** koji želite pretvoriti u gateway poslužitelj.
4. Kliknite **Napravi gateway**. Poslužitelj je premješten iz kućice **Glavni poslužitelji** u kućicu **Gateway poslužitelji**.
5. Kliknite **OK**.

Uklanjanje uloge gateway poslužitelj od glavnog poslužitelja.

1. Kliknite **Upravljanje gateway poslužiteljima**.
2. Izaberite poslužitelj iz kućice **Gateway poslužitelji** koji želite pretvoriti u glavni poslužitelj.
3. Kliknite **Napravi glavni poslužitelj**. Poslužitelj je premješten iz kućice **Gateway poslužitelji** u kućicu **Glavni poslužitelji**.
4. Kliknite **OK**.

Bilješka: Zapamtite da može postojati samo jedan gateway poslužitelj po stranici replikacije. Kada kreirate dodatne gateway poslužitelje u svojoj topologiji, Web Administration Tool tretira gateway kao ravnopravni poslužitelj i kreira ugovore za sve poslužitelje u topologiji. Pazite da deselektirate sve ugovore koji nisu s ostalim gateway poslužiteljima ili u sklopu vlastite stranice replikacije gatewaya.

Pogledajte poglavlje Postavljanje gateway topologije u niže navedenim odgovarajućim vezama za više informacija.

Srodni zadaci

"Postavljanje gateway topologije" na stranici 150
Koristite ovu informaciju za postavljanje gateway topologije.

Pregledavanje informacija o poslužitelju

Možete gledati ime poslužitelja, ime hosta, port, ID poslužitelja, ulogu, način konfiguracije, ime instance i sigurnost iz panela Pregled poslužitelja.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije Web Administration Tool-a i kliknite **Upravljanje topologijom**.

1. Izaberite podstablo koje želite pregledati i kliknite na **Pokazivanje topologije**.
2. Izaberite poslužitelj koji želite pregledati.
3. Kliknite **Pregled poslužitelja** za prikaz panela pregled poslužitelja.

Panel Pregled poslužitelja prikazuje sljedeće informacije:

Ime poslužitelja
Ovo polje prikazuje ime poslužitelja na kojem instanca direktorija radi. Ta se informacija prikazuje u formatu hostname:port.

Ime hosta
Ovo polje prikazuje ime hosta stroja na kojem instanca directory servera radi.

Port Ovo polje instanca prikazuje nesigurni port na kojem poslužitelj sluša.

ID poslužitelja
Ovo polje prikazuje jedinstveni ID dodijeljene poslužitelju kod prvog pokretanje poslužitelja. Taj se ID koristi u topologiji replikacije za uloge poslužitelja.

Uloga Ovo polje prikazuje konfiguriranu ulogu poslužitelja u topologiji replikacije.

Način konfiguracije
Ovo polje identificira radi li poslužitelj u načinu konfiguracije. Ako je TRUE, poslužitelj je u načinu konfiguracije. Ako je FALSE, poslužitelj nije u načinu konfiguracije.

Ime instance
Ovo polje prikazuje ime instance directory servera koji radi na poslužitelju.

Sigurnost
Ovo polje prikazuje siguran SSL port koji poslužitelj sluša.

Ime poslužitelja, ID i uloga te informacije o potrošaču se prikazuju.

Pregled rasporeda replikacije

Za pregled rasporeda replikacije pomoću Web Administration tool-a, slijedite ove korake.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije Web Administration Tool-a i kliknite **Upravljanje topologijom**.

1. Izaberite podstablo koje želite pregledati i kliknite na **Pokazivanje topologije**.
2. Izaberite glavni ili gateway poslužitelj koji želite pregledati.
3. Klikni **Pregledaj raspored**.

Ako raspored replikacije postoji između izabranog poslužitelja i njegovih potrošača, oni se prikazuju. Možete modificirati ili brisati te rasporede. Ako ne postoje rasporedi, a vi jedan želite kreirati, morate koristiti funkciju **Upravljanje rasporedima** iz područja navigacije Web Administration Toola. Pogledajte Kreiranje rasporeda replikacije u niže navedenim odgovarajućim vezama za informacije o upravljanju rasporedima.

Srodni zadaci

“Kreiranje rasporeda replikacije” na stranici 154
Koristite ovu informaciju za kreiranje rasporeda replikacije.

Uređivanje ugovora

Koristite ovu informaciju za uređivanje ugovora replikacije.

Možete promijeniti dodatne informacije za repliku:

1. Na kartici **Poslužitelj** možete jedino promijeniti:
   - Ime glavnog poslužitelja
   - Port
   - Omogućavanje SSL-a
   - Opis
2. Na kartici **Dodatno** možete promijeniti:
   - Vjerodajnice - pogledajte “Kreiranje vjerodajnica replikacije” na stranici 141.
   - Rasporede replikacija - pogledajte “Kreiranje rasporeda replikacije” na stranici 154.
   - Promijenite svojstva koja su replicirana na repliku potrošača. Iz popisa sposobnosti dobavljača možete poništiti izbor bilo kojih sposobnosti za koje ne želite da se repliciraju na potrošača.
3. Kada završite, kliknite na **OK**.

Premještanje ili promoviranje poslužitelja

Koristite ovu informaciju za premještanje ili promoviranje poslužitelja.

1. Izaberite poslužitelj koji želite i kliknite na **Premjesti**.
2. Izaberite poslužitelj na kojeg želite premjestiti repliku ili izaberite **Topologija replikacije** kako bi promovirali repliku na glavnog poslužitelja. Kliknite **Premjesti**.
3. U nekim će slučajevima iskočiti panel Biranje vjerodajnice koji će od vas tražiti vjerodajnicu koja je smještena negdje drugdje, a ne na cn=replication,cn=localhost. U takvim situacijama morate osigurati objekt vjerodajnice koji se nalazi negdje drugdje, a ne na cn=replication,cn=localhost. Izaberite vjerodajnice koje će koristiti podstablo, oblikujte postojeće skupove vjerodajnica ili kreirajte nove vjerodajnice. Pogledajte “Kreiranje vjerodajnica replikacije” na stranici 141.
4. **Kreiraj dodatne ugovore dobavljača** se prikazuje. Izaberite ugovore dobavljača koji su prikladni za ulogu poslužitelja. Na primjer, ako se replika poslužitelj promovira da bude ravnopravan poslužitelj, morate kreirati ugovore dobavljača sa svim drugim poslužiteljima i njihovim replikama prve razine. Ti ugovori omogućuju promoviranom poslužitelju da se ponaša kao dobavljač za druge poslužitelje i njihove replike. Postojeći ugovori dobavljača iz drugih poslužitelja na novo promovirane poslužitelje su i dalje aktivni i ne trebaju se ponovno kreirati.
5. Kliknite **OK**.

Promjena u stablu topologije odražava premještanje poslužitelja.

Srodni zadaci

“Kreiranje kompleksne topologije s ravnopravnom replikacijom” na stranici 148
Koristite ovu informaciju za kreiranje kompleksne topologije s ravnopravnom replikacijom.

Spuštanje glavnog na nižu razinu

Koristite ovu informaciju za promjenu uloge poslužitelja iz glavnog u repliku.

Da promijenite ulogu poslužitelja iz glavnog na repliku, napravite sljedeće:

1. Povežite Web administracijski alat na poslužitelj koji želite degradirati.
2. Kliknite na **Upravljanje topologijom**.
3. Izaberite podstablo i kliknite na **Prikaz topologije**.
4. Obrišite sve ugovore za poslužitelj koji želite degradirati.
5. Izaberite poslužitelj koji ćete degradirati i kliknite na **Premjesti**.
6. Izaberite poslužitelj pod koji ćete smjestiti poslužitelj koji ste degradirali i kliknite na **Premjesti**.
7. Kao što bi to napravili i za novu repliku, kreirajte nove ugovore dobavljača između poslužitelja koji ste degradirali i njegovog dobavljača. Pogledajte “Kreiranje poslužitelja replike” na stranici 143 radi uputa.

Repliciranje podstabla

Koristite ovu informaciju za repliciranje podstabla.

Bilješka: Poslužitelj mora raditi da bi se mogao izvesti ovaj zadatak.

Proširite kategoriju **Upravljanje replikacijom** u području navigacije i kliknite na **Upravljanje topologijom**.

1. Kliknite na **Dodavanje podstabla**.
2. Unesite DN podstabla koje želite replicirati ili kliknite na **Pregled** da proširite unose i izaberete unos koji će biti korijen podstabla.
3. Unesite URL referal glavnog poslužitelja. To mora biti u obliku LDAP URL-a, na primjer:
   `ldap://<myservername>.<mylocation>.<mycompany>.com`
4. Kliknite **OK**.

Novi se poslužitelj prikazuje na panelu Upravljanje topologijom ispod naslova **Replicirana podstabla**

Uređivanje podstabla

Koristite ovu informaciju za promjenu URL-a glavnog poslužitelja kojem ovo podstablo i njegove replike šalju ažuriranja. To trebate učiniti ako promijenite broj porta ili host ime glavnog poslužitelja ili promijenite glavni poslužitelj u različit poslužitelj.

1. Izaberite podstablo koje želite uređivati.
2. Kliknite na **Uredi podstablo**.
3. Unesite URL referal glavnog poslužitelja. To mora biti u obliku LDAP URL-a, na primjer:
   `ldap://<mynewservername>.<mylocation>.<mycompany>.com`

Ovisno o ulozi poslužitelja na tom podstablu (da li je glavni, replika ili prosljeditelj), na panelu će se pojavljivati različite oznake i gumbi.

- Kada je uloga podstabla replika, prikazuje se oznaka koja označava da se poslužitelj ponaša kao replika ili prosljeditelj, zajedno s gumbom **Napravi poslužitelj glavnim**. Ako se klikne na taj gumb, onda poslužitelj na kojeg je povezan Web administracijski alat postaje glavni poslužitelj.
- Kada je podstablo konfigurirano za replikaciju samo dodavanjem pomoćnih klasa (nema default grupe i podunosa), onda se prikazuje oznaka **To podstablo nije replicirano** zajedno s gumbom **Repliciraj podstablo**. Ako se klikne na taj gumb, dodaje se default grupa i podunos tako da poslužitelj s kojim je povezan Web administracijski alat postane glavnim.
- Ako nisu pronađeni podunosi za glavne poslužitelje, prikazuje se oznaka **Nije definiran glavni poslužitelj za to podstablo** zajedno s gumbom pod nazivom **Napravi poslužitelj glavnim**. Ako se klikne na taj gumb, dodaje se nedostajući podunos tako da poslužitelj s kojim je povezan Web administracijski alat postane glavnim.

Uklanjanje podstabla

Koristite ovu informaciju za uklanjanje podstabla.

1. Izaberite podstablo koje želite ukloniti.
2. Kliknite na **Brisanje podstabla**.
3. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**.

Podstablo se uklanja iz popisa **Replicirano podstablo**.

Bilješka: Ta će operacija uspjeti samo ako je prazan unos ibm-replicaGroup=default.

Umirivanje podstabla

Koristite ovu informaciju za umirivanje podstabla.

Ta funkcija je korisna kada želite raditi održavanje ili promjene na topologiji. Ona minimizira broj ažuriranja koja se mogu napraviti na poslužitelju. Umireni poslužitelj ne prihvaća zahtjeve klijenta. Prihvaća zahtjeve samo od administratora koji koristi kontrolu Administracije poslužitelja.

Ta funkcija je Booleova.

1. Kliknite na **Umiri/Uznemiri** kako bi umirili podstablo.
2. Kada se od vas zatraži da potvrdite akciju, kliknite na **OK**.
3. Kliknite na **Umiri/Uznemiri** kako bi podstablo izašlo iz umirenog stanja.
4. Kada se od vas zatraži da potvrdite akciju, kliknite na **OK**.

Uređivanje lista kontrole pristupa

Ovo poglavlje sadrži informacije o potrebnim ovlaštenjima za uređivanje lista kontrole pristupa (ACL-ova) i osigurava informacije o radu s ACL-ovima.

Informacije o replikaciji (podunosi replike, ugovori replikacije, rasporedi, možda i vjerodajnice) su pohranjene pod posebnim objektom, **ibm-replicagroup=default**. Objekt ibm-replicagroup se nalazi odmah ispod unosa korijena repliciranog podstabla. Po defaultu, to podstablo nasljeđuje ACL iz unosa korijena repliciranog podstabla. Taj ACL možda neće biti prikladan za kontroliranje pristupa informacijama replikacije.

Potrebna ovlaštenja:

- Replikacija kontrole - Morate imati pristup za pisanje na ibm-replicagroup=default objekt (ili biti vlasnik/administrator).
- Replikacija kaskadne kontrole - Morate imati pristup za pisanje na ibm-replicagroup=default objekt (ili biti vlasnik/administrator).
- Red kontrole - Morate imati pristup za pisanje na ugovor replikacije.

Kako bi pregledali svojstva ACL-a korištenjem Web administracijskog alata i kako bi radili s ACL-ovima, pogledajte “Zadaci Liste kontrole pristupa (ACL)” na stranici 201.

Pogledajte “Lista kontrole pristupa” na stranici 62 za dodatne informacije.

Zadaci svojstava sigurnosti

Koristite ovu informaciju za upravljanje zadacima sigurnosti.

Poslužitelj direktorija ima mnogo mehanizama da osigura sigurnost vaših podataka. One uključuju upravljanje lozinkama, šifriranje koristeći SSL i TLS, Kerberos provjeru ovlaštenja i DIGEST-MD5 provjeru ovlaštenja. Radi više informacija o konceptima sigurnosti, pogledajte “Sigurnost Poslužitelja direktorija” na stranici 50.

Srodni koncepti

“Sigurnost Poslužitelja direktorija” na stranici 50
Saznajte kako se raznolikost funkcija može koristiti da učini vaš Directory Server sigurnim.

Zadaci lozinki

Koristite ovu informaciju za upravljanje zadacima lozinki.

Da bi upravljali lozinkama, proširite **Upravljanje sigurnosnim svojstvima** kategorijom u navigacijskom području od Web administracijskog alata i izaberite **Politika lozinke** karticu.

Srodni koncepti

“Politika lozinke” na stranici 75
Kada se koriste LDAP poslužitelji za provjeru autentičnosti, važno je da LDAP poslužitelj podržava politike koje se odnose na istek dozvole, neuspjeli pokušaj prijave i pravila lozinke. Poslužitelj direktorija osigurava konfigurabilnu podršku za sve tri vrste politika.

Postavljanje svojstva politike lozinke:

Koristite ovu informaciju za postavljanje svojstva politike lozinke.

Da postavite politiku lozinke, poduzmite ove korake:

Bilješka: Ti koraci objašnjavaju kako postaviti politiku lozinke korisnika. Pogledajte poglavlje Postavljanje administracijske lozinke i politike zaključavanje u niže navedenim odgovarajućim vezama kako biste saznali o politici administrativne lozinke koja se primjenjuje na članove administrativne grupe.

1. Proširite **Upravljanje svojstvima sigurnosti** u navigacijskom području alata Web administracije i izaberite **Politika lozinke**. Taj panel prikazuje zaštićeno polje **Atribut lozinke** koje sadrži ime atributa koji politika lozinke koristi.
2. Izaberite tip šifriranja lozinke iz padajuće liste:

   nijedan
   Lozinke se pohranjuju dvosmjerno šifrirane u validacijskoj listi i dohvaćaju se kao dio unosa u originalnom čistom tekstualnom formatu. Vrijednost QRETSVRSEC sistema mora biti postavljena na 1 za upotrebu ove postavke.

   šifriranje
   Lozinke kodira UNIX algoritam za kodiranje prije nego što se pohranjuju u direktorij.

SHA-1 Lozinke su kodirane pomoću SHA-1 algoritma kodiranja prije nego što su pohranjene u direktoriju.

MD5 Lozinke kodira MD5 algoritam za kodiranje prije nego što se pohranjuju u direktorij.

AES128
Lozinke šifrira AES128 algoritam prije nego što se pohranjuju u direktorij i dohvaćaju se kao dio unosa u originalnom čistom formatu.

AES192
Lozinke šifrira AES192 algoritam prije nego što se pohranjuju u direktorij i dohvaćaju se kao dio unosa u originalnom čistom formatu.

AES256
Lozinke šifrira AES256 algoritam prije nego što se pohranjuju u direktorij i dohvaćaju se kao dio unosa u originalnom čistom formatu.

Bilješka: AES nije podržan na pred-V6R1 LDAP poslužiteljima. Ako su AES šifrirane lozinke eksportirane i zatim importirane u pred-V6R1 poslužitelj, lozinke neće biti upotrebljive.

Ako se istovremeno koristi AES šifriranje i višestruki poslužitelji, svi ti poslužitelji bi trebali koristiti istu AES lozinku i salt. Administrator mora pratiti lozinku dok konfiguracija poslužitelja prikazuje dostupan konfigurirani salt. Administrator treba upisati odgovarajuću AES lozinku i salt kod postavljanja dodatnog poslužitelja za upotrebu AES-a.

Za više informacija, pogledajte poglavlje Šifriranje lozinke u niže navedenim odgovarajućim vezama.

3. Izaberite **Omogućena politika lozinke** da omogućite politiku lozinke.

   Bilješka: Ako politika lozinke nije omogućena, niti jedna od drugih funkcija na ovom ili drugim panelima lozinke nisu dostupne dok se kontrolna kućica ne omogući. Po defaultu, politika lozinke je onemogućena.
4. Izaberite kontrolnu kućicu **Korisnik može promijeniti lozinku** da navedete da li korisnik može promijeniti lozinku.
5. Izaberite kontrolnu kućicu **Korisnik mora promijeniti lozinku nakon resetiranja** da navedete da li korisnik mora promijeniti lozinku nakon prijave s resetiranom lozinkom.
6. Izaberite kontrolnu kućicu **Korisnik mora poslati lozinku kod promjene** da navedete da li korisnik, nakon početne prijave, treba navesti lozinku ponovno, prije nego što ju može promijeniti.
7. Postavite granicu isteka lozinke. Kliknite radio gumb **Lozinka nikad ne ističe** da navedete da se lozinka ne treba mijenjati u određenim vremenskim intervalima ili kliknite na radio gumb **Dani** i navedite vremenski interval, u danima, kad se lozinka treba resetirati.
8. Navedite da li sistem izdaje upozorenje o isteku lozinke prije nego što lozinka istekne.

   Ako kliknete **Nemoj upozoriti** korisnik nije upozoren prije nego što prethodna lozinka istekne. Korisnik ne može pristupiti direktoriju dok administrator ne kreira novu lozinku.

   Ako kliknete na **Dani prije isteka** i navedete broj dana (n), korisnik prima upozorenje za promjenu lozinke svaki put kad se prijavi, počevši s n dana prije nego što lozinka istekne. Korisnik ipak može pristupiti direktoriju dok lozinka ne istekne.
9. Navedite koliko puta, ako uopće, se korisnik može prijaviti nakon što lozinka istekne. Ovaj izbor omogućava korisniku da pristupi direktoriju kad mu lozinka istekne.
10. Kliknite **OK**.

Bilješka: Možete koristiti i ldapmodify pomoćni program (pogledajte “ldapmodify i ldapadd” na stranici 205) za postavljanje politike lozinke.

Za više informacija o politici lozinke, pogledajte “Politika lozinke” na stranici 75.

Srodni koncepti

“Šifriranje lozinke” na stranici 53
IBM Tivoli Directory Server omogućuje sprječavanje neovlaštenog pristupa korisničkim lozinkama. Administrator

može konfigurirati poslužitelj da šifrira userPassword vrijednosti atributa u jednosmjerni format šifriranja ili u dvosmjerni format šifriranja. Šifrirane lozinke su označene s imenom algoritma šifriranja tako da lozinke šifrirane u različitim formatima mogu istodobno postojati u direktoriju. Kad je konfiguracija šifriranja promijenjena, postojeće šifrirane lozinke ostaju nepromijenjene i nastavljaju rad.

Srodni zadaci

"Postavljanje administrativne lozinke i politike zaključavanja"
Politika administrativne lozinke se postavlja jedino pomoću reda za naredbe. Web administration tool ne podržava politiku administrativne lozinke.

Postavljanje administrativne lozinke i politike zaključavanja:

Politika administrativne lozinke se postavlja jedino pomoću reda za naredbe. Web administration tool ne podržava politiku administrativne lozinke.

Bilješka: Morate provjeriti autentičnost kao i5/OS korisnik s *ALLOBJ i *IOSYSCFG posebnim ovlaštenjima.

Za uključivanje politike administrativne lozinke s EAL4 sigurnom konfiguracijom, izdajte sljedeću naredbu:

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

gdje <filename> sadrži:

```
dn: cn=pwdPolicy Admin,cn=Configuration
changetype: modify
replace: ibm-slapdConfigPwdPolicyOn
ibm-slapdConfigPwdPolicyOn: true
```

Za omogućavanje politike administrativne lozinke i modificiranje default postavki, izdajte sljedeću naredbu:

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

gdje <filename> sadrži:

```
dn: cn=pwdPolicyAdmin,cn=Configuration
changetype: modify
zamijeniti: ibm-slapdConfigPwdPolicyOn
ibm-slapdConfigPwdPolicyOn: TRUE
-
zamijeniti: pwdlockout
pwdlockout: TRUE
#izabrati TRUE za omogućavanje, FALSE za onemogućavanje
-
zamijeniti: pwdmaxfailure
pwdmaxfailure: 10
-
zamijeniti: pwdlockoutduration
pwdlockoutduration: 300
-
zamijeniti: pwdfailurecountinterval
pwdfailurecountinterval: 0
-
zamijeniti: pwdminlength
pwdminlength: 8
-
zamijeniti: passwordminalphachars
passwordminalphachars: 2
-
zamijeniti: passwordminotherchars
passwordminotherchars: 2
-
zamijeniti: passwordmaxrepeatedchars
passwordmaxrepeatedchars: 2
-
zamijeniti: passwordmindiffchars
passwordmindiffchars: 2
```

Bilješka: Administrativni računi mogu se zaključati u slučaju pretjeranih grešaka u provjeri autentičnosti. Ova se funkcija primjenjuje jedino na povezivanja na udaljeni klijent. Račun se ponovo postavlja kod pokretanja poslužitelja.

Srodni zadaci

"Postavljanje svojstva politike lozinke" na stranici 166
Koristite ovu informaciju za postavljanje svojstva politike lozinke.

Postavljanje svojstva zaključavanje lozinke:

Koristite ovu informaciju za postavljanje svojstva zaključavanje lozinke.

1. Proširite kategoriju **Upravljanje svojstvima sigurnosti** u području navigacije Web administracijskog alata, zatim izaberite karticu **Zaključavanje lozinke**.

   Bilješka: Ako je politika lozinke onemogućena na poslužitelju, funkcije na ovom panelu nemaju utjecaj.
2. Navedite broj sekunda, minuta, sati ili dana koji moraju isteći prije nego što lozinka može biti promijenjena.
3. Navedite da li netočne prijave zaključavaju lozinku.
   - Izaberite radio gumb **Lozinke se nikad ne zaključavaju** ako želite dozvoliti neograničene pokušaje prijave. Ovaj izbor onemogućava funkciju zaključavanja lozinke.
   - Izaberite radio gumb Pokušaji i navedite broj pokušaja prijave koji je dopušten prije nego što se lozinka zaključa. Ovaj izbor omogućava funkciju zaključavanja lozinke.
4. Navedite trajanje zaključavanja. Izaberite radio gumb **Zaključavanje nikad ne ističe** da navedete da sistemski administrator mora resetirati lozinku ili izaberite radio gumb **Sekunde** i navedite broj sekundi prije nego što zaključavanje ističe i pokušaji prijave se mogu nastaviti.
5. Navedite vrijeme isteka za neispravnu prijavu. Kliknite radio gumb **Netočne prijave se čiste samo s ispravnom lozinkom** da navedete da se netočne prijave brišu samo s uspješnom prijavom ili kliknite radio gumb **Sekunde** i navedite broj sekundi prije nego što se neuspješni pokušaj prijave briše iz memorije.

   Bilješka: Ova opcija radi samo ako lozinka nije zaključana.
6. Kada završite kliknite **Primijeni** da spremite vaše izmjene bez izlaska ili kliknite **OK** da primijenite vaše promjene i izađete ili kliknite **Opoziv** da izađete iz ovog panela bez promjena.

Postavljanje svojstva provjere valjanosti lozinke:

Koristite ovu informaciju za postavljanje svojstva provjere valjanosti lozinke.

1. Proširite kategoriju **Upravljanje svojstvima sigurnosti** u području navigacije Web administracijskog alata, zatim izaberite karticu **Provjera lozinke**.

   Bilješka: Ako je politika lozinke onemogućena na poslužitelju, funkcije na ovom panelu nemaju utjecaj.
2. Postavite broj lozinki koje moraju biti korištene prije nego što lozinka može biti ponovno korištena. Unesite broj od 0 do 30. Ako unesete nula, lozinka može biti ponovno korištena bez ograničenja.
3. Iz padajućeg izbornika, izaberite da li se lozinka provjerava na sintaksu definiranu u sljedećim poljima unosa. Možete izabrati:

   Ne provjeravaj sintaksu
   Provjera sintakse se ne izvodi.

   Provjeri sintaksu (osim šifrirane)
   Provjera sintakse se izvodi na svim nešifriranim lozinkama.

   Provjeri sintaksu
   Provjera sintakse se izvodi na svim lozinkama.
4. Navedite brojčanu vrijednost da postavite minimalnu dužinu lozinke. Ako je vrijednost postavljena na nula, provjera sintakse se ne izvodi.
   - Navedite brojčanu vrijednost da postavite minimalni broj abecednih znakova potrebnih za lozinku.

- Navedite brojčanu vrijednost da postavite minimalni broj numeričkih i posebnih znakova potrebnih za lozinku.

  Bilješka: Suma minimalnog broja abecednih, numeričkih i posebnih znakova mora biti jednaka ili manja od broja navedenog kao minimalna dužina lozinke.

5. Navedite maksimalni broj znakova koji mogu biti ponovljeni u lozinci. Ova opcija ograničava koliko puta se određeni znak može pojaviti u lozinci. Ako je vrijednost postavljena na nula, broj ponovljenih znakova se ne provjerava.
6. Navedite minimalni broj znakova koji mora biti različit od prethodne lozinke i broj prethodnih lozinki naveden u polju **Minimalni broj lozinki prije ponovnog korištenja**. Ako je vrijednost postavljena na nula, broj različitih znakova se ne provjerava.
7. Kada završite kliknite **Primijeni** da spremite vaše izmjene bez izlaska ili kliknite **OK** da primijenite vaše promjene i izađete ili kliknite **Opoziv** da izađete iz ovog panela bez promjena.

Pregled atributa politike lozinke:

Koristite ovu informaciju za pregled atributa politike lozinke.

Operativni atributi se vraćaju na zahtjevu pretraživanja samo kad je to posebno zahtijevano od strane klijenta. Da bi koristili atribute u operacijama pretraživanja, vi morate imati dozvole na kritičnim atributima ili dozvole na određene korištene atribute.

1. Da bi pregledali politiku lozinke za određeni unos:

   ```
   > ldapsearch -b "uid=user1,cn=users,o=ibm" -s base "(objectclass=*)"
    pwdChangedTime pwdAccountLockedTime pwdExpirationWarned
    pwdFailureTime pwdGraceUseTime pwdReset
   ```

2. Da napravite upit za unose za koje će lozinka isteći, upotrijebite pwdChangedTime atribut. Na primjer, da pronađete lozinke koje istječu 26. kolovoza, 2004, s politikom isteka lozinke od 186 dana, napravite upit za unose za koje se lozinka promijenila najmanje prije 186 dana (22. veljača, 2004):

   ```
   > ldapsearch -b "cn=users,o=ibm" -s sub
    "(!(pwdChangedTime>20040222000000Z))" 1.1
   ```

   gdje je filter jednak pwdChangedTime od ponoći, 22. veljača, 2004.

3. Da bi pretražili zaključane račune, upotrijebite pwdAccountLockedTime atribut:

   ```
   > ldapsearch -b "cn=users,o=ibm" -s sub "(pwdAccountLockedTime=*)" 1.1
   ```

   gdje ″1.1″ označava da samo DN unosi trebaju biti vraćeni.

4. Da bi napravili upite za račune za koje lozinka mora biti promijenjena zato što je lozinka resetirana, upotrijebite pwdReset atribut:

   ```
   > ldapsearch -b "cn=users,o=ibm" -s sub "(pwdReset=TRUE)" 1.1
   ```

Nadjačavanje atributa politike lozinke:

Koristite ovu informaciju za nadjačavanje atributa politike lozinke.

Ovo trebate najprije napraviti.

Administrator direktorija može nadjačati normalno ponašanje politike lozinke za određene unose izmjenom operativnih atributa politike lozinke i korištenjem kontrole administracije poslužitelja (-k opcija od LDAP uslužnih programa reda za naredbe).

1. Možete spriječiti lozinku za određeni račun od isticanja postavljanjem pwdChangedTime atributa na datum koji je daleko u budućnosti kod postavljanja userPassword atributa. Sljedeći primjer postavlja vrijeme na ponoć, Siječanj 1, 2200.

   ```
   > ldapmodify -D cn=root -w ? -k
   dn: uid=wasadmin,cn=users,o=ibm
   changetype: modify
   replace: pwdChangedTime
   pwdChangedTime: 22000101000000Z
   ```

2. Možete otključati račun koji je zaključan zbog previše neuspjeha kod prijave uklanjanjem pwdAccountLockedTime i pwdFailureTime atributa:

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
delete: pwdAccountLockedTime
-
delete: pwdFailureTime
```

3. Možete otključati račun mijenjanjem pwdChangedTime i brisanjem pwdExpirationWarned i pwdGraceUseTime atributa:

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: pwdChangedTime
pwdChangedTime: 200408260000000Z
-
delete: pwdExpirationWarned
-
delete: pwdGraceUseTime
```

4. Možete očistiti ili postaviti ″lozinka mora biti promijenjena″ status postavljanjem pwdReset atributa:

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
delete: pwdReset

> ldapmodify -D cn=root -w ? -k
dn: uid=user2,cn=users,o=ibm
changetype: modify
replace: pwdReset
pwdReset: TRUE
```

5. Račun može biti administrativno zaključan postavljanjem ibm-pwdAccountLocked operativnog atributa na TRUE.

   Korisnička postavka koju ovaj atribut mora imati za dozvolu za pisanje je ibm-pwdAccountLocked atribut, koji je definiran kao CRITICAL klasa pristupa.

```
> ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: TRUE
```

6. Račun može biti otključan postavljanjem atributa na FALSE. Otključavanje računa na ovaj način ne utječe status računa u odnosu na zaključavanje zbog pretjeranih neuspjeha lozinke ili lozinke koja je istekla.

   Korisnička postavka koju ovaj atribut mora imati za dozvolu za pisanje je ibm-pwdAccountLocked atribut, koji je definiran kao CRITICAL klasa pristupa.

```
> ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: FALSE
```

Omogućavanje SSL-a i sigurnosti sloja prijenosa na Directory Server-u

Koristite ovu informaciju za omogućavanje SSL-a i sigurnosti sloja prijenosa na Directory Server-u.

Ako imate Upravitelj digitalnih certifikata instaliran na vašem sistemu, možete koristiti sigurnost Sloja sigurnih utičnica (SSL) za zaštitu pristupa na vaš Poslužitelj direktorija. Prije omogućavanja SSL-a na directory server-u, možda će vam biti korisno pročitati Sloj sigurnih utičnica (SSL) i Sigurnost sloja prijenosa (TLS) s poglavljem Directory Server.

Da omogućite SSL na vašem LDAP poslužitelju, napravite sljedeće:

1. **Pridružite certifikat Poslužitelju direktorija**

a. Ako želite upravljati Directory Server-om preko veze SSL iz System i Navigator, pogledajte *System i Access za Windows Vodič za korisnike* (opcijski se instalira na računalo nakon što instalirate System i Navigator). Ako planirate dozvoliti SSL i ne-SSL veze prema poslužitelju direktorija, možete izabrati preskakanje ovog koraka.

b. Pokrenite IBM Upravitelj digitalnim certifikatima. Pogledajte Pokretanje Upravitelja digitalnih certifikata u poglavlju Upravitelj digitalnih certifikata za više informacija.

c. Ako želite dobiti ili kreirati certifikate ili promijeniti postav ili promijeniti svoj sistem certifikata, učinite to sada. Pogledajte Upravitelj digitalnih certifikata za više informacija o sistemu certifikata. Postoje dvije aplikacije poslužitelja i jedna aplikacija klijenta koje su pridružene Poslužitelju direktorija. Oni su:

   Aplikacija Poslužitelja direktorija
   Aplikacija Poslužitelja direktorija je sam poslužitelj.

   Aplikacija objavljivanja Poslužitelja direktorija
   Aplikacija objavljivanja Poslužitelja direktorija identificira certifikat kojeg koristi objavljivanje.

   Aplikacija klijenta Poslužitelja direktorija
   Aplikacija klijenta Poslužitelja direktorija identificira default certifikat kojeg koriste aplikacije koje koriste LDAP klijent ILE API-je.

d. Kliknite na gumb **Izbor spremišta certifikata**.

e. Izaberite ***SYSTEM**. Kliknite **Nastavak**.

f. Unesite prikladnu lozinku za *SYSTEM spremište certifikata. Kliknite **Nastavak**.

g. Kad se lijevi navigacijski izbornik ponovno napuni, proširite **Upravljanje aplikacijama**.

h. Kliknite **Ažuriraj dodjeljivanje certifikata**.

i. Na sljedećem ekranu izaberite aplikaciju **Poslužitelj**. Kliknite **Nastavak**.

j. Izaberite **Poslužitelj poslužitelja direktorija**.

k. Kliknite na **Ažuriraj dodjeljivanja certifikata** kako bi dodijelili certifikat Poslužitelju direktorija kojeg će koristiti kako bi uspostavio svoj identitet na System i Access za Windows klijentima.

   Bilješka: Ako izaberete certifikat od CA čiji CA certifikat nije u vašoj System i Access za Windows bazi podataka ključa klijenta, trebat ćete ga dodati kako bi koristili SSL. Dovršite tu procedure prije nego počnete drugu.

l. Izaberite certifikat iz liste kojeg ćete dodijeliti poslužitelju.

m. Kliknite na **Dodijeli novi certifikat**.

n. DCM se ponovno učitava na stranicu **Ažuriraj dodjeljivanje certifikata** s potvrdnom porukom. Kada ste dovršili postavljanje certifikata za Poslužitelj direktorija, kliknite na **Gotovo**.

2. Opcijsko: **Pridružite certifikat za objavljivanje Poslužitelja direktorija**. Ako također želite omogućiti izdavanje iz sistema u Directory Server preko veze SSL, možda ćete htjeti pridružiti i certifikat s izdavanjem Directory Servera. Time se identificira default certifikat i povjerljivi CA-ovi za aplikacije koje koriste LDAP ILE API-je koji ne specificiraju svoj ID aplikacije ili zamjensku bazu podataka ključa.

   a. Pokrenuti IBM Upravitelj digitalnim certifikatima.

   b. Kliknite na gumb **Izbor spremišta certifikata**.

   c. Izaberite ***SYSTEM**. Kliknite **Nastavak**.

   d. Unesite prikladnu lozinku za *SYSTEM spremište certifikata. Kliknite **Nastavak**.

   e. Kad se lijevi navigacijski izbornik ponovno napuni, proširite **Upravljanje aplikacijama**.

   f. Kliknite **Ažuriraj dodjeljivanje certifikata**.

   g. Na sljedećem certifikatu izaberite aplikaciju **Klijent**. Kliknite **Nastavak**.

   h. Izaberite **Objavljivanje Poslužitelja direktorija**.

   i. Kliknite na **Ažuriranje dodjele certifikata** da dodijelite certifikat objavljivanju Poslužitelja direktorija koji će uspostaviti njegov identitet.

   j. Izaberite certifikat iz liste kojeg ćete dodijeliti poslužitelju.

   k. Kliknite na **Dodjela novog certifikata**.

l. DCM se ponovno učitava na stranicu **Ažuriraj dodjeljivanje certifikata** s potvrdnom porukom.

Bilješka: Ti koraci pretpostavljaju da već objavljujete informacije na Poslužitelju direktorija s ne-SSL vezom. Pogledajte “Objavljivanje informacija Directory Server-u” na stranici 123 za potpune informacije o postavljanju objavljivanja.

3. Opcijsko: **Pridružite certifikat za klijenta Poslužitelja direktorija**. Ako imate druge aplikacije koje koriste veze SSL na Directory Server, morate također pridružiti certifikat s klijentom Directory Servera.
   a. Pokrenuti IBM Upravitelj digitalnim certifikatima.
   b. Kliknite na gumb **Izbor spremišta certifikata**.
   c. Izaberite ***SYSTEM**. Kliknite **Nastavak**.
   d. Unesite prikladnu lozinku za *SYSTEM spremište certifikata. Kliknite **Nastavak**.
   e. Kad se lijevi navigacijski izbornik ponovno napuni, proširite **Upravljanje aplikacijama**.
   f. Kliknite **Ažuriraj dodjeljivanje certifikata**.
   g. Na sljedećem certifikatu izaberite aplikaciju **Klijent**. Kliknite **Nastavak**.
   h. Izaberite **klijenta Poslužitelja direktorija**.
   i. Kliknite na **Ažuriranje dodjele certifikata** da dodijelite certifikat klijentu Poslužitelja direktorija koji će uspostaviti njegov identitet.
   j. Izaberite certifikat iz liste kojeg ćete dodijeliti poslužitelju.
   k. Kliknite na **Dodijeli novi certifikat**.
   l. DCM se ponovno učitava na stranicu **Ažuriraj dodjeljivanje certifikata** s potvrdnom porukom.

Nakon što se omogući SSL, možete promijeniti port koji Poslužitelj direktorija koristi za sigurne veze.

Kako biste koristili SSL ili TLS, morate ga omogućiti u System i Navigator.

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Desnom tipkom miša kliknite na **Direktorij** i izaberite **Svojstva**.
4. Na kartici **Mreža** označite kućicu pokraj **Sigurno**.

   Također možete navesti broj porta koji želite napraviti sigurnim. Klik na kućicu **Sigurno** je indikacija da aplikacija može pokrenuti SSL ili TSL vezu preko sigurnog porta. Također je to indikacija da aplikacija može izdati StartTLS operaciju da bi dozvolila TLS vezu preko nesigurnog porta. Alternativno, TLS može biti dozvan korištenjem -Y opcije iz klijentskog pomoćnog programa reda za naredbe. Ako koristite red za naredbe, ibm-slapdSecurity atribut mora biti jednak TLS ili SSLTLS.

   Srodni koncepti

   “Sloj sigurnih utičnica (SSL) i Sigurnost razine prijenosa (TLS) s Poslužiteljem direktorija” na stranici 51
   Da bi komunikacija s Directory Server-om bila još sigurnija, Directory Server mora koristiti sigurnost Sloja sigurnih utičnica (SSL) i Sigurnost sloja transporta (TLS).

Omogućavanje provjere autentičnosti Kerberos na Directory Server-u

Koristite ovu informaciju za omogućavanje provjere autentičnosti Kerberos na Directory Server-u.

Ako imate Uslugu provjere autentičnosti mreže konfiguriranu na vašem sistemu, možete postaviti svoj Poslužitelj direktorija tako da koristi Kerberos provjeru autentičnosti. Kerberos provjera autentičnosti se odnosi na korisnike i administratore. Prije omogućavanja Kerberos-a na directory server-u, korisno pročitati pregled upotrebe Kerberosa s Directory Server-om.

Za omogućavanje Kerberos provjere ovlaštenja, slijedite ove korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.

4. Desno kliknite na **IBM poslužitelj direktorija** i izaberite **Svojstva**.
5. Kliknite karticu **Kerberos**.
6. Označite **Omogući Kerberos provjeru ovlaštenja**.
7. Odredite ostale postavke na stranici **Kerberos** kako odgovaraju vašoj situaciji. Pogledajte online pomoć stranice za informacije o pojedinačnim poljima.

Srodne reference

"Provjera autentičnosti" na stranici 78
Koristite metodu provjere autentičnosti za kontroliranje pristupa unutar Directory Servera.

Konfiguriranje provjere autentičnosti DIGEST-MD5 na Directory Server-u

Koristite ovu informaciju za konfiguriranje provjere autentičnosti DIGEST-MD5 na Directory Server-u.

DIGEST-MD5 je SASL mehanizam provjere autentičnosti. Kada klijent koristi DIGEST-MD5, lozinka nije prenesena u jasnom tekstu i protokol sprečava ponovne napade. Alat Web administracije je korišten za konfiguriranje DIGEST-MD5.

1. Pod **Administracija poslužitelja**, proširite **Upravljanje sigurnosnim svojstvima** kategoriju u navigacijskom području i izaberite **DIGEST-MD5** karticu.

   Bilješka: Za promjenu postavki konfiguracije poslužitelja pomoću zadataka u kategoriji Administracija poslužitelja Web Administration tool-a, morate provjeriti autentičnost poslužitelju kao i5/OS korisnički profil koji ima *ALLOBJ i IOSYSCFG posebna ovlaštenja. To može biti napravljeno ovlašćivanjem kao projicirani korisnik s lozinkom za taj profil. Da bi se vezali kao projicirani korisnik iz Web administracijskog alata, unesite korisničko ime oblika os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, gdje su MYUSERNAME i MYSYSTEM.COM nizovi zamijenjeni s vašim imenom korisničkog profila i konfiguriranim projiciranim nastavkom sistema.
2. Pod **Područje poslužitelja**, upotrijebite predizabranu **Default** postavku, koja je kvalificirano host ime poslužitelja ili možete kliknuti **Područje** i upisati ime područja za koje želite konfigurirati poslužitelj. To ime područja je korišteno od strane klijenta da odredi koje korisničko ime i lozinku treba koristiti. Kod korištenja replikacije, želite imati sve poslužitelje konfigurirane s istim područjem.
3. Pod atributom **Korisničko ime** upotrijebite predizabranu **Default** postavku, koja je uid ili možete kliknuti **Atribut** i upisati ime atributa koji želite da poslužitelj koristi da jedinstveno identificirate korisnički unos za vrijeme DIGEST-MD5 SASL vezivanja.
4. Ako ste prijavljeni kao administrator direktorija, pod **Korisničko ime administratora**, upišite korisničko ime administratora. To polje ne može biti uređivano od strane članova administrativne grupe. Ako korisničko ime navedeno na DIGEST-MD5 SASL vezivanju odgovara ovom nizu, korisnik je administrator.

   Bilješka: Korisničko ime administratora je osjetljivo na veličinu slova.
5. Kada završite, kliknite na **OK**.

Srodne reference

"Provjera autentičnosti" na stranici 78
Koristite metodu provjere autentičnosti za kontroliranje pristupa unutar Directory Servera.

Zadaci sheme

Koristite ovu informaciju za upravljanje shemom.

Shemom se može upravljati korištenjem Web administracijskog alata ili LDAP aplikacije poput ldapmodify u kombinaciji s LDIF datotekama. Kada prvo definirate nove objectclasse ili atribute, možda bi bilo najprikladnije korištenje alata Web administracije. Ako trebate kopirati novu shemu na druge poslužitelje (možda kao dio proizvoda ili alata koji izdajete), ldapmodify uslužni program može biti korisnije, pogledajte "Kopiranje sheme na druge poslužitelje" na stranici 183 radi više informacija.

Srodni koncepti

"Sufiks (kontekst imenovanja)" na stranici 12
Sufiks (poznat i kao kontekst imenovanja) je DN koji identificira najviši unos u lokalno zadržanoj hijerarhiji direktorija.

"Shema" na stranici 14
Shema je skup pravila koji upravlja načinom na koji se podaci mogu pohraniti u direktorij. Shema definira dozvoljeni tip unosa, njihovu strukturu atributa i sintaksu atributa.

Pregled klasa objekta

Koristite ovu informaciju za pregled klasa objekta.

Možete pregledati klase objekta pomoću Web administration tool-a ili pomoću reda za naredbe.

1. Proširite **Upravljanje shemom** u području navigacije i kliknite na **Upravljanje klasama objekata**. Prikazan je panel samo za čitanje koji vam omogućava da pregledate klase objekata u shemi i njihove karakteristike. Klase objekata su prikazane u abecednom redu. Možete ići jednu stranicu natrag ili naprijed tako da kliknete na Prethodno ili Sljedeće. Polje uz te gumbe identificira stranicu na kojoj se nalazite. Možete koristite i padajući izbornik tog polja kako bi skočili na određenu stranicu. Prva klasa objekata ispisana na stranici je prikazana s brojem stranice kako bi lakše mogli locirati klasu objekata koju želite pregledati. Na primjer, ako ste tražili klasu objekata **person**, proširite padajući izbornik i spuštajte se dolje tako dugo dok ne vidite **Stranica 14 od 16 nsLiServer** i **Stranica 15 od 16 printerLPR**. Budući je person prema abecedi između nsLiServer i printerLPR, izaberite Stranicu 14 i kliknite na **Kreni**.

   Možete prikazati klase objekta sortirane prema tipu. Izaberite **Tip** i kliknite na **Sort**. Klase objekata su abecedno sortirane unutar njihova tipa, Sažetak, Pomoćno ili Strukturalno. Isto tako, poredak popisa možete obrnuti tako da izaberete **Silazno** i kliknete na **Sort**.
2. Nakon što locirate klasu objekta koju želite, možete pregledati njezin tip, nasljeđe, potrebne atribute ili neobvezne atribute. Proširite padajuće izbornike za nasljeđivanje, potrebne atribute i neobvezne atribute kako bi vidjeli potpuno ispisivanje za svaku osobinu. Možete izabrati operacije klase objekata koje želite izvoditi iz desne trake s alatima, kao što je:
   - Dodavanje
   - Uređivanje
   - Kopiranje
   - Brisanje
3. Kada ste završili kliknite **Zatvaranje** da se vratite na IBM poslužitelj direktorija panel **Dobrodošlica**.

Za pregled klasa objekta koje se nalaze u shemi pomoću reda naredbe, upišite:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Dodavanje klase objekta

Koristite ovu informaciju za dodavanje klase objekta.

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje klasama objekta**. Kako bi kreirali novu klasu objekata:

1. Kliknite **Dodavanje**.

   Bilješka: Tom panelu možete pristupiti tako da proširite **Upravljanje shemom** u području navigacije i nakon toga kliknete na **Dodavanje klase objekta**.
2. Na kartici **Općenita svojstva**:
   - Unesite **Ime klase objekta**. To je potrebno polje i ono opisuje funkciju klase objekta. Na primjer, **privZaposlenik** za klasu objekta koja se koristi za praćenje privremenih zaposlenika.
   - Unesite **Opis** klase objekta, na primjer, **Klasa objekta koja se koristi za privremene zaposlenike**.
   - Unesite **OID** za klasu objekta. To je potrebno polje. Pogledajte "Identifikator objekta (OID)" na stranici 25. Ako nemate OID, možete koristiti **Ime klase objekta** kojem je pridodano **-oid**. Na primjer, ako je ime klase objekta **privZaposlenik**, onda je OID **privZaposlenik-oid**. Možete promijeniti vrijednost tog polja.

- Izaberite **Superiorna klasa objekta** iz padajućeg popisa. Time se određuje klasa objekata iz koje se nasljeđuju drugi atributi. Tipično je **Superiorna klasa objekta** na **vrhu**, međutim, može biti i druga klasa objekta. Na primjer, superiorna klasa objekta za **privZaposlenik** može biti **ePerson**.
- Izaberite **Tip klase objekta**. Pogledate “Klase objekta” na stranici 16 za dodatne informacije o tipovima klase objekta.
- Kliknite na karticu Atributi kako bi specificirali potrebne i neobvezne atribute za klasu objekta i pregledajte naslijeđene atribute ili kliknite na **OK** kako bi dodali novu klasu objekta ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekata** bez da činite promjene.

3. Na kartici **Atributi**:
   - Izaberite atribut iz abecednog popisa **Dostupni atributi** i kliknite na **Dodavanje potrebnom** kako bi napravili atribut potrebnim ili kliknite na **Dodavanje neobveznom** kako bi napravili atribut neobveznim za klasu objekata. Atribut je prikazan u odgovarajućem popisu izabranih atributa.
   - Ponovite taj proces za sve atribute koje želite izabrati.
   - Možete premještati atribute iz jednog popisa na drugi ili obrisati atribut iz izabranih popisa tako da ga izaberete i kliknete na odgovarajući **Premjesti** ili **Obriši** gumb.
   - Možete pregledati popise potrebnih i neobveznih naslijeđenih atributa. Naslijeđeni atributi se temelje na **Superiornoj klasi objekta** izabranoj na kartici **Općenito**. Ne možete promijeniti naslijeđene atribute. No, ako promijenite **Superiornu klasu objekta** na kartici **Općenito**, prikazuje se drugačiji skup naslijeđenih atributa.
4. Kliknite na **OK** kako bi dodali novu klasu objekta ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekata** bez da činite bilo kakve promjene.

Bilješka: Ako ste kliknuli na **OK** na kartici **Općenito** bez da ste dodali bilo koje atribute, možete dodati atribute uređivanjem nove klase objekta.

Kako bi dodali klasu objekta korištenjem reda za naredbe, izdajte sljedeću naredbu:

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

gdje<*ime datoteke*>sadrži:

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: ( <myobjectClass-oid> NAME '<myObjectClass>' DESC '<Klasa objekta
                I definirana za moju LDAP aplikaciju>' SUP '<objectclassinheritance>'
                <objectclasstype> MAY (<attribute1> $ <attribute2>))
```

Uređivanje klase objekta

Koristite ovu informaciju za uređivanje klase objekta.

Nisu dozvoljene sve promjene sheme. Pogledajte “Nedozvoljene promjene sheme” na stranici 27 kako bi promijenili ograničenja.

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje klasama objekta**. Kako bi uređivali klasu objekta:

1. Kliknite na radijski gumb koji se nalazi uz klasu objekta koju želite uređivati.
2. Kliknite **Uređivanje**.
3. Izaberite karticu:
   - Koristite karticu **Općenito** kako bi:
     - Promijenite **Opis**.
     - Promijenili **Superiornu klasa objekta**. Izaberite Superiornu klasu objekta iz padajućeg popisa. Time se određuje klasa objekata iz koje se nasljeđuju drugi atributi. Tipično je **Superiorna klasa objekta** na **vrhu**, međutim, može biti i druga klasa objekta. Na primjer, superiorna klasa objekta za **privZaposlenik** može biti **ePerson**.

– Promijenite **Tip klase objekta**. Izaberite tip klase objekta. Pogledate “Klase objekta” na stranici 16 za dodatne informacije o tipovima klase objekta.
– Kliknite na karticu Atributi kako bi promijenili potrebne i neobvezne atribute za klasu objekta i pregledali naslijeđene atribute ili kliknite na **OK** kako bi primijenili svoje promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekta** bez bilo kakvih promjena.

• Koristite karticu **Atributi** kako bi:

Izaberite atribut iz abecednog popisa **Dostupni atributi** i kliknite na **Dodavanje potrebnom** kako bi napravili atribut potrebnim ili kliknite na **Dodavanje neobveznom** kako bi napravili atribut neobveznim za klasu objekata. Atribut je prikazan u odgovarajućem popisu izabranih atributa.

Ponovite taj proces za sve atribute koje želite izabrati.

Možete premještati atribute iz jednog popisa na drugi ili obrisati atribut iz izabranih popisa tako da ga izaberete i kliknete na odgovarajući **Premjesti** ili **Obriši** gumb.

Možete pregledati popise potrebnih i neobveznih naslijeđenih atributa. Naslijeđeni atributi se temelje na **Superiornoj klasi objekta** izabranoj na kartici **Općenito**. Ne možete promijeniti naslijeđene atribute. No, ako promijenite **Superiornu klasu objekta** na kartici **Općenito**, prikazuje se drugačiji skup naslijeđenih atributa.

4. Kliknite na **OK** kako bi primijenili promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekata** bez ikakvih promjena.

Za pregled klasa objekta koje se nalaze u shemi pomoću reda naredbe, izdajte sljedeću naredbu:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Kako bi uređivali klasu objekta korištenjem reda za naredbe, izdajte sljedeću naredbu:

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

gdje <*ime datoteke*>sadrži:

```
dn: cn=schema
changetype: modify
replace: objectclasses
objectclasses: ( <myobjectClass-oid> NAME '<myObjectClass>' DESC '<Klasa objekta
                 koju sam definirao za svoju LDAP aplikaciju >' SUP '<newsuperiorclassobject>'
                 <newobjectclasstype> MAY (attribute1> $ <attribute2>
                  $ <newattribute3>) )
```

Kopiranje klase objekta

Koristite ovu informaciju za kopiranje klase objekta.

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje klasama objekta**. Kako bi kopirali klasu objekta:

1. Kliknite na radijski gumb uz klasu objekta koju želite kopirati.
2. Kliknite **Kopiranje**.
3. Biranje kartice:
   • Koristite karticu **Općenito** kako bi:
   – Promijenili**ime klase objekta**. Default ime je ime kopirane klase objekata kojoj je pridodana riječ COPY. Na primjer, **tempPerson** se kopirao kao **tempPersonCOPY**.
   – Promijenite **Opis**.
   – Promijenite **OID**. Default OID je OID kopirane klase objekte kojoj je pridodana riječ COPY. Na primjer, **tempPerson-oid** se kopira kao **tempPerson-oidCOPY**.
   – Promijenite**Superiornu klasa objekta**. Izaberite superiornu klasu objekta iz padajuće liste. Time se određuje klasa objekata iz koje se nasljeđuju drugi atributi. Tipično je **Superiorna klasa objekta** na **vrhu**, međutim, može biti i druga klasa objekta. Na primjer, superiorna klasa objekta za **tempEmployeeCOPY** bi mogla biti **ePerson**.
   – Promijenite **Tip klase objekta**. Izaberite tip klase objekta. Pogledate “Klase objekta” na stranici 16 za dodatne informacije o tipovima klase objekta.

– Kliknite na karticu **Atributi** kako bi promijenili potrebne i neobvezne atribute za klasu objekta i pregledali naslijeđene atribute ili kliknite na **OK** kako bi primijenili svoje promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekata** bez ikakvih promjena.

- Koristite karticu **Atributi** kako bi:

  Izaberite atribut iz abecednog popisa **Dostupni atributi** i kliknite na **Dodavanje potrebnom** kako bi napravili atribut potrebnim ili kliknite na **Dodavanje neobveznom** kako bi napravili atribut neobveznim za klasu objekata. Atribut je prikazan u odgovarajućem popisu izabranih atributa.

  Ponovite taj proces za sve atribute koje želite izabrati.

  Možete premještati atribute iz jednog popisa na drugi ili obrisati atribut iz izabranih popisa tako da ga izaberete i kliknete na odgovarajući **Premjesti** ili **Obriši** gumb.

  Možete pregledati popise potrebnih i neobveznih naslijeđenih atributa. Naslijeđeni atributi se temelje na **Superiornoj klasi objekta** izabranoj na kartici **Općenito**. Ne možete promijeniti naslijeđene atribute. No, ako promijenite **Superiornu klasu objekta** na kartici **Općenito**, prikazuje se drugačiji skup naslijeđenih atributa.

4. Kliknite na **OK** kako bi primijenili promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekata** bez ikakvih promjena.

Za pregled klasa objekta koje se nalaze u shemi pomoću reda naredbe, izdajte naredbu:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Izaberite klase objekta koje želite kopirati. Koristite editor za promjenu odgovarajuće informacije i spremite promjene u <*ime datoteke*>. Izdajte sljedeću naredbu:

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

gdje <*ime datoteke*>sadrži:

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( <mynewobjectClass-oid> NAME '<mynewObjectClass>'
                 DESC '<Nova klasa objekta koju sam
                   kopirao za svoju LDAP aplikaciju>'
                SUP '<superiorclassobject>'<objectclasstype> MAY (attribute1>
                $ <attribute2> $ <attribute3>) )
```

Brisanje klase objekta

Koristite ovu informaciju za brisanje klase objekta.

Nisu dozvoljene sve promjene sheme. Pogledajte “Nedozvoljene promjene sheme” na stranici 27 kako bi promijenili ograničenja.

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje klasama objekta**. Kako bi obrisali klasu objekta:

1. Kliknite na radijski gumb koji se nalazi uz klasu objekta koju želite obrisati.
2. Kliknite **Brisanje**.
3. Promptirani ste kako bi potvrdili brisanje klase objekta. Kliknite na **OK** kako bi obrisali klasu objekta ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje klasama objekta** bez ikakvih promjena.

Pregledajte klase objekata koje su sadržane u shemi i izdajte naredbu:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Izaberite klasu objekta koju želite obrisati i izdajte sljedeću naredbu:

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

gdje <*ime datoteke*>sadrži:

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: (<myobjectClass-oid>)
```

Pregled atributa

Koristite ovu informaciju za pregled atributa.

Možete pregledati atribute u shemi korištenjem Web administracijskog alata, preferirane metode ili korištenjem reda za naredbe.

1. Proširite **Upravljanje shemom** u području navigacije i kliknite na **Upravljanje atributima**.

   Prikazuje se panel samo za čitanje koji vam omogućuje da pregledate atribute u shemi i njihove karakteristike. Atributi su prikazani u abecednom poretku. Možete ići jednu stranicu natrag ili naprijed tako da kliknete na Prethodno ili Sljedeće. Polje uz te gumbe identificira stranicu na kojoj se nalazite. Možete koristite i padajući izbornik tog polja kako bi skočili na određenu stranicu. Prva klasa objekata ispisana na stranici je prikazana s brojem stranice kako bi lakše mogli locirati klasu objekata koju želite pregledati. Na primjer, ako ste tražili atribut **authenticationUserID**, proširite padajući izbornik i spustite se dolje dok ne vidite **Stranica 3 od 62 applSystemHint** i **Stranica 4 od 62 authorityRevocatonList**. Budući je authenticationUserID prema abecedi između applSystemHint i authorityRevocatonList, izaberite Stranicu 3 i kliknite na **Kreni**.

   Možete prikazati atribute sortirane prema sintaksi. Izaberite **Sintaksa** i kliknite na **Sort**. Ti atributi su sortirani abecedno unutar njihove sintakse. Pogledajte “Sintaksa atributa” na stranici 23 za ispisivanje ili tipove sintakse. Isto tako, poredak popisa možete obrnuti tako da izaberete **Silazno** i kliknete na **Sort**.

   Nakon što pronađete atribut kojeg želite, možete pregledati njegovu sintaksu, da li ima više vrijednosti i klase objekta koje sadrži. Proširite padajući izbornik za klasu objekta kako bi vidjeli popis klasa objekata za atribut.
2. Kada ste završili kliknite **Zatvaranje** da se vratite na IBM poslužitelj direktorija panel **Dobrodošlica**.

Za pregled atributa koji se nalaze u shemi, izdajte naredbu:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Dodavanje atributa

Koristite ovu informaciju za dodavanje atributa.

Koristite bilo koju od sljedećih metoda za kreiranje novog atributa. Web administracijski alat je preferirana metoda.

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje atributima**. Za kreiranje novog atributa:

1. Kliknite **Dodavanje**.

   Bilješka: Tom panelu možete pristupiti proširivanjem **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Dodavanje atributa**.
2. Unesite **Ime atributa**, na primjer, **tempId**. To je potrebno polje i mora započeti s abecednim znakom.
3. Unesite **Opis** atributa, na primjer, **ID broj dodijeljen privremenom zaposleniku**.
4. Unesite **OID** za atribut. To je potrebno polje. Pogledajte “Identifikator objekta (OID)” na stranici 25. Ako nemate OID, možete koristiti ime atributa kojem je pridodan -oid. Na primjer, ako je ime atributa **tempID**, onda je default OID **tempID-oid**. Možete promijeniti vrijednost tog polja.
5. Izaberite **Superiorni atribut** iz padajućeg izbornika. Superiorni atribut određuje atribut iz kojeg se nasljeđuju svojstva.
6. Izaberite **Sintaksu** iz padajućeg popisa. Pogledajte “Sintaksa atributa” na stranici 23 za dodatne informacije o sintaksi.
7. Unesite **Dužina atributa** koja specificira maksimalnu dužinu tog atributa. Dužina je izražena kao broj bajtova.
8. Izaberite kontrolnu kućicu **Dozvola više vrijednosti** kako bi omogućili da atributi imaju više vrijednosti.
9. Izaberite pravilo podudaranja iz svakog od padajućih izbornika za pravila podudaranja jednakosti, poretka i podniza. Pogledajte “Pravila podudaranja” na stranici 21 za potpuni ispis pravila podudaranja.

10. Kliknite karticu **IBM proširenja** da navedete dodatna proširenja za atribut ili kliknite **OK** za dodavanje novog atributa ili kliknite **Opoziv** da se vratite na **Upravljanje atributima** bez ikakvih promjena.
11. Na **IBM proširenja** kartici:
    - Promijenite **DB2 ime tablice** . Poslužitelj generira DB2 ime tablice ako je ovo polje ostavljeno prazno. Ako unesete DB2 ime tablice, morate također unijeti DB2 ime stupca.
    - Promijenite **DB2 ime stupca**. Poslužitelj generira DB2 ime stupca ako je to polje ostavljeno prazno. Ako unesete DB2 ime stupca, također morate unijeti DB2 ime tablice.
    - Postavite **Klasu sigurnosti** tako da izaberete **normalno**, **osjetljivo** ili **kritično** iz padajućeg popisa.
    - Postavite **Pravila indeksiranja** izborom jednog ili više pravila indeksiranja. Pogledajte “Pravila indeksiranja” na stranici 22 za dodatne informacije o pravilima indeksiranja.

      Bilješka: Ako ništa drugo, preporuča se da specificirate indeksiranje Jednakosti na bilo kojim atributima koji će se koristiti u filterima pretraživanja.
12. Kliknite na **OK** da dodate nove atribute ili kliknite na **Opoziv** da se vratite na **Upravljanje atributima** bez ikakvih promjena.

Bilješka: Ako ste kliknuli na OK na kartici Općenito bez dodavanja bilo kojih proširenja, možete dodati proširenja uređivanjem novog atributa.

Za dodavanje atributa pomoću reda za naredbe, izdajte sljedeću naredbu. U sljedećem primjeru se dodaje definicija tipa atributa za atribut koji se naziva ″myAttribute″, sa sintaksom Niz direktorija (pogledajte “Sintaksa atributa” na stranici 23) i podudaranjem Jednakost sa zanemarivanjem velikih i malih slova (pogledajte “Pravila podudaranja” na stranici 21). IBM-specifični dio definicije govori da su atributi podataka pohranjeni u stupcu pod imenom ″myAttrColumn″ u tablici pod nazivom ″myAttrTable″. Ako ta imena nisu bila specificirana, ime stupca i ime tablice bi se postavilo na ″myAttribute″. Atribut je dodijeljen na ″normalnoj″ klasi pristupa, a vrijednosti imaju maksimalnu dužinu od 200 bajtova.

```
ldapmodify -D <admindn> -w <adminpw> -i myschema.ldif
```

gdje **myschema.ldif** datoteka sadrži:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' )
                  DESC 'Atribut kojeg sam definirao za svoju LDAP aplikaciju'
                  EQUALITY 2.5.13.2 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
                  USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                     ACCESS-CLASS normal LENGTH 200 )
```

Uređivanje atributa

Koristite ovu informaciju za uređivanje atributa.

Nisu dozvoljene sve promjene sheme. Pogledajte “Nedozvoljene promjene sheme” na stranici 27 kako bi promijenili ograničenja.

Bilo koji dio definicije se može promijeniti prije nego imate dodane unose koji koriste atribut. Koristite bilo koju od sljedećih metoda kako bi uređivali atribut. Web administracijski alat je preferirana metoda.

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje atributima**. Kako bi uređivali atribut:

1. Kliknite na radijski gumb koji se nalazi uz atribut kojeg želite uređivati.
2. Kliknite **Uređivanje**.
3. Izaberite karticu:

- Koristite karticu **Općenito** kako bi:
  - Izaberite karticu, ili:
    - **Općenito** kako bi:
      - Promijenili **Opis**
      - Promijenili**Sintaksu**
      - Postavili **Dužinu atributa**
      - Promijenili postavke **Više vrijednosti**
      - Izabrali **Podudarajuće pravilo**
      - Promijenili **Superiorni atribut**
    - Kliknite **IBM proširenja** karticu da navedete dodatna proširenja za atribut ili kliknite **OK** radi dodavanja novog atributa ili kliknite **Opozvati** da se vratite na **Upravljanje atributima** bez ikakvih promjena.
    - **IBM proširenja**, ako koristite IBM Poslužitelj direktorija da:
      - Promijenite **Superiorna klasa**
      - Promijenite **Indeksirajuća pravila**
  - Kliknite na **OK** da primijenite svoje promjene ili kliknite na **Opoziv** da se vratite na **Upravljanje atributima** bez ikakvih promjena.
4. Kliknite na **OK** kako bi primijenili promjene ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje atributima** bez promjena.

Za uređivanje atributa pomoću reda za naredbe, izdajte sljedeću naredbu. Taj primjer dodaje indeksiranje na atribut, tako da pretraživanje bude brže. Koristite ldapmodify naredbu i LDIF datoteku kako bi promijenili definiciju:

```
ldapmodify -D <admindn> -w <adminpw> -i myschemachange.ldif
```

Gdje **myschemachange.ldif** datoteka sadrži:

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' ) DESC 'Atribut kojeg
                 sam definirao za moju LDAP aplikaciju' EQUALITY 2.5.13.2
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
replace: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                  ACCESS-CLASS normal LENGTH 200 EQUALITY SUBSTR )
```

Bilješka: Oba dijela definicije (**attributetypes** i **ibmattributetypes**) moraju biti uključeni u operaciju zamjene, iako se mijenja samo dio **ibmattributetypes**. Jedina promjena je dodavanje ″EQUALITY SUBSTR″ na kraj definicije kako bi se zatražili indeksi za podudaranje jednakosti i podniza.

Kopiranje atributa

Koristite ovu informaciju za kopiranje atributa.

Koristite bilo koju od sljedećih metoda kako bi kopirali atribut. Web administracijski alat je preferirana metoda.

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje atributima**. Kako bi kopirali atribut:

1. Kliknite na radijski atribut uz atribut kojeg želite kopirati.
2. Kliknite **Kopiranje**.
3. Promjena **Ime atributa**. Default ime je ime kopiranog atributa kojem je pridodana riječ COPY. Na primjer **tempID** se kopira kao **tempIDCOPY**.
4. Promijenite **Opis** atributa, na primjer, **ID broj dodijeljen privremenom zaposleniku**.

5. Promjena **OID**. Default OID je OID kopiranog atributa kojem je dodijeljena riječ COPYOID. Na primjer, **tempID-oid** se kopira kao **tempID-oidCOPYOID**.
6. Izaberite **Superiorni atribut** iz padajućeg izbornika. Superiorni atribut određuje atribut iz kojeg se nasljeđuju svojstva.
7. Izaberite **Sintaksu** iz padajućeg popisa. Pogledajte “Sintaksa atributa” na stranici 23 za dodatne informacije o sintaksi.
8. Unesite **Dužina atributa** koja specificira maksimalnu dužinu tog atributa. Dužina je izražena kao broj bajtova.
9. Izaberite **Dozvoli više vrijednosti** kontrolnu kućicu kako bi omogućili da atributi imaju više vrijednosti.
10. Izaberite pravilo podudaranja iz svakog od padajućih izbornika za pravila podudaranja jednakosti, poretka i podniza. Pogledajte “Pravila podudaranja” na stranici 21 za potpuni ispis pravila podudaranja.
11. Kliknite **IBM proširenja** karticu da promijenite dodatna proširenja za atribut ili kliknite **OK** da primijenite vaše izmjene ili kliknite **Opozvati** da se vratite na **Upravljanje atributima** bez ikakvih promjena.
12. Na kartici **IBM proširenja**:
    - Promjena **DB2 imena tablice** . Poslužitelj generira DB2 ime tablice ako je ovo polje ostavljeno prazno. Ako unesete DB2 ime tablice, morate također unijeti DB2 ime stupca.
    - Promjena **DB2 imena stupca**. Poslužitelj generira DB2 ime stupca ako je to polje ostavljeno prazno. Ako unesete DB2 ime stupca, također morate unijeti DB2 ime tablice.
    - Promijenite **Klasa sigurnosti** izborom **normalno**, **osjetljivo** ili **kritično** iz padajuće liste.
    - Promijenite **Pravila indeksiranja** izborom jednog ili više pravila indeksiranja. Pogledajte “Pravila indeksiranja” na stranici 22 za dodatne informacije o pravilima indeksiranja.

      Bilješka: Preporuča se da barem specificirate indeksiranje Jednako na bilo kojim atributima koji će se koristiti u filterima pretraživanja.
13. Kliknite na **OK** da primijenite svoje promjene ili kliknite na **Opoziv** da se vratite na **Upravljanje atributima** bez ikakvih promjena.

Bilješka: Ako ste kliknuli na **OK** na kartici **Općenito** bez dodavanja drugih proširenja, možete dodati ili promijeniti proširenja uređivanjem novog atributa.

Za pregled atributa koji se nalaze u shemi, izdajte naredbu:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Izaberite atribut kojeg želite kopirati. Koristite editor za promjenu odgovarajuće informacije i spremite promjene u <*ime datoteke*>. Nakon toga izdajte sljedeću naredbu:

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

gdje <*ime datoteke*>sadrži:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( <mynewAttribute-oid> NAME '<mynewAttribute>' DESC '<Novi
                 atribut koji sam kopirao za svoju LDAP aplikaciju> EQUALITY 2.5.13.2
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                     ACCESS-CLASS normal LENGTH 200 )
```

Brisanje atributa

Koristite ovu informaciju za brisanje atributa u stablu direktorija.

Nisu dozvoljene sve promjene sheme. Pogledajte “Nedozvoljene promjene sheme” na stranici 27 kako bi promijenili ograničenja.

Koristite bilo koju od sljedećih metoda kako bi obrisali atribut. Web administracijski alat je preferirana metoda.

Ako to već niste napravili, proširite **Upravljanje shemom** u području navigacije, nakon toga kliknite na **Upravljanje atributima**. Kako bi obrisali atribut:

1. Kliknite na radijski gumb uz atribut kojeg želite obrisati.
2. Kliknite **Brisanje**.
3. Promptirani ste kako bi potvrdili brisanje atributa. Kliknite na **OK** kako bi obrisali atribut ili kliknite na **Opoziv** kako bi se vratili na **Upravljanje atributima** bez ikakvih promjena.

Za brisanje atributa pomoću reda za naredbe, izdajte sljedeću naredbu:

```
ldapmodify -D <admindn> -w <adminpw> -i myschemadelete.ldif
```

Gdje **myschemadelete.ldif** datoteka uključuje:

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

Kopiranje sheme na druge poslužitelje

Koristite ovu informaciju za kopiranje sheme na druge poslužitelje.

Za kopiranje sheme na druge poslužitelje, napravite sljedeće:

1. Koristite ldapsearch pomoćni program kako bi kopirali shemu u datoteku:

   ```
   ldapsearch -b cn=schema -L "(objectclass=*)" > schema.ldif
   ```

2. Datoteka sheme će uključiti sve klase i atribute objekta Uredite LDIF datoteku da uključuje samo elemente sheme koje želite, ili, možda možete filtrirati ldapsearch izlaz koristeći alat kao što je grep. Vodite računa o tome da stavite atribute prije nego klase objekta koje ih referenciraju. Na primjer, mogli bi završiti sa sljedećom datotekom (primijetite da svaka linija koja se nastavlja ima jedno prazno mjesto na kraju, a linija koja nastavlja ima barem jedno prazno mjesto na početku linije).

   ```
   attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Neki dio
     informacija.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1'  'myattr1' )
     ACCESS-CLASS normal LENGTH 500 )
   attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Neki dio
     informacija.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2'  'myattr2' )
     ACCESS-CLASS normal LENGTH 500 )
   objectclasses: ( myobject-oid NAME 'myobject' DESC 'Predstavlja
     nešto.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
   ```

3. Umetnite linije prije svake linije objectclasses ili attributetype kako bi izgradili LDIF direktive za dodavanje tih vrijednost na unos cn=schema. Svaka klasa objekta i atribut moraju biti dodani kao pojedinačne preinake.

   ```
   dn: cn=schema
   changetype: modify
   add: attributetypes ibmattributetypes
   attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Neki dio
     informacija.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1'  'myattr1' )
     ACCESS-CLASS normal LENGTH 500 )

   dn: cn=schema
   changetype: modify
   add: attributetypes ibmattributetypes
   attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Neki dio
     informacija.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2'  'myattr2' )
   ```

```
  ACCESS-CLASS normal LENGTH 500 )

dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( myobject-oid NAME 'myobject' DESC 'Predstavlja
  nešto.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

4. Učitajte shemu na druge poslužitelje korištenjem ldapmodify pomoćnog programa:

```
ldapmodify -D cn=administrator -w <password> -f schema.ldif
```

Zadaci unosa direktorija

Koristite ovu informaciju za upravljanje unosima direktorija.

Za upravljanje unosima direktorija, proširite kategoriju **Upravljanje direktorijom** u području navigacije Web administracijskog alata.

Srodni koncepti

"Sufiks (kontekst imenovanja)" na stranici 12
Sufiks (poznat i kao kontekst imenovanja) je DN koji identificira najviši unos u lokalno zadržanoj hijerarhiji direktorija.

"Shema" na stranici 14
Shema je skup pravila koji upravlja načinom na koji se podaci mogu pohraniti u direktorij. Shema definira dozvoljeni tip unosa, njihovu strukturu atributa i sintaksu atributa.

"Vlasništva objekata LDAP direktorija" na stranici 74
Svaki objekt u LDAP direktoriju ima najmanje jednog vlasnika. Vlasnici objekata imaju tu moć da mogu brisati objekte. Vlasnici i administrator poslužitelja su jedini korisnici koji mogu mijenjati vlasnička svojstva i listu kontrole pristupa (ACL) objekta. Vlasništvo nad objektom može biti naslijeđeno ili eksplicitno.

Pregled stabla direktorija

Koristite ovu informaciju za pregled stabla direktorija.

Ovo trebate najprije napraviti.

Stupanj mora biti postavljen upravo tako.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije.
2. Kliknite na **Upravljanje unosima**.

Možete proširiti različita podstabla i izabrati unos na kojem želite raditi. Iz desne trake s alatima možete izabrati operaciju koju želite izvoditi.

Dodavanje unosa

Koristite ovu informaciju za dodavanje unosa u stablo direktorija.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijem** u području navigacije.
2. Kliknite na **Dodavanje unosa**.
3. Izaberite jednu **Strukturalnu klasu objekta** iz padajućeg popisa.
4. Kliknite **Sljedeće**.
5. Iz kućice Dostupno izaberite bilo koje **Pomoćne klase objekta** koje želite koristiti i kliknite na **Dodavanje**. Ponovite taj proces za svaku pomoćnu klasu objekta koju želite dodati. Možete i obrisati pomoćnu klasu objekta iz Kućice Izabrano tako da je izaberete i kliknete na **Ukloni**.
6. Kliknite **Sljedeće**.
7. U polje **Relativno DN** unesite relativno razlikovno ime (RDN) unosa kojeg dodajete, na primjer, cn=John Doe.
8. U polje **Nadređeno DN** unesite razlikovno ime unosa drveta kojeg ste izabrali, na primjer, ou=Austin, o=IBM. Možete i kliknuti na **Pregled** kako bi izabrali Nadređeno DN iz popisa. Možete i proširiti izbor kako bi vidjeli

druge izbore koji se nalaze niže u podstablu. Specificirajte svoj izbor i kliknite na **Izbor** kako bi specificirali Nadređeno DN koje želite. **Nadređeno DN** se postavlja na unos koji je izabran u stablu.

Bilješka: Ako ste pokrenuli taj zadatak iz panela **Upravljanje unosima**, to polje je već ispunjeno za vas.

9. Na kartici **Potrebni atributi** unesite vrijednosti za potrebne atribute. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
10. Kliknite na **Neobvezni atributi**.
11. Na karticu **Neobvezni atributi** unesite vrijednosti kako je to prikladno za neobvezne atribute. Pogledajte "Promjena binarnih atributa" na stranici 189 za informacije o dodavanju binarnih vrijednosti. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
12. Kliknite na OK kako bi kreirali unos.
13. Kliknite **ACL** gumb da promijenite listu kontrole pristupa za ovaj unos. Pogledajte "Lista kontrole pristupa" na stranici 62 za informacije o ACL-ovima.
14. Nakon što dovršite barem potrebna polja, kliknite na **Dodavanje** kako bi dodali novi unos ili kliknite na **Opoziv** kako bi se vratili na **Pregled stabla** bez ikakvih promjena na direktoriju.

Dodavanje unosa koji sadrži atribute s oznakama jezika

Koristite ovu informaciju za kreiranje unosa koji sadrži atribute s oznakama jezika.

Da bi kreirali unos koji sadrži atribute s oznakama jezika:

1. Omogućite oznake jezika. Pogledajte "Omogućavanje oznaka jezika" na stranici 120.
2. Iz kategorije **Upravljanje direktorijem** u navigacijskom područja u kliknite **Upravljanje unosima**.
3. Kliknite tipku **Uredi atribute**.
4. Izaberite atribut za koji želite kreirati oznaku jezika.
5. Kliknite **Vrijednost oznake jezika** da pristupite panelu **Vrijednosti oznake jezika**.
6. U polje **Oznaka jezika** unesite ime oznake koju kreirate. Oznaka mora počinjati s nastavkom lang-.
7. Unesite vrijednost za oznaku u polje **Vrijednost**.
8. Kliknite **Dodavanje**. Oznaka jezika i njena vrijednost se prikazuju u listi izbornika.
9. Kreirajte dodatne oznake jezika ili promijenite postojeće oznake jezika za atribute ponavljanjem koraka 4, 5 i 6. Nakon što kreirate oznake jezika koje želite, kliknite **OK**.
10. Proširite izbornik **Prikaz s oznakama jezika** i izaberite oznaku jezika. Kliknite **Promjena pogleda** i vrijednost atributa koju ste unijeli za tu oznaku jezika će se prikazati. Bilo koje vrijednosti koje dodate ili uredite u ovom pogledu primjenjuju se samo na izabranu oznaku jezika.
11. Kliknite **OK** kada završite.

Srodne reference

"Oznake jezika" na stranici 48
Termin *oznake jezika* definira mehanizam koji omogućuje Directory Serveru da pridruži kodove prirodnog jezika s vrijednostima koje se nalaze u direktoriju i omogućava klijentima da direktoriju šalju upite za vrijednosti koje odgovaraju određenim zahtjevima prirodnog jezika.

Brisanje unosa

Koristite ovu informaciju za brisanje unosa iz stabla direktorija.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla, sufiks ili unos na kojem želite raditi. Kliknite na **Obriši** iz desne trake s alatima.
2. Od vas se traži da potvrdite brisanje. Kliknite **OK**. Unos je obrisan iz direktorija i vraćeni ste na listu unosa.

Uređivanje unosa

Koristite ovu informaciju za uređivanje unosa u stablu direktorija.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos na kojem želite raditi. Kliknite na **Uredi atribute** iz desne trake s alatima.
2. Na kartici **Potrebni atributi** unesite vrijednosti za potrebne atribute. Pogledajte “Promjena binarnih atributa” na stranici 189 za informacije o dodavanju binarnih vrijednosti. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
3. Kliknite na **Neobvezni atributi**.
4. Na karticu **Neobvezni atributi** unesite vrijednosti kako je to prikladno za neobvezne atribute. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
5. Kliknite **Memberships**.
6. Ako ste kreirali bilo koje grupe na kartici **Članstvo**:
   - Izaberite grupu iz **Dostupne grupe** i kliknite na **Dodavanje** da napravite unos članom izabranog **Članstva statičke grupe**.
   - Izaberite grupu iz **Članstva statičke grupe** i kliknite na **Ukloni** kako bi uklonili unos iz izabrane grupe.
7. Ako je unos grupni unos, dostupna je kartica **Članovi**. Kartica **Članovi** prikazuje članove izabrane grupe. Možete dodati ili ukloniti članove iz grupe.
   - Kako bi dodali člana grupi:
     a. Kliknite na karticu **Višestruke vrijednosti** uz karticu **Članovi** ili na kartici **Članovi** kliknite na **Članovi**.
     b. U polje Član unesite DN unosa kojeg želite dodati.
     c. Kliknite **Dodavanje**.
     d. Kliknite **OK**.
   - Da uklonite član iz grupe:
     a. Kliknite na **Višestruke vrijednosti** uz karticu **Članovi** ili kliknite na karticu **Članovi** i kliknite na **Članovi**.
     b. Izaberite unos koji želite ukloniti.
     c. Kliknite **Ukloni**.
     d. Kliknite **OK**.
   - Da osvježite listu članova, kliknite na **Ažuriraj**.
8. Kliknite **OK** za promjenu unosa.

Dodavanje unosa

Koristite ovu informaciju za kopiranje unosa u stablo direktorija.

Ova funkcija je korisna ako kreirate slične unose. Kopija nasljeđuje sve atribute originala. Morate napraviti neke preinake na imenu novog unosa.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos, kao što je John Doe, na kojem želite raditi. Kliknite na **Kopiranje** iz desne trake s alatima.
2. Promijenite RDN unos u DN polje. Na primjer, promijenite cn=John Doe u cn=Jim Smith.
3. Na potrebnoj kartici s atributima promijenite unos na novi RDN. U ovom primjeru Jim Smith.
4. Promijenite druge potrebne atribute na odgovarajući način. U ovom primjeru promijenite sn iz Doe u Smith.
5. Kada ste dovršili potrebne promjene, kliknite na **OK** kako bi kreirali novi unos. Novi unos Jim Smith se dodajte na dno liste unosa.

Bilješka: Tom procedurom se kopiraju samo atributi unosa. Članstva grupe originalnog unosa se ne kopiraju na novi unos. Koristite funkciju Uređivanje atributa kako bi dodali članstvo.

Uređivanje lista kontrole pristupa

Koristite ovu informaciju za upravljanje lista kontrole pristupa (ACL-a).

Kako bi pregledali ACL svojstva korištenjem pomoćnog programa Web administracijski alat i kako bi radili s ACL-ovima, pogledajte “Zadaci Liste kontrole pristupa (ACL)” na stranici 201.

Srodni koncepti

“Lista kontrole pristupa” na stranici 62
Liste kontrole pristupa (ACL-ovi) sadrže sredstvo za zaštitu informacija pohranjenih u LDAP direktoriju. Administratori koriste ACL-ove kako bi ograničili pristup različitim dijelovima direktorija ili određenim unosima direktorija.

Dodavanje pomoćne klase objekta

Koristite ovu informaciju za dodavanje pomoćne klase objekta.

Koristite gumb **Dodavanje pomoćne klase** na traci s alatima kako bi dodali klasu pomoćnog objekta na postojeći unos u stablu direktorija. Pomoćna klasa objekta osigurava dodatne atribute na unos na koji se dodaje.

Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos, kao što je John Doe, na kojem želite raditi. Kliknite na **Dodavanje pomoćne klase** iz desne trake s alatima.

1. Iz kućice Dostupno izaberite bilo koje **Pomoćne klase objekta** koje želite koristiti i kliknite na **Dodavanje**. Ponovite taj proces za svaku pomoćnu klasu objekta koju želite dodati. Možete i obrisati pomoćnu klasu objekta iz Kućice Izabrano tako da je izaberete i kliknete na **Ukloni**.
2. Na kartici **Potrebni atributi** unesite vrijednosti za potrebne atribute. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
3. Kliknite na **Neobvezni atributi**.
4. Na karticu **Neobvezni atributi** unesite vrijednosti kako je to prikladno za neobvezne atribute. Ako želite dodati više od jedne vrijednosti za određeni atribut, kliknite na **Višestruke vrijednosti** i onda dodajte vrijednosti jednu po jednu.
5. Kliknite **Memberships**.
6. Ako ste kreirali bilo koje grupe na kartici **Članstvo**:
   - Izaberite grupu iz **Dostupne grupe** i kliknite na **Dodavanje** da napravite unos članom izabranog **Članstva statičke grupe**.
   - Izaberite grupu iz **Članstva statičke grupe** i kliknite na **Ukloni** kako bi uklonili unos iz izabrane grupe.
7. Kliknite **OK** za promjenu unosa.

Brisanje pomoćne klase

Koristite ovu informaciju za brisanje pomoćne klase.

Iako možete obrisati pomoćne klase za vrijeme procedure dodaj pomoćnu klasu, lakše je koristiti funkciju obriši pomoćnu klasu ako ćete brisati jednu pomoćnu klasu iz unosa. No, ako ćete obrisati više pomoćnih klasa iz unosa, možda je prikladnije korištenje funkcije dodavanje pomoćne klase.

1. Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije i nakon toga kliknite na **Upravljanje unosima**. Možete proširiti različita podstabla i izabrati unos, kao što je John Doe, na kojem želite raditi. Kliknite na **Brisanje pomoćne klase** iz desne trake s alatima.
2. U listi pomoćnih klasa izaberite onu koju želite obrisati i pritisnite **OK**.
3. Od vas će se tražiti da potvrdite brisanje, kliknite na **OK**.
4. Pomoćna klasa se briše iz unosa i vi se vraćate na popis unosa.

Ponovite te korake za svaku pomoćnu klasu koju želite obrisati.

Promjena članstva grupe

Koristite ovu informaciju za promjenu članstva grupe.

Ako to već niste napravili, proširite kategoriju **Upravljanje direktorijom** u području navigacije.

1. Kliknite na **Upravljanje unosima**.
2. Izaberite korisnika iz stabla direktorija i kliknite na ikonu **Uređivanje atributa** na traci s alatima.
3. Kliknite karticu **Članstva**.
4. Da bi promijenili članstvo korisnika. Na panelu **Promjena članstva** prikazuju se **Dostupne grupe** na koje se može dodati korisnik, kao i **Članstvo statičke grupe** unosa.
   - Izaberite grupu iz **Dostupne grupe** i kliknite na **Dodavanje** kako bi unos postao članom izabrane grupe.
   - Izaberite grupu iz **Članstvo statičke grupe** i kliknite ne **Ukloni** kako bi uklonili unos iz izabrane grupe.
5. Kliknite na **OK** kako bi spremili svoje promjene ili kliknite na **Opoziv** kako bi se vratili na prethodni panel bez da se spreme vaše promjene.

Pretraživanje unosa direktorija

Koristite ovu informaciju za pretraživanje unosa direktorija.

Postoje tri opcije za pretraživanje stabla direktorija:

- Jednostavno pretraživanje koje koristi preddefinirani skup kriterija pretraživanja
- Napredno pretraživanje koje koristi korisnički definiran skup kriterija pretraživanja
- Ručno pretraživanje

Opcije pretraživanja su dostupne proširivanjem kategorije **Upravljanje direktorija** u području navigacije, kliknite na **Nalaženje unosa**. Izaberite karticu **Filteri pretraživanja** ili **Opcije**.

Bilješka: Binarni unosi, kao što su lozinke, se ne mogu pretraživati.

Jednostavno pretraživanje koristi default kriterij pretraživanja:

- Bazni DN je **Svi sufiksi**
- Opseg pretraživanje je **Podstablo**
- Veličina pretraživanja je **Neograničena**
- Vremensko ograničenje je **Neograničeno**
- Derefenciranje zamjenskog imena je **nikad**
- Referali potjere nisu izabrani (off)

Napredno pretraživanje vam omogućava da specificirate ograničenja pretraživanja i omogućite filtere pretraživanja. Koristite Jednostavno pretraživanje kako bi koristili default kriterij pretraživanja.

1. Kako bi izvodili jednostavno pretraživanje:
   a. Na kartici **Filter pretraživanja** kliknite na **Jednostavno pretraživanje**.
   b. Izaberite klasu objekta iz padajuće liste.
   c. Izaberite određeni atribut za izabrani tip unosa. Ako ste izabrali traženje određenog atributa, izaberite atribut iz padajuće liste i unesite vrijednost atributa u kućicu **Isto kao**. Ako ne specificirate atribut, pretraživanje vraća sve unose direktorija izabranog tipa unosa.
2. Kako bi izvodili napredno pretraživanje:
   a. Na kartici **Filter pretraživanja** kliknite na **Napredno pretraživanje**.
   b. Izaberite **Atribut** iz padajuće liste.
   c. Izaberite operater **Usporedba**.
   d. Unesite **Vrijednost** za usporedbu.
   e. Koristite gumbe operatora pretraživanja za kompleksne upite.
      - Ako ste već dodali barem jedan filter pretraživanja, specificirajte dodatni kriterij i kliknite na **AND**. **AND** naredba vraća unose koji se podudaraju za oba skupa kriterija pretraživanja.
      - Ako ste već dodali barem jedan filter pretraživanja, specificirajte dodatni kriterij i kliknite na **OR**. Naredba **OR** vraća unose koji se podudaraju s bilo kojim skupom kriterija pretraživanja.

- Kliknite na **Dodavanje** da dodate kriterij filtera pretraživanja naprednom pretraživanju.
- Kliknite na **Obriši** da uklonite kriterij filtera pretraživanja iz naprednog pretraživanja.
- Kliknite na **Reset** da obrišete sve filtere pretraživanja.

3. Za izvođenje ručnog pretraživanje, kreirajte filter pretraživanja.

   Na primjer, kako bi pretraživali prezimena unesite sn=* u polje. Ako pretražujete više atributa, morate koristiti sintaksu filtera pretraživanja. Na primjer, kako bi pretraživali prezimena određenog unosa, unesite:

   `(&(sn=*)(dept=<departmentname>))`

Na **kartici Opcije**:

- **Pretražite bazni DN** - Izaberite sufiks iz padajuće liste kako bi pretraživali samo unutar tog sufiksa.

  Bilješka: Ako ste započeli ovaj zadatak iz **Upravljanje unosima** panela, ovo je polje uneseno za vas. Izabrali ste **Nadređeno DN** prije nego ste kliknuli na **Dodavanje** kako bi pokrenuli proces dodaj unos.

  Možete izabrati i **Svi sufiksi** kako bi pretražili cijelo stablo.

  Bilješka: Pretraživanje po podstablu s izabranim **Svi nastavci** neće vratiti informacije o shemi, promijeniti informacije o dnevniku, niti bilo što iz sistemski zaštićene pozadine.
- **Opseg pretraživanja**
  - Izaberite **Objekt** kako bi pretraživali samo unutar izabranog objekta.
  - Izaberite **Jedna razina** kako bi pretraživali samo neposredno podređene izabranog objekta.
  - Izaberite **Podstablo** kako bi pretraživali sve potomke izabranog unosa.
- **Granica veličine pretraživanja** - Unesite maksimalan broj unosa koje ćete pretraživati ili izaberite **Neograničeno**.
- **Granica vremena pretraživanja** - Unesite maksimalan broj sekundi za pretraživanje ili izaberite **Neograničeno**.
- Izaberite tip **Dereferenciranja zamjenskog imena** iz padajućeg popisa.
  - **Nikad** - Ako je izabrani unos zamjensko ime, on se ne dereferencira za pretraživanje, odnosno, pretraživanje zanemaruje referencu na zamjensko ime.
  - **Pronalaženje** - Ako je izabrani unos zamjensko ime, pretraživanje dereferencira zamjensko ime i pretražuje iz lokacije zamjenskog imena.
  - **Pretraživanje** - Izabrani unos se ne dereferencira, no dereferenciraju se svi unosi pronađeni u pretraživanju.
  - **Uvijek** - Dereferenciraju se sva zamjenska imena na koje se je naišlo kod pretraživanja.
- Izaberite **Referali potjere** kontrolnu kućicu kako bi slijedili referale na drugog poslužitelja ako se referal vrati u pretraživanju. Kada referal usmjerava pretraživanje na drugog poslužitelja, veza na poslužitelja koristi trenutne vjerodajnice. Ako ste prijavljeni kao Anoniman, možda ćete se trebati prijaviti na poslužitelja korištenjem ovlaštenog DN-a.

Srodni zadaci

"Prilagođavanje postavki pretraživanja" na stranici 122
Koristite ovu informaciju za kontroliranje korisničkih sposobnosti pretraživanja.

Srodne reference

"Parametri pretraživanja" na stranici 46
Da bi ograničili broj resursa korištenih od strane poslužitelja, administrator može postaviti parametre pretraživanja da ograniči korisničke mogućnosti pretraživanja. Mogućnosti pretraživanja se također mogu proširiti za posebne korisnika.

Promjena binarnih atributa

Koristite ovu informaciju za unos, eksport ili brisanje binarnih podataka.

Ako atribut traži binarne podatke, gumb **Binarni podaci** je prikazan uz polje atributa. Ako atribut nema podatke, polje je prazno. Budući se binarni atributi ne mogu prikazati, ako atribut sadrži binarne podatke, polje prikazuje **Binarni podaci - 1**. Ako atribut sadrži više vrijednosti, polje se prikazuje kao padajući popis.

Kliknite na gumb **Binarni podaci** kako bi radili s binarnim atributima.

Možete unositi, eksportirati ili brisati binarne podatke.

1. Kako bi dodali binarne podatke na atribut:
   a. Kliknite tipku **Binarni podaci**.
   b. Kliknite **Import**.
   c. Možete unijeti ime staze za datoteku koju želite ili kliknuti na **Pregled** kako bi locirali i izabrali binarnu datoteku.
   d. Kliknite na **Submitiraj datoteku**. Prikazat će se poruka Datoteka učitana.
   e. Kliknite **Zatvaranje**. Sada je prikazano **Binarni podaci - 1** pod **Unosi binarnih podataka**.
   f. Ponovite proces importiranja za onoliko binarnih datoteka koliko ih želite dodati. Naredni upisi se ispisuju kao **Binarni podaci - 2**, **Binarni podaci -3** itd.
   g. Kada završite s dodavanjem binarnih podataka, kliknite na **OK**.
2. Kako bi eksportirali binarne podatke:
   a. Kliknite tipku **Binarni podaci**.
   b. Kliknite **Eksport**.
   c. Kliknite na vezu **Binarni podaci za učitati**.
   d. Slijedite upute na vašem čarobnjaku kako bi prikazali binarnu datoteku ili je spremili na novu lokaciju.
   e. Kliknite **Zatvaranje**.
   f. Ponovite proces eksportiranja za toliko binarnih datoteka koliko ih želite eksportirati.
   g. Kada završite s importiranjem binarnih podataka, kliknite na **OK**.
3. Kako bi obrisali binarne podatke:
   a. Kliknite tipku **Binarni podaci**.
   b. Označite binarnu datoteku koju želite obrisati. Može se izabrati više datoteka.
   c. Kliknite **Brisanje**.
   d. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**. Binarni podaci koji su bili označeni za brisanje se uklanjaju iz popisa.
   e. Kada dovršite brisanje podataka, kliknite na **OK**.

Bilješka: Binarni atributi se mogu pretraživati samo da li postoje.

Zadaci korisnika i grupe

Koristite ovu informaciju za upravljanje korisnicima i grupama.

Za upravljanje korisnicima i grupama, proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

Srodni koncepti

“Grupe i uloge” na stranici 55
Koristite grupe i uloge za organiziranje i kontroliranje pristupa ili dozvola članova.

Zadaci korisnika

Koristite ovu informaciju za upravljanje korisnicima.

Nakon što ste postavili svoja područja i predloške, možete ih popuniti korisnicima.

Srodne reference

“Provjera autentičnosti” na stranici 78
Koristite metodu provjere autentičnosti za kontroliranje pristupa unutar Directory Servera.

Dodavanje korisnika:

Koristite ovu informaciju za dodavanje korisnika.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Dodavanje korisnika** ili kliknite na **Upravljanje korisnicima** i kliknite na **Dodavanje**.
2. Iz padajućeg izbornika izaberite područje kojem želite dodati korisnika.
3. Kliknite **Sljedeće**. Prikazat će se predložak koji je pridružen tom području. Popunite potrebna polja koja su označena zvjezdicom (*) i bilo koja druga polja na karticama. Ako ste već kreirali grupe unutar područja, možete dodati korisnika na jednu ili više grupa.
4. Kada ste završili, kliknite na **Završetak**.

Pronalaženje korisnika unutar područja:

Koristite ovu informaciju za pronalaženje korisnika unutar područja.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Nalaženje korisnika** ili kliknite na **Upravljanje korisnicima** i kliknite na **Nalaženje**.
2. Izaberite područje koje želite pretraživati iz polja **Izbor područja**.
3. Unesite niz pretraživanja u polje **Atribut imenovanja**. Podržani su zamjenski znakovi, na primjer, ako ste unijeli ***smith**, rezultat su svi unosi čiji atribut imenovanja završava sa smith.
4. Možete izvoditi sljedeće operacije na izabranom korisniku:
   - **Uređivanje** - Pogledajte “Uređivanje informacije o korisniku”.
   - **Kopiranje** - Pogledajte “Kopiranje korisnika”.
   - **Brisanje** - Pogledajte “Uklanjanje korisnika” na stranici 192.
5. Kada ste gotovi, kliknite na **OK**.

Uređivanje informacije o korisniku:

Koristite ovu informaciju za uređivanje informacija o korisniku.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljanje korisnicima**.
2. Izaberite područje iz padajućeg izbornika. Kliknite na **Pregled korisnika**, ako korisnici nisu već prikazani u kućici **Korisnici**.
3. Izaberite korisnike koje želite uređivati i kliknite na **Uređivanje**.
4. Promijenite informacije o zadatku, promijenite članstvo grupe.
5. Kada ste gotovi, kliknite na **OK**.

Kopiranje korisnika:

Koristite ovu informaciju za kopiranje korisnika.

Ako trebate kreirati više korisnika koji imaju većinom identične informacije, možete kreirati dodatne korisnike kopiranjem inicijalnog korisnika i modificiranjem informacija.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljanje korisnicima**.
2. Izaberite područje iz padajućeg izbornika. Kliknite na **Pregled korisnika**, ako korisnici nisu već prikazani u kućici **Korisnici**.
3. Izaberite korisnike koje želite kopirati i kliknite na **Kopiranje**.
4. Promijenite odgovarajuće informacije za novog korisnika, na primjer potrebne informacije koje identificiraju određenog korisnika, kao što je sn ili cn. Informacije koje su zajedničke za oba korisnika se ne trebaju mijenjati.

5. Kada ste gotovi, kliknite na **OK**.

Uklanjanje korisnika:

Koristite ovu informaciju za uklanjanje korisnika.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljanje korisnicima**.
2. Izaberite područje iz padajućeg izbornika. Kliknite na **Pregled korisnika**, ako korisnici nisu već prikazani u kućici **Korisnici**.
3. Izaberite korisnika kojeg želite ukloniti i kliknite na **Brisanje**.
4. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**.
5. Korisnik se uklanja iz popisa korisnika.

Zadaci grupe

Koristite ovu informaciju za upravljanje grupama.

Nakon što ste postavili svoja područja i predloške, možete kreirati grupe.

Dodavanje grupa:

Koristite ovu informaciju za dodavanje grupa.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Dodavanje grupe** ili kliknite na **Upravljanje grupama** i kliknite na **Dodavanje**.
2. Unesite ime grupe koju želite kreirati.
3. Izaberite područje u koje želite dodati grupu iz padajućeg izbornika.
4. Kliknite na **Završetak** kako bi kreirali grupu. Ako već imate korisnike u području, možete kliknuti na **Sljedeće** i izabrati korisnike koji će se dodati grupi. Zatim kliknite **Završi**.

   Srodni koncepti

   “Grupe i uloge” na stranici 55
   Koristite grupe i uloge za organiziranje i kontroliranje pristupa ili dozvola članova.

Dodavanje grupa unutar područja:

Koristite ovu informaciju za dodavanje grupa unutar područja.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Nalaženje grupe** ili kliknite na **Upravljanje grupama** i kliknite na **Nalaženje**.
2. Izaberite područje koje želite pretraživati iz polja **Izbor područja**.
3. Unesite niz pretraživanja u polje **Atribut imenovanja**. Podržani su zamjenski znakovi, na primjer, ako ste unijeli ***klub**, rezultat su sve grupe koje imaju atribut imenovanja klub, na primjer, knjižni klub, šahovski klub, vrtni klub itd.
4. Možete izvoditi sljedeće operacije na izabranoj grupi:
   - **Uređivanje** - Pogledajte “Uređivanje informacije o grupi”.
   - **Kopiranje** - Pogledajte “Kopiranje grupe” na stranici 193.
   - **Brisanje** - Pogledajte “Uklanjanje grupe” na stranici 193.
5. Kada ste gotovi, kliknite na **Zatvaranje**.

Uređivanje informacije o grupi:

Koristite ovu informaciju za uređivanje informacija o grupi.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljanje grupama**.
2. Izaberite područje iz padajućeg izbornika. Kliknite na **Pregled grupa** ako grupe nisu već prikazane u kućici **Grupe**.
3. Izaberite grupu koju želite obrađivati i kliknite na **Uređivanje**.
4. Možete kliknuti na **Filter** kako bi ograničili broj **Dostupnih korisnika**. Na primjer, unošenje *smith u polje Prezime ograničava dostupne korisnike na one čije ime završava sa smith, kao što su Ann Smith, Bob Smith, Joe Goldsmith itd.
5. Možete dodati ili ukloniti korisnike iz grupe.
6. Kada ste gotovi, kliknite na **OK**.

Kopiranje grupe:

Koristite ovu informaciju za kopiranje grupe.

Ako trebate kreirati više grupa koje imaju većinom iste članove, možete kreirati dodatne grupe kopiranjem inicijalne grupe i modificiranjem informacije.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljanje grupama**.
2. Izaberite područje iz padajućeg izbornika. Kliknite na **Pregled grupa** ako grupe već nisu prikazane u kućici **Grupe**.
3. Izaberite grupu koju želite kopirati i kliknite na **Kopiranje**.
4. Promijenite ime grupe u polju **Ime grupe**. Nova grupa ima iste članove kao i originalna grupa.
5. Možete promijeniti članove grupe.
6. Kada ste gotovi, kliknite na **OK**. Kreirana je nova grupa i ona sadrži iste članove kao originalna grupa sa svim preinakama dodavanja ili uklanjanja koje ste izveli za vrijeme procedure kopiranja.

Uklanjanje grupe:

Koristite ovu informaciju za uklanjanje grupe.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljanje grupama**.
2. Izaberite područje iz padajućeg izbornika. Kliknite na **Pregled grupa** ako grupe nisu već prikazane u kućici **Grupe**.
3. Izaberite grupu koju želite ukloniti i kliknite na **Brisanje**.
4. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**.
5. Grupa se uklanja iz popisa grupa.

Zadaci područja i predložaka korisnika

Koristite ovu informaciju za upravljanje područjima i predlošcima korisnika.

Za upravljanje područjima i predlošcima korisnika, kliknite na **Područja i predlošci** u području navigacije Web administracijskog alata. Koristite područja i predloške korisnika kako bi olakšali drugima da unose podatke u direktorij.

Srodni koncepti

“Područja i predlošci korisnika” na stranici 45
Područje i objekti predloška korisnika nađeni u Web administration tool koriste se kako bi se korisniku olakšala obveza da razumije neka temeljna LDAP pitanja.

Kreiranje područja

Koristite ovu informaciju za kreiranje područja.

Za kreiranje područja, napravite sljedeće:

1. Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.
2. Kliknite na **Dodavanje područja**.
   - Unesite ime za područje. Na primjer, **realm1**.
   - Unesite Nadređeno DN koje identificira lokaciju područja. Taj unos je u obliku sufiksa, na primjer o=ibm,c=us. Taj unos može biti sufiks ili unos negdje drugdje u direktoriju. Možete kliknuti i na **Pregled** da izaberete lokaciju podstabla koju želite.
3. Kliknite na **Sljedeće** za nastavak ili kliknite na **Završetak**.
4. Ako ste kliknuli na **Sljedeće**, ponovno pregledajte informacije. U tom trenutku još niste stvarno kreirali područje tako da se mogu zanemariti **Predložak korisnika** i **Filter pretraživanja korisnika**.
5. Kliknite na **Završetak** da kreirate područje.

Srodni koncepti

"Područja i predlošci korisnika" na stranici 45
Područje i objekti predloška korisnika nađeni u Web administration tool koriste se kako bi se korisniku olakšala obveza da razumije neka temeljna LDAP pitanja.

Kreiranje administratora područja

Koristite ovu informaciju za kreiranje administratora područja.

Kako bi kreirali administratora područja, morate kreirati grupu administracije za područje tako da napravite sljedeće:

1. Kreirajte grupu administracije područja.
   a. Proširite kategoriju **Upravljanje direktorijom** u području navigacije Web administracijskog alata.
   b. Kliknite na **Upravljanje unosima**.
   c. Proširite stablo i izaberite područje koje ste upravo kreirali, **cn=realm1,o=ibm,c=us**.
   d. Kliknite na **Uredi ACL**.
   e. Kliknite karticu **Vlasnici** .
   f. Provjerite da li je označeno **Proširivanje korisnika**.
   g. Unesite DN za područje, **cn=realm1,o=ibm,c=us**.
   h. Promijenite **Tip** u grupu.
   i. Kliknite **Dodavanje**.
2. Kreirajte unos administratora. Ako već nemate unos korisnika za administratora, morate ga kreirati.
   a. Proširite kategoriju **Upravljanje direktorijom** u području navigacije Web administracijskog alata.
   b. Kliknite na **Upravljanje unosima**.
   c. Proširite drvo na lokaciju na kojoj želite da prebiva unos administratora.

      Bilješka: Smještanjem unosa administratora izvan područja se izbjegava da bi administrator mogao slučajno obrisati njega ili nju. U ovom primjeru bi lokacija mogla biti **o=ibm,c=us**.
   d. Kliknite **Dodavanje**.
   e. Izaberite **Strukturalna klasa objekta**, na primjer **inetOrgPerson**.
   f. Kliknite **Sljedeće**.
   g. Izaberite pomoćnu klasu objekta koju želite dodati.
   h. Kliknite **Sljedeće**.
   i. Unesite potrebne atribute za unos. Na primjer,
      - **RDN** cn=JohnDoe
      - **DN** o=ibm,c=us

- **cn** John Doe
- **sn** Doe

j. Na kartici **Drugi atributi** provjerite da li vam je dodijeljena lozinka.
k. Kada ste završili, kliknite na **Završetak**.

3. Dodavanje administratora na grupu administracije.
   a. Proširite kategoriju **Upravljanje direktorijom** u području navigacije Web administracijskog alata.
   b. Kliknite na **Upravljanje unosima**.
   c. Proširite stablo i izaberite područje koje ste upravo kreirali, **cn=realm1,o=ibm,c=us**.
   d. Kliknite na **Uredi atribute**.
   e. Kliknite karticu **Članovi**.
   f. Kliknite **Članovi**.
   g. U polje **Članovi** unesite DN administratora, u ovom primjeru **cn=John Doe,o=ibm,c=us**.
   h. Kliknite **Dodavanje**. DN se prikazuje u popisu **Članovi**.
   i. Kliknite **OK**.
   j. Kliknite **Ažuriraj**. DN se prikazuje u popisu **Trenutni članovi**.
   k. Kliknite **OK**.
4. Kreirali ste administratora koji može upravljati unosima unutar područja.

Kreiranje predloška

Koristite ovu informaciju za kreiranje predloška.

Nakon što ste kreirali područje, vaš sljedeći korak je kreiranje predloška korisnika. Predložak vam pomaže da organizirate informacije koje želite unijeti. Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite **Dodavanje predloška korisnika**.
   - Unesite ime za predložak, na primjer **template1**.
   - Unesite lokaciju na kojoj će predložak prebivati. U svrhu replikacije, locirajte predložak u podstablu područja koje će koristiti taj predložak. Na primjer, područje kreirano u prethodnim operacijama **cn=realm1,o=ibm,c=us**. Možete kliknuti na **Pregled** za izbor drugog podstabla za lokaciju predloška.
2. Kliknite **Sljedeće**. Možete kliknuti na **Završetak** kako bi kreirali prazan predložak. Kasnije možete dodati informacije predlošku, pogledajte “Uređivanje predloška” na stranici 200.
3. Ako ste kliknuli na **Sljedeće**, za predložak izaberite strukturalnu klasu objekta, na primjer **inetOrgPerson**. Možete dodati i sve pomoćne klase objekta koje želite.
4. Kliknite **Sljedeće**.
5. Tablica **Potrebno** je bila kreirana na predlošku. Možete promijeniti informacije sadržane u ovoj kartici.
   a. Izaberite **Potrebno** u izborniku kartice i kliknite na **Uredi**. Prikazan je panel **Uredi karticu**. Možete vidjeti ime kartice **Potrebno** i izabrane atribute koje treba klasa objekta, **inetOrgPerson**:
      - *sn - prezime
      - *cn - uobičajeno ime

      Bilješka: * označava potrebne informacije.
   b. Ako želite dodati dodatne informacije na tu karticu, izaberite atribut iz izbornika **Atributi**. Na primjer, izaberite **departmentNumber** i kliknite na **Dodavanje**. Izaberite **employeeNumber** i kliknite **Dodavanje**. Izaberite **title** i kliknite **Dodavanje**. Izbornik **Izabrani atributi** sada izgleda:
      - title
      - employeeNumber
      - departmentNumber
      - *sn

- *cn

c. Možete promijeniti način na koji se ta polja pojavljuju na predlošku tako da osvijetlite izabrane atribute i kliknete na **Premjesti gore** ili **Premjesti dolje**. Time se mijenja položaj atributa za jedan položaj. Ponavljajte tu proceduru tako dugo dok sve atribute ne stavite u željeni poredak. Na primjer,
   - *sn
   - *cn
   - title
   - employeeNumber
   - departmentNumber

d. Također možete promijeniti svaki izabrani atribut.
   1) Osvijetlite atribut u kućici **Izabrani atributi** i kliknite na **Uredi**.
   2) Možete promijeniti ime prikaza polja kojeg koristite na predlošku. Na primjer, ako želite da se **brojOdjela** prikaže kao **Broj odjela**, unesite to u polje **Prikaz imena**.
   3) Možete osigurati i default vrijednost kojom će se popuniti polja atributa u predlošku. Na primjer, ako su većina korisnika koji će se unijeti članovi Odjela 789, možete unijeti 789 kao default vrijednost. Polje na predlošku će biti ispunjeno sa 789. Vrijednost se može promijeniti kada dodate stvarne informacije o korisniku.
   4) Kliknite **OK**.

e. Kliknite **OK**.

6. Kako bi kreirali drugu kategoriju kartice za dodatne informacije, kliknite na **Dodavanje**.
   - Unesite ime za novu karticu. Na primjer, Informacije o adresi.
   - Za tu karticu izaberite atribute iz izbornika **Atributi**. Na primjer, izaberite **homePostalAddress** i kliknite na **Dodavanje**. Izaberite **postOfficeBox** i kliknite **Dodavanje**. Izaberite **telephoneNumber** i kliknite **Dodavanje**. Izaberite **homePhone** i kliknite **Dodavanje**. Izaberite **facsimileTelephoneNumber** i kliknite na **Dodavanje**. Izbornik **Izabrani atributi** sada izgleda:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone
     – facsimileTelephoneNumber
   - Možete promijeniti način na koji se ta polja pojavljuju na predlošku tako da osvijetlite izabrane atribute i kliknete na **Premjesti gore** ili **Premjesti dolje**. Time se mijenja položaj atributa za jedan položaj. Ponavljajte tu proceduru tako dugo dok sve atribute ne stavite u željeni poredak. Na primjer,
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – facsimileTelephoneNumber
     – homePhone
   - Kliknite **OK**.

7. Ponovite taj proces za onoliko kartica koliko ih želite kreirati. Kada ste gotovi, kliknite na **Završetak** kako bi kreirali predložak.

Dodavanje predloška poslužitelju područja

Koristite ovu informaciju za dodavanje predloška poslužitelju područja.

Nakon što ste kreirali područje i predložak, trebate dodati predložak na područje. Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljanje područjima**.
2. Izaberite područje kojem želite dodati predložak, u ovom primjeru **cn=realm1,o=ibm,c=us** i kliknite na **Uredi**.

3. Spustite se na **Predložak korisnika** i proširite padajući izbornik.
4. Izaberite predložak, u ovom primjeru **cn=template1,cn=realm1,o=ibm,c=us**.
5. Kliknite **OK**.
6. Kliknite **Zatvaranje**.

Kreiranje grupa

Koristite ovu informaciju za kreiranje grupa.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite **Dodavanje grupe**.
2. Unesite ime grupe koju želite kreirati. Na primjer **grupa1**.
3. Iz padajućeg izbornika izaberite područje kojem želite dodati korisnika. U ovom slučaju **područje1**.
4. Kliknite na **Završetak** kako bi kreirali grupu. Ako već imate korisnike u području, možete kliknuti na **Sljedeće** i izabrati korisnike koji će se dodati grupi grupa1. Zatim kliknite **Završi**.

Srodni koncepti

"Grupe i uloge" na stranici 55
Koristite grupe i uloge za organiziranje i kontroliranje pristupa ili dozvola članova.

Dodavanje korisnika poslužitelju područja

Koristite ovu informaciju za dodavanje korisnika poslužitelja područja.

Proširite kategoriju **Korisnici i grupe** u području navigacije Web administracijskog alata.

1. Kliknite **Dodavanje korisnika**.
2. Iz padajućeg izbornika izaberite područje kojem želite dodati korisnika. U ovom slučaju **područje1**.
3. Kliknite **Sljedeće**. Prikazuje se predložak kojeg ste upravo kreirali, predložak1. Popunite potrebna polja koja su označena zvjezdicom (*) i bilo koja druga polja na karticama. Ako ste već kreirali grupe unutar područja, možete dodati korisnika na jednu ili više grupa.
4. Kada ste završili, kliknite na **Završetak**.

Zadaci područja

Koristite ovu informaciju za upravljanje područjima.

Nakon što ste postavili i popunili svoje početno područje, možete dodavati više područja ili mijenjati postojeća područja.

Proširite kategoriju **Područja i predlošci** u području navigacije i kliknite na **Upravljanje područjima**. Prikazuje se popis postojećih područja. Iz tog panela možete dodati područje, uređivati područje, ukloniti područje ili uređivati liste kontrole pristupa (ACL-ovi) područja.

Dodavanje poslužitelja područja:

Koristite ovu informaciju za dodavanje poslužitelja područja.

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite na **Dodavanje područja**.
   - Unesite ime za područje. Na primjer, **područje2**.
   - Ako imate područja koja postoje već od ranije, na primjer, **područje1**, možete izabrati to područje kako bi se njegove postavke kopirale na područje koje kreirate.
   - Unesite Nadređeno DN koje identificira lokaciju područja. Taj unos je u obliku sufiksa, na primjer **o=ibm,c=us**. Možete kliknuti i na **Pregled** da izaberete lokaciju podstabla koju želite.
2. Kliknite **Sljedeće** za nastavak ili **Završi**.
3. Ako ste kliknuli na **Sljedeće**, ponovno pregledajte informacije.

4. Izaberite **Predložak korisnika** iz padajućeg izbornika. Ako ste kreirali postavke iz područja koje je već ranije postojalo, predložak je već popunjen.
5. Unesite **Filter pretraživanja korisnika**.
6. Kliknite na **Završetak** da kreirate područje.

Uređivanje područja:

Koristite ovu informaciju za uređivanje područja.

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

- Kliknite na **Upravljanje područjima**.
- Izaberite područje koje želite uređivati iz popisa područja.
- Kliknite **Uređivanje**.
  - Možete koristiti gumb **Pregled** za promjenu
    - Grupe administratora
    - Spremnika grupe
    - Spremnika korisnika
  - Možete izabrati drugi predložak iz padajućeg izbornika.
  - Kliknite **Uredi** da promijenite **Korisnički filter pretraživanja**.
- Kliknite **OK** pri završetku.

Uklanjanje područja:

Koristite ovu informaciju za uklanjanje područja.

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljanje područjima**.
2. Izaberite područje koje želite ukloniti.
3. Kliknite **Brisanje**.
4. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**.
5. Područje je uklonjeno iz popisa područja.

Uređivanje ACL-ova na području:

Koristite ovu informaciju za uređivanje ACL-ova na području.

Kako bi pregledali ACL svojstva korištenjem pomoćnog programa Web administracijski alat i kako bi radili s ACL-ovima, pogledajte “Zadaci Liste kontrole pristupa (ACL)” na stranici 201.

Srodni koncepti

“Lista kontrole pristupa” na stranici 62
Liste kontrole pristupa (ACL-ovi) sadrže sredstvo za zaštitu informacija pohranjenih u LDAP direktoriju. Administratori koriste ACL-ove kako bi ograničili pristup različitim dijelovima direktorija ili određenim unosima direktorija.

Zadaci predloška

Koristite ovu informaciju za upravljanje predlošcima.

Nakon što ste kreirali vaš početni predložak, možete dodati više predložaka ili promijeniti postojeće predloške.

Proširite kategoriju **Područja i predlošci** u području navigacije i kliknite na **Upravljanje predlošcima korisnika**. Prikazuje se popis postojećih predložaka. Iz tog panela možete dodati predložak, uređivati predložak, ukloniti predložak ili uređivati liste kontrole pristupa (ACL-ovi) predloška.

Dodavanje predloška:

Koristite ovu informaciju za dodavanje predloška korisnika.

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite na **Dodavanje predloška korisnika** ili kliknite na **Upravljanje predlošcima korisnika** i kliknite na **Dodavanje**.
   - Unesite ime za novi predložak. Na primjer, **predložak2**.
   - Ako imate predloške koji postoje od ranije, na primjer **predložak1**, možete izabrati predložak kako bi se njegove postavke kopirale na predložak kojeg kreirate.
   - Unesite Nadređeno DN koje identificira lokaciju predloška. Taj unos je u obliku DN-a, na primjer **cn=realm1,o=ibm,c=us**. Možete kliknuti i na **Pregled** da izaberete lokaciju podstabla koju želite.
2. Kliknite **Sljedeće**. Možete kliknuti na **Završetak** kako bi kreirali prazan predložak. Kasnije možete dodati informacije predlošku, pogledajte “Uređivanje predloška” na stranici 200.
3. Ako ste kliknuli na **Sljedeće**, za predložak izaberite strukturalnu klasu objekta, na primjer **inetOrgPerson**. Možete dodati i sve pomoćne klase objekta koje želite.
4. Kliknite **Sljedeće**.
5. Tablica **Potrebno** je bila kreirana na predlošku. Možete promijeniti informacije sadržane u ovoj kartici.
   a. Izaberite **Potrebno** u izborniku kartice i kliknite na **Uredi**. Prikazan je panel **Uredi karticu**. Možete vidjeti ime kartice **Potrebno** i izabrane atribute koje treba klasa objekta, **inetOrgPerson**:
      - *sn - prezime
      - *cn - uobičajeno ime

      Bilješka: * označava potrebne informacije.
   b. Ako želite dodati dodatne informacije na tu karticu, izaberite atribut iz izbornika **Atributi**. Na primjer, izaberite **departmentNumber** i kliknite na **Dodavanje**. Izaberite **employeeNumber** i kliknite **Dodavanje**. Izaberite **naslov** i kliknite **Dodavanje**. Izbornik **Izabrani atributi** sada izgleda:
      - title
      - employeeNumber
      - departmentNumber
      - *sn
      - *cn
   c. Možete promijeniti način na koji se ta polja pojavljuju na predlošku tako da osvijetlite izabrane atribute i kliknete na **Premjesti gore** ili **Premjesti dolje**. Time se mijenja položaj atributa za jedan položaj. Ponavljajte tu proceduru tako dugo dok sve atribute ne stavite u željeni poredak. Na primjer,
      - *sn
      - *cn
      - title
      - employeeNumber
      - departmentNumber
   d. Također možete promijeniti svaki izabrani atribut.
      1) Osvijetlite atribut u kućici **Izabrani atributi** i kliknite na **Uredi**.
      2) Možete promijeniti ime prikaza polja kojeg koristite na predlošku. Na primjer, ako želite da se **brojOdjela** prikaže kao **Broj odjela**, unesite to u polje **Prikaz imena**.
      3) Možete osigurati i default vrijednost kojom će se popuniti polja atributa u predlošku. Na primjer, ako su većina korisnika koji će se unijeti članovi Odjela 789, možete unijeti 789 kao default vrijednost. Polje na predlošku će biti ispunjeno sa 789. Vrijednost se može promijeniti kada dodate stvarne informacije o korisniku.
      4) Kliknite **OK**.

e. Kliknite **OK**.

6. Kako bi kreirali drugu kategoriju kartice za dodatne informacije, kliknite na **Dodavanje**.
   - Unesite ime za novu karticu. Na primjer, Informacije o adresi.
   - Za tu karticu izaberite atribut iz izbornika **Atributi**. Na primjer, izaberite **homePostalAddress** i kliknite na **Dodavanje**. Izaberite **postOfficeBox** i kliknite na **Dodavanje**. Izaberite **telephoneNumber** i kliknite **Dodavanje**. Izaberite **homePhone** i kliknite **Dodavanje**. Izaberite **facsimileTelephoneNumber** i kliknite na **Dodavanje**. Izbornik **Izabrani atributi** sada izgleda:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone
     – facsimileTelephoneNumber
   - Možete promijeniti način na koji se ta polja pojavljuju na predlošku tako da osvijetlite izabrane atribute i kliknete na **Premjesti gore** ili **Premjesti dolje**. Time se mijenja položaj atributa za jedan položaj. Ponavljajte tu proceduru tako dugo dok sve atribute ne stavite u željeni poredak. Na primjer,
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – facsimileTelephoneNumber
     – homePhone
   - Kliknite **OK**.
7. Ponovite taj proces za onoliko kartica koliko ih želite kreirati. Kada ste gotovi, kliknite na **Završetak** kako bi kreirali predložak.

Uređivanje predloška:

Koristite ovu informaciju za uređivanje predloška.

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

- Kliknite na **Upravljanje predlošcima korisnika**.
- Izaberite područje koje želite uređivati iz popisa područja.
- Kliknite **Uređivanje**.
- Ako imate predloške koji postoje od ranije, na primjer predložak1, možete izabrati predložak tako da se njegove postavke kopiraju na predložak kojeg uređujete.
- Kliknite **Sljedeće**.
  – Možete koristiti padajući izbornik za promjenu strukturalne klase objekta predloška.
  – Možete dodati ili ukloniti pomoćne klase objekta.
- Kliknite **Sljedeće**.
- Možete promijeniti kartice i atribute sadržane u predlošku. Pogledajte 5 na stranici 199 redi informacija o tome kako promijeniti kartice.
- Kada ste završili, kliknite na **Završetak**.

Uklanjanje predloška:

Koristite ovu informaciju za uklanjanje predloška.

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljanje predlošcima korisnika**.
2. Izaberite predložak kojeg želite ukloniti.

3. Kliknite **Brisanje**.
4. Kada se od vas zatraži da potvrdite brisanje, kliknite na **OK**.
5. Predložak se uklanja iz popisa predložaka.

Uređivanje ACL-ova na predlošku:

Koristite ovu informaciju za uređivanje ACL-ova na predlošku.

Proširite kategoriju **Područja i predlošci** u području navigacije Web administracijskog alata.

1. Kliknite na **Upravljanje predlošcima korisnika**.
2. Izaberite predložak za kojeg želite uređivati ACL-ove.
3. Kliknite na **Uredi ACL**.

Kako bi pregledali ACL svojstva korištenjem pomoćnog programa Web administracijski alat i kako bi radili s ACL-ovima, pogledajte "Zadaci Liste kontrole pristupa (ACL)".

Srodni koncepti

"Lista kontrole pristupa" na stranici 62
Liste kontrole pristupa (ACL-ovi) sadrže sredstvo za zaštitu informacija pohranjenih u LDAP direktoriju. Administratori koriste ACL-ove kako bi ograničili pristup različitim dijelovima direktorija ili određenim unosima direktorija.

Zadaci Liste kontrole pristupa (ACL)

Koristite ovu informaciju za upravljanje lista kontrole pristupa (ACL-a).

Srodni koncepti

"Lista kontrole pristupa" na stranici 62
Liste kontrole pristupa (ACL-ovi) sadrže sredstvo za zaštitu informacija pohranjenih u LDAP direktoriju. Administratori koriste ACL-ove kako bi ograničili pristup različitim dijelovima direktorija ili određenim unosima direktorija.

Gledanje prava pristupa za specifičan učinkovit ACL

Koristite ovu informaciju za gledanje prava pristupa za specifičnu učinkovitu listu kontrole pristupa (ACL).

Učinkoviti ACL-ovi su eksplicitni i naslijeđeni ACL-ovi izabranog unosa.

1. Izaberite unos direktorija. Na primjer, cn=John Doe,ou=Advertising,o=ibm,c=US.
2. Kliknite na **Uredi ACL**. Panel Uređivanje ACL-a prikazuje se s ranije izabranom karticom **Učinkoviti ACL-i**. Kartica **Učinkoviti ACL-i** sadrži informacije samo za čitanje o ACL-ima.
3. Izaberite specifični učinkoviti ACL-a i kliknite tipku **Pogled**. Otvara se panel **Pregled prava pristupa**.
4. Kliknite na **OK** kako bi se vratili na karticu Učinkoviti ACL-ovi.
5. Kliknite na **Opoziv** kako bi se vratili na panel Uređivanje ACL-a.

Gledanje učinkovitih vlasnika

Koristite ovu informaciju za prikaz učinkovitih vlasnika.

Učinkoviti vlasnici su eksplicitni i naslijeđeni vlasnici izabranog unosa.

1. Izaberite unos direktorija. Na primjer, cn=John Doe,ou=Advertising,o=ibm,c=US.
2. Kliknite na **Uredi ACL**.
3. Kliknite karticu **Učinkoviti vlasnici**. Kartica **Učinkoviti vlasnici** sadrži informacije samo za čitanje o ACL-ima.
4. Kliknite na **Opoziv** kako bi se vratili na panel Uređivanje ACL-a.

Dodavanje, uređivanje i uklanjanje filtriranih ACL-ova

Koristite ovu informaciju za upravljanje nefiltriranim listama kontrole pristupa (ACL-i).

Možete dodati nove nefiltrirane ACL-ove u unos ili urediti postojeće nefiltrirane ACL-ove.

Nefiltrirani ACL-ovi se mogu širiti. To znači da se informacije kontrole pristupa definirane za jedan unos mogu primijeniti na sve njegove podređene unose. ACL izvor je izvor trenutnog ACL-a za izabrani unos. Ako unos nema ACL, on nasljeđuje ACL od nadređenih objekata na temelju ACL postavki nadređenih objekata.

Unesite sljedeće informacije na karticu **Nefiltrirani** ACL-ovi:

- ACL-ovi širenja - Izaberite kontrolnu kućicu **Širenje** kako bi dozvolili potomcima bez izričito definiranog ACL-a da nasljeđuju iz ovog unosa. Ako je kontrolna kućica izabrana, potomci nasljeđuju ACL-ove iz ovog unosa, a ako je ACL izričito definiran za unos podređenog, onda se ACL koji je bio naslijeđen iz nadređenog zamjenjuje s novim ACL-om koji je bio dodan. Ako kontrolna kućica nije izabrana, unosi potomka bez izričito definiranog ACL će naslijediti ACL-ove iz onog koji je nadređen unosu koji je omogućio tu opciju.
- DN (Razlikovno ime) - Unesite **(DN) Razlikovno ime** entiteta koji traži pristup za izvođenje operacija na izabranom unosu, na primjer, cn=Marketing Group.
- Tip - Unesite **Tip** DN-a. Na primjer, izaberite access-id ako je DN korisnik.

Kliknite na **Dodavanje** gumb da dodate DN u DN (Razlikovno Ime) polje ACL liste ili gumb Uređivanje da promijenite ACL-ove postojećeg DN.

Paneli **Dodavanje prava pristupa** i **Uređivanje prava pristupa** vam omogućavaju da postavite prava pristupa za nove ili postojeće liste kontrole pristupa (ACL-ovi). Polje **Tip** se postavlja na tip kojeg ste izabrali na panelu **Uredi ACL**. Ako dodajete ACL, sva druga polja postaju prazna. Ako uređujete ACL, polja sadrže vrijednosti koje su postavljene kada je zadnji put bio modificiran ACL.

Možete:

- Promijeniti ACL tip
- Postaviti prava dodavanja i brisanja
- Postaviti dozvole za klase sigurnosti

Da postavite prava pristupa:

1. Izaberite **Tip** unosa za ACL. Na primjer, izaberite access-id ako je DN korisnik.
2. Odlomak **Prava** prikazuje prava dodavanja i brisanja subjekta.
   - **Dodavanje podređenog** dodjeljuje ili ne dodjeljuje subjektu pravo da doda unos direktorija ispod izabranog unosa.
   - **Brisanje unos** dodjeljuje ili ne dodjeljuje subjektu pravo da obriše izabrani unos.
3. Odlomak **Klasa sigurnosti** definira dozvole za klase atributa. Atributi su grupirani u klase sigurnosti:
   - **Normalne** - Normalne klase atributa traže najmanje sigurnosti, na primjer, atribut commonName.
   - **Osjetljive** - Osjetljive klase atributa traže umjerenu količinu sigurnosti, na primjer homePhone.
   - **Kritične** - Kritične klase atributa traže najviše sigurnosti, na primjer, atribut userpassword.
   - **Sistem** - Sistemski atributi su atributi samo za čitanje koje održava poslužitelj.
   - **Ograničeno** - Ograničeni atributi su korišteni za definiranje kontrole pristupa.

   Svaka klasa sigurnosti ima dozvole koje su joj pridružene.
   - Čitanje - subjekt može čitati atribute.
   - Pisanje - subjekt može mijenjati atribute.
   - Traženje - subjekt može tražiti atribute.
   - Uspoređivanje - subjekt može uspoređivati atribute.

Dodatno, možete navesti dozvole bazirane na atributima umjesto sigurnosne klase u koju atribut pripada. Odlomak o atributima je ispisan ispod **Kritična klasa sigurnosti**.

- Izaberite atribut iz padajućeg izbornika **Definiranje atributa**.
- Kliknite **Definiraj**. Atribut se prikazuje s tablicom dozvola.
- Specificirajte da li želite da se dodijele ili ne dodijele svakoj od četiri klase sigurnosti dozvole koje su pridružene atributu.
- Tu proceduru možete ponoviti za više atributa.
- Da uklonite atribut, jednostavno izaberite atribut i kliknite na **Obriši**.
- Kada ste gotovi kliknite na **OK**.

ACL-ove možete ukloniti na dva načina:

- Izaberite radijski gumb koji se nalazi uz ACL kojeg želite obrisati. Kliknite **Ukloni**.
- Kliknite na **Ukloni sve** kako bi obrisali sve DN-ove iz popisa.

Dodavanje, uređivanje i uklanjanje filtriranih ACL-ova

Koristite ovu informaciju za gledanje prava pristupa za filtriranu listu kontrole pristupa (ACL).

Možete dodati nove filtrirane ACL-ove na unos ili uređivati postojeće filtrirane ACL-ove.

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

Default ponašanje filter-zasnovanih ACL-ova je da prikuplja od najniže sadržanog unosa, preko lanca unosa prethodnika, do unosa koji je sadržan na vrhu DIT-a. Učinkovit pristup se izračunava kao unija dodijeljenih ili odbijenih prava pristupa od strane sastavnih unosa prethodnika. Postoji iznimka od tog ponašanja. Radi kompatibilnosti s funkcijom replikacije podstabla i da bi dozvolili veću administrativnu kontrolu, atribut stropa je korišten kao način zaustavljanja skupljanja na unosu na kojem je sadržan.

Unesite sljedeće informacije na karticu Filtrirani ACL-ovi:

- Prikupite filtrirane ACL-ove -
  - Izaberite radijski gumb **Nije specificirano** kako bi uklonili ibm-filterACLInherit atribut iz izabranog unosa.
  - Izaberite radijski gumb **True** kako bi dozvolili da se ACL-ovi za izabrani unos akumuliraju iz tog unosa, preko lanca prethodnika do najvišeg filtriranog ACL sadržanog unosa u DIT-a.
  - Izaberite radijski gumb **False** kako bi zaustavili skupljanje filtriranih ACL-ova na izabranom unosu.
- DN (Razlikovno ime) - Unesite **(DN) Razlikovno ime** entiteta koji traži pristup za izvođenje operacija na izabranom unosu, na primjer, cn=Marketing Group.
- Tip - Unesite **Tip** DN-a. Na primjer, izaberite access-id ako je DN korisnik.

Kliknite na **Dodavanje** gumb da dodate DN u DN (Razlikovno Ime) polje u ACL listu ili gumb Uređivanje da promijenite ACL-ove postojećeg DN.

Paneli **Dodavanje prava pristupa** i **Uređivanje prava pristupa** vam omogućavaju da postavite prava pristupa za nove ili postojeće liste kontrole pristupa (ACL-ovi). Polje tip se postavlja na tip kojeg ste izabrali na panelu Uređivanje ACL-a. Ako dodajete ACL, sva druga polja postaju prazna. Ako uređujete ACL, polja sadrže vrijednosti koje su postavljene kada je zadnji put bio modificiran ACL.

Možete:

- Promijeniti ACL tip
- Postaviti prava dodavanja i brisanja
- Postaviti filter objekta za filtrirane ACL-ove
- Postaviti dozvole za klase sigurnosti

Da postavite prava pristupa:

1. Izaberite **Tip** unosa za ACL. Na primjer, izaberite access-id ako je DN korisnik.
2. Odlomak **Prava** prikazuje prava dodavanja i brisanja subjekta.
   - **Dodavanje podređenog** dodjeljuje ili ne dodjeljuje subjektu pravo da doda unos direktorija ispod izabranog unosa.
   - **Obriši unos** dodjeljuje ili ne dodjeljuje subjektu pravo da obriše izabrani unos.
3. Postavite filter objekta za filter zasnovanu usporedbu. U polje **Filter objekta** unesite željeni filter objekta za izabrani ACL. Kliknite na gumb **Uredi filter** za pomoć kod sastavljanja niza filtera pretraživanja. Trenutni filtrirani ACL se širi na sve podređene objekte u pridruženom podstablu koje se podudara s filterom u tom polju.
4. Odlomak **Klasa sigurnosti** definira dozvole za klase atributa. Atributi su grupirani u klase sigurnosti:
   - **Normalne** - Normalne klase atributa traže najmanje sigurnosti, na primjer, atribut commonName.
   - **Osjetljive** - Osjetljive klase atributa traže umjerenu količinu sigurnosti, na primjer homePhone.
   - **Kritične** - Kritične klase atributa traže najviše sigurnosti, na primjer, atribut userpassword.
   - **Sistem** - Sistemski atributi su atributi samo za čitanje koje održava poslužitelj.
   - **Ograničeno** - Ograničeni atributi su korišteni za definiranje kontrole pristupa.

   Svaka klasa sigurnosti ima dozvole koje su joj pridružene.
   - Čitanje - subjekt može čitati atribute.
   - Pisanje - subjekt može mijenjati atribute.
   - Traženje - subjekt može tražiti atribute.
   - Uspoređivanje - subjekt može uspoređivati atribute.

   Dodatno, možete navesti dozvole bazirane na atributima umjesto sigurnosne klase u koju atribut pripada. Odlomak o atributima je ispisan ispod **Kritična klasa sigurnosti**.
   - Izaberite atribut iz padajućeg izbornika **Definiranje atributa**.
   - Kliknite **Definiraj**. Atribut se prikazuje s tablicom dozvola.
   - Specificirajte da li želite da se dodijele ili ne dodijele svakoj od četiri klase sigurnosti dozvole koje su pridružene atributu.
   - Tu proceduru možete ponoviti za više atributa.
   - Da uklonite atribut, jednostavno izaberite atribut i kliknite na **Obriši**.
   - Kada ste gotovi kliknite na **OK**.

ACL-ove možete ukloniti na dva načina:

- Izaberite radijski gumb koji se nalazi uz ACL kojeg želite obrisati. Kliknite **Ukloni**.
- Kliknite na **Ukloni sve** kako bi obrisali sve DN-ove iz popisa.

Dodavanje ili uklanjanje vlasnika

Koristite ovu informaciju za dodavanje ili uklanjanje vlasnika.

Vlasnici unosa imaju potpune dozvole za izvođenje bilo kojih operacija na objektu. Vlasnici unosa mogu biti eksplicitni ili proširen (naslijeđeni).

Unesite sljedeće informacije na karticu **Vlasnici**:

1. Izaberite kontrolnu kućicu **Širi korisnike** kako bi omogućili potomcima bez izričito definiranog vlasnika da nasljeđuju iz tog unosa. Ako nije izabrana kontrolna kućica, unosi potomka bez izričito definiranog vlasnika će naslijediti vlasnika iz onog koji je nadređen tom unosu koji je omogućio tu opciju.
2. DN (Razlikovno ime) - Unesite **(DN) Razlikovno ime** entiteta koji traži pristup za izvođenje operacija na izabranom unosu, na primjer, cn=Marketing Group. Korištenje cn=this s objektima koji šire svoja vlasništvo na druge objekte olakšava kreiranje podstabla direktorija u kojem je svaki objekt vlasnik sam sebi.
3. Tip - Unesite **Tip** DN-a. Na primjer, izaberite access-id ako je DN korisnik.

Za dodavanje vlasnika, kliknite **Dodavanje** za dodavanje DN-a u polje **DN (razlikovno ime)** na to listu.

Možete ukloniti vlasnika na dva načina:

- Izaberite radijski gumb koji se nalazi uz DN vlasnika kojeg želite obrisati. Kliknite **Ukloni**.
- Kliknite na **Ukloni sve** kako bi iz popisa obrisali sve DN-ove vlasnika.

Upute

Materijali s uputama koje se odnose na Direktorij poslužitelja, kao što su informacije o redu za naredbe i LDIF-u.

Pogledajte sljedeće za dodatne referentne informacije.

Pomoćni program reda za naredbe Directory Servera

Ovaj odlomak opisuje pomoćne programe Directory Servera koji se mogu izvoditi iz okoline Qshell naredbe.

Primijetite da neki nizovi moraju biti okruženi navodnicima kako bi se ispravno obradili u okolini Qshell naredbe. To se u pravilu odnosi na nizove koji su DN-ovi, filtere pretraživanja i popise atributa koje će vratiti ldapsearch. Kao primjere, pogledajte sljedeći popis.

- Nizovi koji sadržavaju razmake: "cn=John Smith,cn=users"
- Nizovi koji sadržavaju zamjenske znakove: "*"
- Nizovi koji sadržavaju zagrade: "(objectclass=person)"

Za više informacija o okolini Qshell naredbe, pogledajte poglavlje “Qshell”.

Pogledajte sljedeće naredbe za dodatne informacije:

ldapmodify i ldapadd

Pomoćni programi reda za naredbe LDAP modificiraj-unos i LDAP dodaj-unos.

Pregled

```
ldapmodify [-a] [-b] [-c] [-C charset] [-d debuglevel][-D binddn] [-e errorfile]
[-g] [-f file][-F][-g][-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile]
[-m mechanism] [-M][-n][-N certificatename] [-O maxhops] [-p ldapport]
[-P keyfilepw] [-r] [-R][-U username] [-v] [-V] [-w passwd | ?] [-y proxydn]
[-Y] [-Z]
```

```
ldapadd [-a] [-b] [-c] [-C charset] [-d debuglevel] [-D binddn] [-e errorfile]
[-g] [-f file][-F][-g][-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile]
[-m mechanism] [-M][-n][-N certificatename] [-O maxhops] [-p ldapport]
[-P keyfilepw] [-r] [-R][-U username] [-v] [-V] [-w passwd | ?] [-y proxydn]
[-Y] [-Z]
```

Opis

ldapmodify je sučelje reda za naredbe za ldap_modify, ldap_add, ldap_delete i ldap_rename sučelja aplikativnog programiranja (API-ije). **ldapadd** je implementiran kao preimenovana verzija ldapmodify-a. Kada je dozvan ldapadd, **-a** (dodaj novi unos) oznaka se automatski postavlja.

ldapmodify otvara veze s LDAP poslužiteljem i povezuje se na poslužitelj. Možete koristiti **ldapmodify** da promijenite ili dodate unose. Informacije unosa se čitaju iz standardnog unosa ili iz datoteke upotrebom **-i** opcije.

Kako bi prikazali pomoć sintakse za **ldapmodify** ili **ldapadd**, upišite

```
ldapmodify -?
```

ili

```
ldapadd -?
```

Opcije

-a Dodavanje novih unosa. Default akcija za **ldapmodify** je da promijenite postojeće unose. Ako je dozvan kao **ldapadd**, ta oznaka je uvijek poznata.

-b Pretpostavite da su bilo koje vrijednosti koje počinju s `/' binarne vrijednosti i da je stvarna vrijednost u datoteci čija je staza navedena umjesto vrijednosti.

-c Kontinuirani operativni način. Izvješteno je o greškama, no **ldapmodify** nastavlja s preinakama. U suprotnom je default akcija izlazak nakon izvještavanja o greški.

-C *charset*
Specificira da su nizovi dobavljeni kao ulaz u **ldapmodify** i **ldapadd** pomoćnim programima predstavljeni u lokalnom skupu znakova kako je to specificirano skupom znakova i mora se konvertirati u UTF-8. Koristite opciju **-C** *charset* ako je kodna stranica niza ulaza različita od vrijednosti kodne stranice posla. Pogledajte ldap_set_iconv_local_charset() API-je kako bi vidjeli podržane vrijednosti skupa znakova.

-d *debuglevel*
Postavite razinu LDAP otkrivanja grešaka na debuglevel.

-D *binddn*
Upotrijebite ***binddn*** za povezivanje na LDAP direktorij. ***binddn*** je niz-predstavljeno DN. Kada je korišten s -m DIGEST-MD5, korišten je da navede autorizacijski ID. Može biti ili DN ili authzId niz koji počinje s ″u:″ ili ″dn:″.

-e *errorfile*
Specificira datoteku u koju se upisuju odbijeni unosi. Ta opcija zahtijeva -c opciju neprekidne operacije. Ako obrada unosa ne uspije, taj unos se upisuje u datoteku odbijanja i zbroj odbijenih unosa se povećava. Ako je unos u ldapmodify ili ldapadd naredbe iz datoteke, kad se datoteka obrađuje, dobiva se broj ukupnih unosa upisanih u datoteku odbijanja.

-f *file* Čita podatke o modifikaciji sloga iz LDIF datoteke umjesto iz standardnog ulaza. Ako LDIF datoteka nije navedena, morate koristiti standardne ulazne podatke kad određujete slogove za ažuriranje u LDIF formatu. Može se koristiti ili -i ili -f opcija za specificiranje datoteka ulaza; ponašanje je isto.

-F Prisilite aplikacije na sve promjene bez obzira na sadržaj ulaznih redova koji počinju s replikom: (po defaultu, replika: linije su uspoređene u osnovu na LDAP poslužitelj host i port koji se koristi radi odlučivanja da li zapis dnevnika replikacije treba biti primjenjen).

-g Nemojte izostaviti prazna mjesta na kraju vrijednosti atributa.

–G Navodi područje. Ovaj parametar je neobvezan. Kada je korišten s -m DIGEST-MD5, vrijednost je predana na poslužitelj za vrijeme vezivanja.

-h *ldaphost*
Specificirajte zamjenski host na kojem se izvodi ldap poslužitelj.

-i *file* Čita podatke o modifikaciji sloga iz LDIF datoteke umjesto iz standardnog ulaza. Ako LDIF datoteka nije navedena, morate koristiti standardne ulazne podatke kad određujete slogove za ažuriranje u LDIF formatu. Može se koristiti ili -i ili -f opcija za specificiranje datoteka ulaza; ponašanje je isto.

-k Specificira korištenje kontrole administracije poslužitelja.

-K *keyfile*
Specificirajte ime SSL datoteke ključeva baze podataka s default proširenjem **kdb**. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva. Ako nije specificirano ime datoteke baze podataka ključeva, taj pomoćni program će prvo tražiti prisutnost SSL_KEYRING varijable okoline s pridruženim imenom datoteke. Ako nije definirana SSL_KEYRING varijabla okoline, koristit će se sistemska datoteka prstena ključeva, ako postoji.

Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

-l Ne replicirajte promjenu. Kontrola Ne repliciraj koristi se za davanje zahtjeva da se određena promjena ne replicira. To bi trebala koristiti Topologija replikacije kako bi se spriječilo da ciljni poslužitelj ne replicira promjene napravljene kako bi se topologija replikacije harmonizirala, s ciljem da ne dođe do promjena na drugim poslužiteljima. Ovu kontrolu može također koristiti administrativni klijent.

-m *mechanism*
Koristite ***mechanism*** kako bi specificirali SASL mehanizam koji će se koristiti za vezivanje na poslužitelj. Koristi se ldap_sasl_bind_s() API. **-m** parametar se zanemaruje ako je postavljeno **-V 2**. Ako **-m** nije naveden, koristi se jednostavna provjera identiteta. Valjani mehanizmi su:

- CRAM-MD5 - štiti lozinku koja je poslana na poslužitelja.
- EXTERNAL - koristi SSL certifikat. Treba -Z.
- GSSAPI - koristi Kerberos vjerodajnice korisnika.
- DIGEST-MD5 - zahtjeva da klijent pošalje vrijednost korisničkog imena poslužitelju. Zahtjeva -U. -D parametar (obično vezani DN) je korišten da navede autorizacijski ID. Može biti DN ili authzId niz koji počinje s u: ili dn:.
- OS400_PRFTKN - provjerava autentičnost lokalnog LDAP poslužitelja kao trenutnog i5/OS korisnika pomoću DN-a korisnika u pozadini projiciranog sistema. -D (vezani DN) i -w (lozinka) parametri ne trebaju biti navedeni.

-M Upravljajte referal objektima kao pravilnim unosima.

-n Specificirajte negativnu opciju operacije kako biste omogućili pregledavanje rezultata naredbe koju izdajete bez stvarnog izvođenja akcije na direktoriju. Promjenama koje bi se napravile prethodi uskličnik i ispisuju se na standardnom izlazu. Bilo kakva greška sintakse koja se pronađe u obradi datoteke ulaza, prije pozivanja funkcija koje izvode promjene u direktoriju, prikazuje se kao standardna greška. Ta je opcija posebno korisna s -v opcijom za operacije ispravljanje, ako se naiđe na greške.

-N *certificatename*
Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti potreban. ***certificatename*** nije potrebno ako je par certifikat/privatni ključ označen kao default za datoteku baze podatka ključa. Slično, ***certificatename*** nije potreban ako je jednostruk par certifikat/privatan ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

-O *maxhops*
Specificirajte ***maxhops*** kako bi postavili maksimalan broj skokova koje poduzima knjižnica klijenta kada traži referale. Default broj skokova je 10.

-p *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje ldap poslužitelj. Default LDAP port je 389. Ako nije specificirano **-p**, a specificirano je **-Z**, koristi se default LDAP SSL port 636.

-P *keyfilepw*
Određuje lozinku baze ključeva. Ta lozinka je potrebna kako bi se pristupilo šifriranim informacijama u datoteci baze podataka ključa, a to bi moglo uključivati jedan ili više privatnih ključeva. Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključa, lozinka se dobiva od datoteke skrivene lozinke, a **-P** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

-r Zamijeni postojeće vrijednosti po defaultu.

-R Određuje da se preporuke ne slijede automatski.

–U Navedite korisničko ime. Potrebno kod -m DIGEST-MD5 i zanemareno s bilo kojim drugim mehanizmom.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-V *version*
Specificira LDAP verziju koju koristi **ldapmodify** kada se povezuje na LDAP poslužitelj. Po defaultu, uspostavlja se LDAP V3 veza. Kako bi izričito izabrali LDAP V3, specificirajte **-V 3**. Specificirajte **-V 2** kako bi ga izvodili kao LDAP V2 aplikaciju.

-w *passwd* **| ?**
Koristite ***passwd*** kao lozinku za provjeru ovlaštenja. Koristite ? kako bi generirali prompt lozinke.

-y *proxydn*
Postavite proksiran ID za opciju autorizacije proksijem.

-Y Koristite sigurnu LDAP vezu (TLS).

-Z Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

Format ulaza

Sadržaj datoteke (ili standardni ulaz ako nema **-i** oznake na redu za naredbe) bi se trebao prilagoditi LDIF formatu.

Primjeri

Pod pretpostavkom da postoji datoteka /tmp/entrymods i da ima sljedeći sadržaj:

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

naredba:

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

će zamijeniti sadržaje unosa Modificiraj mene atributa pošte s vrijednosti modme@student.of.life.edu, dodati naslov Grand Poobah i sadržaje datoteke /tmp/modme.jpeg kao jpegPhoto i u potpunosti ukloniti atribut opisa. Te iste modifikacije se mogu izvoditi korištenjem starijeg ldapmodify formata ulaza:

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

i naredba:

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

Pod pretpostavkom da postoji datoteka /tmp/newentry i da ima sljedeće sadržaje:

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

naredba:

```
ldapadd -i /tmp/entrymods
```

dodaje novi unos za John Doe, korištenjem vrijednosti iz datoteke /tmp/newentry.

Napomene

Ako informacija unosa nije dobavljena iz datoteke korištenjem **-i** opcije, **ldapmodify** naredba će čekati da pročita unose iz standardnog ulaza.

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

Srodni koncepti

"Sufiks (kontekst imenovanja)" na stranici 12
Sufiks (poznat i kao kontekst imenovanja) je DN koji identificira najviši unos u lokalno zadržanoj hijerarhiji direktorija.

Lightweight Directory Access Protocol (LDAP) API-ji
Pogledajte Lightweight Directory Access Protocol (LDAP) API-je za više informacija o API-jima Directory Servera.

"Shema konfiguracije Poslužitelja direktorija" na stranici 242
Ove informacije opisuju Stablo informacija direktorija (DIT) i atribute koji se koriste za konfiguriranje ibmslapd.conf datoteke.

Srodne reference

"LDAP format razmjene podataka (LDIF)" na stranici 236
LDAP format razmjene podataka je standardni tekstualni format za prikazivanje LDAP objekata i LDAP ažuriranja (dodaj, modificiraj, obriši, modificiraj DN) u tekstualnom obliku. Datoteke koje sadrže LDIF slogove mogu se koristiti za prijenos podataka između directory servera ili kao ulaz LDAP alatima poput **ldapadd** i **ldapmodify**.

ldapdelete

Pomoćni programi reda za naredbe LDAP obriši-unos.

Pregled

```
ldapdelete [-c] [-C charset] [-d debuglevel][-D binddn] [-f file]
[-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile] [-m mechanism]
[-M] [-n] [-N certificatename] [-O maxops] [-p ldapport]
[-P keyfilepw] [-R] [-s][-U username} [-v] [-V version]
[-w passwd | ?] [-y proxydn][-Y] [-Z] [dn]......
```

Opis

ldapdelete je sučelje reda za naredbe u sučelje aplikativnog programiranja ldap_delete (API).

ldapdelete otvara vezu na LDAP poslužitelj, veže i briše jedan ili više unosa. Ako je dobavljen jedan ili više argumenata Razlikovnog imena (DN), brišu se unosi s tim DN-ovima. Svaki DN je niz-predstavljeni DN. Ako su dobavljeni DN argumenti, čita se lista DN-ova iz standardnog ulaza ili iz datoteke ako se koristi **-i** oznaka.

Kako bi prikazali pomoć sintakse za **ldapdelete**, upišite:

```
ldapdelete -?
```

Opcije

-c Kontinuirani operativni način. Greške se izvještavaju, ali **ldapdelete** nastavlja s brisanjima. U suprotnom je default akcija da se izađe nakon izvještaja o greški.

-C *charset*

Specificira da su DN-ovi dobavljeni kao ulaz u **ldapdelete** pomoćni program, predstavljeni u lokalnom skupu znakova, kako je to specificirano s charset. Koristite **-C** *charset* opciju ako se kodna stranica ulaznog niza razlikuje od vrijednosti kodne stranice posla. Pogledajte ldap_set_iconv_local_charset() API-je kako bi vidjeli podržane vrijednosti skupa znakova.

-d *debuglevel*

Postavite razinu LDAP otkrivanja grešaka na debuglevel.

-D *binddn*

Upotrijebite ***binddn*** za povezivanje na LDAP direktorij. ***binddn*** je niz-predstavljeno DN. Kada je korišten s -m DIGEST-MD5, korišten je da navede autorizacijski ID. Može biti DN ili authzId niz koji počinje s ″u:″ ili ″dn:″.

-f *file* Čita serije linija iz datoteke izvodeći LDAP brisanje za svaku liniju u datoteci. Svaki red u datoteci treba sadržavati jedinstveno razlikovno ime (DN).

-G *područje*

Navodi područje. Ovaj parametar je neobvezan. Kada je korišten s -m DIGEST-MD5, vrijednost je predana na poslužitelj za vrijeme vezivanja.

-h *ldaphost*

Određuje alternativni host na kojemu radi LDAP poslužitelj.

-i *file* Čita serije linija iz datoteke izvodeći LDAP brisanje za svaku liniju u datoteci. Svaka linija u datoteci bi trebala sadržavati jedno razlikovno ime.

-k Specificira korištenje kontrole administracije poslužitelja.

-K *keyfile*

Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva.

Ako pomoćni program ne može locirati bazu ključeva, koristit će čvrsto kodirani skup default povjerljivih korijena izdavača certifikata. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori.

Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat pridružen ID-u Directory Services aplikacije klijenta.

-m *mechanism*

Koristite ***mechanism*** kako bi specificirali SASL mehanizam koji će se koristiti za vezivanje na poslužitelj. Koristi se ldap_sasl_bind_s() API. **-m** parametar se zanemaruje ako je postavljeno **-V 2**. Ako **-m** nije naveden, koristi se jednostavna provjera identiteta. Valjani mehanizmi su:

- CRAM-MD5 - štiti lozinku koja je poslana na poslužitelja.
- EXTERNAL - koristi SSL certifikat. Treba -Z.
- GSSAPI - koristi Kerberos vjerodajnice korisnika.
- DIGEST-MD5 - zahtjeva da klijent pošalje vrijednost korisničkog imena poslužitelju. Zahtjeva -U. -D parametar (obično vezani DN) je korišten da navede autorizacijski ID. Može biti DN ili authzId niz koji počinje s u: ili dn:.
- OS400_PRFTKN - provjerava autentičnost lokalnog LDAP poslužitelja kao trenutnog i5/OS korisnika pomoću DN-a korisnika u pozadini projiciranog sistema. -D (vezani DN) i -w (lozinka) parametri ne trebaju biti navedeni.

-M Upravljajte referal objektima kao pravilnim unosima.

-n Pokazuje što će se napraviti, ali ne mijenja stvarne unose. Korisno za analizu u spoju s **-v**.

-N *certificatename*

Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti

potreban. ***certificatename*** nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, ***certificatename*** nije potreban ako je jednostruk par certifikat/privatan ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

-O *maxhops*
Specificirajte ***maxhops*** kako bi postavili maksimalan broj skokova koje poduzima knjižnica klijenta kada traži referale. Default broj skokova je 10.

-p *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje LDAP poslužitelj. Default LDAP port je 389. Ako nije specificirano **-p**, a specificirano je **-Z**, koristi se default LDAP SSL port 636.

-P *keyfilepw*
Određuje lozinku baze ključeva. Lozinka je potrebna za pristup šifriranim informacijama u datoteci ključeva baze podataka, koja može uključivati jedan ili više privatnih ključeva. Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključa, lozinka se dobiva od datoteke skrivene lozinke, a **-P** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

-R Određuje da se preporuke ne slijede automatski.

-s Koristite tu opciju kako bi obrisali podstablo koje ima korijen na specificiranom unosu.

–U *username*
Navedite korisničko ime. Potrebno kod -m DIGEST-MD5 i zanemareno s bilo kojim drugim mehanizmom.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-V *version*
Specificira LDAP verziju koju koristi **ldapdelete** kada se povezuje na LDAP poslužitelj. Po defaultu, uspostavlja se LDAP V3 veza. Kako bi izričito izabrali LDAP V3, specificirajte **-V 3**. Specificirajte **-V 2** kako bi ga izvodili kao LDAP V2 aplikaciju.

-w *passwd* **| ?**
Koristite ***passwd*** kao lozinku za provjeru ovlaštenja. Koristite ? kako bi generirali prompt lozinke.

-y proxydn
Postavite proksiran ID za operaciju autorizacije proksijem.

–Y Koristite sigurnu LDAP vezu (TLS).

-Z Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

dn Specificira jedan ili više DN argumenata. Svako DN bi trebalo biti niz-predstavljeno DN.

Primjeri

Sljedeća naredba

```
ldapdelete -D cn=administrator -w secret "cn=Delete Me, o=University of Life, c=US"
```

pokušava obrisati unos koji je imenovan sa zajedničkim imenom ″Delete Me″ točno ispod University of Life unosa organizacije.

Napomene

Ako nisu dobavljeni DN argumenti, **ldapdelete** naredbe čekaju da pročitaju popis DN-ova iz standardnog ulaza.

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

Srodni koncepti

Directory Server API-ji

ldapexop

Pomoćni program reda za naredbe LDAP proširene operacije.

Pregled

```
ldapexop [-C charset] [-d debuglevel][-D binddn][-e] [-G realm]
[-h ldaphost][-help][-K keyfile] [-m mechanism] [-N certificatename]
[-p ldapport] [-P keyfilepw] [-?] [-U] [-v] [-w passwd | ?] [-Y] [-Z]
-op {cascrepl | controlqueue | controlrepl | getAttributes |
getusertype | quiesce | readconfig | uniqueattr}
```

Opis

Pomoćni program **ldapexop** je sučelje reda za naredbe koje osigurava sposobnost za vezanje na poslužitelj direktorija i izdaje jednu proširenu operaciju zajedno s podacima koji čine vrijednost proširene operacije.

Pomoćni program **ldapexop** podržava standardni host, port, SSL i opcije provjere autentičnosti koje koriste svi pomoćni programi LDAP klijenta. Usto, skup opcija je definiran za specificiranje operacije koje se mora izvesti i argumenata za svaku proširenu operaciju.

Kako bi prikazali pomoć sintakse za **ldapexop**, upišite:

```
ldapexop -?
```

ili

```
ldapexop -help
```

Opcije

Opcije za ldapexop naredbu se dijele u dvije kategorije:

1. Općenite opcije koje specificiraju kako se treba spojiti na poslužitelj direktorija. Te opcije moraju biti specificirane prije opcija koje su specifične za operaciju.
2. Opcija proširene operacije koja identificira proširenu operaciju koja će se izvoditi.

Općenite opcije

Te opcije specificiraju metode povezivanja na poslužitelj i moraju biti specificirane prije **-op** opcije.

-C *charset*
: Specificira da su DN-ovi dobavljeni kao ulaz u **ldapexop** pomoćni program, predstavljeni u lokalnom skupu znakova, kako je to specificirano s charset. Koristite opciju **-C** *charset* ako je kodna stranica niza ulaza različita od vrijednosti kodne stranice posla. Pogledajte ldap_set_iconv_local_charset() API-je kako bi vidjeli podržane vrijednosti skupa znakova.

-d *debuglevel*
: Postavite razinu LDAP otkrivanja grešaka na debuglevel.

-D *binddn*
: Upotrijebite ***binddn*** za povezivanje na LDAP direktorij. ***binddn*** je niz-predstavljeno DN. Kada je korišten s -m DIGEST-MD5, korišten je da navede autorizacijski ID. Može biti DN ili authzId niz koji počinje s ″u:″ ili ″dn:″.

-e
: Prikazuje informacije o verziji LDAP knjižnice i nakon toga izlazi.

-G
: Navodi područje. Ovaj parametar je neobvezan. Kada je korišten s -m DIGEST-MD5, vrijednost je predana na poslužitelj za vrijeme vezivanja.

-h *ldaphost*
Određuje alternativni host na kojemu radi LDAP poslužitelj.

-help Prikazuje sintaksu naredbe i informacije o upotrebljivosti.

-K *keyfile*
Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva.

Ako pomoćni program ne može pronaći bazu podataka ključa, koristi se sistemska baza podataka ključa. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori.

Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

-m *mechanism*
Koristite ***mechanism*** kako bi specificirali SASL mehanizam koji će se koristiti za vezivanje na poslužitelj. Koristi se ldap_sasl_bind_s() API. **-m** parametar se zanemaruje ako je postavljeno **-V 2**. Ako **-m** nije naveden, koristi se jednostavna provjera identiteta. Valjani mehanizmi su:

- CRAM-MD5 - štiti lozinku koja je poslana na poslužitelja.
- EXTERNAL - koristi SSL certifikat. Treba -Z.
- GSSAPI - koristi Kerberos vjerodajnice korisnika.
- DIGEST-MD5 - zahtjeva da klijent pošalje vrijednost korisničkog imena poslužitelju. Zahtjeva -U. -D parametar (obično vezani DN) je korišten da navede autorizacijski ID. Može biti DN ili authzId niz koji počinje s u: ili dn:.
- OS400_PRFTKN - provjerava autentičnost lokalnog LDAP poslužitelja kao trenutnog i5/OS korisnika pomoću DN-a korisnika u pozadini projiciranog sistema. -D (vezani DN) i -w (lozinka) parametri ne trebaju biti navedeni.

-N *certificatename*
Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti potreban. ***certificatename*** nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, ***certificatename*** nije potreban ako je jednostruk par certifikat/privatan ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

-p *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje LDAP poslužitelj. Default LDAP port je 389. Ako nije specificirano **-p**, a specificirano je **-Z**, koristi se default LDAP SSL port 636.

-P *keyfilepw*
Određuje lozinku baze ključeva. Lozinka je potrebna za pristup šifriranim informacijama u datoteci ključeva baze podataka, koja može uključivati jedan ili više privatnih ključeva. Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključa, lozinka se dobiva od datoteke skrivene lozinke, a **-P** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

-? Prikazuje sintaksu naredbe i informacije o upotrebljivosti.

–U Navedite korisničko ime. Potrebno kod -m DIGEST-MD5 i zanemareno s bilo kojim drugim mehanizmom.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-w *passwd* **| ?**
Koristite ***passwd*** kao lozinku za provjeru ovlaštenja. Koristite ? kako bi generirali prompt lozinke.

–Y Koristite sigurnu LDAP vezu (TLS).

-Z Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

Opcija Proširene operacije

Opcija **-op** extended-op identificira proširene operacije koje će se izvoditi. Proširena operacija može biti jedna od sljedećih vrijednosti:

- **acctstatus**: Proširena operacija statusa računa. Prikazuje status specificiranog računa.

```
ldapexop –op acctstatus –d <DN>
```

-d DN

Identificira DN unosa za koji se treba dohvatiti status računa.

Status računa može biti otvoren, zaključan ili zastario.

- **cascrepl**: kaskadna proširena operacija kontrole replikacije. Tražena akcija se odnosi na specificirani poslužitelj i propušta se svim replikama danog podstabla. Ako su bilo koje od tih replike prosljeđivanja, one propuštaju proširene operacije do njihovih replika. Operacija je kaskadna nad cijelom topologijom replikacije.

  -action quiesce | unquiesce | replnow | wait
  To je potreban atribut koji specificira akciju koja će se izvoditi.

  quiesce
  Nisu dozvoljena daljnja ažuriranja, osim od strane replikacije.

  unquiesce
  Nastavlja se s normalnom operacijom, prihvaćena su ažuriranja klijenta.

  replnow
  Replicira sve promjene u redu na sve replika poslužitelje čim je to moguće, bez obzira na raspored.

  wait Čeka da se sva ažuriranja repliciraju na sve replike.

  -rc *contextDn*
  To je potreban atribut koji specificira korijen podstabla.

  -timeout *secs*
  To je neobvezan atribut koji, ako je prisutan, specificira timeout period u sekundama. Ako nije prisutan ili je 0, operacija čeka neodređeno dugo.

  Primjer:

```
ldapexop -op cascrepl -action -quiesce -rc "o=acme,c=us" -timeout 60
```

- **clearlog | getlogsize | readlog -log ...**

Te tri operacije podržavaju novu datoteku dnevnika:

LostAndFound

Te se operacije mogu koristiti s i5/OS directory serverom (V6R1 i kasnije), ali su samo određene datoteke dnevnika podržane:

LostAndFound – datoteka dnevnika sukoba replikacije

- **controlqueue**: proširena operacija replikacije kontrolnog reda. Ta operacija vam omogućava da obrišete ili uklonite promjene u stanju čekanja iz popisa promjena replikacije koje su se nagomilale i nisu se izvodile zbog kvarova replikacije. Ta operacija je korisna kada se podaci replike ručno popravljaju. Tu operaciju bi koristili kako bi preskočili izvođenje nekih nagomilanih kvarova.

  -skip all | change-id
  To je potreban atribut.
  - **-preskoči sve** pokazuje da preskočite sve promjene koje su u toku za ovaj ugovor.
  - **change-id** identificira jednu promjenu koja će se preskočiti. Ako poslužitelj trenutno ne replicira tu promjenu, zahtjev neće uspjeti.

  -ra *agreementDn*
  To je potreban atribut koji specificira DN ugovora replikacije.

  Primjeri:

```
ldapexop -op controlqueue -skip all -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"

ldapexop -op controlqueue -skip 2185 -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"
```

- **controlrepl**: proširena operacija kontrole replikacije

  -action suspend | resume | replnow
  To je potreban atribut koji specificira akciju koja će se izvoditi.

  -rc *contextDn* **| -ra** *agreementDn*
  -rc *contextDn* je DN konteksta replikacije. Akcija se izvodi za sve ugovore za taj kontekst. **-ra** *agreementDn* je DN ugovora replikacije. Akcija se izvodi za specificirani ugovor replikacije.

  Primjer:

```
ldapexop -op controlrepl -action suspend -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"
```

- **controlreplerr**

  controlreplerr proširena operacija dozvoljava upravljanje tablicom grešaka replikacije na i5/OS V6R1 (ili IBM Tivoli Directory Server-u v6.0) ili novijem poslužitelju. Opcije su:

  `ldapexop -op controlreplerr –show <failure_ID> -ra <agreementDN>`

  Dozvoljava pogled unosa u tablicu grešaka replikacije

  <failure_ID>
  ID kvara. Specificirajte 0 za prikaz svih unosa.

  <agreementDN>
  Ugovor replikacije kojem je pridružen unos.

  `ldapexop -op controlreplerr –delete <failure_ID> -ra <agreementDN>`

  Dozvoljava brisanje unosa tablice grešaka replikacije

  <failure_ID>
  ID kvara. Specificirajte 0 za prikaz svih unosa.

  <agreementDN>
  Ugovor replikacije kojem je pridružen unos.

  `ldapexop -op controlreplerr –retry <failure_ID> -ra <agreementDN>`

  Dozvoljava ponovni pokušaj unosa u tablicu grešaka replikacije

  <failure_ID>
  ID kvara. Specificirajte 0 za prikaz svih unosa.

  <agreementDN>
  Ugovor replikacije kojem je pridružen unos.

- **evaluateGroups**

  Novu evaluateGroups operaciju podržava ldapexop pomoćni program:

  `ldapexop –op evaluateGroups –d userDN –a <lista parova atributa i vrijednosti svaki odijeljen razmakom>`

  Prikazuje listu grupe kojoj pripada userDN.

  ″–a″ opcija se koristi za specificiranje vrijednosti atributa za unos i dohvaćanje dinamičkih grupa koje se podudaraju s tim unosom. Ako ″–a″ opcija nije specificirana zahtjev će se poslati na poslužitelj samo za statičke grupe. Ta proširena operacija koristi se za dohvaćanje informacija o grupnom članstvu za userDN koji ne postoji na poslužitelju (Na primjer, userDN prikazuje udaljenog člana grupe). ibm-allGroups operativni atribut bi se trebao koristiti za ispisivanje grupnih članstava za poslužitelj koji sadrži userDN.

  Primjer:

| Za procjenu grupnog članstva za unos uid=sample,cn=users,o=ibm baziran na *departmentnumber* i *objectclass* vrijednostima atributa unosa:

```
ldapexop -op evaluateGroups -d uid=sample,cn=users,o=ibm -a objectclass=person
departmentnumber=abc
```

Bilješka: Tipično bi se toj proširena operacija dodijelile sve vrijednosti atributa za zanimljiv unos.

- **getattributes -attrType<*type*> -matches bool<*value*>**

  -attrType {operational | language_tag | attribute_cache | unique | configuration}
  Ovo je potreban atribut koji navodi tip atributa koji se zahtjeva.

  -matches bool {true | false}
  Navodi da li vraćena lista atributa odgovara tipu atributa navedenom pomoću -attrType< opcije.

  Primjer:

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

  Vraća listu svih atributa koji su određeni kao jedinstveni atributi.

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

  Vraća listu svih atributa koji nisu određeni kao jedinstveni atributi.

- **getusertype:** zahtjeva korisnički tip proširenu operaciju

  Ova proširena operacija vraća korisnički tip baziran na vezanom DN.

  Primjer:

  ```
  ldapexop - D <AdminDN> -w <Adminpw> -op getusertype
  ```

  vraća:

  ```
  User : root_administrator
  Role(s) : server_config_administrator directory_administrator
  User : global_admin_group_member
  Role(s) : directory_administrator
  ```

- **quiesce**: proširena operacija replikacije umirenog ili uznemirenog podstabla

  -rc *contextDn*
  To je potreban atribut koji specificira da li DN konteksta replikacije (podstablo) bude umiren ili uznemiren.

  -end To je neobvezan atribut koji, ako je prisutan, specificira da se uznemiri podstablo. Ako nije specificiran, default je da se umiri podstablo.

  Primjeri:

  ```
  ldapexop -op quiesce -rc "o=acme,c=us"

  ldapexop -op quiesce -end -rc "o=ibm,c=us"
  ```

- **readconfig**: ponovno čita proširene operacije datoteke konfiguracije

  -scope entire | single<*entry DN***><***attribute***>**
  To je potreban atribut.
  - **entire** označava da treba pročitati cijelu datoteku konfiguracije.
  - **single** znači da treba pročitati jedan specificiran unos i atribut.

  Primjeri:

  ```
  ldapexop -op readconfig -scope entire

  ldapexop -op readconfig -scope single "cn=configuration" ibm-slapdAdminPW
  ```

  Bilješka: Sljedeći unosi označeni s:
  - [1] postaju učinkoviti odmah nakon readconfig
  - [2] postaju učinkoviti na novim operacijama
  - [3] postaju učinkoviti ako lozinka nije promijenjena (nije potrebno readconfig)
  - [4] podržava pomoćni program reda za naredbe na i5/OS, ali ih ne podržava Directory Server na i5/OS

```
cn=Configuration
ibm-slapdadmindn[2]
ibm-slapdadminpw[2, 3]
ibm-slapderrorlog[1, 4]
ibm-slapdpwencryption[1]
ibm-slapdsizelimit[1]
ibm-slapdsysloglevel[1, 4]
ibm-slapdtimelimit[1]

cn=Front End, cn=Configuration
ibm-slapdaclcache[1]
ibm-slapdaclcachesize[1]
ibm-slapdentrycachesize[1]
ibm-slapdfiltercachebypasslimit[1]
ibm-slapdfiltercachesize[1]
ibm-slapdidletimeout[1]

cn=Event Notification, cn=Configuration
ibm-slapdmaxeventsperconnection[2]
ibm-slapdmaxeventstotal[2]

cn=Transaction, cn=Configuration
ibm-slapdmaxnumoftransactions[2]
ibm-slapdmaxoppertransaction[2]
ibm-slapdmaxtimelimitoftransactions[2]


cn=ConfigDB, cn=Config Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdreadonly[2]

cn=Directory, cn=RDBM Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdbulkloaderrors[1, 4]
ibm-slapdclierrors[1, 4]
ibm-slapdpagedresallownonadmin[2]
ibm-slapdpagedreslmt[2]
ibm-slapdpagesizelmt[2]
ibm-slapdreadonly[2]
ibm-slapdsortkeylimit[2]
ibm-slapdsortsrchallownonadmin[2]
ibm-slapdsuffix[2]
```

- **repltopology -rc [options]**:

repltopology proširena operacija koristi se za podudaranje informacija o topologiji replikacije o poslužitelju potrošača s topologijom na poslužitelju dobavljača.

```
ldapexop –op repltopology –rc  [-timeout secs] [-ra agreementDn]
```

gdje je

-rc contextDn
To je potreban atribut koji specificira korijen podstabla.

-timeout secs
To je neobvezan atribut koji, ako je prisutan, specificira timeout period u sekundama. Ako nije prisutan ili je 0, operacija čeka neodređeno dugo.

-ra agreementDn
-ra agreementDn je DN ugovora replikacije. Akcija se izvodi za specificirani ugovor replikacije. Ako -ra opcija nije specificirana, izvodi se akcija za sve ugovore replikacije definirane kontekstom.

Primjer:

```
ldapexop -op repltopology -rc "o=acme,c=us" -ra "cn=server3,
          ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
          o=acme,c=us"-timeout 60
```

Poslužitelj dobavljača povezuje se na poslužitelj potrošača pomoću konfiguriranih vjerodajnica replikacije. DN-ovi dobavljača imaju ovlaštenje dodavati sufikse dobavljaču konfiguracije poslužitelju (replike)potrošača. To koristi poslužitelj dobavljača kao dio proširene operacije Topologija replikacije za dodavanje sufiksa koji nedostaju na

| poslužitelj potrošača. Za sufikse za koje contextDN unos još ne postoji, DN-ovi dobavljača imaju ovlaštenje kreirati
| novo replicirano podstablo. Ako contextDN unos već postoji, mora biti definiran kao korijen repliciranog podstabla;
| tj. mora imati ibm-replicationcontext klasu objekta.

- **unbind** {**-dn**<*specificDN*>| **-ip**<*sourceIP*> | **-dn**<*specificDN*> **-ip**<*sourceIP*> | **all**}:

  odspojite veze bazirane na DN, IP, DN/IP ili odspojite sve veze. Sve veze bez operacija i sve veze s operacijama na radnom redu su prekinute odmah. Ako radnik trenutno radi na vezi, ona je prekinuta čim radnik završi tu jednu operaciju.

  -dn<*specificDN*>
  Izdaje zahtjev za prekidanjem veze samo s DN. Ovaj zahtjev rezultira u čišćenju svih veza vezanih na određeni DN.

  -ip<*sourceIP*>
  Izdaje zahtjev za prekidanjem veze samo s IP. Ovaj zahtjev rezultira u čišćenju svih veza iz navedenog IP izvora.

  -dn<*specificDN*> **-ip**<*sourceIP*>
  Izdaje zahtjev za prekidanjem veze određene pomoću DN/IP para. Ovaj zahtjev rezultira čišćenjem svih veza vezanih na određeni DN i iz navedenog IP izvora.

  -all Izdaje zahtjev za prekidanjem svih veza. Ovaj zahtjev rezultira u čišćenju svih veza osim veze iz koje je ovaj zahtjev dan. Ovaj atribut ne može biti korišten s -D ili -IP. atributima

  Primjeri:

  ```
  ldapexop -op unbind -dn cn=john
  ldapexop -op unbind -ip 9.182.173.43
  ldapexop -op unbind -dn cn=john -ip 9.182.173.43
  ldapexop -op unbind -all
  ```

- **uniqueattr -a <*attributeType*>:** identificirajte sve nejedinstvene vrijednosti za određeni atribut.

  -a <*attribute*>
  Navedite atribut za koji su sve konfliktne vrijednosti izlistane.

  Bilješka: Duplikat vrijednosti za binarne, operativne, konfiguracijske atribute i objectclass atribut nisu prikazane. Ovi atributi su nepodržane proširene operacije za jedinstvene atribute.

  Primjer:

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

  Sljedeća linije je dodana u konfiguracijsku datoteku pod ″cn=Directory,cn=RDBM Backends,cn=IBM Directory,cn=schema,cn=Configuration″ unos za ovu proširenu operaciju:

  ```
  ibm-slapdPlugin: extendedop /QSYS.LIB/QGLDRDBM.SRVPGM initUniqueAttr
  ```

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

Srodni koncepti

Directory Server API-ji

“Tablica grešaka replikacije” na stranici 43
Tablica grešaka replikacije zapisuje neuspjela ažuriranja za kasnije obnavljanje. Kad se replikacija pokrene, broj kvarova prijavljenih za svaki ugovor replikacija se broji. To se brojanje povećava ako ažuriranje rezultira kvarom, a novi se unos dodaje u tablicu.

Srodni zadaci

“Pregledavanje datoteke dnevnika izgubljeno i nađeno” na stranici 157
Datoteka dnevnika replikacije izgubljeno i nađeno može se pregledati pomoću IBM Tivoli Directory Server Web Administration Toola, pomoću opcija datoteke dnevnika ldapexop pomoćnog programa ili izravnim pregledavanjem datoteke.

ldapmodrdn

Pomoćni program reda za naredbe LDAP modificiraj-unos RDN.

Pregled

```
ldapmodrdn [-c] [-C charset] [-d debuglevel][-D binddn]
[-f file][-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile]
[-m mechanism] [-M] [-n] [-N certificatename] [-O hopcount]
[-p ldapport] [-P keyfilepw] [-r] [-R] [-U username] [-v] [-V version]
[-w passwd | ?] [-y proxydn] [-Y] [-Z] [dn newrdn | [-i file]]
```

Opis

ldapmodrdn je sučelje reda za naredbe u sučelju aplikativnog programiranja ldap_rename (API).

ldapmodrdn otvara vezu na LDAP poslužitelj, povezuje i premješta ili preimenuje unose. Informacija unosa se čita iz standardnog ulaza korištenjem **- f** opcije ili iz para reda za naredbe dn i rdn. Kod upotrebe -s opcije za premještanje unosa, -s opcija se primjenjuje na sve unose na koje se djelovalo naredbom.

Kako bi prikazali pomoć sintakse za **ldapmodrdn**, upišite:

```
ldapmodrdn -?
```

Opcije

-c Kontinuirani operativni način. Izvješteno je o greškama, no **ldapmodrdn** nastavlja s preinakama. U suprotnom je default akcija da se izađe nakon izvještaja o greški.

-C *charset*
Specificira da su nizovi dobavljeni kao ulaz na **ldapmodrdn** pomoćni program prikazani u lokalnom skupu znakova, kako je to specificirano s charset. Koristite **-C** *charset* opciju ako se kodna stranica ulaznog niza razlikuje od vrijednosti kodne stranice posla. Konzultirajte ldap_set_iconv_local_charset() API kako vidjeli podržane charset vrijednosti. Primijetite da su podržane vrijednosti za charset jednake vrijednostima podržanim za charset oznaku koja je neobvezno definirana u Verziji 1 LDIF datoteke.

-d *debuglevel*
Postavite razinu LDAP otkrivanja grešaka na debuglevel.

-D *binddn*
Upotrijebite ***binddn*** za povezivanje na LDAP direktorij. ***binddn*** treba biti nizom-prikazani DN. Kada je korišten s -m DIGEST-MD5, korišten je da navede autorizacijski ID. Može biti ili DN ili authzId niz koji počinje s ″u:″ ili ″dn:″.

-f *file* Čitaj informacije preinake unosa iz LDIF datoteke umjesto iz standardnog ulaza na redu za naredbe (navođenjem dn i novog rdn). Standardni ulaz može također biti dobavljen iz datoteke (< datoteka).

-G *područje*
Navodi područje. Ovaj parametar je neobvezan. Kada je korišten s -m DIGEST-MD5, vrijednost je predana na poslužitelj za vrijeme vezivanja.

-h *ldaphost*
Specificirajte zamjenski host na kojem se izvodi ldap poslužitelj.

-i *file* Pročitajte informacije o modifikaciji unosa iz datoteke umjesto iz standardnog ulaza ili reda za naredbe (specificiranjem rdn i newrdn). Standardni ulaz može biti dobavljen iz datoteke kao i (″< datoteke″).

-k Specificira korištenje kontrole administracije poslužitelja.

-K *keyfile*
Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva.

Ako pomoćni program ne može locirati bazu ključeva, koristit će čvrsto kodirani skup default povjerljivih korijena izdavača certifikata. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori.

Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

-m *mechanism*
Koristite ***mechanism*** kako bi specificirali SASL mehanizam koji će se koristiti za vezivanje na poslužitelj. Koristi se ldap_sasl_bind_s() API. **-m** parametar se zanemaruje ako je postavljeno **-V 2**. Ako **-m** nije naveden, koristi se jednostavna provjera identiteta. Valjani mehanizmi su:

- CRAM-MD5 - štiti lozinku koja je poslana na poslužitelja.
- EXTERNAL - koristi SSL certifikat. Treba -Z.
- GSSAPI - koristi Kerberos vjerodajnice korisnika.
- DIGEST-MD5 - zahtjeva da klijent pošalje vrijednost korisničkog imena poslužitelju. Zahtjeva -U. -D parametar (obično vezani DN) je korišten da navede autorizacijski ID. Može biti DN ili authzId niz koji počinje s u: ili dn:.
- OS400_PRFTKN - provjerava autentičnost lokalnog LDAP poslužitelja kao trenutnog i5/OS korisnika pomoću DN-a korisnika u sistemski projiciranoj pozadini. -D (vezani DN) i -w (lozinka) parametri ne trebaju biti navedeni.

-M Upravljajte referal objektima kao pravilnim unosima.

-n Pokazuje što će se napraviti, ali ne mijenja stvarne unose. Korisno za analizu u spoju s **-v**.

-N *certificatename*
Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Primijetite da ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti, certifikat klijenta nije potreban. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti potreban. ***certificatename*** nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, ***certificatename*** nije potreban ako je jednostruk par certifikat/privatan ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

-O *hopcount*
Specificirajte ***hopcount*** kako bi postavili maksimalan broj skokova knjižnice klijenta kada progoni referale. Default broj skokova je 10.

-p *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje ldap poslužitelj. Default LDAP port je 389. Ako nije specificiran, a specificirano je -Z, koristi se default LDAP SSL port 636.

-P *keyfilepw*
Određuje lozinku baze ključeva. Lozinka je potrebna za pristup šifriranim informacijama u datoteci ključeva baze podataka (koja može uključivati jedan ili više privatnih ključeva). Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključa, lozinka se dobiva od datoteke skrivene lozinke, a **-P** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

-r Uklonite stare RDN vrijednosti iz unosa. Default akcija je da se zadrže stare vrijednosti.

-R Određuje da se preporuke ne slijede automatski.

-s newSuperior
Specificira DN novog superiornog unosa prema kojem se premješta preimenovani unos. newSuperior argument može biti niz bez duljine (-s ″″).

Bilješka: Nova superiorna opcija nije podržana kod povezivanja na poslužitelj kod izdanja prije V6R1 (ITDS v6.0). Opcija je sada dozvoljena jedino na završnom unosu.

–U *username*
Navedite korisničko ime. Potrebno kod -m DIGEST-MD5 i zanemareno s bilo kojim drugim mehanizmom.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-V *version*
Specificira LDAP verziju koju koristi **ldapmodrdn** kada se povezuje na LDAP poslužitelj. Po defaultu, uspostavlja se LDAP V3 veza. Kako bi izričito izabrali LDAP V3, specificirajte **-V 3**. Specificirajte **-V 2** kako bi ga izvodili kao LDAP V2 aplikaciju. Aplikacija kao što je **ldapmodrdn** bira LDAP V3 kao preferirani protokol korištenjem ldap_init umjesto ldap_open.

-w *passwd* **| ?**
Koristite ***passwd*** kao lozinku za provjeru ovlaštenja. Koristite ? kako bi generirali prompt lozinke.

-y proxydn
Postavite proksiran ID za operaciju autorizacije proksijem.

–Y Koristite sigurnu LDAP vezu (TLS).

-Z Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

dn newrdn
Pogledajte sljedeći odlomak, “Format ulaza za dn newrdn”, za više informacija.

Format ulaza za dn newrdn

Ako su argumenti reda za naredbe *dn* i *newrdn* dani, *newrdn* zamjenjuje RDN unosa koji je specificirao DN, *dn*. U suprotnom, datoteka (ili standardan ulaz ako nema **- i** oznake) se sastoji od više od jednog unosa:

```
Razlikovno ime (DN)

Relativno razlikovno ime (RDN)
```

Jedna ili više praznih korišten mogu se koristiti za odvajanje svakog DN i RDN para.

Primjeri

Pod pretpostavkom da datoteka /tmp/entrymods postoji i da ima sadržaj:

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

naredba:

```
ldapmodrdn -r -i /tmp/entrymods
```

mijenja RDN Modificiraj me unosa iz Modificiraj me u Novo ja, a stari cn, Modificiraj me se uklanja.

Napomene

Ako informacija o unosu nije dobavljena iz datoteke korištenjem **-i** opcije (ili iz para reda za naredbe *dn* i *rdn*), **ldapmodrdn** naredba čeka kako bi pročitala unose iz standardnog ulaza.

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

Srodni koncepti

Directory Server API-ji

“Razlikovna imena (DN-ovi)” na stranici 9
Svaki unos u direktorij ima razlikovno ime (DN). DN je ime koje jednoznačno identificira unos u direktorij. Prva komponenta DN-a se naziva Relativno razlikovno ime (RDN).

ldapsearch

Pomoćni programi reda za naredbe LDAP pretraživanja.

Pregled

```
ldapsearch [-a deref] [-A] [-b searchbase] [-B] [-C charset] [-d debuglevel]
[-D binddn] [-e] [-f file] [-F sep] [-G realm] [-h ldaphost] [-i file] [-K keyfile]
[-l timelimit] [-L] [-m mechanism] [-M] [-n] [-N certificatename]
[-o attr_type] [-O maxhops] [-p ldapport] [-P keyfilepw] [-q pagesize]
[-R] [-s scope ] [-t] [-T seconds] [-U username] [-v] [-V version]
[-w passwd | ?] [-z sizelimit] [-y proxydn] [-Y] [-Z]
filter [-9 p] [-9 s] [attrs...]
```

Opis

ldapsearch je sučelje reda za naredbe ldap_search sučelja aplikativnog programiranja (API).

ldapsearch otvara vezu s LDAP poslužiteljem, povezuje i izvodi pretraživanja korištenjem filtera. Filter bi trebao biti u skladu s prikazom niza za LDAP filtere (pogledajte ldap_search u API-ji Poslužitelja direktorija za više informacija o filterima).

Ako **ldapsearch** pronađe jedan ili više unosa, dohvaćaju se atributi specificirani pomoću attr-ova i unosi i vrijednosti se ispisuju na standardan izlaz. Ako nijedan attr nije ispisan, vraćaju se svi atributi.

Kako bi prikazali pomoć sintakse za **ldapsearch**, upišite ldapsearch -?.

Opcije

-a deref
Određuje kako se radi dereferenciranje pseudonima. deref bi trebao biti nešto od nikad, uvijek, pretraži ili pronađi da bi specificirao da se pseudonimi nikad ne dereferenciraju, da se uvijek dereferenciraju, dereferenciraju kod pretraživanja ili dereferenciraju samo kada se locira bazni objekt za pretraživanje. Default je da se pseudonimi nikad ne dereferenciraju.

-A Učitaj samo atribute (bez vrijednosti). Ovo je korisno kad samo želite pogledati je li neki atribut prisutan u nekom slogu, a ne zanima vas pojedinačna vrijednost.

-b searchbase
Koristite searchbase kao početnu točku za pretraživanje umjesto defaulta. Ako **-b** nije specificirano, taj pomoćni program će ispitati LDAP_BASEDN varijablu okoline kako bi pronašao searchbase definiciju. Ako nije specificirano ni jedno ni drugo, default baza je postavljena na "".

-B Nemoj potisnuti prikaz ne-ASCII vrijednosti. To je korisno kada se radi s vrijednostima koje se pojavljuju u zamjenskim skupovima znakova kao što je ISO-8859.1. Tu opciju implicira **-L** opcija.

-C charset
Specificira da su nizovi koji su dobavljeni kao ulaz za ldapsearch pomoćni program prikazani u lokalnom skupu znakova (kako je to specificirano s charset). Ulaz niza uključuje filter, DN vezanja i bazni DN. Slično tome, kada prikazuje podatke **ldapsearch** konvertira podatke koji su primljeni iz LDAP poslužitelja u specificirani skup znakova. Koristite opciju **-C charset** ako je kodna stranica niza ulaza različita od vrijednosti kodne stranice posla. Pogledajte ldap_set_iconv_local_charset() API-je kako bi vidjeli podržane vrijednosti skupa znakova. Isto tako, ako je specificirana **-C** opcija i **-L** opcija, za ulaz se pretpostavlja da se nalazi u specificiranom skupu znakova, ali izlaz iz **ldapsearch** se uvijek sačuva u svojem UTF-8 prikazu ili u baznom-64 kodiranom prikazu podataka kada se otkriju znakovi koji se ne mogu ispisati. To je tako jer standardne LDIF datoteke sadrže samo UTF-8 (ili bazni-64 kodirani UTF-8) prikaze podataka niza. Primijetite da su podržane vrijednosti za charset iste vrijednosti koje su podržane za charset oznaku koja je neobvezno definirana u verziji 1 LDIF datoteka.

-d debuglevel
Postavite razinu LDAP otkrivanja grešaka na debuglevel.

-D binddn

Koristite binddn kako bi se vezali na LDAP direktorij. ***binddn*** treba biti nizom-prikazani DN (pogledajte LDAP Razlikovna Imena). Kada je korišten s -m DIGEST-MD5, korišten je da navede autorizacijski ID. Može biti DN ili authzId niz koji počinje s ″u:″ ili ″dn:″.

-e Prikažite informacije o verziji LDAP knjižnice i nakon toga izađite.

-F sep Koristite sep kao odjelitelje polja između imena atributa i vrijednosti. Default odjelitelj je `=', ako nije specificirana **-L** oznaka jer se u tom slučaju ta opcija zanemaruje.

-G *područje*

Navodi područje. Ovaj parametar je neobvezan. Kada je korišten s -m DIGEST-MD5, vrijednost je predana na poslužitelj za vrijeme vezivanja.

-h ldaphost

Specificirajte zamjenski host na kojem se izvodi ldap poslužitelj.

-i file Čita sljedove linija iz datoteke i izvodi jedno LDAP pretraživanje za svaku liniju. U tom slučaju, filter koji je dan na redu za naredbe se tretira kao obrazac gdje se prvo pojavljivanje % zamjenjuje s linijom za datoteku. Ako je datoteka jedan ″-″ znak, onda se linije čitaju iz standardnog ulaza.

-K keyfile

Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva.

Ako pomoćni program ne može locirati bazu ključeva, koristit će čvrsto kodirani skup default povjerljivih korijena izdavača certifikata. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori.

Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača **-Z**. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

-l timelimit

Čeka do najviše timelimit sekundi kako bi se dovršilo pretraživanje.

-L Prikazuje rezultate traženja u LDIF formatu. Ta se opcija isto vraća na **-B** opciju i uzrokuje da se zanemari **-F** opcija.

-m *mechanism*

Koristite ***mechanism*** kako bi specificirali SASL mehanizam koji će se koristiti za vezivanje na poslužitelj. Koristi se ldap_sasl_bind_s() API. **-m** parametar se zanemaruje ako je postavljeno **-V 2**. Ako **-m** nije naveden, koristi se jednostavna provjera identiteta. Valjani mehanizmi su:

- CRAM-MD5 - štiti lozinku koja je poslana na poslužitelja.
- EXTERNAL - koristi SSL certifikat. Treba -Z.
- GSSAPI - koristi Kerberos vjerodajnice korisnika.
- DIGEST-MD5 - zahtjeva da klijent pošalje vrijednost korisničkog imena poslužitelju. Zahtjeva -U. -D parametar (obično vezani DN) je korišten da navede autorizacijski ID. Može biti DN ili authzId niz koji počinje s u: ili dn:.
- OS400_PRFTKN - provjerava autentičnost lokalnog LDAP poslužitelja kao trenutnog i5/OS korisnika pomoću DN-a korisnika u sistemski projiciranoj pozadini. -D (vezani DN) i -w (lozinka) parametri ne trebaju biti navedeni.

-M Upravljajte referal objektima kao pravilnim unosima.

-n Pokazuje što će se napraviti, ali ne mijenja stvarne unose. Korisno za analizu u spoju s **-v**.

-N certificatename

Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva.

Bilješka: Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti potreban. *certificatename* nije

potreban ako je kao default određen par certifikat/privatni ključ. Slično, *certificatename* nije potreban ako je jednostruk par certifikat/privatan ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

-o *attr_type*

Kako bi specificirali atribut koji će se koristiti za kriterij sortiranja rezultata pretraživanja, možete koristiti -o (poredak) parametar. Možete koristi više -o parametara kako bi detaljnije definirali poredak sortiranja. U sljedećem primjeru, rezultati pretraživanja su prvo sortirani prezimenom (sn), a onda danim imenom, s time da se dano ime (givenname) sortira obrnutim poretkom (silazno) kako je specificirano minus znakom prefiksa (-):

```
-o sn -o -givenname
```

Stoga je sintaksa parametra sortiranja kako slijedi:

```
[-]<attribute name>[:<matching rule OID>]
```

gdje je

- attribute name ime atributa prema kojem želite sortirati.
- matching rule OID je neobvezan OID pravila podudaranja koje želite koristiti za sortiranje. Pravilo podudaranja OID atribut nije podržan od strane Poslužitelja direktorija, međutim drugi LDAP poslužitelji mogu podržavati ovaj atribut.
- Znak minusa (-) označava da rezultat mora biti sortiran u obrnutom poretku.
- Kritičnost je uvijek kritična.

Default ldapsearch operacija je da se ne sortiraju vraćeni rezultati.

-O maxhops

Specificirajte maxhops kako bi postavili maksimalan broj skokova knjižnice klijenta kada traži referale. Default broj skokova je 10.

-p ldapport

Specificirajte zamjenski TCP port na kojem osluškuje ldap poslužitelj. Default LDAP port je 389. Ako nije specificiran, a specificirano je -Z, koristi se default LDAP SSL port 636.

-P keyfilepw

Određuje lozinku baze ključeva. Lozinka je potrebna za pristup šifriranim informacijama u datoteci ključeva baze podataka (koja može uključivati jedan ili više privatnih ključeva). Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključa, lozinka se dobiva od datoteke skrivene lozinke, a **-P** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

-q *pagesize*

Kako bi specificirali podjelu rezultata u stranice možete koristiti dva parametra: -q (veličina stranice upita) i -T (vrijeme između pretraživanja u sekundama). U sljedećem primjeru, rezultati pretraživanja vraćaju stranicu (25 unosa) svakih 15 sekundi tako dugo dok se ne vrate svi rezultati za to pretraživanje. ldapsearch klijent rukuje svim nastavcima veze za svaki zahtjev podjele u stranice za vrijeme dok traje operacija pretraživanja.

Ti parametri mogu biti korisni kada klijent ima ograničene resurse ili kada je povezan preko veze s malom pojasnom širinom. Općenito, omogućava vam da kontrolirate brzinu kojem se podaci vraćaju iz zahtjeva za pretraživanjem. Umjesto da odjednom primite sve rezultate, možete dobivati po nekoliko unosa (stranicu). Osim toga, možete kontrolirati trajanje odgode između svakog zahtjeva za stranicom, dajući tako klijentu vremena da obradi rezultate.

```
 -q 25  -T 15
```

Ako je specificiran -v (opširno) parametar, ldapsearch nakon što se iz poslužitelja vrati svaka stranica unosa ispisuje koliko je unosa vraćeno do sada, na primjer, **Vraćeno je ukupno 30 unosa.**

Omogućeno je više -q parametara tako da možete specificirati različite veličine stranica za vrijeme trajanja jedne operacije pretraživanja. U sljedećem primjeru, prva stranica ima 15 unosa, druga stranica ima 20 unosa, a treći parametar završava operaciju rezultat/pretraživanje podijeljenu u stranice:

```
-q 15 -q 20 -q 0
```

U sljedećem primjeru, prva stranica ima 15 unosa, a sve ostale stranice imaju 20 unosa, nastavljajući se na zadnju specificiranu **-q** vrijednost dok se operacija pretraživanja ne dovrši:

```
-q 15 -q 20
```

Default ldapsearch operacija je da se vrate svi unosi u jednom zahtjevu. Nije napravljena nikakva podjela u stranice za default ldapsearch operaciju.

-R Određuje da se preporuke ne slijede automatski.

-s scope
Određuje raspon pretraživanja. scope bi trebao biti jedno od bazno, jedna ili pod kako bi se specificiralo pretraživanje baznog objekta, jedne-razine ili podstabla. Default je pod.

-t Piše učitane vrijednosti u skup privremenih datoteka. To je korisno kada se radi s ne-ASCII vrijednostima kao što je jpegPhoto ili audio.

-T *seconds*
Vrijeme između pretraživanja (u sekundama). **-T** opcija je podržana samo kada je specificirana **-q** opcija.

–U *username*
Navedite korisničko ime. Potrebno kod -m DIGEST-MD5 i zanemareno s bilo kojim drugim mehanizmom.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-V Specificira LDAP verziju koju će koristiti ldapmodify kada se povezuje na LDAP poslužitelj. Po defaultu, uspostavlja se LDAP V3 veza. Kako bi izričito izabrali LDAP V3, specificirajte ″-V 3″. Specificirajte ″-V 2″ da se izvodi kao LDAP V2 aplikacija. Aplikacija kao što je ldapmodify bira LDAP V3 kao preferirani protokol korištenjem ldap_init umjesto ldap_open.

-w *passwd* **| ?**
Koristite ***passwd*** kao lozinku za provjeru ovlaštenja. Koristite ? kako bi generirali prompt lozinke.

-y proxydn
Postavite proksiran ID za operaciju autorizacije proksijem.

–Y Koristite sigurnu LDAP vezu (TLS).

-z sizelimit
Ograničite rezultate pretraživanja na najviše sizelimit unosa. Time postaje moguće odrediti gornju granicu broja slogova koji se vraćaju kod operacije pretraživanja.

-Z Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

filter Specificira prikaz niza filtera koji će se primijeniti u pretraživanju. Jednostavni filteri mogu biti specificirani kao attributetype=attributevalue. Složeniji filteri su specificirani korištenjem bilježenja prefiksa u skladu sa sljedećim Backus Naur Form (BNF):

```
<filter> ::='('<filtercomp>')'
<filtercomp> ::= <and>|<or>|<not>|<simple>
<and> ::= '&' <filterlist>
<or> ::= '|' <filterlist>
<not> ::= '!' <filter>
<filterlist> ::= <filter>|<filter><filterlist>
<simple> ::= <attributetype><filtertype>
<attributevalue>
<filtertype> ::= '='|'~='|'<='|'>='
```

'~=' konstrukt se koristi za specificiranje približnog uparivanja. Prikaz za <*attributetype*> i <*attributevalue*> su opisani u RFC 2252, LDAP V3 definicije sintakse atributa. Nadalje, ako je filtertype '=' tada <*attributevalue*> može biti pojedinačni * za postizanje provjere postojanja atributa ili može sadržavati tekst i zvjezdice (*) razbacane za postizanje uparivanja podniza.

Na primjer, filter ″mail=*″ pronalazi sve vrijednosti koje imaju atribut pošte. Filter ″mail=*@student.of.life.edu″ pronalazi sve unose koji imaju atribut pošte koji završava sa specificiranim nizom. Kada želite staviti zavjese u filter, izbjegnite ih sa znakom obrnuta kosa crta (\).

Bilješka: Filter poput "cn=Bob *", gdje postoji razmak između Boba i zvjezdice (*), podudara se s ″Bob Carter″, ali ne i s ″Bobby Carter″ u IBM direktoriju. Razmak između ″Bob″ i zamjenskog znaka (*) utječe na rezultate pretraživanja koje koristi filtere.

Pogledajte RFC 2254, Prikaz niza LDAP filtera pretraživanja za potpuniji opis dopustivih filtera.

Format izlaza

Ako je pronađen jedan ili više unosa, svaki unos se ispisuje na standardan izlaz u obliku:

```
Razlikovno ime (DN)

attributename=vrijednost

attributename=vrijednost

attributename=vrijednost

...
```

Višestruki upisi su razdvojeni jednim praznim retkom. Ako se **-F** opcija koristi kako bi se specificirao znak odjelitelj, on će se koristiti umjesto `=' znaka. Ako se koristi **-t** opcija, umjesto stvarne vrijednosti se koristi ime privremene datoteke. Ako je dana **-A** opcija, zapisuje se samo dio ″attributename″.

Primjeri

Sljedeća naredba:

```
ldapsearch "cn=john doe" cn telephoneNumber
```

izvodi pretraživanje podstabla (korištenjem default baze pretraživanja) za unose sa zajedničkim imenom (commonName) ″john doe″. Dohvaćaju se commonName i telephoneNumber vrijednosti i ispisuju se na standardan izlaz. Ispis bi mogao izgledati približno ovako ako se pronađu dva unosa:

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

  cn=John Doe

  cn=John Edward Doe

  cn=John E Doe 1

  cn=John E Doe

  telephoneNumber=+1 313 555-5432



  cn=John B Doe, ou=Information Technology Division,
ou=Faculty and Staff, ou=People, o=University of Higher Learning, c=US

  cn=John Doe

  cn=John B Doe 1
```

```
  cn=John B Doe

  telephoneNumber=+1 313 555-1111
```

Naredba:

```
ldapsearch -t "uid=jed" jpegPhoto audio
```

izvodi pretraživanje podstabla korištenjem default baze pretraživanja za unose s ID-om korisnika ″jed″. Dohvaćaju se vrijednosti jpegPhoto i audio i zapisuju se u privremene datoteke. Izlaz bi mogao izgledati slično ovome ako se pronađe jedan unos s jednom vrijednosti za svaki od traženih atributa:

```
cn=John E Doe, ou=Information Technology Division,

  ou=Faculty and Staff,

  ou=People, o=University of Higher Learning, c=US

  audio=/tmp/ldapsearch-audio-a19924

  jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

Naredba:

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

izvodi pretraživanje jedne razine na c=US razini za sve organizacije čije ime organizacije (organizationName) počinje s university. Rezultati pretraživanja su prikazani u LDIF formatu (pogledajte LDAP Format razmjene podataka). Dohvatit će se vrijednosti atributa organizationName i description i ispisat će se na standardnom izlazu, a to će rezultirati izlazom koji je sličan ovome:

```
dn: o=University of Alaska Fairbanks, c=US

  o: University of Alaska Fairbanks

  description: Preparing Alaska for a brave new tomorrow

  description: leaf node only


  dn: o=University of Colorado at Boulder, c=US

  o: University of Colorado at Boulder

  description: No personnel information

  description: Institution of education and research


  dn: o=University of Colorado at Denver, c=US

  o: University of Colorado at Denver

  o: UCD

  o: CU/Denver

  o: CU-Denver

  description: Institute for Higher Learning and Research


  dn: o=University of Florida, c=US
```

```
  o: University of Florida

  o: UFl

  description: Shaper of young minds


 ...
```

Naredba:

```
ldapsearch -b "c=US" -o ibm-slapdDN "objectclass=person" ibm-slapdDN
```

izvodi pretraživanje na razini podstabla na c=US razini za sve osobe. Kada se taj posebni atribut (ibm-slapdDN) koristi za sortirana pretraživanja, on sortira rezultate pretraživanja znakovnim prikazom Razlikovnog imena (DN). Izlaz bi mogao izgledati slično ovom:

```
cn=Al Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US

cn=Al Garcia,ou=Home Entertainment,ou=Austin,o=IBM,c=US

cn=Amy Nguyen,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Arthur Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US

cn=Becky Garcia,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Ben Catu,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Ben Garcia Jr,ou=Home Entertainment,ou=Austin,o=IBM,c=US

cn=Bill Keller Jr.,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Bob Campbell,ou=In Flight Systems,ou=Austin,o=IBM,c=US
```

Naredba:

```
ldapsearch –h hostname –o sn –b "o=ibm,c=us" "title=engineer"
```

vraća sve unose u IBM direktorij zaposlenika čiji je naslov ″inženjer″, s rezultatima sortiranim prema prezimenu.

Naredba:

```
ldapsearch –h hostname –o -sn –o cn –b "o=ibm,c=us" "title=engineer"
```

vraća sve unose u IBM direktorij zaposlenika čiji je naslov ″inženjer″, s rezultatima sortiranim prema prezimenu (silaznim redoslijedom) i zatim prema imenu (uzlaznim redoslijedom).

Naredba:

```
ldapsearch –h hostname –q 5 –T 3 –b o=ibm,c=us "title=engineer"
```

vraća pet unosa po stranici, sa zakašnjenjem od 3 sekunde između stranica za sve unose u IBM direktoriju zaposlenika čiji je naslov ″inženjer″.

Ovaj primjer pokazuje pretraživanja u kojima je uključen i referalni objekt. Directory Server LDAP direktoriji mogu sadržavati referalne objekte pod uvjetom da sadrže samo sljedeće:

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

Pretpostavimo da ’System_A’ sadrži unos referala:

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

Svi atributi koji su pridruženi unosu bi trebali prebivati na ’System_B’.

System_B sadrži slog:

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

Kada klijent izdaje zahtjev na ’System_A’, LDAP poslužitelj na System_A odgovara klijentu s URL-om:

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

Klijent koristi te informacije kako bi izdao zahtjev na System_B. Ako unos na System_A sadrži atribute kao dodatak za dn, objectclass i ref, poslužitelj zanemaruje te atribute (ako ne specificirate **-R** oznaku koja označava da ne treba loviti referale).

Kad klijent primi referalni odgovor iz poslužitelja, on ponovno izdaje zahtjev, ali ovaj puta poslužitelju na koga se odnosi vraćena adresa URL. Novi zahtjev ima isti opseg kao i originalni zahtjev. Rezultati ovog pretraživanja su različiti ovisno o vrijednosti koju navedete za raspon pretraživanja (**-b**).

Ako ste specificirali -s base kao što je to ovdje prikazano:

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

pretraživanje vraća sve atribute za sve unose sa ’sn=Jensen’ koji prebivaju u ’ou=Rochester, o=Big Company, c=US’ na System_A i System_B.

Ako navedete -s sub, kako je prikazano ovdje:

```
ldapsearch -s sub "cn=John"
```

poslužitelj bi pretražio sve nastavke i vratio sve unose s ″cn=John″. To je poznato kao pretraživanje po podstablu na null bazi. Cijeli direktorij je pretražen s jednom operacijom pretraživanja umjesto višestrukih pretraživanja svaka s drugačijim nastavcima u bazi pretraživanja. Ovaj tip operaciji pretraživanja traje dulje i troši više sistemskih resursa zato što se pretražuje cijeli direktorij (svi nastavci).

Bilješka: Pretraživanje podstabla na null bazi ne vraća informacije o shemi, mijenja informacije o dnevniku, niti bilo što iz sistemski zaštićene pozadine.

Ako navedete -s sub, kako je prikazano ovdje:

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

pretraživanje vraća sve atribute za sve unose sa ’sn=Jensen’ koji prebivaju u ili ispod ’ou=Rochester, o=Big Company, c=US’ na System_A i System_B.

Ako navedete -s one, kako je prikazano ovdje:

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

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

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

Klijent na to šalje zahtjev:

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

To isto tako ne daje nikakve rezultate, jer unos

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
```

prebiva na

```
ou=Rochester, o=Big Company, c=US
```

Pretraživanje sa `-s` pokušava pronaći unose u razini koja je neposredno ispod

```
ou=Rochester, o=Big Company, c=US
```

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

Srodni koncepti

Directory Server API-ji

“Referali LDAP direktorija” na stranici 49
Referali omogućuju Poslužiteljima direktorija da rade u timovima. Ako DN koji klijent zahtijeva nije u jednom direktoriju, poslužitelj može automatski poslati (uputiti) zahtjev na neki drugi LDAP poslužitelj.

Srodne reference

“LDAP format razmjene podataka (LDIF)” na stranici 236
LDAP format razmjene podataka je standardni tekstualni format za prikazivanje LDAP objekata i LDAP ažuriranja (dodaj, modificiraj, obriši, modificiraj DN) u tekstualnom obliku. Datoteke koje sadrže LDIF slogove mogu se koristiti za prijenos podataka između directory servera ili kao ulaz LDAP alatima poput **ldapadd** i **ldapmodify**.

Srodne informacije

RFC 2252, LDAP V3 Atribut Definicije sintakse

RFC 2254, Predstavljanje niza za LDAP filtere za pretraživanje

ldapchangepwd

Pomoćni programi reda za naredbe LDAP modificiraj lozinku.

Pregled

```
ldapchangepwd -D binddn -w passwd | ? -n newpassword | ?
[-C charset] [-d debuglevel][-G realm][-h ldaphost]
[-K keyfile] [-m mechanism] [-M] [-N certificatename]
[-O maxhops] [-p ldapport] [-P keyfilepw] [-R]
[-U username] [-v] [-V version] [-y proxydn] [-Y] [-Z] [-?]
```

Opis

Šalje zahtjev za modificiranjem lozinke na LDAP poslužitelj. Dopušta promjenu lozinke za unos direktorija.

Opcije

-C *charset*
: Specificira da su DN-ovi dobavljeni kao ulaz u ldapdelete pomoćni program, predstavljeni u lokalnom skupu

znakova, kako je to specificirano s charset. Koristite opciju -C charset ako je kodna stranica niza ulaza različita od vrijednosti kodne stranice posla. Pogledajte ldap_set_iconv_local_charset() API-je kako bi vidjeli podržane vrijednosti skupa znakova.

-d *debuglevel*
Postavite razinu LDAP otkrivanja grešaka na debuglevel.

-D *binddn*
Upotrijebite ***binddn*** za povezivanje na LDAP direktorij. ***binddn*** je niz-predstavljeno DN. Kada je korišten s -m DIGEST-MD5, korišten je da navede autorizacijski ID. Može biti ili DN ili authzId niz koji počinje s ″u:″ ili ″dn:″.

–G *područje*
Navodi područje. Ovaj parametar je neobvezan. Kada je korišten s -m DIGEST-MD5, vrijednost je predana na poslužitelj za vrijeme vezivanja.

-h *ldaphost*
Specificirajte zamjenski host na kojem se izvodi ldap poslužitelj.

-K *keyfile*
Određuje ime SSL baze ključeva. Ako baza ključeva nije u tekućem direktoriju, navedite puno ime datoteke baze ključeva.

Ako pomoćni program ne može locirati bazu ključeva, koristit će čvrsto kodirani skup default povjerljivih korijena izdavača certifikata. Baza ključeva obično sadržava jedan ili više certifikata izdavača certifikata (CA) kojima klijent vjeruje. Ovi tipovi X.509 certifikata su poznati i kao pouzdani izvori.

Ovim se parametrom djelotvorno omogućuje aktiviranje prekidača -Z. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

-m *mechanism*
Koristite ***mechanism*** kako bi specificirali SASL mehanizam koji će se koristiti za vezivanje na poslužitelj. Koristi se ldap_sasl_bind_s() API. **-m** parametar se zanemaruje ako je postavljeno **-V 2**. Ako **-m** nije naveden, koristi se jednostavna provjera identiteta. Valjani mehanizmi su:

- CRAM-MD5 - štiti lozinku koja je poslana na poslužitelja.
- EXTERNAL - koristi SSL certifikat. Treba -Z.
- GSSAPI - koristi Kerberos vjerodajnice korisnika.
- DIGEST-MD5 - zahtjeva da klijent pošalje vrijednost korisničkog imena poslužitelju. Zahtjeva -U. -D parametar (obično vezani DN) je korišten da navede autorizacijski ID. Može biti DN ili authzId niz koji počinje s u: ili dn:.

-M Upravljajte referal objektima kao pravilnim unosima.

-n *newpassword* **| ?**
Specificira novu lozinku. Koristite ? kako bi generirali prompt lozinke.

-N *certificatename*
Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti potreban. ***certificatename*** nije potreban ako je kao default određen par certifikat/privatni ključ. Slično, ***certificatename*** nije potreban ako je jednostruk par certifikat/privatan ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

-O *maxhops*
Specificirajte ***maxhops*** kako bi postavili maksimalan broj skokova koje poduzima knjižnica klijenta kada traži referale. Default broj skokova je 10.

-p *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje ldap poslužitelj. Default LDAP port je 389. Ako nije specificirano **-p**, a specificirano je **-Z**, koristi se default LDAP SSL port 636.

-P *keyfilepw*
Određuje lozinku baze ključeva. Lozinka je potrebna za pristup šifriranim informacijama u datoteci ključeva baze podataka, koja može uključivati jedan ili više privatnih ključeva. Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključa, lozinka se dobiva od datoteke skrivene lozinke, a **-P** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-Z** niti **-K**.

-R Određuje da se preporuke ne slijede automatski.

-U *username*
Navedite korisničko ime. Potrebno kod -m DIGEST-MD5 i zanemareno s bilo kojim drugim mehanizmom.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

-V *version*
Specificira LDAP verziju koju koristi **ldapdchangepwd** kada se povezuje na LDAP poslužitelj. Po defaultu, uspostavlja se LDAP V3 veza. Kako bi izričito izabrali LDAP V3, specificirajte **-V 3**. Specificirajte **-V 2** kako bi ga izvodili kao LDAP V2 aplikaciju. Aplikacija kao što je **ldapdchangepwd** bira LDAP V3 kao preferirani protokol korištenjem ldap_init umjesto ldap_open.

-w *passwd* **| ?**
Koristite ***passwd*** kao lozinku za provjeru ovlaštenja. Koristite ? kako bi generirali prompt lozinke.

-y proxydn
Postavite proksiran ID za operaciju autorizacije proksijem.

–Y Koristite sigurnu LDAP vezu (TLS).

-Z Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem. Ako za Directory Server na i5/OS koristite -Z, a ne -K ili -N, koristit će se certifikat povezan s ID-om aplikacije klijenta usluga direktorija.

-? Prikazuje sintaksnu pomoć za ldapchangepwd.

Primjeri

Sljedeća naredba

```
ldapchangepwd -D cn=John Doe -w a1b2c3d4 -n wxyz9876
```

mijenja lozinku za unos koji ima commonName ″John Doe″ s a1b2c3d4 u wxyz9876

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

Srodni koncepti

Lightweight Directory Access Protocol (LDAP) API-ji
Pogledajte Lightweight Directory Access Protocol (LDAP) API-je za više informacija o API-jima Directory Servera.

ldapdiff

Pomoćni programi reda za naredbe LDAP sinkronizacije replike.

Bilješka: Ta naredba bi se mogla izvoditi duže vrijeme ovisno o broju unosa (i atributa za te unose) koji se repliciraju.

Pregled

(Uspoređuje i usklađuje unose podataka između dva poslužitelja unutar okoline replikacije.)

```
ldapdiff -b baseDN -sh host -ch host [-a] [-C countnumber]
 [-cD dn] [-cK keyStore] [-cw password] -[cN keyLabel]
 [-cp port] [-cP keyStorePwd]  [-cZ] [-F] [-L filename] [-sD dn] [-sK keyStore]
 [-sw password] -[sN keyLabel] [-sp port] [-sP keyStorePwd]
 [-sZ] [-v]
```

ili

(Uspoređuje shemu između dva poslužitelja.)

```
 ldapdiff -S -sh host -ch host [-a] [-C countnumber][-cD dn]
 [-cK keyStore] [-cw password] -[cN keyLabel] [-cp port]
 [-cP keyStorePwd] [-cZ] [-L filename] [-sD dn]
 [-sK keyStore] [-sw password] [-sN keyLabel] [-sp port]
 [-sP keyStorePwd] [-sZ] [-v]
```

Opis

Taj alat usklađuje replika poslužitelj s njegovim glavnim poslužiteljem. Kako bi prikazali pomoć sintakse za **ldapdiff**, upišite:

```
ldapdiff -?
```

Opcije

Sljedeće opcije se odnose na **ldapdiff** naredbu. Postoje dvije podgrupe koje se točno određeno odnose na poslužitelja dobavljača ili poslužitelja potrošača.

-a Specificira korištenje kontrole administracije poslužitelja za pisanja na repliku samo za čitanje.

-b *baseDN*
Koristite searchbase kao početnu točku za pretraživanje umjesto defaulta. Ako **-b** nije specificirano, taj pomoćni program će ispitati LDAP_BASEDN varijablu okoline kako bi pronašao searchbase definiciju.

-C *countnumber*
Broji koliko unosa treba popraviti. Alat postoji ako je pronađeno više od specificiranog broja nepodudarnosti.

-F To je opcija popravka. Ako je specificirana, sadržaj replike potrošača se modificira kako bi se podudarao sa sadržajem dobavljača. To se ne može koristiti ako je specificirano i **-S**.

-L Ako nije specificirana **-F** opcija, koristite ovu opciju kako bi generirali LDIF datoteku za izlaz. LDIF datoteka se može koristiti kako bi se ažurirao potrošač tako da se uklone razlike.

-S Specificira uspoređivanje sheme na oba poslužitelja.

-v Koristi opširni modus, uz ispis brojnih dijagnostičkih poruka u standardnom izlazu.

Opcije za dobavljača replikacije

Sljedeće opcije se odnose na poslužitelj potrošača i označene su s početnim ’s’ u imenu opcije.

-sD *dn* Koristite ***dn*** za povezivanje na LDAP direktorij. ***dn*** je niz-predstavljeno DN.

-sh *host*
Specificira ime hosta.

-sK *keyStore*
Specificirajte ime SSL datoteke ključeva baze podataka s default proširenjem **kdb**. Ako taj parametar nije specificiran ili je vrijednost prazan niz (-sK″″), koristi se sistemski keystore. Ako datoteka baze podataka ključeva nije u trenutnom direktoriju, navedite puno ime datoteke baze ključeva.

-sN *keyLabel*
Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je oznaka specificirana bez da je specificirano keystore, oznaka je identifikator aplikacije u Upravitelju digitalnih certifikata (DCM). Default oznaka (ID aplikacije) je QIBM_GLD_DIRSRV_CLIENT. Ako je LDAP poslužitelj konfiguriran tako da

izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, potreban je certifikat klijenta. ***keyLabel*** nije potrebno ako je bio označen default par certifikat/privatni ključ. Slično tome, ***keyLabel*** nije potreban ako je jednostruk par certifikat/privatni ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-sZ** niti **-sK**.

-sp *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje ldap poslužitelj. Default LDAP port je 389. Ako nije specificirano **-sp**, a specificirano je **-sZ**, koristi se default LDAP SSL port 636.

-sP *keyStorePwd*
Određuje lozinku baze ključeva. Lozinka je potrebna za pristup šifriranim informacijama u datoteci ključeva baze podataka, koja može uključivati jedan ili više privatnih ključeva. Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključeva, lozinka se dobiva od datoteke skrivene lozinke, a **-sP** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-sZ** niti **-sK**. Lozinka se ne koristi ako postoji skrivena datoteka koje se koristi za keystore.

-st *trustStoreType*
Specificirajte oznaku koja je pridružena certifikatu klijenta u pouzdanoj datoteci baze podataka. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, certifikat klijenta bi mogao biti potreban. ***trustStoreType*** nije potreban ako je kao default određen par certifikat/privatni ključ. Slično tome, ***trustStoreType*** nije potreban ako je jednostruk certifikat/privatni par ključeva u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-sZ** niti **-sT**.

-sZ Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem.

Opcije za potrošača replikacije

Sljedeće opcije se odnose na poslužitelja potrošača i označene su s početnim 'c' u imenu opcije. Radi prikladnosti, ako je -cZ specificirano bez da se specificiraju vrijednosti za -cK, -cN ili -cP, te opcije koriste istu vrijednost koja je specificirana za SSL opcije dobavljača. Kako bi nadjačali opcije dobavljača i koristili default postavke, specificirajte -cK ″″ -cN ″″ -cP ″″.

-cD *dn* Koristite ***dn*** za povezivanje na LDAP direktorij. ***dn*** je niz-predstavljeno DN.

-ch *host*
Specificira ime hosta.

-cK *keyStore*
Specificirajte ime SSL datoteke baze podataka ključa s default proširenjem kdb. Ako je vrijednost prazan niz (-sK″″), koristi se sistemski keystore. Ako datoteka baze podataka ključeva nije u trenutnom direktoriju, navedite puno ime datoteke baze ključeva.

-cN *keyLabel*
Određuje oznaku pridruženu certifikatu klijenta u bazi ključeva. Ako je LDAP poslužitelj konfiguriran tako da izvodi samo provjeru autentičnosti poslužitelja, nije potreban certifikat klijenta. Ako je oznaka specificirana bez da je specificirano keystore, oznaka je identifikator aplikacije u Upravitelju digitalnih certifikata (DCM). Default oznaka (ID aplikacije) je QIBM_GLD_DIRSRV_CLIENT. Ako je LDAP poslužitelj konfiguriran tako da izvodi provjeru autentičnosti klijenta i poslužitelja, potreban je certifikat klijenta. ***keyLabel*** nije potrebno ako je bio označen default par certifikat/privatni ključ. Slično tome, ***keyLabel*** nije potreban ako je jednostruk par certifikat/privatni ključ u odredišnoj datoteci baze podataka ključeva. Taj parametar se zanemaruje ako nije specificirano **-cZ** niti **-cK**.

-cp *ldapport*
Specificirajte zamjenski TCP port na kojem osluškuje ldap poslužitelj. Default LDAP port je 389. Ako nije specificirano **-cp**, a specificirano je **-cZ**, koristi se default LDAP SSL port 636.

-cP *keyStorePwd*
Određuje lozinku baze ključeva. Lozinka je potrebna za pristup šifriranim informacijama u datoteci ključeva

baze podataka, koja može uključivati jedan ili više privatnih ključeva. Ako je datoteka skrivene lozinke pridružena datoteci baze podataka ključeva, lozinka se dobiva od datoteke skrivene lozinke, a **-cP** parametar nije potreban. Taj parametar se zanemaruje ako nije specificirano **-cZ** niti **-cK**.

-cw *password* **| ?**
Koristite ***password*** kao lozinku za provjeru autentičnosti. Koristite ? kako bi generirali prompt lozinke.

-cZ Koristi zaštićenu SSL vezu za komunikaciju s LDAP poslužiteljem.

Primjeri

```
ldapdiff -b <baseDN> -sh <supplierhostname> -ch <consumerhostname> [options]
```

ili

```
ldapdiff -S  -sh <supplierhostname> -ch <consumerhostname> [options]
```

Dijagnostika

Status izlaza je 0 ako se ne jave greške. Greške rezultiraju izlaznim statusom različitim od nule i dijagnostičkom porukom koja se upisuje u standardnu grešku.

Srodni zadaci

"Upravljanje redovima replikacije" na stranici 155
Koristite ovu informaciju za nadgledanje statusa replikacije za svaki ugovor (red) replikacije koji koristi ovaj poslužitelj.

Srodne reference

"Pregled replikacije" na stranici 37
Preko replikacije se promjene koje su učinjene na jednom direktoriju šire na još jedan ili više dodatnih direktorija. U stvari, promjena na jednom direktoriju se pojavljuje na više različitih direktorija.

Upotreba SSL-a s pomoćnim programima LDAP reda za naredbe

Koristite ovu informaciju kako biste razumjeli kako koristiti SSL s pomoćnim programima LDAP reda za naredbe.

"Sloj sigurnih utičnica (SSL) i Sigurnost razine prijenosa (TLS) s Poslužiteljem direktorija" na stranici 51 raspravlja upotrebu SSL s Directory Server LDAP poslužiteljem. Ove informacije uključuju upravljanje i kreiranje povjerljivih Izdavača certifikata s Upraviteljem digitalnih certifikata.

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

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

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

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

- Definirajte jedan ili više pouzdanih glavnih certifikata u spremištu certifikata. Time se klijent uvjerava da je ciljnom LDAP poslužitelju certifikat izdao pouzdani izdavač certifikata (CA). Uz to, sve LDAP transakcije s poslužiteljem

koje teku preko SSL veze su šifrirane. To obuhvaća i LDAP vjerodajnice koje isporučuje neko aplikativno programsko sučelje (API) koje se koristi za povezivanje na poslužitelj direktorija.

- Kreirajte par ključeva i zatražite klijentov certifikat od nekog izdavača certifikata (CA). Nakon što primite potpisani certifikat od izdavača, primite ga i u datoteku prstenova ključeva na klijentu.

Srodni koncepti

"Sloj sigurnih utičnica (SSL) i Sigurnost razine prijenosa (TLS) s Poslužiteljem direktorija" na stranici 51
Da bi komunikacija s Directory Server-om bila još sigurnija, Directory Server mora koristiti sigurnost Sloja sigurnih utičnica (SSL) i Sigurnost sloja transporta (TLS).

LDAP format razmjene podataka (LDIF)

LDAP format razmjene podataka je standardni tekstualni format za prikazivanje LDAP objekata i LDAP ažuriranja (dodaj, modificiraj, obriši, modificiraj DN) u tekstualnom obliku. Datoteke koje sadrže LDIF slogove mogu se koristiti za prijenos podataka između directory servera ili kao ulaz LDAP alatima poput **ldapadd** i **ldapmodify**.

LDIF slogovi sadržaja koriste se za prikazivanje LDAP sadržaja direktorija i sastoje se od linije koja identificira objekt, te linija koje sadrže parove vrijednosti atributa za objekt. Taj tip datoteke koristi **ldapadd** Qshell pomoćni program kao i alati za importiranje i eksportiranje direktorija u System i Navigator i CPYFRMLDIF (LDIF2DB) i CPYTOLDIF (DB2LDIF) CL naredbe.

Bilješka: Preporuča se izvođenje DB2LDIF naredbe u samostalnom poslu.

LDIF slogovi promjene se koriste za prikazivanje ažuriranja direktorija. Ti se slogovi sastoje od linije koja identificira objekt direktorija, te linija koje opisuju promjene na objektu. Promjene uključuju dodavanje, brisanje, preimenovanje ili premještanje objekata kao i modificiranje postojećih objekata.

Postoje dva stila ulaza za oba ta sloga: standardni LDIF stil definiran pomoću RFC 2849: LDAP format razmjene podataka (LDIF) - Tehnička specifikacija; i stariji stil ne-standardnog modificiranja. Preporuča se upotreba standardnog LDIF stila; stariji se stil ovdje dokumentira za upotrebu sa starijim alatima koji proizvode ili koriste taj stil.

Stilovi ulaza

ldapmodify i **ldapadd** Qshell pomoćni programi prihvaćaju dva obrasca ulaza. Tip ulaza se određuje formatom prve linije ulaza dobavljene u **ldapmodify** ili **ldapadd**.

Prva linija ulaza u ldapmodify ili ldapadd naredbu mora naznačiti razlikovno ime unosa direktorija za dodavanje ili modificiranje. Ta linija ulaza mora biti sljedećeg oblika:

```
dn: distinguished_name
```

ili

```
distinguished_name
```

gdje jrdn: slovni niz, a distinguished_name je razlikovno ime unosa direktorija za modificiranje (ili dodavanje). Ako je dn: nađen, stil ulaza je postavljen na RFC 2849 LDIF stil. Ako nije nađen, stil ulaza je postavljen na postaviti modificiranja.

Bilješka:

1. Naredba **ldapadd** ekvivalentna je dozivanju naredbe **ldapmodify -a**.
2. **ldapmodify** i **ldapadd** pomoćni programi ne podržavaju base64 kodirana razlikovna imena.

Srodne reference

"ldapmodify i ldapadd" na stranici 205
Pomoćni programi reda za naredbe LDAP modificiraj-unos i LDAP dodaj-unos.

"ldapsearch" na stranici 222
Pomoćni programi reda za naredbe LDAP pretraživanja.

RFC 2849 LDIF ulaz

Standardni LDIF stil definiran pomoću RFC 2849: LDAP format razmjene podataka (LDIF) se preporuča. LDIF datoteka može se pokrenuti s opcijskim direktivama verzije i skupa znakova : verzija: 1 i skup znakova: ISO-8859-1.

Direktiva skupa znakova je korisna kod upotrebe sistem datoteka na drugim platformama koje ne podržavaju označavanje datoteke s CCSID-om. Na i5/OS, standardno ponašanje je otvoriti LDIF datoteke u UTF-8 (CCSID 1208) i dozvoliti sistem datotekama da konvertiraju podatke iz CCSID-a datoteke u UTF-8, a direktiva skupa znakova uobičajeno nije potrebna.

Nakon opcijskih linija verzije i skupa znakova slijedi serija slogova promjena kako je niže u tekstu opisano.

Kod upotrebe RFC 2849 LDIF unosa, tipovi atributa i vrijednosti su delimitirani jednostrukom dvotočkom (:) ili dvostrukom dvotočkom (::). Nadalje, pojedinačne promjene u vrijednostima atributa su delimitirane s linijom unosa changetype:. Općeniti oblik linija ulaza za RFC 2849 LDIF jest:

```
change_record
<blank line>
change_record
<blank line>
.
.
.
```

Datoteka ulaza u stilu RFC 2849 LDIF sastoji se od jednog ili više change_record skupova linija koje su odijeljene pojedinačnom praznom linijom. Svaki change_record ima sljedeći oblik:

```
dn: <distinguished name>
[changetype: {modify|add|modrdn|moddn|delete}]
change_clause
change_clause
.
.
.
```

Stoga, change_record sastoji se od linije koja pokazuje razlikovno ime unosa direktorija koje se treba modificirati, opcijske linije koja pokazuje tip modifikacije koja se treba izvesti nasuprot unosu direktorija te jedan ili više change_clause skupova linija. Ako je changetype: linija izostavljena, pretpostavlja se da je tip promjene modificiraj osim ako dozivanje naredbe nije bilo ldapmodify -a ili ldapadd, tada se pretpostavlja da je changetype dodaj.

Kad je tip promjene modificiraj, svaka change_clause je definirana kao skup linija oblika:

```
dodati: {attrtype}
{attrtype}{sep}{value}
.
.
.
-
```

ili

```
zamijeniti: {attrtype}
{attrtype}{sep}{value}
.
.
.
-
```

ili

```
brisati: {attrtype}
[{attrtype}{sep}{value}]
.
.
.
-
```

ili

```
{attrtype}{sep}{value}
.
.
.
```

Specificiranjem zamijeni zamjenjuje sve postojeće vrijednosti za atribut sa specificiranim skupom atributa. Specificiranjem dodaj dodaje postojećem skupu vrijednosti atributa. Specificiranjem briši bez ijednog sloga para atribut-vrijednost uklanja sve ukloniti vrijednosti za specificirani atribut. Specificiranjem briši, nakon čega slijedi jedan ili više slogova para atribut-vrijednost, uklanja samo one vrijednosti specificirane u slogovima para atribut-vrijednost.

Ako ijedna od linija dodaj: *attrtype*, zamijeni: *attrtype* ili obriši: *attrtype* (indikator promjene) je specificirana, linija koja sadrži crticu (-) očekuje se zatvarajući odjelitelj za promjene za tu *attrtype*. Parovi atribut-vrijednost su očekivani na ulaznim linijama koje se nalaze između indikatora promjene i linije s crticom. Ako je changetype linija izostavljena, pretpostavlja se da je changetype dodaj za ldapadd i zamijeni za ldapmodify.

Vrijednost atribut može se specificirati kao tekstualni niz, bazna-64 šifrirana vrijednost ili URL datoteke u skladu s odjeliteljem *sep*, se koriste.

attrtype: vrijednost
: jednostruka dvotočka (:) specificira da je vrijednost niz *vrijednost*.

attrtype:: base64string
: dvostruka dvotočka (: :) specificira da *base64string* predstavlja bazni 64 šifrirani niz binarne vrijednosti ili UTF-8 niz koji sadrži višebitne znakove.

attrtype:< fileURL
: dvotočka i lijeva zagrada (:<) specificira da se vrijednost mora čitati iz datoteke koju identificira fileURL. Primjer linije URL datoteke koja specificira da je vrijednost za jpegPhoto atribut u datoteci /tmp/photo.jpg je

  jpegphoto:< datoteka:///tmp/photo.jpg

Svi razmaknuti znakovi između odjelitelja i vrijednosti atributa se zanemaruju. Vrijednosti atributa mogu se nastaviti kroz višestruke linije pomoću jednostrukog znaka praznog mjesta kao prvi znak sljedeće linije ulaza. Ako se koristi dvostruka dvotočka kao odjelitelj, očekuje se da je ulaz u base64 formatu. Taj je format kodiranje koje prikazuje svaka tri binarna bajta s četiri tekstualna znaka.

Višestruke vrijednosti atributa su specificirane pomoću višestrukih {attrtype}{sep}{value} specifikacija.

Kad je tip promjene dodaj, svaka change_clause se definira kao skup linija oblika:

```
{attrtype}{sep}{value}
```

Kao s tipom promjene modificiraj, odjelitelj, sep i vrijednost mogu biti jednostruka dvotočka (:), dvostruka dvotočka (: :) ili dvotočka i lijeva zagrada (:<). Svi razmaknuti znakovi između odjelitelja i vrijednosti atributa se zanemaruju. Vrijednosti atributa mogu se nastaviti kroz višestruke linije pomoću jednostrukog znaka praznog mjesta kao prvi znak sljedeće linije ulaza. Ako se koristi dvostruka dvotočka kao odjelitelj, očekuje se da je ulaz u base64 formatu.

Kad je tip promjene modrdn ili moddn, svaka change_clause je definirana kao skup linija oblika:

```
newrdn: vrijednost
deleteoldrdn:{0|1}
[newsuperior: newSuperiorDn]
```

To su parametri koje možete specificirati na operaciji modificiraj RDN (preimenovati) modifyDN (premjestiti) LDAP. Vrijednost za newrdn postavku je nova RDN koja se mora koristiti kod izvođenja operacije modificiraj RDN. Specificirajte 0 za vrijednost deleteoldrdn postavke kako biste spremili atribut u stari RDN i specificirajte 1 za uklanjanje vrijednosti atributa u starom RDN. Vrijednost za newsuperior postavku je DN novog superiornog (nadređenog) kod premještanje unosa.

Kad je tip promjene briši, nije specificirana nikakva change_clause.

Primjeri LDIF stilova:

Ovo poglavlje osigurava primjere važećeg ulaza za **ldapmodify** naredbu pomoću RFC 2849 LDIF stila.

Dodavanje novog unosa

Sljedeći primjer dodaje novi unos u direktorij pomoću imena cn=Tim Doe, ou=Your Department, o=Your Company, c=US, pretpostavljajući da je **ldapadd** ili **ldapmodify -a** dozvan:

```
dn:cn=Tim Doe, ou=Your Department, o=Your Company, c=US
changetype:add
cn: Tim Doe
sn: Doe
objectclass: organizationalperson
objectclass: osoba
objectclass: top
```

Sljedeći primjer dodaje novi unos u direktorij pomoću imena cn=Tim Doe, ou=Your Department, o=Your Company, c=US, pretpostavljajući da je **ldapadd** ili **ldapmodify -a** dozvan. Primijetite da se jpegphoto atribut učitava iz datoteke /tmp/timdoe.jpg.

```
dn:cn=Tim Doe, ou=Your Department, o=Your Company, c=US
changetype:add
cn: Tim Doe
sn: Doe
jpegphoto:< file:///tmp/timdoe.jpg
objectclass: inetorgperson
objectclass: organizationalperson
objectclass: osoba
objectclass: top
```

Dodavanje tipova atributa

Sljedeći primjer dodaje dva nova tipa atributa u postojeći unos. Primijetite da su registeredaddress atributu dodane dvije vrijednosti:

```
dn:cn=Tim Doe, ou=Your Department, o=Your Company, c=US
changetype: modify
add:telephonenumber
telephonenumber: 888 555 1234
-
add: registeredaddress
registeredaddress: td@yourcompany.com
registeredaddress: ttd@yourcompany.com
```

Promjena imena unosa

Sljedeći primjer mijenja ime postojećeg unosa u cn=Tim Tom Doe, ou=Your Department, o=Your Company, c=US. Stari RDN, cn=Tim Doe, zadržava se kao dodatna vrijednost atributa cn atributa. Novi RDN, cn=Tim Tom Doe, automatski dodaje LDAP poslužitelj vrijednostima cn atributnew u unosu:

```
dn: cn=Tim Doe, ou=Your Department, o=Your Company, c=US
changetype:modrdn
newrdn: cn=Tim Tom Doe
deleteoldrdn: 0
```

Sljedeći primjer premješta cn=Tim Doe u ou=New Department; theRDN (cn=Tim Doe) se ne mijenja.

```
dn: cn=Tim Doe, ou=Your Department, o=Your Company, c=US
changetype:moddn
newrdn: cn=Tim Doe
deleteoldrdn: 0
newsuperior: ou=New Department, o=Your Company, c=US
```

Zamjena vrijednosti atributa

Sljedeći primjer zamjenjuje vrijednosti atributa za telephonenumber i registeredaddress atribute sa specificiranim vrijednostima atributa.

```
dn: cn=Tim Tom Doe, ou=Your Department, o=Your Company, c=US
changetype: modify
replace: telephonenumber
telephonenumber: 888 555 4321
-
replace: registeredaddress
registeredaddress: tim@yourcompany.com
registeredaddress: timtd@yourcompany.com
```

Brisanje i dodavanje atributa

Sljedeći primjer briše telephonenumber atribut, briše pojedinačna registeredaddress vrijednost atributa i dodaje description atribut:

```
dn:cn=Tim Tom Doe, ou=Your Department, o=Your Company, c=US
changetype: modify
add: description
description: Ovo je vrlo duga vrijednost
 atributa koja se nastavlja na sljedećoj liniji.
 Primijetite prored na početku
 nastavljenih linija kako bi se označilo da
 se linija nastavlja.
-
delete: telephonenumber
-
delete: registeredaddress
registeredaddress: tim@yourcompany.com
```

Brisanje unosa

Sljedeći primjer briše unos direktorija s imenom cn=Tim Tom Doe, ou=Your Department, o=Your Company, c=US:

```
dn:cn=Tim Tom Doe, ou=Your Department, o=Your Company, c=US
changetype:delete
```

Modificiraj LDIF ulaz stila

Stariji nestandardni stil modificiranje ulaza za **ldapmodify** ili **ldapadd** naredbe nije fleksibilan poput RFC 2849 LDIF stila. Međutim, katkada ga je lakše koristiti od LDIF stila.

Kod upotrebe ulaza stila modificiranja, tipovi i vrijednosti atribut su razgraničeni znakom jednakosti (=). Općeniti oblik linija ulaza za stil modificiranja jest:

```
change_record
<blank line>
change_record
<blank line>
.
.
.
```

Datoteka ulaza u stilu modificiranja sastoji se od jednog ili više *change_record* skupova linija koje su odijeljene pojedinačnom praznom linijom. Svaki *change_record* ima sljedeći oblik:

```
distinguished_name
[+|-]{attrtype} = {value_line1[\
value_line2[\
...value_lineN]]}
.
.
.
```

Stoga, *change_record* sastoji se od linije koja pokazuje razlikovno ime unosa direktorija koje se treba modificirati zajedno s jednom ili više linija modifikacije atributa. Svaka linija modifikacije atributa se sastoji od opcijskog indikatora dodaj ili obriši (+ ili -), tipa atributa i vrijednosti atributa. Ako je znak plus (+) specificiran, tip modifikacije je postavljen na **dodaj**. Ako je specificirana crtica (-), tip modifikacije je postavljen na briši. Za modifikaciju brisanja, znak jednakosti (=) i *vrijednost* trebali bi biti izostavljeni kako bi se uklonio cijeli atribut. Ako nije specificiran indikator dodaj ili obriši, tip modifikacije je postavljen na dodaj osim ako se koristi -r osim ako i u tom slučaju je tip modifikacije postavljen na zamijeni. Svaki znak vodećeg ili zadnjeg praznog mjesta uklanja se iz vrijednosti atributa. Ako su znakovi zadnjeg praznog mjesta potrebni za vrijednosti atributa, RFC 2849 LDIF stil ulaza se mora koristiti. Linije su nastavljene pomoću obrnute kose crte (\) kao posljednji znak linije. Ako je linija nastavljena, znak obrnute kose crte se uklanja, a sljedeća linija se pridodaje izravno nakon znaka koji prethodi znaku obrnute kose crte. Znak nove linije pri kraju linije ulaza nije zadržan kao dio vrijednosti atributa.

Višestruke vrijednosti atributa su specificirane pomoću višestrukih *attrtype=value* specifikacija.

Ako su pomoćne binarne vrijednosti opcije datoteka (-b) specificirane, *vrijednost* koja započinje s '/' pokazuje da je vrijednost ime datoteke. Na primjer, sljedeća linija pokazuje da se jpegphoto atribut mora čitati iz datoteke /tmp/photo.jpg:

jpegphoto=/tmp/photo.jpg

Modificiraj primjere stila:

Ovo poglavlje osigurava primjere važećeg ulaza za **ldapmodify** naredbu pomoću stila modificiranja.

Dodavanje novog unosa

Sljedeći primjer dodaje novi unos u direktorij pomoću imena cn=Tim Doe, ou=Your Department, o=Your Company, c=US:

```
cn=Tim Doe, ou=Your Department, o=Your Company, c=US
cn=Tim Doe
sn=Doe
objectclass=organizationalperson
objectclass=person
objectclass=top
```

Dodavanje novog tipa atributa

Sljedeći primjer dodaje dva nova tipa atributa u postojeći unos. Primijetite da su registeredaddress atributu dodane dvije vrijednosti:

```
cn=Tim Doe, ou=Your Department, o=Your Company, c=US
+telephonenumber=888 555 1234
+registeredaddress=td@yourcompany.com
+registeredaddress=ttd@yourcompany.com
```

Zamjena vrijednosti atributa

Pretpostavljajući da je dozivanje naredbe bilo:

```
ldapmodify -r ...
```

Sljedeći primjer zamjenjuje vrijednosti atributa za telephonenumber i registeredaddress atribute sa specificiranim vrijednostima atributa. Ako **-r** opcija red za naredbe nije bila specificirana, vrijednosti atributa se dodaju u postojeći skup vrijednosti atributa.

```
cn=Tim Doe, ou=Your Department, o=Your Company, c=US
telephonenumber=888 555 4321
registeredaddress: tim@yourcompany.com
registeredaddress: timtd@yourcompany.com
```

Brisanje tipa atributa

Sljedeći primjer briše pojedinačnu registeredaddress vrijednost atributa iz postojećeg unosa.

```
cn=Tim Doe, ou=Your Department, o=Your Company, c=US
-registeredaddress=tim@yourcompany.com
```

Dodavanje atributa

Sljedeći primjer dodaje opis atribut. opis vrijednost atributa obuhvaća višestruke linije:

```
cn=Tim Doe, ou=Your Department, o=Your Company, c=US
+description=Ovo je vrlo duga vrijednost \
 atributa koja se nastavlja na sljedečoj liniji. \
Primijetite obrnutu kosu crtu na kraju linije koja se \
mora nastaviti kako bi se označio \
nastavak linije.
```

Shema konfiguracije Poslužitelja direktorija

Ove informacije opisuju Stablo informacija direktorija (DIT) i atribute koji se koriste za konfiguriranje ibmslapd.conf datoteke.

U prijašnjim izdanjima, konfiguracijske postavke direktorija su bile pohranjene u vlasničkom formatu u konfiguracijskoj datoteci. Postavke direktorija su sada pohranjene korištenjem LDIF formata u datoteci konfiguracije.

Datoteka konfiguracije se naziva ibmslapd.conf. Sada je dostupna i shema koju koristi datoteka konfiguracije. Tipovi atributa se mogu pronaći u v3.config.at datoteci, a klase objekta se nalaze u v3.config.oc datoteci. Atributi se mogu preinačiti korištenjem ldapmodify naredbe.

Srodni koncepti

“Provjera sheme” na stranici 30
Kada se inicijalizira poslužitelj, čitaju se datoteke sheme i provjerava se njihova konzistentnost i ispravnost.

Srodne reference

“ldapmodify i ldapadd” na stranici 205
Pomoćni programi reda za naredbe LDAP modificiraj-unos i LDAP dodaj-unos.

Stablo informacija direktorija

Ova informacija opisuje stablo informacija direktorija Directory Servera (DIT).

cn=Configuration

- cn=Admin
- cn=Event Notification
- cn=Front End
- cn=Kerberos
- cn=Master Server
- cn=Referral
- cn=Schema
  - cn=IBM Directory

- cn=Config Backends
  - cn=ConfigDB
- cn=RDBM Backends
  - cn=Directory
  - cn=ChangeLog
- cn=LDCF Backends
  - cn=SchemaDB

- cn=SSL
  - cn=CRL
- cn=Transaction

cn=Configuration

DN cn=Configuration

Opis To je unos najviše razine u DIT-u konfiguracije. Sadrži podatke koji su od globalnog interesa za poslužitelja, iako u stvari sadrži i svakovrsne stavke. Svaki atribut u tom unosu dolazi iz prve sekcije (globalna strofa) od ibmslapd.conf.

Broj 1 (potrebno)

Klasa objekta
ibm-slapdTop

Obvezni atributi

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

Neobvezni atributi

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (Depricirano)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion

cn=Admin

DN cn=Admin, cn=Configuration

Opis Globalne konfiguracijske postavke za IBM Admin Daemona

Broj 1 (potrebno)

Klasa objekta
ibm-slapdAdmin

Obvezni atributi

- cn
- ibm-slapdErrorLog
- ibm-slapdPort

Neobvezni atributi

- ibm-slapdSecurePort

cn=Event Notification

DN cn=Event Notification, cn=Configuration

Opis Globalne postavke obavještavanja o događaju za Poslužitelj direktorija

Broj 0 ili 1 (neobvezno; potrebno samo ako želite omogućiti obavještavanje o događaju)

Klasa objekta
ibm-slapdEventNotification

Obvezni atributi

- cn
- ibm-slapdEnableEventNotification
- objectClass

Neobvezni atributi

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

cn=Front End

DN cn=Front End, cn=Configuration

Opis Globalne postavke okoline koje poslužitelj primjenjuje kod pokretanja.

Broj 0 ili 1 (neobvezno)

Klasa objekta
ibm-slapdFrontEnd

Obvezni atributi

- cn
- objectClass

Neobvezni atributi

- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdDB2CP
- ibm-slapdEntryCacheSize
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdPlugin
- ibm-slapdSetenv
- ibm-slapdIdleTimeOut

cn=Kerberos

DN cn=Kerberos, cn=Configuration

Opis Globalne postavke Kerberos provjere autentičnosti za Poslužitelj direktorija.

Broj 0 ili 1 (neobvezno)

Klasa objekta
ibm-slapdKerberos

Obvezni atributi

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

Neobvezni atributi

- nijedan

cn=Master Server

DN cn=Master Server, cn=Configuration

Opis Kada konfigurirate repliku, taj unos sadrži vjerodajnice vezanja i referal URL glavnog poslužitelja.

Broj 0 ili 1 (neobvezno)

Klasa objekta
ibm-slapdReplication

Obvezni atributi

- cn
- ibm-slapdMasterPW (Obvezno ako se ne koristi Kerberos provjera autentičnosti.)

Neobvezni atributi

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Neobvezno ako se koristi Kerberos provjera autentičnosti.)
- ibm-slapdMasterReferral
- objectClass

cn=Referral

DN cn=Referral, cn=Configuration

Opis Taj unos sadrži sve unose referala iz prve sekcije (globalna strofa) od ibmslapd.conf. Ako ne postoje referali (po defaultu ne postoji nijedan), taj unos je neobvezan.

Broj 0 ili 1 (neobvezno)

Klasa objekta
ibm-slapdReferral

Obvezni atributi

- cn
- ibm-slapdReferral
- objectClass

Neobvezni atributi

- nijedan

cn=Schemas

DN cn=Schemas, cn=Configuration

Opis Taj unos služi kao spremnik za sheme. Taj unos nije stvarno potreban jer se sheme mogu razlikovati na temelju klase objekta ibm-slapdSchema. On je uključen kako bi se poboljšala čitljivost DIT-a.

Trenutno je dozvoljen samo jedan unos sheme: cn=IBM Directory.

Broj 1 (potrebno)

Klasa objekta
Spremnik

Obvezni atributi

- cn
- objectClass

Neobvezni atributi

- nijedan

cn=IBM Directory

DN cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Taj unos sadrži sve podatke konfiguracije sheme iz prve sekcije (globalna strofa) od ibmslapd.conf. Služi i kao spremnik za sve pozadine koje koriste shemu. Višestruke sheme nisu trenutno podržane, ali da jesu, onda bi postojao samo jedan ibm-slapdSchema unos po shemi. Primijetite da se smatra da su višestruke sheme nekompatibilne. Stoga se pozadina može pridružiti samo jednoj shemi.

Broj 1 (potrebno)

Klasa objekta
ibm-slapdSchema

Obvezni atributi

- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

Neobvezni atributi

- ibm-slapdSchemaAdditions

cn=Config Backends

DN cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Taj unos služi kao spremnik za Config pozadine.

Broj 1 (potrebno)

Klasa objekta
Spremnik

Obvezni atributi

- cn
- objectClass

Neobvezni atributi
nijedan

cn=ConfigDB

DN cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Konfiguracijska pozadina za konfiguraciju IBM poslužitelja direktorija

Broj 0 - n (neobvezno)

Klasa objekta
ibm-slapdConfigBackend

Obvezni atributi

- ibm-slapdSuffix
- ibm-slapdPlugin

Neobvezni atributi

- ibm-slapdReadOnly

cn=RDBM Backends

DN cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Ovaj unos služi kao spremnik za RDBM pozadine. To učinkovito zamjenjuje rdbm liniju baze podataka iz ibmslapd.conf identificiranjem svih pod-unosa kao DB2 pozadina. Taj unos nije stvarno potreban jer se RDBM pozadine mogu razlikovati pomoću klase objekta ibm-slapdRdbmBackend. On je uključen kako bi se poboljšala čitljivost DIT-a.

Broj 0 ili 1 (neobvezno)

Klasa objekta
Spremnik

Obvezni atributi

- cn
- objectClass

Neobvezni atributi

- nijedan

cn=Directory

DN cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Taj unos sadrži sve postavke konfiguracije baze podataka za default pozadinu RDBM baze podataka.

Iako višestruke pozadine s proizvoljnim imenima mogu biti kreirane, Administracija poslužitelja pretpostavlja da je ″cn=Directory″ glavna pozadina direktorija i da je ″cn=ChangeLog″ opcijska pozadina dnevnika promjena. Samo su nastavci prikazani u ″cn=Directory″ konfigurabilni kroz Administraciju poslužitelja (osim nastavaka dnevnika promjena, koji je postavljen transparentno omogućavanjem dnevnika promjena).

Broj 0 - n (neobvezno)

Klasa objekta
ibm-slapdRdbmBackend

Obvezni atributi

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName

- ibm-slapdDbUserID
- objectClass

Neobvezni atributi

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Bilješka: Ako koristite **ibm-slapdUseProcessIdPw**, morate promijeniti shemu da napravite **ibm-slapdDbUserPW** neobveznim.

cn=Change Log

DN cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Taj unos sadrži sve postavke konfiguracije baze podataka za pozadinu dnevnika promjena.

Broj 0 - n (neobvezno)

Klasa objekta
ibm-slapdRdbmBackend

Obvezni atributi

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Neobvezni atributi

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin

- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Bilješka: Ako koristite **ibm-slapdUseProcessIdPw**, morate promijeniti shemu da napravite **ibm-slapdDbUserPW** neobveznim.

cn=LDCF Backends

DN cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Taj unos služi kao spremnik za LDCF pozadinu. On učinkovito zamjenjuje ldcf liniju baze podataka iz ibmslapd.conf identificiranjem svih pod unosa kao LDCF pozadine. Taj unos nije stvarno potreban jer se LDCF pozadine mogu razlikovati pomoću ibm-slapdLdcfBackend klase objekta. On je uključen kako bi se poboljšala čitljivost DIT-a.

Broj 1 (potrebno)

Klasa objekta
Spremnik

Obvezni atributi

- cn
- objectClass

Neobvezni atributi

- ibm-slapdPlugin

cn=SchemaDB

DN cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Taj unos sadrži sve podatke konfiguracije baze podataka iz sekcije ldcf baze podataka ibmslapd.conf.

Broj 1 (potrebno)

Klasa objekta
ibm-slapdLdcfBackend

Obvezni atributi

- cn
- objectClass

Neobvezni atributi

- ibm-slapdPlugin
- ibm-slapdSuffix

cn=SSL

DN cn=SSL, cn=Configuration

Opis Globalne postavke SSL povezivanja za Poslužitelj direktorija.

Broj 0 ili 1 (neobvezno)

Klasa objekta
ibm-slapdSSL

Obvezni atributi

- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

Neobvezni atributi

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

  Bilješka: **ibm-slapdSslCipherSpecs** je sada uklonjen. Umjesto toga koristite **ibm-slapdSslCipherSpec**. Ako koristite **ibm-slapdSslCipherSpecs**, poslužitelj će se konvertirati na podržane atribute.
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW

cn=CRL

DN cn=CRL, cn=SSL, cn=Configuration

Opis Ovaj unos sadrži podatke popisa opoziva certifikata iz prve sekcije (globalna strofa) od ibmslapd.conf. To je potrebno samo ako je ″ibm-slapdSslAuth = serverclientauth″ u cn=SSL unosu, a certifikati klijenta su bili izdani za CRL provjeru valjanosti.

Broj 0 ili 1 (neobvezno)

Klasa objekta
ibm-slapdCRL

Obvezni atributi

- cn
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPort
- objectClass

Neobvezni atributi

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword

cn=Transaction

DN cn = Transaction, cn = Configuration

Opis Specificira globalne postavke podrške transakcije. Podrška transakcije je osigurana korištenjem plugin-a:

```
extendedop /QSYS.LIB/QGLDTRANEX.SRVPGM tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

Poslužitelj (**slapd**) automatski učitava taj plug-in kod pokretanja ako vrijedi **ibm-slapdTransactionEnable = TRUE**. Plug-in ne treba biti izričito dodan na **ibmslapd.conf**.

Broj 0 ili 1 (neobvezno; potrebno samo ako želite koristiti transakcije.)

Klasa objekta
ibm-slapdTransaction

Obvezni atributi

- cn
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

Neobvezni atributi

- nijedan

Atributi

Ova informacija opisuje atribute Directory Servera koji se koriste za konfiguriranje ibmslapd.conf datoteke.

- cn
- ibm-slapdACIMechanism
- ibm-slapdACLAccess
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN
- ibm-slapdAdminGroupEnabled
- ibm-slapdAdminPW
- ibm-slapdAllowAnon
- ibm-slapdAllReapingThreshold
- ibm-slapdAnonReapingThreshold
- ibm-slapdBoundReapingThreshold
- ibm-slapdBulkloadErrors
- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeAutoAdjust
- ibm-slapdCachedAttributeAutoAdjustTime
- ibm-slapdCachedAttributeAutoAdjustTimeInterval
- ibm-slapdCachedAttributeSize
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConcurrentRW
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdDerefAliases
- ibm-slapdDigestAdminUser
- ibm-slapdDigestAttr
- ibm-slapdDigestRealm
- ibm-slapdEnableEventNotification

- ibm-slapdEntryCacheSize
- ibm-slapdErrorLog
- ibm-slapdESizeThreshold
- ibm-slapdEThreadActivate
- ibm-slapdEThreadEnable
- ibm-slapdETimeThreshold
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- ibm-slapdLanguageTagsEnabled
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword
- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdMasterDN
- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplDbConns
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerId
- ibm-slapdSetenv

- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSuffix
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTransactionEnable
- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- ibm-slapdWriteTimeout
- objectClass

cn

Opis Ovo je X.500 commonName atribut koji sadrži ime objekta.

Sintaksa
Niz direktorija

Maksimalna dužina
256

Vrijednost
Više-vrijednosti

ibm-slapdACIMechanism

Opis Određuje kojeg ACL modela koristi poslužitelj. (Podržano samo na i5/OS i OS/400 od v3.2, zanemareno na drugim platformama.)

- 1.3.18.0.2.26.1 = IBM SecureWay v3.1 ACL model
- 1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL model

Default
1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL model

Sintaksa
Niz direktorija

Maksimalna dužina
256

Vrijednost
Više-vrijednosti.

ibm-slapdACLAccess

Opis Kontrolira da li je omogućen pristup na ACL-ove. Ako je postavljeno na TRUE, omogućen je pristup na ACL-ove. Ako je postavljeno na FALSE, onemogućen je pristup na ACL-ove.

Default
TRUE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdACLCache

Opis Kontrolira da li ili ne poslužitelj stavlja u predmemoriju ACL informacije.

- Ako je postavljeno na TRUE, poslužitelj stavlja ACL informacije u predmemoriju.
- Ako je postavljeno na FALSE, poslužitelj ne stavlja ACL informacije u predmemoriju.

Default
TRUE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdACLCacheSize

Opis Maksimalan broj unosa koji će se sačuvati u ACL predmemoriji.

Default
25000

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdAdminDN

Opis DN vezanja administratora za Poslužitelj direktorija.

Default
cn=root

Sintaksa
DN

Maksimalna dužina
Neograničena

Vrijednost
Jedna-vrijednost

ibm-slapdAdminGroupEnabled

Opis Navodi da li je Administrativna grupa trenutno omogućena. Ako je postavljeno na TRUE, poslužitelj će dozvoliti korisnicima u administrativnoj grupi da se prijave.

Default
FALSE

Sintaksa
Booleov

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdAdminPW

Opis Lozinka vezanja administratora za Poslužitelja direktorija.

Default
tajna

Sintaksa
Binarno

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdAllowAnon

Opis Navodi da li su dozvoljena anonimna vezanja.

Default
Istinito

Sintaksa
Booleov

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdAllReapingThreshold

Opis Navodi broj veza koje treba održavati u poslužitelju prije nego što je aktivirano upravljanje vezama.

Default
1200

Sintaksa
Niz znakova direktorija s uparivanjem osjetljivim na velika slova.

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdAnonReapingThreshold

Opis Navodi broj veza koje treba održavati u poslužitelju prije nego što je aktivirano upravljanje anonimnim vezama.

Default
0

Sintaksa
Niz znakova direktorija s uparivanjem osjetljivim na velika slova.

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdBoundReapingThreshold

Opis Navodi broj veza koje treba održavati u poslužitelju prije nego što je aktivirano upravljanje anonimnim i vezanim vezama.

Default
1100

Sintaksa
Niz znakova direktorija s uparivanjem osjetljivim na velika slova.

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdBulkloadErrors

Opis Staza datoteke ili uređaj na ibmslapd host stroju na koje će se zapisati bulkload poruke o greški.

Default
/var/bulkload.log

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdCachedAttribute

Opis Sadrži imena atributa koja trebaju biti stavljena u predmemoriju atributa, jedno ime atributa po vrijednosti.

Default
nijedan

Sintaksa
Niz direktorija

Maksimalna dužina
256

Vrijednost
Više-vrijednosti

ibm-slapdCachedAttributeAutoAdjust

Opis Kontrolira da li će poslužitelj automatski prilagoditi predmemoriju atributa u konfiguriranim vremenskim intervalima definiranim u ibm-slapdCachedAttributeAutoAdjustTime i ibm-slapdCachedAttributeAutoAdjustTimeInterval.

Default
FALSE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdCachedAttributeAutoAdjustTime

Opis Kada je ibm-slapdCachedAttributeAutoAdjust postavljen na TRUE, kontrolira vrijeme u kojem poslužitelj počinje prilagođavati predmemoriju atributa automatski.

```
Minimum = T000000
Maksimum = T235959
```

Default
T000000

Sintaksa
Vojničko vrijeme

Maksimalna dužina
7

Vrijednost
Jedna-vrijednost

ibm-slapdCachedAttributeAutoAdjustTimeInterval

Opis Kada je ibm-slapdCachedAttributeAutoAdjust postavljen na TRUE, kontrolira vremenske intervale između automatske prilagodbe predmemorije atributa.

```
Minimum = 1
Maksimum = 24
```

Default
2

Sintaksa
Cijeli broj

Maksimalna dužina
2

Vrijednost
Jedna-vrijednost

ibm-slapdCachedAttributeSize

Opis Količina memorije, u bajtovima, koja može biti korištena od strane predmemorije atributa. Vrijednost 0 označava da se neće koristiti predmemorija atributa.

Default
0

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna vrijednost.

ibm-slapdChangeLogMaxEntries

Opis Ovaj atribut se koristi od strane plug-ina dnevnika promjena za navođenje maksimalnog broja unosa dnevnika promjena dozvoljenih u RDBM bazi podataka. Svaki dnevnik promjena ima svoj vlastiti changeLogMaxEntries atribut.

```
Minimum = 0 (neograničeno)
Maksimum = 2,147,483,647 (32-bit, cijeli broj s predznakom)
```

Default
0

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdCLIErrors

Opis Staza datoteke ili uređaj na ibmslapd host stroju na koje će se zapisati CLI poruke o greški.

Default
/var/db2cli.log

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdConcurrentRW

Opis Postavljanjem toga na TRUE se omogućava da se pretraživanja nastave istodobno s ažuriranjima. To omogućava 'prljava čitanja', odnosno, rezultate koji možda neće biti konzistentni s predanim stanjem baze podataka.

Upozorenje: Taj atribut se depricira.

Default
FALSE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdDB2CP

Opis Specificira kodnu stranicu baze podataka direktorija. 1208 je kodna stranica za UTF-8 baze podataka.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdDBAlias

Opis Alias DB2 baze podataka.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
8

Vrijednost
Jedna-vrijednost

ibm-slapdDbConnections

Opis Navodi broj DB2 veza koje će poslužitelj namijeniti za DB2 pozadinu. Vrijednost mora biti između 5 i 50 (uključno).

Bilješka: ODBCCONS varijabla okoline nadjačava vrijednost te direktive.
Ako je ibm-slapdDbConnections (ili ODBCCONS) manji od 5 ili veći od 50, poslužitelj će koristiti 5 ili 50. 1 dodatna veza će biti kreirana za replikaciju (čak i ako nije definirana replikacija). 2 dodatne veze će se kreirati za dnevnik promjena (ako je promjena omogućena).

Default
15

Sintaksa
Cijeli broj

Maksimalna dužina
50

Vrijednost
Jedna-vrijednost

ibm-slapdDbInstance

Opis Navodi instancu DB2 baze podataka za ovu pozadinu.

Default
ldapdb2

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
8

Vrijednost
Jedna-vrijednost

Bilješka: Svi ibm-slapdRdbmBackend objekti moraju koristiti iste ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW i DB2 skup znakova.

ibm-slapdDbLocation

Opis Staza datoteke sistema na kojoj je locirana baza podatka pozadine.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdDbName

Opis Navodi instancu DB2 baze podataka za ovu pozadinu.

Default
ldapdb2

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
8

Vrijednost
Jedna-vrijednost

ibm-slapdDbUserID

Opis Navodi korisničko ime s kojim se veže DB2 baza podataka za ovu pozadinu.

Default
ldapdb2

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
8

Vrijednost
Jedna-vrijednost

Bilješka: Svi ibm-slapdRdbmBackend objekti moraju koristiti iste ibm-slapdDbInstance ibm-slapdDbUserID, ibm-slapdDbUserPW i DB2 skup znakova.

ibm-slapdDerefAliases

Opis Maksimalna razina dereferenciranja na zahtjevima pretraživanja, bez obzira na bilo koje derefAliase koji su navedeni na zahtjevima klijenta. Dozvoljene vrijednosti su **nikada**, **nađi**, **pretraživanje** i **uvijek**.

Default
uvijek

Sintaksa
Niz direktorija

Maksimalna dužina
6

Vrijednost
Jedna-vrijednost

ibm-slapdDbUserPW

Opis Navodi korisničku lozinku s kojim se veže DB2 baza podataka za ovu pozadinu. Ta lozinka može biti šifriran tekst ili imask.

Default
ldapdb2

Sintaksa
Binarno

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

Bilješka: Svi ibm-slapdRdbmBackend objekti moraju koristiti iste ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW i DB2 skup znakova.

ibm-slapdDigestAdminUser

Opis Navodi Digest MD5 Korisničko ime od LDAP administratora ili člana administrativne grupe. Korišteno kada je MD5 Digest provjera autentičnosti korištena za provjeru autentičnosti administratora.

Default
nijedan

Sintaksa
Niz direktorija

Maksimalna dužina
512

Vrijednost
Jedna-vrijednost

ibm-slapdDigestAttr

Opis Nadjačava default DIGEST-MD5 username atribut. Ime atributa za korištenje za DIGEST-MD5 SASL vezanje pregledavanje username-a. Ako vrijednost nije navedena, poslužitelj koristi uid.

Default
Ako nije navedeno, poslužitelj koristi uid.

Sintaksa
Niz znakova direktorija

Maksimalna dužina
64

Vrijednost
Jedna-vrijednost

ibm-slapdDigestRealm

Opis Nadjačava default DIGEST-MD5 područje. Niz znakova koji može omogućiti korisnicima da znaju koje korisničko ime i lozinku koristiti, u slučaju da imaju različite za različite poslužitelje. Konceptualno, to je ime zbirke računa koji mogu uključivati korisničke račune. Ovaj niz treba sadržavati barem ime hosta koji izvodi

provjeru autentičnosti i može dodatno označavati zbirku korisnika koji mogu imati pristup. Primjer može biti registered_users@gotham.news.example.com. Ako atribut nije naveden, poslužitelj koristi potpuno kvalificirano ime hosta poslužitelja.

Default
Potpuno kvalificirano ime hosta poslužitelja

Sintaksa
Niz znakova direktorija

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdEnableEventNotification

Opis Specificira da li treba omogućiti Obavještavanje o događaju. Mora biti postavljeno na TRUE ili FALSE.

Ako je postavljeno na FALSE, poslužitelj odbija sve zahtjeve klijenta kako bi se registrirale obavijesti o događaju s proširenim rezultatom LDAP_UNWILLING_TO_PERFORM.

Default
TRUE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdEntryCacheSize

Opis Maksimalan broj unosa koji će se sačuvati u predmemoriji unosa.

Default
25000

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdErrorLog

Opis Specificira stazu datoteke ili uređaj na stroju Poslužitelja direktorija na kojeg se zapisuju poruke o greški.

Default
/var/ibmslapd.log

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdESizeThreshold

Opis Navodi broj radnih stavki na radnom redu prije nego što je nit Opasnosti aktivirana.

Default
50

Sintaksa
Cijeli broj

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdEThreadActivate

Opis Navodi koji će uvjeti aktivirati Nit opasnosti. Mora biti postavljeno na jednu od sljedećih vrijednosti:

S Samo veličina

T Samo vrijeme

SOT Veličina ili vrijeme

SAT Veličina i vrijeme

Default
SAT

Sintaksa
Niz

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdEThreadEnable

Opis Navodi da li je Nit opasnosti aktivna.

Default
Istinito

Sintaksa
Booleov

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdETimeThreshold

Opis Navodi vrijeme u minutama između stavki uklonjenih iz radnog reda prije nego što se Nit opasnosti aktivira.

Default
5

Sintaksa
Cijeli broj

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdFilterCacheBypassLimit

Opis Filteri pretraživanja kod kojih se podudara više od tog broja unosa se neće dodati na predmemoriju Filtera pretraživanja. Budući je popis ID-ova unosa koji se podudaraju s tim filterom uključen u ovu predmemoriju, ta postavka pomaže kako bi se ograničilo korištenje memorije. Vrijednost 0 označava da nema granice.

Default
100

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdFilterCacheSize

Opis Specificira maksimalan broj unosa koji će se zadržati u Predmemoriji filtera pretraživanja.

Default
25000

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdIdleTimeOut

Opis Maksimalno vrijeme kroz koje će se LDAP veza držati otvorenom kada nema aktivnosti na vezi. Vrijeme mirovanja za LDAP vezu je vrijeme (u sekundama) između zadnje aktivnosti na vezi i trenutnog vremena. Ako je vrijeme veze isteklo, na temelju toga što je vrijeme mirovanja veće od vrijednosti tog atributa, LDAP poslužitelj će očistiti i završiti LDAP vezu i tako je napraviti dostupnom za druge dolazne zahtjeve.

Default
300

Sintaksa
Cijeli broj

Dužina
11

Brojanje
Jedan

Korištenje
Operacija direktorija

Modificiranje korisnika
Da

Klasa pristupa
Kritična

Potrebno
Ne

ibm-slapdIncludeSchema

Opis Specificira stazu direktorija na stroju Poslužitelja direktorija koji sadrži definicije sheme.

Default

- /etc/V3.system.at
- /etc/V3.system.oc
- /etc/V3.config.at
- /etc/V3.config.oc
- /etc/V3.ibm.at
- /etc/V3.ibm.oc
- /etc/V3.user.at
- /etc/V3.user.oc
- /etc/V3.ldapsyntaxes
- /etc/V3.matchingrules

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Više-vrijednosti

ibm-slapdKrbAdminDN

Opis Specificira Kerberos ID od LDAP administratora (na primjer, ibm-kn=admin1@realm1). Koristi se kada se koristi Kerberos provjera autentičnosti kako bi se provjerila autentičnost administratora kada je prijavljen na sučelje Administracija. To se može specificirati umjesto ili kao dodatak adminDN i adminPW.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdKrbEnable

Opis Specificira da li poslužitelj podržava Kerberos. Mora biti TRUE ili FALSE.

Default
TRUE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdKrbIdentityMap

Opis Specificira da li treba koristiti Kerberos mapiranje poduzeća. Mora biti postavljeno na TRUE ili FALSE. Ako je postavljeno na TRUE, kada je klijent ovlašten s Kerberos ID, poslužitelj traži sve lokalne korisnike s podudarajućim Kerberos vjerodajnicama i dodaje DN-ove tih korisnika na vjerodajnice vezanja veze. Time se omogućava da se ACL-ovi zasnovani na DN-ovima LDAP korisnika mogu koristiti s Kerberos.

Default
FALSE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdKrbKeyTab

Opis Specificira Kerberos datoteku tablice ključeva LDAP poslužitelja. Ta datoteka sadrži privatni ključ LDAP poslužitelja koji je pridružen njegovom Kerberos računu. Ta datoteka se treba zaštititi (kao datoteka baze podataka ključa SSL poslužitelja).

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdKrbRealm

Opis Specificira Kerberos područje LDAP poslužitelja. Koristi se za objavljivanje ldapservicename atributa u ishodišnom DSE. Primijetite da LDAP poslužitelj može služiti kao spremište informacija računa za više KDC-ova (i područja), no LDAP poslužitelj, kao poslužitelj pod utjecajem Kerberosa, može biti član samo jednog područja.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
256

Vrijednost
Jedna-vrijednost

ibm-slapdLanguageTagsEnabled

Opis Da li poslužitelj treba dozvoliti oznake jezika. Vrijednost učitana iz ibmslapd.conf datoteke za ovaj atribut je FALSE, ali se može postaviti na TRUE.

Default
FALSE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdLdapCrlHost

Opis Specificira ime hosta LDAP poslužitelja koji sadrži Liste opoziva certifikata (CRL-ovi) za provjeru valjanosti x.509v3 certifikata klijenta. Taj parametar je potreban kada se ibm-slapdSslAuth=serverclientauth i certifikati klijenta izdaju za CRL provjeru valjanosti.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
256

Vrijednost
Jedna-vrijednost

ibm-slapdLdapCrlPassword

Opis Specificira lozinku koju SSL na strani poslužitelja koristi za vezanje na LDAP poslužitelj koji sadrži Liste opoziva certifikata (CRL-ovi) za provjeru valjanosti x.509v3 certifikata klijenta. Taj parametar bi mogao biti potreban kada se ibm-slapdSslAuth=serverclientauth i certifikati klijenta izdaju za CRL provjeru valjanosti.

Bilješka: Ako LDAP poslužitelj koji sadrži CRL-ove dopušta neovlaštene pristupe na CRL-ove (odnosno, anonimni pristup), onda nije potrebno ibm-slapdLdapCrlPassword.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Binarno

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdLdapCrlPort

Opis Specificira port koji će se koristiti za povezivanje na LDAP poslužitelj koji sadrži Listu opoziva certifikata (CRL-ovi) za provjeru valjanosti x.509v3 certifikata klijenta. Taj parametar je potreban kada se ibm-slapdSslAuth=serverclientauth i certifikati klijenta izdaju za CRL provjeru valjanosti. (IP portovi nisu označeni, 16-bitni cijeli brojevi u rasponu od 1 - 65535)

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdLdapCrlUser

Opis Specificira DN vezanja kojeg SL na strani poslužitelja koristi za vezanje na LDAP poslužitelj koji sadrži Liste opoziva certifikata (CRL-ovi) za provjeru valjanosti x.509v3 certifikata klijenta. Taj parametar bi mogao biti potreban kada se ibm-slapdSslAuth=serverclientauth i certifikati klijenta izdaju za CRL provjeru valjanosti.

Bilješka: Ako LDAP poslužitelj koji sadrži CRL-ove dopušta neovlaštene pristupe na CRL-ove (odnosno, anonimni pristup), onda nije potrebno ibm-slapdLdapCrlUser.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
DN

Maksimalna dužina
1000

Vrijednost
Jedna-vrijednost

ibm-slapdMasterDN

Opis Specificira DN vezanja glavnog poslužitelja. Vrijednost se mora podudarati s replicaBindDN u replicaObject definiranom za glavnog poslužitelja. Kada se Kerberos koristi za ovlaštenje na repliku, ibm-slapdMasterDN mora specificirati DN prikaz Kerberos ID-a (na primjer, ibm-kn=freddy@realm1). Kada se koristi Kerberos, zanemaruje se MasterServerPW.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
DN

Maksimalna dužina
1000

Vrijednost
Jedna-vrijednost

ibm-slapdMasterPW

Opis Specificira lozinku vezanja glavnog replika poslužitelja. Vrijednost se mora podudarati s replicaBindDN u replicaObject definiranom za glavnog poslužitelja. Kada se Kerberos koristi za ovlaštenje na repliku, ibm-slapdMasterDN mora specificirati DN prikaz Kerberos ID-a (na primjer, ibm-kn=freddy@realm1). Kada se koristi Kerberos, zanemaruje se MasterServerPW.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Binarno

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdMasterReferral

Opis Specificira URL glavnog replika poslužitelja. Na primjer:

```
ldap://master.us.ibm.com
```

Za sigurnost postavljenu samo na SSL:

```
ldaps://master.us.ibm.com:636
```

Za sigurnost postavljenu na ništa i korištenje nestandardnog porta:

```
ldap://master.us.ibm.com:1389
```

Default
nijedan

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
256

Vrijednost
Jedna-vrijednost

ibm-slapdMaxEventsPerConnection

Opis Specificira maksimalan broj obavještavanja o događaju koja se mogu registrirati po vezi.

```
Minimum = 0 (neograničeno)
Maksimum = 2,147,483,647
```

Default
100

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdMaxEventsTotal

Opis Specificira maksimalan ukupan broj obavještavanja o događaju koja se mogu registrirati za sve veze.

```
Minimum = 0 (neograničeno)
Maksimum = 2,147,483,647
```

Default
0

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdMaxNumOfTransactions

Opis Specificira maksimalan broj transakcija po poslužitelju.

Minimum = 0 (neograničeno)
Maksimum = 2,147,483,647

Default
20

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdMaxOpPerTransaction

Opis Specificira maksimalan broj operacija po transakciji.

Minimum = 0 (neograničeno)
Maksimum = 2,147,483,647

Default
5

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdMaxPendingChangesDisplayed

Opis Maksimalan broj promjena u toku koje će se prikazati.

Default
200

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdMaxTimeLimitOfTransactions

Opis Specificira maksimalnu timeout vrijednost u sekundama za transakcije koje su u toku.

Minimum = 0 (neograničeno)
Maksimum = 2,147,483,647

Default
300

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdPagedResAllowNonAdmin

Opis Da li bi poslužitelj trebao ili ne, dozvoliti vezanje ne-Administratora za zahtjeve s rezultatima podijeljenim u stranice na zahtjevima pretraživanja. Ako je vrijednost pročitana s ibmslapd.conf datoteke FALSE, poslužitelj će obrađivati samo one zahtjeve klijenta koje je poslao na izvođenje korisnik s Administrator ovlaštenjem. Ako klijentovi rezultati zahtjeva podijeljeni u stranice za operaciju pretraživanja nemaju Administrator ovlaštenje, a vrijednost pročitana iz ibmslapd.conf datoteke za taj atribut je FALSE, poslužitelj će vratiti klijentu povratni kod insufficientAccessRights; neće se izvoditi pretraživanje ili podjela u stranice.

Default
FALSE

Sintaksa
Booleov

Dužina
5

Brojanje
Jedan

Korištenje
directoryOperation

Modificiranje korisnika
Da

Klasa pristupa
kritično

Klasa objekta
ibm-slapdRdbmBackend

Potrebno
Ne

ibm-slapdPagedResLmt

Opis Maksimalan broj istaknutih rezultata zahtjeva pretraživanja koji su podijeljeni u stranice koji mogu istovremeno biti aktivni. Raspon = 0.... Ako klijent zahtjeva operaciju s rezultatima podijeljenim u stranice, a trenutno je aktivan maksimalan broj istaknutih rezultata podijeljenih u stranice, onda će poslužitelj vratiti klijentu povratni kod busy; neće se izvoditi pretraživanje ili podjela u stranice.

Default
3

Sintaksa
Cijeli broj

Dužina
11

Brojanje
Jedan

Korištenje
directoryOperation

Modificiranje korisnika
Da

Klasa pristupa
kritično

Potrebno
Ne

Klasa objekta
ibm-slapdRdbmBackend

ibm-slapdPageSizeLmt

Opis Maksimalan broj unosa koji će se vratiti iz pretraživanja za jednu stranicu kada je specificirana kontrola rezultata podijeljenih u stranice, bez obzira na veličinu stranice koja bi mogla biti specificirana na zahtjevu pretraživanja klijenta. Raspon = 0.... Ako je klijent premašio veličinu stranice, onda će se koristiti manja vrijednosti od vrijednosti klijenta i vrijednosti pročitane iz ibmslapd.conf.

Default
50

Sintaksa
Cijeli broj

Dužina
11

Brojanje
Jedan

Korištenje
directoryOperation

Modificiranje korisnika
Da

Klasa pristupa
kritično

Potrebno
Ne

Klasa objekta
ibm-slapdRdbmBackend

ibm-slapdPlugin

Opis Plugin je dinamički učitana knjižnica koja proširuje sposobnosti poslužitelja. Atribut ibm-slapdPlugin specificira poslužitelju kako treba učitati i inicijalizirati plug-in knjižnicu. Sintaksa je:

```
keyword filename init_function [args...]
```

Sintaksa se malo razlikuje za svaku platformu zbog konvencija imenovanja knjižnice.

Većina plug-inova je neobvezna, no plug-in RDBM pozadine je potreban za sve RDBM pozadine.

Default
baza podataka /bin/libback-rdbm.dll rdbm_backend_init

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
2000

Vrijednost
Više-vrijednosti

ibm-slapdPort

Opis Specificira TCP/IP port koji se koristi za ne-SSL veze. Ne može imati istu vrijednost kao i ibm-slapdSecurePort. (IP portovi nisu označeni, 16-bitni cijeli brojevi u rasponu 1 - 65535.)

Default
389

Sintaksa
Cijeli broj

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdPWEncryption

Opis Specificira mehanizam kodiranja za lozinke korisnika prije nego se pohrane u direktorij. Mora biti specificiran kao none, imask, crypt ili sha (morate koristiti ključnu riječ **sha** za SHA-1 kodiranje). Vrijednost mora biti postavljena na none kako bi uspjelo SASL cram-md5 vezanje.

Default
nijedan

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdReadOnly

Opis Atribut se normalno odnosi samo na pozadinu Direktorija. Specificira da li se može zapisati pozadina. Mora biti specificiran kao TRUE ili FALSE. Ako nije specificiran, postavlja se na FALSE. Ako je postavljen na TRUE, poslužitelj vraća LDAP_UNWILLING_TO_PERFORM (0x35) kao odgovor na bilo koji zahtjev klijenta koji mijenja podatke u bazi podataka samo za čitanje.

Default
FALSE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdReferral

Opis Specificira LDAP URL referala koji će se vratiti onda kada se sa zahtjevom ne podudaraju lokalni sufiksi. Koristi se za superiorne referale (odnosno, sufiks nije unutar konteksta imenovanja poslužitelja).

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
32700

Vrijednost
Više-vrijednosti

ibm-slapdReplDbConns

Opis Maksimalan broj veza baze podataka koje može koristiti replikacija.

Default
4

Sintaksa
Cijeli broj

Maksimalna dužina
11

Vrijednost
Jedna-vrijednost

ibm-slapdReplicaSubtree

Opis Identificira DN repliciranog podstabla

Sintaksa
DN

Maksimalna dužina
1000

Vrijednost
Jedna-vrijednost

ibm-slapdSchemaAdditions

Opis Atribut ibm-slapdSchemaAdditions se koristi kako bi se izričito identificiralo koja datoteka sadrži unose nove sheme. To je po defaultu postavljeno da bude /etc/V3.modifiedschema. Ako taj atribut nije definiran, poslužitelj se vraća na korištenje posljednje ibm-slapdIncludeSchema datoteke u prethodnim izdanjima.

Prije verzije 3.2, posljednji includeSchema unos u **slapd.conf** je bila datoteka na koju su se svi novi unosi sheme dodavali od strane poslužitelja ako je primio i dodao zahtjev klijenta. U pravilu je posljednja includeSchema V3.modifiedschema datoteka koja je prazna datoteka koja je instalirana samo u tu svrhu.

Bilješka: Naziv modificirana krivo upućuje jer ona samo pohranjuje nove unose. Promjene na postojećim unosima sheme se izvode u njihovim originalnim datotekama.

Default
/etc/V3.modifiedschema

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdSchemaCheck

Opis Specificira mehanizam provjeravanja sheme za operacije dodaj/modificiraj/obriši. Mora biti specificiran kao V2, V3 ili V3_lenient.

- V2 - Zadržava v2 i v2.1 provjeravanje. Preporuča se u svrhu migriranja.
- V3 - Izvodi v3 provjeravanje.
- V3_lenient - Nisu potrebne sve nadređene klase objekta. Potrebne su samo neposredne klase objekta kada se dodaju unosi.

Default
V3_lenient

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
10

Vrijednost
Jedna-vrijednost

ibm-slapdSecurePort

Opis Specificira TCP/IP port koji se koristi za SSL veze. Ne može imati istu vrijednost kao i ibm-slapdPort. (IP portovi nisu označeni, 16-bitni cijeli brojevi u rasponu 1 - 65535.)

Default
636

Sintaksa
Cijeli broj

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdSecurity

Opis Omogućava SSL i TLS veze. Mora biti ništa, SSL, Samo SSL, TLS ili SSLTLS.

- ništa - Poslužitelj sluša samo na neosiguranom portu.
- SSL - Poslužitelj sluša na SSL i ne-SSL portovima. Sigurni port je jedini način korištenja sigurne veze.
- SSLOnly - Poslužitelj sluša samo na SSL portu.
- TLS - Poslužitelj sluša samo na neosiguranom portu. StartTLS proširena operacija je jedini način korištenja sigurne veze.
- SSLTLS - Poslužitelj sluša na default i sigurnim portovima. StartTLS proširena operacija može biti korištena radi dobivanja sigurne veze preko default porta ili klijent može koristiti sigurni port direktno. Slanje StartTLS preko sigurnog porta će vratiti poruku LDAP_OPERATIONS_ERROR.

Default
nijedan

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
7

Vrijednost
Jedna-vrijednost

ibm-slapdServerId

Opis Identificira poslužitelj koji će se koristiti u replikaciji.

Sintaksa
IA5 niz s uspoređivanjem osjetljivim na velika i mala slova

Maksimalna dužina
240

Vrijednost
Jedna-vrijednost

ibm-slapdSetenv

Opis Poslužitelj izvodi **putenv()** za sve vrijednosti od ibm-slapdSetenv kod pokretanja da bi promijenili poslužiteljsko okruženje vremena izvođenja. Varijable ljuske (kao što je %PATH% ili $LANG) se ne proširuju.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
2000

Vrijednost
Više-vrijednosti

ibm-slapdSizeLimit

Opis Specificira maksimalan broj unosa koji će se vratiti iz pretraživanja, bez obzira na ograničenje veličine koje je možda bilo specificirano na klijentovom zahtjevu za pretraživanje (Raspon = 0...). Ako je klijent premašio granicu, koristit će se manja vrijednost od vrijednosti klijenta i vrijednosti koja je pročitana iz **ibmslapd.conf**. Ako klijent nije premašio granicu i ima ograničenje kao admin DN, smatra se da ograničenje ne postoji. Ako klijent nije premašio ograničenje i nije ograničen kao admin DN, onda je ograničenje ono koje je pročitano iz **ibmslapd.conf** datoteke. 0 = neograničeno.

Default
500

Sintaksa
Cijeli broj

Maksimalna dužina
12

Vrijednost
Jedna-vrijednost

ibm-slapdSortKeyLimit

Opis Maksimalan broj uvjeta sortiranja (ključeva) koji mogu biti specificirani na jednom zahtjevu za pretraživanjem. Raspon = 0.... Ako je klijent propustio zahtjev pretraživanja s više ključeva sortiranja od dozvoljenih, a kritičnost kontrole sortiranog pretraživanja je FALSE, onda će poslužitelj poštovati vrijednost koja je pročitana iz ibmslapd.conf datoteke i zanemariti sve ključeve sortiranja na koje naiđe nakon što je dosegnuta granica - izvodit će se pretraživanje i sortiranje. Ako je klijent predao zahtjev pretraživanja s više ključeva nego što ograničenje dozvoljava i sortirana kritičnost kontrole pretraživanja je TRUE, onda će poslužitelj vratiti klijentu kod vraćanja **adminLimitExceeded** - pretraživanje ili sortiranje neće biti izvedeno.

Default
3

Sintaksa
cis

Dužina
11

Brojanje
Jedan

Korištenje
directoryOperation

Modificiranje korisnika
Da

Klasa pristupa
kritično

Klasa objekta
ibm-slapdRdbmBackend

Potrebno
Ne

ibm-slapdSortSrchAllowNonAdmin

Opis Da li bi poslužitelj trebao ili ne, dozvoliti vezanje ne-Administratora za sortiranje na zahtjevu pretraživanja. Ako je vrijednost pročitana s ibmslapd.conf datoteke FALSE, poslužitelj će obrađivati samo one zahtjeve klijenta koje je poslao na izvođenje korisnik s Administrator ovlaštenjem. Ako klijentov zahtjev za sortiranjem zahtjeva pretraživanja nema Administrator ovlaštenje, a vrijednost pročitana iz ibmslapd.conf datoteke za taj atribut je FALSE, poslužitelj će vratiti klijentu povratni kod insufficientAccessRights - neće se izvoditi pretraživanje ili sortiranje.

Default
FALSE

Sintaksa
Booleov

Dužina
5

Brojanje
Jedan

Korištenje
directoryOperation

Modificiranje korisnika
Da

Klasa pristupa
kritično

Klasa objekta
ibm-slapdRdbmBackend

Potrebno
Ne

ibm-slapdSslAuth

Opis Specificira tip provjere autentičnosti za ssl vezu, serverauth ili serverclientauth.

- serverauth - podržava provjeru autentičnosti poslužitelja na klijentu. Ovo je default.
- serverclientauth - podržava provjeru autentičnosti klijenta i poslužitelja.

Default
serverauth

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
16

Vrijednost
Jedna-vrijednost

ibm-slapdSslCertificate

Opis Specificira oznaku koja identificira Osobni certifikat poslužitelja u datoteci baze podataka ključa. Ta oznaka je specificirana kada su privatni ključ poslužitelja i certifikat kreirani s **gsk4ikm** aplikacijom. Ako nije definirano ibm-slapdSslCertificate, default privatni ključ, kako je to definirano u datoteci baze podataka ključa, koristi LDAP poslužitelj za SSL veze.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdSslCipherSpec

Specificira metodu za SSL šifriranje za klijente koji pristupaju poslužitelju. Mora biti postavljen na jedno od sljedećeg:

Tablica 6. Metode SSL šifriranja

Atribut	Razina šifriranja
TripleDES-168	Trostruko DES šifriranje sa 168-bitnim ključem i SHA-1 MAC
DES-56	DES šifriranje s 56-bitnim ključem i SHA-1 MAC
RC4-128-SHA	RC4 šifriranje sa 128-bitnim ključem i SHA-1 MAC
RC4-128-MD5	RC4 šifriranje sa 128-bitnim ključem i MD5 MAC
RC2-40-MD5	RC4 šifriranje sa 40-bitnim ključem i MD5 MAC
RC4-40-MD5	RC4 šifriranje sa 40-bitnim ključem i MD5 MAC
AES	AES šifriranje

Sintaksa
IA5 niz

Maksimalna dužina
30

ibm-slapdSslKeyDatabase

Opis Specificira stazu datoteke do SSL datoteke baze podataka ključa LDAP poslužitelja. Ta datoteka baze podataka ključa se koristi za rukovanje SSL vezama s LDAP klijenata, kao i za kreiranje sigurnih SSL veza do replika LDAP poslužitelja.

Default
/etc/key.kdb

Sintaksa
Niz direktorija s podudaranjem velikih i malih slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdSslKeyDatabasePW

Opis Specificira lozinku koja je pridružena SSL datoteci baze podataka ključa LDAP poslužitelja, kako je to specificirano na ibm-slapdSslKeyDatabase parametru. Ako datoteka baze podataka ključa LDAP poslužitelja ima pridruženu datoteku skrivene lozinke, onda se ibm-slapdSslKeyDatabasePW parametar može izostaviti ili postaviti na none.

Bilješka: Datoteka skrivene lozinke mora biti smještena u istom direktoriju kao i datoteka baze podataka ključa i mora imati isto ime datoteke kao i datoteka baze podataka ključa, no s ekstenzijom .sth umjesto .kdb.

Default
nijedan

Sintaksa
Binarno

Maksimalna dužina
128

Vrijednost
Jedna-vrijednost

ibm-slapdSslKeyRingFile

Opis Staza do SSL datoteke baze podataka ključa LDAP poslužitelja. Ta datoteka baze podataka ključa se koristi za rukovanje SSL vezama s LDAP klijenata, kao i za kreiranje sigurnih SSL veza do replika LDAP poslužitelja.

Default
key.kdb

Sintaksa
Niz direktorija s uspoređivanjem osjetljivim na velika i mala slova

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

ibm-slapdSuffix

Opis Specificira kontekst imenovanja koji će se pohraniti u ovoj pozadini.

Bilješka: To ima isto ime kao i klasa objekta.

Default
Nije definiran unaprijed postavljen default.

Sintaksa
DN

Maksimalna dužina
1000

Vrijednost
Više-vrijednosti

ibm-slapdSupportedWebAdmVersion

Opis Taj atribut definira najraniju verziju Web administracijskog alata koji podržava taj poslužitelj od cn=configuration.

Default

Sintaksa
Niz direktorija

Maksimalna dužina

Vrijednost
Jedna-vrijednost

ibm-slapdSysLogLevel

Opis Specificira razinu na kojoj se zapisuju statistike otkrivanja grešaka i operacije u datoteci slapd.errors. Mora biti specificirano kao l, m ili h.

- h - visoko (osigurava najviše informacija)
- m - srednje (default)
- l - nisko (osigurava najmanje informacija)

Default
m

Sintaksa
Niz direktorija koji nije osjetljiv na podudaranje velikih i malih slova

Maksimalna dužina
1

Vrijednost
Jedna-vrijednost

ibm-slapdTimeLimit

Opis Specificira maksimalan broj sekundi koje se mogu potrošiti na zahtjev pretraživanja, bez obzira na bilo koje ograničenje vremena koje je možda specificirano na zahtjevu klijenta. Ako je klijent premašio granicu, koristit će se manja vrijednost od vrijednosti klijenta i vrijednosti koja je pročitana iz **ibmslapd.conf**. Ako klijent nije premašio granicu i ima ograničenje kao admin DN, smatra se da ograničenje ne postoji. Ako klijent nije premašio ograničenje i nije ograničen kao admin DN, onda je ograničenje ono koje je pročitano iz **ibmslapd.conf** datoteke. 0 = neograničeno.

Default
900

Sintaksa
Cijeli broj

Maksimalna dužina

Vrijednost
Jedna-vrijednost

ibm-slapdTransactionEnable

Opis Ako je učitan plugin transakcije, ali je ibm-slapdTransactionEnable postavljeno na FALSE, poslužitelj odbija sve StartTransaction zahtjeve s odgovorom LDAP_UNWILLING_TO_PERFORM.

Default
TRUE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdUseProcessIdPw

Opis Ako je postavljeno na TRUE, poslužitelj ignorira ibm-slapdDbUserID i ibm-slapdDbUserPW atribute i koristi svoje vlastite vjerodajnice procesa da autorizira DB2.

Default
FALSE

Sintaksa
Booleov

Maksimalna dužina
5

Vrijednost
Jedna-vrijednost

ibm-slapdVersion

Opis IBM Slapd Broj verzije

Default

Sintaksa
Niz direktorija s uspoređivanjem osjetljivim na velika i mala slova

Maksimalna dužina

Vrijednost
Jedna-vrijednost

ibm-slapdWriteTimeout

Opis Navodi vrijednost vremenskog prekoračenja u sekundama za blokirana pisanja. Kada je vremensko ograničenje dosegnuto veza će biti otpuštena.

Default
120

Sintaksa
Cijeli broj

Maksimalna dužina
1024

Vrijednost
Jedna-vrijednost

objectClass

Opis Vrijednost objectClass atributa opisuje vrstu objekta kojeg predstavlja unos.

Sintaksa
Niz direktorija

Maksimalna dužina
128

Vrijednost
Više-vrijednosti

Identifikatori objekata (OID-i)

Ove informacije sadrže identifikatore objekta (OID-i) koji se koriste u Directory Server-u.

OID-ovi prikazani u sljedećim tablicama su korišteni u Poslužitelju direktorija. Ti OID-i su u korijenu DSE. Korijenski DSE unos sadrži informacije o samom poslužitelju. Saznajte više o Identifikatorima objekta (OID-i) za proširene operacije i kontrole, uključujući kodiranje podataka o zahtjevu i odgovoru povezane sa sljedećim kontrolama i proširenim operacijama, u Tivoli Software informacijskom centru

Kontrole

Tablica 7. Podržane kontrole Poslužitelja direktorija

Ime	OID	Najraniji ili i5/OS ili OS/400 izdanje	Najranije IBM Tivoli Directory Server verzija	Opis
Upravljanje s DSA IT	2.16.840.1.1137.30.3.4.2	V4R5	V3.2	Tretira referal objekte kao obične unose.
"Transakcije" na stranici 50	1.3.18.0.2.10.5	V4R5	V3.2	Označava operaciju kao dio transakcije.
os400-dltusrprf-ownobjopt	1.3.18.0.2.10.8	V5R2		Obrišite korisnički profil opciju za vlasnika objekta. Za detalje pogledajte "Projicirana pozadina operativnog sistema" na stranici 82.
os400-dltusrprf-pgpopt	1.3.18.0.2.10.9	V5R2		Obrišite korisnički profil opciju za primarnu grupu. Za detalje pogledajte "Projicirana pozadina operativnog sistema" na stranici 82.
Sortirano pretraživanje	1.2.840.113556.1.4.473 (zahtjev) i 1.2.840.113556.1.4.474 (dogovor)	V5R2 s PTF-om	V4.1	Sortira rezultate pretraživanja prije vraćanja unosa na klijenta. Pogledajte "Parametri pretraživanja" na stranici 46.
Pretraživanje na stranici	1.2.840.113556.1.4.319	V5R2 s PTF-om	V4.1	Vraća klijentu rezultate pretraživanje u stranicama umjesto da vrati sve odjednom. Pogledajte "Parametri pretraživanja" na stranici 46.

Tablica 7. Podržane kontrole Poslužitelja direktorija (nastavak)

Ime	OID	Najraniji ili i5/OS ili OS/400 izdanje	Najranije IBM Tivoli Directory Server verzija	Opis
Kontrola Brisanja drveta	1.2.840.113556.1.4.805	V5R3	V5.1	Ta kontrola je dodana zahtjevu Brisanje kako bi se označilo da će se obrisati specificirani unos i svi njegovi podređeni unosi. Korisnik mora biti administrator direktorija. Unos koji će se obrisati ne može biti kontekst replikacije.
"Politika lozinke" na stranici 75	1.3.6.1.4.1.42.2.27.8.5.1	V5R3	V5.1	Vraća klijentu posebne informacije o greški politike lozinke.
Administracija poslužitelja	1.3.18.0.2.10.15	V5R3	V5.1	Dozvoljava administratoru da izvodi operacije popravljanja koje bi se normalno odbile (na primjer: ažuriranje replike samo za čitanje, ažuriranje umirenog poslužitelja ili postavljanje određenih operativnih atributa).
"Proxy autorizacija" na stranici 62	2.16.840.1.113730.3.4.18	V5R4	V5.2	Aplikacija klijenta se može vezati na direktorij s vlastitim identitetom, ali joj je dozvoljeno izvoditi operacije u ime drugih.
Kontrola vezivanja dobavljača replikacije	1.3.18.0.2.10.18	V5R3	V5.2	Ova kontrola je dodana od strane dobavljača, ako je dobavljač poslužitelj prilaza.
Kontrola Osvježi unos	1.3.18.0.2.10.24	V6R1	V6.0	Ovu kontrola interno koristi poslužitelj za podršku rezoluciji sukoba replikacije.
Nema rezolucije sukoba replikacije	1.3.19.0.2.10.27	V6R1	V6.0	Ovu kontrola interno koristi poslužitelj za podršku rezoluciji sukoba replikacije.
Kontrola Ne repliciraj	1.3.19.0.2.10.23	V6R1	V6.0	Ovu kontrolu može specificirati administrator kako bi zahtijevao da se pridružena operacija ne replicira na druge poslužitelje. Kontrola nema vrijednost kontrole.

Tablica 7. Podržane kontrole Poslužitelja direktorija (nastavak)

Ime	OID	Najraniji ili i5/OS ili OS/400 izdanje	Najranije IBM Tivoli Directory Server verzija	Opis
Revizijska kontrola	1.3.18.0.2.10.22	V6R1	V6.0	Ovu kontrolu koriste ovlašteni klijenti, uključujući proxy poslužitelj, za identificiranje klijenta koji je pokrenuo zahtjev koji bi se mogao usmjeriti kroz višestruke poslužitelje.
Kontrola Ovlaštenje grupe	1.3.18.0.2.10.21	V6R1	V6.0	Ova se kontrola koristi za traženje grupnog članstva identiteta ovlaštenja klijenta, umjesto grupnog članstva lokalnog poslužitelja. Koristi se zajedno s kontrolom proxy ovlaštenja.
Kontrola Modificiraj samo grupe	1.3.18.0.2.10.25	V6R1	V6.0	Operaciju s tom kontrolom (brisati ili modrdn/dn) prepoznat će pozadinski poslužitelj kao poseban tip operacije gdje se dn ne briše ili preimenuje; umjesto toga, grupe u kojima se nalazi se modificiraju u brisati ili preimenovati referencu u ciljni dn u svom članstvu.
Kontrola Izostavi referentni integritet grupe	1.3.18.0.2.10.26	V6R1	V6.0	Izostavite referentni integritet grupe obrađivanjem zahtjeva brisati ili modrdn. ACI i grupno članstvo se ne ažuriraju za prikazivanje promjene.
Kontrola AES vezanje	1.3.18.0.2.10.28	V6R1	V6.0	Ova kontrola omogućuje IBM Tivoli Directory Server-u slanje ažuriranja na poslužitelj potrošača s lozinkama koje su već šifrirane pomoću AES-a.

Proširene operacije

Tablica 8. OID-i za proširene operacije

Ime	OID	Najraniji ili i5/OS ili OS/400 izdanje	Najranija IBM Tivoli Directory Server verzija	Opis
Registriraj događaje	1.3.18.0.2.12.1	V4R5	V3.2	Registracija zahtjeva za događaje u podršci događaja Tivoli Directory Servera
Deregistriraj događaje	1.3.18.0.2.12.3	V4R5	V3.2	Deregistriraj za događaje koji su registrirani za upotrebu Zahtjeva za registraciju događaja.
Započni transakciju	1.3.18.0.2.12.5	V4R5	V3.2	Započni transakcijski kontekst
Završi transakciju	1.3.18.0.2.12.6	V4R5	V3.2	Završi transakcijski kontekst (pokreni/vrati)
Zahtjev DN normalizacije	1.3.18.0.2.12.30	V5R3	V5.1	Zahtjev za normalizaciju DN ili sekvenci DN-a.
StartTLS	1.3.6.1.4.1.1466.20037	V5R4	V5.2	Zahtjev za pokretanjem Sigurnosti razine prijenosa.

Definirane su dodatne proširene operacije koje ne bi trebao pokrenuti klijent. Te operacije su korištene kroz ldapexop uslužni program ili kroz operacije koje izvodi Web administracijski alat. Dolje su ispisane te operacije i ovlaštenja koja su potrebna za njihovo pokretanje:

Tablica 9. Dodatne proširene operacije

Ime	OID	Najranije i5/OS izdanje	Najranija IBM Tivoli Directory Server verzija	Opis
Kontroliraj replikaciju	1.3.18.0.2.12.16	V5R3	V5.1	Ta operacija izvodi traženu akciju na poslužitelju na kojem je izdana i prosljeđuje poziv do svih potrošača koji su u topologiji replikacije ispod nje. Klijent mora biti administrator direktorija ili imati ovlaštenje pisanja na ibm-replicagroup=default objektu za pridruženi kontekst replikacije.
Kontroliraj red replikacije	1.3.18.0.2.12.17	V5R3	V5.1	Ta operacija označava stavke kao već replicirane za specificirani ugovor. Ta operacija je dozvoljena samo kad klijent ima ovlaštenje za pisanje na ugovoru replikacije.
Umirivanje ili deumirivanje	1.3.18.0.2.12.19	V5R3	V5.1	Ta operacija stavlja podstablo u stanje u kojem ne prihvaća ažuriranja klijenta (ili prekida to stanje), osim za klijente koji su ovlašteni kao administratori direktorija na kojem postoji kontrola Administracije poslužitelja. Klijent mora biti ovlašten kao administrator direktorija ili imati ovlaštenje pisanja za ibm-replicagroup=default objekt za pridruženi kontekst replikacije.

Tablica 9. Dodatne proširene operacije (nastavak)

Ime	OID	Najranije i5/OS izdanje	Najranija IBM Tivoli Directory Server verzija	Opis
Kaskadna kontrola replikacije	1.3.18.0.2.12.15	V5R3	V5.1	Ta operacija izvodi traženu akciju na poslužitelju na kojem je izdana i prosljeđuje poziv do svih potrošača koji su u topologiji replikacije ispod nje. Klijent mora biti administrator direktorija ili imati ovlaštenje pisanja na ibm-replicagroup=default objektu za pridruženi kontekst replikacije.
Ažuriraj konfiguraciju	1.3.18.0.2.12.28	V5R3	V5.1	Ta operacija se koristi kako bi se uzrokovalo da poslužitelj ponovno pročita specificirane postavke iz svoje konfiguracije. Operacija je dozvoljena samo kada je klijent administrator direktorija.
Zahtjev Prekini Vezu	1.3.18.0.2.12.35	V5R4	V5.2	Zahtjev za prekidanjem veze na poslužitelju. Pozivatelj mora biti administrator direktorija.
Zahtjev jedinstven atribut	1.3.18.0.2.12.44	V5R4	V5.2	Zahtjeva da poslužitelj vrati listu svih ne-jedinstvenih vrijednosti za dano ime atributa. Pogledajte “ldapexop” na stranici 212 -op uniqueattr. Pozivatelj mora biti administrator direktorija.
Zahtjev tip atributa	1.3.18.0.2.12.46	V5R4	V5.2	Zahtjeva da poslužitelj vrati listu imena atributa koji imaju određenu osobinu. Pogledajte “ldapexop” na stranici 212 -op getattributes
Zahtjev korisničkog tipa	1.3.18.0.2.12.37	V5R3	V5.2	Zahtjev za dohvaćanjem Korisničkog tipa vezanog korisnika.
Proširena operacija dnevnika grešaka replikacije	1.3.18.0.2.12.56	V6R1	V6.0	Proširena zahtjev IBM Kontrole grešaka replikacije koristi se za pogled dnevnika grešaka replikacije, ponovno pokušaj unosa iz dnevnika ili brisanje unosa dnevnika. Pozivatelj mora biti administrator direktorija ili imati ovlaštenje pisati u ibm-replicagroup=default objekt za kontekst pridružene replikacije.
Proširena operacija procjene grupe	1.3.18.0.2.12.50	V6R1	V6.0	Zahtijeva sve grupe kojima određeni korisnik pripada. Pozivatelj mora biti administrator direktorija.
Proširena operacija topologije replikacije	1.3.18.0.2.12.54	V6R1	V6.0	Okinite replikaciju unosa povezanih s topologijom replikacije u sklopu određenog konteksta replikacije. Pozivatelj mora biti administrator direktorija ili imati ovlaštenje pisati u ibm-replicagroup=default objekt za kontekst pridružene replikacije.

Tablica 9. Dodatne proširene operacije (nastavak)

Ime	OID	Najranije i5/OS izdanje	Najranija IBM Tivoli Directory Server verzija	Opis
Proširena operacija statusa računa	1.3.18.0.2.12.58	V6R1	V6.0	Ova proširena operacija šalje poslužitelju DN unosa koji sadrži userPassword atribut, a poslužitelj vraća status korisničkog računa za koji je poslan upit: otvoren, zaključan ili zastario. Pozivatelj mora biti administrator direktorija.
Proširena operacija Dohvati datoteku	1.3.18.0.2.12.73	V6R1	V6.0	Vraća sadržaj određene datoteke na poslužitelj. Pozivatelj mora biti administrator direktorija. Podržava LostAndFound dnevnik i Tivoli Directory Server dnevnik revizije. Dnevnik revizije se ne odnosi na i5/OS sposobnosti sigurnosnog revidiranja directory servera.
Proširena operacija Dohvati linije	1.3.18.0.2.12.22	V6R1	V6.0	Zahtjev za dohvaćanje linija iz datoteke dnevnika. Pozivatelj mora biti administrator direktorija. Podržava LostAndFound dnevnik i Tivoli Directory Server dnevnik revizije. Dnevnik revizije se ne odnosi na i5/OS sposobnosti sigurnosnog revidiranja directory servera.
Proširena operacija Dohvati broj linija	1.3.18.0.2.12.24	V6R1	V6.0	Zahtjev za brojem linija u datoteci dnevnika. Pozivatelj mora biti administrator direktorija. Podržava LostAndFound dnevnik i Tivoli Directory Server dnevnik revizije. Dnevnik revizije se ne odnosi na i5/OS sposobnosti sigurnosnog revidiranja directory servera.

Podržane i omogućene sposobnosti

Sljedeća tablica pokazuje OID-ove za podržane i omogućene sposobnosti. Možete koristiti te OID-ove da pogledate da li određeni poslužitelj podržava te značajke.

Tablica 10. OID za podržane i omogućene sposobnosti

Ime	OID	Opis
Poboljšan model repliciranja	1.3.18.0.2.32.1	Identificira model repliciranja uveden u IBM Poslužitelju direktorija v5.1 uključujući replikaciju podstabla i kaskadnu replikaciju.
Kontrolna suma unosa	1.3.18.0.2.32.2	Označava da ovaj poslužitelj podržava ibm-entrychecksum i ibm-entrychecksumop značajke.
Ulazni UUID	1.3.18.0.2.32.3	Identificira da ovaj poslužitelj podržava ibm-entryuuid operativni atribut.
Filter ACL-e	1.3.18.0.2.32.4	Identificira da ovaj poslužitelj podržava IBM Filter ACL model.
Politika lozinke	1.3.18.0.2.32.5	Identificira da ovaj poslužitelj podržava politike lozinke

Tablica 10. OID za podržane i omogućene sposobnosti (nastavak)

Ime	OID	Opis
Sortiranje po DN	1.3.18.0.2.32.6	Pokazuje da ovaj poslužitelj podržava korištenje ibm-slapdDn atributa za sortiranje po DN.
Delegiranje administrativne grupe	1.3.18.0.2.32.8	Poslužitelj podržava delegiranje administracije poslužiteljem grupi administratora koji su navedeni u pozadini konfiguracije.
Sprečavanje Odbijanja usluge	1.3.18.0.2.32.9	Poslužitelj podržava značajku sprječavanje odbijanja usluge. Uključujući vremensko prekoračenje čitanja/pisanja i nit opasnosti.
Dinamička ažuriranja unosa i podstabla	1.3.18.0.2.32.15	Poslužitelj podržava dinamička ažuriranja konfiguracije na unosima i podstablima
Opcija dereferencije aliasa	1.3.18.0.2.32.10	Poslužitelj podržava opciju da ne radi dereferenciju aliasa po defaultu
Granice pretraživanja određene za grupu	1.3.18.0.2.32.17	Granice pretraživanja određene za grupu podržavaju proširene granice pretraživanja za grupu ljudi
Dinamičko praćenje	1.3.18.0.2.32.14	Poslužitelj podržava aktivno praćenje za poslužitelj pomoću LDAP proširene operacije.
TLS Sposobnosti	1.3.18.0.2.32.28	Navodi da je poslužitelj ustvari sposoban raditi TLS.
Revizija admin demona	1.3.18.0.2.32.11	Poslužitelj podržava reviziju admin demona.
Kerberos Sposobnosti	1.3.18.0.2.32.30	Navodi da je poslužitelj sposoban izvoditi Kerberos.
Neblokirajuća replikacija	1.3.18.0.2.32.29	Dobavljač ne pokušava uvijek poslati ažuriranje ako potrošač izvještava grešku
ibm-allMembers i ibm-allGroups operativni atributi	1.3.18.0.2.32.31	Pozadina podržava statičko, dinamičko i ugniježđeno grupno pretraživanje preko ibm-allMembers i ibm-allGroups operativnih atributa. Članovi statičke, dinamičke i/ili ugniježđene grupe mogu biti dobivene izvođenjem pretraživanja na ibm-allMembers operativnim atributima. Statički, dinamički i/ili ugniježđene grupe kojima pripada član DN mogu biti dobiveni izvođenjem pretraživanja na ibm-allGroups operativnim atributima.
Globalno jedinstveni atributi	1.3.18.0.2.32.16	Značajka poslužitelja da prisili globalno jedinstvene vrijednosti atributa.
Nadgledanje Broja operacija	1.3.18.0.2.32.24	Poslužitelj omogućuje nadgledavanje broja operacija za inicirane i dovršene tipove operacija.
Nadgledanje broja zapisivanja	1.3.18.0.2.32.20	Poslužitelj omogućuje nadgledanje broja zapisivanja za poruke dodane na poslužitelj, CLI i datoteke dnevnika revizije.
Nadgledanje brojača tipova povezivanja	1.3.18.0.2.32.22	Poslužitelj omogućuje nadgledanje brojanja tipova veza za SSL i TLS veze.
Nadgledanje informacija aktivnih radnika	1.3.18.0.2.32.21	Poslužitelj omogućuje informacije nadgledanja aktivnih radnika (cn=workers,cn=monitor).
Nadgledanje informacija povezivanja	1.3.18.0.2.32.23	Poslužitelj omogućuje nadgledanje informacija o vezama po IP adresama umjesto po ID-ovima veza (cn=connections, cn=monitor).
Nadgledanje informacija o praćenju	1.3.18.0.2.32.25	Poslužitelj omogućava nadgledanje informacija za praćenje opcija koje se trenutno koriste.
Rješavanje filtera pretraživanja za stavljanje atributa u predmemoriju	1.3.18.0.2.32.13	Poslužitelj podržava stavljanje atributa u predmemoriju za rješavanje filtera pretraživanja.
Proxy autorizacija	1.3.18.0.2.32.27	Poslužitelj podržava Proxy autorizaciju za grupu korisnika.
Podrška opcije oznake jezika	1.3.6.1.4.1.4203.1.5.4	Označava da poslužitelj podržava oznake jezika kao što je definirano u RFC 2596.

Tablica 10. OID za podržane i omogućene sposobnosti (nastavak)

Ime	OID	Opis
ChangeLog unosi maksimalne starosti	1.3.18.0.2.32.19	Navodi da je poslužitelj sposoban zadržati changelog unose bazirano na starosti.
IBMpolicies Podstablo replikacije	1.3.18.0.2.32.18	Poslužitelj podržava replikaciju od cn=IBMpolicies podstabla.
NULL bazirano pretraživanje podstabla	1.3.18.0.2.32.26	Poslužitelj dozvoljava null bazirano pretraživanje podstabla koje pretražuje cijeli DIT definiran na poslužitelju.
Autonomno stavljanje atributa u predmemoriju	1.3.18.0.2.32.50	Podržava autonomno stavljanje atributa u predmemoriju
ibm-entrychecksumop	1.3.18.0.2.32.56	6.0 IDS ibm-entrychecksumop funkcionalnost
Sposobnost poslužitelja filtriranih upućivanja	1.3.18.0.2.32.36	Koristi se pokazivanje podrške za poboljšana filtrirana upućivanja. To znači da će filtrirana vrijednost u upućivanju biti kombinirana s originalnim filterom na zahtjev pretraživanja.
Sposobnost poslužitelja globalne administrativne grupe	1.3.18.0.2.32.38	Koristi se pokazivanje podrške za globalnu administrativnu grupu.
Revidiranje sposobnosti usporediti	1.3.18.0.2.32.40	Koristi se pokazivanje podrške za revidiranje operacije usporediti.
AES šifriranje lozinke	1.3.18.0.2.32.39	Pokazuje podršku za AES šifriranje lozinke.
Maksimum veličine unosa	1.3.18.0.2.32.51	Koristi se za rješavanje sukoba replikacije. Na temelju tog broja, dobavljač može odlučiti trebali se neki unos ponovno dodati ciljnom poslužitelju kako bi se riješio sukob replikacije.
LostAndFound datoteka dnevnika	1.3.18.0.2.32.52	Datoteka koja arhivira zamijenjene unose kao rezultat rezolucije sukoba replikacije.
Upravljanje dnevnikom	1.3.18.0.2.32.41	Pokazuje podršku za proširene operacije pristupa datoteci dnevnika i za Tivoli Directory Server dnevnik revizije.
Višenitna replikacija	1.3.18.0.2.32.42	
Konfiguracija poslužitelja dobavljača za replikaciju	1.3.18.0.2.32.43	
IBMPolicies podstabla replikacije	1.3.18.0.2.32.18	Podržava replikaciju za cn=ibmpolicies i cn=shema pomoću cn=ibmpolicies podstabla.

OID-i za ACL mehanizme

Sljedeća tablica prikazuje OID-e za ACL mehanizme.

Tablica 11. OID-i za ACL mehanizme

Ime	OID	Opis
IBM SecureWay V3.2 ACL Model	1.3.18.0.2.26.2	Označuje da LDAP poslužitelj podržava IBM SecureWay V3.2 ACL model
IBM ACL Mehanizam baziran na filteru	1.3.18.0.2.26.3	Označuje da LDAP poslužitelj podržava IBM Poslužitelj direktorija v5.1 filter bazirani ACL
Sistemski ograničena ACL podrška	1.3.18.0.2.26.4	Označuje da poslužitelj podržava sistemsku i ograničenu klasu pristupa u ACL unosima.

Srodni koncepti

"Kontrole i proširene operacije" na stranici 90
Kontrole i proširene operacije dozvoljavaju LDAP protokolu da bude proširen bez promjene samog protokola.

Jednakost IBM Tivoli Directory Server

Directory Server kompatibilan je s proizvodom IBM Tivoli Directory Servera dostupnog na drugim platformama. Sljedeća tablica ispisuje jednakovrijednu verziju proizvoda IBM Tivoli Directory Servera koji odgovara određenim verzijama i5/OS Directory Servera. Ta bi tablica mogla biti korisna kod određivanja zadovoljava li i5/OS Directory Server preduvjete directory servera za određen proizvod.

Tablica 12. Jednakost IBM Tivoli Directory Server

i5/OS Directory Server	IBM Tivoli Directory Server
Verzija 6 izdanje 1	Verzija 6.0 IBM Tivoli Directory Servera
Verzija 5 izdanje 4	Verzija 5.2 IBM Tivoli Directory Servera
Verzija 5 izdanje 3	Verzija 5.1 IBM Directory Servera
Verzija 5 izdanje 2 (s PTF SI08487)	Verzija 4.1 IBM Directory Servera
Verzija 5 izdanje 2 (GA)	Verzija 3.2.2IBM SecureWay Directory Servera

Default konfiguracija za Directory Server

Directory Server se automatski instalira kad instalirate i5/OS. Ta instalacija uključuje default konfiguraciju.

Poslužitelj direktorija koristi default konfiguraciju kada je sve od sljedećeg istina:

- Administratori nisu pokrenuli čarobnjak konfiguracije za Directory Server ili zamijenili postavke direktorija sa stranicama svojstava.
- Izdavanje Directory Servera nije konfigurirano.
- Poslužitelj direktorija ne može pronaći bilo koje LDAP DNS informacije.

Ako Poslužitelj direktorija koristi default konfiguraciju, onda dolazi do sljedećeg:

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

Srodni zadaci

“Konfiguriranje Directory Servera” na stranici 97
Pokrenite čarobnjaka konfiguracije Directory Servera za prilagođavanje postavki Directory Servera.

Directory Server rješavanja problema

Informacije koje će vam pomoći da riješite probleme. Sadrži prijedloge za skupljanje servisnih podataka i rješavanje određenih problema.

Nažalost, čak i pouzdani poslužitelji poput Directory Server katkada imaju problema. Kada vaš Poslužitelj direktorija ima probleme, sljedeće informacije vam mogu pomoći da utvrdite u čemu je problem i kako ga ispraviti.

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

Za dodatne informacije o zajedničkim problemima Directory Servera, pogledajte početnu stranicu Directory Servera (www.iseries.ibm.com/ldap).

Directory Server koristi nekoliko Structured Query Language (SQL) poslužitelja koji su QSQSRVR poslovi. Kad dođe do neke SQL greške, QDIRSRV dnevnik posla će obično sadržavati sljedeću poruku:

```
desila se SQL greška -1
```

U tim slučajevima će vas dnevnik posla QDIRSRV uputiti na dnevnike posla SQL poslužitelja. Međutim, u nekim slučajevima QDIRSRV možda neće sadržavati ovu poruku i ovu preporuku, čak i ako je SQL poslužitelj uzrok problema. U tom slučaju je dobro da znate koje je poslove SQL poslužitelja pokrenuo poslužitelj, tako da znate u kojim QSQSRVR dnevnicima posla treba tražiti dodatne greške.

Kada se Poslužitelj direktorija normalno pokrene, on generira poruku koje je slična sljedećem:

```
                                                    System:   MYSYSTEM
 Posao . :   QDIRSRV       Korisnik :   QDIRSRV       Broj . . . . :   174440

  >> CALL PGM(QSYS/QGLDSVR)
     Posao 057448/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057340/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057448/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057166/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Posao 057279/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
   Posao 057288/QUSER/QSQSRVR korišten za obradu u načinu SQL poslužitelja.
     Poslužitelj direktorija se je uspješno pokrenuo.
```

Poruke se odnose na QSQSRVR poslove koji su bili pokrenuti za poslužitelj. Broj poruka se može razlikovati na vašem poslužitelju ovisno o konfiguraciji i broju QSQSRVR poslova potrebnih za postizanje pokretanja poslužitelja.

Na directory serverima **Baza podataka/Sufiksi** stranica Svojstva u System i Navigator specificirajte ukupan broj SQL poslužitelja koje Directory Server koristi za operacije direktorija nakon pokretanja poslužitelja. Dodatni SQL poslužitelji su pokrenuti za replikaciju.

Srodne informacije

Directory Server početna stranica

Nadgledanje grešaka i pristupa s dnevnikom posla Directory Servera

Kada se pojavi greška na vašem Poslužitelju direktorija i želite više detalja, druga akcija koju možete poduzeti je pregledavanje QDIRSRV dnevnika posla.

Pregledavanje dnevnika posla za vaš Poslužitelj direktorija vas može upozoriti na greške i pomoći vam da nadgledate pristupanje poslužitelju. Dnevnik posla sadrži:

- Poruke o operacijama poslužitelja i sve probleme unutar poslužitelja kao što su poslovi SQL poslužitelja ili neuspješne replikacije.
- Poruke koje se odnose na sigurnost, a koje odražavaju operacije klijenta kao što su krive lozinke.
- Poruke koje sadrže detalje o greškama klijenta kao što je nedostajanje potrebnih atributa.

Možda nećete htjeti zapisivati greške klijenta osim ako ne pokušavate otkriti probleme klijenta. Možete kontrolirati zapisivanje grešaka klijenta na karticu svojstava **Općenito** Directory Servera u System i Navigator.

Pregledajte QDIRSRV dnevnik posla ako je poslužitelj pokrenut

Ako je poslužitelj pokrenut, a želite pogledati QDIRSRV dnevnik posla, poduzmite ove korake:

1. U System i Navigator, proširite **Mreža**.
2. Proširite **Poslužitelji**.
3. Kliknite **TCP/IP**.
4. Desno kliknite na **IBM poslužitelj direktorija** i izaberite **Poslovi poslužitelja**.
5. Iz izbornika **Datoteka**, izaberite **Dnevnik posla**.

Pregledajte QDIRSRV dnevnik posla ako je poslužitelj zaustavljen

Ako je poslužitelj zaustavljen, a želite pogledati QDIRSRV dnevnik posla, poduzmite ove korake:

1. U System i Navigator, proširite **Osnovne operacije**.
2. Kliknite **Izlaz pisača**.
3. QDIRSRV se pojavljuje u **User** stupcu System i Navigator desnog panela. Da bi pregledali dnevnik posla, dva puta kliknite **Qpjoblog** s lijeve strane od QDIRSRV u istom redu.

   Bilješka: System i Navigator može biti konfigurirano da prikazuje samo spool datoteke. Ako se QDIRSRV ne pojavljuje na listi, kliknite **Izlaz pisača**, onda izaberite **Uključi** iz **Opcije** izbornika. Navedite **Sve** u polju **Korisnik**, a zatim kliknite **OK**.

Bilješka: Directory Server koristi druge sistemske resurse za izvođenje zadataka. Ako dođe do greške kod jednog od tih resursa, u dnevniku posla će biti naznačeno kamo ići po potrebne informacije. U nekim slučajevima Directory Server možda neće moći odrediti kamo gledati. U tim slučajevima, pogledajte poslužiteljev Structured Query Language (SQL) dnevnik posla da vidite je li problem vezan za SQL poslužitelje.

Upotreba TRCTCPAPP za pomoć pronalaženja problema

Kod grešaka koje se ponavljaju, možete koristiti naredbu Prati TCP/IP aplikacije (TRCTCPAPP APP(*DIRSRV)) kako bi pratili greške.

Vaš poslužitelj daje komunikacijsko praćenje za skupljanje podataka na komunikacijskoj liniji, kao što je sučelje mreže lokalnog područja (LAN) ili mreže širokog područja (WAN). Prosječan korisnik možda neće shvatiti cijeli sadržaj podataka praćenja. Ipak, morate koristiti unose praćenja da odredite je li bilo izmjene podataka između dvije točke.

| Naredna Prati TCP/IP aplikaciju (TRCTCPAPP) može se koristiti na Directory Server-u za pomoć u pronalaženju
| problema s klijentima ili aplikacijama.

| Možete koristiti naredbu TRCTCPAPP za praćenje aktivne instance poslužitelja. Na primjer:

| TRCTCPAPP APP(*DIRSRV) INSTANCE(QUSRDIR)

| Možete također početi praćenje pomoću naredbe STRTCPSVR i dodavanjem '-h dft' vrijednosti startup instance. To će
| pokrenuti praćenje u instanci poslužitelja i pokrenuti instancu poslužitelja. Na primjer:

| STRTCPSVR SERVER(*DIRSRV) INSTANCE(QUSRDIR '-h dft')

| Za završetak praćenja koristite sljedeću naredbu:

| TRCTCPAPP APP(*DIRSRV) SET(*OFF)

Srodni koncepti

Praćenje komunikacija

Srodne informacije

Praćenje TCP/IP aplikacija (TRCTCPAPP)

Upotreba opcije LDAP_OPT_DEBUG za praćenje grešaka

Pratite probleme s klijentima koji koriste LDAP C API-je.

Možete koristiti LDAP_OPT_DEBUG opciju **ldap_set_option()** API-ja kako bi pratili probleme s klijentima koji koriste LDAP C API-je. Debug opcija ima višestruke razine debug postavki koje možete koristiti kao pomoć u uklanjanju problema s ovim aplikacijama.

Sljedeće je primjer omogućavanja klijentske debug opcije praćenja.

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

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

Primjer omogućavanja praćenja klijenta korištenjem LDAP_DEBUG varijable okruženja je sljedeći:

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

Nakon pokretanja klijenta koji proizvodi problem koji imate, upišite sljedeće u red za naredbe:

```
DMPUSRTRC  ClientJobNumber
```

gdje je ClientJobNumber broj posla klijenta.

Za interaktivni prikaz ove informacije, upišite sljedeće u red za naredbe:

```
DSPPFM QAP0ZDMP QP0Znnnnnn
```

gdje QAP0ZDMP sadrži nulu, a nnnnnn je broj posla.

Da sačuvate ove informacije za njihovo slanje servisu, poduzmite sljedeće korake:

1. Kreirajte SAVF datoteku koristeći naredbu kreiranje SAVF (CRTSAVF).
2. Upišite sljedeće u red za naredbe.

   ```
   SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
   ```

   gdje QAP0ZDMP sadrži nulu, a *xxx* je ime koje ste specificirali za SAVF datoteku.

Srodni koncepti

Lightweight Directory Access Protocol (LDAP) API-ji
Pogledajte Lightweight Directory Access Protocol (LDAP) API-je za više informacija o API-jima Directory Servera.

Srodne informacije

Dodavanje varijable okoline (ADDENVVAR)

Dump praćenja korisnika (DMPUSRTRC)

Prikaz člana fizičke datoteke (DSPPFM)

Kreiranje datoteke spremanja (CRTSAVF)

Spremanje objekta (SAVOBJ)

Identifikatori GLEnnnn poruka

Ova informacija ispisuje identifikatore GLE poruka i njihove opise.

Identifikatori poruka uzimaju formu GLEnnnn, gdje je nnnn decimalni broj greške. Na primjer, opis povratnog koda 50 (0x32) može biti pregledan unošenjem sljedeće naredbe:

```
| DSPMSGD RANGE(GLE0050) MSGF(QGLDMSG)
```

Ovo bi vam dalo opis za LDAP_INSUFFICIENT_ACCESS.

Sljedeća tablica ispisuje GLE identifikatore poruka i njihove opise.

Identifikatori poruka	Opis
GLE0000	Zahtjev je bio uspješan (LDAP_SUCCESS)
GLE0001	Operacijska greška (LDAP_OPERATIONS_ERROR)

Identifikatori poruka	Opis
GLE0002	Protokolarna greška (LDAP_PROTOCOL_ERROR)
GLE0003	Vremensko ograničenje premašeno (LDAP_TIMELIMIT_EXCEEDED)
GLE0004	Ograničenje veličine premašeno (LDAP_SIZELIMIT_EXCEEDED)
GLE0005	Uspoređeni tip i vrijednost ne postoji u unosu (LDAP_COMPARE_FALSE)
GLE0006	Uspoređeni tip i vrijednost postoji u unosu (LDAP_COMPARE_TRUE)
GLE0007	Metoda provjere autentičnosti nije podržana (LDAP_AUTH_METHOD_NOT_SUPPORTED)
GLE0008	Jaka provjera autentičnosti potrebna (LDAP_STRONG_AUTH_REQUIRED)
GLE0009	Primljeni parcijalni rezultati (LDAP_PARTIAL_RESULTS)
GLE0010	Vraćena preporuka (LDAP_REFERRAL)
GLE0011	Administrativna granica premašena (LDAP_ADMIN_LIMIT_EXCEEDED)
GLE0012	Kritična ekstenzija nije podržana (LDAP_UNAVAILABLE_CRITICAL_EXTENSION)
GLE0013	Potrebna je tajnost (LDAP_CONFIDENTIALITY_REQUIRED)
GLE0014	SASL vezanje u toku (LDAP_SASLBIND_IN_PROGRESS)
GLE0016	Nema takvog atributa (LDAP_NO_SUCH_ATTRIBUTE)
GLE0017	Nedefinirani tip atributa (LDAP_UNDEFINED_TYPE)
GLE0018	Neodgovarajuće uparivanje (LDAP_INAPPROPRIATE_MATCHING)
GLE0019	Povreda ograničenja (LDAP_CONSTRAINT_VIOLATION)
GLE0020	Tip ili vrijednost postoji (LDAP_TYPE_OR_VALUE_EXISTS)
GLE0021	Nevažeća sintaksa (LDAP_INVALID_SYNTAX)
GLE0032	Nema takvog objekta (LDAP_NO_SUCH_OBJECT)
GLE0033	Problem s aliasom (LDAP_ALIAS_PROBLEM)
GLE0034	Nevažeća DN sintaksa (LDAP_INVALID_DN_SYNTAX)
GLE0035	Objekt je list (LDAP_IS_LEAF)
GLE0036	Problem s dereferenciranjem aliasa (LDAP_ALIAS_DEREF_PROBLEM)
GLE0048	Neodgovarajuća provjera autentičnosti (LDAP_INAPPROPRIATE_AUTH)
GLE0049	Nevažeće vjerodajnice (LDAP_INVALID_CREDENTIALS)
GLE0050	Nedovoljan pristup (LDAP_INSUFFICIENT_ACCESS)
GLE0051	Poslužitelj direktorija je zauzet (LDAP_BUSY)
GLE0052	Agent servisa direktorija je nedostupan (LDAP_UNAVAILABLE)
GLE0053	Poslužitelj direktorija nije voljan izvesti zahtijevanu operaciju (LDAP_UNWILLING_TO_PERFORM)
GLE0054	Otkrivena petlja (LDAP_LOOP_DETECT)
LE0064	Prekršaj imenovanja (LDAP_NAMING_VIOLATION)

Identifikatori poruka	Opis
LE0065	Prekršaj objekta klase (LDAP_OBJECT_CLASS_VIOLATION)
GLE0066	Operacija nije dozvoljena na objektu koji nije list (LDAP_NOT_ALLOWED_ON_NONLEAF)
GLE0067	Operacija nije dozvoljena na relativnom razlikovnom imenu (LDAP_NOT_ALLOWED_ON_RDN)
GLE0068	Već postoji (LDAP_ALREADY_EXISTS)
GLE0069	Ne mogu modificirati objekt klase (LDAP_NO_OBJECT_CLASS_MODS)
GLE0070	Rezultati preveliki (LDAP_RESULTS_TOO_LARGE)
GLE0071	Utječe na višestruke poslužitelje. (LDAP_AFFECTS_MULTIPLE_DSAS)
GLE0080	Nepoznata greška (LDAP_OTHER)
GLE0081	Ne mogu kontaktirati LDAP poslužitelj (LDAP_SERVER_DOWN)
GLE0082	Lokalna greška (LDAP_LOCAL_ERROR)
GLE0083	Greška u kodiranju (LDAP_ENCODING_ERROR)
GLE0084	Greška u dekodiranju (LDAP_DECODING_ERROR)
GLE0085	Zahtjev napravio vremensko prekoračenje (LDAP_TIMEOUT)
GLE0086	Nepoznata metoda provjere autentičnosti (LDAP_AUTH_UNKNOWN)
GLE0087	Loš filter pretraživanja (LDAP_FILTER_ERROR)
GLE0088	Korisnik opozvao operaciju (LDAP_USER_CANCELLED)
GLE0089	Loš parametar LDAP rutini (LDAP_PARAM_ERROR)
GLE0090	Nema memorije (LDAP_NO_MEMORY)
GLE0091	Greška u povezivanju (LDAP_CONNECT_ERROR)
GLE0092	Značajka nije podržana (LDAP_NOT_SUPPORTED)
GLE0093	Kontrola nije nađena (LDAP_CONTROL_NOT_FOUND)
GLE0094	Rezultati nisu vraćeni (LDAP_NO_RESULTS_RETURNED)
GLE0095	Još rezultata treba vratiti (LDAP_MORE_RESULTS_TO_RETURN)
GLE0096	Nije LDAP URL (LDAP_URL_ERR_NOTLDAP)
GLE0097	URL nema DN (LDAP_URL_ERR_NODN)
GLE0098	URL opseg vrijednosti nije važeći (LDAP_URL_ERR_BADSCOPE)
GLE0099	Greška u dodjeljivanju memorije (LDAP_URL_ERR_MEM)
GLE0100	Klijentska petlja (LDAP_CLIENT_LOOP)
GLE0101	Dosegnuta granica (LDAP_REFERRAL_LIMIT_EXCEEDED)
GLE0112	SSL okruženje već inicijalizirano (LDAP_SSL_ALREADY_INITIALIZED)
GLE0113	Poziv inicijalizacije nije uspio (LDAP_SSL_INITIALIZE_FAILED)
GLE0114	SSL okruženje nije inicijalizirano (LDAP_SSL_CLIENT_INIT_NOT_CALLED)

Identifikatori poruka	Opis
GLE0115	Ilegalna vrijednost SSL parametra (LDAP_SSL_PARAM_ERROR)
GLE0116	Neuspjeh u dogovaranju sigurne veze (LDAP_SSL_HANDSHAKE_FAILED)
GLE0118	SSL knjižnica nije pronađena (LDAP_SSL_NOT_AVAILABLE)
GLE0128	Nije pronađen izričit vlasnik (LDAP_NO_EXPLICIT_OWNER)
GLE0129	Ne mogu dobiti zaključavanje na potrebnim resursima (LDAP_NO_LOCK)
GLE0133	Nema LDAP poslužitelja u DNS (LDAP_DNS_NO_SERVERS)
GLE0134	Skraćeni DNS rezultati (LDAP_DNS_TRUNCATED)
GLE0135	Ne mogu raščlaniti DNS podatke (LDAP_DNS_INVALID_DATA)
GLE0136	Ne mogu riješiti domenu sistema ili DNS (LDAP_DNS_RESOLVE_ERROR)
GLE0137	DNS greška konfiguracijske datoteke (LDAP_DNS_CONF_FILE_ERROR)
GLE0160	Pretek izlaznog međuspremnika (LDAP_XLATE_E2BIG)
GLE0161	Skraćen ulazni međuspremnik (LDAP_XLATE_EINVAL)
GLE0162	Neupotrebljiv ulazni znak (LDAP_XLATE_EILSEQ)
GLE0163	Znak se ne mapira na točku kodne stranice (LDAP_XLATE_NO_ENTRY)

Srodne informacije

Prikaz opisa poruke (DSPMSGD)

Uobičajene greške na LDAP klijentu

Ova informacija opisuje zajedničke greške LDAP klijenta.

Poznavanje uzroka uobičajenih grešaka na LDAP klijentu vam može pomoći da riješite probleme sa svojim poslužiteljem. Za potpunu lista uvjeta greške LDAP klijenta, pogledajte “API-ji Directory Servera” u zbirci poglavlja Programiranje.

Poruke o greškama na klijentu imaju sljedeći format:

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

Bilješka: Objašnjenje tih grešaka pretpostavlja da klijent komunicira s LDAP poslužiteljem na i5/OS. Klijent koji s poslužiteljem komunicira na nekoj drugoj platformi može dobiti slične greške, ali će uzroci i rješenja najvjerojatnije biti drugačiji.

Srodni koncepti

Lightweight Directory Access Protocol (LDAP) API-ji
Pogledajte Lightweight Directory Access Protocol (LDAP) API-je za više informacija o API-jima Directory Servera.

ldap_search: Premašena vremenska granica

Ova se greška dešava kad se ldapsearch naredba sporo izvodi.

Ako ispravljate ovu grešku, napravite jednu od sljedećih stvari ili obje:

- Povećajte ograničenje vremena pretraživanja za Poslužitelj direktorija.

- Smanjite aktivnost na vašem sistemu. Možete i smanjiti broj aktivnih poslova LDAP klijenta koji se izvode.

Srodni zadaci

"Prilagođavanje postavki pretraživanja" na stranici 122
Koristite ovu informaciju za kontroliranje korisničkih sposobnosti pretraživanja.

[Neuspjela LDAP operacija]: Greška operacije

Ovu grešku može generirati nekoliko stvari.

Za dobivanje informacija o uzroku ove greške za određenu instancu, pogledajte dnevnike posla QDIRSRV i dnevnike posla poslužitelja Structured Query Language (SQL).

Srodni koncepti

"Directory Server rješavanja problema" na stranici 290
Informacije koje će vam pomoći da riješite probleme. Sadrži prijedloge za skupljanje servisnih podataka i rješavanje određenih problema.

Srodni zadaci

"Nadgledanje grešaka i pristupa s dnevnikom posla Directory Servera" na stranici 291
Kada se pojavi greška na vašem Poslužitelju direktorija i želite više detalja, druga akcija koju možete poduzeti je pregledavanje QDIRSRV dnevnika posla.

ldap_bind: Nema takvog objekta

Uobičajeni uzrok ove greške je da korisnik radi grešku upisivanja pri izvođenju operacije.

Drugi uobičajeni uzrok je kad se LDAP poslužitelj pokušava povezati s DN koji ne postoji. Ovo se često dešava kad korisnik navodi ono što pogrešno misli da je administratorov DN. Na primjer, korisnik može specificirati QSECOFR ili Administrator, kada stvarni administrator DN može biti nešto kao cn=Administrator.

Za detalje o grešci, pogledajte dnevnik posla QDIRSRV.

Srodni zadaci

"Nadgledanje grešaka i pristupa s dnevnikom posla Directory Servera" na stranici 291
Kada se pojavi greška na vašem Poslužitelju direktorija i želite više detalja, druga akcija koju možete poduzeti je pregledavanje QDIRSRV dnevnika posla.

ldap_bind: Neodgovarajuća provjera autentičnosti

Poslužitelj vraća nevažeće vjerodajnice kad je lozinka ili DN veza netočna.

Poslužitelj vraća neodgovarajuća provjera autentičnosti kad se klijent pokušava povezati kao jedno od sljedećeg:

- Unos koji nema atribut korisničke lozinke.
- Unos koji predstavlja i5/OS korisnika, koji ima UID atribut, a ne atribut korisničke lozinke. Zbog toga je potrebna usporedba između specificirane lozinke i i5/OS korisničke lozinke, koje se ne podudaraju.
- Unos koji predstavlja projiciranog korisnika i način povezivanja različit od zahtijevanog.

Ova greška se obično pojavi kad klijent pokušava povezivanje s lozinkom koja nije valjana. Za dobivanje detalja o grešci, pogledajte dnevnik posla QDIRSRV.

Srodni zadaci

"Nadgledanje grešaka i pristupa s dnevnikom posla Directory Servera" na stranici 291
Kada se pojavi greška na vašem Poslužitelju direktorija i želite više detalja, druga akcija koju možete poduzeti je pregledavanje QDIRSRV dnevnika posla.

[Neuspjela LDAP operacija]: Nedovoljan pristup

Ova se greška obično pojavi kad DN koji se povezuje nema ovlaštenje za izvođenje operacije (kao što je dodavanje ili brisanje) koju zahtijeva klijent.

Za dobivanje informacija o grešci, pogledajte dnevnik posla QDIRSRV.

Srodni zadaci

"Nadgledanje grešaka i pristupa s dnevnikom posla Directory Servera" na stranici 291
Kada se pojavi greška na vašem Poslužitelju direktorija i želite više detalja, druga akcija koju možete poduzeti je pregledavanje QDIRSRV dnevnika posla.

[Neuspjela LDAP operacija]: Ne može se kontaktirati LDAP poslužitelj

Najuobičajeniji uzroci te greške uključuju zahtjev prije nego što je poslužitelj spreman ili je broj porta nevažeći.

Najuobičajeniji uzroci ove greške obuhvaćaju sljedeće:

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

Za dobivanje informacija o grešci, pogledajte dnevnik posla QDIRSRV. Ako je Poslužitelj direktorija uspješno pokrenut, poruka da je Poslužitelj direktorija uspješno pokrenut će biti u QDIRSRV dnevniku posla.

Srodni zadaci

"Nadgledanje grešaka i pristupa s dnevnikom posla Directory Servera" na stranici 291
Kada se pojavi greška na vašem Poslužitelju direktorija i želite više detalja, druga akcija koju možete poduzeti je pregledavanje QDIRSRV dnevnika posla.

[Neuspjeh u LDAP operaciji]: Neuspjeh u povezivanju na SSL poslužitelj

Ova greška se javlja kad LDAP poslužitelj odbije spajanje klijenta zato što se ne može uspostaviti SSL veza.

To može biti uzrokovano nečim od sljedećeg:

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

Za i5/OS C aplikacije, dostupna je dodatna informacija o SSL grešci. Pogledajte "Directory Server API-i" u poglavlju Programiranje za detalje.

Srodni koncepti

Lightweight Directory Access Protocol (LDAP) API-ji
Pogledajte Lightweight Directory Access Protocol (LDAP) API-je za više informacija o API-jima Directory Servera.

Greške u vezi politike lozinki

Omogućavanje politike lozinke može ponekad uzrokovati neočekivane greške.

Kada su određene politike lozinke omogućene, one mogu uzrokovati kvarove koji možda nisu očiti. Pregledajte sljedeće radi pomoći u rješavanju problema povezanih s politikom lozinke.

Vezanje s odgovarajućom lozinkom ne uspijeva s ″nevažeće vjerodajnice″: Lozinka je možda istekla ili je račun zaključan. Pogledajte pwdchangedtime i pwdaccountlockedtime atribute unosa.

Zahtjevi ne uspijevaju s ″ne želim izvesti″ nakon uspješnog vezanja: Lozinka je možda ponovno postavljena, u kojem će slučaju vezanje uspjeti, ali jedina operacija koja je dozvoljena od strane poslužitelja je da korisnik promijeni lozinku. Drugi zahtjevi neće uspjeti s ″ne želim izvesti″ dok se lozinka ne promijeni.

Provjera autentičnosti s lozinkom koja je ponovno postavljena se ponaša neočekivano: Kada je lozinka ponovno postavljena, zahtjev za vezanjem će uspjeti, kao što je opisano iznad. To znači da će korisnik možda moći provjeriti autentičnost neograničeno dugo koristeći ponovno postavljenu lozinku.

Srodne reference

"Savjeti za politike lozinki" na stranici 78
Politika lozinka neće se uvijek ponašati kako se i očekuje.

Rješavanje problema QGLDCPYVL API

Korištenje svojstva Korisničkog praćenja može objasniti grešku ili utvrditi da li je servis potreban.

Ovaj API koristi Korisničko praćenje mogućnost za zapisivanje svojih operacija. Ako se dogode greške ili ako se sumnja na njih, praćenje može objasniti očitu grešku ili je potreban servis. Praćenje se može postići ovako:

```
STRTRC SSNID(COPYVLDL) JOBTRCTYPE(*TRCTYPE) TRCTYPE((*DIRSRV *INFO))
CALL QGLDCPYVL PARM(...)
ENDTRC SSNID(COPYVLDL) DTALIB(QTEMP) PRTTRC(*YES)
```

Da sačuvate ove informacije za njihovo slanje servisu, poduzmite sljedeće korake:

1. Kreirajte SAVF datoteku koristeći naredbu kreiranje SAVF (CRTSAVF).
2. Upišite sljedeće na prompt za naredbe.

   ```
   SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
   ```

   gdje QAP0ZDMP sadrži nulu, a *xxx* je ime koje ste specificirali za SAVF datoteku.

Srodni koncepti

Lightweight Directory Access Protocol (LDAP) API-ji
Pogledajte Lightweight Directory Access Protocol (LDAP) API-je za više informacija o API-jima Directory Servera.

Srodne informacije

Pokretanje praćenja (STRTRC)

Kreiranje datoteke spremanja (CRTSAVF)

Spremanje objekta (SAVOBJ)

Povezane informacije

Niže su popisane IBM Redbooks publikacije (u PDF formatu), Web stranice i poglavlja Informacijskog centar koji se odnose na poglavlje Directory Servera. Možete pregledati ili ispisati bilo koji od PDF-ova.

IBM Redbooks publikacije (www.redbooks.ibm.com)

- Razumijevanje LDAP-a, SG24-4986 .
- Korištenje LDAP za integraciju direktorija: Pogled u IBM SecureWay direktorij, aktivni direktorij i Domino, SG24-6163 .
- Implementacija i praktična upotreba LDAP-a na iSeries poslužitelju, SG24-6193 .

Web stranica

- IBM Directory Server za iSeries Web stranicu (www.ibm.com/servers/eserver/iseries/ldap)
- Web stranica vodiča Java imenovanje i sučelje direktorija (JNDI) (java.sun.com/products/jndi/tutorial/)

Ostale informacije

"API-ji protokola pristupa direktorija (LDAP) " u kategoriji Programiranje.

Dodatak. Napomene

Ove informacije su razvijene za proizvode i usluge koji se nude u SAD.

IBM možda ne nudi proizvode, usluge ili dodatke o kojima se raspravlja u ovom dokumentu u drugim zemljama. Za informacije o proizvodima i uslugama koji su trenutno dostupni u vašem području kontaktirajte vašeg lokalnog IBM predstavnika. Bilo koje upućivanje na neki IBM proizvod, program ili uslugu, nema namjeru tvrditi da se samo taj IBM proizvod, program ili usluga mogu koristiti. Bilo koji funkcionalno ekvivalentan proizvod, program ili usluga koji ne narušava nijedno IBM pravo na intelektualno vlasništvo, se može koristiti kao zamjena. Međutim, na korisniku je odgovornost da procijeni i provjeri rad bilo kojeg ne-IBM proizvoda, programa ili usluge.

IBM može imati patente ili molbe za patente koje su još u toku, a koje pokrivaju predmet o kojem se govori u ovom dokumentu. Posjedovanje ovog dokumenta ne daje vam nikakvu dozvolu za korištenje tih patenata. Možete poslati upit za licence, u pismenom obliku, na:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Za upite o licenci u vezi s dvobajtnim (DBCS) informacijama, kontaktirajte IBM odjel intelektualnog vlasništva u vašoj zemlji ili pošaljite upite, u pisanom obliku na adresu:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Sljedeći odlomak se ne primjenjuje na Ujedinjeno Kraljevstvo ili bilo koju drugu zemlju gdje su takve izjave nekonzistentne s lokalnim zakonima: INTERNATIONAL BUSINESS MACHINES CORPORATION DAJE OVU PUBLIKACIJU “KAKVA JE ”, BEZ IKAKVIH JAMSTAVA, BILO IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA O NE-POVREĐIVANJU, PROĐI NA TRŽIŠTU ILI SPOSOBNOSTI ZA ODREĐENU SVRHU. Neke zemlje ne dozvoljavaju odricanje od izravnih ili posrednih jamstava u određenim transakcijama, zbog toga, se ova izjava možda ne odnosi na vas.

Ove informacije mogu sadržavati tehničke netočnosti ili tipografske pogreške. Promjene se povremeno rade u ovim informacijama; te promjene će biti uključene u nova izdanja publikacije. IBM može raditi poboljšanja i/ili promjene u proizvodu(ima) i/ili programu/ima opisanim u ovoj publikaciji, bilo kad, bez prethodne obavijesti.

Bilo koje upućivanje u ovim informacijama na ne-IBM Web stranice, služi samo kao pomoć i ni na kakav način ne služi za promicanje tih Web stranica. Materijali na tim Web stranicama nisu dio materijala za ovaj IBM proizvod i upotreba tih Web stranica je na vaš osobni rizik.

IBM može koristiti ili distribuirati sve informacije koje vi dobavite, na bilo koji način za koji smatra da je prikladan i bez ikakvih obveza prema vama.

Vlasnici licence za ovaj program, koji žele imati informacije o njemu u svrhu omogućavanja: (i) izmjene informacija između neovisno kreiranih programa i drugih programa (uključujući i ovaj) i (ii) uzajamne upotrebe informacija koje su bile izmijenjene, trebaju kontaktirati:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Takve informacije mogu biti dostupne, uz odgovarajuće termine i uvjete, uključujući u nekim slučajevima i plaćanje pristojbe.

Licencni program opisan u ovim informacijama i sav licencni materijal koji je za njega dostupan IBM isporučuje pod uvjetima IBM Ugovora s korisnicima, IBM Internacionalnog ugovora o licenci za programe, IBM Ugovora o licenci za strojni kod ili bilo kojeg ekvivalentnog ugovora između nas.

Svi podaci o izvedbi koji su ovdje sadržani su utvrđeni u kontroliranoj okolini. Zbog toga se rezultati dobiveni u drugim operativnim okolinama mogu značajno razlikovati. Neka mjerenja su možda bila izvedena na sistemima na razvojnoj razini i ne postoji nikakvo jamstvo da će ta mjerenja biti ista na općenito dostupnim sistemima. Osim toga, neka mjerenja su možda bila procijenjena pomoću ekstrapolacije. Stvarni rezultati se mogu razlikovati. Korisnici ovog dokumenta bi trebali provjeriti primjenjive podatke za njihovo specifično okruženje.

Informacije koje se tiču ne-IBM proizvoda su dobivene od dobavljača tih proizvoda, njihovih objavljenih najava ili drugih dostupnih javnih izvora. IBM nije testirao te proizvode i ne može potvrditi koliko su točne tvrdnje o performansama, kompatibilnosti ili druge tvrdnje koje se odnose na ne-IBM proizvode. Pitanja o sposobnostima ne-IBM proizvoda bi trebala biti adresirana na dobavljače tih proizvoda.

Sve izjave koje se odnose na buduća usmjerenja ili namjere IBM-a su podložne promjenama i mogu se povući bez najave, a predstavljaju samo ciljeve i smjernice.

Sve pokazane IBM cijene su IBM-ove predložene maloprodajne cijene, trenutne su i podložne promjeni bez obavijesti. Cijene kod zastupnika se mogu razlikovati.

Ove informacije služe samo u svrhu planiranja. Ovdje sadržane informacije su podložne promjenama prije nego opisani proizvodi postanu dostupni.

Ove informacije sadrže primjere podataka i izvještaja koji se koriste u svakodnevnim operacijama. Da ih se što bolje objasni, primjeri uključuju imena pojedinaca, poduzeća, trgovačkih marki i proizvoda. Sva ta imena su izmišljena i svaka sličnost s imenima i adresama koja koriste stvarna poduzeća je potpuno slučajna.

LICENCA O AUTORSKOM PRAVU:

Ove informacije sadrže uzorke aplikativnih programa na izvornom jeziku, koji objašnjavaju tehnike programiranja na različitim operativnim platformama. Možete kopirati, modificirati i distribuirati te primjere programa u bilo kojem obliku, bez plaćanja IBM-u, za svrhe razvoja, upotrebe, marketinga ili distribucije aplikacijskih programa, u skladu sa sučeljem programiranja aplikacija za operativnu platformu za koju su primjeri programa napisani. Ti primjeri nisu temeljito testirani pod svim uvjetima. IBM, zbog toga, ne može jamčiti ili potvrditi pouzdanost, upotrebljivost ili funkcioniranje tih programa.

Ako gledate ove informacije kao nepostojanu kopiju, fotografije i slike u boji se možda neće vidjeti.

Zaštitni znaci

Sljedeći termini su zaštitni znaci International Business Machines Corporation u Sjedinjenim Državama, drugim zemljama ili oboje:

Application System/400
AS/400
DB2
Domino
e(logo)server
eServer

i5/OS
IBM
iSeries
Java
Lotus
Lotus Notes
Operating System/400
OS/400
Redbooks
RDN
SecureWay
System i
Tivoli
UNIX
WebSphere
XT
400

Adobe, Adobe logo, PostScript i PostScript logo su registrirani zaštitni znaci ili zaštitni znaci Adobe Systems Incorporated u Sjedinjenim Državama i/ili drugim zemljama.

Microsoft, Windows, Windows NT i Windows logo su zaštitni znaci Microsoft Corporation u Sjedinjenim Državama, drugim zemljama ili oboje.

Java i svi Java bazirani zaštitni znaci su zaštitni znaci Sun Microsystems, Inc. u Sjedinjenim Državama, drugim zemljama ili oboje.

UNIX je registrirani zaštitni znak The Open Group u Sjedinjenim Državama i drugim zemljama.

Ostala imena poduzeća, proizvoda i usluga mogu biti zaštitni znaci ili servisne oznake drugih.

Termini i uvjeti

Dozvole za upotrebu ovih publikacija se dodjeljuju prema sljedećim terminima i uvjetima.

Osobna upotreba: Možete reproducirati ove publikacije za vašu osobnu, nekomercijalnu upotrebu, uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete distribuirati, prikazivati ili raditi izvedena djela iz ovih publikacija ili bilo kojeg njihovog dijela, bez izričite suglasnosti IBM-a.

Komercijalna upotreba: Možete reproducirati, distribuirati i prikazivati ove publikacije samo unutar vašeg poduzeća uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete raditi izvedena dijela iz ovih publikacija ili kopirati, distribuirati ili prikazivati te publikacije ili bilo koji njihov dio izvan vašeg poduzeća, bez izričite suglasnosti IBM-a.

Osim kako je izričito dodijeljeno u ovoj dozvoli, nisu dane nikakve dozvole, licence ili prava, niti izričita niti posredna, na publikacije ili bilo koje podatke, softver ili bilo koje drugo intelektualno vlasništvo sadržano unutar.

IBM rezervira pravo da bilo kad, po vlastitom nahođenju, povuče ovdje dodijeljene dozvole, ako je upotreba publikacija štetna za njegove interese ili je ustanovljeno od strane IBM-a da gornje upute nisu bile ispravno slijeđene.

Ne smijete spustiti, eksportirati ili reeksportirati ove informacije, osim kod potpune usklađenosti sa svim primjenjivim zakonima i propisima, uključujući sve zakone i propise o izvozu Sjedinjenih Država.

IBM NE DAJE NIKAKVA JAMSTVA NA SADRŽAJ OVIH PUBLIKACIJA. PUBLIKACIJE SE DAJU ″KAKVE JESU″ I BEZ JAMSTAVA BILO KOJE VRSTE, IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA PROĐE NA TRŽIŠTU, NEKRŠENJA I PRIKLADNOSTI ZA ODREĐENU SVRHU.

Tiskano u Hrvatskoj