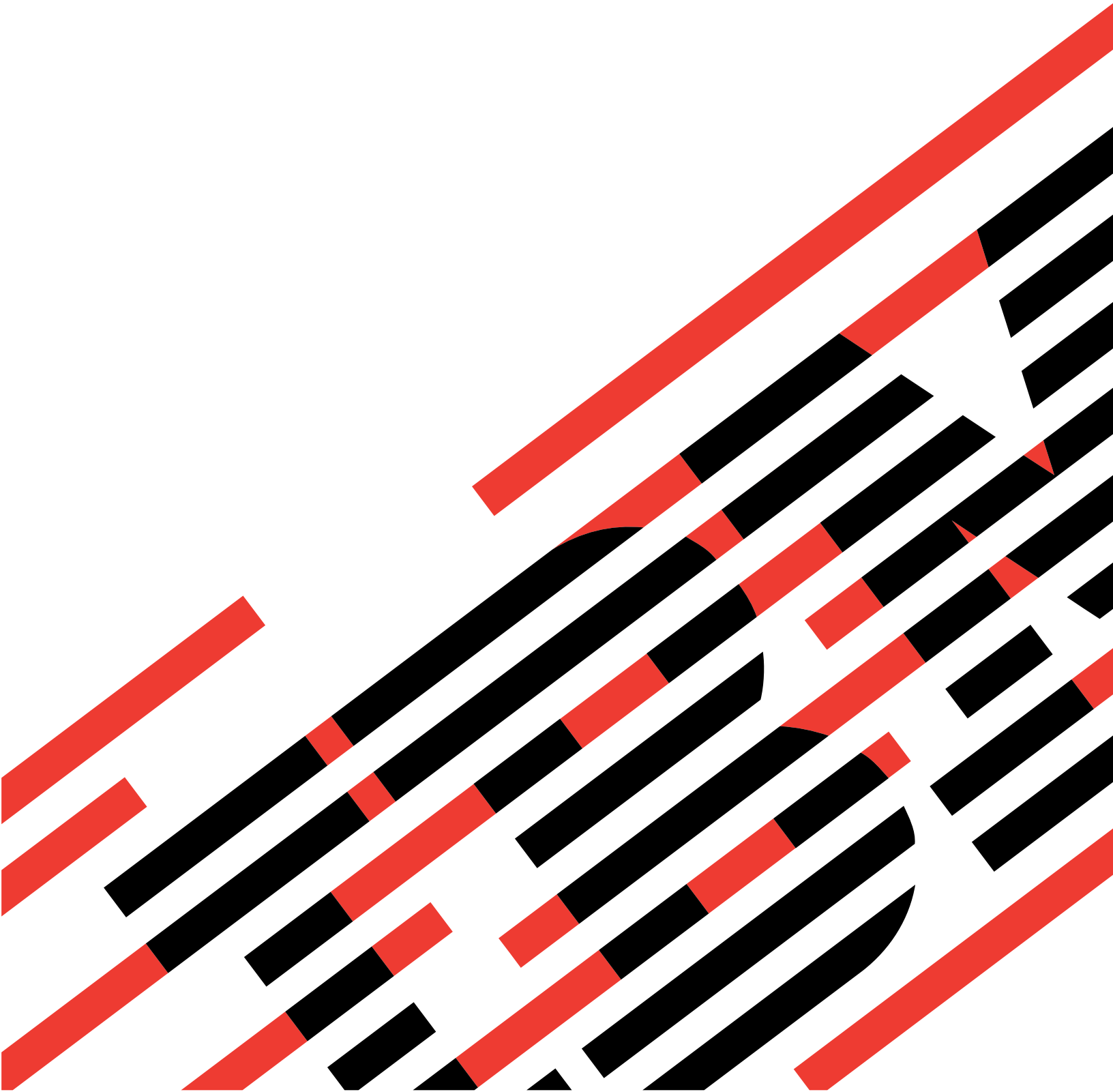
IBM Systems - iSeries

IBM Directory Server (LDAP)

Verzia 5 Vydanie 4



IBM Systems - iSeries

IBM Directory Server (LDAP)

Verzia 5 Vydanie 4

Poznámka

Pred použitím týchto informácií a produktu, ktorý podporujú, si prečítajte informácie v “Poznámky”, na strane 271 a v príručke *IBM eServer Safety Information,*.

Ôsme vydanie (Február 2006)

Toto vydanie platí pre verziu 5, vydanie 4, modifikáciu 0 operačného systému IBM i5/OS (číslo produktu 5722–SS1) a pre všetky nasledujúce vydania a modifikácie, pokiaľ sa v nových vydaniach neuvádza inak. Táto verzia nie je určená pre všetky modely RISC (reduced instruction set computer) ani pre všetky modely CISC.

Obsah

Kapitola 1. IBM Directory Server for iSeries (LDAP)

IBM Directory Server for iSeries (ďalej sa naň odkazuje ako na Adresárový server) je funkcia systému i5/OS, ktorú poskytuje server LDAP (Lightweight Directory Access Protocol) na serveri iSeries. LDAP sa spúšťa cez TCP/IP (Transmission Control Protocol/Internet Protocol) a je obľúbený ako adresárová služba pre internetové, aj neinternetové aplikácie.

V nasledujúcich témach nájdete informácie, ktoré vám pomôžu pochopiť a používať adresárový server na vašom serveri iSeries:

Kapitola 2. Novinky vo V5R4

Directory Server for iSeries má vo V5R4 nasledujúce vylepšenia a nové funkcie:

Replikácia

- **Replikácia pomocou brány:** K replikácii môže dôjsť cez replikačné siete použitím bránových serverov. Bránové servery môžu efektívnejšie zhromažďovať a distribuovať informácie počas zníženia prevádzky siete. Pozrite si ″Replikácia pomocou brány″ v "Prehľad replikácie" na strane 36.
- **cn=IBMpolicies:** Nový objekt kontajnera pre položky, ktoré sa majú zdieľať medzi replikačnými servermi. Kontajner cn=IBMpolicies pre položky, ktoré sa nereplikujú, obsahuje v porovnaní s cn=localhost, informácie podobné konfigurácii, ktoré bude pravdepodobne treba replikovať. Pozrite si "Prípona (názvový kontext)" na strane 14.

Zabezpečenie

- **Autentifikácia DIGEST-MD5** DIGEST-MD5 je mechanizmus autentifikácie SASL (simple authentication security layer). Keď klient používa Digest-MD5, heslo sa neodošle v čistom texte a protokol predíde náporom odpovedí. Pozrite si "Autentifikácia" na strane 69.
- **TLS (Transport layer security):** Bola pridaná rozšírená operácia StartTLS, ktorá má umožniť klientovi zaktualizovať nezabezpečené pripojenie na pripojenie zabezpečené pomocou TLS. Okrem toho, server podporuje AES 256-bitové TLS šifrovanie. Pozrite si "Secure Sockets Layer (SSL) a Transport Layer Security (TLS) s adresárovým serverom" na strane 47.

Hľadanie

- **Vyhľadávanie v podstrome na nulovom základe:** Všetky prípony zadefinované v konfiguračnom súbore možno vyhľadávať len s jednou požiadavkou na vyhľadávanie. Toto vylučuje potrebu viacerých vyhľadávaní (každé s inou príponou ako základom pre vyhľadávanie) na prehľadanie celého adresára. Pozrite si "Hľadanie položiek adresára" na strane 166.
- **Skupiny s limitmi vyhľadávania** Táto funkcia umožňuje správcovi priraďovať ku konkrétnym skupinám rôzne limity vyhľadávania okrem všeobecných limitov určených pre všetkých užívateľov. Správcom poskytuje pružnosť pri zisťovaní, kto má limity vyhľadávania na príslušnom serveri. Pozrite si "Parametre vyhľadávania" na strane 42.
- **Vylepšenia v spracovaní dereferencovania aliasov:** Výkon vyhľadávaní, ktoré používajú voľby dereferencovania, sa výrazne zlepší, ak adresár neobsahuje žiadne aliasy. Okrem toho existujú teraz voľby konfigurácie, ktoré majú nahradiť voľby dereferencovania špecifikované v požiadavkách klienta na vyhľadávanie. Pozrite si "Parametre vyhľadávania" na strane 42.
- **Cache pamäť atribútov:** Funkcia cache pamäte atribútov je vylepšenie výkonu rozlíšenia vyhľadávacieho filtra v pamäti namiesto vykonávania úvodného rozlíšenia v databáze a jeho uloženia do cache pamäte filtra. Cache pamäť atribútov na rozdiel od cache pamäte filtra sa nečistí pri každom vykonávaní operácie pridania, úpravy alebo vymazania LDAP. Keď je server nakonfigurovaný, automaticky upravuje cache pamäte atribútov v nakonfigurovaných časových intervaloch tieto atribúty ukladá do cache pamäte, čo bude najužitočnejšie v rámci maximálneho množstva nakonfigurovanej cache pamäte pre ukladanie atribútov do cache pamäte. Pozrite si "Pamäť cache atribútov" na strane 80.

Atribúty

- **Jedinečné atribúty:** Funkcia jedinečných atribútov zabezpečuje, že špecifikované atribúty budú mať v rámci adresára vždy jedinečné hodnoty. Napríklad, správca bude možno musieť špecifikovať, že atribút, ktorý ukladá čísla sociálneho zabezpečenia, musí byť jedinečný, pretože ni je možné, aby dve osoby mali rovnaké číslo. Pozrite si "Jedinečné atribúty" na strane 79.
- **Uchovanie operačných atribútov** Operačné atribúty creatorsName, createTimestamp, modifiersName a modifyTimestamp sa teraz replikujú na spotrebiteľské servery a importujú a exportujú sa do súborov LDIF. Pozrite si "Prevádzkové atribúty" na strane 79.

- **Jazykové značky:** Jazykové značky sú mechanizmy, ktoré umožňujú, aby adresár priraďoval kódy prirodzeného jazyka k hodnotám držaným v adresári a umožnil klientom vyžiadať dotazom od adresára hodnoty, ktoré spĺňajú určité požiadavky prirodzeného jazyka. Pozrite si “Jazykové značky” na strane 44.

Skupiny

- **Skupina užívateľov - administrátorov** Viaceré rozlišovacie názvy (DN) užívateľov môžu mať takmer rovnaké oprávnenie administrátora ako správca servera LDAP. Táto funkcia umožňuje viacerým užívateľom vykonávať administratívne úlohy bez toho, aby museli zdieľať ID a heslo užívateľa. Pozrite si “Administratívny prístup” na strane 54.
- **Autorizácia proxy:** Autorizácia proxy poskytuje klientovi LDAP spôsob pripojiť sa ako jeden užívateľ, ale k cieľovému adresáru pristupovať ako iný užívateľ. Toto poskytuje klientskym aplikáciám väčšiu flexibilitu, pretože môžu vykonávať operácie v zastúpení viacerých užívateľov bez toho, aby bolo treba každého užívateľa nanovo pripájať. Pozrite si “Autorizácia proxy” na strane 54.

Iné

- **Vylepšenia monitora:** Webový administračný nástroj sa teraz používa na zobrazovanie informácií o serveri a pripojení. V podpore monitora boli teraz vykonané nasledujúce vylepšenia:
  - Prevádzkyschopnosť a odmietnutie služby
    - Do výstupu monitora boli pridané nové informácie, ktoré majú zahrňovať súčty vykonaných operácií podľa typu (BIND, MODIFY, COMPARE, SEARCH atď.), hĺbku frontu prác, počet dostupných vlákien pracovníka, súčty správ pridaných do protokolu servera, protokol auditu, chyby CLI, súčty počtu pripojení cez SSL (secure sockets layer) aj pripojení cez TLS, informácie o neaktívnom pripojení a štatistiku núdzových vlákien.
    - Na vrátenie informácií o vláknach pracovníka sa poskytuje nová vyhľadávacia báza ″cn=workers,cn=monitor″.
  - Cache pamäť atribútov
    - Budú sa zaznamenávať informácie o cache pamäti a o atribútoch v nej uložených (nakonfigurovaná veľkosť, celková veľkosť, rýchlosť požiadaviek na prístup).
    - Na vrátenie informácií o cache pamäti atribútov pre protokol zmien sa použije nová vyhľadávacia báza ″cn=changelog,cn=monitor″.
- **Podpora pre klientske aplikácie na autentifikáciu ako aktuálny užívateľ:** Vylepšené sú pomocné programy klienta a príkazového riadka LDAP, ktoré budú podporovať autentifikovanie na lokálny adresárový server ako aktuálny užívateľ. Toto je obzvlášť užitočné v prípade vykonávania administratívnych úloh, ak je užívateľ prihlásený ako užívateľ i5/OS, ktorý má oprávnenie správcu na adresár.
- **Riadenia prístupov v systéme a obmedzených atribútoch:** Teraz môžete riadiť prístup k systému a obmedzeným atribútom súvisiaci s riadením prístupu a inými serverom riadenými atribútmi položiek LDAP.
- **Kopírovanie užívateľov vo validačnom zozname do adresára LDAP:** Adresárový server možno naplniť objektmi adresára na základe užívateľov zadefinovaných vo validačnom zozname štýlu HTTP. Okrem toho, adresárový server môže autentifikovať užívateľov na základe oprávnení skopírovaných z validačných zoznamov HTTP. Tento proces uľahčujú nové aplikačné programovacie rozhrania (API). Pozrite si “Kopírovanie užívateľov z validačného zoznamu servera HTTP na Adresárový server” na strane 92.
- **Odmietnutie služby a odpojenie pripojeného DN:** Nové vylepšenia umožňujú serveru identifikovať, obnovovať a vydržať mnoho foriem odmietnutia náporov služieb. Tieto vylepšenia zahrňujú poskytnutie väčšieho riadenia správcovi a automatické úpravy zo strany servera. Pozrite si “Odmietnutie služby” na strane 72.
- **Viac funkcií webovej administrácie:** Použitím webového administračného nástroja je možné vykonávať viac úloh. Väčšinu nových funkcií nájdete pod novou kategóriou **Server administration**.

Kapitola 3. PDF na tlač

Keď si chcete pozrieť alebo stiahnuť PDF verziu tohto dokumentu, vyberte Directory Server (LDAP) (okolo 2700 KB).

Ostatné informácie

Ak chcete zobraziť alebo tlačiť PDF súvisiacich príručiek a publikácií Redbook, pozrite si Kapitola 10, “Súvisiace informácie”, na strane 269.

Ukladanie súborov PDF

Keď chcete uložiť PDF súbor na vašej pracovnej stanici pre prezeranie alebo tlač:

1. Kliknite pravým tlačidlom myši na PDF súbor vo vašom prehliadači (kliknite pravým tlačidlom na hore uvedený odkaz).
2. Kliknite na voľbu, ktorá ukladá PDF lokálne.
3. Prejdite do adresára, v ktorom chcete uložiť PDF súbor.
4. Kliknite na **Uložiť**.

Stiahnutie Adobe Reader

Aby ste si mohli prezerať alebo tlačiť tieto PDF, musíte si na svoj systém nainštalovať program Adobe Reader.

Bezplatnú kópiu si môžete stiahnuť z webovej stránky Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Kapitola 4. Základné pojmy adresárového servera

Adresárový server implementuje špecifikácie IETF (Internet Engineering Task Force) LDAP V3. Zahrňuje aj vylepšenia pridané spoločnosťou IBM v oblastiach funkcií a výkonu. Táto verzia používa IBM DB2 Universal Database for iSeries ako záložnú pamäť na poskytnutie integrity transakcií, vysokovýkonných operácií a schopnosti online zálohovania a obnovy prostredníctvom operácie LDAP. Je kompatibilná s klientmi vyhovujúcim IETF LDAP V3. Koncepty a úvahy týkajúce sa adresárového servera nájdete v týchto častiach:

Adresáre

Adresárový server umožňuje prístup k typu databázy, ktorá ukladá informácie v hierarchickej štruktúre podobnej spôsobu, akým je usporiadaný integrovaný súborový systém i5/OS.

Ak je známy názov objektu, dajú sa získať jeho charakteristiky. Ak názov konkrétneho samostatného objektu nie je známy, je možné prehľadať adresár a získať zoznam objektov, ktoré vyhovujú určitej požiadavke. Adresáre sa zvyčajne prehľadávajú pomocou špecifického kritéria, nie len podľa preddefinovanej množiny kategórií.

Adresár je špecializovaná databáza s charakteristikami, ktoré ju odlišujú od relačných databáz so všeobecným účelom. Charakteristika adresára je, že sa k nemu pristupuje (čítanie alebo hľadanie) oveľa častejšie ako sa aktualizuje (zápis). Adresáre musia podporovať veľké množstvá požiadaviek o čítanie, preto sú zvyčajne optimalizované pre prístup na čítanie. Adresáre nie sú určené na poskytovanie toľkých funkcií, ako poskytujú všeobecné databázy, preto sa dajú zoptimalizovať na ekonomické poskytovanie rýchleho prístupu k údajom v adresári z viacerých aplikácií vo veľkých distribuovaných prostrediach.

Adresár môže byť centralizovaný alebo distribuovaný. Ak je adresár centralizovaný, na jednom mieste exituje jeden adresárový server (alebo klaster serverov), ktorý poskytuje prístup k adresáru. Ak je adresár distribuovaný, existuje viacero serverov, zvyčajne geograficky vzdialených, ktoré poskytujú prístup k adresáru.

Keď je adresár distribuovaný, informácie uložené v adresári sa dajú rozdeľovať a replikovať. Keď sú informácie rozdelené, každý adresárový server obsahuje jedinečnú neprekrývajúcu sa podmnožinu informácií. To znamená, že každá položka adresára je uložená len v jednom jedinom serveri. Technikou na rozdelenie adresára sú odvolávky LDAP. Odvolávky LDAP dovoľujú užívateľom smerovať požiadavky LDAP (Lightweight Directory Access Protocol) do rovnakých alebo odlišných priestorov názvov, uložených v inom (alebo rovnakom) serveri. Keď sa informácie replikujú, rovnaká položka adresára je uložená vo viac ako jednom serveri. V distribuovanom adresári je možné niektoré informácie rozdeliť a niektoré replikovať.

Model adresárového servera LDAP je založený na položkách (nazývané tiež objekty). Každá položka obsahuje jeden alebo viac atribútov, ako je názov, adresa a typ. Typy zvyčajne obsahujú mnemonické reťazce, napríklad cn pre bežný názov (common name) alebo mail pre e-mailové adresy.

Vzorový adresár v časti Obrázok 1 na strane 9 znázorňuje položku pre Tima Jonesa, ktorá obsahuje atribúty mail a telephoneNumber. Iné možné atribúty sú fax, title, sn (surname, priezvisko) a jpegPhoto.

Každý adresár má schému, ktorá je množina pravidiel určujúcich štruktúru a obsah adresára. Schému môžete zobraziť pomocou webového administratívneho nástroja. Viac informácií o schéme nájdete v časti “Schéma” na strane 15.

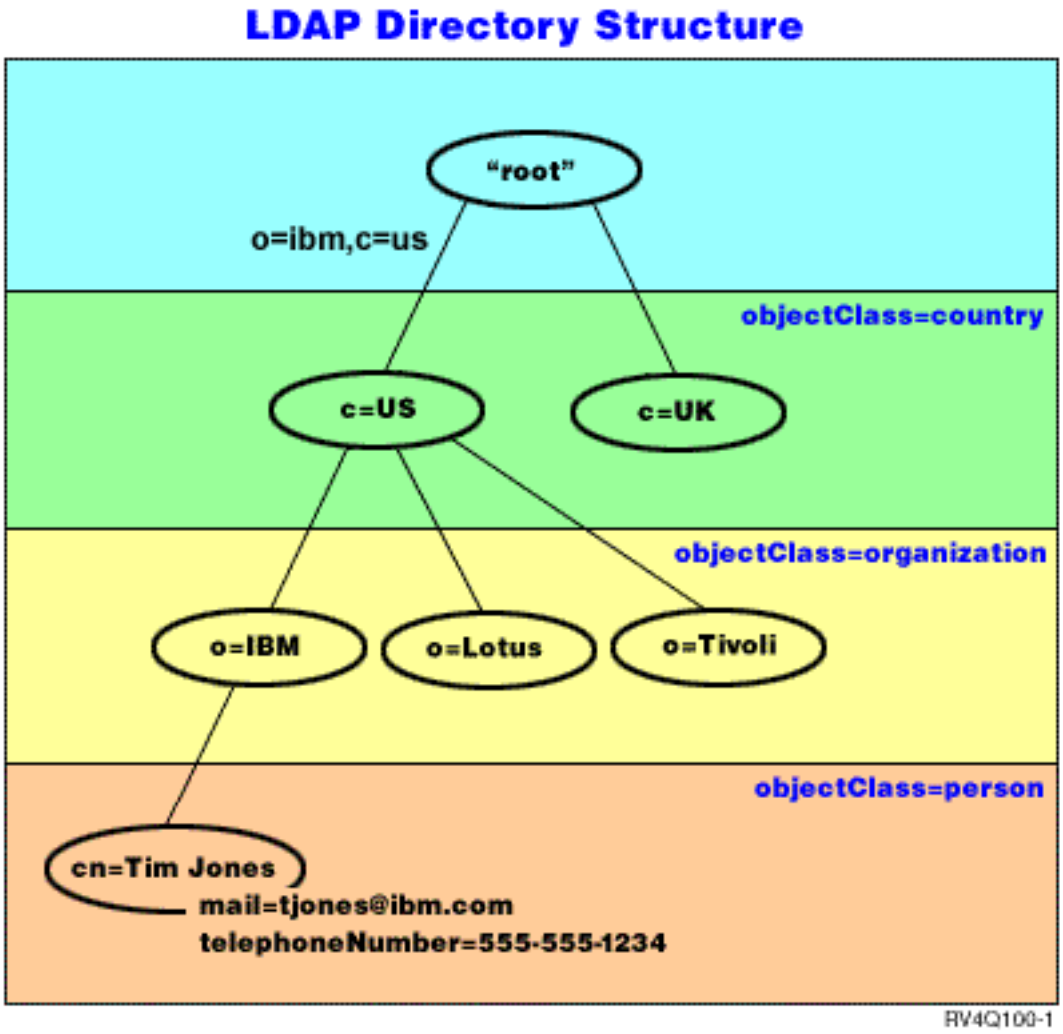
Každá položka adresára má špeciálny atribút nazvaný objectClass. Tento atribút kontroluje, ktoré atribúty položka požaduje a ktoré povoľuje. Inak povedané, hodnoty atribútu objectClass určujú pravidlá schémy, ktoré musí položka dodržať.

Okrem atribútov definovaných schémou, položky tiež majú množinu atribútov, ktoré udržiava server. Tieto atribúty, známe ako prevádzkové atribúty, zahŕňajú informácie ako čas vytvorenia položky a informácie o riadení prístupu. Viac informácií o prevádzkových atribútoch nájdete v časti “Prevádzkové atribúty” na strane 79.

Položky adresára LDAP sú bežne zoradené v hierarchickej štruktúre, ktorá rešpektuje politické, geografické a organizačné hranice (pozrite si časť Obrázok 1 na strane 9). Položky, ktoré reprezentujú krajiny alebo regióny sú zobrazené navrchu hierarchie. Položky predstavujúce štáty alebo národné organizácie sú pod nimi. Dole uvedené položky potom môžu predstavovať ľudí, organizačné jednotky, tlačiarne, dokumenty alebo iné položky.

LDAP narába s položkami pomocou rozlišovacích názvov (DN). Rozlišovacie názvy sa skladajú z názvu samotnej položky, ako aj z názvov v poradí zhora i nadol, z objektov nad nimi v adresári. Napríklad úplné DN pre položku v spodnom ľavom rohu v časti Obrázok 1 na strane 9 je cn=Tim Jones, o=IBM, c=US. Každý záznam má najmenej jeden atribút, ktorý sa používa na pomenovanie položky. Tento názvový atribút sa nazýva relatívny rozlišovací názov (RDN) položky. RDN dané vyššie uvedenej položke sa nazýva jej rodičovský rozlišovací názov. V príklade hore, cn=Tim Jones pomenúva položku, preto to je RDN. o=IBM, c=US je rodičovské DN pre cn=Tim Jones. Viac informácií o názvoch DN nájdete v časti “Rozlišovacie názvy (DN)” na strane 11.

Ak chcete dať adresárovému serveru možnosť riadiť adresár LDAP, v konfigurácii servera špecifikujte najvyššiu úroveň rodičovských rozlišovacích názvov (DN). Tieto rozlišovacie názvy sa nazývajú prípony. Server môže mať prístup k všetkým objektom v adresári, ktoré sú pod špecifickou príponou v hierarchii adresára. Napríklad, ak server LDAP obsahuje adresár zobrazený v časti Obrázok 1 na strane 9, vo svojej konfigurácii by mal mať príponu o=ibm, c=us, aby sa dalo odpovedať na dotazy klientov, týkajúce sa Tima Jonesa.



Obrázok 1. Štruktúra adresára LDAP

Nie ste obmedzený na tradičnú hierarchiu pri štruktúrovaní vášho adresára. Popularitu si získava napríklad štruktúra komponentu domény. Pri tejto štruktúre sa položky skladajú z častí názvov domén TCP/IP. Napríklad pre o=ibm,c=us môže byť vhodnejšie dc=ibm,dc=com.

Predpokladajme, že chcete vytvoriť adresár pomocou štruktúry komponentov domény, ktorý bude obsahovať údaje o zamestnancoch, ako sú mená, telefónne čísla a e-mailové adresy. Používate príponu alebo názvový kontext založený na doméne TCP/IP. Tento adresár sa dá vizualizovať takto:

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

Keď to zadáte do adresárového servera, tieto údaje môžu v skutočnosti vyzerať takto:

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

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

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

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

Všimnite si, že každá položka obsahuje hodnoty atribútov s názvom objectclass. Hodnoty objectclass definujú, ktoré atribúty sú dovolené v položke, napríklad telephonenumber alebo givenname. Dovolené triedy objektov sú definované v schéme. Schéma je množina pravidiel, ktoré definujú typ položiek dovolených v databáze.

Klienti a adresárové servery

K adresárom sa zvyčajne pristupuje modelom komunikácie typu klient/server. Procesy klienta a servera môžu a nemusia byť v rovnakom počítači. Server dokáže obsluhovať veľa klientov. Aplikácia, ktorá chce čítať alebo zapisovať informácie do adresára nemá priamy prístup k adresáru. Namiesto toho zavolá funkciu alebo aplikačné programové rozhranie (API), ktoré spôsobí odoslanie správy do iného procesu. Tento druhý proces sprístupní informácie v adresári v mene žiadajúcej aplikácie. Výsledky čítania alebo zápisu sa následne vrátia do žiadajúcej aplikácie.

API definuje programové rozhranie, ktoré konkrétny programovací jazyk používa na prístup k službe. Formát a obsah správ vymieňaných medzi klientom a serverom musí byť dohodnutý protokolom. LDAP definuje protokol správ, ktorý používajú klienti adresára aj adresárové servery. Existuje tiež združené LDAP API pre jazyk C a spôsoby prístupu k adresáru z Java aplikácie pomocou JNDI (Java Naming and Directory Interface).

Bezpečnosť adresára

Adresár by mal podporovať základné funkcie potrebné na implementáciu bezpečnostnej politiky. Adresár nemusí priamo poskytovať bezpečnostné funkcie z nižšej úrovne, ale môže byť integrovaný v bezpečnostnej službe

dôveryhodnej siete, ktorá poskytuje základné bezpečnostné služby. Ako prvá je potrebná metóda na autentifikovanie užívateľov. Autentifikácia kontroluje, že užívatelia sú tými, za koho sa vyhlasujú. Základnou autentifikačnou schémou je meno užívateľa a heslo. Keď sú užívatelia autentifikovaní, musí sa určiť, či majú autorizáciu alebo oprávnenie vykonať požadovanú operáciu na špecifickom objekte.

Autorizácia je často založená na zoznamoch riadenia prístupu (ACL). ACL je zoznam autorizácií, ktoré sa môžu pripojiť k objektom a atribútom v adresári. ACL uvádza, ktorý typ prístupu je povolený alebo zakázaný pre každého užívateľa alebo skupinu užívateľov. Za účelom skrátenia zoznamov ACL a zjednodušenia ich správy sa užívatelia s rovnakými prístupovými právami často vkladajú do skupín.

Rozlišovacie názvy (DN)

Každá položka v adresári má rozlišovací názov (DN). DN je názov, ktorý jedinečne identifikuje položku v adresári. DN je tvorené pármi atribút=hodnota, oddelenými čiarkami, napríklad:

```
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
```

Každý z atribútov, zadefinovaných v schéme adresárov, sa môže použiť na vytvorenie DN. Poradie párov hodnôt atribútov komponentov je dôležité. DN obsahuje jeden komponent pre každú úroveň hierarchie adresárov, od koreňa nadol k úrovni, kde sa nachádza položka. Názvy DN LDAP DN začínajú najšpecifickejším atribútom (zvyčajne časť názvu) a pokračujú postupne rozširujúcimi sa atribútmi, ktoré často končia atribútom krajiny. Prvý komponent DN sa nazýva relatívny rozlišovací názov (RDN). Identifikuje položku jednoznačne od iných položiek, ktoré majú rovnakého rodiča. V príkladoch hore, RDN ″cn=Ben Gray″ oddeľuje prvú položku od druhej položky (s RDN ″cn=Lucille White″). Tieto dva vzorové názvy DN sú inak ekvivalentné. Pár atribút=hodnota, ktorý vytvára RDN pre položku musí byť tiež prítomný v položke. (Toto neplatí pre ostatné komponenty DN.)

Pomocou nasledujúceho príkladu vytvorte položku pre person:

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

Pravidlá zmeny významu DN

Niektoré znaky majú špeciálny význam v DN. Napríklad = (rovná sa) oddeľuje názov atribútu a hodnotu, a , (čiarka) oddeľuje páry atribút=hodnota. Špeciálnymi znakmi sú **,** (čiarka), **=** (rovná sa), **+** (plus), **<** (menej ako), **>** (viac ako), **#** (znak čísla), **;** (bodkočiarka), \ (spätná lomka) a **"** (úvodzovka, ASCII 34).

Špeciálny znak sa dá v hodnote atribútu zmeniť, aby sa odstránil špeciálny význam. Na zmenu významu týchto špeciálnych znakov alebo iných znakov v hodnote atribútu v reťazci DN použite tieto metódy:

1. Ak znak, ktorého význam chcete zmeniť je jeden zo špeciálnych znakov, dajte pred neho opačnú lomku (’\’ ASCII 92). Tento príklad znázorňuje metódu zmeny významu čiarky v názve organizácie:

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

   Toto je preferovaná metóda.
2. Inak môžete nahradiť znak, ktorého význam chcete zmeniť pomocou opačnej lomky a dvoch šestnástkových číslic, ktoré tvoria jeden bajt kódu znaku. Kód znaku **musí** byť v množine kódov UTF-8.

   ```
   CN=L. Eagle,O=Sue\2C Grabbit and Runn,C=GB
   ```
3. Celú hodnotu atribútu uzatvorte do **""** (úvodzovky, ASCII 34), ktoré nie sú súčasťou hodnoty. Medzi dvojicou úvodzoviek sa všetky znaky berú tak ako sú, okrem znaku \ (spätná lomka). Znak \ (opačná lomka) sa dá použiť na zmenu významu opačnej lomky (ASCII 92) alebo úvodzoviek (ASCII 34), každého predtým spomenutého špeciálneho znaku alebo šestnástkových párov ako v metóde 2. Napríklad, ak chcete zmeniť úvodzovky v cn=xyz"qrs"abc, stane sa z neho cn=xyz\"qrs\"abc, alebo ak chcete zmeniť \:

```
"jednu opačnú lomku je potrebné zmeniť
takto \\"
```

Iný príklad, "\Zoo" je neplatné, pretože 'Z' v tomto kontexte nemá zmenený význam.

Pseudonázvy DN

Pseudonázvy DN sa používajú pri definícii a vyhodnocovaní riadenia prístupu. Adresár LDAP podporuje niekoľko pseudonázvov DN (napríklad ″group:CN=THIS″ a ″access-id:CN=ANYBODY″), ktoré sa používajú na referencovanie veľkého počtu názvov DN, ktoré zdieľajú spoločné charakteristiky vo vzťahu k operácii vykonávanej na objekte alebo k objektu, na ktorom sa vykonáva operácia. Viac informácií o riadení prístupu nájdete v časti "Bezpečnosť adresárového servera" na strane 46.

Adresárový server podporuje tri pseudonázvy DN:

- access-id: CN=THIS

  Ak to je zadané ako súčasť ACL, toto DN referencuje bindDN, ktoré je rovné DN, na ktorom sa vykonáva operácia. Napríklad, ak sa operácia vykonáva na objekte ″cn=personA, ou=IBM, c=US″ a bindDn je ″cn=personA, ou=IBM, c=US″, udelené oprávnenia sú kombináciou pre oprávnenia udelené pre ″CN=THIS″ a udelené pre ″cn=personA, ou=IBM, c=US″.
- group: CN=ANYBODY

  Ak to je zadané ako súčasť ACL, toto DN referencuje všetkých užívateľov, aj užívateľov bez autentifikácie. Užívatelia sa nedajú odstrániť z tejto skupiny a táto skupina sa nedá odstrániť z databázy.
- group: CN=AUTHENTICATED

  Toto DN referencuje každé DN, ktoré bolo autentifikované adresárom. Metóda autentifikácia sa nezohľadňuje.

  Poznámka: ″CN=AUTHENTICATED″ referencuje DN, ktoré bolo autentifikované kdekoľvek v serveri, bez ohľadu na umiestnenie objektu reprezentujúceho DN. Mali by ste to však používať opatrne. Napríklad pod príponou ″cn=Secret″ môže byť uzol s názvom ″cn=Confidential Material″, ktorý má aclentry ″group:CN=AUTHENTICATED:normal:rsc″. Pod inou príponou ″cn=Common″ môže byť uzol ″cn=Public Material″. Ak sú tieto dva stromy v rovnakom serveri, pripojenie k ″cn=Public Material″ sa považuje za autentifikované a získa sa oprávnenie na normálnu triedu pre objekt ″cn= Confidential Material″.

Príklady pseudonázvov DN:

Príklad 1

Uvažujme o nasledujúcom ACL pre objekt: cn=personA, c=US

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

Určenie užívateľa ako	By získalo
cn=personA, c=US	normal:rsc:sensitive:rcs:critical:rwsc
cn=personB, c=US	normal:rsc:sensitive:rsc
Anonymous	normal:rsc

V tomto príklade personA získa oprávnenia udelené pre ID ″CN=THIS″ a oprávnenia udelené obom pseudoskupinám DN ″CN=ANYBODY″ a ″CN=AUTHENTICATED″.

Príklad 2

Uvažujme o nasledujúcom ACL pre 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
```

Pre operáciu vykonanú na cn=personA, c=US:

Určenie užívateľa ako	By získalo
cn=personA, c=US	object:ad:critical:rwsc
cn=personB, c=US	normal:rsc:sensitive:rsc
Anonymous	normal:rsc

V tomto príklade personA získa oprávnenia udelené pre ID ″CN=THIS″ a tie, ktoré sú udelené samotnému DN ″cn=personA, c=US″. Dôležité je, že oprávnenia skupiny sa neudelia, pretože existuje špecifickejšie aclentry (″access-id:cn=personA, c=US″) pre DN pripojenia (″cn=personA, c=US″).

Spracovanie rozšírených DN

Zložené RDN rozlišovacieho názvu sa môže skladať z viacerých komponentov spojených operátormi '+'. Server má vylepšenú podporu pre vyhľadávanie položiek, ktoré majú také DN. Zložené RDN je možné zadať v ľubovoľnom poradí ako základ pre operáciu hľadania.

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

Server podporuje rozšírenú operáciu normalizácie DN. Rozšírené operácie normalizácie DN normalizujú DN pomocou schémy servera. Táto rozšírená operácia môže byť užitočná pre aplikácie, ktoré používajú názvy DN. Viac informácií o rozšírených operáciách nájdete v časti "Kontroly a rozšírené operácie" na strane 81.

Syntax rozlišovacieho názvu

Formálna syntax pre rozlišovací názov (DN) je založená na RFC 2253. Syntax BNF (Backus Naur Form) je definovaná takto:

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

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

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

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

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

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

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

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

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


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

   <pair> ::= "\" ( <special> | "\" | '"')
   <stringchar> ::= any character except <special> or "\" or '"'
```

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

Znak bodkočiarky (;) sa môže použiť na oddelenie názvov RDN v rozlišovacom názve, hoci typickou notáciou je znak čiarky (,).

Biele znaky (medzery) sa môžu nachádzať na ľubovoľnej strane čiarky alebo bodkočiarky. Biele znaky sa ignorujú a bodkočiarka sa nahradí čiarkou.

Okrem toho, znaky medzery (' ' ASCII 32) sa môžu nachádzať buď pred alebo za '+' alebo '='. Tieto znaky medzery sa pri analýze ignorujú.

Nasledujúci príklad je rozlišovací názov zapísaný pomocou notácie, ktorá je určená pre bežné formáty názvov. Prvý je názov obsahujúci tri komponenty. Prvý z komponentov je zložené RDN. Zložené RDN obsahuje viac ako jeden pár atribút:hodnota a môže sa použiť na jednoznačné identifikovanie špecifickej položky v prípadoch, kedy jedna hodnota CN môže byť nejednoznačná:

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

Prípona (názvový kontext)

Prípona (známa tiež ako názvový kontext) je DN, ktoré identifikuje najvyššiu položku v lokálne vedenej hierarchii adresárov. V LDAP sa používa relatívna názvová schéma, preto je toto DN tiež príponou každej inej položky v danej hierarchii adresárov. Adresárový server môže mať viacero prípon a každá identifikuje lokálne vedenú hierarchiu adresárov, napríklad o=ibm,c=us.

Do adresára sa musí pridať špecifická položka, ktorá sa zhoduje s príponou. Položku, ktorú musíte vytvoriť musí používať objectclass, ktoré obsahuje použitý názvový atribút. Na vytvorenie položky s touto príponou môžete použiť webový administratívny nástroj alebo pomocný program ldapadd z Qshell. Bližšie informácie nájdete v "Manažovanie položiek adresára" na strane 162 alebo v "ldapmodify a ldapadd" na strane 185.

Koncepčne, existuje globálny priestor názvov LDAP. V globálnom priestore názvov LDAP môžete nájsť názvy DN podobné týmto:

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

Prípona ″o=IBM″ hovorí serveru, že len prvé DN je v priestore názvov, vedeného serverom. Pokúša sa odkazovať na objekty, ktoré sa nenachádzajú v rámci niektorej z prípon, čo má za následok chybu kvôli neexistencii takéhoto objektu, alebo odvolávka na iný adresárový server.

Server môže mať viacero prípon. Adresárový server má niekoľko preddefinovaných prípon, ktoré uchovávajú špecifické údaje pre našu implementáciu:

- cn=schema, obsahuje pre LDAP prístupnú reprezentáciu schémy
- cn=changelog, uchováva protokol zmien servera, ak je povolený
- cn=localhost, obsahuje nereplikované informácie, ktoré riadia niektoré aspekty prevádzky servera, napríklad replikačné konfiguračné objekty
- cn=IBMpolicies obsahuje informácie o operácii servera, ktorá *sa replikuje*.
- cn=pwdpolicy, obsahuje politiku hesiel pre celý server
- Prípona ″os400-sys=system-name.mydomain.com″ poskytuje dostupnosť LDAP pre objekty i5/OS, aktuálne limitované pre profily a skupiny užívateľov

Adresárový server je dodaný predkonfigurovaný so štandardnou príponou dc=system-name,dc=domain-name, kvôli jednoduchšiemu začiatku práce so serverom. Používanie tejto prípony nie je pre vás povinné. Môžete pridať svoje vlastné prípony, a predkonfigurovanú príponu môžete vymazať.

Pre prípony existujú dve bežne používané názvové konvencie. Jedna je založená na doméne TCP/IP pre vašu organizáciu. Druhá má ako základ názov a sídlo organizácie.

Napríklad pri danej doméne TCP/IP mycompany.com si môžete vybrať príponu ako dc=mycompany,dc=com, pričom atribút dc odkazuje na komponent domény. V tomto prípade môže položka najvyššej úrovne, ktorú vytvoríte v adresári, vyzerať ako nasledujúca (pomocou LDIF, formátu textového súboru pre podobu položiek LDAP):

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

Trieda objektov domain obsahuje aj niektoré voliteľné atribúty, ktoré sa vám môžu zísť. Ak chcete vidieť ďalšie atribúty, ktoré môžete používať, prezrite si schému alebo upravte položku, ktorú ste vytvorili pomocou webového administratívneho nástroja. Ďalšie informácie nájdete v časti “Manažovanie schémy” na strane 152.

Ak sa váš podnik nazýva My Company a má sídlo v USA, môžete si vybrať nasledovné prípony:

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

Pričom ou je názov pre triedu objektov organizationalUnit, o je názov organizácie pre triedu objektov organization a c je štandardná dvojpísmenová skratka krajiny, ktorá sa používa na pomenovanie triedy objektov country. V tomto prípade môže položka najvyššej úrovne, ktorú vytvoríte, vyzerať nasledovne:

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

Aplikácie, ktoré používate, môžu vyžadovať zadefinovanie konkrétnych prípon alebo použitie určitej názvovej konvencie. Napríklad, ak sa váš adresár používa na riadenie digitálnych certifikátov, môže sa od vás vyžadovať, aby ste časť svojho adresára štruktúrovali tak, aby sa názvy položiek zhodovali s DN predmetu certifikátov, ktoré uchováva.

Položky, ktoré sa majú do adresára pridať musia mať príponu, ktorá sa zhoduje s hodnotou DN, napríklad ou=Marketing,o=ibm,c=us. Ak dotaz obsahuje príponu, ktorá sa nezhoduje so žiadnou príponou nakonfigurovanou pre lokálnu databázu, dotaz bude odkazovať na server LDAP, ktorý identifikuje štandardná odvolávka. Ak nie je špecifikovaná žiadna štandardná odvolávka na LDAP, vráti sa výsledok, že objekt neexistuje.

Ďalšie informácie o pridávaní alebo odstraňovaní prípony si pozrite v časti “Pridávanie a odstraňovanie prípon adresárového servera” na strane 114.

Schéma

Schéma je množina pravidiel, ktoré riadia spôsob, ktorým sa údaje ukladajú do adresára. Schéma definuje typ povolených položiek, štruktúru ich atribútov a syntax atribútov.

Údaje sa ukladajú do adresára pomocou položiek adresára. Položka pozostáva z triedy objektov, ktorá je povinná, a z jej atribútov. Atribúty môžu byť buď povinné alebo voliteľné. Trieda objektov špecifikuje druh informácií, ktoré položka opisuje a definuje množinu atribútov, ktoré obsahuje. Každý atribút má jednu alebo viaceré priradené hodnoty. Ďalšie informácie o spôsoboch riadenia položiek nájdete v časti “Manažovanie položiek adresára” na strane 162.

Detailnejšie informácie týkajúce sa schémy nájdete v nasledujúcich témach:

- “Schéma adresárového servera IBM” na strane 16
- “Podpora bežnej schémy” na strane 17
- “Triedy objektov” na strane 18

Schéma adresárového servera IBM

Schéma pre adresárový server je preddefinovaná, ak však máte ďalšie požiadavky, môžete ju zmeniť. Bližšie informácie o tom, ako môžete túto schému zmeniť, nájdete v “Manažovanie schémy” na strane 152.

Adresárový server obsahuje podporu dynamickej schémy. Schéma sa zverejní ako súčasť informácií o adresári a je k dispozícii v položke podschémy (DN=″cn=schema″). Schému môžete vyžiadať dotazom použitím API ldap_search() a zmeniť ju použitím ldap_modify(). Viac informácií o týchto API nájdete v téme “API adresárového servera”.

Schéma má viac konfiguračných informácií ako tie, ktoré sú zahrnuté v požiadavke na komentáre (RFC) LDAP verzie 3 alebo v štandardných špecifikáciách. Napríklad pri danom atribúte môžete uviesť, ktoré indexy sa majú udržiavať. Tieto dodatkové konfiguračné informácie sa podľa potreby udržiavajú v položke podschémy. Ďalšia trieda objektov je definovaná pre položku podschémy IBMsubschema, ktorá má atribúty ″MAY″, ktoré uchovávajú rozšírené informácie o schéme.

Adresárový server definuje jednu schému pre celý server, ktorá je prístupná prostredníctvom osobitnej položky adresára, ″cn=schema″. Položka obsahuje celú schému definovanú pre server. Ak chcete získať informácie o schéme, môžete vykonať ldap_search pomocou nasledujúceho:

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

Schéma poskytuje hodnoty pre nasledovné typy atribútov:

- objectClasses (Viac informácií o objectClasses nájdete v časti “Triedy objektov” na strane 18.)
- attributeTypes (Viac informácií o attributeTypes nájdete v časti “Atribúty” na strane 19.)
- IBMAttributeTypes (Viac informácií o IBMAttributeTypes nájdete v časti “Atribút IBMAttributeTypes” na strane 21.)
- zhodujúce sa pravidlá (bližšie informácie o zhodujúcich sa pravidlách nájdete v časti “Pravidlá zhody” na strane 22).
- syntaxi ldap (Viac informácií o syntaxiach ldap nájdete v časti “Syntax atribútov” na strane 24).

Syntax týchto definícií schém je založená na dokumentoch RFC LDAP verzie 3.

Položka vzorovej schémy môže obsahovať:

```
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 'Binary' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.7 DESC 'Boolean' )
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 'Directory String' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.24 DESC 'Generalized Time' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.26 DESC 'IA5 String' )
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 'Telephone Number' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.53 DESC 'UTC Time' )

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 )
```

Informácie o schéme sa dajú modifikovať prostredníctvom API ldap_modify. Ďalšie informácie vám poskytne téma “API adresárového servera”. Cez DN ″cn=schema″ môžete pridať, vymazať alebo nahradiť typ atribútu alebo triedu objektov. Viac informácií si pozrite v témach “Dynamická schéma” na strane 27 a “Manažovanie schémy” na strane 152. Môžete poskytnúť aj úplný opis. Položku schémy môžete pridať alebo nahradiť definíciou LDAP verzie 3 alebo definíciou rozšírenia atribútu IBM alebo oboma definíciami.

Podpora bežnej schémy

IBM Directory podporuje štandardnú schému adresárov, ako je zadefinované v nasledovnom:

- IETF (Internet Engineering Task Force)  RFC pre LDAP verzie 3, napríklad RFC 2252 a 2256.
- DEN (Directory Enabled Network) 
- CIM (Common Information Model) z DMTF (Desktop Management Task Force) 
- LIPS (Lightweight Internet Person Schema) od spoločnosti Network Application Consortium 

Táto verzia LDAP obsahuje schému definovanú v LDAP verzie 3 v štandardnej konfigurácii schémy. Obsahuje aj definície schémy DEN.

IBM poskytuje aj skupinu rozšírených definícií bežných schém, ktoré ostatné produkty IBM zdieľajú pri využívaní adresára LDAP. Tieto schémy obsahujú:

- Objekty pre aplikácie bielych stránok, napríklad e-osoba, skupina, krajina, organizácia, organizačná jednotka a rola, miesto, štát, a tak ďalej
- Objekty pre ostatné podsystémy napríklad kontá, servisné a prístupové body, autorizácia, autentifikácia, bezpečnostná politika, a tak ďalej.

Triedy objektov

Trieda objektov špecifikuje množinu atribútov, ktoré sa používajú na opis objektu. Napríklad, ak ste vytvorili triedu objektov **tempEmployee**, môže obsahovať atribúty priradené k dočasnému zamestnancovi, napríklad **idNumber**, **dateOfHire** alebo **assignmentLength**. Môžete pridávať vlastné triedy objektov, ktoré budú vyhovovať potrebám vašej organizácie. Schéma adresárového servera IBM poskytuje niektoré základné typy tried objektov vrátane:

- Skupiny
- Miesta
- Organizácie
- Ľudia

Poznámka: Triedy objektov, ktoré sú špecifické pre adresárový server majú predponu 'ibm-'.

Triedy objektov sú definované charakteristikami typu, dedenia a atribútov.

Typ triedy objektov

Existujú tri typy tried objektov:

Štrukturálna:
Každá položka musí patriť do jedinej štrukturálnej triedy objektov, ktorá definuje základný obsah položky. Táto trieda objektov predstavuje objekt skutočného sveta. Pretože všetky položky musia patriť do štrukturálnej triedy objektov, je to najbežnejší typ triedy objektov.

Abstraktná:
Tento typ sa používa ako nadtrieda alebo šablóna pre ostatné (štrukturálne) triedy objektov. Definuje množinu atribútov, ktoré sú spoločné pre množinu štrukturálnych tried objektov. Tieto triedy objektov, ak sú definované ako podtriedy abstraktnej triedy, zdedia definované atribúty. Atribúty nemusia byť definované pre každú podriadenú triedu objektov.

Pomocná:
Tento typ indikuje ďalšie atribúty, ktoré môžu byť priradené položke, ktorá patrí určitej štrukturálnej triede objektov. I keď môže položka patriť len k jednej triede štrukturálneho objektu, môže patriť k viacerým pomocným triedam objektov.

Dedenie tried objektov

Táto verzia adresárového servera podporuje dedenie objektov pre triedy objektov a definície atribútov. Nová trieda objektov sa dá definovať cez rodičovské triedy (viacnásobné dedenie) a dodatočné alebo zmenené atribúty.

Každá položka je priradená k jednej štrukturálnej triede objektov. Všetky triedy objektov dedia z abstraktnej triedy objektov s názvom **top**. Môžu dediť aj z iných tried objektov. Štruktúra triedy objektov určuje zoznam povinných a povolených atribútov pre určitú položku. Dedenie triedy objektov závisí od postupnosti definícií triedy objektov. Trieda objektov môže dediť iba z tried objektov, ktoré sú pred ňou. Napríklad štruktúra triedy objektov pre položku person môže byť v súbore LDIF definovaná takto:

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

V tejto štruktúre bude organizationalPerson dediť z tried objektov person a top, zatiaľ čo trieda objektov person bude dediť iba z triedy objektov top. Preto keď triedu objektov organizationalPerson priradíte k položke, automaticky zdedí povinné a povolené atribúty z nadtried objektov (v tomto prípade je to trieda objektov person).

Operácie aktualizácie schémy sa pred spracovaním a potvrdením kontrolujú na konzistentnosť voči hierarchii tried schémy.

Atribúty

Každá trieda objektov obsahuje niekoľko povinných a niekoľko voliteľných atribútov. Povinné atribúty sú atribúty, ktoré musia byť prítomné v položkách, ktoré používajú triedu objektov. Voliteľné atribúty sú atribúty, ktoré môžu byť prítomné v položkách používajúcich triedu objektov.

Atribúty

Každá položka adresára má skupinu atribútov, priradenú cez jej triedu objektov. Zatiaľ čo triedy objektov opisuje typ informácií, ktoré položka obsahuje, skutočné údaje sa nachádzajú v atribútoch. Atribút je zastúpený jedným alebo viacerými pármi názov-hodnota ktoré uchovávajú špecifický údajový prvok, napríklad meno, adresu alebo telefónne číslo. Adresárový server zobrazuje údaje ako páry názov-hodnota, opisné atribúty, napríklad commonName (cn) a špecifické informácie, napríklad John Doe.

Napríklad položka pre John Doe môže obsahovať niekoľko párov názov atribútu-hodnota.

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

Zatiaľ čo sú štandardné atribúty v schéme už definované, vy môžete vytvárať, upravovať, kopírovať alebo vymazávať definície atribútov, aby vyhovovali potrebám vašej organizácie.

Viac informácií nájdete v nasledujúcich témach:

- “Spoločné prvky podschém”
- “Atribút objectclass” na strane 20
- “Atribút attributetypes” na strane 20
- “Atribút IBMAttributeTypes” na strane 21
- “Pravidlá zhody” na strane 22
- “Pravidlá indexovania” na strane 23
- “Syntax atribútov” na strane 24

Spoločné prvky podschém

Nasledujúce prvky sa používajú na definovanie gramatiky pre hodnoty atribútov podschémy:

- 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 ; množina oids obidvoch foriem (numerické OID alebo názvy)
- oids = woid / (″(″ oidlist ″)″)
- oidlist = woid *(″$″ woid) ; deskriptory objektov používané ako názvy prvkov podschémy
- qdescrs = qdescr / (whsp ″(″ qdescrlist ″)″ whsp)
- qdescrlist = [qdescr *(qdescr)]
- whsp ″'″ descr ″'″ whsp

Atribút objectclass

Atribút objectclasses vypisuje zoznam tried objektov, ktoré podporuje server. Každá hodnota tohto atribútu predstavuje definíciu samostatnej triedy objektov. Definície triedy objektov sa môžu pridávať, vymazávať alebo modifikovať pomocou vhodných modifikácií atribútu objectclasses z položky cn=schema. Hodnoty atribútu objectclasses majú nasledovnú gramatiku, ako bola definovaná pomocou RFC 2252:

```
ObjectClassDescription = "(" whsp
        numericoid whsp ; Objectclass identifier
        [ "NAME" qdescrs ]
        [ "DESC" qdstring ]
        [ "OBSOLETE" whsp ]
        [ "SUP" oids ] ; Superior objectclasses
        [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ] ; default is structural
        [ "MUST" oids ] ; AttributeTypes
        [ "MAY" oids ] ; AttributeTypes
        whsp ")"
```

Napríklad definícia person objectclass je:

(2.5.6.6 NAME 'person' DESC 'Defines entries that generically represent people. ' STRUCTURAL SUP top MUST (cn $ sn) MAY (userPassword $ telephoneNumber $ seeAlso $ description))

- OID pre túto triedu je 2.5.6.6
- Názov je ″person″
- Je to štrukturálna trieda objektov
- Dedí z triedy objektov ″top″
- Nasledujúce atribúty sú povinné: cn, sn
- Nasledujúce atribúty sú voliteľné: userPassword, telephoneNumber, seeAlso, description

Viac informácií o spôsobe zmeny tried objektov, ktoré podporuje server, nájdete v časti “Manažovanie schémy” na strane 152.

Atribút attributetypes

Atribút attributetypes vypisuje zoznam atribútov, ktoré podporuje server. Každá hodnota tohto atribútu predstavuje definíciu samostatného atribútu. Definície triedy objektov sa môžu pridávať, vymazávať alebo modifikovať pomocou vhodných modifikácií atribútu attributetypes z položky cn=schema. Hodnoty atribútu attributetypes majú nasledovnú gramatiku, ako bola definovaná pomocou RFC 2252:

```
AttributeTypeDescription = "(" whsp
        numericoid whsp ; AttributeType identifier
        [ "NAME" qdescrs ] ; name used in AttributeType
        [ "DESC" qdstring ] ; description
        [ "OBSOLETE" whsp ]
        [ "SUP" woid ] ; derived from this other AttributeType
        [ "EQUALITY" woid ; Matching Rule name
        [ "ORDERING" woid ; Matching Rule name
        [ "SUBSTR" woid ] ; Matching Rule name
        [ "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-shared
        "dSAOperation" ; DSA-specific, value depends on server
```

Pravidlá zhody a hodnoty syntaxe musia mať niektorú z hodnôt, ktorú definuje:

- “Pravidlá zhody” na strane 22
- “Syntax atribútov” na strane 24

Iba atribúty ″userApplications″ sa dajú definovať alebo modifikovať v schéme. Atribúty ″directoryOperation″, ″distributedOperation″ a ″dSAOperation″ definuje server a majú špecifický význam pre prevádzku servera.

Napríklad atribút ″description″ má nasledujúcu definíciu:

(2.5.4.13 NAME ’description’ DESC ’Attribute common to CIM and LDAP schema to provide lengthy description of a directory object entry.’ EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications)

- Jeho OID je 2.5.4.13
- Jeho názov je ″description″
- Jeho syntax je 1.3.6.1.4.1.1466.115.121.1.15 (Reťazec adresára)

Viac informácií o spôsobe zmeny typov atribútov, ktoré podporuje server, nájdete v časti “Manažovanie schémy” na strane 152.

Atribút IBMAttributeTypes

Atribút IBMAttributeTypes sa dá použiť na definovanie informácií o schéme, ktoré nie sú zahrnuté v štandarde LDAP verzie 3 pre atribúty. Hodnoty IBMAttributeTypes musia vyhovovať nasledujúcej gramatike:

```
IBMAttributeTypesDescription = "(" whsp
      numericoid whsp
     [ "DBNAME"   qdescrs ]            ; at most 2 names (table, column)
     [ "ACCESS-CLASS" whsp IBMAccessClass whsp ]
     [ "LENGTH" wlen whsp ]            ; maximum length of attribute
     [ "EQUALITY" [ IBMwlen ] whsp ]   ; create index for matching rule
     [ "ORDERING" [ IBMwlen ] whsp ]   ; create index for matching rule
     [ "APPROX"   [ IBMwlen ] whsp ]   ; create index for matching rule
     [ "SUBSTR"   [ IBMwlen ] whsp ]   ; create index for matching rule
     [ "REVERSE"  [ IBMwlen ] whsp ]   ; reverse index for substring
     whsp ")"

   IBMAccessClass =
      "NORMAL"           / ; this is the default
      "SENSITIVE"        /
      "CRITICAL"         /
      "RESTRICTED"       /
      "SYSTEM"           /
      "OBJECT"

   IBMwlen = whsp len
```

Numericoid

Používa sa na koreláciu hodnoty v attributetypes s hodnotou v IBMAttributeTypes.

DBNAME

Najviac môžete zadať 2 názvy, ak sú v skutočnosti 2 názvy dané. Prvý je názov tabuľky, ktorá sa pre tento atribút používa. Druhý je názov stĺpca, ktorý sa používa pre úplne normalizovanú hodnotu atribútu v tabuľke. Ak zadáte iba jeden názov, tento sa bude používať aj ako názov tabuľky aj ako názov stĺpca. Ak neposkytnete žiadne DBNAME, použije sa názov podľa prvých 17 znakov názvu atribútu (ktoré musia byť jedinečné). Názvy databázových tabuliek a stĺpcov sú obmedzené na 17 znakov.

ACCESS-CLASS
Klasifikácia prístupu pre tento typ atribútu. Ak bude ACCESS-CLASS vynechané, štandardne sa nastaví na hodnotu normal.

LENGTH
Maximálny dĺžka tohto atribútu. Dĺžka je vyjadrená ako počet bajtov. Adresárový server je ustanovený na špecifikovanie dĺžky atribútu. V hodnote attributetypes, reťazec:

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

sa dá použiť na indikáciu, že atribút attributetype spolu s oid attr-oid má maximálnu dĺžku.

EQUALITY, ORDERING, APPROX, SUBSTR, REVERSE
Ak sa použije niektorý z týchto atribútov, pre zodpovedajúce pravidlo zhody sa vytvorí index. Voliteľná dĺžka špecifikuje šírku indexovaného stĺpca. Na implementáciu viacerých pravidiel zhody sa použije jeden index. Adresárový server priradí dĺžku 500, ak ju nezadá užívateľ. Server môže použiť aj kratšiu dĺžku ako požadoval užívateľ, ak to bude opodstatnené. Napríklad, keď dĺžka indexu prekročí maximálnu dĺžku atribútu, dĺžka indexu sa bude ignorovať.

Pravidlá zhody

Pravidlo zhody poskytuje návod pre porovnanie reťazcov počas operácie vyhľadávania. Tieto pravidlá sú rozdelené do troch kategórií:

- Rovnosť
- Zoradenie
- Podreťazec

Adresárový server podporuje zhody rovnosti pre všetky syntaxe okrem binárnej. V prípade atribútov zadefinovaných použitím binárnej syntaxe podporuje server len vyhľadávania existencií, napríklad ″(jpegphoto=*)″. V prípade syntaxí Reťazca IA5 a Reťazca adresára je možné definíciu atribútu ďalej zadefinovať ako rozlišujúcu alebo ignorujúcu veľkosť písmen. Napríklad, atribút cn používa pravidlo zhody caseIgnoreMatch, ktoré zrovnoprávni hodnoty ″John Doe″ a ″john doe″. Pri pravidlách zhody, ktoré veľkosť písmen ignorujú, sa porovnanie vykoná po konverzii hodnôt na veľké písmená. Algoritmus veľkých písmen nezohľadňuje lokál a nemusí byť správny pre všetky lokály.

V prípade atribútov syntaxí Reťazca IA5, Reťazca adresára a Charakteristického názvu podporuje adresárový server porovnávanie podreťazcov. Vyhľadávacie filtre pre porovnávanie podreťazcov používajú na porovnanie nulového počtu alebo viacerých znakov v reťazci znak ″*″. Napríklad, vyhľadávací filter ″(cn=*smith)″ vyhľadá všetky hodnoty končiace znakom ″smith″.

Vyhľadávania s triedením sú podporované pre syntaxe Celočíselné, Reťazec adresára, Reťazec IA5 a Charakteristický názov. Pri reťazcových syntaxách je triedenie založené na reťazcových hodnotách UTF-8. Ak je atribút definovaný s pravidlom, ktoré ignoruje veľkosť písmen, triedenie sa vykoná podľa reťazcových hodnôt veľkých písmen. Ako bolo uvedené vyššie, algoritmus veľkých písmen nemusí byť správny pre všetky lokály.

V adresárovom serveri IBM je správanie porovnávania podreťazcov a triedenia implikované pravidlom zhody: všetky syntaxe, ktoré podporujú porovnávanie podreťazov, majú implikované pravidlo zhody podreťazcov a všetky syntaxe, ktoré podporujú triedenie, majú implikované pravidlo triedenia. Pre atribúty definované pomocou pravidla zhody, ktoré ignoruje veľkosť písmen, implikované pravidlá zhody podreťazcov a pravidlá zhody s triedením budú tiež ignorovať veľkosť písmen.

Pravidlá zhody rovnosti		
Pravidlo zhody	**OID**	**Syntax**
caseExactIA5Match	1.3.6.1.4.1.1466.109.114.1	Syntax reťazca adresára
caseExactMatch	2.5.13.5 IA5	Syntax reťazca
caseIgnoreIA5Match	1.3.6.1.4.1.1466.109.114.2	Syntax reťazca IA5
caseIgnoreMatch	2.5.13.2	Syntax reťazca adresára

Pravidlá zhody rovnosti		
Pravidlo zhody	**OID**	**Syntax**
distinguishedNameMatch	2.5.13.1	DN - rozlišovací názov
generalizedTimeMatch	2.5.13.27	Syntax zovšeobecneného času
ibm-entryUuidMatch	1.3.18.0.2.22.2	Syntax reťazca adresára
integerFirstComponentMatch	2.5.13.29	Celočíselná syntax - celé číslo
integerMatch	2.5.13.14	Celočíselná syntax - celé číslo
objectIdentifierFirstComponentMatch	2.5.13.30	Reťazec pre obsiahnutie OID. OID je reťazec, ktorý obsahuje číslice (0-9) a desatinné čiarky (.).
objectIdentifierMatch	2.5.13.0	Reťazec pre obsiahnutie OID. OID je reťazec, ktorý obsahuje číslice (0-9) a desatinné čiarky (.)
octetStringMatch	2.5.13.17	Syntax reťazca adresára
telephoneNumberMatch	2.5.13.20	Syntax telefónneho čísla
uTCTimeMatch	2.5.13.25	Syntax pre čas UTC

Pravidlá zhody zoradenia		
Pravidlo zhody	**OID**	**Syntax**
caseExactOrderingMatch	2.5.13.6	Syntax reťazca adresára
caseIgnoreOrderingMatch	2.5.13.3	Syntax reťazca adresára
distinguishedNameOrderingMatch	1.3.18.0.2.4.405	DN - rozlišovací názov
generalizedTimeOrderingMatch	2.5.13.28	Syntax zovšeobecneného času

Pravidlá zhody podreťazca		
Pravidlo zhody	**OID**	**Syntax**
caseExactSubstringsMatch	2.5.13.7	Syntax reťazca adresára
caseIgnoreSubstringsMatch	2.5.13.4	Syntax reťazca adresára
telephoneNumberSubstringsMatch	2.5.13.21	Syntax telefónneho čísla

Poznámka: Čas UTC je formát časového reťazca, ktorý definujú štandardy ASN.1. Pozrite si ISO 8601 a X680. Túto syntax používajte na ukladanie časových hodnôt vo formáte času UTC. Pozrite si tému “Zovšeobecnený čas a čas UTC” na strane 33.

Pravidlá indexovania

K atribútom pripojené pravidlá indexu umožňujú rýchlejšie získanie informácií. Ak je daný iba atribút, nebudú sa udržiavať žiadne indexy. Adresárový server poskytuje nasledujúce pravidlá indexovania:

- Rovnosť
- Zoradenie
- Približne
- Podreťazec
- Obrátene

Špecifikácie pravidiel indexovania pre atribúty: Špecifikovanie pravidiel indexovania pre atribút riadi vytváranie a údržbu špeciálnych indexov pre hodnoty atribútu. Veľmi to zlepší časy odozvy vo vyhľadávaniach s filtrami, ktoré obsahujú tieto atribúty. Päť možných typov pravidiel indexovania súvisí s operáciami, ktoré boli použité vo vyhľadávacom filtri.

Rovnosť

Platí pre nasledujúce operácie vyhľadávania:

- equalityMatch '='

Napríklad:

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

Zoradenie

Platí pre nasledujúce operácie vyhľadávania:

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

Napríklad:

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

Približne

Platí pre nasledujúce operácie vyhľadávania:

- approxMatch '~='

Napríklad:

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

Podreťazec

Platí pre operáciu vyhľadávania, ktorá používa syntax podreťazca:

- substring '*'

Napríklad:

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

Obrátene

Platí pre nasledujúce operácie vyhľadávania:

- '*' substring

Napríklad:

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

Odporúča sa, aby ste minimálne zadali rovnaké indexovanie na všetkých atribútoch, ktoré sa majú použiť vo vyhľadávacích filtroch .

Syntax atribútov

Syntax atribútov definuje dovolené hodnoty pre atribút. Server používa definíciu syntaxe pre atribút na overenie platnosti údajov a na určenie spôsobu párovania hodnôt. Napríklad, atribút ″Boolean″ môže mať len hodnoty ″TRUE″ a ″FALSE″.

Atribúty sa definujú buď s jednou hodnotou alebo s viacerými hodnotami. Atribúty s viacerými hodnotami nie sú usporiadané, preto by aplikácia nemala byť závislá na množine hodnôt pre daný atribút, ktoré sa vracajú v určitom poradí. Ak potrebujete usporiadanú množinu hodnôt, pouvažujte o vložení zoznamu hodnôt do atribútu s jednou hodnotou:

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

Alebo pouvažujte o začlenení informácie o poradí do hodnoty:

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

Atribúty s viacerými hodnotami sú užitočné, keď je položka známa pod viacerými názvami. Napríklad cn (common name), má viacero hodnôt. Položka môže byť definovaná takto:

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

To umožňuje, aby vyhľadávania hodnoty John Smith a Jack Smith vrátili rovnaké informácie.

Binárne atribúty obsahujú ľubovoľný bajtový reťazec, napríklad fotografia JPEG a nedajú sa použiť na vyhľadávanie položiek.

Boolovské atribúty obsahujú reťazce TRUE alebo FALSE.

DN atribúty obsahujú rozlišovacie názvy LDAP. Hodnoty nemusia byť DN existujúcich položiek, ale musia mať platnú DN syntax.

Atribúty adresárového reťazca obsahujú textový reťazec, ktorý používa znaky UTF-8. Pri atribúte sa buď rozlišuje veľkosť písmen alebo sa veľkosť písmen ignoruje s ohľadom na hodnoty použité vo vyhľadávacích filtroch (na základe pravidla o zhode, ktoré je pre atribút definované), hoci hodnota bude vždy vrátená, ako bola pôvodne zadaná.

Atribúty zovšeobecneného času obsahujú reťazcovú reprezentáciu bezpečného dátumu a času roku 2000 použitím časov GMT s voliteľným posunom časového pásma GMT. Viac detailov pre syntax týchto hodnôt nájdete v časti “Zovšeobecnený čas a čas UTC” na strane 33.

Atribúty reťazca IA5 obsahujú textový reťazec, ktorý používa znakovú sadu IA5 (7-bit US ASCII. Pri atribúte sa buď rozlišuje veľkosť písmen alebo sa veľkosť písmen ignoruje s ohľadom na hodnoty použité vo vyhľadávacích filtroch (na základe pravidla o zhode, ktoré je pre atribút definované), hoci hodnota bude vždy vrátená, ako bola pôvodne zadaná. Reťazec IA5 taktiež umožňuje použitie zástupného znaku pri vyhľadávaniach podreťazcov.

Celočíselné atribúty obsahujú reprezentáciu hodnoty formou textového reťazca. Napríklad 0 alebo 1000. Hodnoty pre atribúty syntaxe Celočíselného typu musia byť v rozsahu -2147483648 až 2147483647.

Atribúty telefónneho čísla obsahujú reprezentáciu telefónneho čísla vo forme textového reťazca. Adresárový server nepredpisuje žiadnu konkrétnu syntax pre tieto hodnoty. Všetky nasledujúce hodnoty sú platné: (555)555-5555, 555.555.5555 a +1 43 555 555 5555.

Atribúty času UTC používajú starší formát reťazca, ktorý nie je bezpečný pre zobrazenie dátumov a časov roku 2000. Viac detailov nájdete v časti “Zovšeobecnený čas a čas UTC” na strane 33.

V schéme adresárov je syntax atribútu špecifikovaná pomocou Identifikátorov objektov (OID) priradených každej syntaxe. Nasledovná tabuľka uvádza syntaxe podporované adresárovým serverom a ich OID.

Syntax	OID
Syntax opisu typu atribútu	1.3.6.1.4.1.1466.115.121.1.3
Binárna - oktetový reťazec	1.3.6.1.4.1.1466.115.121.1.5
Boolovská - TRUE/FALSE	1.3.6.1.4.1.1466.115.121.1.7
Syntax reťazca adresára	1.3.6.1.4.1.1466.115.121.1.15
Syntax opisu pravidla obsahu DIT	1.3.6.1.4.1.1466.115.121.1.16

Syntax	OID
Syntax opisu pravidla štruktúry DIT	1.3.6.1.4.1.1466.115.121.1.17
DN - rozlišovací názov	1.3.6.1.4.1.1466.115.121.1.12
Syntax zovšeobecneného času	1.3.6.1.4.1.1466.115.121.1.24
Syntax reťazca IA5	1.3.6.1.4.1.1466.115.121.1.26
Popis typu atribútu IBM	1.3.18.0.2.8.1
Celočíselná syntax - celé číslo	1.3.6.1.4.1.1466.115.121.1.27
Syntax opisu syntaxe LDAP	1.3.6.1.4.1.1466.115.121.1.54
Opis pravidla zhody	1.3.6.1.4.1.1466.115.121.1.30
Opis použitia pravidla zhody	1.3.6.1.4.1.1466.115.121.1.31
Opis formy názvu	1.3.6.1.4.1.1466.115.121.1.35
Syntax opisu triedy objektov	1.3.6.1.4.1.1466.115.121.1.37
Reťazec pre obsiahnutie OID. OID je reťazec, ktorý obsahuje číslice (0-9) a desatinné čiarky (.). Pozrite si tému “Identifikátor objektov (OID)”.	1.3.6.1.4.1.1466.115.121.1.38
Syntax telefónneho čísla	1.3.6.1.4.1.1466.115.121.1.50
Syntax pre čas UTC. Čas UTC je formát časového reťazca, ktorý definujú štandardy ASN.1. Pozrite si ISO 8601 a X680. Túto syntax používajte na ukladanie časových hodnôt vo formáte času UTC. Pozrite si tému “Zovšeobecnený čas a čas UTC” na strane 33.	1.3.6.1.4.1.1466.115.121.1.53

Identifikátor objektov (OID)

Identifikátor objektu (OID) je reťazec desiatkových čísiel, ktorý jedinečne identifikuje objekt. Týmito objektmi sú zvyčajne trieda objektov alebo atribút.

Ak nemáte OID, môžete špecifikovať triedu objektov alebo názov atribútu, ku ktorému bude pripojený **-oid**. Napríklad, ak vytvoríte atribút tempID, OID môžete špecifikovať ako **tempID-oid**.

Najdôležitejšie zo všetkého je, aby súkromné OID boli získané od oprávnených orgánov. Existujú dve základné stratégie pre získanie zákonných OID:

- Zaregistrujte objekty na úrade. Táto stratégia je vhodná, ak potrebujete malý počet OID.
- Z úradu si zabezpečte arc (arc je konkrétny podstrom stromu OID) a podľa potreby priraďte svoje vlastné OID. Táto stratégia môže byť preferovaná, ak je potrebné veľké množstvo OID, alebo ak priradenia OID nie sú stabilné.

ANSI (American National Standards Institute) je registračný úrad pre názvy organizácií v USA a to podľa globálneho registračného procesu, ktorý vytvorili organizácie ISO (International Standards Organization) a ITU (International Telecommunication Union). Viac informácií o registrácii názvu organizácie nájdete na webovej stránke ANSI (www.ansi.org). ANSI OID arc pre organizácie je 2.16.840.1. ANSI priradí číslo (NEWNUM), ktoré vytvorí nový OID arc: 2.16.840.1.NEWNUM.

Vo väčšine krajín a regiónov spravuje register OID Združenie pre štátne normy. Podobne ako pre ANSI arc, toto sú všeobecné arc, priradené pod OID 2.16. Nájdenie oprávnenia OID pre konkrétnu krajinu alebo región môže vyžadovať hlbšie skúmanie. Organizácia pre národné štandardy pre vašu krajinu alebo región by mohla byť členom ISO. Názvy a kontaktné informácie členov ISO môžete nájsť na webovej stránke ISO (www.iso.ch).

IANA (Internet Assigned Numbers Authority) priraďuje čísla súkromných podnikov, ktoré sú OID, v arc 1.3.6.1.4.1. IANA priradí číslo (NEWNUM) tak, že nový OID arc bude 1.3.6.1.4.1.NEWNUM. Tieto čísla môžete získať z webovej stránky IANA (www.iana.org).

Hneď ako bude vašej organizácii priradené OID, svoje vlastné OID môžete definovať pripojením na koniec OID. Napríklad predpokladajme, že vašej organizácii bolo priradené fiktívne OID 1.1.1. Žiadnej inej organizácii nebude priradené OID, ktoré bude začínať na ″1.1.1″. Rozsah pre LDAP môžete vytvoriť pripojením ″.1″, čím sa vytvorí 1.1.1.1. Toto môžete ďalej deliť na rozsahy pre triedy objektov (1.1.1.1.1), typy atribútov (1.1.1.1.2), a tak ďalej a atribútu ″foo″ priradiť OID 1.1.1.1.2.34.

Položky podschémy

Pre každý server existuje jedna položka podschémy. Všetky položky v adresári majú odvodený typ atribútu subschemaSubentry. Hodnota typu atribútu subschemaSubentry je DN položky podschémy, ktorá zodpovedá položke. Všetky položky pod rovnakým serverom zdieľajú rovnakú položku podschémy a ich typ atribútu subschemaSubentry má rovnakú hodnotu. Položka podschémy má pevne zapísaný DN 'cn=schema'.

Položka podschémy patrí do tried objektov 'top', 'subschema' a 'IBMsubschema'. Trieda objektov 'IBMsubschema' nemá žiadne atribúty MUST a jeden typ atribútu MAY ('IBMattributeTypes').

Trieda objektov IBMsubschema

Trieda objektov IBMsubschema sa používa iba v položke podschémy a to takto:

```
( 1.3.18.0.2.6.174
NAME 'ibmSubSchema'
DESC 'IBM specific object class that stores all the attributes and object classes for a given directory
 server.'
SUP 'subschema'
STRUCTURAL MAY ( IBMAttributeTypes ) )
```

Dotazy schémy

API ldap_search() sa dá použiť na dotazovanie položky podschémy, ako to ukazuje nasledujúci príklad:

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

Tento príklad získa celú schému. Ak chcete získať všetky hodnoty vybraných typov atribútov, v ldap_search použite parameter attrs. Nemôžete získať iba špecifickú hodnotu špecifického typu atribútu.

Viac informácií o API ldap_search nájdete v téme "API adresárového servera".

Dynamická schéma

Ak chcete vykonať zmenu dynamickej schémy, použite API ldap_modify a DN ″cn=schema″. Naraz sa môže pridať, vymazať alebo nahradiť iba jedna entita schémy (napríklad typ atribútu alebo trieda objektov).

Ak chcete vymazať položku schémy, špecifikujte atribút schémy, ktorý definuje položku schémy (objectclasses alebo attributetypes) a pre jeho hodnotu špecifikujte OID v zátvorkách. Napríklad, ak chcete vymazať atribút s OID <attr-oid>:

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

Môžete poskytnúť aj úplný opis. V každom prípade pravidlo zhody, ktoré sa použije na vyhľadanie entity schémy, ktorá sa má vymazať, bude objectIdentifierFirstComponentMatch.

Ak chcete pridať alebo odstrániť entitu schémy, MUSITE zabezpečiť definíciu LDAP verzie 3 a MÔŽETE zabezpečiť definíciu IBM. Vo všetkých prípadoch musíte poskytnúť iba definíciu alebo definície entity schémy, ktorú chcete ovplyvniť.

Napríklad, ak chcete vymazať typ atribútu ’cn’ (jeho OID je 2.5.4.3), použite ldap_modify() a:

```
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);
```

Ak chcete pridať novú lištu typov atribútov s OID 20.20.20, ktorá bude dediť z atribútu ″name″ a má dĺžku 20 znakov:

```
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);
```

Verzia LDIF horeuvedeného by bola:

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

Riadiace prvky prístupu

Zmeny dynamickej schémy sa dajú vykonať iba replikáciou DN dodávateľa alebo administrátora.

Replikácia

Ak sa vykoná zmena dynamickej schémy, schéma sa zreplikuje.

Nedovolené zmeny schémy

Nie sú dovolené všetky zmeny schémy. K obmedzeniam pre zmeny patrí nasledovné:

- Každá zmena v schéme musí schému zanechať v konzistentnom stave.
- Typ atribútu, ktorý je nadtypom iného typu atribútu, nemožno vymazať. Typ atribútu, ktorý je typom atribútu ″MAY″ alebo ″MUST″ triedy objektu, nemožno vymazať.
- Triedu objektu, ktorá je supertriedou iného subjektu, nemožno vymazať.
- Typy atribútov alebo triedy objektov, ktoré odkazujú na neexistujúce entity (napríklad syntaxe alebo triedy objektov), nemôžu byť pridané.
- Typy atribútov alebo triedy objektov sa nemôžu modifikovať takým spôsobom, že nakoniec budú odkazovať na neexistujúce entity (napríklad syntaxe alebo triedy objektov).
- Nové atribúty nemôžu používať existujúce databázové tabuľky v ich definícii IBMattributestype.
- Atribúty, ktoré sa používajú v ľubovoľnej existujúcej položke adresára, nemožno vymazať.
- Dĺžku a syntax atribútu nemožno zmeniť.
- Databázovú tabuľku alebo stĺpec priradený k atribútu, nemožno zmeniť.
- Atribúty používané v definíciách existujúcich tried objektov nemožno vymazať.

- Triedy objektov, ktoré sa používajú v ľubovoľnej existujúcej položke adresára, nemožno vymazať.

Zmeny v schéme, ktorá má vplyv na prevádzku servera, nie sú povolené. Adresárový server vyžaduje nasledujúce definície schémy. Tieto sa nesmú meniť.

Triedy objektov:

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

Atribúty:

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

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

- os400-usropt
- ou, organizationalUnit, organizationalUnitName
- owner
- ownerPropagate
- ownerSource
- ref
- replicaBindDN
- replicaBindMethod
- replicaCredentials, replicaBindCredentials
- replicaHost
- replicaPort
- replicaUpdateTimeInterval
- replicaUseSSL
- seeAlso

Syntaxi:
Všetky

Pravidlá zhody:
Všetky

Kontrolovanie schémy

Keď sa server inicializuje, súbory schémy sa čítajú a kontroluje sa ich konzistentnosť a správnosť. Ak kontroly nebudú úspešné, server sa nedokáže inicializovať a vydá chybové hlásenie. Aj počas každej zmeny dynamickej schémy sa kontroluje konzistentnosť a správnosť výslednej schémy. Ak kontroly neboli úspešné, vráti sa chyba a zmena zlyhá. Niektoré zmeny sú súčasťou gramatiky (napríklad typ atribútu môže mať najviac jeden nadtyp, alebo trieda objektov môže mať ľubovoľný počet nadtried).

Pri typoch atribútov sa kontrolujú nasledujúce položky:

- Dva rôzne typy atribútov nemôžu mať rovnaký názov alebo OID.
- Hierarchia dedenia typov atribútov nemá cykly.
- Nadtyp typu atribútu musí byť tiež definovaný, aj keď jeho definícia sa môže zobraziť neskôr alebo v samostatnom súbore.
- Ak je typ atribútu podtypom iného typu atribútu, obidva budú mať rovnaký atribút USAGE.
- Všetky typy atribútov majú buď priamo definovanú alebo zdedenú syntax.
- Iba prevádzkové atribúty môžu byť označené ako NO-USER-MODIFICATION.

Pri triedach objektov sa kontrolujú nasledujúce položky:

- Dve rôzne triedy objektov nemôžu mať rovnaký názov alebo OID.
- Hierarchia dedenia tried objektov nemá cykly.
- Nadtriedy triedy objektov musia byť tiež definované, hoci ich definície sa môžu objaviť neskôr alebo v samostatnom súbore.
- Musia byť definované aj typy atribútov ″MUST″ a ″MAY″ triedy objektov, hoci ich definície sa môžu objaviť neskôr alebo v samostatnom súbore.
- Každá štrukturálna trieda objektov je priamou alebo nepriamou podtriedou triedy top.
- Ak má abstraktná trieda objektov nadtriedy, tieto nadtriedy musia byť tiež abstraktné.

Kontrola vhodnosti položky pre schému

Keď sa položka pridá alebo modifikuje prostredníctvom operácie LDAP, skontroluje sa vhodnosť položky pre schému. Štandardne sa vykonajú všetky kontroly, ktoré sú uvedené v tejto časti. Vy však môžete cielene niektoré kontroly schémy zakázať, keď zmeníte úroveň kontroly schémy. To sa vykonáva cez aplikáciu iSeries Navigator zmenou hodnoty poľa **Kontrola schémy** na stránke **Databáza/prípony** vlastností adresárového servera. Informácie o atribútoch konfigurácie schémy nájdete v časti “Schéma konfigurácie adresárového servera” na strane 216.

Aby bola položka v súlade so schémou, skontroluje sa, či položka spĺňa nasledujúce podmienky:

S ohľadom na triedy objektov:

- Musí mať aspoň jednu hodnotu typu atribútu ″objectClass″.
- Môže mať ľubovoľný počet pomocných tried objektov vrátane nuly. Toto nie je kontrola, ale objasnenie. Neexistujú žiadne voľby na jeho zakázanie.
- Môže mať ľubovoľný počet abstraktných tried objektov, ale iba ako výsledok dedenia z tried. To znamená, že pri každej abstraktnej triede objektov, ktorú položka má, musí mať aj štrukturálnu alebo pomocnú triedu objektov, ktorá priamo alebo nepriamo dedí z tejto abstraktnej triedy objektov.
- Musí mať aspoň jednu štrukturálnu triedu objektov.
- Musí mať presne jednu bezprostrednú alebo základnú štrukturálnu triedu objektov. To znamená, že zo všetkých štrukturálnych tried objektov, ktorými je položka vybavená, tieto všetky musia byť nadtriedami presne jednej z nich. Najodvodzovanejšia trieda objektov sa nazýva ″bezprostredná″ alebo ″základná štrukturálna″ trieda objektov položky, alebo jednoducho ″štrukturálna″ trieda objektov položky.
- Nemôže zmeniť svoju bezprostrednú štrukturálnu triedu objektov (na ldap_modify).
- Pri každej triede objektov, ktorou je položka vybavená, sa množina jej všetkých priamych a nepriamych nadtried vypočíta; ak niektorou z týchto nadtried nie je položka vybavená, bude takáto nadtrieda automaticky pridaná.
- Ak je úroveň kontroly schémy nastavená na **Verzia 3 (prísne)** musia byť poskytnuté všetky štrukturálne nadtriedy. Napríklad, ak chcete vytvoriť položku s triedou objektov inetorgperson, musia byť špecifikované nasledujúce triedy objektov: person, organizationalperson a inetorgperson.

Platnosť typov atribútov pre položku sa stanovuje nasledovne:

- Množina typov atribútov MUST pre položku sa vypočíta ako zjednotenie množín typov atribútov MUST všetkých jej tried objektov, vrátane odvodených zdedených tried objektov. Ak množina typov atribútov MUST pre položku nie je podmnožinou množiny typov atribútov, ktoré položka obsahuje, položka bude odmietnutá.
- Množina typov atribútov MAY pre položku sa vypočíta ako zjednotenie množín typov atribútov MAY všetkých jej tried objektov, vrátane odvodených zdedených tried objektov. Ak množina typov atribútov, ktoré položka obsahuje, nie je podmnožinou zjednotenia množín typov atribútov MUST a MAY pre položku, položka bude odmietnutá.
- Ak bude niektorý z definovaných typov atribútov pre položku označený ako NO-USER-MODIFICATION, položka bude odmietnutá.

Platnosť hodnôt typov atribútov pre položku sa stanovuje nasledovne:

- Pri každom type atribútu, ktorý položka obsahuje, ak má tento typ atribútu mať jednu hodnotu, ale položka má viac ako jednu hodnotu, položka bude odmietnutá.
- Pri každej hodnote atribútu každého typu atribútu, ktorý položka obsahuje, ak jej syntax nebude v súlade s rutinou kontroly syntaxe pre syntax takéhoto atribútu, položka bude odmietnutá.
- Pri každej hodnote atribútu každého typu atribútu, ktorý položka obsahuje, ak je jej dĺžka väčšia ako maximálna dĺžka priradená takémuto typu atribútu, položka bude odmietnutá.

Platnosť DN sa kontroluje nasledovne:

- Skontroluje sa, či je syntax v súlade s BNF pre DistinguishedNames. Ak nie je v súlade, položka bude odmietnutá.
- Overí sa, či RDN tvoria iba typy atribútov, ktoré sú pre túto položku platné.
- Overí sa, či sa hodnoty typov atribútov, ktoré sa používajú v RDN objavia v položke.

Kompatibilita s iPlanet

Syntaktický analyzátor, ktorý používa adresárový server umožňuje špecifikáciu hodnôt atribútov pre typy atribútov schémy (objectClasses a attributeTypes) pomocou gramatiky iPlanet. Napríklad descrs a numeric-oids sa dajú špecifikovať uzavreté v jednoduchých úvodzovkách (ako keby boli qdescrs). Avšak informácie o schéme sa vždy sprístupňujú prostredníctvom ldap_search. Hneď ako bude v súbore vykonaná jedna dynamická zmena (pomocou ldap_modify) v hodnote atribútu, celý súbor bude nahradený súborom, v ktorom sa budú všetky hodnoty atribútov riadiť špecifikáciami adresárového servera. Pretože syntaktický analyzátor, ktorý sa používa pre súbory a požiadavky na ldap_modify je rovnaký, ldap_modify, ktorý pre hodnoty atribútov používa gramatiku iPlanet, bude tiež správne spracovaný.

Keď sa na položku podschémy servera iPlanet vytvorí dotaz, výsledná položka môže mať pre dané OID viac ako jednu hodnotu. Napríklad, ak má určitý typ atribútu dva názvy (napríklad 'cn' a 'commonName'), potom opis tohto typu atribútu bude poskytnutý dvakrát, pre každý názov raz. Adresárový server dokáže analyzovať schému, v ktorej sa opis jediného typu atribútu alebo triedy objektov objavuje viackrát s rovnakým opisom (s výnimkou NAME a DESCR). Keď však adresárový server zverejní schému, poskytne iba jeden opis takéhoto typu atribútu, pri ktorom budú uvedené všetky názvy (krátke názvy ako prvé). Napríklad takto iPlanet opisuje atribút common name:

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

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

Takto ho opisuje adresárový server:

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

Adresárový server podporuje podtypy. Ak nechcete, aby bol 'cn' podtypom názvu (ktorý sa odchyľuje od štandardu), môžete deklarovať nasledujúce:

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

Prvý názov ('cn') sa preberá ako preferovaný alebo krátky názov a všetky ostatné názvy za 'cn' ako alternatívne názvy. Počínajúc týmto okamihom sa reťazce '2.3.4.3', 'cn' a 'commonName' (rovnako ako aj ich ekvivalenty , v ktorých sa nerozlišuje veľkosť písmen) dajú navzájom zamieňať v rámci schémy alebo pre položky, pridané do adresára.

Zovšeobecnený čas a čas UTC

Existujú rôzne zápisy, ktoré sa používajú na označenie informácií ohľadne dátumu a času. Napríklad štvrtý deň februára v roku 1999 sa dá zapísať ako:

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

rovnako aj mnohými inými zápismi.

Adresárový server štandardizuje zobrazenie časovej značky, keď od serverov LDAP vyžaduje podporu dvoch syntaxí:

- Syntax zovšeobecneného času, ktorá je vo forme:
  `YYYYMMDDHHMMSS[.|,fraction][(+|-HHMM)|Z]`

  Sú v nej 4 číslice pre rok, po 2 čísliciach pre mesiac, deň, hodinu, minútu a sekundu a voliteľný zlomok sekundy. Bez akýchkoľvek ďalších dodatkov sa predpokladá, že dátum a čas je z miestneho časového pásma. Ak chcete indikovať, že čas sa meria v Koordinovanom svetovom čase, k času alebo k rozdielu miestneho času pripojte veľké písmeno Z. Napríklad:

```
"19991106210627.3"
```

čo v miestnom čase vyjadruje 6 minút, 27,3 sekúnd po 21. hodine, 6 november 1999.

```
"19991106210627.3Z"
```

čo je vyjadrené v koordinovanom svetovom čase.

```
"19991106210627.3-0500"
```

čo je miestny čas, ako v prvom príklade, s 5 hodinovým rozdielom vo vzťahu ku koordinovanému svetovému času.

Ak označíte voliteľný zlomok sekundy, vyžaduje sa bodka alebo čiarka. Pre rozdiel miestneho času platí, že pred jeho hodnotou hodina-minúta sa musí uvádzať znamienko '+' alebo '-'

- Syntax svetového času, ktorá je vo forme:

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

Syntax má po 2 čísliciach pre rok, mesiac, deň, hodinu, minútu a voliteľné polia sekúnd. Ako pri atribúte GeneralizedTime aj tu sa dá špecifikovať voliteľný časový rozdiel. Napríklad, ak je miestny čas predpoludnie 2. január 1999 a koordinovaný svetový čas je poludnie 12 hodín 2. januára 1999, hodnota UTCTime je buď:

```
"9901021200Z"
alebo "9901020700-0500"
```

Napríklad, ak je miestny čas predpoludnie 2. január 2001 a koordinovaný svetový čas je poludnie 12 hodín 2. januára 2001, hodnota UTCTime je buď:

```
"0101021200Z"
alebo "0101020700-0500"
```

UTCTime povoľuje pre hodnotu roku iba 2 číslice, preto sa jeho používanie neodporúča.

Podporované pravidlá zhody sú generalizedTimeMatch pre rovnosť a generalizedTimeOrderingMatch pre nerovnosť. Vyhľadávanie podreťazca nie je povolené. Napríklad platné sú nasledujúce filtre:

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

Nasledujúce filtre sú neplatné:

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

Zverejňovanie

i5/OS poskytuje schopnosť, že systém bude publikovať určité druhy informácií do adresára LDAP. To znamená, že systém vytvorí a bude aktualizovať položky LDAP, ktoré predstavujú rôzne typy údajov.

i5/OS má vstavanú podporu pre publikovanie nasledovných informácií na server LDAP:

Užívatelia

Keď nakonfigurujete operačný systém, aby publikoval informačný typ Užívatelia na adresárový server, automaticky exportuje položky zo systémového distribučného adresára na adresárový server. AS/400 použije aplikačné rozhranie programu (API) QGLDSSDD. AS/400 tiež synchronizuje adresár LDAP so zmenami vykonanými v systémovom distribučnom adresári. Informácie o API QGLDSSDD si pozrite v časti "API adresárového servera" v téme Programovanie.

Publikovanie užívateľov je užitočné pre poskytovanie LDAP vyhľadávacieho prístupu k informáciám zo systémového distribučného adresára (napríklad na poskytnutie prístupu LDAP k adresnej knihe pre POP3 poštových klientov podporujúcich LDAP ako je Netscape Communicator alebo Microsoft Outlook Express).

Publikovaní užívatelia sa môžu používať aj na podporu autentifikácie LDAP, pričom niektorí užívatelia budú publikovanými zo systémového distribučného adresára a iní užívatelia pridané do adresára inými prostriedkami. Zverejnený užívateľ má atribút uid, ktorý pomenúva užívateľský profil a nemá atribút userPassword. Keď sa z takejto položky prijme požiadavku na vytvorenie väzby, server zavolá bezpečnosť operačného systému na overenie uid a hesla ako platného užívateľského profilu a hesla pre tento profil. Ak chcete použiť autentifikáciu LDAP a chceli by ste, aby existujúci užívatelia boli schopní autentifikácie pomocou ich hesiel operačného systému, zatiaľ užívatelia iných systémov ako i5/OS sa pridávajú do adresára manuálne, vyskúšajte túto funkciu.

Iným spôsobom na publikovanie užívateľov, je zobrať položky z existujúceho validačného zoznamu HTTP a vytvoriť zodpovedajúce položky LDAP v adresárovom serveri. To sa vykoná cez aplikačné rozhranie programu (API) QGLDPUBVL. Toto API vytvorí položky adresára inetOrgPerson s heslami, ktoré sú prepojené k pôvodnej položke validačného zoznamu. Toto API je možné spustiť raz alebo naplánovať na pravidelné spúšťanie za účelom kontroly nových položiek, ktoré sa majú pridať do adresárového servera.

Poznámka: Toto API podporuje len položky validačného zoznamu, vytvorené na používanie so Serverom HTTP (využívajúci Apache). Existujúce položky v adresárovom serveri nebudú aktualizované. Užívatelia, ktorí boli vymazaní z validačného zoznamu, nebudú zistení.

Po pridaní užívateľov do adresára sa títo môžu autentifikovať k aplikáciám, ktoré používajú overovanie, ako aj k aplikáciám, ktoré podporujú autentifikáciu LDAP. Bližšie informácie o QGLDPUBVL API nájdete v časti "Rozhrania API adresárového servera" v téme Programovanie.

Informácie o systéme

Keď nakonfigurujete operačný systém, aby publikoval informačný typ Systém na adresárový server, budú sa publikovať nasledovné typy informácií.

- Základné informácie o tomto počítači a o vydaní operačného systému.
- Voliteľne môžete vybrať na zverejnenie jednu alebo viaceré tlačiarne. V takomto prípade bude systém automaticky synchronizovať adresár LDAP podľa zmien, ktoré sa na takýchto tlačiarňach uskutočnia.

K informáciám o tlačiarni, ktoré sa môžu zverejniť patrí:

- Umiestnenie
- Rýchlosť tlače v stránkach za minútu
- Podpora pre obojstrannú tlač a farbu
- Typ a model
- Opis

Táto informácia pochádza z opisu zariadenia v systéme, ktorý je publikovaný. V sieťovom prostredí môžu užívatelia použiť túto informáciu pri výbere tlačiarne. Informácie sa najprv zverejnia pri výbere tlačiarne na zverejnenie a bude sa aktualizovať, keď sa zapisovač tlačiarne zastaví alebo spustí, alebo keď sa zmení opis tlačového zariadenia.

Zdieľania tlačiarne

Keď nakonfigurujete operačný systém, aby publikoval zdieľania tlačiarní, budú sa publikovať informácie o zvolených zdieľaniach tlačiarní aplikácie iSeries NetServer na nakonfigurovaný aktívny adresárový server. Publikovanie zdieľaní tlače na aktívny adresár umožňuje užívateľom pridávať tlačiarne iSeries na ich pracovnú plochu systému Windows 2000 pomocou Sprievodcu pridaním tlačiarne systému Windows 2000 . Aby ste to mohli urobiť pomocou Sprievodcu pridaním tlačiarne, uveďte, že chcete nájsť tlačiareň vo Windows 2000 Active Directory. Zdieľania tlačiarne musíte zverejniť do adresárového servera, ktorý podporuje schému Active Directory spoločnosti Microsoft.

TCP/IP Quality of Service

Server Kvalita služieb TCP/IP (QOS) je možné nakonfigurovať tak, aby používal zdieľanú politiku QOS definovanú v adresári LDAP pomocou schémy definovanej spoločnosťou IBM. Na čítanie informácií o politike používa server QoS publikačného agenta TCP/IP QOS. Tieto informácie definujú server, informácie o autentifikácii a kde v adresári sú informácie o politike uložené.

Takisto môžete vytvoriť aplikáciu na zverejňovanie alebo vyhľadávanie ostatných druhov informácií v adresári LDAP s použitím tejto štruktúry, keď zadefinujete ďalších publikačných agentov a budete používať API pre zverejňovanie adresárov. Bližšie informácie nájdete v časti “Publikovanie informácií na adresárový server” na strane 90 a Rozhrania API adresárového servera v téme Programovanie.

Replikácia

Replikácia je technika, ktorú používajú adresárové servery na zlepšenie výkonnosti a spoľahlivosti. Replikačný proces uchováva údaje vo viacerých adresároch synchronizované.

Informácie o spôsobe správy replikácie nájdete v časti “Riadenie replikácie” na strane 127. Bližšie informácie o replikácii nájdete na nasledovných miestach:

- “Prehľad replikácie”
- “Názvoslovie pre replikáciu” na strane 39
- “Zmluvy o replikácii” na strane 40
- “Ako sú v serveri uložené informácie o replikácii” na strane 40
- “Bezpečnostné hľadiská pre informácie replikácie” na strane 41
- “Replikácia v prostredí s vysokou dostupnosťou” na strane 41

Prehľad replikácie

Replikácia poskytuje dve hlavné výhody:

- Redundanciu informácií - repliky zálohujú obsah svojich dodávateľských serverov.
- Rýchlejšie vyhľadávania - požiadavky na vyhľadávanie sa dajú rozdeliť medzi niekoľko rôznych serverov, ktoré majú rovnaký obsah, namiesto poslania do jediného servera. To zlepšuje čas odozvy pre dokončenie požiadavky.

Špecifické položky v adresári sú identifikované ako korene replikovaných podstromov tak, že sa do nich pridá trieda objektov ibm-replicationContext. Každý podstrom sa replikuje samostatne. Podstrom pokračuje smerom nadol cez strom informácií o adresári (DIT) kým nedosiahne položky na listoch alebo iné replikované podstromy. Položky sa pridajú pod koreň replikovaného podstromu, aby obsahovali informácie o topológii replikácie. Tieto položky sú položky jednej alebo viacerých skupín replík, pod ktorými sa vytvárajú podpoložky replík. Ku každej podpoložke repliky sú priradené zmluvy o replikácii, ktoré identifikujú servery, ktoré dodáva (replikuje) každý server, ako aj definovanie poverení a informácií o plánovaní.

Počas replikácie sa bude zmena vykonaná v jednom adresári šíriť do jedného alebo viacerých ďalších adresárov. V skutočnosti sa zmena v jednom adresári prejaví vo viacerých rôznych adresároch. Adresár IBM podporuje rozvinutý replikačný model nadriadený-podriadený. Replikačné topológie sú rozvinuté, aby zahŕňali:

- Replikáciu podstromov DIT (Directory Information Tree) do špecifických serverov
- Viacvrstvovú topológiu, ktorá sa označuje ako kaskádovitá replikácia
- Priradenie role servera (hlavný alebo replika) pomocou podstromu.
- Viaceré hlavné servery, čo sa označuje ako rovnocenná replikácia.
- Replikácia pomocou brány v sieťach.

Replikovanie pomocou podstromov má tú výhodu, že replika nemusí replikovať celý adresár. Môže to byť replika časti alebo podstromu adresára.

Rozvinutý model mení koncept hlavný a replika. Tieto pojmy už ďalej neplatia pre servery, ale skôr pre roly, ktoré má server s ohľadom na určitý replikovaný podstrom. Server môže pri niektorých podstromoch vystupovať ako hlavný a pri

ostatných zas ako replika. Pojem Hlavný sa používa pre server, ktorý akceptuje klientske aktualizácie pre replikovaný podstrom. Pojem Replika sa používa pre server, ktorý akceptuje iba aktualizácie z ostatných serverov, ktoré sú označené ako dodávateľ pre replikovaný podstrom.

Typy serverov definované funkciou sú *hlavný/rovnocenný*, *kaskádovitý*, *brána* a *replika*.

Tabuľka 1. Roly servera

Adresár	Opis
Hlavný/rovnocenný	Hlavný/rovnocenný server obsahuje informácie o hlavnom adresári, z ktorého sa aktualizácie rozširujú do replík. Všetky zmeny sa vykonávajú a dochádza k nim na hlavnom serveri a hlavný server je zodpovedný za rozšírenie týchto zmien do replík. Pre informácie o adresároch môže existovať niekoľko serverov, ktoré vystupujú ako hlavné servery, pričom je každý hlavný server zodpovedný za aktualizovanie ostatných hlavných serverov a replikačných serverov. Označuje sa to ako rovnocenná replikácia. Rovnocenná replikácia dokáže zlepšiť výkonnosť a spoľahlivosť. Výkonnosť sa zlepší, keď poskytnete lokálny server na spracovanie aktualizácií v široko distribuovanej sieti. Spoľahlivosť sa zlepší, keď pripravíte záložný hlavný server, aby mohol okamžite nahradiť primárny hlavný server, v prípade zlyhania. **Poznámky:** 1. Hlavné servery replikujú všetky klientske aktualizácie, ale nereplikujú aktualizácie, ktoré boli prijaté z iných hlavných serverov. 2. Aktualizovanie rovnakej položky viacerými servermi môže spôsobiť nezrovnalosti v údajoch adresára, pretože nebol spozorovaný konflikt.
Kaskádovitý (posielajúci ďalej)	Kaskádovitý server je replikačný server, ktorý replikuje všetky zmeny, ktoré boli do neho odoslané. Tým sa odlišuje od hlavného/rovnocenného servera, že hlavný/rovnocenný server replikuje iba zmeny, ktoré vykonali klienti, ktorí sú k takémuto serveru pripojení. Kaskádovitý server dokáže uvoľniť replikačné pracovné zaťaženie z hlavných serverov v sieti, ktoré obsahujú veľké množstvo rozptýlených replík.
Brána	Replikácia pomocou brány pomocou bránových serverov zhromažďuje a efektívne distribuuje informácie o replikácii po replikačnej sieti. Primárnou výhodou replikácie brány je zníženie intenzity sieťovej premávky.
Replika (iba na čítanie)	Replika je doplnkový server, ktorý obsahuje kópiu informácií o adresári. Repliky sú kópie hlavného adresára (alebo podstromu, z ktorého replika pochádza). Replika poskytuje zálohu replikovaného podstromu.

Ak replikácia zlyhá, zopakuje sa a to aj vtedy, keď bude hlavný server reštartovaný. Okno Riadenie frontov vo webovom administratívnom nástroji sa dá použiť na kontrolu zlyhávajúcej replikácie.

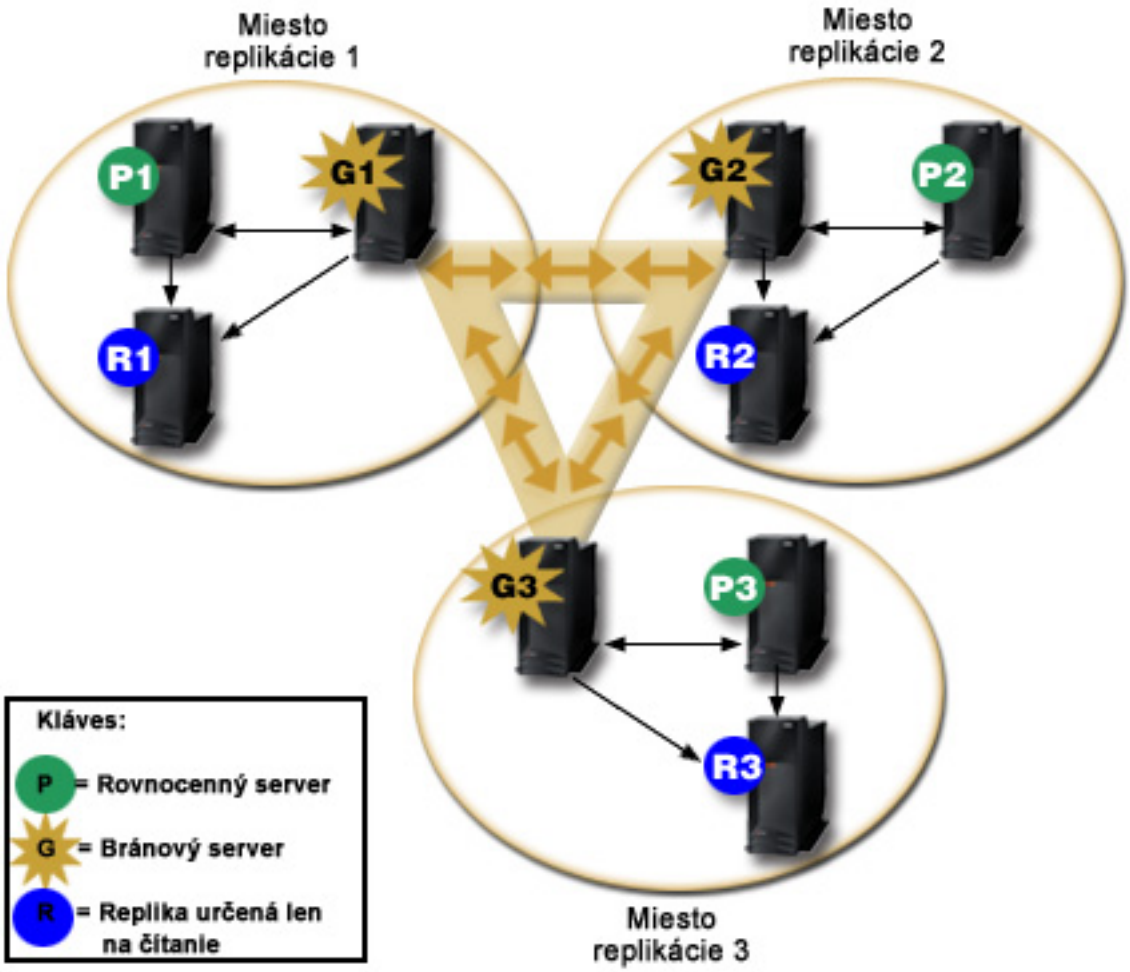
Môžete požadovať aktualizácie na replikačnom serveri, ale aktualizácia sa v skutočnosti pošle ďalej do hlavného servera vrátením odvolávky do klienta. Ak bude aktualizácia úspešná, hlavný server potom odošle aktualizáciu do replík. Kým hlavný server nedokončí replikáciu aktualizácie, zmena sa neprejaví na replikačnom serveri, na ktorom bola pôvodne požadovaná. Zmeny sa replikujú v poradí, v ktorom boli na hlavnom serveri uskutočnené.

Ak už repliku viac nepoužívate, musíte z dodávateľa odstrániť zmluvu o replikácii. Ponechanie definície spôsobí, že server bude zaraďovať do frontu všetky aktualizácie a bude zbytočne používať potrebný adresárový priestor. Takisto dodávateľ sa bude stále pokúšať o spojenie s chýbajúcim spotrebiteľom, aby sa pokúsil o opakované odoslanie údajov.

Replikácia pomocou brány

Replikácia pomocou brány pomocou bránových serverov zhromažďuje a efektívne distribuuje informácie o replikácii po replikačnej sieti. Primárnou výhodou replikácie brány je zníženie intenzity sieťovej premávky. Bránové servery musia byť hlavné (zapisovateľné).

Nasledovný obrázok ilustruje spôsob práce replikácie pomocou brány:



Obrázok 2. Replikačná sieť s bránovými servermi

Replikačná sieť na predchádzajúcom obrázku obsahuje tri replikačné miesta, z ktorých každé obsahuje bránový server. Bránový server zhromažďuje aktualizácie replikácie z hlavných/rovnocenných serverov v replikačnom mieste, kde sa nachádza a posiela tieto aktualizácie na všetky ostatné bránové servery v replikačnej sieti. Zhromažďuje tiež aktualizácie replikácie z ostatných bránových serverov v replikačnej sieti a odosiela tieto aktualizácie na hlavné/rovnocenné servery v replikačnej sieti, kde sa nachádza.

Bránové servery pomocou ID serverov a ID spotrebiteľov určia, ktoré aktualizácie sa pošlú na iné bránové servery v replikačnej sieti a ktoré aktualizácie sa pošlú na lokálne servery v replikačnej sieti.

Ak chcete nastaviť replikáciu pomocou brány, musíte vytvoriť minimálne dva bránové servery. Vytvorením bránového servera sa vytvorí replikačné miesto. Potom musíte vytvoriť zmluvy o replikácii medzi bránou a všetkými hlavnými/rovnocennými servermi, ktoré chcete zahrnúť do replikačného miesta tejto brány.

Bránové servery musia byť hlavné (zapisovateľné). Ak sa pokúsite pridať triedu objektu brány, ibm-replicaGateway, do podpoložky, ktorá nie je hlavnou, vráti sa chybové hlásenie.

Na vytvorenie bránového servera sú dve metódy. Môžete:

- Vytvoriť nový bránový server
- Skonvertovať existujúci rovnocenný server na bránový server

Poznámka: Je veľmi dôležité, aby ste jednému replikačnému miestu priradili len jeden bránový server.

Názvoslovie pre replikáciu

Časť názvoslovia, ktorá sa používa pri opise replikácie:

Kaskádovitá replikácia
Topológia replikácie, v ktorej existujú viaceré vrstvy serverov. Rovnocenný/hlavný server replikuje do množiny serverov iba-na-čítanie (posielajúcich ďalej), ktoré zas replikujú do ostatných serverov. Takáto topológia znižuje zaťaženie hlavných serverov pri replikačnej činnosti.

Spotrebiteľský server
Server, ktorý prijíma zmeny prostredníctvom replikácie z iného (dodávateľského) servera.

Poverenia
Identifikujú metódu a povinné informácie, ktoré dodávateľ používa pri vytváraní väzieb na spotrebiteľa. Pri jednoduchých väzbách je tu zahrnuté DN a heslo. Poverenia sú uložené v položke DN, ktorá je špecifikovaná v zmluve o replikácii.

Postupovací server
Server iba-na-čítanie, ktorý replikuje všetky zmeny, ktoré mu odošle hlavný alebo rovnocenný server. Požiadavky na aktualizáciu klientov sú odkazované na hlavný alebo rovnocenný server.

Bránový server
Server, ktorý posiela ďalej všetku replikačnú premávku z lokálneho replikačného miesta, kde sa nachádza, na iné bránové servery v replikačnej sieti. Bránový server prijíma replikačnú premávku od iných bránových serverov v replikačnej sieti, ktorú posiela ďalej všetkým serverom vo vlastnom replikačnom mieste. Bránové servery musia byť hlavné (zapisovateľné).

Hlavný server
Server, do ktorého sa dá zapisovať (dá sa aktualizovať) pre daný podstrom.

Vnorený podstrom
Podstrom vo vnútri replikovaného podstromu adresára.

Rovnocenný server
Pojem používaný pre hlavný server, keď pre daný podstrom existuje viacero hlavných serverov.

Skupina replík
Prvá položka vytvorená pod kontextom replikácie má triedu objektov ibm-replicaGroup a predstavuje kolekcia serverov, ktoré sa zúčastňujú na replikácii. Poskytuje vhodné umiestnenie pre nastavenie ACL na ochranu informácií o topológii replikácie. Nástroje pre správu v súčasnosti podporujú jednu skupinu replík pod každým kontextom replikácie, ktorá sa nazýva **ibm-replicagroup=default**.

Podpoložka repliky
Pod položkou skupiny replík je možné vytvoriť jednu alebo viac položiek s triedou objektu ibm-replicaSubentry, jednu pre každý server zúčastňujúci sa replikácie ako dodávateľ. Podpoložka repliky identifikuje rolu, ktorú má server v replikácii : hlavný alebo iba-na-čítanie. Server iba-na-čítanie môže mať zas zmluvy o replikácii pre podporu kaskádovitej replikácie.

Replikovaný podstrom
Časť DIT, ktorá sa replikuje z jedného servera na druhý. V tejto úprave sa môže daný podstrom replikovať do niektorých serverov, ale nie do iných. Podstrom môže byť zapisovateľný na danom serveri, zatiaľ čo iné podstromy môžu byť len na čítanie.

Replikačná sieť
Sieť, ktorá obsahuje pripojené replikačné miesta.

Zmluva o replikácii
Informácie, ktoré obsahuje adresár, ktorý definuje ’pripojenie’ alebo ’replikačnú cestu’ medzi dvoma servermi. Jeden server sa nazýva dodávateľ (server, ktorý odosiela zmeny) a druhý je spotrebiteľ (server, ktorý prijíma zmeny). Zmluva obsahuje všetky informácie, ktoré sú potrebné na vytvorenie pripojenia z dodávateľa do spotrebiteľa a pre plánovanie replikácie.

Kontext replikácie
Identifikuje koreň replikovaného podstromu. Pomocnú triedu objektu ibm-replicationContext možno pridať do položky na jej označenie ako koreňa replikačnej oblasti. Informácie súvisiace s topológiou replikácie sa udržiavajú v množine položiek, ktoré boli vytvorené pod kontextom replikácie.

Replikačné miesto
Bránový server a akékoľvek hlavné, rovnocenné a replikačné servery nakonfigurované na spoločnú replikáciu.

Plán Replikácia sa dá naplánovať, aby sa uskutočnila v určitom čase, so zmenami, ktoré dodávateľ nazhromaždil a odoslal v dávke. Zmluva o replike obsahuje DN pre položku ktorá dodáva plán.

Dodávateľský server
Server, ktorá odosiela zmeny do iného (spotrebiteľského) servera.

Zmluvy o replikácii

Zmluva o replikácii je položka v adresári s triedou objektov **ibm-replicationAgreement**, ktorá bola vytvorená pod podpoložkou repliky, aby definovala replikáciu zo servera, ktorý podpoložka zastupuje, do iného servera. Tieto objekty sa podobajú na položky replicaObject, ktoré používali predchádzajúce verzie adresárového servera. Zmluva o replikácii obsahuje nasledujúce položky:

- Užívateľsky orientovaný názov, ktorý sa používa ako atribút názvu pre zmluvu.
- LDAP URL, ktoré špecifikuje server, číslo portu a či sa má použiť SSL.
- Ak je známe, ID spotrebiteľského servera. Adresárové servery do verzie V5R3 nemajú ID servera.
- DN objektu, ktorý obsahuje poverenia, ktoré dodávateľ používa na vytvorenie väzby na spotrebiteľa.
- Voliteľný smerník DN na objekt, ktorý obsahuje informácie o pláne pre replikáciu. Ak atribút nie je prítomný, zmeny sa budú replikovať okamžite.

Užívateľsky orientovaný názov môže byť názvom spotrebiteľského servera alebo iný opisný reťazec.

ID spotrebiteľského servera používa administratívne GUI na prechádzanie topológie. Zadaním ID servera spotrebiteľa môže GUI vyhľadať zodpovedajúcu podpoložku a jej zmluvy. Aby sa uľahčilo vynútenie presnosti údajov, keď dodávateľ vytvára väzby na spotrebiteľa, získa ID servera z koreňového DSE a porovná ho s hodnotou v zmluve. Ak sa ID servera nezhodujú, zaprotokoluje sa varovanie.

Pretože zmluva o replikácii sa dá replikovať, používa sa DN pre objekt poverení. To umožňuje ukladanie poverení v nereplikovanej oblasti adresára. Replikovanie objektov poverení (z ktorých sa musí dať získať 'čistý text' poverenia) predstavuje možné bezpečnostné riziko. Prípona cn=localhost je vhodným štandardným umiestnením pre vytvorenie objektov poverení.

Triedy objektov sú definované pre každú z podporovaných metód autentifikácie:

- Jednoduchá väzba
- SASL
- Mechanizmus EXTERNAL so SSL
- Autentifikácia Kerberos

Môžete označiť, aby sa časť replikovaného podstromu nereplikovala, keď do koreňa podstromu pridáte pomocnú triedu ibm-replicationContext a nebudete definovať žiadne podpoložky repliky.

Poznámka: Webový administratívny nástroj odkazuje na zmluvy aj ako na 'fronty', keď odkazuje na množinu zmien, ktoré čakajú na replikáciu podľa danej zmluvy.

Ako sú v serveri uložené informácie o replikácii

Informácie o replikácii sa v adresári ukladajú na troch miestach:

- Konfigurácia servera, ktorá obsahuje informácie o tom, ako sa ostatné servery môžu autentifikovať na tento server, aby vykonali replikáciu (napríklad komu tento server umožňuje, aby vystupoval ako dodávateľ).

- Do adresára na vrchole replikovaného podstromu. Ak sa ″o=my company″ nachádza na vrchole replikovaného podstromu, objekt s názvom ″ibm-replicagroup=default″ sa vytvorí priamo pod ním (ibm-replicagroup=default,o=my company). Pod objektom ″ibm-replicagroup=default″ budú ďalšie objekty, ktoré opisujú servery uchovávajúce repliky podstromu a zmluvy medzi servermi.
- Objekt s názvom ″cn=replication,cn=localhost″ sa používa na zahrnutie informácií replikácie, ktoré používa iba jeden server. Napríklad objekt, ktorý obsahuje poverenia, ktoré používa dodávateľský server potrebuje iba dodávateľský server. Poverenia sa môžu umiestniť pod ″cn=replication,cn=localhost″, čím sa sprístupnia iba pre tento server.
- Objekt s názvom ″cn=replication, cn=IBMpolicies″ sa používa na uloženie informácií o replikácii na iné servery.

Bezpečnostné hľadiská pre informácie replikácie

Zrevidujte bezpečnostné hľadiská pre nasledujúce objekty:

- ibm-replicagroup=default: Ovládacie prvky prístupu na tomto objekte riadia, kto si môže prezerať alebo meniť informácie replikácie, ktoré sú tu uložené. Tento objekt štandardne dedí riadenie prístupu od svojho rodiča. Mali by ste zvážiť nastavenie riadenia prístupu na tomto objekte pre obmedzenie prístupu k informáciám replikácie. Napríklad mohli by ste definovať skupinu, ktorá obsahuje užívateľov, ktorí budú replikáciu riadiť. Túto skupinu môžete spraviť vlastníkom objektu ″ibm-replicagroup=default″ a ostatným užívateľom neposkytnete žiadny prístup k objektu.
- cn=replication,cn=localhost: Pri tomto objekte existujú dve bezpečnostné hľadiská:
  - Riadenie prístupu na tomto objekte riadi, kto si môže prezerať alebo aktualizovať objekty, ktoré sú tu uložené. Štandardné riadenie prístupu umožňuje anonymným užívateľom čítať väčšinu informácií, s výnimkou hesiel a na pridávanie, zmenu alebo vymazanie objektov vyžaduje administrátorské oprávnenie.
  - Objekty uložené v ″cn=localhost″ sa nikdy nereplikujú do iných serverov. Replikačné poverenia môžete umiestniť do tohto kontajnera na serveri, ktorý tieto poverenia používa, a potom nebudú prístupné pre iné servery. Alebo sa môžete rozhodnúť umiestniť poverenia pod objekt ″ibm-replicagroup=default″, takže viaceré servery budú zdieľať rovnaké poverenia.
- cn=IBMpolicies: Do tohto kontajnera môžete umiestniť replikačné poverenia, ale údaje v ňom sa replikujú akémukoľvek spotrebiteľovi servera. Umiestnenie povoľovacích údajov v cn=replication,cn=localhost sa považuje za bezpečnejšie.

Replikácia v prostredí s vysokou dostupnosťou

Adresárový server je často využívaný v riešeniach s jedným prihlásením, čo môže mať za následok jednoduchý bod zlyhania. Adresárový server je možné široko sprístupniť pomocou replikácie dvoma spôsobmi: pomocou aplikácie IBM Load Balancer alebo prevzatia adresy IP. Bližšie informácie o tejto téme možno nájsť v Kapitole 13.2 publikácie IBM Redbook IBM WebSphere V5.1 Performance, Scalability, and High Availability. 

Realmy a užívateľské šablóny

Realmy a objekty šablóny, nájdené vo webovom administratívnom nástroji, sa používajú, aby bol užívateľ zbavený potreby poznať niektoré podstatné otázky LDAP.

Realm identifikuje kolekciu užívateľov a skupín. V plochej adresárovej štruktúre špecifikuje informácie, napríklad kde sú umiestnení užívatelia a kde sú umiestnené skupiny. Realm definuje umiestnenie pre užívateľov (napríklad ″cn=users,o=acme,c=us″) a vytvára užívateľov ako okamžitých podriadených tejto položky (napríklad John Doe bude vytvorený ako ″cn=John Doe,cn=users,o=acme,c=us″). Môžete definovať viacero realmov a môžete im dať bežné názvy (napríklad weboví užívatelia). Bežný názov môžu použiť ľudia, ktorí vytvárajú a udržiavajú užívateľov.

Šablóna opisuje, ako užívateľ vyzerá. Špecifikuje triedy objektov, ktoré sa používajú pri vytváraní užívateľov (aj štrukturálnu triedu objektov aj všetky pomocné triedy, ktoré chcete). Šablóna tiež špecifikuje rozmiestnenie panelov, ktoré sa používajú na vytváranie alebo úpravu užívateľov (napríklad názvy záložiek, štandardné hodnoty a atribúty, ktoré sa majú objaviť na každej záložke).

Keď pridáte nový realm, v adresári vytvárate objekt ibm-realm. Objekt ibm-realm dozerá na vlastnosti realmu, napríklad kde sú definovaní užívatelia a skupiny a na to, aká šablóna sa má použiť. Objekt ibm-realm môže ukazovať na existujúcu položku adresára, ktorá je rodičom užívateľov, alebo môže ukazovať na seba (štandard), čím sa z neho stáva kontajner pre nových užívateľov. Napríklad môžete mať existujúci kontajner cn=users,o=acme,c=us a niekde inde v adresári vytvoriť realm s názvom užívatelia (možno kontajnerový objekt s názvom cn=realms,cn=admin stuff,o=acme,c=us), ktorá identifikuje cn=users,o=acme,c=us ako umiestnenie pre užívateľov a skupiny. To vytvorí objekt ibm-realm:

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

Alebo, ak objekt cn=users,o=acme,c=us neexistoval, môžete realm užívatelia vytvoriť pod o=acme,c=us a nechať ju odkazovať na samu seba.

Administrátor adresárov je zodpovedný za riadenie užívateľských šablón, realmov a skupín administrátora realmov. Po vytvorení realmu sú členovia tejto administrátorskej skupiny realmu zodpovední za riadenie užívateľov a skupín v rámci tohto realmu.

Viac informácií o spôsobe riadenia realmov a užívateľských šablón nájdete v časti “Manažovanie realmov a šablón užívateľov” na strane 172.

Parametre vyhľadávania

Na ohraničenie množstva prostriedkov využívaných serverom môže administrátor nastaviť parametre vyhľadávania na obmedzenie vyhľadávacích možností užívateľa. Vyhľadávacie možnosti je možné rozšíriť pre špeciálnych užívateľov. Užívateľské vyhľadávania možno obmedziť alebo rozšíriť pomocou nasledovných metód:

Obmedziť vyhľadávanie

- Paged search
- Sorted search
- Zakázať dereferencovanie aliasov

Rozšíriť vyhľadávanie

- Skupiny s obmedzeniami vyhľadávania

Stránkované vyhľadávanie

Stránkované výsledky umožňujú klientovi spravovať množstvo údajov vrátených z požiadavky na vyhľadávanie. Klient namiesto prijímania naraz všetkých výsledkov zo servera môže požadovať podmnožinu položiek (stránku). Následné požiadavky na vyhľadávanie vrátia nasledujúcu stránku výsledkov, kým sa operácia nezruší, alebo kým sa nevráti posledný výsledok. Administrátor môže obmedziť jeho použitie len povolením jeho používania administrátormi.

Triedené vyhľadávanie

Triedené vyhľadávanie umožňuje klientovi prijímať výsledky vyhľadávania utriedené podľa zoznamu kritérií, kde každé kritérium predstavuje triediaci kľúč. Presúva sa tým zodpovednosť za triedenie z klientskej aplikácie na server.Administrátor môže obmedziť jeho použitie len povolením jeho používania administrátormi.

Zakázať dereferencovanie aliasov

Položka adresára s triedou objektu s hodnotou alias alebo aliasObject obsahuje atribút aliasedObjectName, ktorý sa používa na odkazovanie inej položky v adresári Len požiadavky na vyhľadávanie môžu špecifikovať, či sú aliasy diferencované. *Dereferencovanie* znamená sledovanie aliasu spätne až k pôvodnej položke. Čas odozvy Adresárového servera IBM pre vyhľadávania s voľbou dereferencovania aliasov nastavenou na **vždy** alebo **vyhľadávanie** by mohol byť dlhší ako čas odozvy pri voľbe dereferencovania nastavenou na **nikdy**, aj keby v adresári neexistovali žiadne položky aliasov. Dve nastavenia určujú správanie dereferencovania aliasov servera: voľba dereferencovania špecifikovaná klientskou požiadavkou na vyhľadávanie a voľba dereferencovania, ako je nakonfigurovaná na serveri administrátorom. Ak je server tak nakonfigurovaný, môže automaticky obísť dereferencovanie aliasov, ak v adresári neexistujú žiadne objekty aliasov, ako aj prepísať voľbu dereferencovania špecifikovanú v klientsky ch požiadavkách na vyhľadávanie. Nasledovná tabuľka popisuje, ako sa hašuje dereferencovanie aliasov medzi klientom a serverom.

Tabuľka 2. Skutočné dereferencovanie aliasov založené na nastaveniach klienta a servera

Server	Klient	Skutočné
nikdy	ľubovoľné nastavenie	nikdy
vždy	ľubovoľné nastavenie	nastavenie klienta
ľubovoľné nastavenie	vždy	nastavenie servera
vyhľadávanie	nájsť	nikdy
nájsť	vyhľadávanie	nikdy

Skupiny s obmedzeniami vyhľadávania

Administrátor môže vytvoriť skupinu s obmedzeniami vyhľadávania, ktorá môže mať flexibilnejšie obmedzenia vyhľadávania ako všeobecný užívateľ. Jednotlivým členom alebo skupinám nachádzajúcim sa v skupine s obmedzeniami vyhľadávania sa udelia menej obmedzujúce ohraničenia vyhľadávania, ako sú uložené pre všeobecných užívateľov.

Keď užívateľ zaháji vyhľadávanie, najskôr sa skontrolujú obmedzenia požiadavky na vyhľadávanie. Ak je užívateľ členom skupiny s obmedzeniami vyhľadávania, porovnajú sa obmedzenia. Ak sú ohraničenia skupiny s obmedzeniami vyhľadávania vyššie ako v prípade požiadavky na vyhľadávanie, použijú sa obmedzenia požiadavky na vyhľadávanie. Ak sú ohraničenia požiadavky na vyhľadávanie vyššie ako v prípade skupiny s obmedzeniami vyhľadávania, použijú sa obmedzenia skupiny s obmedzeniami vyhľadávania. Ak sa nenájdu žiadne položky skupiny s obmedzeniami vyhľadávania, rovnaké porovnanie sa vykoná voči ohraničeniam vyhľadávania na serveri. Ak neboli nastavené žiadne obmedzenia vyhľadávania na serveri, vykoná sa porovnanie voči predvolenému nastaveniu servera. Použité obmedzenia sú vždy najnižšie nastavenia v porovnávaní.

Ak užívateľ patrí do viacerých skupín s obmedzeniami vyhľadávania, užívateľovi sa pridelí až najvyššia úroveň schopnosti vyhľadávania. Napríklad, užívateľ patrí do skupiny vyhľadávania 1, ktorá udeľuje obmedzenie vyhľadávania pre veľkosť vyhľadávania 2000 položiek a dobu vyhľadávania 4000 sekúnd a do skupiny vyhľadávania 2, ktorá udeľuje obmedzenie vyhľadávania pre veľkosť vyhľadávania v neobmedzenom množstve a dobu vyhľadávania 3000 sekúnd. Užívateľ má obmedzenie vyhľadávania pre neobmedzenú veľkosť vyhľadávania a dobu vyhľadávania 4000 sekúnd.

Skupiny s limitmi vyhľadávania môžu byť uložené pod lokálnym hostiteľom alebo IBMpolicies. Skupiny s limitmi vyhľadávania pod IBMpolicies sú replikované, tie pod lokálnym hostiteľom nie sú. Tú istú skupinu s limitmi vyhľadávania môžete uložiť pod lokálneho hostiteľa aj IBMpolicies. Ak skupina s limitmi vyhľadávania nie je uložená pod jedným z týchto názvov DN, server bude ignorovať časť skupiny s obmedzením vyhľadávania a bude ju považovať za normálnu skupinu.

Keď užívateľ zaháji vyhľadávanie, najskôr sa skontrolujú položky skupiny s limitmi vyhľadávania pod lokálnym hostiteľom. Ak sa pre užívateľa nenájdu žiadne položky, potom sa prehľadajú položky skupiny s limitmi vyhľadávania pod IBMpolicies. Ak sa nájdu položky pod lokálnym hostiteľom, položky skupiny s limitmi vyhľadávania pod IBMpolicies sa nebudú kontrolovať. Položky skupiny s limitmi vyhľadávania pod lokálnym hostiteľom majú prednosť pred položkami pod IBMpolicies.

Bližšie informácie parametroch vyhľadávania nájdete v časti:

- "Úprava nastavení hľadania" na strane 123
- "Hľadanie položiek adresára" na strane 166
- "Riadenie skupín limitov vyhľadávania" na strane 117

Charakteristiky národnej jazykovej podpory (NLS)

Počítajte s nasledujúcimi hľadiskami NLS:

- Údaje sa prenášajú medzi servermi LDAP a klientmi vo formáte UTF-8. Všetky znaky ISO 10646 sú povolené.
- Adresárový server používa na ukladanie údajov do databázy metódu mapovania UTF-16.
- Server a klient vykonávajú porovnávanie reťazcov, ktoré nerozlišuje malé a veľké písmená. Algoritmus veľkých písmen neodstráni chybu pre všetky jazyky (lokály).

Viac informácií o UCS-2 nájdete v časti "Globalizácia" v téme Plánovanie.

Jazykové značky

Termín *Jazykové značky* definuje mechanizmy, ktoré umožňujú, aby adresár priraďoval kódy prirodzeného jazyka k hodnotám uloženým v adresári a umožnil klientom vyžiadať dotazom od adresára hodnoty, ktoré spĺňajú určité požiadavky prirodzeného jazyka. Jazyková značka je komponent popisu atribútu. Jazyková značka je reťazec s predponou lang-, primárnou vedľajšou značkou z abecedných znakov a, voliteľne, následných vedľajších značiek pripojených pomocou pomlčky (-). Následné vedľajšie značky môžu byť ľubovoľnou kombináciou alfanumerických znakov, len primárna vedľajšia značka musí byť abecedná. Vedľajšie značky môžu mať ľubovoľnú dĺžku, jediným obmedzením je, aby celková dĺžka značky nepresahovala 240 znakov. Jazykové značky nerozlišujú veľkosť písmen, teda značky en-us, en-US a EN-US sú identické. Jazykové značky nie sú povolené v komponentoch DN alebo RDN. Povolená je len jedna jazyková značka na jeden popis atribútu.

Poznámka: Na báze jedného atribútu sa jazykové značky sa navzájom vylučujú s jedinečnými atribútmi. Ak máte určený konkrétny atribút ako jedinečný atribút, nemôže mať k sebe priradené jazykové značky.

Ak sú pri pridávaní údajov do adresára zahrnuté aj jazykové značky, možno ich použiť s vyhľadávacími operáciami na selektívnu obnovu hodnôt atribútov v konkrétnych jazykoch. Ak sa jazyková značka nachádza v popise atribútu v požadovanom zozname atribútov vyhľadávania, potom sa vrátia len hodnoty atribútov v položke adresára, ktoré majú rovnakú jazykovú značku ako tie zadané. Takže pri vyhľadávaní:

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

server vráti hodnoty atribútu ″description;lang-en″, ale nevráti hodnoty atribútu ″description″ alebo ″description;lang-fr″.

Ak sa vykoná požiadavka špecifikujúca atribút bez zadania jazykovej značky, vrátia sa všetky hodnoty atribútov, bez ohľadu na ich jazykovú značku.

Typ atribútu a jazyková značka sú oddelené znakom bodkočiarky (;).

Poznámka: Použitie znaku bodkočiarky je povolené v časti ″NAME″ v AttributeType. Keďže však tento znak sa používa na oddelenie AttributeType od jazykovej značky, jeho použitie v časti ″NAME″ v AttributeType nie je povolené.

Napríklad, ak klient požaduje atribút ″description″ a zhodná položka obsahuje:

```
 objectclass: top
 objectclass: organization
o: Software GmbH
description: softvér
```

```
description;lang-en: software products
description;lang-de: Softwareprodukte
postalAddress: Berlín 8001 Nemecko
postalAddress;lang-de: Berlin 8001 Deutschland
```

server vráti:

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

Ak vyhľadávanie požaduje atribút ″description;lang-de″, server vráti:

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

Použitie jazykových značiek umožňuje použitie viacjazyčných údajov v adresároch, ktoré môžu podporovať klientov pracujúcich v rôznych jazykoch. Pomocou jazykových značiek možno napísať aplikáciu tak, že nemecký klient vidí len údaje zadané pre atribút lang-de a francúzsky klient zase vidí len údaje zadané pre atribút lang-fr.

Ak chcete určiť, či je povolená funkcia jazykovej značky, zadajte vyhľadávanie koreňového DSE zadaním atribútu ″ibm-enabledCapabilities″.

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

Ak sa vráti OID ″1.3.6.1.4.1.4203.1.5.4″, funkcie je povolená.

Ak podpora jazykovej značky nie je povolená, akákoľvek operácia LDAP, ktorá priradí jazykovej značke atribút, bude odmietnutá s chybovým hlásením.

Niektoré atribúty môžu mať priradených niekoľko jazykových značiek, zatiaľ čo iné nemôžu. Ak chcete určiť, či nejaký atribút povoľuje jazykové značky, použite príkaz ldapexop:

- Pre atribúty, ktoré povoľujú jazykové značky: ldapexop -op getattributes -attrType language_tag -matches true
- Pre atribúty, ktoré nepovoľujú jazykové značky: ldapexop -op getattributes -attrType language_tag -matches false

Ďalšie informácie nájdete v časti “Pridanie položky, ktorá obsahuje atribúty s označeniami jazyka” na strane 163.

Odvolávky na adresár LDAP

Odvolávky umožňujú adresárovým serverom pracovať v tímoch. Ak sa DN, ktoré klient požaduje, nenachádza v jednom adresári, server môže automaticky odoslať (posunúť) požiadavku na iný server LDAP.

Adresárový server vám umožňuje použiť dva rôzne typy odvolávok. Môžete špecifikovať štandardné servery odvolávok, na ktorých bude server LDAP odkazovať klientov vždy, keď sa DN nebude nachádzať v adresári. Svojho klienta LDAP môžete použiť aj na pridanie položiek do adresárového servera, ktorý má odvolávku na objectClass. Umožní vám to uviesť odvolávky založené na tom, ktorý špecifický DN klient požaduje.

Poznámka: Pri adresárovom serveri musia obsahovať objekty odvolávok len tieto atribúty: rozlišovací názov (dn), triedu objektu (objectClass) a odvolávku (ref). Názorný príklad pre toto obmedzenie nájdete v časti “ldapsearch” na strane 200.

Servery odvolávok úzko súvisia s replikačnými servermi. Pretože údaje na replikačných serveroch nemôžu klienti meniť, replikačný server odkáže každú požiadavku na zmenu servera na hlavný server.

Transakcie

Svoj adresárový server môžete nakonfigurovať, aby umožňoval klientom používať transakcie. (Viac informácií o nastaveniach konfigurácie transakcií nájdete v časti "Uviesť nastavenie transakcie" na strane 113.) Transakcia je skupina adresárových operácií LDAP, s ktorými sa narába ako s jedným celkom. Žiadna z jednotlivých operácií LDAP, ktoré tvoria transakciu, nie je trvalá, pokiaľ neboli všetky operácie v transakcii dokončené úspešne a celá transakcia dokončená. Ak zlyhá hociktorá z operácií alebo je transakcia zrušená, ostatné operácie sa vrátia späť. Táto schopnosť môže pomôcť užívateľom udržať LDAP operácie organizované. Napríklad užívateľ môže vytvoriť transakciu na svojom klientovi, ktorá vymaže niekoľko položiek adresára. Ak klient stratí spojenie so serverom počas tejto transakcie, žiadny zo záznamov nie je vymazaný. Užívateľ môže preto jednoducho začať transakciu znovu namiesto toho, aby musel kontrolovať, ktoré záznamy boli úspešne zmazané.

Nasledujúce operácie LDAP môžu byť súčasťou transakcie:

- pridať
- upraviť
- upraviť RDN
- vymazať

Poznámka: Nevkladajte zmeny do schémy adresárov (prípona cn=schema) do transakcií. Aj keď je možné ich zahrnúť do transakcie, v prípade zlyhania transakcie ich nemožno vrátiť späť. Toto môže vášmu adresárovému serveru spôsobiť nepredpokladateľné problémy.

Bezpečnosť adresárového servera

Viac informácií o bezpečnosti adresárového servera nájdete v nasledujúcich témach:

- "Auditovanie"
- "Secure Sockets Layer (SSL) a Transport Layer Security (TLS) s adresárovým serverom" na strane 47
- "Autentifikácia Kerberos na adresárovom serveri" na strane 47
- "Skupiny a roly" na strane 48
- "Administratívny prístup" na strane 54
- "Autorizácia proxy" na strane 54
- "Zoznamy riadenia prístupu" na strane 55
- "Vlastníctvo objektov adresára LDAP" na strane 66
- "Politika hesiel" na strane 66
- "Autentifikácia" na strane 69
- "Odmietnutie služby" na strane 72

Súvisiace koncepty

"Riadenie vlastností zabezpečenia" na strane 145

Auditovanie

Adresárový server podporuje Auditovanie bezpečnosti i5/OS. Auditovateľné sú nasledujúce položky:

- Pripojenia k a odpojenia od adresárového servera.
- Zmeny a povolenia adresárových objektov LDAP.
- Zmeny vo vlastníctve adresárových objektov LDAP.
- Vytvorenie, zmazanie, prehľadávanie a zmeny adresárových objektov LDAP.
- Zmeny hesiel administrátora a aktualizovanie rozlišovacích názvov (DN).
- Zmeny hesiel užívateľov.
- Import a export súborov.

Predtým, ako bude fungovať auditovanie položiek adresára, môžete vykonať zmeny v nastaveniach auditovania. Ak je systémová hodnota QAUDTL nastavená na *OBJAUD, môžete umožniť auditovanie objektov pomocou iSeries Navigator. Viac informácií o auditovaní nájdete v téme *Bezpečnosť - Referencia*  alebo v téme "Auditovanie bezpečnosti".

Secure Sockets Layer (SSL) a Transport Layer Security (TLS) s adresárovým serverom

Pre bezpečnejšiu komunikáciu s vaším adresárovým serverom môže Adresárový server použiť zabezpečenie Secure Sockets Layer (SSL) a Transport Layer Security (TLS).

SSL je štandardom pre bezpečnosť internetu. SSL môžete použiť pri komunikácii s klientmi LDAP, ako aj s replikami serverov LDAP. Autentifikáciu klienta môžete použiť okrem autentifikácie servera na poskytovanie ďalšej bezpečnosti pre vaše pripojenia SSL. Autentifikácia klienta vyžaduje, aby klient LDAP poskytol digitálny certifikát, ktorý serveru potvrdí identitu klienta pred vytvorením pripojenia.

Ak chcete používať SSL, musíte mať v systéme nainštalovaného Správcu digitálnych certifikátov (DCM), voľba 34 systému i5/OS. DCM je rozhraním na vytváranie a riadenie digitálnych certifikátov a skladov certifikátov. Informácie o digitálnych certifikátoch a používaní DCM nájdete v téme "Správca digitálnych certifikátov (DCM)". Informácie o SSL v iSeries nájdete v téme "SSL (Secure Sockets Layer)".

| TLS bol vytvorený ako nasledovník SSL a používa rovnaké šifrovacie algoritmy, ale podporuje viac šifrovacích
| algoritmov. Informácie o TLS na serveri iSeries nájdete v protokoloch podporovaných SSL a TLS (Transport Layer
| Security).TLS umožňuje serveru prijímať zabezpečenú a nezabezpečenú komunikáciu od klienta cez predvolený port,
| 389. Pre zabezpečenú komunikáciu musí klient používať rozšírenú operáciu StartTLS.

Aby mohol klient používať TLS:

1. Adresárový server musí byť nakonfigurovaný na používanie TLS alebo SSLTLS. Pozrite si "Povolenie SSL a TLS (Transport Layer Security) v adresárovom serveri" na strane 149.
2. V pomocných programoch príkazového riadku klienta musí byť zadaná voľba -Y.

Poznámka: TLS nie sú SSL schopné spolupracovať. Zadaním požiadavky o TLS (voľba -Y) cez port SSL vznikne chyba operácií.

Klient sa môže pripojiť k zabezpečenému portu (636) buď pomocou TLS alebo SSL. StartTLS je funkcia LDAP, ktorá umožňuje spúšťanie zabezpečenej komunikácie cez existujúce zabezpečené pripojenie (t.j. port 389). StartTLS (alebo voľbu -Y pomocného programu príkazového riadku) môžete ako také používať len so štandardným nezabezpečeným portom (389). StartTLS nemôžete používať so zabezpečeným pripojením.

Ďalšie informácie nájdete v časti "Povolenie SSL a TLS (Transport Layer Security) v adresárovom serveri" na strane 149.

Autentifikácia Kerberos na adresárovom serveri

Adresárový server vám umožňuje používať autentifikáciu Kerberos. Kerberos je sieťový autentifikačný protokol, ktorý používa kryptografiu tajnými kľúčmi, čím sa zabezpečuje silná autentifikácia klient/server aplikácií.

Ak chcete povoliť autentifikáciu Kerberos, musíte mať nakonfigurovanú službu autentifikácie siete.

Podpora Kerberosu pre adresárový server zabezpečuje podporu pre mechanizmus GSSAPI SASL. Toto umožní klientom Adresárového servera aj Windows 2000 LDAP používať autentifikáciu Kerberos s Adresárovým serverom.

Názov principálu Kerberosu, ktorý server používa, má nasledujúci tvar:

```
názov-služby/názov-hostiteľa@realm
```

service-name je ldap (ldap musí byť malými písmenami), host-name je plne kvalifikovaný TCP/IP názov systému a realm je štandardný realm špecifikovaný v systémovej konfigurácii pre Kerberos.

Napríklad pri systéme s názvom my-as400 v doméne TCP/IP acme.com a pri štandardnom realme Kerberos s názvom ACME.COM by hlavný názov pre Kerberos servera LDAP bol ldap/my-as400.acme.com@ACME.COM . Štandardný realm Kerberos je uvedený v konfiguračnom súbore Kerberos (štandardne /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) s direktívou default_realm (default_realm = ACME.COM). Adresárový server nemožno nakonfigurovať, aby používal autentifikáciu Kerberosom, ak nebol nakonfigurovaný štandardný realm.

Keď sa používa autentifikácia Kerberos, adresárový server priradí rozlišovací názov (DN) k pripojeniu, ktoré určuje prístup k údajom adresára. Môžete si zvoliť, aby bol rozlišovací názov servera priraďovaný jedným z nasledujúcich postupov:

- Server môže vytvoriť DN založený na ID Kerberosu. Keď si vyberáte túto voľbu, identita Kerberos v tvare principal@realm generuje DN v tvare ibm-kn=principal@realm. ibm-kn= je ekvivalent k ibm-kerberosName=.
- Server môže hľadať v adresári rozlišovací názov (DN), ktorý obsahuje záznam pre princípál Kerberosu a realm. Keď vyberiete túto voľbu, server bude v adresári vyhľadávať položku, ktorá špecifikuje túto identitu Kerberos.

Musíte mať súbor tabuľky kľúčov (keytab), ktorý obsahuje kľúč pre princípál služby LDAP. Pozrite si Information Center, tému Služba sieťovej autentifikácie pod Bezpečnosťou, kde nájdete ďalšie informácie o Kerberos na tomto serveri iSeries. Časť Konfigurovanie služby autentifikácie siete obsahuje informácie o pridávaní informácií do súborov tabuľky kľúčov.

Skupiny a roly

Skupina je zoznam, kolekcia názvov. Skupinu možno použiť v atribútoch **aclentry**, **ibm-filterAclEntry** a **entryowner** na riadenie prístupu alebo pri využitiach špecifických pre aplikáciu, ako je poštový adresár, pozrite časť “Zoznamy riadenia prístupu” na strane 55. Skupiny sa dajú definovať buď ako statické, dynamické alebo vnorené. Informácie o spôsobe práce so skupinami si pozrite v časti “Manažovanie užívateľov a skupín” na strane 169.

Roly sa podobajú na skupiny v tom, že sú v adresári zastúpené pomocou objektu. Roly okrem toho obsahujú skupinu DN.

Viac informácií nájdete v týchto častiach:

Statické skupiny

Statická skupina definuje každého člena osobitne pomocou štrukturálnej triedy objektov **groupOfNames**, **groupOfUniqueNames**, **accessGroup** alebo **accessRole**; alebo pomocou pomocnej triedy objektov **ibm-staticgroup**. Statická skupina, ktorá používa štruktúrované triedy objektov **groupOfNames** alebo **groupOfUniqueNames** musí mať aspoň jedného člena. Skupina, ktorá používa triedy objektov **accessGroup** alebo **accessRole** môže byť prázdna. Statická skupina môže byť definovaná aj pomocou pomocnej triedy objektu: **ibm-staticGroup**, ktorá nevyžaduje atribút **member**, a preto môže byť prázdna.

Typickou položkou skupiny 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
```

Každý objekt skupiny obsahuje atribút s viacerými hodnotami, ktorý pozostáva z DN členov.

Pri vymazaní prístupovej skupiny bude prístupová skupina vymazaná aj zo všetkých ACL, v ktorých bola použitá.

Dynamické skupiny

Dynamická skupina definuje svojich členov inak statická skupina. Namiesto výpisu každého jedného člena definuje dynamická skupina svojich členov pomocou vyhľadávania LDAP. Dynamická skupina používa štrukturálnu triedu objektov **groupOfURLs** (alebo pomocnú triedu objektov **ibm-dynamicGroup**) a atribút **memberURL** na definovanie vyhľadávania pomocou zjednodušenej syntaxe LDAP URL.

```
ldap:///<základ vyhľadávania DN> ? ? <rozsah vyhľadávania> ? <vyhľadávací filter>
```

Poznámka: Ako vidíte na príklade, názov hostiteľa sa nesmie v syntaxi vyskytnúť. Ostatné parametre sú rovnaké ako pri normálnej syntaxi ldap URL. Každé pole parametra musí byť oddelené ? (otáznikom), a to aj vtedy, keď nie je zadaný žiadny parameter. Bežne by bol zoznam atribútov, ktoré sa majú vrátiť, začlenený medzi základným DN a rozsahom vyhľadávania. Tento parameter tiež nevyužíva server pri určovaní dynamického členstva a je možné ho vynechať, ale oddeľovač **?** musí byť aj naďalej prítomný.

kde:

základné DN vyhľadávania
Je bod, od ktorého vyhľadávanie v adresári začína. Môže to byť prípona alebo koreň adresára, napríklad **ou=Austin**. Je to povinný parameter.

rozsah vyhľadávania
Špecifikuje rozsah vyhľadávania. Štandardný rozsah je základný.

základný
Vráti informácie iba o základnom DN, ktoré bolo špecifikované v URL

jedna Vráti informácie o položkách ktoré sú jednu úroveň pod základným DN, ktoré bolo špecifikované v URL. Nepatrí sem základná položka.

pod Vráti informácie o položkách na všetkých úrovniach pod a obsahuje základné DN.

filter vyhľadávania
Je filter, ktorý chcete použiť pre položky v rámci rozsahu vyhľadávania. Informácie o syntaxi filtra vyhľadávania nájdete v časti “voľba filtra ldapsearch” na strane 204. Štandard je objectclass=*

Vyhľadávanie dynamických členov na serveri je vždy interné, preto nikdy nie je špecifikované úplné ldap URL, názov hostiteľa a číslo portu a protokol je vždy **ldap** (nikdy nie **ldaps**). Atribút **memberURL** môže obsahovať ľubovoľný druh URL, ale server na určenie dynamického členstva použije len **URL členov** začínajúce na **ldap:///**.

Príklady

Jedna položka, v ktorej sa rozsah štandardne nastaví na základný a filter sa štandardne nastaví na objectclass=*:

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

Všetky položky, ktoré sú 1 úroveň pod cn=Employees a filter sa štandardne nastaví na objectclass=*:

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

Všetky položky, ktoré sú pod o-Acme a majú objectclass=person:

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

V závislosti od tried objektov, ktoré používate na definovanie užívateľských položiek, tieto položky nemusia obsahovať atribúty, ktoré sú vhodné pre určovanie členstva v skupine. Ak chcete svoje užívateľské položky rozšíriť, aby zahŕňali atribút **ibm-group** môžete použiť pomocnú triedu objektov **ibm-dynamicMember**. Tento atribút vám umožňuje pridať ľubovoľné hodnoty do vašich užívateľských položiek, aby slúžili ako ciele pre filtre vašich dynamických skupín. Napríklad:

Členmi tejto dynamickej skupiny sú položky priamo pod položkou cn=users,ou=Austin, ktorá má atribút ibm-group s hodnotou GROUP1:

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

Tu je príklad člena cn=GROUP1,ou=Austin:

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

Vnorené skupiny

Vnáranie skupín povoľuje vytvárať hierarchické vzťahy, ktoré sa dajú použiť na definovanie zdedeného príslušenstva k skupine. Vnorená skupina je definovaná ako položka skupiny potomka, na DN ktorého odkazuje atribút, nachádzajúci sa vo vnútri položky skupiny rodiča. Rodičovská skupina sa vytvorí rozšírením niektorej štrukturálnej skupinovej triedy objektov (**groupOfNames**, **groupOfUniqueNames**, **accessGroup**, **accessRole** alebo **groupOfURLs**) spolu s pridaním pomocnej triedy objektov **ibm-nestedGroup**. Po prípone vnorenej skupiny je možné pridať nulový počet alebo viac atribútov **ibm-memberGroup** s hodnotami nastavenými na DN vnorených skupín potomkov. Napríklad:

```
dn: cn=Group 2, cn=Groups, o=IBM, c=US
 objectclass: groupOfNames
 objectclass: ibm-nestedGroup
 objectclass: top
 cn: Group 2
 description: Group composed of static, and nested members.
 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
```

Zavedenie cyklov do hierarchie vnorenej skupiny nie je povolené. Ak je stanovené, že výsledkom operácie vnorenej skupiny bude cyklický odkaz buď priamo alebo prostredníctvom dedenia, bude sa to považovať za porušenie obmedzenia a z tohto dôvodu zlyhá aktualizácia položky.

Hybridné skupiny

Všetky štrukturálne skupinové triedy objektov sa dajú rozšíriť tak, že členstvo v skupine sa popíše pomocou kombinácie statických, dynamických a vnorených typov členov. Napríklad:

```
dn: cn=Group 10, cn=Groups, o=IBM, c=US
 objectclass: groupOfURLs
 objectclass: ibm-nestedGroup
 objectclass: ibm-staticGroup
 objectclass: top
 cn: Group 10
 description: Group composed of static, dynamic, and nested members.
 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
```

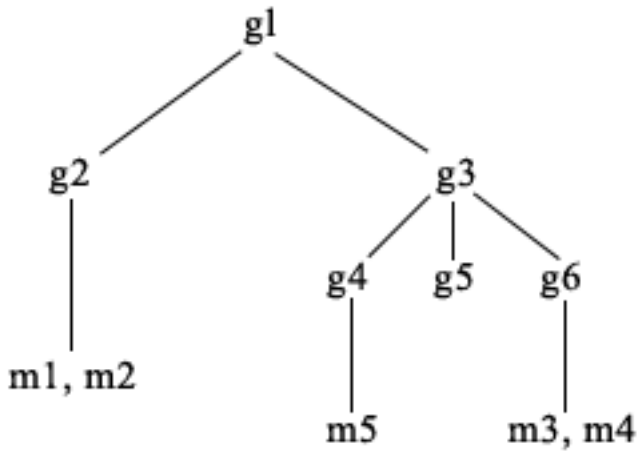
Určovanie členstva v skupine

Na dotazovanie súhrnného členstva v skupine sa dajú použiť dva prevádzkové atribúty. Pri danej položke skupiny vymenuje prevádzkový atribút **ibm-allMembers** súhrnnú množinu členstva v skupine vrátane statických, dynamických

a vnorených členov, ktoré sú opísané pomocou hierarchie vnorenej skupiny. Pri danej užívateľskej položke vymenuje prevádzkový atribút **ibm-allGroups** súhrnnú množinu skupín vrátane rodičovských skupín, pre ktoré má tento užívateľ členstvo.

Žiadateľ dostane len podmnožinu celkových požadovaných údajov, v závislosti od toho, ako boli nastavené zoznamy ACL na údajoch. Každý môže žiadať prevádzkové atribúty **ibm-allMembers** a **ibm-allGroups**, ale vrátená množina údajov bude obsahovať iba údaje pre položky LDAP a atribúty, ku ktorým žiadateľ prístupové práva. Užívateľ, ktorý požaduje atribút **ibm-allMembers** alebo **ibm-allGroups** musí mať prístup na hodnoty atribútov **member** alebo **uniquemember** pre skupinu a vnorené skupiny, aby mohlo vidieť statických členov a musí byť schopný vykonávať vyhľadávania, ktoré špecifikujú hodnoty atribútu **memberURL**, aby mohol vidieť dynamických členov. Napríklad:

Príklady hierarchie



V tomto príklade **m1** a **m2** sú v atribúte member s hodnotou **g2**. ACL pre **g2** umožňuje, aby **user1** čítal atribút member, ale **user 2** nemá prístup na atribút member. Položky LDIF pre položku **g2** je takáto:

```
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
```

Položka **g4** používa štandardný aclentry, ktorý umožňuje aj **user1** aj **user2**, aby čítal svoj atribút member. LDIF pre položku **g4** je takýto:

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

Položka **g5** je dynamická skupina, ktorá získava svojich dvoch členov z atribútu memberURL. LDIF pre položku **g5** je takýto:

```
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))
```

Položky **m3** a **m4** sú členmi skupiny **g5**, pretože sa zhodujú s **memberURL**. ACL pre položku **m3** umožňuje aj **user1** aj **user2**, aby ju vyhľadávali. ACL pre položky **m4** neumožňuje **user2**, aby ju vyhľadával. LDIF pre **m4** je takýto:

```
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
```

Príklad 1:

User 1 vykoná vyhľadávanie, aby získal všetkých členov skupiny **g1**. User 1 má prístup k všetkým členom, preto budú všetci vrátení.

```
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
```

Príklad 2:

User 2 vykoná vyhľadávanie, aby získal všetkých členov skupiny **g1**. User 2 nemá prístup k členom **m1** alebo **m2**, pretože nemajú prístup na atribút member pre skupinu **g2**. User 2 má prístup na atribút member pre **g4**, a preto má prístup na člena **m5**. User 2 môže v skupine **g5** memberURL vykonávať vyhľadávanie položky **m3** tak, že sa vypíše zoznam členov, ale nemôže vyhľadávať **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
```

Príklad 3:

User 2 vykoná vyhľadávanie, aby zistil či je **m3** členom skupiny **g1**. User 2 má prístup, aby vykonal toto vyhľadávanie, preto vyhľadávanie ukáže, že **m3** je členom skupiny **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
```

Príklad 4:

User 2 vykoná vyhľadávanie, aby zistil či **m1** je členom skupiny **g1**. User 2 nemá prístup na atribút member, preto vyhľadávanie neukáže, či je **m1** členom skupiny **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
```

Skupinové triedy objektov pre vnorené a dynamické skupiny

ibm-dynamicGroup

Táto pomocná skupina povoľuje voliteľný atribút **memberURL**. Používajte ju so štruktúrovanou triedou, napríklad **groupOfNames**, na vytvorenie hybridnej skupiny so statickými a dynamickými členmi.

ibm-dynamicMember

Táto pomocná trieda povoľuje voliteľný atribút **ibm-group**. Použite ju ako atribút filtra pre dynamické skupiny.

ibm-nestedGroup
Táto pomocná trieda povoľuje voliteľný atribút **ibm-memberGroup**. Použite ju so štruktúrovanou triedou, napríklad **groupOfNames**, aby sa povolilo vnorenie podskupín do rodičovskej skupiny.

ibm-staticGroup
Táto pomocná trieda povoľuje voliteľný atribút **member**. Použite ju so štruktúrovanou triedou, napríklad **groupOfURLs**, na vytvorenie hybridnej skupiny so statickými aj dynamickými členmi.

Poznámka: **ibm-staticGroup** je jedinou triedou, pre ktorú atribút **member** je *optional*, všetky ostatné triedy preberajúce atribút **member** vyžadujú minimálne 1 člena.

Typy skupinových atribútov

ibm-allGroups
Zobrazuje všetky skupiny, ku ktorým položka patrí. Položka môže byť členom priamo, podľa atribútov **member**, **uniqueMember** alebo **memberURL**, alebo nepriamo, podľa atribútu **ibm-memberGroup**. Tento prevádzkový atribút **iba na čítanie** nie je povolený vo vyhľadávacom filtri. Atribút **ibm-allGroups** sa môže použiť v požiadavke na porovnanie na stanovenie, či je položka členom danej skupiny. Napríklad ak chcete určiť, či ″cn=john smith,cn=users,o=my company″ je členom skupiny ″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
Zobrazuje všetkých členov skupiny. Položka môže byť členom priamo, podľa atribútov **member**, **uniqueMember** alebo **memberURL**, alebo nepriamo, podľa atribútu **ibm-memberGroup**. Tento prevádzkový atribút **iba na čítanie** nie je povolený vo vyhľadávacom filtri. Atribút **ibm-allMembers** sa dá použiť v požiadavke na porovnanie na stanovenie, či DN je členom danej skupiny. Napríklad ak chcete určiť, či ″cn=john smith,cn=users,o=my company″ je členom skupiny ″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 atribút prevzatý pomocnou triedou **ibm-dynamicMember**. Použite ho na definovanie ľubovoľných hodnôt pre riadenie členstva položky v dynamických skupinách. Napríklad pridajte hodnotu ″Bowling Team″, aby zahŕňala položku v každej **memberURL**, ktorá má filter ″ibm-group=Bowling Team″.

ibm-memberGroup
Je atribút prevzatý pomocnou triedou **ibm-nestedGroup**. Identifikuje podskupiny položky rodičovskej skupiny. Členovia všetkých takýchto podskupín sa považujú za členov rodičovskej skupiny pri spracovaní ACL alebo prevádzkových atribútov **ibm-allMembers** a **ibm-allGroups**. Položky podskupín *nie* sú samy o sebe členmi. Vnorené členstvo je rekurzívne.

member
Identifikuje rozlišovacie názvy pre každého člena skupiny. Napríklad: member: cn=John Smith, dc=ibm, dc=com.

memberURL
Identifikuje URL, ktoré je priradené ku každému členovi skupiny. Môže sa použiť každý typ návestím označeného URL. Napríklad: memberURL: ldap:///cn=jsmith,dc=ibm,dc=com.

uniquemember
Identifikuje skupinu názvov, ktoré sú priradené k položke, v ktorej každý názov dostal uniqueIdentifier, aby sa zabezpečila jeho jedinečnosť. Hodnota pre atribút uniqueMember je DN, za ktorým nasleduje uniqueIdentifier. Napríklad: uniqueMember: cn=John Smith, dc=ibm, dc=com 17.

Roly

Autorizácia na základe role je koncepčným doplnkom pre autorizáciu na základe skupiny a v niektorých prípadoch je užitočná. Ako člen role máte oprávnenie vykonať to, čo je potrebné pre rolu, aby sa mohla dokončiť úloha. Na rozdiel

od skupiny, rola prichádza s implicitnou množinou oprávnení. Neexistuje zabudovaná pravdepodobnosť toho, ktoré oprávnenia budú získané (alebo stratené) pri jestvovaní ako člen skupiny.

Roly sa podobajú na skupiny v tom, že sú v adresári zastúpené pomocou objektu. Roly okrem toho obsahujú skupinu DN. Roly, ktoré sa majú použiť riadení prístupu musia mať triedu objektov 'AccessRole'. Trieda objektov 'Accessrole' je podtriedou triedy objektov 'GroupOfNames'.

Napríklad, ak existuje kolekcia názvov DN, napríklad 'sys admin', vašou prvou reakciou by mohlo byť považovať ich za 'sys admin group' (keďže skupiny a užívatelia sú najznámejšie typy atribútov privilégií). Ale keďže existuje množina povolení, ktorých príjem by ste mohli očakávať ako člen 'sys admin', kolekciu názvov DN možno presnejšie definovať ako 'sys admin role'.

Administratívny prístup

Adresárový server IBM umožňuje nasledovné typy administratívneho prístupu:

- **Projektovaný administrátor i5/OS:** Klient autentifikovaný ako projektovaný užívateľ (položka LDAP reprezentujúca užívateľský profil operačného systému) s mimoriadnymi oprávneniami *ALLOBJ a *IOSYSCFG má oprávnenie na zmenu konfigurácie adresára pomocou rozhraní LDAP (podstrom cn=configuration alebo úlohy webového administratívneho nástroja ″Správa servera″), a tiež funguje ako administrátor LDAP pre ostatné položky adresára (položky uložené v jednej z prípon alebo schém DB2). Len projektovaní administrátori i5/OS môžu meniť konfiguráciu servera.
- **Administrátor LDAP:** Adresárový server IBM umožňuje, že ID jedného užívateľa (DN) môže byť administrátorom primárneho servera LDAP. iSeries umožňuje tiež, že projektované užívateľské profily operačného systému môžu byť administrátormi LDAP. Administrátori servera LDAP môžu vykonávať celý rad administratívnych úloh, napríklad správu položiek replikácie, schémy a adresára. Ďalšie informácie nájdete v časti "Pridelenie administrátorského prístupu projektovaným užívateľom" na strane 115.
- **Skupina užívateľov - administrátorov:** Projektovaný administrátor i5/OS môže vymenovať niekoľko užívateľov za administratívnu skupinu. Členovia tejto skupiny môžu vykonávať množstvo úloh, lebo majú rovnaký administratívny prístup ako administrátor servera LDAP.

  Poznámka: Pri použití webovej administrácie sú úlohy, ktoré neboli povolené členom administratívnej skupiny, zakázané.

Administrátor LDAP alebo člen administratívnej skupiny môže vykonávať nasledovné úlohy administrácie servera:

- Zmeniť ich vlastné heslo
- Ukončiť pripojenia
- Povoliť a zmeniť politiku hesiel, okrem šifrovania hesiel, ktoré môže zmeniť len projektovaný administrátor i5/OS.
- Spravovať jedinečné atribúty
- Spravovať schému servera
- Spravovať replikáciu, okrem úlohy vlastností replikácie (zahrňuje DN a heslo väzby hlavného servera a predvolenú odvolávku), ktoré môže vykonávať len projektovaný administrátor i5/OS.

Informácie o tom, ako vytvoriť administratívnu skupinu, nájdete v časti "Práca s administračnou skupinou" na strane 116.

Autorizácia proxy

Autorizácia proxy je špeciálna forma autentifikácie. Pomocou tohto mechanizmu autorizácie proxy môže klientska aplikácia vytvoriť väzby k adresáru so svojou vlastnou identitou, ale má povolené vykonávať operácie v mene iného užívateľa za účelom prístupu do cieľového adresára. Množina dôveryhodných aplikácií alebo užívateľov má prístup na adresárový server v mene viacerých užívateľov.

Členovia v skupine autorizácie proxy môžu predpokladať akékoľvek autentifikované identity okrem administrátora alebo členov administratívnej skupiny.

| Skupina autorizácie proxy môže byť uložená pod lokálnym hostiteľom alebo IBMpolicies. Skupina autorizácie proxy pod IBMpolicies je replikovaná, skupina autorizácie proxy pod lokálnym hostiteľom nie je. Skupinu autorizácie proxy môžete uložiť pod lokálneho hostiteľa aj IBMpolicies. Ak skupina autorizácie proxy nie je uložená pod jedným z týchto názvov DN, server bude ignorovať časť skupiny autorizácie proxy a bude ju považovať za normálnu skupinu.

| Napríklad klientska aplikácia, klient1, môže vytvoriť väzby na adresárový server s vyššou úrovňou povolení na prístup. Užívateľ A s obmedzenými povoleniami odošle požiadavku do klientske j aplikácie. Ak je klient členom skupiny autorizácie proxy, namiesto odovzdania požiadavky na adresárový server ako klient1 môže odovzdať požiadavku ako Užívateľ A pomocou obmedzenejšej úrovne povolení. Znamená to, že namiesto vykonania požiadavky ako klient1, má aplikačný server prístup len k tým informáciám, alebo vykonávať len tie úkony, ku ktorým má prístup alebo ktoré je schopný vykonávať len Užívateľ A. Vykoná požiadavku v mene proxy alebo v jeho mene pre Užívateľa A.

| **Poznámka:** Člen atribútu musí mať svoju hodnotu vo formáte DN. V opačnom prípade sa vráti správa neplatná syntax DN. DN skupiny nemá povolené byť členom skupiny autorizácie proxy.

| Administrátori a členovia administratívnej skupiny nemajú povolené byť členmi skupiny autorizácie proxy. Auditový protokol zaznamená DN väzby aj DN proxy pre každú činnosť vykonanú pomocou autorizácie proxy.

| Ďalšie informácie nájdete v časti “Riadenie skupiny proxy autorizácie” na strane 119.

Zoznamy riadenia prístupu

Zoznamy riadenia prístupu (ACL) poskytujú prostriedky na ochranu informácií, ktoré sú uložené v adresári LDAP. Administrátori používajú ACL na obmedzenie prístupu k rôznym častiam adresára alebo k špecifickým položkám adresára. Zmeny pre každú položku a atribút v adresári sa dajú riadiť s použitím ACL. ACL pre danú položku alebo atribút môže byť zdedený po svojej rodičovskej položke alebo sa môže definovať explicitne.

Svoju stratégiu riadenia prístupu si najlepšie navrhnete vytvorením skupín užívateľov, ktoré použijete pri nastavovaní prístupu pre objekty a atribúty. Nastavte vlastníctvo a prístup na najvyššej povolenej úrovni stromu a nechajte, aby sa ovládacie prvky dedili v strome smerom nadol.

Prevádzkové atribúty, priradené k riadeniu prístupu, napríklad entryOwner, ownerSource, ownerPropagate, aclEntry, aclSource a aclPropagate sú nezvyčajné v tom, že sú logicky priradené ku každému objektu, ale môžu mať hodnoty, ktoré závisia od iných objektov, ktoré sú v strome umiestnené vyššie. Podľa toho ako boli vytvorené, môžu byť tieto hodnoty atribútov pri objekte explicitné alebo zdedené po rodičoch.

Model riadenia prístupu definuje dve množiny atribútov: Informácie riadenia prístupu (ACI) a informácie entryOwner. ACI definuje prístupové práva poskytnuté špecifikovanému subjektu s ohľadom na operácie, ktoré môžu vykonávať na objektoch, pre ktoré sa použijú. Atribúty aclEntry a aclPropagate sa použijú pre definíciu ACI. Informácie entryOwner definujú subjekty, ktoré môžu definovať ACI pre priradený objekt položky. Atribúty entryOwner a ownerPropagate sa použijú pre definíciu entryOwner.

Môžete si vybrať z dvoch druhov zoznamov riadenia prístupu: ACL založené na filtroch a nefiltrované ACL. Nefiltrované zoznamy ACL sa explicitne aplikujú na položku adresára, ktorá ich obsahuje, ale možno ich rozšíriť na žiadnu alebo všetky jeho následné položky. ACL založené na filtroch sa líšia tým, že využívajú porovnávanie na základe filtrov, s použitím špecifikovaného filtra objektov, pre spárovanie cieľových objektov s efektívnym prístupom, ktorý sa pre ne používa.

Keď sa používajú ACL, administrátori môžu obmedziť prístup do rôznych častí adresára, špecifických položiek adresára a na základe názvu atribútu alebo triedy prístupu atribútu, na atribúty, ktoré tieto položky obsahujú. Každá položka v rámci adresára LDAP má množinu priradených ACI. Podľa modelu LDAP sa informácie ACI a entryOwner budú zobrazovať ako páry atribút-hodnota. Okrem toho sa na správu týchto hodnôt používa syntax LDIF. Týmito atribútmi sú:

- aclEntry
- aclPropagate
- ibm-filterAclEntry

- ibm-filterAclInherit
- entryOwner
- ownerPropagate

Informácie o spôsobe práce s ACL si pozrite v časti “Manažovanie zoznamov riadenia prístupu (ACL)” na strane 179. Ďalšie informácie nájdete v nasledujúcich témach:

- “Filtrované ACL”
- “Syntax atribútov riadenia prístupu”
- “AclEntry a ibm-filterAclEntry” na strane 57
- “EntryOwner” na strane 60
- “Rozširovanie” na strane 60
- “Vyhodnotenie prístupu” na strane 60
- “Definovanie ACI a vlastníkov položiek” na strane 62
- “Zmena hodnôt ACI a vlastníka položky” na strane 63
- “Vymazanie hodnôt ACI/vlastníka položky” na strane 65
- “Získanie hodnôt ACI/vlastníka položky” na strane 65
- “Hľadiská replikácie podstromov” na strane 66

Filtrované ACL

ACL založené na filtroch využívajú porovnávanie na základe filtrov, s použitím špecifikovaného filtra objektov, pre spárovanie cieľových objektov s efektívnym prístupom, ktorý sa pre ne používa.

ACL založené na filtroch sa dedične rozširujú do všetkých spárovaných objektov porovnávania v priradenom podstrome. Z tohto dôvodu sa atribút aclPropagate, ktorý sa používa na zastavenie šírenia nefiltrovaných ACL, nepoužije pre nové ACL založené na filtroch.

Štandardným správaním ACL na báze filtrov je zhromažďovanie od najnižšej zahrnutej položky smerom nahor, pozdĺž reťaze rodičovských položiek, k najvyššej položke zahrnutej v DIT. Efektívny prístup sa vypočíta ako zjednotenie prístupových práv, ktoré povolili alebo zakázali ustanovujúce rodičovské položky. Existuje výnimka z tohto správania. Pre kompatibilitu s funkciou replikácie podstromu a na umožnenie širšej administratívnej kontroly, sa atribút hornej hranice použije ako prostriedok na zastavenie zhromažďovania na položke, v ktorej sa nachádza.

Špecificky pre podporu ACL na báze filtrov sa dáva prednosť používaniu novej množiny atribútov riadenia prístupu, pred zlučovaním charakteristík, ktoré sú založené na filtroch, do existujúcich nefiltrovaných ACL. Týmito atribútmi sú:

- ibm-filterAclEntry
- ibm-filterAclInherit

Atribút ibm-filterAclEntry má rovnaký formát ako aclEntry a má pridaný komponent filtra objektov. Pridružený atribút hodnej hranice je ibm-filterAclInherit. štandardne je nastavený na hodnotu TRUE. Keď je nastavený na hodnotu FALSE, ukončuje zhromažďovanie.

Syntax atribútov riadenia prístupu

Každý z týchto atribútov sa dá riadiť použitím notácie LDIF. Syntax pre nové atribúty ACL na báze filtrov sú modifikované verzie aktuálnych atribútov ACL, ktoré nie sú na báze filtrov. Nasleduje definovanie syntaxe pre atribúty ACI a entryOwner pomocou BNF (baccus naur form).

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

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

<ibm-filterAclInherit> ::=  "true" | "false"
```

```
<entryOwner> ::=  <subject>

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

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

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

<subjectDn> ::= <DN>

<DN> ::= distinguished name as described in RFC 2251, section 4.1.3.

<pseudoDn> ::= "group:cn=anybody" | "group:cn=authenticated" |
                         "access-id:cn=this"
<object filter> ::= string search filter as defined in RFC 2254, section 4
                                (extensible matching is not supported).
<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.
                        (OID or alpha-numeric string with leading
                         alphabet, "-" and ";" allowed)

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

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

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

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

AclEntry a ibm-filterAclEntry

Subjekt: Subjekt (entita požadujúca prístup na prácu s objektom) sa skladá z kombinácie typu DN (rozlišovacieho názvu) a DN. Platné typy DN sú: access-id, skupina a rola.

DN identifikuje konkrétne prístupové ID, rolu alebo skupinu. Napríklad subjekt môže byť access-id: cn=personA, o=IBM alebo group: cn=deptXYZ, o=IBM.

Pretože oddeľovačom polí je dvojbodka (:), DN, ktorý obsahuje dvojbodky, musí byť uzavretý v dvojitých úvodzovkách (“”). Ak už DN obsahuje znaky s dvojitými úvodzovkami, význam týchto znakov sa musí zmeniť pomocou opačnej lomky (\).

Pri riadení prístupu sa môžu použiť všetky adresárové skupiny.

Poznámka: Každá skupina štrukturálnych tried objektov **AccessGroup**, **GroupOfNames**, **GroupofUniqueNames** alebo **groupOfURLs** alebo pomocných tried objektov **ibm-dynamicGroup**, **ibm-staticGroup** sa môže použiť pri riadení prístupu.

Iný typ DN, ktorý sa používa v rámci modelu riadenia prístupu, je rola. Aj keď majú roly a skupiny podobnú implementáciu, koncepčne sa odlišujú. Keď je užívateľ priradený k role, existuje implicitná pravdepodobnosť, že nevyhnutné oprávnenia pre vykonanie úlohy, ktorá je k tejto role priradená, už boli nastavené. Pri členstve v skupine neexistuje zabudovaná pravdepodobnosť toho, ktoré oprávnenia budú získané (alebo stratené) pri jestvovaní ako člen skupiny.

Roly sa podobajú na skupiny v tom, že sú v adresári zastúpené pomocou objektu. Roly okrem toho obsahujú skupinu DN. Roly, ktoré sa používajú v riadení prístupu musia mať triedu objektov **AccessRole**.

Pseudo DN: Adresár LDAP obsahuje niekoľko pseudo DN. Tieto sa používajú, aby odkazovali na veľké množstvá DN, ktoré v čase vytvárania väzieb, zdieľajú spoločné charakteristiky buď vo vzťahu k operácii, ktorá sa vykonáva, alebo vo vzťahu k cieľovému objektu, na ktorom sa operácia vykonáva.

Aktuálne sú definované tri pseudo DN:

group:cn=anybody
Odkazuje na všetky subjekty, vrátane tých, ktoré nie sú autentifikované. Do tejto skupiny patria automaticky všetci užívatelia.

group:cn=authenticated
Odkazuje na každé DN, ktoré bolo autentifikované do adresára. Metóda autentifikácia sa nezohľadňuje.

access-id:cn=this
Odkazuje na DN vytvorenia väzby, ktorý sa zhoduje s DN cieľového objektu, na ktorom sa operácia vykonáva.

Filter objektov: Tento parameter sa použije iba pre filtrované ACL. Vyhľadávací filter reťazca, ako je definovaný v RFC 2254, sa používa ako formát filtra objektov. Pretože cieľový objekt je už známy, reťazec sa nepoužije na vykonanie skutočného vyhľadávania. Namiesto toho sa na spomínanom cieľovom objekte vykoná porovnanie založené na filtroch, aby sa stanovilo, či sa daná množina hodnôt ibm-filterAclEntry preň použije.

Práva: Prístupové práva môžu platiť pre celý objekt alebo pre atribúty objektu. Prístupové práva LDAP sú oddelené. Jedno právo nezahŕňa do seba iné právo. Práva možno vzájomne kombinovať na dosiahnutie požadovaného zoznamu práv, ktoré spĺňajú množinu pravidiel prejednávaných ďalej. Práva nemusia mať špecifikovanú hodnotu, čo indikuje, že subjekt nemá na cieľovom objekte pridelené žiadne prístupové práva. Práva sa skladajú z troch častí:

Akcia:
Definované hodnoty sú **povoliť** alebo **zakázať**. Ak toto pole nie je prítomné, hodnota sa štandardne nastaví na **povoliť**.

Oprávnenie:
Existuje šesť základných operácií, ktoré možno vykonávať na objekt adresára. Z týchto operácií sa vezme základná množina oprávnení ACI. Sem patria: pridať položku, vymazať položku, čítať hodnotu atribútu, zapísať hodnotu atribútu, vyhľadávať atribút a porovnať hodnotu atribútu.

Povolené oprávnenia na atribúty sú: čítať (r), zapisovať (w), vyhľadávať (s) a porovnať (c). Okrem toho, oprávnenia na objekty platia pre položku ako celok. Tieto oprávnenia sú pridať položky potomka (a) a vymazať túto položku (d).

Nasledujúca tabuľka sumarizuje oprávnenia, potrebné na vykonanie každej operácie LDAP.

Operácia	Potrebné oprávnenie
ldapadd	pridať (na rodičovi)
ldapdelete	vymazať (na objekte)
ldapmodify	zapísať (na modifikujúcich sa atribútoch)

Operácia	Potrebné oprávnenie
ldapsearch	• vyhľadávať, čítať (na atribútoch v RDN) • vyhľadávať (na atribútoch, špecifikovaných vo vyhľadávacom filtri) • vyhľadávať (na atribútoch, vrátených iba s názvami) • vyhľadávať, čítať (na atribútoch, vrátených s hodnotami)
ldapmodrdn	zapísať (na atribútoch RDN)
ldapcompare	porovnať (na porovnanom atribúte)

Poznámka: Pri operáciách vyhľadávania musí mať predmet prístup na vyhľadávanie pre všetky atribúty vo vyhľadávacom filtri, inak sa nevrátia žiadne položky. Pre položky vrátené z vyhľadávania sa vyžaduje, aby predmet mal prístup na vyhľadávanie a čítanie ku všetkým atribútom v RDN vrátených položiek, inak tieto položky nebudú vrátené.

Cieľ prístupu:

Tieto oprávnenia sa dajú použiť pre celý objekt (pridať položku potomka, vymazať položku), pre konkrétny atribút v rámci položky alebo sa môže použiť pre skupiny atribútov (Triedy prístupu k atribútom), ako je opísané ďalej.

Atribúty, ktoré vyžadujú podobné oprávnenia pre prístup, sú spoločne zoskupené do tried. Atribúty sa mapujú do ich tried atribútov v súbore schémy adresára. Tieto triedy sú oddelené; prístup do jednej triedy nezahŕňa v sebe prístup do inej triedy. Oprávnenia sú nastavené s ohľadom na triedu prístupu k atribútom, ako celok. Oprávnenia nastavené na konkrétnu triedu atribútov sa použijú pre všetky atribúty v rámci takejto triedy prístupu, pokiaľ nebudú špecifikované konkrétne oprávnenia na prístup k atribútom.

Spoločnosť IBM definuje tri triedy atribútov, ktoré sa používajú pri vyhodnocovaní prístupu k užívateľským atribútom: **normal**, **sensitive** a **critical**. Napríklad atribút **commonName** spadá do triedy normálne a atribút userpassword patrí do triedy kritické. Užívateľom definované atribúty patri do prístupovej triedy normálne, pokiaľ nebolo špecifikované inak.

Ostatné dve prístupové triedy sú tiež definované: systémové a obmedzené. Atribúty triedy systémové sú:

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

Tieto atribúty udržiava server LDAP a pre užívateľov adresára sa poskytujú iba-na-čítanie. **OwnerSource** a **aclSource** sú opísané v časti Rozširovanie (pozrite si “Rozširovanie” na strane 60).

Medzi atribúty obmedzenej triedy, ktoré definujú riadenie prístupu patria:

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

Všetci užívatelia majú prístup na čítanie k obmedzeným atribútom, ale len **entryOwners** môžu vytvárať, meniť a vymazávať tieto atribúty.

Poznámka: Atribút **ibm-effectiveAcl** je iba-na-čítanie.

EntryOwner

Vlastníci položiek majú úplné oprávnenia na vykonávanie každej operácie na objekte bez ohľadu na aclEntry. Okrem toho sú vlastníci položiek jediní, ktorí majú povolené spravovať aclEntries pre tento objekt. EntryOwner je subjekt riadenia prístupu, ktorý môže byť definovaný ako jednotlivci, skupiny alebo roly.

Poznámka: Administrátor adresára je štandardne jedným z entryOwners pre všetky objekty v adresári, a entryOwnership administrátora adresára nemôže byť odstránený zo žiadneho objektu.

Rozširovanie

Položky, do ktorých bola umiestnená aclEntry, sa považujú za položky, ktoré majú explicitnú **aclEntry**. Podobne, ak bol určitej položke nastavený **entryOwner**, táto položka má explicitného vlastníka. Tieto dve nie sú navzájom previazané. Položka s explicitným vlastníkom môže ale nemusí mať explicitnú **aclEntry** a položka s explicitnou **aclEntry** môže mať explicitného vlastníka. Ak niektorá z týchto hodnôt nie je na položke explicitne prítomná, chýbajúca hodnota sa zdedí z uzla potomka do adresárového stromu.

Každá explicitná **aclEntry** alebo **entryOwner** sa použije pre položku, na ktorej je nastavená. Okrem toho sa môže hodnota použiť pre všetkých potomkov, ktorí nemajú explicitne nastavenú hodnotu. Tieto hodnoty sa považujú za rozšírené; ich hodnoty sa rozširujú cez adresárový strom. Rozširovanie určitej hodnoty pokračuje, kým nebude dosiahnutá iná rozširujúca sa hodnota.

Poznámka: ACL založené na filtroch sa nerozširujú rovnakým spôsobom ako ACL, ktoré nie sú založené na filtroch. Rozširujú sa do všetkých pri porovnaní spárovaných objektoch v priradenom podstrome. Viac informácií o odlišnostiach nájdete v časti “Filtrované ACL” na strane 56.

AclEntry a **entryOwner** sa dajú nastaviť, aby sa použili iba pre určitú položku, ktorej hodnota rozširovania bude nastavená na ″false″, alebo pre položku, ktorá spoločne so svojím podstromom bude mať hodnotu rozšírenia nastavenú na ″true″. Hoci aj **aclEntry** aj **entryOwner** sa môžu šíriť, ich šírenie nie je nijako prepojené.

Atribúty **aclEntry** a **entryOwner** umožňujú viaceré hodnoty, avšak atribúty šírenia (**aclPropagate** a **ownerPropagate**) môžu mať v rámci jednej položky iba jednu hodnotu pre všetky hodnoty atribútov **aclEntry** alebo **entryOwner**.

Systémové atribúty **aclSource** a **ownerSource** obsahujú DN efektívneho uzla, z ktorého sú **aclEntry** alebo **entryOwner** hodnotené v uvedenom poradí. Ak neexistuje žiadny takýto uzol, priradí sa hodnota **default**.

Definície riadenia efektívneho prístupu objektu sa dajú odvodiť pomocou nasledujúcej logiky:

- Ak sa na objekte nachádza množina explicitných atribútov riadenia prístupu, potom bude definíciou riadenia prístupu objektu.
- Ak neexistujú žiadne explicitne definované atribúty riadenia prístupu, potom prejdite krížom cez adresárový strom smerom hore, kým nedosiahnete rodičovský uzol s množinou šírených atribútov riadenia prístupu.
- Ak nenájdete žiadny takýto rodičovský uzol, subjektu sa pridelí štandardný prístup, ktorý je opísaný nižšie.

Administrátor adresára je vlastníkom položky. Pseudoskupine cn=anybody (všetci užívatelia) bol pridelený prístup na čítanie, vyhľadávanie a porovnanie pre atribúty v triede prístupu normálne.

Vyhodnotenie prístupu

Prístup pre určitú operáciu sa povolí alebo zamietne na základe DN pre vytváranie väzieb subjektu pre takúto operáciu na cieľovom objekte. Spracovanie sa zastaví hneď po stanovení prístupu.

Kontroly prístupu sa vykonajú najprv nájdením definícií pre efektívne **entryOwnership** a **ACI**, kde sa skontroluje vlastníctvo položky a následne sa vyhodnotia hodnoty ACI objektu.

ACL na báze filtrov zhromažďujú od najnižšej zahrnutej položky smerom nahor, pozdĺž reťaze rodičovských položiek, k najvyššej položke zahrnutej v DIT. Efektívny prístup sa vypočíta ako zjednotenie prístupových práv, ktoré povolili

alebo zakázali ustanovujúce rodičovské položky. Existujúca množina pravidiel špecifickosti a kombinatoriky sa používajú na vyhodnotenie efektívneho prístupu pre ACL na báze filtrov.

Filtrované a nefiltrované atribúty sa v rámci adresára s jednou položkou vzájomne vylučujú. Umiestnenie obidvoch typov atribútov do rovnakej položky nie je povolené a je to narušenie obmedzenia. Operácie, priradené k vytvoreniu alebo aktualizácii položky adresára zlyhajú, ak bude takýto stav zistený.

Pri výpočte efektívneho prístupu nastavuje režim výpočtu prvý typ ACL, ktorý bude zistený v reťazi rodičov položky cieľového objektu. V režime na báze filtrov sa budú pri výpočte efektívneho prístupu ignorovať nefiltrované ACL. Podobne v režime nie-na-báze-filtrov sa budú pri výpočte efektívneho prístupu ignorovať ACL na báze filtrov.

Ak chcete obmedziť zhromažďovanie zoznamov ACL na báze filtrov vo výpočte efektívneho prístupu, atribút **ibm-filterAclInherit** nastavený na hodnotu ″false″ možno vložiť do ľubovoľnej položky medzi najvyšší a najnižší výskyt atribútu **ibm-filterAclEntry** v danom podstrome. To spôsobí, že podmnožina atribútov **ibm-filterAclEntry** nad ňou v reťazi rodičov cieľového objektu, sa bude ignorovať.

Ak sa v režime ACL na báze filtrov nepoužije žiadny ACL na báze filtrov, použije sa štandardný ACL (cn=anybody bude mať pridelený prístup na čítanie, vyhľadávanie a porovnanie pre atribúty v triede prístupu normálne). Táto situácia môže nastať, keď sa sprístupnená položka nezhoduje so žiadnym z filtrov, ktoré boli špecifikované v hodnotách **ibm-filterAclEntry**. Ak nechcete, aby sa použilo predvolené riadenie prístupu, môžete zadať zoznam predvoleného filtra, ako v nasledovnom príklade:

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

V tomto príklade nebude pridelený nijaký prístup. Zmeňte to, aby ste dostali prístup, ktorý chcete použiť.

Administrátor adresárov a hlavný server alebo rovnocenný server (pre replikáciu) štandardne dostanú úplné prístupové práva na všetky objekty v adresári, s výnimkou prístupu na zápis pre systémové atribúty. Ostatní **entryOwners** dostanú úplné prístupové práva pre objekty, ktoré majú vo vlastníctve, s výnimkou prístupu na zápis pre systémové atribúty. Všetci užívatelia majú prístupové práva na čítanie pre systémové a obmedzené atribúty. Tieto preddefinované práva sa nedajú zmeniť. Ak má žiadajúci subjekt **entryOwnership**, prístup sa stanoví podľa horeuvedených štandardných nastavení a zastavení spracovania prístupu.

Ak žiadajúci objekt nie je entryOwner, potom sa skontrolujú hodnoty ACI pre položky objektu. Prístupové práva, ako sú definované v ACI pre cieľový objekt sa vypočítajú podľa pravidiel špecifickosti a kombinatoriky.

Pravidlo špecifickosti

Najšpecifickejšie definície aclEntry sú definície, ktoré sa používajú pri vyhodnotení pridelených/zamietnutých oprávnení pre užívateľa. Úrovne špecifickosti sú:

- Access-id, je špecifickejšia ako skupina alebo rola. Skupiny a roly sú na rovnakej úrovni.
- V rámci rovnakej úrovne **dnType** sú oprávnenia úrovne konkrétnych atribútov špecifickejšie ako oprávnenia úrovne triedy atribútov.
- V rámci rovnakej úrovne atribútov alebo triedy atribútov je hodnota **deny** špecifickejšia ako hodnota **grant**.

Pravidlo kombinatoriky

Oprávnenia pridelené subjektom rovnakej špecifickosti budú kombinované. Ak sa prístup nedá určiť v rámci rovnakej úrovne špecifickosti, použijú sa definície prístupu nižšej špecifickej úrovne. Ak nebude prístup určený po použití všetkých definovaných ACI, prístup bude zamietnutý.

Poznámka: Keď bude pri vyhodnocovaní prístupu nájdená zhodná **aclEntry** úrovne ID prístupu, aclEntries úrovne skupiny nebudú zahrnuté do výpočtu prístupu. Výnimkou je, ak sú všetky zhodné **aclEntries** úrovne ID prístupu definované pod cn=this, potom sa aj všetky zhodné **aclEntries** úrovne skupiny skombinujú vo vyhodnotení.

Inak povedané, ak definovaná položka ACI v rámci položky objektu obsahuje DN subjektu id-prístupu, ktoré sa zhoduje s DN pre vytvorenie väzby, potom sa oprávnenia budú najprv vyhodnocovať na základe takejto aclEntry. Ak sú pod rovnakým DN subjektu definované zhodné oprávnenia úrovne atribútov, tieto nahrádzajú všetky oprávnenia, ktoré

boli definované pod triedami atribútov. Ak sú pod definíciou rovnakej úrovne atribútov alebo triedy atribútov prítomné rozporné oprávnenia, zamietnuté oprávnenia vyradia udelené oprávnenia.

Poznámka: Oprávnenie definovanej hodnoty null zamedzí včlenenie menej špecifických definícií oprávnení.

Ak sa prístup stále nedá určiť a všetky nájdené zhodné aclEntries sú definované pod ″cn=this″, potom sa vyhodnotí členstvo v skupine. Ak užívateľ patrí do viacerých skupín, užívateľ prijme z týchto skupín kombinované oprávnenia. Okrem toho bude užívateľ automaticky patriť do skupiny cn=Anybody a možno do skupiny cn=Authenticated, ak užívateľ vytvoril autentifikované väzby. Ak sú pre tieto skupiny definované oprávnenia, užívateľ dostane špecifikované oprávnenia.

Poznámka: Členstvo v skupine a v role sa stanovuje v čase vytvárania väzieb a trvá kým nebude vytvorená iná väzba, alebo kým nebude prijatá požiadavka na zrušenie väzieb. Vnorené skupiny a roly, ktoré skupina alebo rola definovala ako člena inej skupiny alebo role, nebudú analyzované pri určovaní členstva ani pri vyhodnocovaní prístupu.

Napríklad predpokladajme, že attribute1 je v skupine atribútov citlivé a užívateľ cn=Person A, o=IBM patrí aj do group1 aj do group2 s nasledujúcimi definovanými aclEntries:

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

Tento užívateľ dostane:

- Prístup na ’rsc’ pre attribute1, (definícia z 1. úrovne atribútov nahrádza definíciu úrovne triedy atribútov).
- Žiadny prístup do iných atribútov triedy citlivé na cieľovom objekte, (z 1).
- Nebudú pridelené žiadne iné práva (2 a 3 NIE sú zahrnuté vo vyhodnotení prístupu).

Ďalší príklad s nasledovnými aclEntries:

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

Užívateľ má:

- žiadny prístup pre atribúty triedy citlivé, (z 1. hodnoty Null definovanej pod access-id zamedzuje začlenenie oprávnení k atribútom triedy citlivé z group1).
- a prístup ’rsc’ pre triedu atribútov normálne (z 2).

Definovanie ACI a vlastníkov položiek

Nasledujúce dva príklady ukazujú vytváranie administratívnej poddomény. Prvý príklad ukazuje priradenie jedného užívateľa ako entryOwner pre celú doménu. Druhý príklad ukazuje priradenie skupiny ako entryOwner.

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

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

Nasledujúci príklad ukazuje, ako sa pre access-id ″cn=Person 1, o=IBM″ prideľujú oprávnenia na čítanie, vyhľadávanie a porovnanie pre attribute1. Oprávnenie sa použije pre každý uzol v celom podstrome, na alebo pod uzlom, ktorý obsahuje toto ACI, ktoré sa zhoduje s filtrom porovnania ″(objectclass=groupOfNames)″. Zhromažďovanie zhodných atribútov ibm-filteraclentry vo všetkých rodičovských uzloch bolo ukončené na tejto položke, nastavením atribútu ibm-filterAclInherit na hodnotu ″false″.

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

ibm-filterAclInherit: false
```

Nasledujúci príklad ukazuje ako sa pre skupinu ″cn=Dept XYZ, o=IBM″ prideľujú oprávnenia na čítanie, vyhľadávanie a porovnanie pre attribute1. Oprávnenie sa použije pre celý podstrom pod uzlom, ktorý obsahuje toto ACI.

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

Nasledujúci príklad ukazuje, ako sa pre rolu ″cn=System Admins,o=IBM″ prideľujú oprávnenia na pridanie objektov pod tento uzol a na čítanie, vyhľadávanie a porovnanie pre attribute2 a triedu atribútov kritické. Oprávnenie sa použije iba pre uzol, ktorý obsahuje toto ACI.

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

Zmena hodnôt ACI a vlastníka položky

Modify-replace

Modify-replace funguje rovnakým spôsobom, ako všetky ostatné atribúty. Ak hodnota atribútu neexistuje, vytvorte hodnotu. Ak hodnota atribútu existuje, nahraďte hodnotu.

Pre položku boli dané nasledujúce ACI:

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

vykonajte nasledujúcu zmenu:

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

Výsledné ACI je:

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

Hodnoty ACI pre Dept ABC sa počas nahradenia stratili.

Pre položku boli dané nasledujúce ACI:

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

vykonajte nasledujúce zmeny:

```
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
```

Výsledné ACI je:

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

Hodnoty ACI pre Dept ABC sa počas nahradenia stratili.

Modify-add

Ak ACI alebo entryOwner neexistujú, počas ldapmodify-add sa vytvorí ACI alebo entryOwner so špecifickými hodnotami. Ak ACI alebo entryOwner existujú, potom pre dané ACI alebo entryOwner pridajte špecifikované hodnoty. Napríklad pre ACI je dané:

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

s modifikáciou:

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

by dalo aclEntry s viacerými hodnotami:

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

Napríklad pre ACI je dané:

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

s modifikáciou:

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

by dalo aclEntry s viacerými hodnotami:

```
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
```

Oprávnenia pod rovnakým atribútom alebo triedou atribútov sa považujú za základné stavebné bloky a akcie sa považujú za kvalifikátory. Ak bude rovnaká hodnota oprávnenia pridaná viackrát, uloží sa iba jedna hodnota. Ak bude rovnaká hodnota oprávnenia pridaná viackrát, ale s rôznymi hodnotami akcií, použije sa posledná hodnota akcie. Ak je pole výsledného oprávnenia prázdne (″″), hodnota tohto oprávnenia sa nastaví na null a hodnota akcie sa nastaví na **grant**.

Napríklad, ak je dané nasledujúce ACI:

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

s modifikáciou:

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

prinesie aclEntry:

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

Napríklad, ak je dané nasledujúce ACI:

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

s modifikáciou:

```
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
```

prinesie aclEntry:

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

Modify-delete

Ak chcete vymazať určitú hodnotu ACI, použite bežnú syntax ldapmodify-delete.

Ak je dané ACI:

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

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

poskytne zostávajúce ACI na server :

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

Ak je dané ACI:

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

poskytne zostávajúce ACI na server :

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

Výsledkom vymazania hodnoty ACI alebo entryOwner, ktorá neexistuje, bude nezmenené ACI alebo entryOwner a návratový kód, ktorý bude špecifikovať, že hodnota atribútu neexistuje.

Vymazanie hodnôt ACI/vlastníka položky

Pri operácii ldapmodify-delete, môžete entryOwner vymazať, keď zadáte

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

V tomto prípade by položka nemala žiadneho explicitného entryOwner. Automaticky sa odstráni aj ownerPropagate. Táto položka by zdedila svojho entryOwner z rodičovského uzla v adresárovom strome, pri dodržaní pravidla o šírení.

To isté môžete urobiť, ak chcete úplne vymazať aclEntry:

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

Vymazanie poslednej hodnoty ACI alebo entryOwner z položky nie je to isté, ako vymazanie ACI alebo entryOwner. Položka môže obsahovať ACI alebo entryOwner bez hodnôt. V tomto prípade sa klientovi pri dotazovaní ACI alebo entryOwner nevráti nič a šírenia sa nastavia do uzlov potomkov, kým nebudú vyradené. Aby sa zamedzili túlavé položky, na ktoré nebude mať nikto prístup, administrátor adresárov bude mať vždy úplný prístup na položku, dokonca aj vtedy, ak má položka hodnotu null ACI alebo entryOwner.

Získanie hodnôt ACI/vlastníka položky

Platné hodnoty ACI alebo entryOwner sa dajú jednoducho získať, keď vo vyhľadávaní zadáte požadované atribúty ACL alebo entryOwner, napríklad,

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

vráti všetky informácie ACL alebo entryOwner, ktoré sa používajú vo vyhodnocovaní prístupu na objekt A. Uvedomte si, že vrátené hodnoty nemusia vyzerať presne rovnako, ako keď boli prvýkrát definované. Hodnoty sú ekvivalentom pôvodnej formy.

Vyhľadávanie iba atribútu ibm-filterAclEntry vráti iba hodnoty, ktoré sú špecifické pre obsiahnutú položku.

Prevádzkový atribút iba-na-čítanie s názvom ibm-effectiveAcl sa používa na zobrazenie zhromaždeného efektívneho prístupu. Požiadavka na vyhľadávanie ibm-effectiveAcl vráti efektívny prístup, ktorý sa použije na cieľovom objekte na báze: bezfiltrových ACL alebo ACL s filtrami, podľa toho ako boli v DIT distribuované.

Pretože ACL na báze filtrov môžu pochádzať z niekoľkých rodičovských zdrojov, vyhľadávanie atribútu aclSource poskytne zoznam priradených zdrojov.

Hľadiská replikácie podstromov

Ak má byť prístup na báze filtrov zaradený do replikácie podstromu, všetky atribúty ibm-filterAclEntry musia byť trvalo umiestnené na alebo pod priradenou položkou ibm-replicationContext.

Pretože efektívny prístup sa nedá zhromaždiť z rodičovskej položky nad replikovaným podstromom, atribút ibm-filterAclInherit musí byť nastavený na hodnotu **false** a musí byť trvalo umiestnený na priradenej položke ibm-replicationContext.

Vlastníctvo objektov adresára LDAP

Každý objekt vo vašom adresári LDAP má aspoň jedného vlastníka. Vlastníci objektov majú možnosť objekt vymazať. Vlastníci a administrátor servera sú jediní užívatelia, ktorí môžu meniť atribúty vlastníctva vlastností a zoznamu riadenia prístupu (ACL) každého objektu. Vlastníctvo objektov môže byť buď zdedené alebo explicitné. Ak chcete priradiť vlastníctvo, môžete urobiť nasledujúce činnosti:

- Explicitne nastaviť vlastníctvo špecifického objektu.
- Určiť, či objekty zdedia vlastníkov od objektov, ktoré sa nachádzajú vyššie v hierarchii adresára LDAP.

Adresárový server vám umožňuje uviesť pre ten istý objekt viacerých majiteľov. Môžete tiež uviesť, že objekt vlastní sám seba. Spravíte to tak, že do zoznamu vlastníkov objektov zahrniete špeciálne DN cn=this. Predpokladajme napríklad, že objekt cn=A má majiteľa cn=this. Každý užívateľ bude mať prístup k objektu cn=A ako vlastník, ak sa k serveru pripojí ako cn=A.

Viac informácií o spôsobe práce s vlastnosťami vlastníctva nájdete v časti “Manažovanie položiek adresára” na strane 162.

Politika hesiel

Keď sa na autentifikáciu používajú servery LDAP, je dôležité, aby server LDAP podporoval politiky súvisiace s exspiráciou hesla, chybnými pokusmi o prihlásenie a pravidlami hesla. Adresárový server poskytuje konfigurovateľnú podporu pre všetky tri z týchto druhov politík. Táto politika sa týka všetkých položiek adresára s atribútom userPassword. Nemôžete definovať jednu politiku pre jednu skupinu užívateľov a iné politiky pre ostatné skupiny užívateľov. Adresárový server tiež poskytuje mechanizmus pre klientov, aby boli informovaní o podmienkach súvisiacich s politikou hesiel (heslo exspiruje o tri dni) a o skupine prevádzkových atribútov, ktoré môže administrátor použiť na vyhľadanie takých vecí, ako sú užívatelia s exspirovaným heslom alebo zablokované kontá.

Viac informácií o tom, ako pracovať s vlastnosťami politiky hesiel, nájdete v časti “Riadenie hesiel” na strane 145.

Konfigurácia

Môžete nakonfigurovať správanie servera s ohľadom na heslá v týchto oblastiach:

- Globálny prepínač ″on/off″ pre povolenie alebo zakázanie politiky hesiel
- Pravidlá pre zmenu hesiel, vrátane týchto:
  - Užívatelia môžu meniť svoje vlastné heslá. Táto politika sa používa navyše okrem všetkých kontrol prístupu. To znamená, že riadenie prístupu musí dať užívateľovi oprávnenie na zmenu atribútu userPassword, ako aj politiku hesiel, ktorá umožňuje užívateľom meniť svoje vlastné heslá. Ak je táto politika zakázaná, užívatelia nemôžu meniť svoje vlastné heslá. Iba administrátor alebo iný užívateľ s oprávnením na zmenu atribútu userPassword môžu meniť heslo.
  - Heslá musia byť zmenené po resetovaní. Ak je táto politika povolená, keď mení heslo ktokoľvek iný ako ten užívateľ, heslo je označené ako resetované a musí byť zmenené užívateľom skôr ako bude môcť vykonať iné adresárové operácie. Požiadavka na pripojenie s resetovaným heslom je úspešná. Aby aplikácia vedela, že heslo musí byť resetované, musí poznať politiku hesiel.
  - Užívatelia musia pri zmene hesla odoslať staré heslo. Ak je táto politika povolená, heslo môže byť zmenené len požiadavkou na modifikáciu, ktorá zahŕňa vymazanie atribútu userPassword (so starou hodnotou) aj pridanie novej hodnoty userPassword. Toto zabezpečí, že len užívateľ, ktorý pozná svoje heslo, ho môže zmeniť. Administrátor alebo iní užívatelia oprávnení na zmenu atribútu userPassword, môžu vždy nastaviť heslo.
- Pravidlá pre exspiráciu hesla vrátane týchto:
  - Heslá nikdy neexspirujú alebo heslá exspirujú po konfigurovateľnom čase od poslednej zmeny.
  - Nevarovať užívateľov, keď heslo exspiruje, alebo varovať užívateľov o konfigurovateľný čas pred exspiráciou hesla. Aby bola aplikácia varovaná o blížiacej sa exspirácii hesla, musí poznať politiku hesiel.
  - Povoliť konfigurovateľný počet povolených prihlásení po exspirácii hesla užívateľa. Aplikácia, ktorá pozná politiku hesiel, bude poznať počet zostávajúcich povolených prihlásení. Ak nie sú povolené žiadne prihlásenia po exspirovaní, užívateľ nemôže autentifikovať ani zmeniť svoje vlastné heslo.
- Pravidlá pre overenie platnosti hesla, vrátane týchto:
  - Konfigurovateľná veľkosť histórie hesla, ktorá povie serveru, či má uchovávať históriu posledných N hesiel a odmietnuť heslá, ktoré boli v minulosti použité.
  - Kontrola syntaxe hesla, vrátane nastavenia, ako sa má server správať, keď sú heslá hašované. Toto nastavenie ovplyvňuje, či má server ignorovať politiku podľa niektorej z týchto podmienok:
    - Server ukladá hašované heslá.
    - Klient doručí serveru hašované heslo (to sa môže stať pri prenose položiek medzi servermi pomocou súboru LDIF, ak zdrojový server ukladá hašované heslá).

    V oboch z týchto prípadov server nebude schopný aplikovať všetky pravidlá pre syntax. Podporované sú nasledujúce pravidlá syntaxe: minimálna dĺžka, minimálny počet abecedných znakov, minimálny počet numerických alebo špeciálnych znakov, počet opakovaných znakov a počet znakov, v ktorých sa heslo musí odlišovať od predchádzajúceho hesla.
- Pravidlá pre neúspešné prihlasovania, vrátane týchto:
  - Minimálny čas povolený medzi zmenami hesla, ktorý bráni užívateľom pred rýchlym cyklením skupiny hesiel, aby sa dostali späť k svojmu pôvodnému heslu.
  - Maximálny počet neúspešných pokusov o prihlásenie pred zablokovaním konta.
  - Konfigurovateľné trvanie blokovania hesla. Po tomto čase sa môže opäť používať zablokované konto. Toto môže pomôcť zablokovať pokusy hakerov o crack hesla, keď pomáhate užívateľovi, ktorý zabudol svoje heslo.
  - Konfigurovateľný čas, po ktorý server sleduje neúspešné pokusy o prihlásenie. Ak sa počas tohto času dosiahne maximálny počet neúspešných pokusov o prihlásenie, konto sa zablokuje. Keď uplynie tento čas, server zruší informácie o predchádzajúcich neúspešných pokusoch o prihlásenie pre toto konto.

Nastavenia politiky hesiel pre adresárový server sa uložia do objektu ″cn=pwdpolicy″, ktorý vyzerá nasledovne:

```
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
```

Aplikácie informované o politike hesiel

Podpora politiky hesiel Adresárového servera pre iSeries obsahuje množinu ovládacích prvkov LDAP, ktoré môžu využívať pomocou aplikácie, ktorá pozná politiku hesiel, na prijímanie oznámení o stavoch súvisiacich s politikou hesiel.

Aplikácia môže byť informovaná o týchto varovných stavoch:
- Čas zostávajúci do exspirácie hesla
- Počet povolených prihlásení zostávajúci po exspirovaní hesla

Aplikácia môže byť tiež informovaná o týchto chybových stavoch:
- Heslo exspirovalo
- Konto je zablokované
- Heslo bolo resetované a musí byť zmenené
- Užívateľ nemôže zmeniť svoje heslo
- Keď sa mení heslo, musí byť dodané staré heslo
- Nové heslo porušuje syntaktické pravidlá
- Nové heslo je príliš krátke
- Heslo bolo zmenené priskoro
- Nové heslo je v histórii

Používajú sa dve kontroly. Kontrola požiadavky o politiku hesiel sa používa na informovanie servera, ktorý si aplikácia želá informovať o stavoch súvisiacich s politikou hesiel. Táto kontrola musí byť špecifikovaná aplikáciou na všetkých operáciách, o ktoré sa zaujíma, zvyčajne je to požiadavka o úvodné pripojenie a všetky požiadavky o zmenu hesla. Ak je prítomná kontrola požiadavky politiky hesiel, server vráti odpoveď na kontrolu politiky hesiel, keď sa vyskytne niektorý z hore uvedených chybových stavov.

API klienta adresárového servera obsahujú množinu API, ktoré môžu používať C aplikácie na prácu s týmito kontrolami. Tieto API sú:
- ldap_parse_pwdpolicy_response
- ldap_pwdpolicy_err2string

Pre aplikácie, ktoré nepoužívajú tieto API, sú kontroly definované dole. Musíte používať schopnosti, ktoré poskytujú API klienta LDAP používané na spracovanie kontrol. Napríklad JNDI (Java Naming and Directory Interface) má zabudovanú podporu pre niektoré známe ovládače a tiež poskytuje rámec pre podporovanie ovládačov, ktoré JNDI nepozná.

Kontrola požiadavky politiky hesiel

```
Názov kontroly: 1.3.6.1.4.1.42.2.27.8.5.1
Kritickosť kontroly: FALSE
Hodnota kontroly: None
```

Kontrola odpovede politiky hesiel

```
Názov kontroly: 1.3.6.1.4.1.42.2.27.8.5.1 (rovnaký ako kontrola požiadavky)
Kritickosť kontroly: FALSE
Hodnota kontroly: Hodnota kódovaná BER definovaná v ASN.1 nasledovne:
  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) } }
```

Ako ostatné prvky protokolu LDAP, aj kódovanie BER používa implicitné označovanie.

Prevádzkové atribúty politiky hesiel

Adresárový server udržiava množinu prevádzkových atribútov pre každú položku, ktorá má atribút userPassword. Tieto atribúty možno vyhľadať podľa autorizovaných užívateľov, buď použitých vo vyhľadávacích filtroch alebo vrátených požiadavkou na vyhľadanie. Tieto atribúty sú:

- pwdChangedTime - Atribút GeneralizedTime obsahujúci čas, kedy bolo poslednýkrát zmenené heslo.
- pwdAccountLockedTime - Atribút GeneralizedTime obsahujúci čas, kedy bolo zablokované konto. Ak konto nie je zablokované, tento atribút nie je prítomný.
- pwdExpirationWarned - Atribút GeneralizedTime obsahujúci čas, kedy bolo prvýkrát klientovi poslané varovanie o exspirácii hesla.
- pwdFailureTime - Viachodnotový atribút GeneralizedTime obsahujúci časy predchádzajúcich po sebe nasledujúcich neúspešných pokusov o prihlásenie. Ak bolo posledné prihlásenie úspešné, tento atribút nie je prítomný.
- pwdGraceUseTime - Viachodnotový atribút GeneralizedTime obsahujúci časy predchádzajúcich povolených prihlásení po exspirácii hesla.
- pwdReset - Boolovský atribút obsahujúci hodnotu TRUE, ak bolo heslo resetované a muselo byť zmenené užívateľom.
- ibm-pwdAccountLocked - Boolovský atribút signalizujúci, že konto bolo administratívne uzamknuté.

Replikácia politiky hesiel

Informácie o politike hesiel sú replikované z dodávateľských serverov spotrebiteľom. Zmeny v položke cn=pwdpolicy sú replikované ako globálne zmeny, podobne ako zmeny v schéme. Informácie o stave politiky hesiel pre individuálne položky sú tiež replikované, takže ak je napríklad položka zablokovaná na dodávateľskom serveri, táto akcia bude replikovaná všetkým spotrebiteľom. Zmeny stavu politiky hesiel na replike určenej len na čítanie sa však nereplikujú na všetky ostatné servery.

Autentifikácia

Riadenie prístupu v adresárovom serveri je založené na rozlišovacom názve (DN) združenom s daným pripojením. Toto DN je vytvorené ako výsledok pripojenia k (prihlásenie do) adresárovému serveru.

Keď je adresárový server prvýkrát konfigurovaný, na autentifikáciu servera sa môžu použiť tieto identity:

- Anonymous
- Administrátor adresára (štandardne cn=administrator)
- Projektovaný užívateľský profil i5/OS (pozrite časť “Projektované pozadie operačného systému” na strane 73)

Je dobré vytvoriť ďalších užívateľov, ktorým možno dať oprávnenie na riadenie rôznych častí adresára bez požiadavky, aby ste zdieľali identitu administrátora adresára.

Ďalšie informácie nájdete v časti “Manažovanie užívateľov” na strane 169.

Z perspektívy LDAP sú rámce pre autentifikáciu na LDAP nasledovné:

- Jednoduché spojenie, v ktorom aplikácia poskytuje DN a čisté textové heslo pre toto DN
- Simple Authentication and Security Layer (SASL), ktorý poskytuje niekoľko ďalších autentifikačných metód, vrátane CRAM-MD5, DIGEST-MD5, EXTERNAL, GSSAPI a OS400-PRFTKN.

Jednoduchá väzba, DIGEST-MD5 a CRAM-MD5

Keď chcete použiť jednoduché spojenie, klient musí poskytnúť DN existujúcej položky LDAP a heslo, ktoré je zhodné s atribútom userPassword pre túto položku. Mohli by ste napríklad vytvoriť takúto položku pre Johna Smitha:

```
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
```

Teraz môžete použiť DN ″cn=John Smith,cn=users,o=acme,c=us″ v riadení prístupu, alebo urobiť ho členom skupiny používanej v riadení prístupu.

Niektoré preddefinované objectclasses umožňujú špecifikovanie userPassword vrátane (no nielen): person, organizationalperson, inetorgperson, organization, organizationalunit a iných.

Heslá adresárového servera rozlišujú veľké a malé písmená. Ak vytvoríte položku s hodnotou userPassword secret, spojenie, ktoré špecifikuje heslo SECRET zlyhá.

Keď používate jednoduché spojenie, klient odošle čisté textové heslo do servera ako súčasť požiadavky o spojenie. Takéto heslo je ľahko zistiteľné sledovaním na úrovni protokolu. Na ochranu hesla sa môže použiť pripojenie SSL (všetky informácie odosielané cez pripojenie SSL sú šifrované). Alebo je možné použiť metódy DIGEST-MD5 alebo CRAM-MD5 SASL.

Metóda CRAM-MD5 vyžaduje, aby mal server prístup k čistému textovému heslu (ochrana hesla je nastavená na hodnotu none, čo v skutočnosti znamená, že heslo je uložené v dešifrovateľnej forme a vráti sa z vyhľadávaní ako čistý text) a systémová hodnota QRETSVRSEC (Uchovať bezpečnostné údaje servera) musí byť 1 (uchovať údaje). Klient odosiela DN na server. Server získa hodnotu userPassword pre túto položku a vygeneruje náhodný reťazec. Náhodný reťazec je odoslaný klientovi. Klient aj server transformujú tento náhodný reťazec pomocou hesla na kľúč, a klient odošle výsledok serveru. Ak sú tieto dva transformované reťazce zhodné, požiadavka na spojenie je úspešná a heslo nikdy nebolo odoslané na server.

Metóda DIGEST-MD5 je podobná metóde CRAM-MD5. Vyžaduje, aby server mal prístup k čistému textovému heslu (ochrana hesla je nastavená na hodnotunone) a aby systémová hodnota QRETSVRSEC bola nastavená na 1. Namiesto odoslania DN na server vyžaduje DIGEST-MD5aby klient odoslal na server hodnotu mena užívateľa. Aby bolo možné používať DIGEST-MD5 pre bežného užívateľa, (nie admina), žiadne iné položky v adresári nesmú mať rovnakú hodnotu pre atribút mena užívateľa. K ďalším rozdielom s DIGEST-MD5 patrí viac konfiguračných volieb: realm servera, atribút mena užívateľa a heslo administrátora. iSeries umožňuje užívateľom vytvoriť väzby ako projektovaní

alebo publikovaní užívatelia, kde server overí zadané heslo voči heslu užívateľského profilu v systéme. Keďže čisté textové heslo pre užívateľské profily nie je pre server dostupné, metódu DIGEST-MD5 nemožno používať s projektovanými alebo publikovanými užívateľmi.

Ďalšie informácie nájdete v časti “Konfigurácia autentifikácie DIGEST-MD5 na adresárovom serveri” na strane 151.

Spojenie ako publikovaný užívateľ

Adresárový server zabezpečuje prostriedky na udržanie položky LDAP, ktorej heslo je heslom užívateľského profilu operačného systému, na tom istom systéme. Ak to chcete urobiť, táto položka:

- Musí mať atribút UID, ktorého hodnota je názov užívateľského profilu operačného systému
- Nesmie mať atribút userPassword

Keď server prijme požiadavku na vytvorenie väzby pre položku, ktorá má hodnotu UID, ale nie userPassword, server požiada bezpečnosť operačného systému o overenie, či UID je platný názov užívateľského profilu a či zadané heslo je správnym heslom pre tento užívateľský profil. Takáto položka sa volá publikovaný užívateľ kvôli zverejneniu systémového distribučného adresára (SDD) do LDAP, ktorý vytvorí takéto položky.

Spojenie ako projektovaný užívateľ

Položka LDAP reprezentujúca užívateľský profil operačného systému sa nazýva projektovaný užívateľ. DN projektovaného užívateľa môžete použiť spolu so správnym heslom pre tento užívateľský profile v jednoduchom spojení. Napríklad DN pre užívateľa JSMITH v systéme my-system.acme.com by bol:

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

Spojenie SASL EXTERNAL

Ak sa používa SSL alebo TLS pripojenie s klientskou autentifikáciou (napríklad klient má súkromný certifikát), môže sa použiť metóda SASL EXTERNAL. Táto metóda povie serveru, že má získať identitu klienta z externého zdroja, v tomto prípade pripojenia SSL. Server získa verejnú časť klientskeho certifikátu (odoslanú serveru ako časť vybudovania pripojenia SSL) a extrahuje DN subjektu. Toto DN je pripojeniu priradené serverom LDAP.

Napríklad daný certifikát priradený k:

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

DN subjektu by bolo:

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

Prvky cn, ou, o, l, st a c sa používajú v tomto poradí na generovanie DN subjektu.

Spojenie SASL GSSAPI

Spojovací mechanizmus SASL GSSAPI sa používa na autentifikáciu na serveri pomocou lístka Kerberos. Toto je užitočné, keď klient vykonal KINIT alebo inú formu autentifikácie Kerberos (napríklad prihlásenie do domény Windows 2000). V tomto prípade server overuje lístok klienta a potom získa názvy principála a realmu Kerberos; napríklad principál jsmith v realme acme.com, bežne vyjadrené ako jsmith@acme.com. Server môže byť nakonfigurovaný, aby namapoval túto identitu do DN jedným z dvoch spôsobov:

- Generovať pseudo DN v tvare ibm-kn=jsmith@acme.com
- Vyhľadať položku, ktorá má dodatočnú triedu ibm-securityidentities a hodnotu altsecurityidenties v tvare KERBEROS:<principál>@<realm>.

Položka, ktorá sa môže použiť pre jsmith@acme.com, môže vyzerať takto:

```
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
```

Informácie o tom, ako povoliť autentifikáciu Kerberos, nájdete v časti “Povolenie autentifikácie Kerberos na adresárovom serveri” na strane 151.

Spojenie OS400-PRFTKN

Spojovací mechanizmus OS400-PRFTKN SASL sa používa na autentifikáciu na serveri pomocou tokenu profilu (pozrite si API Generovanie tokenu profilu). Keď sa používa tento mechanizmus, server overuje token profilu a priraďuje DN projektovaného užívateľského profilu pripojeniu (napríklad os400-profile=JSMITH,cn=accounts,os400-system=my-as400.mycompany.com). Ak už má aplikácia token profilu, tento mechanizmus ruší potrebu získania mena užívateľského profilu a hesla užívateľa na vykonanie jednoduchého spojenia. Keď chcete používať tento mechanizmus, použite API ldap_sasl_bind s, špecifikujte nulové DN, OS400-PRFTKN pre tento mechanizmus a berval (binárne údaje, ktoré sú kódované pomocou zjednodušených základných pravidiel kódovania) obsahujúci 32-bajtový token profilu pre oprávnenia. Pri použití rozhraní YPI LDAP v systéme i5/OS alebo použití príkazových pomocných programov QSH (napríklad ldapsearch) na prístup k lokálnemu adresárovému serveru, môžete vynechať heslo a rozhrania API klienta sa autentifikujú na server ako aktuálny užívateľský profil pre túto úlohu. Napríklad:

```
> ldapsearch -m OS400-PRFTKN -b "o=ibm,c=us" "(uid=johndoe)"
```

vykoná vyhľadávanie pod oprávnením aktuálneho užívateľského profilu, ako keby ste použili:

```
> ldapsearch -D os400-profile=myprofile,cn=accounts,os400-sys=mysystem -w mypassword -b
"o=ibm,c=us" "(uid=johndoe)"
```

LDAP ako autentifikačná služba

LDAP sa zvyčajne používa na poskytovanie autentifikačnej služby. Môžete konfigurovať webový server, aby sa autentifikoval v LDAP. Nastavením viacerých webových serverov (alebo iných aplikácií) na autentifikáciu v LDAP môžete vytvoriť jeden register užívateľov pre tieto aplikácie, a nemusíte definovať užívateľov stále dokola pre každú aplikáciu alebo inštanciu webového servera.

Ako to funguje? V skratke, webový server vyzve užívateľa na zadanie mena užívateľa a hesla. Webový server zoberie tieto informácie a potom vyhľadá v adresári LDAP položku s týmto menom užívateľa (môžete napríklad nakonfigurovať webový server, aby namapoval meno užívateľa do atribútov LDAP ’uid’ alebo ’mail’). Ak webový server nájde presne jednu položku, odošle požiadavku na spojenie serveru, kde použije DN položky, ktorú práve našiel a heslo, ktoré poskytol užívateľ. Ak je spojenie úspešné, užívateľ je teraz autentifikovaný. Na ochranu informácií o hesle pred sledovaním na úrovni protokolu možno použiť pripojenia SSL.

Webový server tiež môže sledovať použitý DN tak, že daná aplikácia môže používať tento DN, napríklad ukladaním údajov o prispôsobení v tejto položke, inej položke s ním spojenej alebo v samostatnej databáze používajúcej DN ako kľúč na vyhľadávanie informácií.

Bežná možnosť používania požiadavky na spojenie je použitie porovnávacej operácie LDAP. Napríklad ldap_compare(ldap_session, dn, "userPassword", enteredPassword). Toto umožňuje aplikácii používať jednu reláciu LDAP a nie spúšťať a ukončovať relácie pre každú autentifikačnú požiadavku.

Odmietnutie služby

Adresárový server chráni pred nasledovnými typmi útokmi odmietnutím služby:

- Klienti, ktorí odosielajú údaje pomaly, odosielajú parciálne údaje alebo neodosielajú žiadne údaje

- Klienti, ktorí nečítajú údajové výsledky, alebo ktorí čítajú výsledky pomaly
- Klienti, ktorí nerušia väzby
- Klienti, ktorí vykonávajú požiadavky, ktoré spôsobujú dlhotrvajúce požiadavky na databázu
- Klienti, ktorí vytvárajú väzby anonymne
- Zaťaženia servera, ktoré zamedzujú administrátorovi v správe servera

Adresárový server poskytuje administrátorovi niekoľko metód na zabránenie útokom cez odmietnutie služby. Administrátor má vždy prístup na server cez použitie núdzového vlákna, aj keď je server zaneprázdnený dlhotrvajúcim operáciami. Okrem toho administrátor môže riadiť cez prístup na server vrátane schopnosti odpájať klientov s konkrétnym DN väzby alebo adresou IP a nakonfigurovať server tak, aby nepovoľoval anonymný prístup. Ostatné konfiguračné voľby možno aktivovať tak, aby umožňovali serveru aktívne zabraňovať útokom cez odmietnutie služby.

Bližšie informácie nájdete v časti:

- "Riadenie pripojení servera" na strane 109
- "Riadenie vlastností pripojenia" na strane 110

Projektované pozadie operačného systému

Projektované pozadie systému má schopnosť namapovať objekty i5/OS ako položky v adresárovom strome dostupnosti LDAP. Projektované objekty sú reprezentácie LDAP objektov operačného systému namiesto skutočných položiek uložených v databáze servera LDAP. Užívateľské profily sú jediné objekty, ktoré sú mapované alebo projektované ako položky v adresárovom strome. Mapovanie objektov užívateľského profilu sa nazýva Užívateľské projektované pozadie operačného systému.

Operácie LDAP sa namapujú na objekty operačného systému nižšej úrovne a operácie LDAP vykonajú funkcie operačného systému za účelom prístupu k týmto objektom. Všetky operácie LDAP vykonávané na užívateľských profiloch sa vykonávajú pod oprávnením užívateľského profilu priradeného ku pripojeniu klienta.

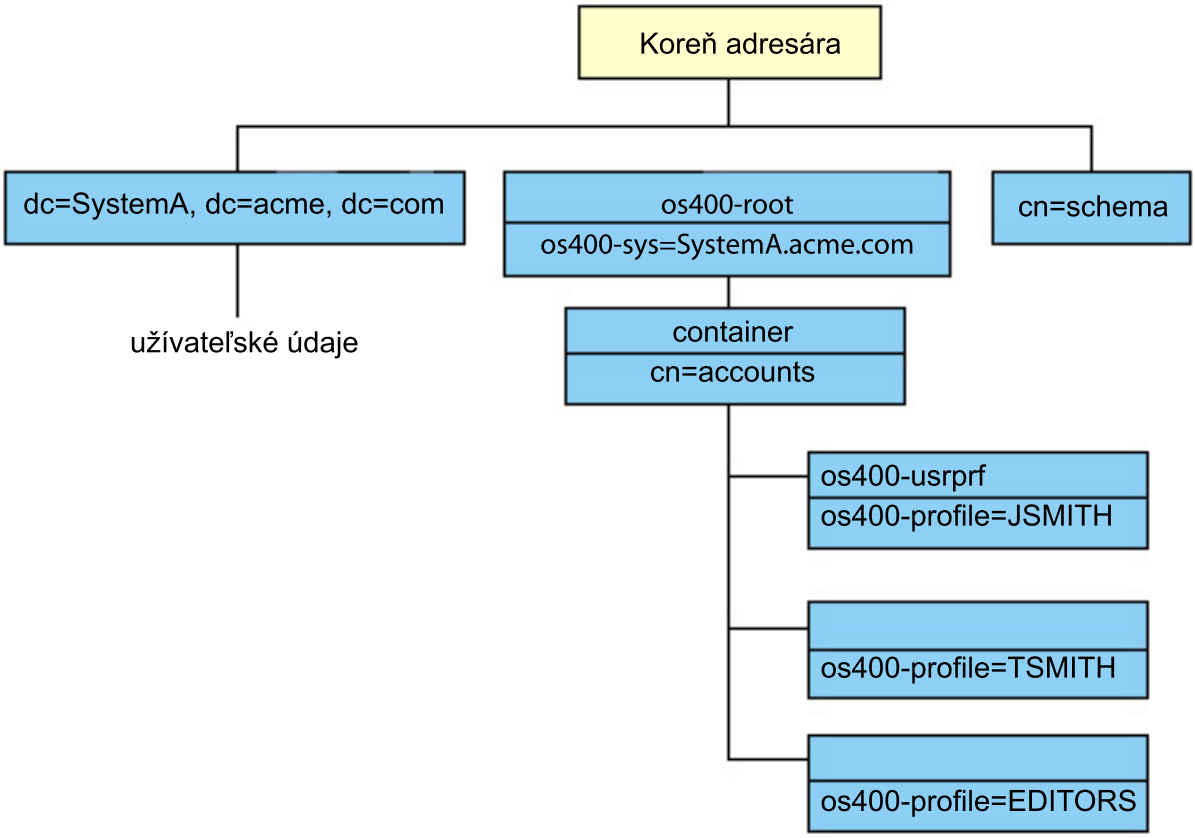
Podrobnejšie informácie o projektovanej funkčnosti operačného systému nájdete v nasledujúcom:

- "Užívateľský projektovaný adresárový informačný strom"
- "Operácie LDAP" na strane 74
- "DN pripojenia administrátora a repliky" na strane 78
- "Užívateľská projektovaná schéma" na strane 78

Užívateľský projektovaný adresárový informačný strom

Nasledujúci obrázok znázorňuje vzorový adresárový informačný strom (DIT) pre projektované pozadie užívateľa. Obrázok znázorňuje jednotlivé, aj skupinové profily. Na obrázku sú JSMITH a TSMITH užívateľské profily, ktoré sa indikujú interne skupinovým identifikátorom (GID), GID=*NONE (alebo 0); EDITORS je skupinový profil, ktorý sa indikuje interne nenulovým GID.

Prípona dc=SystemA,dc=acme,dc=com je zaradená v obrázku kvôli referencii. Táto prípona predstavuje aktuálne databázové pozadie, ktoré riadi ostatné položky LDAP. Prípona cn=schema je aktuálne používaná schéma na celom serveri.



Koreňom stromu je prípona na os400-sys=*SystemA.acme.com*, kde *SystemA.acme.com* je názov vášho systému. Trieda objektu je os400-root. Hoci strom DIT nie je možné upraviť ani vymazať, môžete prekonfigurovať príponu systémového objektu. Musíte však zabezpečiť, aby sa aktuálna prípona nepoužívala v ACL alebo nikde v systéme, kde by bolo treba modifikovať položky, keby sa prípona zmenila.

Na predchádzajúcom obrázku sa kontajner cn=accounts zobrazí pod koreňom. Tento objekt nemožno modifikovať. Kontajner je umiestnený na tejto úrovni v očakávaní iných druhov informácií alebo objektov, ktoré by mohli byť v budúcnosti projektované operačným systémom. Pod kontajnerom cn=accounts sa nachádzajú užívateľské profily, ktoré sú naprojektované ako objectclass=os400-usrprf. Tieto užívateľské profily sa nazývajú projektované užívateľské profily a sú LDAP známe v tvare os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com.

Operácie LDAP

Nasledujú operácie LDAP, ktoré možno vykonať pomocou projektovaných užívateľských profilov.

Vytváranie väzieb

Klient LDAP sa môže pripojiť (autentifikovať) k serveru LDAP pomocou projektovaného užívateľského profilu. Toto sa vykoná špecifikovaním charakteristického názvu (DN) projektovaného užívateľského profilu pre DN väzby a správneho hesla užívateľského profilu pre autentifikáciu. Príkladom DN používaného v požiadavke na vytvorenie väzby je os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com.

Klient sa musí pripojiť ako projektovaný užívateľ, aby mohol mať prístup k informáciám v systémovom projektovanom pozadí.

Na autentifikáciu na adresárový server ako projektovaný užívateľ sú k dispozícii dva ďalšie mechanizmy:

- Spojenie GSSAPI SASL. Ak je operačný systém nakonfigurovaný na používanie aplikácie Enterprise Identity Mapping (EIM), adresárový server požiada EIM o zistenie, či existuje asociácia na lokálny užívateľský profil z počiatočnej identity Kerberos. Ak existuje také priradenie, server priradí užívateľský profil k pripojeniu a môže sa použiť na prístup k funkciám projekcie systému. Viac informácií o EIM nájdete v časti EIM.
- Spojenie OS400-PRFTKN SASL. Token profilu sa môže použiť na autentifikáciu do adresárového servera. Server priradí užívateľský profil tokenu profilu k pripojeniu.

Server vykonáva všetky operácie pomocou oprávnenia na daný užívateľský profil. DN projektovaného užívateľského profilu možno použiť v ACL LDAP ako iné DN položky LDAP. Jednoduchá metóda vytvorenia väzby je jedinou povolenou metódou vytvorenia väzby, keď je na požiadavke vytvorenia väzby uvedený projektovaný užívateľský profil.

Hľadanie

Projektované pozadie systému podporuje niektoré základné vyhľadávacie filtre. Vo vyhľadávacích filtroch môžete uviesť atribúty objectclass, os400-profile a os400-gid. Atribút os400-profile podporuje znaky wildcard. Atribút os400-gid je obmedzený na zadanie (os400-gid=0), čo je individuálny užívateľský profil, alebo !(os400-gid=0), čo je skupinový profil. Môžete získať všetky atribúty užívateľského profilu s výnimkou hesla a podobných atribútov.

Pre určité filtre sa vracajú len hodnoty DN objectclass a os400-profile. Je však možné pokračovať v hľadaní podrobnejších informácií.

Nasledujúca tabuľka opisuje správanie projektovaného pozadia systému pre operácie hľadania.

Tabuľka 3. Správanie projektovaného pozadia systému pre operácie hľadania

Požadované hľadanie	Základ hľadania	Rozsah hľadania	Vyhľadávací filter	Komentáre
Návrat informácií pre os400-sys=SystemA (voliteľne) pre kontajnery pod nimi a (voliteľne) pre objekty v týchto kontajneroch.	os400-sys=SystemA.acme.com	base, sub alebo one	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	Návrat príslušných atribútov a ich hodnôt na základe uvedeného rozsahu a filtra. Atribúty s náročným kódovaním a ich hodnoty sa vracajú pre príponu systémových objektov a kontajner pod ňou.
Návrat všetkých užívateľských profilov.	cn=accounts, os400-sys=SystemA.acme.com	one alebo sub	os400-gid=0	Pre projektované užívateľské profily sa vracajú len hodnoty DN (rozlišovací názov), objectclass a os400-profile. Ak je uvedený akýkoľvek iný filter, vráti sa LDAP_UNWILLING_ TO_PERFORM.
Návrat všetkých skupinových profilov.	cn=accounts, os400-sys=SystemA.acme.com	one alebo sub	(!(os400-gid=0))	Pre projektované užívateľské profily sa vracajú len hodnoty DN (rozlišovací názov), objectclass a os400-profile. Ak je uvedený akýkoľvek iný filter, vráti sa LDAP_UNWILLING_ TO_PERFORM.

Tabuľka 3. Správanie projektovaného pozadia systému pre operácie hľadania (pokračovanie)

Požadované hľadanie	Základ hľadania	Rozsah hľadania	Vyhľadávací filter	Komentáre
Návrat všetkých užívateľských a skupinových profilov.	cn=accounts, os400-sys=SystemA.acme.com	one alebo sub	os400-profile=*	Pre projektované užívateľské profily sa vracajú len hodnoty DN (rozlišovací názov), objectclass a os400-profile. Ak je uvedený akýkoľvek iný filter, vráti sa LDAP_UNWILLING_ TO_PERFORM.
Návrat informácií pre určitý užívateľský alebo skupinový profil, napríklad užívateľský profil JSMITH.	cn=accounts, os400-sys=SystemA.acme.com	one alebo sub	os400-profile=JSMITH	Možno uviesť ostatné atribúty, ktoré sa majú vrátiť.
Návrat informácií pre určitý užívateľský alebo skupinový profil, napríklad užívateľský profil JSMITH.	os400-profile=JSMITH, cn=accounts, os400-sys=SystemA.acme.com	bas, sub alebo one	objectclass=os400-usrprf objectclass=* os400-profile=JSMITH	Možno uviesť ostatné atribúty, ktoré sa majú vrátiť. Aj keď je možné uviesť rozsah jednej úrovne, výsledky hľadania nevrátia žiadne hodnoty, pretože pod užívateľským profilom JSMITH v DIT sa nič nenachádza.
Návrat všetkých užívateľských a skupinových profilov začínajúcich sa na A.	cn=accounts, os400-sys=SystemA.acme.com	one alebo sub	os400-profile=A*	Pre projektované užívateľské profily sa vracajú len hodnoty DN (rozlišovací názov), objectclass a os400-profile. Ak je uvedený akýkoľvek iný filter, vráti sa LDAP_UNWILLING_ TO_PERFORM.
Návrat všetkých skupinových profilov začínajúcich sa na G.	cn=accounts, os400-sys=SystemA.acme.com	one alebo sub	(&(!(os400-gid=0)) (os400-profile=G*))	Pre projektované užívateľské profily sa vracajú len hodnoty DN (rozlišovací názov), objectclass a os400-profile. Ak je uvedený akýkoľvek iný filter, vráti sa LDAP_UNWILLING_ TO_PERFORM.
Návrat všetkých užívateľských profilov začínajúcich sa na A.	cn=accounts, os400-sys=SystemA.acme.com	one alebo sub	(&(os400-gid=0) (os400-profile=A*))	Pre projektované užívateľské profily sa vracajú len hodnoty DN (rozlišovací názov), objectclass a os400-profile. Ak je uvedený akýkoľvek iný filter, vráti sa LDAP_UNWILLING_ TO_PERFORM.

Porovnávanie

Operáciu porovnávania LDAP možno použiť na porovnanie hodnoty atribútu projektovaného užívateľského profilu. Atribúty os400-aut a os400-docpwd nemožno porovnávať.

Pridávanie a modifikácia

Užívateľské profily môžete vytvárať pomocou operácie pridania LDAP a môžete tiež meniť užívateľské profily pomocou operácie úpravy LDAP.

Vymazávanie

Užívateľské profily možno vymazať pomocou operácie vymazania LDAP. Na špecifikáciu správania sa parametrov DLTUSRPRF OWNOBJOPT a PGPOPT sa teraz poskytujú dva ovládacie prvky servera LDAP, ktoré možno uviesť na operácii vymazávania LDAP. Pozrite si príkaz DLTUSRPRF (Delete User Profile), kde nájdete viac informácií o správaní týchto parametrov.

Nasledujú ovládacie prvky a ich identifikátory objektov (OID), ktoré možno uviesť na operácii klienta vymazávania LDAP.

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  Kontrolná hodnota je reťazec v tomto formáte:
  - controlValue ::= ownObjOpt [newOwner]
  - ownObjOpt ::= *NODLT / *DLT / *CHGOWN

  Hodnota ovládacieho prvku ownObjOpt uvádza akciu, ktorú treba vykonať, ak užívateľský profil vlastní objekty. Hodnota *NODLT indikuje nevymazať užívateľský profil, ak tento vlastní objekty. Hodnota *DLT indikuje vymazať objekty vo vlastníctve a hodnota *CHGOWN indikuje prenos vlastníctva na ďalší profil.

  Hodnota newOwner uvádza profil, na ktorý sa presúva vlastníctvo. Táto hodnota sa vyžaduje, keď je ownObjOpt nastavené na *CHGOWN.

  Nasledujú príklady hodnoty ovládacieho prvku:
  - *NODLT: uvádza, že profil nemožno vymazať, ak vlastní objekty.
  - *CHGOWN SMITH: uvádza prenos vlastníctva ľubovoľných objektov na užívateľský profil SMITH.
- Identifikátor objektu (OID) je definovaný v ldap.h as LDAP_OS400_OWNOBJOPT_CONTROL_OID.
  - os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

    Kontrolná hodnota je definovaná ako reťazec v tomto formáte:

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

    Hodnota pgpOpt uvádza akciu, ktorú treba vykonať, ak je vymazávaný profil primárnou skupinou pre ktorékoľvek objekty. Ak je uvedené *CHGPGP, musí byť uvedené aj newPgp. Hodnota newPgp uvádza názov profilu primárnej skupiny alebo *NONE. Ak sa zadá nový profil primárnej skupiny, môže sa zadať aj hodnota newPgpAut. Hodnota newPgpAut uvádza oprávnenie na objekty, ktoré dostala nová primárna skupina.

  Nasledujú príklady hodnoty ovládacieho prvku:
  - *NOCHG: uvádza, že profil nemožno vymazať, ak ide o primárnu skupinu pre ľubovoľné objekty.
  - *CHGPGP *NONE: uvádza odstránenie primárnej skupiny pre dané objekty.
  - *CHGPGP SMITH *USE: uvádza zmeniť primárnu skupinu na užívateľský profil SMITH a udeliť primárnej skupine oprávnenie *USE.

  Ak nie je na vymazávaní uvedený ani jeden z týchto ovládacích prvkov, namiesto nich sa použijú momentálne platné štandardné hodnoty pre príkaz QSYS/DLTUSRPRF.

ModRDN

Nemôžete premenovať projektované užívateľské profily, pretože operačný systém to nepodporuje.

API importu a exportu

API QgldImportLdif a QgldExportLdif nepodporujú import alebo export údajov v rámci projektovaného pozadia systému.

DN pripojenia administrátora a repliky

Projektovaný užívateľský profil môžete uviesť ako DN pripojenia nakonfigurovaného administrátora alebo repliky. Použije sa heslo užívateľského profilu. Projektované užívateľské profily sa môžu stať administrátormi LDAP, ak majú oprávnenie na identifikátor funkcie administrátora adresárového servera (QIBM_DIRSRV_ADMIN). Prístup administrátora môže byť udelený viacerým užívateľským profilom.

Ďalšie informácie nájdete v časti “Administratívny prístup” na strane 54.

Užívateľská projektovaná schéma

Triedy a atribúty objektov z projektovaného pozadia možno nájsť v serverovej schéme. Názvy atribútov LDAP sú vo formáte os400–*nnn*, kde *nnn* je zvyčajne kľúčové slovo atribútu v príkazoch užívateľského profilu. Napríklad atribút os400-usrcls zodpovedá parametru USRCLS príkazu CRTUSRPRF. Hodnoty atribútov korešpondujú s hodnotami parametrov, ktoré akceptujú príkazy CRTUSRPRF a CHGUSRPRF, alebo hodnotami zobrazovanými pri zobrazovaní užívateľského profilu. Použite webový administratívny nástroj alebo inú aplikáciu na zobrazenie definícií triedy objektov os400-usrprf a priradených atribútov os400-xxx.

Podpora žurnálovania Adresárový server a i5/OS

Adresárový server používa podporu databáz i5/OS na ukladanie informácií o adresároch. Adresárový server používa riadenie potvrdenia na ukladanie položiek adresára v databáze. To vyžaduje podporu žurnálovania i5/OS.

Keď sa server alebo importovací nástroj LDIF spustí po prvýkrát, zostavia sa nasledujúce položky:

- Žurnál
- Prijímač žurnálov
- Všetky databázové tabuľky, ktoré sú na začiatku potrebné

Žurnál QSQJRN sa tvorí v knižnici databázy, ktorú ste pri konfigurácii zadali. Prijímač žurnálov QSQJRN0001 je pôvodne vytvorený v knižnici databázy, ktorú ste pri konfigurácii zadali.

Vaše prostredie, veľkosť a štruktúra adresárov alebo stratégia ukladania a obnovovania môže predpisovať niektoré rozdiely od predvolených hodnôt, vrátane toho, ako sú tieto objekty riadené či použitého prahu pre veľkosť. Ak je to potrebné, môžete zmeniť parametre príkazov žurnálovania. Žurnálovanie LDAP je štandardne nastavené na vymazávanie starých prijímačov. Ak je nakonfigurovaný protokol zmien a chcete si ponechať starých príjemcov, v príkazovom riadku vykonajte:

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

Ak je nakonfigurovaný protokol zmien, môžete vymazať jeho staré žurnálové prijímače nasledujúcim príkazom:

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

Informácie o príkazoch žurnalizácie nájdete v časti “Príkazy OS/400” v téme Programovanie.

Jedinečné atribúty

Funkcia jedinečných atribútov zabezpečí, že zadané atribúty vždy budú mať v adresári jedinečné hodnoty. Tieto atribúty možno zadávať len v dvoch položkách, cn=uniqueattribute,cn=localhost a cn=uniqueattribute,cn=IBMpolicies. Výsledky vyhľadávania pre jedinečné atribúty sú jedinečné len pre databázu tohto servera. Výsledky vyhľadávania obsahujúce výsledky z odvolávok nemusia byť jedinečné.

Poznámka: Binárne atribúty, prevádzkové atribúty, konfiguračné atribúty a atribút triedy objektu nemôžu byť stanovené ako jedinečné.

Nie všetky atribúty je možné zadávať ako jedinečné. Ak chcete určiť, že atribút možno zadať ako jedinečný, použite príkaz ldapexop:

- Pre atribúty, ktoré môžu byť jedinečné: ldapexop -op getattributes -attrType unique -matches true
- Pre atribúty, ktoré nemôžu byť jedinečné: ldapexop -op getattributes -attrType unique -matches false

Bližšie informácie o jedinečných atribútoch nájdete v časti “Riadenie jedinečných atribútov” na strane 120.

Prevádzkové atribúty

Existuje niekoľko atribútov, ktoré majú špeciálny význam pre adresárový server. Sú známe ako prevádzkové atribúty. Sú to atribúty, ktoré udržiava server a buď odzrkadľujú informácie o položkách, ktoré server manažuje, alebo ovplyvňujú fungovanie servera. Tieto atribúty majú zvláštne charakteristiky:

- Atribúty nie sú vracané operáciou vyhľadávania pokiaľ nie sú špecificky požiadané (podľa mena) v požiadavke na hľadanie
- Tieto atribúty nie sú súčasťou žiadnej triedy objektov. Server riadi, ktoré položky majú tieto atribúty.

Nasledujúca množina prevádzkových atribútov sú niektoré prevádzkové atribúty, ktoré podporuje adresárový server:

- creatorsName, createTimestamp, modifiersName, modifyTimestamp sa nachádzajú na každej položke. Tieto atribúty ukazujú DN spojenia a čas, kedy bola položka prvýkrát vytvorená alebo poslednýkrát modifikovaná. Tieto atribúty môžete použiť vo vyhľadávacích filtroch, napríklad na nájdenie všetkých položiek modifikovaných po určenom čase. Tieto atribúty nemôžu byť modifikované žiadnym užívateľom. Tieto atribúty sa replikujú na servery spotrebiteľov a importujú a exportujú sa v súboroch LDIF.
- ibm-entryuuid. Prítomný na každej položke, ktorá je vytvorená pokiaľ je server vo V5R3 alebo novšej. Tento atribút je unikátny reťazcový identifikátor, priradený každej položke serverom pri vytváraní položky. Je užitočný pre aplikácie, ktoré potrebujú rozoznávať medzi identicky nazvanými položkami na rôznych serveroch. Tento atribút používa algoritmus DCE UUID na generovanie ID, ktoré je unikátne medzi všetkými položkami na všetkých serveroch, pomocou časovej značky, adresy adaptéra a ostatných informácií.
- entryowner, ownersource, ownerpropagate, aclentry, aclsource, aclpropagate, ibm-filteracl, ibm-filteraclinherit, ibm-effectiveAcl. Ďalšie informácie nájdete v časti “Zoznamy riadenia prístupu” na strane 55.
- hasSubordinates. Prítomný na každej položke a má hodnotu TRUE, ak má položka podriadené položky.
- numSubordinates. Prítomný na každej položke a obsahuje počet položiek, ktoré sú deťmi tejto položky.
- pwdChangedTime, pwdAccountLockedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdReset, pwdHistory. Ďalšie informácie nájdete v časti “Politika hesiel” na strane 66.
- subschemasubentry - Prítomný na každej položke a identifikuje umiestnenie schémy pre tú časť stromu. Je to užitočné pre servery s viacerými schémami, ak chcete nájsť schému, ktorú môžete použiť v tejto často stromu.

Kompletný zoznam prevádzkových atribútov získate pomocou nasledovnej rozšírenej operácie: ldapexop -op getattributes -attrType operational -matches true.

Pamäte cache servera

Pamäte cache LDAP sú rýchle vyrovnávacie pamäte v pamäti, ktoré sa používajú na ukladanie informácií o LDAP, ako sú dotazy, odpovede a autentifikácia užívateľov, pre budúce použitie. Naladenie pamätí cache LDAP je kľúčové na zlepšenie výkonu.

Vyhľadávanie LDAP, ktoré využije prístup k pamäti cache LDAP, môže byť rýchlejšie ako vyhľadávanie, ktoré vyžaduje pripojenie na DB2, aj keď sú informácie uložené v pamäti cache v DB2. Z tohto dôvodu vyladenie pamätí cache LDAP môže zlepšiť výkon, keďže sa vyhne volaniam do databázy. Pamäte cache LDAP sú zvlášť užitočné pre aplikácie, ktoré často obnovujú opakujúce sa informácie uložené v pamäti cache.

V nasledovných častiach sa prejednávajú pamäte cache LDAP a demonštrujú, ako určovať a nastavovať tie najlepšie nastavenia pamäte cache pre váš systém.

- "Pamäť cache atribútov"
- "Pamäť cache filtrov" na strane 81
- "Pamäť cache položiek" na strane 81
- "Pamäť cache pre ACL" na strane 81

Informácie o konfigurovaní pamätí cache nájdete v časti "Úprava nastavení výkonu" na strane 124.

Pamäť cache atribútov

Pamäť cache atribútov má výhodu, že je schopná rozpoznať filtre v pamäti, nielen v databáze. Rovnako má výhodu, že sa aktualizuje vždy, keď sa vykoná operácia LDAP add, delete, modify alebo modrdn.

Pri rozhodovaní, ktoré atribúty chcete uložiť do pamäte, musíte vziať do úvahy:

- Množstvo pamäte, ktoré je k dispozícii pre server
- Veľkosť adresára
- Typy vyhľadávacích filtrov, ktoré aplikácia zvyčajne používa

Poznámka: Manažér pamäte cache rozpoznáva nasledovné typy jednoduchých filtrov: filtre presnej zhody a filtre prítomnosti. Dokáže rozpoznať komplexné filtre, ktoré sú konjunktívne alebo disjunktívne, a podfiltre musia byť presnej zhody konjunktívne prítomnostné alebo disjunktívne.

Nie všetky atribúty je možné pridávať do pamäte cache atribútov. Ak chcete určiť, či nejaký atribút je možné pridať do pamäte cache, použite príkaz ldapexop:

- Pre atribúty, ktoré možno pridať: `ldapexop -op getattributes -attrType attribute_cache -matches true`
- Pre atribúty, ktoré nemožno pridať: `ldapexop -op getattributes -attrType attribute_cache -matches false`

Ukladanie atribútov do pamäte cache možno nakonfigurovať dvoma spôsobmi: manuálne alebo automaticky. Ak chcete manuálne nakonfigurovať ukladanie atribútov do pamäte cache, administrátor by mal vykonať vyhľadávania cn=monitor, aby porozumel, ako nastaviť ukladanie atribútov do pamäte cache čo najefektívnejšie. Tieto vyhľadávania vrátia výpis aktuálnych informácií, ktoré atribúty sú v pamäti cache, množstvo pamäte využívanej každou pamäťou cache atribútov, množstvo pamäte využívanej ukladaním atribútov do pamäte cache, množstvo pamäte nakonfigurovanej pre ukladanie atribútov do pamäte cache a zoznam atribútov, najčastejšie používaných vo vyhľadávacích filtroch. Pomocou týchto informácií môže administrátor zmeniť množstvo pamäte, ktoré je povolená na používanie pre ukladanie atribútov do pamäte cache, ako aj to, ktoré atribúty sa majú ukladať do pamäte cache podľa potreby na základe nových vyhľadávaní cn=monitor.

Alebo administrátor môže nakonfigurovať automatické ukladanie atribútov do pamäte cache. Keď je povolené automatické ukladanie atribútov do pamäte cache, adresárový server vysleduje kombináciu atribútov, ktoré by mohlo byť najužitočnejšie uložiť do pamäti cache v rámci pamäťových ohraničení definovaných administrátorom. Potom aktualizuje ukladanie atribútov do pamäte cache v čase a časovom intervale nakonfigurovanom administrátorom.

Pamäť cache filtrov

Keď klient vydá dotaz na údaje a tento dotaz nie je možné vyriešiť v pamäti manažérom pamäti cache atribútov, dotaz prejde do pamäte cache filtrov. Táto pamäť cache obsahuje ID položiek uložených do pamäte cache. Sú dve udalosti, ktoré sa môžu prihodiť, keď príde dotaz do pamäte cache filtrov:

- **ID, ktoré sa zhodujú s nastaveniami filtra použitých v dotaze, sa nachádzajú v pamäte cache filtrov.** V takomto prípade sa zoznam ID zhodných položiek odošle do pamäte cache.
- **ID zhodných položiek sa neukladá do pamäte cache v pamäti cache filtrov.** V takomto prípade musí dotaz pri vyhľadávaní požadovaných údajov použiť prístup do DB2.

Na určenie, aká veľká by vaša pamäť cache mala byť, spustite pracovné zaťaženie s pamäťou cache nastavenou na iné hodnoty a odmerajte rozdiely v počte operácií za sekundu.

Konfiguračná premenná ohraničenia obídenia pamäte cache filtrov obmedzuje počet položiek, ktoré je možné pridať do pamäte cache filtrov. Napríklad, ak premenná ohraničenia obídenia je nastavená na hodnotu 1000, vyhľadávacie filtre, ktoré nájdu viac ako 1000 položiek, sa nepridajú do pamäte cache filtrov. Takto sa zabráni tomu, aby veľké neznáme vyhľadávania prepisovali užitočné položky pamäte cache. Ak chcete určiť najlepšieho ohraničenia obídenia pamäte cache filtrov pre vaše pracovné zaťaženie, opakovane spúšťajte pracovné zaťaženie a merajte priepustnosť.

Pamäť cache položiek

Pamäť cache položiek obsahuje údaje položiek uložené v pamäti cache. ID položiek sa odosielajú do pamäte cache položiek. Ak položky, ktoré sa zhodujú s ID položiek sú v pamäti cache položiek, výsledky sa vrátia klientovi. Ak pamäť cache položiek neobsahuje položky, ktoré zodpovedajú ID položiek, dotaz pri vyhľadávaní zhodných položiek prejde do DB2.

Na určenie, aká veľká by vaša pamäť cache položiek mala byť, spustite pracovné zaťaženie s pamäťou cache položiek nastavenou na iné veľkosti a odmerajte rozdiely v počte operácií za sekundu.

Pamäť cache pre ACL

Pamäť cache pre ACL obsahuje informácie o riadení prístupu, napríklad vlastníka položky a oprávnenia položky pre práve pristupované položky. Táto pamäť cache sa používa na zlepšenie výkonu pri vyhodnocovaní prístupu na pridávanie, mazanie, úpravu alebo vyhľadávanie položiek. Ak sa položka nenájde v pamäti cache pre ACL, informácie o riadení prístupu sa získajú z databázy. Ak chcete určiť vhodnú veľkosť pamäte cache pre ACL, odmerajte výkon servera pomocou typického pracovného zaťaženia s rôznymi veľkosťami pamäte cache pre ACL.

Kontroly a rozšírené operácie

Kontroly

Kontroly poskytujú dodatočné informácie serveru na riadenie, ako interpretujú danú požiadavku. Napríklad kontrola delete subtree môže byť špecifikovaná na LDAP požiadavke vymazávania, indikujúca, že server by mal vymazať položku a všetky podriadené položky, a nielen vymazať špecifikovanú položku. Kontrola sa skladá z troch častí:

- Typ kontroly, čo je OID identifikujúci kontrolu.
- Indikátor kritickosti, ktorý špecifikuje ako by sa mal server správať, ak nepodporuje túto kontrolu. Je to boolovská hodnota. FALSE znamená, že kontrola nie je kritická a server by ju mal ignorovať, ak ju nepodporuje. TRUE znamená, že kontrola je kritická a celá požiadavka by mala byť neúspešná (s nepodporovanou chybou kritického rozšírenia), ak server nemôže uznať túto kontrolu.
- Voliteľná kontrolná hodnota, ktorá obsahuje iné informácie špecifické pre kontrolu. Obsah tejto kontrolnej hodnoty je špecifikovaný pomocou notácie ASN.1. Samotná hodnota je BER kódovanie kontrolných údajov.

Rozšírené operácie

Rozšírené operácie sa používajú na spúšťanie dodatočných operácií okrem základných operácií LDAP. Napríklad môžu byť definované na zoskupenie viacerých operácií do jednej transakcie. Rozšírená operácia sa skladá z:

- Názvu požiadavky, OID ktoré identifikuje konkrétnu operáciu.
- Voliteľnej hodnoty požiadavky, ktorá obsahuje ostatné informácie, špecifické pre túto operáciu. Obsah hodnoty požiadavky je špecifikovaný pomocou notácie ASN.1. Samotná hodnota je BER kódovanie údajov požiadavky.

Rozšírené operácie majú zvyčajne rozšírenú odpoveď. Odpoveď sa skladá z:

- Komponentov štandardného výsledku LDAP (chybový kód, príslušné DN a chybová správa)
- Názvu odpovede, OID ktoré identifikuje typ odpovede
- Voliteľnej hodnoty, ktorá obsahuje ostatné informácie špecifické pre odpoveď. Obsah hodnoty odpovede je špecifikovaný pomocou notácie ASN.1. Samotná hodnota je BER kódovanie údajov odpovede.

Kompletný zoznam ovládacích prvkov a rozšírených operácií, ako aj ich príslušných identifikátorov objektov (OID) a popisov, nájdete v časti “Identifikátory objektov (OID)” na strane 254.

Kapitola 5. Začíname s adresárovým serverom

Adresárový server sa automaticky nainštaluje, keď nainštalujete systém i5/OS. Adresárový server obsahuje štandardnú konfiguráciu. Keď chcete začať používať adresárový server, urobte toto:

1. Ak inštalujete V5R4 a na predchádzajúcom vydaní ste používali adresárový server, pozrite si úvahy o migrácii. Ďalšie informácie nájdete v časti "Informácie o migrácii".
2. Naplánujte svoj adresárový server. Ďalšie informácie nájdete v časti "Plánovanie vášho adresárového servera" na strane 87.
3. Keď chcete prispôsobiť nastavenia adresárového servera, spustite Sprievodcu konfiguráciou adresárového servera. Ďalšie informácie nájdete v časti "Konfigurácia adresárového servera" na strane 88.
4. Spustite server. Ďalšie informácie obsahuje časť "Spustenie/zastavenie adresárového servera" na strane 108
5. Použite webový administratívny nástroj na vytvorenie alebo editovanie adresárov LDAP. Ďalšie informácie nájdete v časti "Webová administrácia" na strane 95.
6. Pozrite si informácie v časti Kapitola 7, "Správa adresárového servera", na strane 107, kde nájdete viac informácií o tom, ako vykonať rôzne úlohy adresárového servera.

Informácie o migrácii

Adresárový server sa automaticky nainštaluje, keď nainštalujete systém i5/OS. Keď je adresárový server prvýkrát spustený, automaticky migruje existujúcu konfiguráciu a údaje. To môže spôsobiť dlhé oneskorenie pred prvým spustením servera.

Poznámka: Migrácia súborov konfigurácie a schém sa vykoná počas inštalácie a prvého spustenia servera. Po dokončení prvého spustenia servera, ak sa súbory konfigurácie a schém v adresári /qibm/userdata/os400/dirsrv obnovia zo zálohy predchádzajúceho vydania, schéma a konfigurácia pre nové vydanie sa prekryje súbormi predchádzajúceho vydania, ktoré sa nebudú znova migrovať. Obnova schémy a konfigurácie predchádzajúceho vydania po tom, ako sa vykonala migrácia, môže spôsobiť, že server sa nespustí, prípadne nastanú iné nepredvídateľné chyby. Ak je potrebná záloha konfigurácie a schémy servera, tieto údaje sa musia uložiť po úspešnom spustení servera.

Ak máte adresárový server pracujúci na V5R3 alebo V5R21, pozrite časť "Migrácia na V5R4 z V5R3 alebo V5R2".

Ak máte adresárový server pracujúci na V4R4, V4R5 alebo V5R1, môžete migrovať údaje na V5R4. Ďalšie informácie nájdete v časti "Migrovanie údajov z V4R4 ,V4R5 alebo V5R1 na V5R4" na strane 84.

Ak máte sieť replikačných serverov, pozrite si "Migrovanie siete replikačných serverov" na strane 85, kde nájdete viac informácií.

Ak používate Kerberos, pozrite si "Zmena názvu služby Kerberos" na strane 87.

Migrácia na V5R4 z V5R3 alebo V5R2

Systém i5/OS V5R4 uvádza nové funkcie a schopnosti pre Adresárový server. Tieto zmeny sa týkajú tak adresárového servera LDAP, ako aj grafického užívateľského prostredia (GUI) iSeries Navigator. Ak chcete využiť nové funkcie GUI, musíte nainštalovať iSeries Navigator na PC, ktoré môže komunikovať cez TCP/IP s vaším serverom iSeries. iSeries Navigator je komponent iSeries Access for Windows. Ak máte nainštalovanú staršiu verziu iSeries Navigator, mali vy ste vykonať rozšírenie na V5R4.

Systém i5/OS V5R4 podporuje priame rozšírenia z V5R2 a V5R3. Keď vykonáte rozšírenie na i5/OS V5R4, údaje adresára LDAP aj súbory schém adresárov sa automaticky migrujú tak, aby vyhovovali formátom V5R4.

Keď vykonáte rozšírenie na i5/OS V5R4, mali by ste vedieť o určitých problémoch pri migrácii:

- Keď vykonáte rozšírenie na V5R4, Adresárový server automaticky migruje vaše súbory schém na V5R4 a vymaže staré súbory schém. Ak ste však vymazali alebo premenovali súbory schém, adresárový server ich nemôže migrovať. Môžete dostať chybu, alebo Adresárový server môže predpokladať, že súbory už boli migrované.
- Po vykonaní rozšírenia na V5R4 by ste mali pred importovaním nových údajov najskôr raz spustiť server za účelom migrácie existujúcich údajov. Ak sa pokúsite importovať údaje pred týmto jediným spustením servera a nemáte dostatočné oprávnenie, importovanie by mohlo zlyhať. Adresárový server migruje údaje adresára na formát V5R4 pri vašom prvom spustení servera alebo importovaní súboru LDIF. Rátajte s tým, že chvíľu bude trvať, kým sa migrácia ukončí.
- Po migrácii sa bude adresárový server LDAP automaticky spúšťať, keď sa spustí TCP/IP. Ak nechcete, aby sa adresárový server spúšťal automaticky, použite iSeries Navigator na zmenu nastavenia.

Migrovanie údajov z V4R4 ,V4R5 alebo V5R1 na V5R4

Systém i5/OS V5R4 nepodporuje priame rozšírenia z V4R4, V4R5 alebo V5R1. Ak chcete migrovať tieto vydania na V5R4, môžete použiť niektorý z nasledovných postupov:

- "Rozšírenie z V4R4, V4R5 alebo V5R1 na medzivydanie"
- "Uloženie knižnice databáz a inštalácia V5R4"

Keď vykonáte rozšírenie z V4R4 na akékoľvek novšie vydanie, mali by ste vedieť o nasledovných problémoch:

- Vydania adresárového servera V4R4 a staršie pri vytváraní záznamov s časovou značkou nebrali do úvahy časové pásma. Od vydania V4R5 sa používa časové pásmo pri všetkých pridaných a zmenených údajoch adresára. Preto, ak prevádzate údaje z V4R4 alebo staršej verzie, adresárový server upraví existujúce atribúty createtimestamp a modifytimestamp, aby odrážali správnu časovú zónu. Zrealizuje to tak, že odpočíta časové pásmo, ktoré je práve nastavené v systéme iSeries od časových značiek, ktoré sú uložené v adresári. Všimnite si, že ak aktuálna časová zóna nie je rovnaká ako časová zóna, ktorá bola aktívna, keď sa položky pôvodne vytvárali alebo modifikovali, hodnoty novej časovej značky nebudú odrážať pôvodnú časovú zónu.
- Ak prevádzate údaje z verzie V4R4 alebo staršej, adresárové údaje budú vyžadovať približne dvakrát viac úložného priestoru ako vyžadovali predtým. Dôvodom je, že vo V4R4 alebo starších verziách adresárového servera podporovala len znakovú sadu IA5 a ukladala údaje v ccsid 37 (jednobajtový formát). Adresárový server podporuje úplnú znakovú sadu ISO 10646. Po vykonaní prechodu na novú verziu by ste mali raz spustiť svoj server, aby sa migrovali existujúce údaje pred importovaním nových údajov. Ak sa pokúsite importovať údaje pred týmto jediným spustením servera a nemáte dostatočné oprávnenie, importovanie by mohlo zlyhať.

Rozšírenie z V4R4, V4R5 alebo V5R1 na medzivydanie

Hoci nie sú podporované rozšírenia z V4R4, V4R5 a V5R1 na V5R4, podporované sú nasledovné rozšírenia:

- V4R4 a V4R5 rozšírené na V5R1
- V4R5 a V5R1 rozšírené na V5R2
- V5R1 a V5R2 rozšírené na V5R3
- V5R2 a V5R3 rozšírené na V5R4

Jedným zo spôsobov migrácie servera Adresárový server je rozšírenie na medzivydanie (V5R2 alebo V5R3), potom na V5R4. Podrobné informácie o procedúrach inštalácie i5/OS nájdete v dokumente *Software Installation*  . Migráciu vykonáte podľa nasledovných krokov. Zmeny schémy by sa mali migrovať automaticky. Po každej inštalácii skontrolujte, či sú prítomné zmeny schémy.

1. Pri V4R4, nainštalujte V5R1. Potom nainštalujte V5R3.
2. Pri V4R5, nainštalujte V5R1 alebo V5R2. Ak inštalujete na V5R1, potom musíte inštalovať na V5R2 alebo V5R3.
3. Pri V5R1, nainštalujte V5R3.
4. Keď ste pri V5R2 alebo V5R3, nainštalujte V5R4.
5. Spustite adresárový server, ak nie je ešte spustený.

Uloženie knižnice databáz a inštalácia V5R4

Server Adresárový server môžete migrovať uložením knižnice databáz, ktoré Adresárový server používa na V4R4 alebo V4R5, potom jej obnovením po inštalácii V5R4. Týmto ušetríte krok inštalácie medzivydania. Nastavenia servera však

nie sú migrované, takže musíte prekonfigurovať nastavenia servera. Podrobné informácie o procedúrach inštalácie i5/OS nájdete v dokumente *Software Installation* . Pri migrácii postupujte podľa nasledujúcich krokov:

1. Zaznamenajte si všetky zmeny, ktoré ste vykonali v súboroch schém do adresára /QIBM/UserData/OS400/DirSrv. Súbory schém nie sú migrované automaticky, takže ak chcete zachovať svoje zmeny, musíte ich znovu manuálne implementovať. Ak boli vykonané aktualizácie schém pomocou súborov LDIF v spojení s pomocným programom ldapmodify, nájdite tieto súbory, aby ste ich mohli použiť po rozbehnutí servera na novom vydaní. Nástroj na správu adresárov alebo Webový administratívny nástroj (bežiaci na inom systéme V5R4) možno použiť na definície jednotlivých typov atribútov a tried objektov. Ak vaše zmeny spočívajú len v pridaní nových typov atribútov a tried objektov, vytvorte kópiu súboru /qibm/userdata/os400/dirsrv/v3.modifiedschema. Tento súbor môžete použiť na zostavenie súboru LDIF obsahujúceho aktualizácie schém. Pozrite “Schéma” na strane 15, kde nájdete bližšie informácie.
2. Zaznamenajte so všetky konfiguračné nastavenia vo vlastnostiach adresárového servera vrátane názvu databázovej knižnice.
3. Uložte databázovú knižnicu, ktorá je špecifikovaná v konfigurácii adresárového servera. Ak ste nakonfigurovali protokol zmien, budete tiež musieť uložiť knižnicu QUSRDIRCL.
4. Zaznamenajte si publikovanú konfiguráciu. Publikovanú konfiguráciu, s výnimkou informácií o hesle, možno prezerať pomocou aplikácie iSeries Navigator výberom položky **Vlastnosti** pre systém kliknutím na kartu **Adresárové služby**.
5. Nainštalujte i5/OS V5R4 na systém.
6. Použite EZ-Setup na konfiguráciu adresárového servera.
7. Obnovte knižnicu databázy, ktorú ste uložili v kroku 3. Ak ste uložili knižnicu QUSRDIRCL v kroku 3, teraz ju obnovte.
8. Použite iSeries Navigator na rekonfiguráciu adresárového servera. Špecifikujte databázovú knižnicu, ktorá bola predtým nakonfigurovaná a ktorá bola uložená a obnovená v predchádzajúcom kroku
9. Na konfiguráciu publikovania použite iSeries Navigator.
10. Reštartujte adresárový server.
11. Pomocou webového aministratívneho nástroja zmeňte súbory schém pre všetky zmeny užívateľov, ktoré ste zaznamenali v kroku 1.

Migrovanie siete replikačných serverov

Hlavný server pri svojom prvom spustení migruje informácie do adresára, ktorý riadi replikáciu. Položky s objectclass replicaObject pod cn=localhost sa nahrádzajú položkami, ktoré používa nový model replikácie (viac informácií nájdete v časti “Replikácia” na strane 36). Hlavný server sa konfiguruje tak, aby replikoval všetky prípony v tomto adresári. Položky dohody sa vytvárajú pomocou atribútu ibm-replicationOnHold, nastaveného na hodnotu true. Toto umožňuje, aby sa pre repliku nazhromaždili aktualizácie, vykonané na hlavnom serveri, kým bude táto replika hotová.

O týchto položkách sa hovorí ako o replikačnej topológii. Nový hlavný server možno použiť s replikami používajúcimi predchádzajúce verzie. Údaje týkajúce sa nových funkcií nebudú replikované na servery zadanej úrovne. Položky replikačnej topológie je treba po migrovaní replikačného servera vyexportovať z hlavného servera a pridať ich do každej repliky. Na vyexportovanie týchto položiek použite nástroj príkazového riadka Qshell “ldapsearch” na strane 200 a výstup uložte do súboru. Príkaz na vyhľadávanie vyzerá asi takto:

```
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
```

Tento príkaz vytvára v aktuálnom pracovnom adresári výstupný súbor LDIF s názvom replication.topology.ldif. Uvedený súbor obsahuje len nové položky.

Poznámka: Neprirađujte nasledujúce prípony:

- cn=changelog

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

Priraďujte len užívateľom vytvorené prípony.

Opakujte tento príkaz pre položku každej prípony na hlavnom serveri, ale “>” vymeňte za “>>”, aby sa dali pridať údaje do výstupného súboru pre neskoršie vyhľadávania. Keď je súbor úplný, skopírujte ho na replikačné servery.

Súbor pridajte na replikačné servery až po ich úspešnej migrácii; nepridávajte ho na servery, na ktorých bežia staršie verzie adresárového servera. Server musíte pred pridaním súboru spustiť a zastaviť.

Na spustenie servera použite voľbu **Štart** v aplikácii iSeries Navigator. Ďalšie informácie nájdete v časti “Spustenie/zastavenie adresárového servera” na strane 108.

Na zastavenie servera použite voľbu **Stop** v aplikácii iSeries Navigator. Ďalšie informácie nájdete v časti “Spustenie/zastavenie adresárového servera” na strane 108.

Keď pridávate súbor na replikačný server, presvedčte sa, či tento server nie je spustený. Ak chcete pridať údaje, použite voľbu **Importovať súbor** v aplikácii iSeries Navigator.

Po zavedení položiek replikačnej topológie spustite replikačný server a pokračujte v replikácii. V replikácii môžete pokračovať jedným z nasledujúcich spôsobov:

- Na hlavnom serveri vo webovom administratívnom nástroji použite **Manažovanie frontov v manažmente replikácie**.
- Použite pomocný program príkazového riadka **ldapexop**. Napríklad:

  ```
  ldapexop -h master-server-host-name -p master-server-port \
   -D master-server-admin-DN -w master-server-admin-password \
   -op controlrepl -action resume -ra replica-agreement-DN
  ```

  Tento príkaz pokračuje v replikácii v prípade servera, zadefinovaného v položke so špecifikovaným DN.

V súbore replication.topology.ldif zistíte, ktoré DN dohody repliky zodpovedá replikačnému serveru. Hlavný server zaprotokoluje správu, že sa spustila replikácia tejto repliky a varovanie, že ID replikačného servera v dohode sa nezhoduje s ID tohto replikačného servera. Ak chcete aktualizovať dohodu repliky, aby sa použilo správne ID servera, použite **Manažment replikácie** vo webovom administratívnom nástroji alebo nástroj príkazového riadka **ldapmodify**. Napríklad:

```
ldapmodify -c -h názov-hostiteľa-hlavného-servera -p port-hlavného-servera \
 -D master-server-admin-DN -w master-server-admin-password
dn: replica-agreement-DN
changetype: modify
nahradiť: ibm-replicaConsumerID
ibm-replicaConsumerID: replica-server-ID
```

Tieto príkazy môžete zadať priamo v príkazovom riadku, alebo ich môžete uložiť do súboru LDIF a zadávať ich do príkazového riadka s voľbou **-i** *súbor*. Na zastavenie príkazu použite **Ukončiť predchádzajúcu požiadavku**.

Migrácia tejto repliky je dokončená.

Ak chcete ďalej používať repliku, na ktorej beží staršia verzia, je potrebné pokračovať v replikácii použitím nástroja príkazového riadka **ldapexop** alebo **Manažment replikácie** vo webovom administratívnom nástroji pre túto repliku. Ak sa replika, na ktorej beží staršia verzia, migruje neskôr, použite nástroj príkazového riadka **ldapdiff** a zosynchronizujte adresárové údaje. Tým zabezpečíte, že položky alebo atribúty, ktoré neboli replikované, sa na tejto replike zaktualizujú.

Zmena názvu služby Kerberos

Od V5R3 sa zmenil názov služby používaný adresárovým serverom a klientske rozhrania API pre autentifikáciu GSSAPI (Kerberos). Táto zmena nie je kompatibilná s názvom služby, používaným pred V5R3 (V5R2M0 PTF 5722SS1-SI08487 obsahuje tú istú zmenu).

Pred V5R3, Adresárový server a klientske rozhrania API používali názov služby vo forme LDAP/názov-hostiteľa-dns@Kerberos-realm, keď sa na autentifikáciu používal mechanizmus GSSAPI (Kerberos). Tento názov nevyhovuje štandardom, definujúcim autentifikáciu GSSAPI, ktoré stanovujú, že názov principála má začínať malými písmenami ″ldap″. Následkom toho Adresárový server aj klientske rozhrania API nemuseli fungovať v súčinnosti s inými produktmi predajcu. Toto je pravda najmä v prípade, ak má KDC (Kerberos key distribution center) názvy principálov, zohľadňujúce veľkosť písmen. Poskytovateľ servisu LDAP pre JNDI, všeobecne používané API klienta Java LDAP, je príkladom, ktorý je súčasťou operačného systému používajúceho správny názov služby.

V V5R3M0 a zmenil názov služby tak, aby vyhovoval štandardom. Toto však predstavuje jej vlastné problémy s kompatibilitou.

- Adresárový server, nakonfigurovaný na používanie autentifikácie GSSAPI nespustí inštaláciu tohto vydania. Dôvodom je, že súbor obsahujúci kľúče, používaný týmto serverom, má oprávnenia, ktoré používajú starý názov služby (LDAP/mysys.ibm.com@IBM.COM), kým server hľadá oprávnenia, ktoré používajú nový názov služby (ldap/mysys.ibm.com@IBM.COM).
- Adresárový server alebo aplikácia LDAP používajúce rozhrania API LDAP na V5R3M0 by nemusela byť schopná autentifikácie so staršími servermi alebo klientmi OS/400. Na odstránenie tohto problému musíte postupovať nasledovne:
  1. Ak KDC používa názvy principálov, zohľadňujúce veľkosť písmen, vytvorte konto pomocou správneho názvu služby (ldap/mysys.ibm.com@IBM.COM).
  2. Aktualizujte súbor tabuľky kľúčov pomocou Adresárového servera, aby obsahoval poverenia pre nový názov služby. Staré oprávnenia budete pravdepodobne chcieť vymazať. Na aktualizáciu súboru obsahujúceho kľúče môžete použiť pomocný program Qshell. Adresárový server štandardne používa súbor /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab. Sprievodca Služba autentifikácie siete V5R3M0 (Kerberos) v aplikácii iSeries Navigator tiež vytvorí položky tabuľky kľúčov pomocou nového názvu služby.
  3. Aktualizujte systémy V5R2M0 OS/400, kde sa používa GSSAPI aplikovaním PTF 5722SS1-SI08487.

Alternatívne sa môžete rozhodnúť, že adresárový server a klientske API budú naďalej používať starý názov služby. Toto môže byť vhodné v prípade, že používate autentifikáciu Kerberos v zmiešanej sieti systémov, ktoré bežia s a bez PTF. Aby ste to mohli urobiť, uveďte premennú prostredia LDAP_KRB_SERVICE_NAME. Môžete ju uviesť pre celý systém (vyžaduje sa uviesť názov služby pre server) použitím nasledujúceho príkazu:

```
ADDENVVAR ENVVAR(LDAP_KRB_SERVICE_NAME)
```

alebo v QSH (na ovplyvnenie pomocných programov LDAP, spustených z tejto relácie QSH):

```
export LDAP_KRB_SERVICE_NAME=1
```

Plánovanie vášho adresárového servera

Kým nainštalujete adresárový server a začnete konfigurovať svoj adresár LDAP, mali by ste pár minút venovať naplánovaniu adresára. Mali by ste zvážiť tieto faktory:

- **Organizáciu adresára**. Naplánujte si štruktúru vášho adresára a určite, ktoré prípony a atribúty bude váš server vyžadovať. Bližšie informácie nájdete v časti “Odporúčané postupy pre štruktúru adresárov” na strane 94, “Adresáre” na strane 7, “Prípona (názvový kontext)” na strane 14 a “Atribúty” na strane 19.
- **Rozhodnite o veľkosti vášho adresára**. Potom budete môcť odhadnúť, koľko pamäte potrebujete. Veľkosť adresára závisí od:
  - Počtu atribútov v schéme serverov.
  - Počtu položiek na serveri.
  - Typu informácií, ktoré na server ukladáte.

Napríklad prázdny adresár, ktorý používa štandardnú schému adresárového servera vyžaduje približne 10 MB pamäťového priestoru. Adresár, ktorý používa štandardnú schému a obsahuje 1000 položiek bežných informácií o zamestnancoch, vyžaduje asi 30 MB pamäťového priestoru. Tento počet sa bude líšiť v závislosti od presných atribútov, ktoré ste použili. Dané číslo sa tiež značne zvýši, ak ste uložili do adresára veľké objekty, napríklad obrázky.

- **Rozhodnite sa, ktoré bezpečnostné opatrenia prijmete**.

  Adresárový server vám umožňuje používať politiku hesiel, ktorá zabezpečuje, že užívatelia pravidelne menia svoje heslá a že heslá spĺňajú požiadavky organizácie na syntax hesiel.

  Pre bezpečnú komunikáciu podporuje adresárový server používanie SSL (Secure Sockets Layer) a digitálnych certifikátov rovnako ako TLS (Transport Layer Security). Podporuje sa aj autentifikácia Kerberos.

  Adresárový server vám umožňuje riadiť prístup k adresárovým objektom pomocou zoznamov ACL (zoznamy prístupových práv). Na ochranu adresára môžete použiť audit bezpečnosti operačného systému.

  Okrem tohto rozhodnite, ktorá politika hesiel sa má používať.

- **Vyberte DN a heslo administrátora**. Štandardné DN administrátora je cn=administrator. Toto je jediná identita s oprávnením na vytváranie alebo zmenu položiek adresára pri počiatočnom nakonfigurovaní servera. Môžete použiť štandardné DN administrátora alebo si vybrať iné DN. Pre DN administrátora musíte vytvoriť aj heslo.
- **Inštalácia softvéru, nevyhnutného pre webový administratívny nástroj adresárového servera**. Aby ste mohli používať webový administratívny nástroj adresárového servera, na serveri iSeries musia byť nainštalované nasledovné dopredu vyžadované produkty.
  - IBM HTTP Server for iSeries (5722-DG1)
  - IBM WebSphere Application Server - Express (5722-IWE Base a Voľba 2)

  Pozrite tému IBM HTTP Server, kde nájdete bližšie informácie o produkte IBM HTTP Server for iSeries and IBM WebSphere Application Server - Express.

Konfigurácia adresárového servera

1. Ak nie je váš server nakonfigurovaný tak, aby zverejňoval informácie na iný server LDAP a server TCP/IP DNS nepozná žiadne servery LDAP, v tom prípade sa adresárový server automaticky nainštaluje s obmedzenou štandardnou konfiguráciou. Ďalšie informácie nájdete v časti “Štandardná konfigurácia pre adresárový server” na strane 89. Adresárový server poskytuje sprievodcu, ktorý vám má pomôcť pri konfigurovaní adresárového servera podľa vašich konkrétnych potrieb. Tohto sprievodcu môžete spustiť ako súčasť aplikácie EZ-Setup alebo spustiť sprievodcu neskôr z iSeries Navigator. Použite ho, keď po prvýkrát konfigurujete adresárový server. Tohto sprievodcu môžete použiť aj na prekonfigurovanie adresárového servera.

   Poznámka: Ak použijete sprievodcu na prekonfigurovanie adresárového servera, začnete konfigurovať znova. Pôvodná konfigurácia sa vymaže a nedá sa meniť. Adresárové údaje sa však nevymažú, ale ostanú uložené v knižnici, ktorú ste si vybrali pri inštalácii (štandardne je to QUSRDIRDB). Protokol zmeny zostane tiež zachovaný štandardne v knižnici QUSRDIRCL.

   Ak chcete začať úplne nanovo, vymažte tieto dve knižnice pred spustením pomocníka.

   Ak chcete zmeniť konfiguráciu adresárového servera, ale nechcete ho úplne vymazať, kliknite pravým tlačidlom myši na **Adresár** a vyberte **Vlastnosti**. Tak nevymažete pôvodnú konfiguráciu.

   Ak chcete konfigurovať server, musíte mať špeciálne oprávnenia *ALLOBJ a *IOSYSCFG. Ak chcete nakonfigurovať audit bezpečnosti, musíte mať aj mimoriadne oprávnenie *AUDIT.
2. Ak chcete spustiť Sprievodcu konfiguráciou adresárového servera, postupujte podľa nasledujúcich krokov:
   a. V iSeries Navigator rozviňte **Sieť**.
   b. Rozviňte **Servery**.
   c. Kliknite na **TCP/IP**.
   d. Kliknite pravým tlačidlom myši na **Adresárový server IBM** a vyberte **Nakonfigurovať**.

      Poznámka: Ak ste adresárový server nakonfigurovali, kliknite na **Zmeniť konfiguráciu**, nie na **Konfigurovať**.

3. Dodržujte pokyny Sprievodcu konfiguráciou adresárového servera a nakonfigurujte váš adresárový server.

   Poznámka: Môžete tiež umiestniť knižnicu, ktorá uchováva údaje adresára, do užívateľskej pomocnej úložnej oblasti (ASP), nie do systémovej ASP. Túto knižnicu však nemožno uložiť v nezávislej ASP a každý pokus o konfiguráciu, prekonfigurovanie alebo spustenie servera s knižnicou, ktorá sa nachádza v nezávislej ASP, bude neúspešný.
4. Po skončení sprievodcu má váš adresárový server základnú konfiguráciu. Ak na systéme používate aplikáciu Lotus Domino, port 389 (predvolený port pre server LDAP) už môže využívať iná funkcia Domino LDAP. Musíte vykonať jeden z nasledujúcich krokov:
   - Zmeňte port, ktorý používa aplikácia Lotus Domino. Pozrite časť " Hosťovanie Domino LDAP a adresárového servera na tom istom serveri iSeries " v téme E-mail, kde nájdete bližšie informácie.
   - Zmeňte port, ktorý používa adresárový server. Ďalšie informácie nájdete v časti "Zmena portu alebo adresy IP" na strane 113.
   - Použite konkrétne IP adresy. Ďalšie informácie nájdete v časti "Zmena portu alebo adresy IP" na strane 113.
5. Vytvorte položky, zodpovedajúce prípone alebo príponám, ktoré ste nakonfigurovali. Ďalšie informácie nájdete v časti "Pridávanie a odstraňovanie prípon adresárového servera" na strane 114.

Kým budete pokračovať, môžete vykonať jeden alebo všetky z nasledovných úkonov:
- Naimportovať údaje na server - informácie nájdete v časti "Import/export súboru LDIF" na strane 91.
- Aktivovať SSL (Secure Sockets Layer) - informácie nájdete v časti "Povolenie SSL a TLS (Transport Layer Security) v adresárovom serveri" na strane 149.
- Aktivovať autentifikáciu Kerberos - informácie nájdete v časti "Povolenie autentifikácie Kerberos na adresárovom serveri" na strane 151.
- Nastaviť odvolávku - informácie nájdete v časti "Zadanie servera pre odvolávky na adresár" na strane 114.

Štandardná konfigurácia pre adresárový server

Adresárový server sa automaticky nainštaluje, keď nainštalujete systém i5/OS. Táto inštalácia obsahuje štandardnú konfiguráciu. Adresárový server používa predvolenú konfiguráciu, keď platia všetky nasledovné podmienky:
- Administrátori nespustili Sprievodcu konfiguráciou adresárovým serverom alebo nezmenili nastavenia adresárov pomocou strán vlastností.
- Adresárový server nie je nakonfigurovaný publikovanie.
- Adresárový server nevie nájsť žiadne informácie o DNS LDAP.

Ak adresárový server použije štandardnú konfiguráciu, dochádza k nasledovnému:
- Adresárový server sa spúšťa automaticky pri spustení TCP/IP.
- Systém vytvorí štandardného správu cn=Administrator. Tiež vygeneruje heslo, ktoré sa bude interne používať. Ak potrebujete neskôr použiť heslo administrátora, môžete definovať nové zo strany vlastností adresárového servera.
- Vytvorí sa štandardná prípona, založená na systémovom názve IP. Na základe systémového názvu sa vytvorí aj prípona systémových objektov. Ak je napríklad systémový názov vášho IP mary.acme.com, prípona je dc=mary,dc=acme,dc=com.
- Adresárový server používa štandardnú knižnicu údajov QUSRDIRDB. Túto systém vytvorí v ASP systéme.
- Pre nezabezpečenú komunikáciu používa systém port 389. Ak bol pre LDAP nakonfigurovaný digitálny certifikát, pre bezpečnú komunikáciu bude povolené SSL (secure sockets layer) a použije sa port 636.

Osadzovanie adresára

Existuje množstvo spôsobov na osadzovanie adresára. Viac informácií nájdete v nasledujúcich témach:
- "Publikovanie informácií na adresárový server" na strane 90
- "Import/export súboru LDIF" na strane 91
- "Kopírovanie užívateľov z validačného zoznamu servera HTTP na Adresárový server" na strane 92

Publikovanie informácií na adresárový server

Váš systém môžete nakonfigurovať tak, aby publikoval určité informácie na adresárový server na tom istom systéme alebo na inom systéme, ako aj užívateľom definované informácie. Operačný systém automaticky publikuje tieto informácie na adresárový server, keď pomocou iSeries Navigator zmeníte tieto informácie na systéme i5/OS. Informácie, ktoré môžete zverejňovať zahŕňajú informácie o systéme (systémy a tlačiarne), zdieľania tlače, užívateľské informácie a politiky kvality služby TCP/IP (viac informácií nájdete v časti “Zverejňovanie” na strane 34).

Ak rodičovský DN, do ktorého sa údaje publikujú, neexistuje, adresárový server ho automaticky vytvorí. Rovnako ste mohli nainštalovať iné aplikácie i5/OS, ktoré publikujú informácie v adresári LDAP. Okrem toho môžete do adresára LDAP zverejniť iné typy informácií pomocou volania aplikačných programových rozhraní (API).

Poznámka: Môžete tiež publikovať informácie o i5/OS na adresárový server, ktorý nepoužíva systém i5/OS, ak nakonfigurujete tento server, aby používal schému IBM.

Ak chcete nakonfigurovať váš systém, aby publikoval informácie o i5/OS na adresárový server, vykonajte tieto kroky:

1. V iSeries Navigator kliknite pravým tlačidlom myši na váš systém a zvoľte **Vlastnosti**.
2. Kliknite na záložku **Adresárový server**.
3. Vyberte typy informácií, ktoré chcete publikovať

   Tip: Ak na jedno miesto plánujete zverejňovať viac ako jeden typ informácií, ušetríte čas, ak počas jednej konfigurácie vyberiete viaceré typy informácií. Operations Navigator použije vami zadané hodnoty počas konfigurovania jedného typu informácií ako štandardné hodnoty pri konfigurácii ďalších typov informácií.
4. Kliknite na **Podrobnosti**.
5. Kliknite na začiarkavacie políčko **Publikovať systémové informácie**.
6. Špecifikujte **Metódu autentifikácie**, ktorú má váš server používať, ako aj dostatočné autentifikačné informácie.
7. Kliknite na tlačidlo **Upraviť** vedľa políčka **(Aktívny) Adresárový server**. V zobrazenom dialógu zadajte názov adresárového servera, kam chcete publikovať informácie o i5/OS, potom kliknite na tlačidlo **OK**.
8. V poli **Pod DN** zadajte rozlišovací názov (DN) rodiča, pod ktorého chcete pridať informácie do adresárového servera.
9. Vyplňte políčka v okne **Pripojenie servera**, ktoré sa týkajú vašej konfigurácie.

   Poznámka: Ak chcete publikovať informácie o i5/OS na adresárový server pomocou SSL alebo Kerberos, najskôr musíte si nakonfigurovať adresárový server tak, aby používal príslušný protokol. Viac informácií o SSL a Kerberos nájdete v časti “Autentifikácia Kerberos na adresárovom serveri” na strane 47.
10. Ak váš adresárový server nepoužíva štandardný port, v poli **Port** zadajte správne číslo portu.
11. Kliknite na **Potvrdiť**, aby ste sa uistili, že rodičovské DN na serveri existuje a že informácie o pripojení sú správne. Ak adresárová cesta neexistuje, dialóg vás vyzve k jej vytvoreniu.

    Poznámka: Ak neexistuje rodičovský DN a vy ho nevytvoríte, zverejňovanie nebude úspešné.
12. Kliknite na **OK**.

Poznámka: Môžete tiež publikovať informácie o i5/OS na adresárový server, ktorý je na inej platforme. Informácie o užívateľoch a systéme musíte publikovať na adresárový server, ktorý používa schému kompatibilnú so schémou IBM Adresárový server. Bližšie informácie o Schéme adresárov IBM nájdete v časti “Schéma adresárového servera IBM” na strane 16.

Rozhrania API pre publikovanie informácií o systéme i5/OS na adresárový server

Adresárový server poskytuje vstavanú podporu pre zverejňovanie užívateľských informácií a informácií o systéme. Tieto položky sú uvedené na stránke **Adresárový server** dialógového okna **Vlastnosti** systému. Pomocou konfigurácie servera LDAP a publikačných rozhraní API môžete povoliť programom i5/OS, ktoré ste napísali, publikovať iné typy informácií. Tieto typy informácií sa potom zobrazia na aj na stránke **Adresárový server**. Podobne ako užívatelia a

systémy sú najprv deaktivované a nakonfigurujete ich rovnakým postupom. Program, ktorý pridáva údaje do adresára LDAP, sa nazýva zverejňujúci agent. Typy informácií, ktoré sa zverejňujú, ako je uvedené na stránke **Adresárový server** sa nazývajú názov agenta.

Zverejňovanie vám do vlastných programov umožnia zabudovať nasledujúce API :

QgldChgDirSvrA
: Aplikácia používa formát CSVR0500 s cieľom pridať na začiatku názov agenta, ktorý je označený ako zakázaná položka. Pokyny pre užívateľov aplikácie by im mali oznámiť, aby pomocou iSeries Navigator prešli na stránku vlastností adresárového servera a nakonfigurovali zverejňovacieho agenta. Príkladmi názvov agentov sú názvy agentov systémov a užívateľov, automaticky dostupné na stránke **Adresárový server**.

QgldLstDirSvrA
: Pomocou tohto formátu API LSVR0500 uveďte, ktorí agenti sú momentálne dostupní na vašom systéme.

QgldPubDirObj
: Toto API použite na aktuálne zverejnenie informácií.

Podrobné informácie o týchto API obsahuje téma LDAP (Lightweight Directory Access Protocol) pod Programovaním v iSeries Information Center.

Import/export súboru LDIF

Import súboru LDIF

Pomocou súborov LDIF (LDAP Data Interchange Format) môžete prenášať informácie medzi rôznymi adresárovými servermi. Ďalšie informácie nájdete v časti “Formát LDIF (LDAP data interchange format)” na strane 214. Kým začnete túto procedúru, presuňte súbor LDIF na váš server iSeries ako súbor toku.

Pri importovaní súboru LDIF do adresárového servera postupujte nasledovne:

1. Ak je spustený adresárový server, zastavte ho. Informácie o zastavení adresárového servera nájdete v časti “Spustenie/zastavenie adresárového servera” na strane 108.
2. V iSeries Navigator rozviňte **Sieť**.
3. Rozviňte **Servery**.
4. Kliknite na **TCP/IP**.
5. Kliknite pravým tlačidlom myši na **Adresárový server IBM** a vyberte **Nástroje**, potom **Importovať súbor**.

   Voliteľne môže server pri ďalšom štarte replikovať novo naimportované údaje výberom **Replikovať importované údaje**. Je to užitočné pri pridávaní nových položiek do existujúceho adresárového stromu na hlavnom serveri. Ak importujete údaje na inicializáciu replikačného (alebo partnerského) servera, väčšinou nebudete chcieť replikovať údaje, keďže tie môžu už existovať na serveroch, pre ktoré je dodávateľom tento server.

Poznámka: Na import súborov LDIF môžete tiež použiť pomocný program ldapadd (pozri “ldapmodify a ldapadd” na strane 185).

Export súboru LDIF

Pomocou súborov LDIF (LDAP Data Interchange Format) môžete prenášať informácie medzi rôznymi adresárovými servermi, (pozri “Formát LDIF (LDAP data interchange format)” na strane 214). Do súboru LDIF môžete exportovať celý alebo jeho časť.

Ak chcete exportovať súbor LDIF z adresárového servera, postupujte takto:

1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom myši na **Adresárový server IBM** a vyberte **Nástroje**, potom **Exportovať súbor**.

Poznámka: Ak nezadáte plne kvalifikovanú cestu pre súbor LDIF, do ktorého sa majú exportovať údaje, súbor sa vytvorí v domovskom adresári špecifikovanom v užívateľskom profile vášho operačného systému.

5. Zadajte, či sa má **Exportovať celý adresár** alebo **Exportovať vybraté podstromy**, ako aj to, či **Exportovať prevádzkové atribúty**. Budú sa exportovať prevádzkové atribúty creatorsName, createTimestamp, modifiersName a modifyTimestamp.

Poznámky:

1. Pri exportovaní údajov na importovanie na adresárové servery V5R3 alebo staršie nevyberajte voľbu **Exportovať prevádzkové atribúty**. Tieto prevádzkové atribúty nemožno importovať na adresárové servery V5R3 alebo staršie.
2. Úplný alebo čiastočný súbor LDIF môžete vytvoriť aj použitím služby ldapsearch, pozrite "ldapsearch" na strane 200. Použite voľbu -L a presmerujte výstup do súboru.
3. Uistite sa, že ste pre súbor LDIF nastavili také oprávnenie, ktoré zabráni neoprávnenému prístupu k údajom adresára. Ak to chcete urobiť, pravým tlačidlom kliknite na súbor v iSeries Navigator, potom vyberte **Povolenia**.

Kopírovanie užívateľov z validačného zoznamu servera HTTP na Adresárový server

Ak momentálne používate server HTTP alebo ste ho používali v minulosti, možno ste vytvorili validačné zoznamy a ukladanie užívateľov internetu a ich hesiel. Keď prejdete na Aplikačný server WebSphere, Portal Server a iné aplikácie podporujúce autentifikáciu LDAP, budete chcieť ďalej používať týchto existujúcich užívateľov internetu a ich heslá. To môžete vykonať pomocou API ″Kopírovať validačný zoznam do adresára″, QGLDCPYVL.

QGLDCPYVL prečíta položky z validačného zoznamu a vytvorí zodpovedajúce objekty LDAP v lokálnom adresárovom serveri. Tieto objekty budú kostrové položky inetOrgPerson s atribútom userPassword, ktorý obsahuje kópiu informácií o hesle z položky validačného zoznamu. Môžete rozhodnúť, ako a kedy sa vyvolá API. Môžete ho použiť ako časovú operáciu pre validačný zoznam, ktorý sa nebude meniť, alebo ako naplánovanú úlohu na aktualizáciu adresárového servera, aby reflektoval položky validačného zoznamu.

Podrobnejší popis API QGLDCPYVL nájdete v časti Rozhrania API adresárového servera. Príklad použitia rozhrania API nájdete v časti "Scenár: Kopírovanie užívateľov z validačného zoznamu servera HTTP na Adresárový server".

Scenár: Kopírovanie užívateľov z validačného zoznamu servera HTTP na Adresárový server

Situácia a prehľad

Momentálne máte aplikáciu spustenú na serveri HTTP (využívajúci Apache) používajúcu užívateľov Internetu vo validačnom zozname MYLIB/HTTPVLDL. Chceli by ste používať tých istých užívateľov Internetu s Aplikačným serverom WebSphere (WAS) s autentifikáciou LDAP. Aby nedochádzalo k dvojitej údržbe informácií o užívateľoch vo validačnom zozname a LDAP, nakonfigurujete aj aplikáciu servera HTTP, aby používala autentifikáciu LDAP.

Za tým účelom musíte vykonať tieto kroky:

1. Skopírovať existujúcich užívateľov validačného zoznamu na lokálny adresárový server.
2. Nakonfigurovať server WAS, aby používal autentifikáciu LDAP.
3. Prekonfigurovať server HTTP, aby používal autentifikáciu LDAP namiesto validačného zoznamu.

Krok 1: Skopírujte existujúcich užívateľov validačného zoznamu na lokálny adresárový server.

Predpokladá sa, že adresárový server bol už predtým nakonfigurovaný s príponou ″o=my company″ a je spustený. Užívatelia LDAP sa budú ukladať do adresárového podstromu ″cn=users,o=my company″. DN administrátora adresárového servera je ″cn=administrator″ a heslo administrátora je ″secret″.

Vyvolajte API príkazového riadku nasledovne:

```
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')
```

Po dokončení bude adresárový server obsahovať položky inetorgperson podľa položiek validačného zoznamu. Napríklad, z užívateľa validačného zoznamu:

```
Meno užívateľa: jsmith
Popis: John Smith
Heslo: ******
```

vznikne nasledovná adresárová položka:

```
dn: uid=jsmith,cn=users,o=my company
 objectclass: top
       objectclass: person
objectclass: organizationalperson
         objectclass: inetorgperson
uid: jsmith
sn: jsmith
cn: jsmith
description: John Smith
userpassword: ******
```

Túto položku možno teraz použiť na autentifikáciu adresárového servera. Napríklad, vykonanie tohto QSH ldapsearch prečíta koreňovú položku DSE servera:

```
> ldapsearch -D "uid=jsmith,cn=users,o=my company" -w ****** -s base "(objectclass=*)"
```

Po vytvorení môžete upraviť položky adresára tak, aby obsahovali ďalšie informácie. Napríklad, chcete zmeniť hodnoty cn a sn tak, aby reflektovali celé meno resp. priezvisko užívateľa, alebo pridať telefónne číslo a adresu elektronickej pošty.

Krok 2: Nakonfigurujte server WAS, aby používal autentifikáciu LDAP

Bezpečnosť WAS LDAP sa musí nakonfigurovať tak, aby vyhľadávala položky pod dn ″cn=users,o=my company″, pomocou vyhľadávacieho filtra, ktorý namapuje zadané meno užívateľa na položky inetOrgPerson obsahujúce hodnotu atribútu tohto uid. Napríklad, autentifikácia na WAS pomocou mena užívateľa jsmith spôsobí vyhľadávanie položiek vyhovujúcich vyhľadávaciemu filtru ″(uid=jsmith)″. Bližšie informácie nájdete v časti Konfigurovanie vyhľadávacích filtrov LDAP v Informačnom centre Aplikačný server Websphere pre iSeries.

Prekonfigurujte server HTTP, aby používal autentifikáciu LDAP namiesto validačného zoznamu

Poznámka: Doleuvedená procedúra je určená ako pomoc pri ilustrácii príkladov v tomto scenári. Uvádza prehľad vyššej úrovne pre konfigurovanie servera HTTP na používanie autentifikácie LDAP. Pravdepodobne budete potrebovať podrobnejšie informácie, ktoré nájdete v publikácii IBM Redbook Implementácia a praktické použitie LDAP na serveri IBM eServer iSeries, SG24-6193  , Časť 6.3.2 ″Nastavenie autentifikácie LDAP pre server používajúci Apache″ ako aj Nastavenie ochrany heslom na serveri HTTP (používajúcom Apache).

1. Kliknite na **Základná autentifikácia** na karte **Konfigurácia** pre váš server HTTP v aplikácii HTTP Administration tool.
2. Pod položkou **Autentifikačná metóda užívateľa** zmeňte**Používať užívateľov Internet vo validačných zoznamoch** na **Používať položky užívateľov na serveri LDAP** a kliknite na tlačidlo **OK**.
3. Vráťte sa na kartu **Konfigurácia** a kliknite na **Riadenie prístupu**. Nakonfigurujte ho podľa popisu v dokumente Redbook uvedenom vyššie a kliknite na tlačidlo **OK**.
4. Na karte **Konfigurácia** kliknite na **Autentifikácia LDAP**.
   a. Zadajte názov hostiteľa a port servera LDAP. V položke **DN vyhľadávacej bázy užívateľa** zadajte cn=users,o=my company.
   b. Pod položkou **Vytvoriť jedinečnú DN LDAP pre autentifikáciu užívateľa** zadajte filter (&objectclass=person)(uid=%v1)).
   c. Zadajte informácie o skupine a kliknite na tlačidlo **OK**.
5. Nakonfigurujte pripojenie na server LDAP podľa popisu v dokumente Redbook uvedenom vyššie.

Odporúčané postupy pre štruktúru adresárov

Adresárový server sa často používa ako archív pre užívateľov a skupiny. Táto časť popisuje niektoré odporúčané postupy na nastavovanie štruktúry, ktorá je optimalizovaná pre správu užívateľov a skupín. Táto štruktúra s priradený model zabezpečenia možno rozšíriť na ostatné použitia adresára.

Užívatelia sa väčšinou ukladajú ja jedno miesto alebo niekoľko málo miest. Môžete mať jeden kontajner, cn=users, ktorý je rodičovskou položkou pre všetkých užívateľov, alebo samostatné kontajnery pre rôzne množiny užívateľov, ktorá sa spravujú samostatne. Napríklad, zamestnanci, predajcovia a samostatne zaregistrovaní užívatelia Internetu sa môžu nachádzať pod objektmi s názvami cn=employees, cn=vendors či cn=internet users Niekoho by mohlo pokúšať umiestniť ľudí pod organizácie, do ktorých patria, ale to môže spôsobiť komplikácie, keď sa presunú do inej organizácie, keďže položku adresára tiež bude treba presunúť a skupiny alebo iné zdroje údajov (interné aj externé vzhľadom adresár) bude treba aktualizovať, aby reflektovali nový DN. Vzťah užívateľov k organizačnej štruktúre možno zachytiť v užívateľskej položke pomocou adresárových atribútov, napríklad ″o″ (organizačný názov), ″ou″ (názov organizačnej jednotky) a departmentNumber, ktoré sú súčasťou štandardnej schémy pre organizationalPerson a inetOrgPerson.

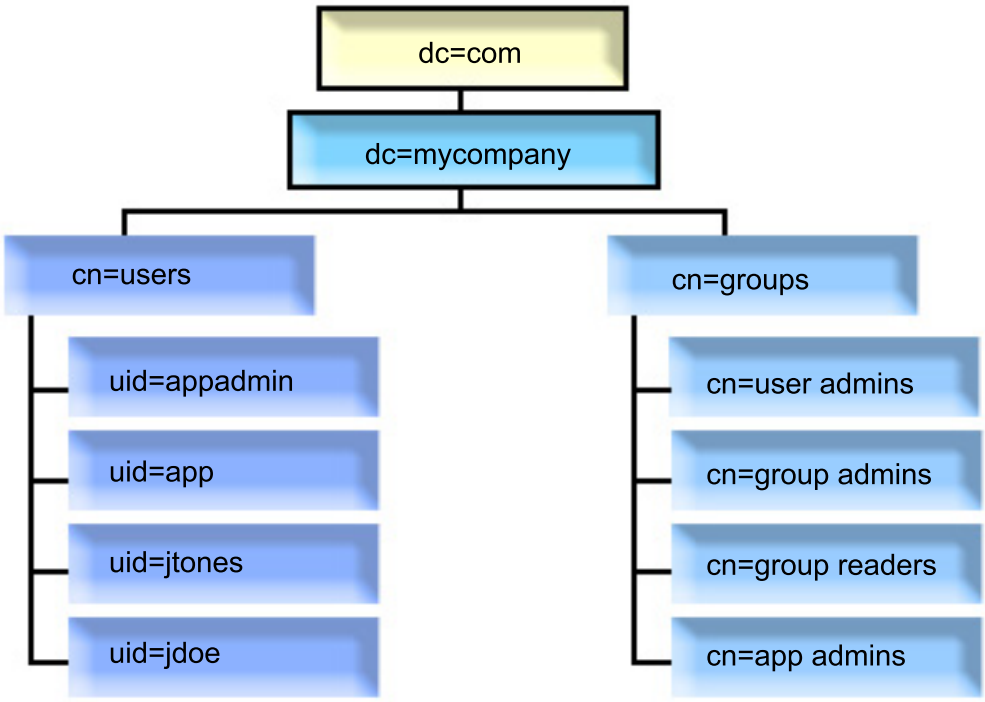
Podobne aj skupiny sa väčšinou umiestňujú do samostatného kontajnera, napríklad kontajnera s názvom ″cn=groups″.

Zorganizovaním užívateľov a skupín takýmto spôsobom vznikne len málo miest, kde je potrebné nastaviť zoznamy riadenia prístupu (ACL).

Podľa toho ako sa používa adresárový server a ako sa riadia užívatelia a skupiny, môžete použiť jeden z nasledovných vzorov riadenia prístupu:

- Ak sa adresár používa pre aplikácie, ako je zoznam adries, môžete udeliť špeciálnej skupine cn=anybody oprávnenia na čítanie a vyhľadávanie pre ″normálne″ atribúty v kontajneri cn=users a jeho rodičovských objektoch.
- Často do kontajnera cn=groups potrebujú prístup len názvy DN používané špecifickými aplikáciami a administrátormi skupín. Môžete vytvoriť skupinu uchovávajúcu názvy DN administrátorov skupín, ktorá zoskupuje vlastníka cn=groups a jeho podriadených. Môžete vytvoriť inú skupinu uchovávajúcu názvy DN používané aplikáciami na čítanie informácií o skupine a udeliť tejto skupine oprávnenia na čítanie a vyhľadávanie pre cn=groups.
- Ak užívateľské objekty aktualizujú priamo užívatelia, môžete udeliť príslušné špeciálne oprávnenia na čítanie, zapisovanie a vyhľadávanie pre access-id cn=this.
- Ak sa užívatelia aktualizujú cez aplikácie, tieto aplikácie často pracujú pod ich vlastnou identitou, a len tieto aplikácie potrebujú oprávnenie na aktualizáciu užívateľských objektov. A znova, je užitočné pridať tieto názvy DN do skupiny, napríklad, cn=user administrators, a udeliť tejto skupine potrebné oprávnenia pre cn=users.

Po aplikovaní tohto typu štruktúry a riadenia prístupu bude váš úvodný adresár vyzerať približne nasledovne:



Obrázok 3. Príklad štruktúry adresára

- c=mycompany, dc=com je vo vlastníctve administrátora adresára alebo iného užívateľa či skupiny s oprávnením na riadenie najvyššej úrovne adresára. Ďalšie položky ACL udeľujú prístup na čítanie pre normálne atribúty pre jednu z cn=anybody alebo cn=authenticated, či prípadne nejakú inú skupinu, ak je potrebný viac obmedzujúci ACL.
- cn=users má položky ACL pod položkami popísanými nižšie, ktoré umožňujú príslušný prístup k užívateľom. Zoznamy ACL môžu obsahovať:
  - prístup na čítanie a zápis do normálnych atribútov pre cn=anybody alebo cn=authenticated
  - prístup na čítanie a zápis do normálnych a citlivých atribútov pre manažérov
  - ostatné položky ACL podľa potreby, napríklad umožňujúce prístup na zápis pre jednotlivcov do ich vlastnej položky.

Poznámka:

- Na zlepšenie čitateľnosti boli použité názvy RDN položiek namiesto plných názvov DN. Napríklad, skupina ″user admins″ môže mať plný DN uid=app,cn=users,dc=mycompany,dc=com ako člen, namiesto skráteného uid=app.
- Niektorých užívateľov a skupiny je možné kombinovať. Napríklad, ak administrátor aplikácie mal oprávnenie na riadenie užívateľov, aplikácia by sa mohla spúšťať pod DN tohto administrátora aplikácie. Ale to by mohlo obmedziť napríklad schopnosť zmeniť heslo administrátora aplikácie bez súčasného prekonfigurovania nového hesla v aplikácii.
- Zatiaľ čo horeuvedené predstavuje najlepšie metódy pre adresáre používané len jednou aplikáciou, spôsobilejšie by bolo vykonať všetku autentifikáciu ako administrátor adresára. Táto metóda sa neodporúča z dôvodov uvedených vyššie.

Webová administrácia

Prostredníctvom webovej administračnej konzoly je možné spravovať jeden alebo viac adresárových serverov. Webová administračná konzola vám umožňuje:

- Pridávať alebo meniť zoznam adresárových serverov, ktoré je možné spravovať.
- Spravovať adresárový server pomocou webového administratívneho nástroja.

- Meniť atribúty webovej administračnej konzoly.

Aby ste mohli používať webovú administračnú konzolu, postupujte nasledovne:

1. Keď prvý raz používate nástroj na správu adresárového servera cez Web, musíte najprv nastaviť webovú administráciu (pozrite si "Prvé nastavenie webovej administrácie") a potom prejsť na ďalší krok.
2. Prihláste sa na webovú administráciu adresárového servera vykonaním jedného z nasledovných úkonov:
   - V aplikácii iSeries Navigator vyberte váš server a kliknite na **Sieť > Servery > TCP/IP**, kliknite pravým tlačidlom na **Adresárový server IBM** a kliknite na **Administrácia servera**.
   - Na stránke Úlohy iSeries (http://*váš_server*:2001) kliknite na **Adresárový server IBM**.
3. Ak chcete spravovať adresárový server, postupujte nasledovne:
   a. V poli **Názov hostiteľa LDAP** vyberte adresárový server, ktorý chcete spravovať.
   b. Zadajte prihlasovacie DN administrátora, ktoré použijete na pripojenie k adresárovému serveru.
   c. Zadajte heslo administrátora.
   d. Kliknite na **Prihlásenie**. Zobrazí sa stránka Webový administratívny nástroj adresárového servera IBM. Bližšie informácie o stránke Webový administratívny nástroj adresárového servera IBM nájdete v časti "Webový administračný nástroj" na strane 97.
4. Ak chcete pridať alebo zmeniť zoznam adresárových serverov, ktoré je možné spravovať, alebo ak chcete zmeniť atribúty webovej administračnej konzoly, postupujte nasledovne:
   a. V poli **Názov hostiteľa LDAP** vyberte **Administrátor konzoly**.
   b. Zadajte prihlasovacie meno administrátora konzoly.
   c. Zadajte heslo administrátora konzoly.
   d. Kliknite na **Prihlásenie**. Zobrazí sa stránka Webový administratívny nástroj adresárového servera IBM. Bližšie informácie o stránke Webový administratívny nástroj adresárového servera IBM nájdete v časti "Webový administračný nástroj" na strane 97.
   e. Kliknite na **Správa konzoly** a vyberte jedno z nasledovného:
      - **Zmena prihlasovacieho mena administrátora konzoly**, ak chcete zmeniť prihlasovacie meno administrátora konzoly.
      - **Zmena hesla administrátora konzoly**, ak chcete zmeniť heslo administrátora konzoly.
      - **Manažovanie serverov konzoly**, ak chcete zmeniť, ktoré adresárové servery možno spravovať prostredníctvom webovej administračnej konzoly.
      - **Manažovanie vlastností konzoly**, ak chcete zmeniť vlastnosti webovej administračnej konzoly.

Prvé nastavenie webovej administrácie

Urobte nasledujúce pre úvodné nastavenie Webového administračného nástroja Adresárového servera.

1. Nainštalujte Aplikačný server IBM WebSphere - Express 5.1 (5722E51 Base a 2) a súvisiaci predbežne vyžadovaný softvér, ak ešte nie sú nainštalované.
2. Aktivujte inštanciu systémového aplikačného servera v inštancii HTTP ADMIN servera.Viac informácií nájdete v téme IBM HTTP Server.
   a. Spustite inštanciu HTTP ADMIN servera vykonaním niečoho z nasledujúceho.
      - V iSeries Navigator kliknite na **Sieť -> Servery -> TCP/IP** a kliknite pravým tlačidlom na **Správa HTTP**. Potom kliknite na **Spustiť**.
      - Do príkazového riadku zadajte STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).
   b. Prihláste sa na Webovú administráciu IBM pre iSeries. Pomocou užívateľského profilu operačného systému sa prihláste na stránku Úlohy iSeries (http://*váš_server*:2001), potom kliknite na položku Webová administrácia **IBM pre iSeries**.
   c. Zo stránky HTTP Server Administration *váš_server* kliknite na záložku **Manažovanie** a potom kliknite na záložku **HTTP Servers**. Skontrolujte, či je zvolená položka **ADMIN – Apache** v rozbaľovacom zozname **Server** a či je zvolená položka **Zahrnúť /QIBM/UserData/HTTPA/admin/conf/admin-cust.conf** v rozbaľovacom zozname **Oblasť servera**.

d. Z volieb v ľavom paneli stránky kliknite na **Všeobecná konfigurácia servera**.

Poznámka: Budete musieť rozvinúť časť **Vlastnosti servera**, aby ste uvideli voľbu **Všeobecná konfigurácia servera**.

e. Nastavte **Spustiť inštanciu systémového aplikačného servera po spustení servera 'Admin'** na **Áno**.

f. Kliknite na **OK**.

g. Reštartujte inštanciu HTTP ADMIN servera kliknutím na tlačidlo reštartu (druhé tlačidlo pod záložkou **HTTP Servers**). Inštanciu servera HTTP ADMIN môžete zastaviť a spustiť aj pomocou aplikácie iSeries Navigator alebo príkazového riadku.

Inštanciu HTTP ADMIN servera môžete zastaviť vykonaním niečoho z nasledujúceho.

- V aplikácii iSeries Navigator kliknite na **Sieť -> Servery -> TCP/IP** a pravým tlačidlom myši kliknite na **Správa HTTP**. Potom kliknite na **Zastaviť**.
- Do príkazového riadku zadajte ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).

Inštanciu HTTP ADMIN servera môžete spustiť vykonaním niečoho z nasledujúceho.

- V aplikácii iSeries Navigator kliknite na **Sieť -> Servery -> TCP/IP** a pravým tlačidlom myši kliknite na **Správa HTTP**. Potom kliknite na **Spustiť**.
- Do príkazového riadku zadajte STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).

Viac informácií nájdete v téme IBM HTTP Server.

3. Prihláste sa na Webový administratívny nástroj adresárového servera.
   a. Zavolajte **stránku Prihlásenie** vykonaním niečoho z nasledujúceho.
      - Z iSeries Navigator vyberte váš server a kliknite na **Sieť** -> **Servery** -> **TCP/IP**, kliknite pravým tlačidlom na **IBM Directory Server** a kliknite na **Administrácia servera**.
      - Zo stránky Úlohy iSeries (http://*váš_server*:2001) kliknite na **IBM Directory Server for iSeries**.
   b. Vyberte **Správca konzoly** v poli **Názov hostiteľa LDAP**.
   c. Napíšte superadmin do poľa **Meno užívateľa**.
   d. Napíšte secret do poľa **Heslo**.
   e. Kliknite na **Prihlásenie**. Zobrazí sa stránka IBM Directory Server Web Administration Tool.
4. Zmeňte prihlasovacie meno administrátora konzoly.
   a. Kliknite na **Správa konzoly** v ľavom paneli, aby sa rozvinula táto časť a potom kliknite na **Zmeniť prihlasovanie administrátora konzoly**.
   b. V poli **Prihlasovacie meno administrátora konzoly** zadajte nové prihlasovacie meno administrátora konzoly.
   c. V poli **Aktuálne heslo** zadajte aktuálne heslo (tajné) .
   d. Kliknite na **OK**.
5. Zmeňte heslo administrátora konzoly. Kliknite na **Zmeniť heslo administrátora konzoly** v ľavom paneli.
6. Uveďte adresárový server, ktorý chcete spravovať. Kliknite na **Manažovať konzolové servery** v ľavom paneli.

   Poznámka: Pri pridávaní adresárového servera sa **Port administrácie** nepoužije a bude sa ignorovať.
7. Ak chcete zmeniť vlastnosti konzoly. Kliknite na **Manažovať vlastnosti konzoly** v ľavom paneli.
8. Kliknite na **Odhlásenie**. Keď sa objaví obrazovka Úspešné odhlásenie, kliknite na odkaz **sem** pre návrat na prihlasovaciu stránku webovej administrácie.

Po prvom nakonfigurovaní konzoly sa na ňu môžete kedykoľvek vrátiť a:

- Zmeniť prihlasovacie meno a heslo administrátora konzoly.
- Zmeniť, ktoré adresárové servery možno spravovať prostredníctvom webového administratívneho nástroja.
- Zmeniť vlastnosti konzoly.

Webový administračný nástroj

Po prihlásení na webový administratívny nástroj nájdete okno aplikácií, ktoré sa skladá z piatich častí:

Oblasť záhlavia
Oblasť záhlavia sa nachádza v hornej časti panela a obsahuje názov aplikácie a logo IBM.

Navigačná oblasť
Navigačná oblasť, umiestnená na ľavej strane panela, zobrazuje kategórie, ktoré je možné rozvinúť pre rozličné úlohy obsahu servera, napríklad:

Vlastnosti užívateľa
Táto úloha vám umožňuje meniť aktuálne heslo užívateľa.

Manažovanie schémy
Táto úloha vám umožňuje pracovať s triedami objektov, atribútmi, zhodnými pravidlami a syntaxami.

Manažovanie adresára
Táto úloha vám umožňuje pracovať s položkami adresára.

Manažovanie replikácií
Táto úloha vám umožňuje pracovať s oprávneniami, topológiou, plánmi a frontmi.

Realmy a šablóny
Táto úloha vám umožňuje pracovať so šablónami užívateľov a realmami.

Užívatelia a skupiny
Táto úloha vám umožňuje pracovať s užívateľmi a skupinami v zadefinovaných realmoch. Ak chcete napríklad vytvoriť nového webového užívateľa, úloha **Užívatelia a skupiny** pracuje s jednou skupinou objectclass, groupOfNames. Podporu skupiny nemôžete upravovať.

Administrácia servera
Pomocou tejto úlohy môžete meniť konfiguráciu servera a nastavenia bezpečnosti.

Pracovná oblasť
Pracovná oblasť zobrazuje úlohy, spojené s vybratou úlohou v navigačnej oblasti. Ak napríklad v navigačnej oblasti vyberiete Manažovanie bezpečnosti servera, pracovná oblasť zobrazí stránku Bezpečnosť servera a záložky, ktoré obsahujú úlohy, týkajúce sa nastavovania bezpečnosti servera.

Oblasť stavu servera
Oblasť stavu servera je umiestnená vo vrchnej časti pracovnej oblasti. Ikona na ľavej strane oblasti stavu servera indikuje aktuálny stav servera. Vedľa tejto ikony je názov spravovaného servera. Ikona na pravej strane oblasti stavu servera poskytuje odkaz na online pomoc.

Oblasť stavu úlohy
Oblasť úloh, umiestnená pod pracovnou oblasťou, zobrazuje stav aktuálnej úlohy.

Kapitola 6. Scenár: Nastavenie adresárového servera

Situácia

Ako administrátor počítačových systémov vo vašej spoločnosti by ste chceli informácie o vašich užívateľoch (napríklad telefónne čísla a e-mailové adresy) umiestniť do centrálneho archívu LDAP.

Ciele

V tomto scenári chce spoločnosť MyCo, Inc. nakonfigurovať adresárový server a vytvoriť adresárovú databázu, ktorá obsahuje informácie o zamestnancoch, napríklad mená, e-mailové adresy a telefónne čísla.

Ciele tohto scenára sú nasledovné:

- Sprístupniť informácie o zamestnancoch v celej podnikovej sieti pre zamestnancov, ktorí používajú poštového klienta Lotus Notes alebo Microsoft Outlook Express.
- Umožniť manažérom meniť v adresárovej databáze údaje o zamestnancoch, túto možnosť však nedať osobám, ktoré nie sú na manažérskych pozíciách.
- Umožniť, aby server iSeries mohol publikovať údaje o zamestnancoch do adresárovej databázy.

Podrobnosti

Adresárový server bude spustený na serveri iSeries s názvom myiSeries.

Nasledujúci príklad znázorňuje informácie, ktoré chce spoločnosť MyCo, Inc. zaradiť do svojej adresárovej databázy v prípade každého zamestnanca.

```
Meno: Jose Alvirez
Oddelenie: DEPTA
Telefónne číslo: 999 999 9999
E-mailová adresa: jalvirez@my_co.com
```

Štruktúra adresára v tomto scenári môže vyzerať približne takto:

```
/
|
+- my_co.com
   |
   +- employees
      |
      +- Jose Alvirez
      |  DEPTA
      |  999-555-1234
      |  jalvirez@my_co.com
      |
      +- John Smith
      |  DEPTA
      |  999-555-1235
      |  jsmith@my_co.com
      |
      +  Skupina manažérov
         Jose Alvirez
         myiSeries.my_co.com
.
.
.
```

Všetci zamestnanci (manažéri aj osoby na iných ako manažérskych pozíciách) existujú v strome adresára zamestnancov. Manažéri patria navyše do skupiny manažérov. Členovia skupiny manažérov majú oprávnenie meniť údaje o zamestnancoch.

Server iSeries (myiSeries) musí mať aj oprávnenie na zmenu údajov o zamestnancoch. V tomto scenári bude server iSeries umiestnený do stromu adresárov zamestnancov a stane sa členom skupiny manažérov.

Ak chcete položky zamestnancov uchovávať oddelene od položky servera iSeries, môžete vytvoriť iný adresárový strom (napríklad: počítače) a doň pridať server iSeries. Server iSeries bude musieť mať rovnaké oprávnenie ako manažéri.

Podmienky a predpoklady

Webový administračný nástroj je správne nakonfigurovaný a beží. Ďalšie informácie nájdete v časti “Webová administrácia” na strane 95.

Kroky nastavovania

Vykonajte nasledujúce úlohy:
1. “Podrobný scenár: Nastavenie adresárového servera”.
2. “Podrobný scenár: Vytvorenie adresárovej databázy” na strane 101.
3. “Podrobný scenár: Zverejňovanie údajov iSeries do adresárovej databázy” na strane 103.
4. “Podrobný scenár: Zadávanie informácií do adresárovej databázy” na strane 104.
5. “Podrobný scenár: Kontrola adresárovej databázy” na strane 105.

Podrobný scenár: Nastavenie adresárového servera

Krok 1: Konfigurácia adresárového servera

Poznámka: Ak chcete konfigurovať server, musíte mať špeciálne oprávnenia *ALLOBJ a *IOSYSCFG.

1. V aplikácii iSeries Navigator kliknite na **Sieť —> Servery —> TCP/IP**.
2. V pravej dolnej časti aplikácie iSeries Navigator, v okne **Úlohy konfigurácie servera** kliknite na **Nakonfigurovať systém ako adresárový server** .
3. Zobrazí sa **Sprievodca konfiguráciou adresárového servera**.
4. V okne **Konfiguračný sprievodca IBM Directory Server - Vitajte** kliknite na **Nakonfigurovať lokálny adresárový server LDAP**.
5. V okne **Konfiguračný sprievodca IBM Directory Server - Vitajte** kliknite na tlačidlo **Ďalej**.
6. V okne **Konfiguračný sprievodca IBM Directory Server - Špecifikácia nastavení** kliknite na voľbu **Nie**. Toto vám umožní nakonfigurovať server LDAP bez štandardných nastavení.
7. V okne **Konfiguračný sprievodca IBM Directory Server - Špecifikácia nastavení** kliknite na tlačidlo **Ďalej**.
8. V okne **Konfiguračný sprievodca IBM Directory Server - Zadanie DN administrátora** zrušte označenie voľby **Systémom generované** a zadajte nasledujúce:

DN administrátora	cn=administrator
Heslo	tajné
Potvrďte heslo	tajné

Poznámka: Všetky heslá, uvedené v tomto scenári, sú len vzorové a používajú sa len ako príklady. Ak chcete predísť ohrozeniu bezpečnosti vášho systému alebo siete, nikdy nepoužívajte tieto heslá ako súčasť vašej vlastnej konfigurácie.

9. V okne **Konfiguračný sprievodca IBM Directory Server - Zadanie DN administrátora** kliknite na tlačidlo **Ďalej**.

10. Do poľa **Prípona** v okne **Konfiguračný sprievodca IBM Directory Server - Zadanie prípon** napíšte dc=my_co,dc=com.
11. V okne **Konfiguračný sprievodca IBM Directory Server - Zadanie prípon** kliknite na tlačidlo **Pridať**.
12. V okne **Konfiguračný sprievodca IBM Directory Server - Zadanie prípon** kliknite na tlačidlo **Ďalej**.
13. V okne **Konfiguračný sprievodca IBM Directory Server - Výber IP adries** vyberte voľbu **Áno, použiť všetky IP adresy**.
14. V okne **Konfiguračný sprievodca IBM Directory Server - Výber IP adries** kliknite na tlačidlo **Ďalej**.
15. V okne **Konfiguračný sprievodca IBM Directory Server - Zadanie preferencie TCP/IP** vyberte voľbu **Áno**.
16. V okne **Konfiguračný sprievodca IBM Directory Server - Zadanie preferencie TCP/IP** kliknite na tlačidlo **Ďalej**.
17. V okne **Konfiguračný sprievodca IBM Directory Server - Súhrn** kliknite na tlačidlo **Dokončiť**.
18. Pravým tlačidlom kliknite na **IBM Directory Server** a kliknite na tlačidlo **Spustiť**.

Krok 2: Konfigurácia webového administratívneho nástroja adresárového servera

1. V prehliadači zadajte adresu http://*myiSeries.my_co.com*:9080/IDSWebApp/IDSjsp/Login.jsp, pričom *myiSeries.my_co.com* je váš server iSeries.
2. Mala by sa objaviť prihlasovacia stránka. Kliknite na zoznam **Názov hostiteľa LDAP** a vyberte **Správa konzoly**. Ako meno užívateľa zadajte superadmin a ako heslo zadajte tajné. Kliknite na **Prihlásenie**.
3. Nakonfigurujte webový administračný nástroj, aby sa pripájal k serveru LDAP na vašom iSeries. V navigácii na ľavej strane vyberte **Správa konzoly —> Manažovanie serverov konzoly**.
4. Kliknite na **Pridať**.
5. V poli **Pridať server** zadajte myiSeries.my_co.com.
6. Kliknite na **Ok**. Nový server sa zobrazí v zozname pod **Manažovanie serverov konzoly**.
7. V navigácii na ľavej strane kliknite na **odhlásenie**.
8. Na prihlasovacej stránke webového administratívneho nástroja kliknite na zoznam **Názov hostiteľa LDAP** a vyberte server, ktorý ste práve nakonfigurovali (**myiSeries.my_co.com**).
9. V poli **Meno užívateľa** zadajte cn=administrator a v poli **Heslo** zadajte tajné. Kliknite na **Prihlásenie**.Mali by ste vidieť hlavnú stránku webového administračného nástroja pre IBM Directory Server.

Podrobný scenár: Vytvorenie adresárovej databázy

Skôr než začnete zadávať údaje, musíte vytvoriť miesto pre údaje, ktoré sa majú ukladať.

Krok 1: Vytvorenie objektu základného DN

1. Vo webovom administračnom nástroji kliknite na **Riadenie adresárov —> Riadiť položky**. V základnej úrovni adresára uvidíte zoznam objektov. Pretože je server nový, uvidíte len štrukturálne objekty, ktoré obsahujú konfiguračné informácie.
2. Chcete pridať nový objekt, ktorý má obsahovať údaje o spoločnosti MyCo, Inc.. Najprv kliknite na **Pridať...** na pravej strane okna. V ďalšom okne sa posúvajte v rámci zoznamu **Trieda objektov**, kde vyberte **doména** a kliknite na **Ďalej**.
3. Nechcete pridať žiadne pomocné triedy objektov, takže znova kliknite na **Ďalej**.
4. V okne **Zadanie atribútov** zadajte údaje, zodpovedajúce prípone, ktorú ste predtým vytvorili v sprievodcovi. Nechajte roletový zoznam **Trieda objektov** na **doména**. V poli **Príbuzné DN** zadajte dc=my_co. Do poľa **Rodičovské DN** napíšte dc=com. V poli **dc** zadajte my_co.
5. V spodnej časti okna kliknite na **Dokončiť**. Keď sa vrátite naspäť do základnej úrovne, mali by ste uvidieť nové základné DN.

Krok 2: Vytvorenie šablóny užívateľa

Ako pomôcku k pridávaniu údajov o zamestnancoch spoločnosti MyCo, Inc. si vytvoríte šablónu užívateľa.

1. Vo webovom administračnom nástroji kliknite na **Realmy a šablóny —> Pridať užívateľskú šablónu**.
2. V poli **Názov šablóny užívateľa** zadajte Zamestnanec.
3. Kliknite na tlačidlo **Prehľadávať...** vedľa poľa **Rodičovské DN**. Kliknite na základné DN **dc=my_co,dc=com**, ktoré ste vytvorili v predchádzajúcej časti a na pravej strane okna kliknite na **Výber**.
4. Kliknite na **Ďalej**
5. V roletovom zozname **Trieda štrukturálnych objektov**
6. vyberte **inetOrgPerson** a kliknite na **Ďalej**.
7. V roletovom zozname **Názvový atribút** vyberte **cn**.
8. V zozname **Záložky** vyberte **Vyžadované** a kliknite na **Úpravy**.
9. Okno **Úprava záložky** je tam, kde si vyberiete polia, ktoré sa majú začleniť do šablóny užívateľa. Vyžadujú sa **sn** a **cn**.
10. V zozname **Atribúty** vyberte **departmentNumber** a kliknite na **Pridať >>>**.
11. Vyberte **telephoneNumber** a kliknite na **Pridať >>>**.
12. Vyberte **pošta** a kliknite na **Pridať >>>**.
13. Vyberte **userPassword** a kliknite na **Pridať >>>**.
14. Kliknite na **OK** a na **Dokončiť**, čím bude vytvorená šablóna užívateľa.

Krok 3: Vytvorenie realmu

1. Vo webovom administratívnom nástroji kliknite na **Realmy a šablóny —> Pridať realm**.
2. V poli **Názov realmu** zadajte zamestnanci.
3. Na pravej strane poľa **Rodičovské DN** kliknite na **Prehliadať...** .
4. Na pravej strane okna vyberte rodičovské DN **dc=my_co,dc=com**, ktoré ste vytvorili a kliknite na **Výber**.
5. Kliknite na tlačidlo **Ďalej**.
6. V ďalšom okne už len zmeníte roletový zoznam **Šablóna užívateľa**. Vyberte šablónu užívateľa **cn=employees,dc=my_co,dc=com**, ktorú ste vytvorili.
7. Kliknite na **Dokončiť**.

Krok 4: Vytvorenie skupiny manažérov

1. Vytvorte skupinu manažérov.
   a. Vo webovom administračnom nástroji kliknite na **Užívatelia a skupiny —> Pridať skupinu**.
   b. V poli **Názov skupiny** zadajte manažéri.
   c. Zabezpečte, aby v roletovom zozname **Realm** bolo vybraté **zamestnanci**.
   d. Kliknite na **Dokončiť**.
2. Nakonfigurujte administrátora skupiny manažérov pre realm **zamestnanci**.
   a. Kliknite na **Realmy a šablóny —> Manažovanie realmov**.
   b. Vyberte realm **cn=employees,dc=my_co,dc=com**, ktorý ste vytvorili a kliknite na **Úprava**.
   c. Vpravo od poľa **Skupina administrátorov** kliknite na **Prehliadať...**.
   d. Vyberte **dc=my_co,dc=com** a kliknite na **Rozvinúť**.
   e. Vyberte **cn=employees** a kliknite na **Rozvinúť**.
   f. Vyberte **cn=managers** a kliknite na **Výber**.
   g. V okne **Úprava realmu** kliknite na **OK**.
3. Skupine manažérov dajte oprávnenie na používanie prípony **dc=my_co,dc=com**.
   a. Kliknite na **Manažovanie adresára —> Manažovanie položiek**.
   b. Vyberte **dc=my_co,dc=com** a kliknite na **Úprava ACL...**.
   c. V okne **Úprava ACL** kliknite na záložku **Vlastníci**.

d. Označte začiarkavacie políčko **Zverejnenie užívateľa**. Každý, kto je členom skupiny manažérov, sa stane vlastníkom stromu údajov **dc=my_co,dc=com**.
e. V roletovom zozname **Typ** vyberte **Skupina**.
f. V poli **DN (rozlišovací názov)** zadajte cn=managers,cn=employees,dc=my_co,dc=com.
g. Kliknite na **Pridať**.
h. Kliknite na **Ok**.

Krok 5: Pridanie užívateľa ako manažéra

1. Vo webovom administratívnom nástroji kliknite na **Užívatelia a skupiny —> Pridať užívateľa**.
2. V sťahovacej ponuke **Realm** vyberte vami vytvorený realm **zamestnanci** a kliknite na tlačidlo **Ďalej**.
3. V poli **cn** zadajte Jose Alvirez.
4. V poli ***sn** (priezvisko) zadajte Alvirez.
5. V poli ***cn** (celé meno) zadajte Jose Alvirez. cn sa používa na vytvorenie DN položky. *cn je atribút objektu.
6. V poli **telephoneNumber** zadajte 999 555 1234.
7. V poli **departmentNumber** zadajte DEPTA.
8. V poli **pošta** zadajte jalvirez@my_co.com.
9. V poli **userPassword** zadajte tajné.
10. Kliknite na záložku **Skupiny užívateľov**.
11. V zozname **Dostupné skupiny** vyberte **manažéri** a kliknite na **Pridať —>**.
12. V spodnej časti okna kliknite na **Dokončiť**.
13. Kliknutím na **Odhlásenie** v navigácii na ľavej strane sa odhláste z webového administratívneho nástroja.

Podrobný scenár: Zverejňovanie údajov iSeries do adresárovej databázy

Nakonfigurujte zverejňovanie, aby ste svojmu serveru iSeries umožnili automaticky zadávať informácie o užívateľoch do adresára LDAP. Informácie o užívateľoch zo systémového distribučného adresára sa zverejňujú do adresára LDAP.

Poznámka: Užívateľom, ktorí boli vytvorení pomocou iSeries Navigator, bude daný aj užívateľský profil aj položka užívateľa systémového distribučného adresára. Ak na vytváranie užívateľov používate CL príkazy, musíte vytvoriť aj užívateľský profil aj (**CRTUSRPRF**) aj položku užívateľa systémového distribučného adresára (**WRKDIRE**). Ak vaši užívatelia existujú len ako užívateľské profily a vy chcete, aby boli zverejnení do adresára LDAP, musíte pre nich vytvoriť položky užívateľov systémového distribučného adresára.

Krok:1 Urobte zo servera iSeries užívateľa adresárového servera

1. Prihláste sa do webového administračného nástroja (http://**myiSeries.my_co.com**:9080/IDSWebApp/IDSjsp/Login.jsp) ako administrátor.
   a. V zozname **Názov hostiteľa LDAP** vyberte **myiSeries.my_co.com**.
   b. Do poľa **Meno užívateľa** napíšte cn=administrator
   c. V poli **Heslo** zadajte tajné.
   d. Kliknite na **Prihlásenie**.
2. Vyberte **Užívatelia a skupiny —> Pridať užívateľa**.
3. V zozname **Realm** vyberte **zamestnanci**.
4. Kliknite na tlačidlo **Ďalej**.
5. Do poľa **cn** napíšte myiSeries.my_co.com.
6. Do poľa ***sn** napíšte myiSeries.my_co.com.
7. Do poľa ***cn** napíšte myiSeries.my_co.com.
8. V poli **userPassword** zadajte tajné.

9. Kliknite na záložku **Skupiny užívateľov**.
10. Vyberte skupinu **manažéri**.
11. Kliknite na **Pridať —>**.
12. Kliknite na **Dokončiť**.

Krok:2 Nakonfigurujte server iSeries pre zverejňovanie údajov

1. V aplikácii iSeries Navigator kliknite pravým tlačidlom na svoj iSeries v navigačnej oblasti po ľavej ruke a vyberte **Vlastnosti**.
2. V dialógovom okne **Vlastnosti** vyberte záložku **Adresárový server**.
3. Vyberte **Užívatelia** a kliknite na **Detaily**.
4. Označte začiarkavacie políčko **Zverejniť informácie o užívateľovi**.
5. V časti **Kde zverejniť** kliknite na tlačidlo **Úprava**. Zobrazí sa okno.
6. Zadajte myiSeries.my_co.com.
7. V poli **Pod DN** zadajte cn=employees,dc=my_co,dc=com.
8. V časti **Pripojenie servera** zabezpečte, aby v poli **Port** bolo zadané číslo štandardného portu **389**. V roletovom zozname **Metóda autentifikácie** vyberte **Rozlišovací názov** a v poli **Rozlišovací názov** zadajte cn=myiSeries,cn=employees,dc=my_co,dc=com.
9. Kliknite na **Heslo**.
10. V poli **Heslo** zadajte tajné.
11. V poli **Potvrdiť heslo** zadajte tajné.
12. Kliknite na **OK**.
13. Kliknite na tlačidlo **Overiť**. Tak sa presvedčíte, či ste všetky informácie zadali správne a či sa iSeries môže pripojiť k adresáru LDAP.
14. Kliknite na **OK**.
15. Kliknite na **OK**.

Podrobný scenár: Zadávanie informácií do adresárovej databázy

Jose Alvirez ako manažér teraz pridáva a aktualizuje údaje o jednotlivých osobách v jeho oddelení. Potrebuje pridať niekoľko ďalších informácií o Jane Doe. Jane Doe je užívateľ na serveri iSeries a informácie o nej boli zverejnené. Jose Alvirez potrebuje pridať aj informácie o Johnovi Smithovi. John Smith nie je užívateľom na serveri iSeries. Jose Alvirez bude postupovať nasledovne:

Krok 1: Prihláste sa do webového administračného nástroja

Prihláste sa na webový administratívny nástroj (http://**myiSeries.my_co.com**:9080/IDSWebApp/IDSjsp/Login.) a postupujte nasledovne:

1. V zozname **Názov hostiteľa LDAP** vyberte **myiSeries.my_co.com**.
2. V poli Meno užívateľa zadajte cn=Jose Alvirez,cn=myco employees,dc=my_co,dc=com.
3. V poli Heslo zadajte tajné.
4. Kliknite na **Prihlásenie**.

Krok 2: Zmeňte údaje o zamestnancoch

1. Kliknite na **Užívatelia a skupiny —> Manažovanie užívateľov**.
2. V zozname **Realm** vyberte **zamestnanci** a kliknite na **Zobrazenie užívateľov**.
3. V zozname užívateľov vyberte **Jane Doe** a kliknite na **Úprava**.
4. V poli **departmentNumber** zadajte DEPTA.
5. Kliknite na **OK**.
6. Kliknite na tlačidlo **Zatvoriť**.

Krok 3: Pridávanie údajov o zamestnancoch

1. Kliknite na **Užívatelia a skupiny —> Pridať užívateľa**.
2. V roletovom zozname **Realm** vyberte **zamestnanci** a kliknite na **Ďalej**.
3. V poli **cn** zadajte John Smith.
4. V poli ***sn** zadajte Smith.
5. V poli ***cn** zadajte John Smith.
6. V poli **telephoneNumber** zadajte 999 555 1235.
7. V poli **departmentNumber** zadajte DEPTA.
8. V poli **pošta** zadajte jsmith@my_co.com.
9. V spodnej časti okna kliknite na **Dokončiť**.

Podrobný scenár: Kontrola adresárovej databázy

Po zadaní údajov o zamestnancoch do adresárovej databázy túto databázu aj adresárový server skontrolujte nasledovne:

Adresárovú databázu prehľadajte pomocou vášho zoznamu e-mailových adries

Informácie v adresári LDAP možno jednoducho vyhľadať pomocou programov, podporujúcich LDAP. Mnohí poštoví klienti môžu prehľadávať adresárové servery LDAP ako súčasť funkcie ich zoznamu adries. Nasledujú vzorové procedúry pre konfiguráciu aplikácií Lotus Notes 6 a Microsoft Outlook Express 6. Procedúra pre väčšinu ostatných e-mailových klientov bude podobná.

Lotus Notes

1. Otvorte svoju knihu adries.
2. Kliknite na **Akcie —> Nové —> Konto**.
3. V poli **Názov konta** zadajte myiSeries.
4. V poli **Názov servera kont** zadajte myiSeries.my_co.com.
5. V poli **Protokol** vyberte **LDAP**.
6. Kliknite na záložku **Konfigurácia protokolu**.
7. V poli **Prehľadať základ** zadajte dc=my_co,dc=com.
8. Kliknite na **Uložiť a zatvoriť**.
9. Kliknite na **Vytvorenie —> Pošta —> Memo**.
10. Kliknite na **Adresa...**.
11. V poli **Výber zoznamu adries** vyberte myiSeries.
12. V poli **Vyhľadať koho** zadajte Alvirez.
13. Kliknite na **Vyhľadať**. Zobrazia sa údaje o Jose Alvirezovi.

Microsoft Outlook Express

1. Kliknite na **Nástroje —> Kontá**.
2. Kliknite na **Pridať —> Adresárové služby**.
3. Webovú adresu iSeries zadajte do poľa **Server internetových adresárov (LDAP)** (myiSeries.my_co.com).
4. Zrušte označenie začiarkavacieho políčka **Môj server LDAP žiada moje prihlásenie**.
5. Kliknite na tlačidlo **Ďalej**.
6. Kliknite na tlačidlo **Ďalej**.
7. Kliknite na **Dokončiť**.
8. Vyberte myiSeries.my_co.com (adresárová služba, ktorú ste práve nakonfigurovali) a kliknite na **Vlastnosti**.

9. Kliknite na tlačidlo **Rozšírené**.
10. Do poľa **Základ hľadania** napíšte dc=my_co,dc=com.
11. Kliknite na **Ok**.
12. Kliknite na tlačidlo **Zatvoriť**.
13. Použite Ctrl+E a otvorte okno **Hľadať osoby**.
14. Zo zoznamu **Pozrieť do** vyberte myiSeries.my_co.com.
15. V poli **Meno** zadajte Alvirez.
16. Kliknite na **Hľadať teraz**. Zobrazia sa údaje o Jose Alvirezovi.

Prehľadávanie adresárovej databázy zadaním príkazu ldapsearch do príkazového riadka

1. V znakovom rozhraní zadajte príkaz CL **QSH** a otvorte reláciu Qshell.
2. Aby ste získali zoznam všetkých položiek LDAP v databáze, zadajte:

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

   Pričom:

   –h je názov hostiteľského počítača, na ktorom beží server LDAP.

   –b je základný DN, pod ktorým sa má vyhľadávať.

   objectclass=*
   vracia všetky položky v adresári.

   Tento príkaz vracia približne toto:

   ```
    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

   .
   .
   .
   ```

   Prvý riadok každej položky sa nazýva rozlišovací názov (DN). Názvy DN sú čosi ako názov celého súboru každej položky. Niektoré položky neobsahujú údaje a sú len štrukturálne. Položky s riadkom **objectclass=inetOrgPerson** zodpovedajú položkám, ktoré ste vytvorili pre osoby. DN Joseho Alvireza je **cn=Jose Alvirez,cn=MyCo Employees,dc=my_co,dc=com**.

Kapitola 7. Správa adresárového servera

Ak chcete spravovať adresárový server, vami používaný užívateľský profil musí mať nasledujúce oprávnenie:

- Ak chcete server nakonfigurovať alebo zmeniť jeho konfiguráciu, musíte mať špeciálne oprávnenia na všetky objekty (*ALLOBJ) a na I/O konfiguráciu systému (*IOSYSCFG).
- Ak chcete spustiť alebo zastaviť server, musíte mať oprávnenie na riadenie úlohy (*JOBCTL) a oprávnenie na objekt na príkazy ENDTCP (End TCP/IP), STRTCP (Start TCP/IP), STRTCPSVR (Start TCP/IP Server) a ENDTCPSVR (End TCP/IP Server).
- Ak chcete nastaviť správanie auditovania pre adresárový server, musíte mať špeciálne oprávnenie na audit (*AUDIT).
- Ak si chcete prezerať protokol úlohy servera, musíte mať špeciálne oprávnenie na spoolové riadenie (*SPLCTL).

Na spravovanie objektov adresára (vrátane zoznamov riadenia prístupu, vlastníctva objektov, a replík) sa do adresára pripojte buď s DN, administrátora alebo s takým DN, ktoré má zodpovedajúce oprávnenie LDAP. Ak sa práve používa integrácia oprávnení, administrátor môže byť aj projektovaným užívateľom (pozrite si “Projektované pozadie operačného systému” na strane 73), ktorý má oprávnenie na ID funkcie administrátora adresárového servera. Väčšinu administračných úloh môžu vykonať aj užívatelia v administračnej skupine (pozrite si“Administratívny prístup” na strane 54).

Úlohy všeobecnej správy

Bezpečnostné úlohy

- “Povolenie autentifikácie Kerberos na adresárovom serveri” na strane 151
- “Konfigurácia autentifikácie DIGEST-MD5 na adresárovom serveri” na strane 151

Úlohy obsahu adresára
- “Manažovanie schémy” na strane 152
- “Manažovanie položiek adresára” na strane 162
- “Manažovanie užívateľov a skupín” na strane 169
- “Manažovanie realmov a šablón užívateľov” na strane 172
- “Manažovanie zoznamov riadenia prístupu (ACL)” na strane 179

Úlohy publikovania
- “Publikovanie informácií na adresárový server” na strane 90

Spustenie/zastavenie adresárového servera

Ak chcete spustiť adresárový server, postupujte nasledovne:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte voľbu **Spustiť**.

   Spustenie adresárového servera môže trvať niekoľko minút, v závislosti od rýchlosti vášho servera a od množstva dostupnej pamäte. Prvé spustenie vášho adresárového servera môže trvať o niekoľko minút dlhšie ako je bežné, pretože server musí vytvoriť nové súbory. Podobné je to pri prvom spustení adresárového servera po rozšírení zo staršej verzie Adresárový server. Spúšťanie môže trvať o niekoľko minút dlhšie ako je bežné, pretože server musí migrovať súbory. Ak chcete vidieť, či sa adresárový server už spustil, môžete pravidelne kontrolovať stav servera (pozri “Kontrola stavu adresárového servera” na strane 109).

Adresárový server možno spustiť aj zo znakového rozhrania zadaním príkazu STRTCPSVR *DIRSRV. Prípadne, ak ste váš adresárový server nakonfigurovali na naštartovanie počas spúšťania TCP/IP, môžete ho naštartovať zadaním príkazu STRTCP.

Len konfiguračný režim

Adresárový server možno spustiť len v konfiguračnom režime zo znakového rozhrania zadaním príkazu TRCTCPAPP APP(*DIRSRV) ARGLIST(SAFEMODE).

Len konfiguračný režim spúšťa server len s aktívnou príponou cn=configuration a nezávisí od úspešnej inicializácie serverov.

Ak chcete zastaviť adresárový server, postupujte nasledovne:

Zastavenie adresárového servera má vplyv na všetky aplikácie používajúce server v čase jeho zastavenia. Zahŕňa to aj aplikácie EIM (Enterprise Identity Mapping), ktoré momentálne používajú adresárový server pre operácie EIM. Všetky aplikácie sú z adresárového servera odpojené, avšak môžu sa snažiť o opätovné pripojenie k serveru.

Ak chcete zastaviť adresárový server, postupujte nasledovne:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte voľbu **Zastaviť**.

   Zastavenie adresárového servera môže trvať niekoľko minút, v závislosti od rýchlosti vášho systému, množstva aktivity servera a množstva dostupnej pamäte. Ak chcete vidieť, či sa adresárový server už spustil, môžete pravidelne kontrolovať stav servera (pozri “Kontrola stavu adresárového servera” na strane 109).

Poznámka: Adresárový server sa tiež dá zastaviť z relácie 5250 zadaním príkazov ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL alebo ENDTCP. ENDTCPSVR *ALL a ENDTCP tiež ovplyvňujú všetky ďalšie TCP/IP servery, ktoré pracujú na vašom systéme. ENDTCP tiež ukončí samotný TCP/IP.

Kontrola stavu adresárového servera

Základné informácie o stave nájdete v aplikácii iSeries Navigator. Rozšírené a ucelenejšie informácie o stave nájdete pomocou webového administračného nástroja.

iSeries Navigator zobrazí stav adresárového servera v stĺpci **Stav** v ľavom rámiku.

Ak chcete skontrolovať stav adresárového servera v aplikácii iSeries Navigator, postupujte nasledovne:
1. Rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**. iSeries Navigator zobrazí stav všetkých TCP/IP serverov, vrátane adresárového servera v stĺpci **Stav**. Na aktualizovanie stavu serverov kliknite na menu **Zobraziť** a vyberte **Aktualizovať**.
4. Ak si chcete zobraziť bližšie informácie o stave adresárového servera, kliknite pravým tlačidlom na **IBM Directory Server** a vyberte voľbu **Stav**. Ten zobrazí počet aktívnych spojení, ako aj iné informácie, napríklad minulé a aktuálne úrovne aktivity.

   Okrem získania ďalších informácií môžete prezeraním stavu touto voľbou ušetriť čas. Stav adresára môžete aktualizovať bez zbytočného plytvania časom, ktorý sa vyžaduje pri zisťovaní stavu iných serverov TCP/IP.

Ak si chcete zobraziť stav adresárového servera pomocou webového administračného nástroja, postupujte nasledovne:
1. V navigačnej oblasti rozviňte kategóriu **Správa servera**.

   Poznámka: Ak chcete konfiguračné nastavenia servera zmeniť pomocou úloh z kategórie Správa servera vo webovom administračnom nástroji, musíte sa na server autentifikovať ako užívateľský profil i5/OS, ktorý má mimoriadne oprávnenia *ALLOBJ a IOSYSCFG. Docielite to autentifikáciou ako projektovaný užívateľ s heslom pre takýto profil. Ak chcete z webového administračného nástroja vytvoriť väzby ako projektovaný užívateľ, zadajte meno užívateľa vo forme os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, pričom reťazce MYUSERNAME a MYSYSTEM.COM budú nahradené názvom vášho užívateľského profilu a príponou projekcie nakonfigurovaného systému.
2. Kliknite na **Zobraziť stav servera**.
3. V paneli **Zobraziť stav servera** vyberte rozličné záložky pre zobrazenie informácií o stave.

Kontrola úloh na adresárovom serveri

Vždy keď budete chcieť monitorovať špecifické úlohy v adresárovom serveri. Ak chcete skontrolovať úlohy servera v aplikácii iSeries Navigator, postupujte nasledovne:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte voľbu **Úlohy servera**.

Riadenie pripojení servera

Administrátor si častokrát potrebuje zobraziť pripojenia k serveru a operácie, ktoré tieto pripojenia vykonávajú. Administrátor sa potom môže rozhodnúť ako má riadiť prístup a zamedziť DoS útokom. robí sa to prostredníctvom webového administračného nástroja.

V navigačnej oblasti rozviňte kategóriu **Správa servera**.Kliknite na **Riadiť pripojenia servera**. Zobrazí sa tabuľka, v ktorej budú pri každom pripojení uvedené nasledujúce informácie:

Poznámka: Ak chcete konfiguračné nastavenia servera zmeniť pomocou úloh z kategórie Správa servera vo webovom administračnom nástroji, musíte sa na server autentifikovať ako užívateľský profil i5/OS, ktorý má mimoriadne oprávnenia *ALLOBJ a IOSYSCFG. Docielite to autentifikáciou ako projektovaný užívateľ s heslom pre takýto profil. Ak chcete z webového administračného nástroja vytvoriť väzby ako projektovaný užívateľ, zadajte meno užívateľa vo forme os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, pričom reťazce MYUSERNAME a MYSYSTEM.COM budú nahradené názvom vášho užívateľského profilu a príponou projekcie nakonfigurovaného systému.

DN Špecifikuje DN klientskeho pripojenia k serveru.

IP adresa
Špecifikuje IP adresu klienta, ktorý má pripojenie k serveru.

Čas spustenia
Špecifikuje dátum a čas (v miestom čase servera), kedy bolo pripojenie vytvorené.

Stav Špecifikuje, či je pripojenie aktívne alebo nečinné. Pripojenie sa považuje za aktívne, ak na ňom prebiehajú nejaké operácie.

Inicializované operácie
Špecifikuje počet operácií, ktoré boli požadované od vytvorenia pripojenia.

Dokončené operácie
Špecifikuje počet operácií, ktoré boli pre každé pripojenie dokončené.

Typ Špecifikuje, či je pripojenie zabezpečené pomocou SSL alebo TLS. Inak je pole prázdne.

Poznámka: V tejto tabuľke sa môže naraz zobraziť až 20 pripojení.

Môžete zadať, aby sa táto tabuľka zobrazovala buď podľa DN alebo podľa IP adresy, keď rozviniete sťahovaciu ponuku v záhlaví panelu a vyberiete si. Predvolený výber je podľa DN. Podobne môžete zadať, či sa má tabuľka zobraziť vo vzostupnom alebo v zostupnom usporiadaní.

Ak chcete aktualizovať aktuálne informácie o pri pojeniach, kliknite na **Obnoviť**.

Ak ste prihlásený ako administrátor alebo ako člen administračnej skupiny, môžete vykonať ďalšie výbery pre odpojenie pripojení servera, ktoré sú k dispozícii v paneli. Táto schopnosť odpojiť pripojenia servera vám dovoľuje zastaviť DoS útoky a riadiť prístup na server. Pripojenie môžete odpojiť, keď rozviniete sťahovacie ponuky a vyberiete DN, IP adresu alebo obidve a kliknete na **Odpojiť**.

Ak chcete odpojiť všetky pripojenia servera, okrem toho, ktoré prináša túto požiadavku, kliknite na **Odpojiť všetko**. Zobrazí sa varovanie s potvrdením. Kliknite na tlačidlo **OK**, ak chcete pokračovať v odpojovaní alebo kliknite na tlačidlo **Zrušiť**, ak chcete akciu ukončiť a vrátiť sa do panelu **Riadiť pripojenia servera**.

Bližšie informácie o tom ako zamedziť DoS útokom nájdete v “Riadenie vlastností pripojenia”.

Riadenie vlastností pripojenia

Schopnosť riadiť vlastnosti pripojení vám dovoľuje zamedziť klientom, aby zablokovali server. Tiež zaručuje, že administrátor bude mať vždy prístup na server v prípadoch, keď je zálohovací proces trvalo zaneprázdnený dlhodobo spustenými úlohami. Riadenie vlastností pripojenia sa vykonáva prostredníctvom webového administračného nástroja.

Poznámka: Tieto výbery sa zobrazia iba vtedy, ak ste sa na server, ktorý podporuje túto funkciu, prihlásili ako administrátor alebo člen administračnej skupiny.

Ak chcete nastaviť vlastnosti pripojenia, postupujte nasledovne:

1. V navigačnej oblasti rozviňte kategóriu **Správa servera** a kliknite na **Riadiť vlastnosti pripojenia**.

Poznámka: Ak chcete konfiguračné nastavenia servera zmeniť pomocou úloh z kategórie Správa servera vo webovom administračnom nástroji, musíte sa na server autentifikovať ako užívateľský profil i5/OS, ktorý má mimoriadne oprávnenia *ALLOBJ a IOSYSCFG. Docielite to autentifikáciou ako projektovaný užívateľ s heslom pre takýto profil. Ak chcete z webového administračného nástroja vytvoriť väzby ako projektovaný užívateľ, zadajte meno užívateľa vo forme os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, pričom reťazce MYUSERNAME a MYSYSTEM.COM budú nahradené názvom vášho užívateľského profilu a príponou projekcie nakonfigurovaného systému.

2. Vyberte záložku **Všeobecné**.
3. Nastavte nastavenie anonymného pripojenia. Zaškrtávacie políčko **Povoliť anonymné pripojenia** je už vybraté, preto je vytváranie anonymných väzieb dovolené. Je to predvolené nastavenie. Ak chcete zrušiť výber zaškrtávacieho políčka **Povoliť anonymné pripojenia**, kliknite naň. Táto akcia spôsobí, že server zruší väzby všetkých anonymných pripojení.

   Poznámka: Ak nepovolíte vytváranie anonymných väzieb, niektoré aplikácie môžu zlyhať.
4. V poli **Prah čistenia pre anonymné pripojenia** nastavte číslo prahu pre inicializáciu zrušenia väzieb anonymných pripojení. Môžete zadať číslo od 0 do 65535.

   Poznámka: Skutočný maximálny počet je ohraničený počtom súborov, ktoré sú povolené pre jeden proces. V systémoch UNIX môžete na zistenie limitov použiť príkaz **ulimit -a**. V systémoch Windows je tento počet pevne stanovený.

   Predvolené nastavenie je 0. Keď bude tento počet anonymných pripojení prekročený, pripojenia budú vyčistené na základe limitu pre uplynutie vyhradeného času nečinnosti, ktorý ste nastavili v poli **Uplynutie vyhradeného času nečinnosti**.
5. V poli **Prah čistenia pre autentifikované pripojenia**nastavte číslo prahu pre inicializáciu zrušenia väzieb autentifikovaných pripojení. Môžete zadať číslo od 0 do 65535.

   Poznámka: Skutočný maximálny počet je ohraničený počtom súborov, ktoré sú povolené pre jeden proces. V systémoch UNIX môžete na zistenie limitov použiť príkaz ulimit -a. V systémoch Windows je tento počet pevne stanovený.

   Predvolené nastavenie je 1100. Keď bude tento počet autentifikovaných pripojení prekročený, pripojenia budú vyčistené na základe limitu pre uplynutie vyhradeného času nečinnosti, ktorý ste nastavili v poli **Uplynutie vyhradeného času nečinnosti**.
6. V poli **Prah čistenia pre všetky pripojenia** nastavte číslo prahu pre inicializáciu zrušenia väzieb všetkých pripojení. Môžete zadať číslo od 0 do 65535.

   Poznámka: Skutočný maximálny počet je ohraničený počtom súborov, ktoré sú povolené pre jeden proces. V systémoch UNIX môžete na zistenie limitov použiť príkaz ulimit -a. V systémoch Windows je tento počet pevne stanovený.

   Predvolené nastavenie je 1200. Keď bude tento celkový počet pripojení prekročený, pripojenia budú vyčistené na základe limitu pre uplynutie vyhradeného času nečinnosti, ktorý ste nastavili v poli **Uplynutie vyhradeného času nečinnosti**.
7. V poli **Limit pre uplynutie vyhradeného času nečinnosti** nastavte počet sekúnd, počas ktorých môže byť pripojenie nečinné, kým ho zatvorí proces čistenia. Môžete zadať číslo od 0 do 65535.

   Poznámka: Skutočný maximálny počet je ohraničený počtom súborov, ktoré sú povolené pre jeden proces. V systémoch UNIX môžete na zistenie limitov použiť príkaz ulimit -a. V systémoch Windows je tento počet pevne stanovený.

   Predvolené nastavenie je 300. Keď sa inicializuje proces čistenia, všetky pripojenia, okrem procesu, ktoré prekračujú limit budú zatvorené.
8. V poli **Limit pre uplynutie vyhradeného času výsledkov** nastavte počet sekúnd, ktoré môžu uplynúť medzi pokusmi o zápis. Môžete zadať číslo od 0 do 65535.Predvolené nastavenie je 120. Všetky pripojenia, ktoré prekračujú tento limit, budú ukončené.

Poznámka: Vzťahuje sa to len na systémy Windows. Operačný systém automaticky zruší pripojenie, ktoré prekračuje 30 sekúnd. Z tohto dôvodu operačný systém vyradí toto nastavenie pre **Limit pre uplynutie vyhradeného času výsledkov** po 30 sekundách.

9. Kliknite na záložku **Núdzové vlákno**.
10. Nastavte nastavenie núdzového vlákna. Zaškrtávacie políčko **Povoliť núdzové vlákno** je už vybraté, preto môže byť núdzové vlákno aktivované. Je to predvolené nastavenie. Ak chcete zrušiť výber zaškrtávacieho políčka **Povoliť núdzové vlákno**, kliknite naň. Táto akcia zamedzí aktivácii núdzového vlákna.
11. V poli **Prah čakajúcich požiadaviek** nastavte číselný limit pre pracovné požiadavky, ktoré aktivujú núdzové vlákno. Zadajte číslo od 0 do 65535, aby ste nastavili limit pracovných požiadaviek, ktoré sa môžu nachádzať vo fronte pred aktiváciou núdzového vlákna. Predvolená hodnota je 50. Keď bude zadaný limit prekročený, núdzové vlákno sa aktivuje.
12. V poli **Časový prah** nastavte počet minút, ktoré môžu uplynúť od posledného odstránenia pracovnej položky z frontu. Ak sa vo fronte nachádzajú pracovné položky a tento limit bude prekročený, núdzové vlákno sa aktivuje. Môžete zadať číslo od 0 do 240. Predvolené nastavenie je 5.
13. Zo sťahovacej ponuky vyberte kritériá, ktoré sa majú použiť na aktiváciu núdzového vlákna. Vyberať môžete z týchto:
    - **Iba veľkosť:** Núdzové vlákno sa aktivuje len vtedy, keď front prekročí zadané množstvo čakajúcich pracovných položiek.
    - **Iba čas:** Núdzové vlákno sa aktivuje len vtedy, keď časový limit medzi odstránenými pracovnými položkami prekročí zadané množstvo.
    - **Veľkosť alebo čas:** Núdzové vlákno sa aktivuje, keď dôjde k prekročeniu veľkosti frontu alebo časového prahu.
    - **Veľkosť a čas:** Núdzové vlákno sa aktivuje, keď zadané množstvá prekročia veľkosť frontu aj časový prah.

    Predvoleným nastavením je Veľkosť a čas.
14. Kliknite na tlačidlo **OK**

Ďalšie informácie nájdete v časti “Riadenie pripojení servera” na strane 109.

Povoliť notifikáciu udalostí

Adresárový server podporuje notifikáciu udalostí, čo klientom umožňuje registrovať sa na serveri LDAP a dostávať notifikáciu o určitej udalosti, ako je napríklad pridanie položky do adresára.

Ak chcete umožniť notifikáciu udalostí pre váš server, postupujte podľa nasledujúcich krokov:

1. V navigačnej oblasti webového administračného nástroja rozviňte kategóriu **Riadiť vlastnosti servera** a vyberte záložku **Oznámenie o udalosti**.
2. Ak chcete povoliť oznamovanie udalostí, vyberte zaškrtávacie políčko **Povoliť oznámenie o udalosti**. Ak je políčko**Povoliť oznámenie o udalosti**zakázané, server bude ignorovať všetky ostatné voľby v tomto paneli.
3. Nastavte **Maximálny počet registrácií na pripojenie**. Buď kliknite na prepínač **Registrácie** alebo na prepínač **Neobmedzené**. Ak vyberiete **Registrácie** musíte v poli zadať maximálny počet registrácií, ktoré budú pre každé pripojenie povolené. Maximálny počet transakcií je 2 147 483 647. Predvolené nastavenie je 100 registrácií.
4. Nastavte **Maximálny počet registrácií celkovo**. Tento výber nastaví, počet registrácií, ktoré môže mať server kedykoľvek. Buď kliknite na prepínač **Registrácie** alebo na prepínač **Neobmedzené**. Ak vyberiete **Registrácie** musíte v poli zadať maximálny počet registrácií, ktoré budú pre každé pripojenie povolené. Maximálny počet transakcií je 2 147 483 647. Predvolený počet registrácií je **Neobmedzené**.
5. Ak už budete mať všetko hotové, kliknite na tlačidlo **Použiť** a zmeny sa uložia bez ukončenia panelu, alebo kliknite na tlačidlo **OK** a zmeny sa uložia aj s ukončením panelu, alebo kliknite na tlačidlo **Zrušiť** a tento panel sa ukončí bez vykonania zmien.
6. Ak ste povolili oznamovanie udalostí, musíte server reštartovať, aby sa zmeny prejavili. Ak ste upravovali iba nastavenia, server nemusíte reštartovať.

Poznámka: Ak chcete zakázať oznamovanie udalostí, zrušte výber zaškrtávacieho políčka **Povoliť oznámenia o udalostiach** a reštartujte server.

Ďalšie informácie o oznamovaní udalostí nájdete v časti Oznamovanie udalostí v príručke IBM Directory Server Version 5.2 Programming Reference.

Uviesť nastavenie transakcie

Adresárový server podporuje transakcie, ktoré umožňujú, aby sa so skupinou operácií adresára LDAP postupovalo, ako s jednou jednotkou. Ďalšie informácie nájdete v časti “Transakcie” na strane 46.

Ak chcete nakonfigurovať nastavenia transakcií svojich serverov, postupujte takto:

1. V navigačnej oblasti webového administračného nástroja rozviňte kategóriu **Riadiť vlastnosti servera** a vyberte záložku **Transakcie**.
2. Ak chcete povoliť spracovanie transakcií, vyberte zaškrtávacie políčko**Povoliť spracovanie transakcií**. Ak je políčko**Povoliť spracovanie transakcií** zakázané, server bude všetky ostatné voľby na tomto paneli, ako napríklad **Maximálny počet operácií na transakciu** a **Čakajúci časový limit**, ignorovať.
3. Nastavte **Maximálny počet transakcií**. Buď kliknite na prepínač **Transakcie** alebo na prepínač **Neobmedzené**. Ak vyberiete**Transakcie**, musíte v poli zadať maximálny počet transakcií. Maximálny počet transakcií je 2 147 483 647. Predvolené nastavenie je 20 transakcií.
4. Nastavte **Maximálny počet operácií na transakciu**. Buď kliknite na prepínač **Operácie** alebo na prepínač **Neobmedzené**. Ak vyberiete **Operácie**, musíte v poli zadať maximálny počet operácií, ktoré budú pre každú transakciu povolené. Maximálny počet operácií je 2 147 483 647. Čím je počet nižší, tým je výkon lepší. Predvolené nastavenie je 5 operácií.
5. Nastavte **Čakajúci časový limit**. Tento výber nastaví maximálnu hodnotu pre uplynutie vyhradeného času čakajúcej transakcie v sekundách. Buď kliknite na prepínač **Sekundy** alebo na prepínač **Neobmedzené**. Ak vyberiete**Sekundy**, musíte v poli zadať maximálny počet sekúnd, ktoré sú pre každú transakciu povolené. Maximálny počet sekúnd je 2 147 483 647. Transakcie, ktoré zostanú nedokončené dlhšie ako je tento čas, budú zrušené (vrátené). Predvolené nastavenie je 300 sekúnd.
6. Ak už budete mať všetko hotové, kliknite na tlačidlo **Použiť** a zmeny sa uložia bez ukončenia panelu, alebo kliknite na tlačidlo **OK** a zmeny sa uložia aj s ukončením panelu, alebo kliknite na tlačidlo **Zrušiť** a tento panel sa ukončí bez vykonania zmien.
7. Ak ste povolili podporu transakcií, musíte server reštartovať, aby sa zmeny prejavili. Ak ste upravovali iba nastavenia, server nemusíte reštartovať.

Poznámka: Ak chcete zakázať spracovanie transakcií, zrušte výber zaškrtávacieho políčka **Povoliť spracovanie transakcií** a reštartujte server.

Zmena portu alebo adresy IP

Adresárový server používa nasledujúce štandardné porty:

- 389 pre nezabezpečené pripojenia.
- 636 pre zabezpečené pripojenia (ak ste použili Správcu digitálnych certifikátov na povolenie adresárového servera, ako tej aplikácie, ktorá môže použiť bezpečný port).

Poznámka: Štandardne sú všetky adresy IP definované na lokálnom systéme pripojené na server.

Ak už tieto porty používate pre ďalšie aplikácie, môžete adresárovému serveru priradiť iný port, alebo môžete pre tieto dva servery použiť iné adresy IP, ak aplikácie podporujú pripojenie k špecifickej adrese IP.

Príklad konfliktu LDAP servera Domino s adresárovým serverom nájdete v časti Hostiteľský LDAP server Domino a adresárový server na rovnakom iSeries

Ak chcete zmeniť porty, ktoré používa adresárový server, postupujte nasledovne:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte **Vlastnosti**.
5. Kliknite na záložku **Sieť**.
6. Zadajte vhodné čísla portov a potom kliknite na **OK**.

Ak chcete zmeniť adresu IP, na ktorej adresárový server prijíma pripojenia, vykonajte tieto kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte **Vlastnosti**.
5. Kliknite na záložku **Sieť**.
6. Kliknite na tlačidlo **Adresy IP...**.
7. Vyberte si **Použiť vybranú adresu IP** a zvoľte si adresy IP pre server, ktoré sa majú použiť, keď sa prijímajú pripojenia.

Zadanie servera pre odvolávky na adresár

Ak chcete adresárovému serveru priradiť servery odvolávok, postupujte nasledovne:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **IBM Directory Server**, a potom vyberte **Vlastnosti**.
5. Vyberte si stránku s vlastnosťami **Všeobecné**.
6. V poli **Nová odvolávka** zadajte URL servera odvolávok.
7. Uveďte názov servera odvolávok vo formáte URL. Nasledujú príklady prijateľných LDAP URL:
   - ldap://test.server.com
   - ldap://test.server.com:400
   - ldap://9.9.99.255

   Poznámka: Ak server odvolávok nepoužíva štandardný port, uveďte správne číslo portu ako súčasť URL, keďže port 400 je zadaný v druhom vyššie uvedenom príklade.
8. Kliknite na **Pridať**.
9. Kliknite na **OK**.

Pridávanie a odstraňovanie prípon adresárového servera

Pridanie prípony do adresárového servera umožňuje serveru riadiť danú časť adresárového stromu.

Poznámka: Nemôžete pridávať príponu, ktorá sa už nachádza na serveri pod ďalšou príponou. Ak boli napríklad o=ibm, c=us príponou na vašom serveri, nemôžete pridávať ou=rochester, o=ibm, c=us.

Na pridanie prípony do adresárového servera vykonajte tieto kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte **Vlastnosti**.
5. Kliknite na záložku **Databáza/Prípony**.
6. V poli **Nová prípona** napíšte názov novej prípony.
7. Kliknite na **Pridať**.
8. Kliknite na **OK**.

Poznámka: Pridanie prípony nasmeruje server do časti adresára, ale nevytvorí žiadne objekty. Ak objekt, ktorý zodpovedá novej prípone predtým neexistoval, musíte ho vytvoriť rovnako, ako by ste vytvorili hocijaký iný objekt.

Pri odstraňovaní prípony z adresárového servera postupujte nasledovne:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte **Vlastnosti**.
5. Kliknite na záložku **Databáza/Prípony**.
6. Kliknutím označte príponu, ktorú chcete odstrániť.
7. Kliknite na **Odstrániť**.

Poznámka: Môžete si zvoliť vymazanie prípony bez vymazania objektov adresára, ktoré sú pod ňou. To zmení údaje na neprístupné z adresárového servera. Avšak spätným pridaním prípony môžete neskôr tieto údaje získať znova.

Ukladanie a obnova informácií adresárového servera

Adresárový server ukladá informácie na nasledujúce miesta:

- Knižnica databázy (QUSRDIRDB by default), ktorá obsahuje obsah adresárových serverov.

  Poznámka: Vami používanú knižnicu databázy môžete vidieť na záložke **Databázy/Prípony** panelu Vlastnosti IBM Directory Server v aplikácii iSeries Navigator.
- Knižnica QDIRSRV2, ktorá slúži na ukladanie publikačných informácií.
- Knižnica QUSRSYS, ktorá uchováva rôzne položky v objektoch začínajúcich na QGLD (pre ich uloženie zadajte QUSRSYS/QGLD*).
- Ak konfigurujete adresárový server na protokolovanie zmien adresára, používa sa databázový server s názvom QUSRDIRCL, ktorý používa protokol zmien.

Ak sa obsah adresára pravidelne mení, mali by ste si pravidelne ukladať databázovú knižnicu a objekty v nej. Konfiguračné údaje sú uložené v adresári:

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

Pri každej zmene konfigurácie alebo používaní PTF by ste mali uložiť v tomto adresári aj súbory.

Informácie o ukladaní a obnove údajov nájdete v publikáciiZálohovanie a obnova, SC41-5304 .

Pridelenie administrátorského prístupu projektovaným užívateľom

Administrátorovi môžete udeliť prístup k užívateľským profilom, ktorým bol daný prístup k identifikátoru (ID) funkcie administrátora adresárového servera (QIBM_DIRSRV_ADMIN).

Ak je napríklad užívateľskému profilu JOHNSMITH udelený prístup k ID funkcie administrátora adresárového servera a z dialógu vlastností adresára je vybraný prístup administrátora Grant k voľbe autorizovaných užívateľov, profil JOHNSMITH bude mať potom oprávnenie administrátora LDAP. Keď sa tento profil použije na pripojenie k adresárovému serveru pomocou nasledujúceho DN, os400-profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com, užívateľ bude mať oprávnenie administrátora. Prípona systémových objektov bude v tomto príklade os400-sys=systemA.acme.com. Viac informácií o projektovaných užívateľoch nájdete v časti “Projektované pozadie operačného systému” na strane 73.

Ak si chcete zvoliť túto voľbu, postupujte takto:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.

3. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
4. Na záložke **Všeobecné** pod **Informáciami administrátora** si zvoľte voľbu **Udeliť prístup administrátora oprávneným užívateľom**.

Pri nastavovaní ID funkcie oprávnenia administrátora adresárového servera v užívateľskom profile postupujte nasledovne:

1. V iSeries Navigator kliknite pravým tlačidlom myši na systémový názov a zvoľte si **Správu aplikácie**.
2. Kliknite na záložku **Hostiteľské aplikácie**.
3. Rozviňte **Operating System/400**.
4. Kliknutím na **Správcu adresárového servera** vysvieťte voľbu.
5. Kliknite na tlačidlo **Upraviť**.
6. Rozviňte **Užívatelia**, **Skupiny** alebo **Užívatelia mimo skupiny**, čo sa hodí pre požadovaného užívateľa.
7. Zvoľte si užívateľa alebo skupinu, ktorú chcete pridať na zoznam **Povolených prístupov**.
8. Kliknite na tlačidlo **Pridať**.
9. Kliknutím na **OK** uložte zmeny.
10. Kliknite na **OK** v dialógu **Správa aplikácie**.

Práca s administračnou skupinou

Administračná skupina poskytuje schopnosť poskytovať administračné schopnosti bez nutnosti zdieľania jedného ID a hesla medzi administrátormi. Členovia administračnej skupiny majú svoje vlastné jedinečné ID a heslá. DN členov administračnej skupiny sa nesmú medzi sebou zhodovať a tiež sa nesmú zhodovať s DN administrátora IBM Directory Server. A naopak DN administrátora IBM Directory Server sa nesmie zhodovať s DN žiadneho člena administračnej skupiny.

Toto pravidlo platí aj pre Kerberos alebo pre ID Digest-MD5 administrátora servera IBM Directory Server a členov administračnej skupiny. Tieto DN sa nesmú zhodovať so žiadnymi DN dodávateľov replikácie IBM Directory Server. To však znamená, že DN dodávateľov replikácie IBM Directory Server sa nesmú zhodovať so žiadnym DN člena administračnej skupiny ani s DN administrátora IBM Directory Server.

Poznámka: DN dodávateľov replikácie IBM Directory Server sa môžu medzi sebou zhodovať.

Bližšie informácie nájdete v:

- “Povolenie administračnej skupiny”
- “Pridanie, úpravy a odstránenie členov administračnej skupiny” na strane 117

Súvisiace informácie

“Administratívny prístup” na strane 54

Povolenie administračnej skupiny

Ak chcete vykonať túto operáciu musíte byť administrátorom IBM Directory Server.

1. V navigačnej oblasti rozviňte kategóriu **Správa servera** a kliknite na **Riadiť administračnú skupinu**.

Poznámka: Ak chcete konfiguračné nastavenia servera zmeniť pomocou úloh z kategórie Správa servera vo webovom administračnom nástroji, musíte sa na server autentifikovať ako užívateľský profil i5/OS, ktorý má mimoriadne oprávnenia *ALLOBJ a IOSYSCFG. Docielite to autentifikáciou ako projektovaný užívateľ s heslom pre takýto profil. Ak chcete z webového administračného nástroja vytvoriť väzby ako projektovaný užívateľ, zadajte meno užívateľa vo forme os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, pričom reťazce MYUSERNAME a MYSYSTEM.COM budú nahradené názvom vášho užívateľského profilu a príponou projekcie nakonfigurovaného systému.

2. Ak chcete povoliť alebo zakázať administračnú skupinu, kliknite na zaškrtávacie políčko vedľa voľby **Povoliť administračnú skupinu**. Ak je políčko označené, administračná skupina je povolená.
3. Kliknite na **OK**.

Poznámka: Ak administračnú skupinu zakážete, každý prihlásený člen môže pokračovať v administračných operáciách, kým sa od tohto člena nebude vyžadovať opakované vytvorenie väzieb.

Pridanie, úpravy a odstránenie členov administračnej skupiny

Nevyhnutná podmienka: Ak chcete vykonať túto operáciu, musíte byť administrátorom IBM Directory Server.

1. V navigačnej oblasti rozviňte kategóriu **Správa servera** a kliknite na **Riadiť administračnú skupinu**.

Poznámka: Ak chcete konfiguračné nastavenia servera zmeniť pomocou úloh z kategórie Správa servera vo webovom administračnom nástroji, musíte sa na server autentifikovať ako užívateľský profil i5/OS, ktorý má mimoriadne oprávnenia *ALLOBJ a IOSYSCFG. Docielite to autentifikáciou ako projektovaný užívateľ s heslom pre takýto profil. Ak chcete z webového administračného nástroja vytvoriť väzby ako projektovaný užívateľ, zadajte meno užívateľa vo forme os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, pričom reťazce MYUSERNAME a MYSYSTEM.COM budú nahradené názvom vášho užívateľského profilu a príponou projekcie nakonfigurovaného systému.

2. Na paneli **Riadiť administračnú skupinu** kliknite na tlačidlo **Pridať**.
3. V paneli **Pridať člena administračnej skupiny**:
   a. Zadajte administrátorské DN člena (musí mať platnú syntax pre DN).
   b. Zadajte heslo člena.
   c. Znovu zadajte heslo člena pre potvrdenie.
   d. Voliteľné: Zadajte Kerberos ID člena. Kerberos ID musí mať buď formát ibm-kn alebo ibm-KerberosName. V hodnotách sa nerozlišuje veľkosť písmen. Napríklad, ibm-kn=root@TEST.ROCHESTER.IBM.COM sa rovná zápisu ibm-kn=ROOT@TEST.ROCHESTER.IBM.COM.
4. Voliteľné: zadajte členovo **meno užívateľa Digest-MD5**.

Poznámka: V mene užívateľa Digest-MD5 sa rozlišuje veľkosť písmen.

5. Kliknite na **OK**.
6. Tento postup zopakujte pri každom členovi, ktorého chcete pridať do administračnej skupiny.

Administrátorské DN člena, meno užívateľa Digest-MD5, ak bolo zadané a Kerberos ID, ak bolo zadané sa zobrazia v posuvnom zozname členov administračnej skupiny.

Ak chcete zmeniť alebo odstrániť členov administračnej skupiny, využite rovnaký postup, uvedený vyššie, ale v paneli **Riadiť administračnú skupinu** použite tlačidlá **Upraviť** a **Vymazať**.

Riadenie skupín limitov vyhľadávania

Aby sa zamedzilo prílišnej spotrebe prostriedkov a následnému postupnému zhoršovaniu výkonu servera kvôli požiadavkám užívateľa na vyhľadávanie, boli pre tieto požiadavky nariadené limity vyhľadávania na každom príslušnom serveri. Administrátor nastavuje tieto limity vyhľadávania pre veľkosť a trvanie vyhľadávania, keď konfiguruje server.

Výnimku z týchto limitov vyhľadávania má iba administrátor a členovia administračnej skupiny. Inak platia pre všetkých ostatných užívateľov. Avšak administrátor môže podľa potreby vytvoriť skupiny limitov vyhľadávania, ktoré môžu mať flexibilnejšie limity vyhľadávania ako obyčajný užívateľ. Takto môže administrátor prideliť mimoriadne vyhľadávacie privilégiá skupine užívateľov.

Bližšie informácie nájdete v:

| Webový administračný nástroj sa používa na riadenie skupín limitov vyhľadávania.

| **Súvisiaci koncept**

| “Parametre vyhľadávania” na strane 42

Vytvorenie skupiny limitov vyhľadávania

| Ak chcete vytvoriť skupinu limitov vyhľadávania, položku skupiny musíte vytvoriť pomocou webového administračného nástroja.

1. Rozviňte kategóriu **Riadenie adresárov** v navigačnej oblasti a kliknite na **Pridať položku**.Alebo kliknite na **Riadiť položky** a vyberte umiestnenie (cn=IBMpolicies alebo cn=localhost), potom kliknite na tlačidlo **Pridať**. Položky pod cn=IBMpolicies sa budú replikovať a položky pod cn=localhost sa nebudú replikovať.
2. V ponuke **Štrukturálna trieda objektov** vyberte niektorú zo skupinových tried objektov.
3. Kliknite na tlačidlo **Ďalej**.
4. V ponuke **Dostupné** vyberte pomocnú triedu objektov **ibm-searchLimits** a kliknite na tlačidlo **Pridať**. Tento postup zopakujte pri každej ďalšej pomocnej triede objektov, ktorú je treba pridať. Pomocnú triedu objektov môžete z ponuky **Vybraté** odstrániť, keď ju vyberiete a kliknete na tlačidlo **Odstrániť**.
5. Kliknite na tlačidlo **Ďalej**.
6. Do poľa **Relatívne DN** zadajte relatívny charakteristický názov (RDN) skupiny, ktorá sa práve pridáva. Napríklad, cn=Search Group1.
7. Do poľa **Rodičovské DN** zadajte charakteristický názov položky stromu, ktorá sa práve vyberá. Napríklad, cn=localhost. Môžete tiež kliknúť na **Prehľadať** a vybrať Rodičovské DN zo zoznamu. Vyberte si voľbu a kliknite na **Vybrať**, aby ste zadali Rodičovské DN. **Rodičovské DN** sa štandardne nastaví na vybratú položku v strome.

   Poznámka: Ak ste spustili túto úlohu v paneli **Riadiť položky**, toto pole vám bude vyplnené. **Rodičovské DN** bolo vybraté pred kliknutím na tlačidlo **Pridať**, aby sa spustil proces pridania položky.
8. V záložke **Vyžadované atribúty** zadajte hodnoty pre vyžadované atribúty.
   - **cn** je relatívne DN, ktoré ste zadali predtým.
   - Do poľa **ibm-searchSizeLimit** zadajte počet položiek, na ktorý sa má veľkosť vyhľadávania ohraničiť. Toto číslo môže byť v rozsahu od 0 do 2 147 483 647. Nastavenie hodnoty 0 je rovnaké ako nastavenie hodnoty **Neobmedzené**.
   - Do poľa **ibm-searchTimeLimit** zadajte počet sekúnd, na ktorý sa trvanie vyhľadávania ohraničí. Toto číslo môže byť v rozsahu od 0 do 2 147 483 647. Nastavenie hodnoty 0 je rovnaké ako nastavenie hodnoty **Neobmedzené**.
   - V závislosti od vami vybratej triedy objektov môžete vidieť pole **Člen** alebo **Jedinečný člen**. Sú to členovia skupiny, ktorú vytvárate. Položka je vo forme DN, napríklad, cn=Bob Garcia,ou=austin,o=ibm,c=us.
9. Ak chcete pre určitý atribút pridať viac ako jednu hodnotu, kliknite na **Viac hodnôt** a potom po jednej pridávajte hodnoty. Kliknite na tlačidlo **OK**, keď ste dokončili pridávanie viacerých hodnôt. Hodnoty sa pridajú do rozvinovacej ponuky, ktorá sa zobrazuje v atribúte.
10. Ak má váš server povolené označenia jazykov, kliknite na **Hodnota označenia jazyka**, aby ste mohli pridať alebo odstrániť deskriptory označenia jazykov.
11. Kliknite na **Ostatné atribúty**.
12. Na záložke **Ostatné atribúty** zadajte vhodné hodnoty pre atribúty. Ďalšie informácie nájdete v časti “Zmena binárnych atribútov” na strane 168.
13. Kliknite na tlačidlo **Dokončiť**, aby sa položka mohla vytvoriť.

Zmena skupiny limitov vyhľadávania

Skupine limitov vyhľadávania môžete zmeniť atribúty veľkosti alebo časového limitu. Rovnako môžete pridávať a vymazávať členov skupiny. Na zmenu skupiny limitov vyhľadávania použite webový administračný nástroj.

Ak chcete zmeniť skupinu limitov vyhľadávania, pozrite si “Úprava položky” na strane 164.

Kopírovanie skupiny limitov vyhľadávania

Skupinu limitov vyhľadávania je užitočné skopírovať, ak chcete mať rovnakú skupinu limitov vyhľadávania aj pod localhost aj pod IBMpolicies. Je to užitočné aj vtedy, keď chcete vytvoriť novú skupinu, ktorá má podobné informácie ako existujúca skupina len s malými rozdielmi.

Ak chcete skopírovať skupinu limitov vyhľadávania, pozrite si “Kopírovanie položky” na strane 165.

Odstránenie skupiny limitov vyhľadávania

Ak chcete odstrániť skupinu limitov vyhľadávania, pozrite si “Vymazanie položky” na strane 164.

Riadenie skupiny proxy autorizácie

Členovia zo skupiny proxy autorizácie môžu pristupovať na adresárový server a vykonávať mnohé úlohy v mene viacerých užívateľov bez nutnosti opakovaného vytvárania väzieb pre každého užívateľa. Členovia zo skupiny proxy autorizácie môžu prevziať všetky autentifikované identity, okrem identity administrátora alebo členov administračnej skupiny. Ďalšie informácie nájdete v časti “Autorizácia proxy” na strane 54.

Na riadenie proxy autorizácie sa používa webový administračný nástroj.

Bližšie informácie nájdete v:

- “Vytvorenie skupiny proxy autorizácie”
- “Zmena skupiny proxy autorizácie” na strane 120
- “Kopírovanie skupiny proxy autorizácie” na strane 120
- “Odstránenie skupiny proxy autorizácie” na strane 120

Vytvorenie skupiny proxy autorizácie

1. Rozviňte kategóriu **Riadenie adresárov** v navigačnej oblasti a kliknite na **Pridať položku**.Alebo kliknite na **Riadiť položky** a vyberte umiestnenie (cn=ibmPolicies alebo cn=localhost), potom kliknite na tlačidlo **Pridať**.
2. V ponuke **Štrukturálna trieda objektov** vyberte skupinové triedy objektov **groupof Names**.
3. Kliknite na tlačidlo **Ďalej**.
4. V ponuke **Dostupné** vyberte pomocnú triedu objektov **ibm-proxyGroup** a kliknite na tlačidlo **Pridať**. Opakujte tento proces pre každú ďalšiu pomocnú triedu objektov, ktorú chcete pridať.
5. Kliknite na tlačidlo **Ďalej**.
6. Do poľa **Relatívne DN** napíšte cn=proxyGroup.
7. Do poľa **Rodičovské DN** zadajte charakteristický názov položky stromu, ktorú práve vyberáte, napríklad, cn=localhost. Tiež môžete kliknúť na tlačidlo **Prehľadávať**, ak chcete **Rodičovské DN** vybrať zo zoznamu. Vyberte svoju voľbu a kliknutím na **Vybrať** zadáte požadované rodičovské DN. Predvolenou hodnotou pre Rodičovské DN je položka, vybratá zo stromu.

   Poznámka: Ak ste túto úlohu spustili v paneli Riadiť položky, toto pole sa vám vopred vyplní. Rodičovské DN ste vybrali pred kliknutím na tlačidlo Pridať, čo by spustilo proces pridania položky.
8. Na záložke **Vyžadované atribúty** napíšte hodnoty pre vyžadované atribúty.
   - **cn** je proxyGroup.
   - **Člen** je vo forme DN, napríklad, cn=Bob Garcia,ou=austin,o=ibm,c=us.

Bližšie informácie o pridávaní binárnych hodnôt nájdete v “Zmena binárnych atribútov” na strane 168.

9. Ak chcete pre určitý atribút pridať viac ako jednu hodnotu, kliknite na **Viac hodnôt** a potom po jednej pridávajte hodnoty.

   Poznámka: Pre hodnotu cn nevytvárajte viacero hodnôt. Skupina proxy autorizácie musí mať známy názov proxyGroup.

   Kliknite na tlačidlo **OK**, keď ste dokončili pridávanie viacerých hodnôt. Hodnoty sa pridajú do rozvinovacej ponuky, ktorá sa zobrazuje v atribúte.
10. Ak má váš server povolené označenia jazykov, kliknite na **Hodnota označenia jazyka**, aby ste mohli pridať alebo odstrániť deskriptory označenia jazykov.
11. Kliknite na **Ostatné atribúty**.
12. Na záložke **Ostatné atribúty** zadajte vhodné hodnoty pre atribúty. Bližšie informácie o pridávaní binárnych hodnôt nájdete v “Zmena binárnych atribútov” na strane 168.
13. Ak chcete pre určitý atribút pridať viac ako jednu hodnotu, kliknite na **Viac hodnôt** a potom po jednej pridávajte hodnoty. Kliknite na tlačidlo **OK**, keď ste dokončili pridávanie viacerých hodnôt. Hodnoty sa pridajú do rozvinovacej ponuky, ktorá sa zobrazuje v atribúte.
14. Ak má váš server povolené označenia jazykov, kliknite na **Hodnota označenia jazyka**, aby ste mohli pridať alebo odstrániť deskriptory označenia jazykov.
15. Kliknite na tlačidlo **Dokončiť**, aby sa položka mohla vytvoriť.

Zmena skupiny proxy autorizácie

Skupinu proxy autorizácie môžete meniť pomocou webového administračného nástroja, ako napríklad pridaním alebo vymazaním členov skupiny.

Ak chcete zmeniť skupinu proxy autorizácie, pozrite si “Úprava položky” na strane 164.

Kopírovanie skupiny proxy autorizácie

Skupinu proxy autorizácie je užitočné skopírovať, ak chcete mať rovnakú skupinu proxy autorizácie aj pod localhost aj pod IBMpolicies.

Ak chcete skopírovať skupinu proxy autorizácie, pozrite si “Kopírovanie položky” na strane 165.

Odstránenie skupiny proxy autorizácie

Ak chcete zo skupiny proxy autorizácie odstrániť člena pomocou webového administračného nástroja, pozrite si “Vymazanie položky” na strane 164.

Riadenie jedinečných atribútov

Riadenie jedinečných atribútov sa vykonáva prostredníctvom kategórie **Správa servera** webového administračného nástroja. Viac informácií nájdete v týchto častiach:

- “Vytvorenie zoznamu jedinečných atribútov” na strane 121
- “Odstránenie položky zo zoznamu jedinečných atribútov” na strane 121

Poznámka: Pri jednotlivých atribútoch sa označenie jazyka vzájomne vylučuje s jedinečnými atribútmi. Ak konkrétny atribút označíte, že je jedinečným atribútom, nemôže mať priradené označenia jazyka.

Poznámka: Ak chcete konfiguračné nastavenia servera zmeniť pomocou úloh z kategórie Správa servera vo webovom administračnom nástroji, musíte sa na server autentifikovať ako užívateľský profil i5/OS, ktorý má mimoriadne oprávnenia *ALLOBJ a IOSYSCFG. Docielite to autentifikáciou ako projektovaný užívateľ s heslom pre takýto profil. Ak chcete z webového administračného nástroja vytvoriť väzby ako projektovaný užívateľ, zadajte meno užívateľa vo forme os400-

profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, pričom reťazce MYUSERNAME a MYSYSTEM.COM budú nahradené názvom vášho užívateľského profilu a príponou projekcie nakonfigurovaného systému.

Vytvorenie zoznamu jedinečných atribútov

1. V navigačnej oblasti rozviňte kategóriu **Správa servera**.Kliknite na **Riadiť jedinečné atribúty**.
2. V ponuke **Dostupné atribúty** vyberte atribút, ktorý chcete pridať ako jedinečný atribút. Uvedené dostupné atribúty sú atribúty, ktoré môžete označiť ako jedinečné; napríklad sn.
3. Buď kliknite na **Pridať do cn=localhost** alebo **Pridať do cn=IBMpolicies**. Rozdiel medzi týmito dvoma kontajnermi je taký, že položky cn=IBMpolicies sa replikujú a položky cn=localhost sa nereplikujú. Atribút sa zobrazí v príslušnom posuvnom zozname. Rovnaký atribút môžete uvádzať v zozname v obidvoch kontajneroch.

   Poznámka: Ak bude položka vytvorená aj pod cn=localhost aj pod cn=IBMpolicies, výsledným zlúčením týchto dvoch položiek bude zoznam jedinečných atribútov. Napríklad, ak sú atribúty cn a employeeNumber v cn=localhost označené ako jedinečné a atribúty cn a telephoneNumber sú označené ako jedinečné v cn=IBMploicies, server bude s atribútmi cn, employeeNumber a telephoneNumber zaobchádzať ako s jedinečnými atribútmi.
4. Opakujte tento postup pri každom atribúte, ktorý chcete pridať ako jedinečný atribút.
5. Kliknite na tlačidlo **OK**, ak chcete uložiť zmeny.

Ak sa pri pridávaní alebo úpravách položky jedinečného atribútu skončí vytváranie jedinečného obmedzenia pre ľubovoľný uvedený typ jedinečných atribútov chybou, položka nebude do adresára pridaná ani vytvorená. Problém sa musí vyriešiť a príkaz na pridanie alebo úpravu musí byť opätovne zadaný skôr ako sa bude môcť položka vytvoriť alebo upraviť. Napríklad, ak pri pridávaní položky jedinečného atribútu do adresára zlyhá vytváranie jedinečného obmedzenia v tabuľke pre jeden z uvedených typov jedinečných atribútov (to znamená z dôvodu existencie duplicitných hodnôt v databáze), položka jedinečného atribútu nebude do adresára pridaná. Objaví sa chyba.

Keď sa aplikácia pokúša pridať položku s hodnotou pre atribút, ktorá je duplikátom existujúcej adresárovej položky, do adresára, zo serveru LDAP bude vydaná chyba s kódom výsledku 20 (LDAP: kód chyby 20 - Atribút alebo hodnota existuje).

Keď sa server spustí, skontroluje zoznam jedinečných atribútov a zistí, či pre každý z nich existujú obmedzenia DB2. Ak pre atribút obmedzenie neexistuje, pretože ho odstránil pomocný program bulkload alebo ho manuálne odstránil užívateľ, atribút bude odstránený zo zoznamu jedinečných atribútov a do chybového protokolu ibmslapd.log sa zaprotokoluje chybové hlásenie. Napríklad, ak je atribút cn označený ako jedinečný v cn=uniqueattributes,cn=localhost, ale neexistuje preň žiadne obmedzenie DB2, potom sa zaprotokoluje nasledujúca správa:

```
Hodnoty pre atribút CN nie sú jedinečné.
Atribút CN bol odstránený z položky jedinečného
atribútu: CN=UNIQUEATTRIBUTES,CN=LOCALHOST
```

Odstránenie položky zo zoznamu jedinečných atribútov

Ak sa jedinečný atribút nachádza aj v cn=uniqueattribute,cn=localhost aj v cn=uniqueattribute,cn=IBMpolicies, ale bude odstránený iba z jednej položky, server bude naďalej zaobchádzať s takýmto atribútom ako s jedinečným atribútom. Atribút prestane byť jedinečným, keď bude odstránený z obidvoch položiek.

1. V navigačnej oblasti rozviňte kategóriu **Správa servera** a kliknite na **Riadiť jedinečné atribúty**.
2. Kliknutím na atribút v príslušnom posuvnom zozname vyberte atribút, ktorý chcete odstrániť zo zoznamu jedinečných atribútov.
3. Kliknite na **Odstrániť**.
4. Opakujte tento postup pri každom atribúte, ktorý chcete zo zoznamu odstrániť.
5. Kliknite na tlačidlo **OK**, ak chcete uložiť zmeny.

Poznámka: Keď odstránite posledný jedinečný atribút z posuvného zoznamu cn=localhost alebo z cn=IBMpolicies, položka kontajnera pre tento posuvný zoznam cn=uniqueattribute,cn=localhost alebo cn=uniqueattribute,cn=IBMpolicies sa automaticky vymaže.

Sledovanie prístupu a zmien v adresári LDAP

Možno budete chcieť sledovať prístup a zmeny pre váš adresár LDAP. Na sledovanie zmien adresára môžete použiť protokol zmien adresára LDAP. Protokol zmien je umiestnený pod špeciálnou príponou cn=changelog. Je uložený v knižnici QUSRDIRCL.

Pri sprístupňovaní protokolu zmien vykonajte nasledujúce kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte **Vlastnosti**.
5. Kliknite na záložku **Change Log**.
6. Vyberte **Protokolovať zmeny adresára**.
7. Voliteľné: Do poľa **Maximálny počet položiek** zadajte maximálny počet položiek, ktorý sa má ponechať v protokole zmien. V poli **Maximálny vek** uveďte, ako dlho sa udržujú položky protokolu zmien.

Poznámka: Hoci sú tieto parametre nepovinné, mali by ste vážne pouvažovať buď o zadaní maximálneho počtu položiek alebo o zadaní maximálneho veku. Ak nezadáte ani jeden, protokol zmien si bude uchovávať všetky položky a môže sa stať príliš rozsiahlym.

Trieda objektov changeLogEntry sa používa na reprezentovanie zmien použitých v adresárovom serveri. Množina zmien je daná podľa usporiadanej množiny všetkých položiek v rámci kontajnera protokolu zmien, ktorú definuje changeNumber. Informácie protokolu zmien sú určené len na čítanie.

Každý užívateľ, ktorý sa nachádza na zozname riadenia prístupu pre príponu cn=changelog, môže vyhľadávať položky v protokole zmien. Mali by ste vyhľadávať iba príponu protokolu zmien, cn=changelog. Nepokúšajte sa pridať, zmeniť alebo vymazať príponu protokolu zmien, ani ak na to máte oprávnenie. Spôsobí to nepredvídateľné následky.

Príklad:

Nasledujúci príkaz používa pomocný program príkazového riadku **ldapsearch** na obnovu všetkých položiek protokolu zmien, ktoré boli zaprotokolované na serveri:

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

Povolenie auditovania objektu pre adresárový server

Adresárový server podporuje auditovanie bezpečnosti i5/OS. Ak je systémová hodnota QAUDCTL nastavená na *OBJAUD, môžete aktivovať audit objektov pomocou iSeries Navigator.

Ak chcete umožniť audit objektov pre adresárový server, postupujte podľa nasledujúcich krokov:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte **Vlastnosti**.
5. Kliknite na zložku **Auditovanie**.
6. Zvoľte nastavenie auditovania, ktoré chcete pre svoj server používať.
7. Kliknite na tlačidlo **OK**

Zmeny v nastavení auditovania sa prejavia hneď ako kliknete na tlačidlo **OK**. Adresárový server nie je potrebné reštartovať. Ďalšie informácie obsahuje časť “Bezpečnosť adresárového servera” na strane 46

Úprava nastavení hľadania

Parametre vyhľadávania môžete nastaviť pre riadenie vyhľadávacích schopností užívateľov, ako napríklad stránkované a triedené vyhľadávanie, limity veľkosti a času a voľby pre dereferencovanie aliasov, pomocou webového administračného nástroja.

Stránkované výsledky umožňujú klientovi riadiť množstvo údajov, ktoré bolo vrátené z požiadavky na vyhľadávanie. Klient môže, namiesto prijatia všetkých výsledkov naraz, požadovať podmnožinu položiek (stránka). Ďalšie žiadosti o hľadanie budú až do zrušenia operácie alebo vrátenia posledného výsledku zobrazovať nasledujúcu stránku výsledkov.

Triedené vyhľadávanie umožňuje klientovi prijať výsledky vyhľadávania utriedené podľa zoznamu kritérií, v ktorom každé kritérium predstavuje triediaci kľúč. Presúva sa tým zodpovednosť za triedenie z klientskej aplikácie na server.

Ak chcete prispôsobiť nastavenia vyhľadávania adresárového servera, postupujte nasledovne:

1. V navigačnej oblasti rozviňte kategóriu **Správa servera** a kliknite na **Riadiť vlastnosti servera**.

   Poznámka: Ak chcete konfiguračné nastavenia servera zmeniť pomocou úloh z kategórie Správa servera vo webovom administračnom nástroji, musíte sa na server autentifikovať ako užívateľský profil i5/OS, ktorý má mimoriadne oprávnenia *ALLOBJ a IOSYSCFG. Docielite to autentifikáciou ako projektovaný užívateľ s heslom pre takýto profil. Ak chcete z webového administračného nástroja vytvoriť väzby ako projektovaný užívateľ, zadajte meno užívateľa vo forme os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, pričom reťazce MYUSERNAME a MYSYSTEM.COM budú nahradené názvom vášho užívateľského profilu a príponou projekcie nakonfigurovaného systému.
2. Vyberte záložku **Nastavenia vyhľadávania**.
3. Nastavte **Limit veľkosti vyhľadávania**. Buď kliknite na prepínač **Položky** alebo na prepínač **Neobmedzené**. Ak vyberiete **Položky**, musíte v poli zadať maximálny počet položiek, ktoré sa majú z vyhľadávania vrátiť. Predvolené nastavenie je 500. Ak kritériám vyhľadávania vyhovujú viaceré položky, tie nebudú vrátené. Tento limit neplatí pre administrátorov alebo pre členov skupín limitov vyhľadávania, ktorým boli pridelené väčšie limity pre veľkosť vyhľadávania.
4. Nastavte **Časový limit vyhľadávania**. Buď kliknite na prepínač **Sekundy** alebo na prepínač **Neobmedzené**. Ak vyberiete**Sekundy**, musíte v poli zadať maximálne množstvo času, ktorý server venuje spracovaniu požiadavky. Predvolené nastavenie je 900.Tento limit neplatí pre administrátorov alebo pre členov skupín limitov vyhľadávania, ktorým boli pridelené dlhšie časové limity vyhľadávania.
5. Ak chcete schopnosti triediť vyhľadávania obmedziť len na administrátorov, vyberte zaškrtávacie políčko **Triedenie vyhľadávaní povoliť len administrátorom**.
6. Ak chcete schopnosti stránkovať vyhľadávanie obmedziť len na administrátorov, vyberte zaškrtávacie políčko **Stránkovanie vyhľadávaní povoliť len administrátorom**.
7. Rozviňte sťahovaciu ponuku pre **Dereferencovanie aliasov** a vyberte niektoré z nasledujúcich. Predvolené nastavenie je **Vždy**.

   Nikdy Aliasy sa nebudú nikdy dereferencovať.

   Nájdenie
   Aliasy budú dereferencované, keď sa nájde východiskový bod vyhľadávania, ale nie pri vyhľadávaní pod touto východiskovou položkou.

   Hľadanie
   Aliasy budú dereferencované pri vyhľadávaní v položkách pod východiskovým bodom vyhľadávania, ale nie pri nájdení východiskovej položky.

   Vždy Aliasy budú vždy dereferencované aj pri hľadaní východiskového bodu vyhľadávania a tiež pri vyhľadávaní položiek pod východiskovou položkou. Predvolené nastavenie má hodnotu Vždy.

Bližšie informácie nájdete v “Parametre vyhľadávania” na strane 42 a v “Hľadanie položiek adresára” na strane 166.

Úprava nastavení výkonu

Zmenou jednej z nasledujúcich položiek môžete upraviť nastavenia výkonu vášho adresárového servera:
- Veľkosť ACL pamäte cache, veľkosť položky pamäte cache, maximálny počet hľadaní, ktoré sa majú ukladať vo filtri pamäte cache a najväčšie hľadanie, ktoré sa má uložiť do pamäte cache vo filtri pamäte cache.
- Počet databázových pripojení a serverových vlákien
- Nastavenie pamäte cache atribútov
- Nastavenia transakcií servera

Bližšie informácie nájdete v:
- "Nastavenie databázových pripojení a nastavenia pamäte cache"
- "Konfigurácia pamäte cache atribútov"
- "Nastavenia konfigurácie transakcií" na strane 126

Nastavenie databázových pripojení a nastavenia pamäte cache

Ak chcete nastaviť databázové pripojenia a nastavenie pamäte cache, postupujte nasledovne:

1. V navigačnej oblasti webového administračného nástroja rozviňte kategóriu **Riadiť vlastnosti servera** a v pravom paneli vyberte záložku **Výkon**.
2. Zadajte **Počet databázových pripojení**. Tým sa nastaví počet pripojení DB2, ktoré používa server. Minimálne musíte zadať 4. Predvolené nastavenie je 15. Ak váš server LDAP prijme veľký objem klientskych požiadaviek alebo keď klienti dostávajú chyby ″pripojenie bolo zamietnuté″, lepšie výsledky uvidíte, keď zvýšite nastavenie počtu pripojení, ktoré server vytvára pre DB2. Maximálny počet pripojení sa určí podľa nastavenia vo vašej databáze DB2. Hoci server neohraničuje počet vami zadaných pripojení, každé pripojenie spotrebováva prostriedky.
3. Zadajte **Počet databázových pripojení pre replikáciu**. Tým sa nastaví počet pripojení DB2, ktoré server používa na replikáciu. Minimálne musíte zadať 1. Predvolené nastavenie je 4.

   Poznámka: Celkový počet pripojení, ktorý je zadaný pre databázové pripojenia, vrátane databázových pripojení pre replikáciu, nemôže prekročiť počet pripojení, nastavený vo vašej databáze DB2.
4. Vyberte **Ukladať informácie ACL do pamäte cache**, ak chcete používať nasledujúce nastavenia pamäte cache pre ACL.
5. Zadajte **Maximálny počet prvkov v pamäti cache ACL**. Predvolené nastavenie je 25 000.
6. Zadajte **Maximálny počet prvkov v pamäti cache položiek**. Predvolené nastavenie je 25 000.
7. Zadajte **Maximálny počet prvkov v pamäti cache filtra vyhľadávania**. Predvolené nastavenie je 25 000.Pamäť cache filtra vyhľadávania sa skladá zo skutočných dotazov na požadované filtre atribútov a z identifikátorov výsledných položiek, ktoré vykazovali zhodu. Pri operácii aktualizácie budú všetky položky pamäte cache znehodnotené.
8. Zadajte **Maximálny počet prvkov z jedného vyhľadávania, ktoré sa pridajú do pamäte cache filtra vyhľadávania**. Ak vyberiete **Prvky**, musíte zadať počet. Predvolené nastavenie je 100. Inak vyberte **Neobmedzené**. Položky vyhľadávania, ktoré sa zhodujú s viacerými položkami ako je tu zadaný počet, nebudú pridané do pamäte cache filtra vyhľadávania.
9. Po dokončení kliknite na **OK**.
10. Ak nastavujete počet databázových pripojení, reštartujte server, aby sa prejavili zmeny. Ak ste upravovali iba nastavenia pamäte cache, server sa nemusí reštartovať.

Konfigurácia pamäte cache atribútov

Nastavenia pre pamäť cache atribútov sa dajú nakonfigurovať aj vo webovom administračnom nástroji aj v aplikácii iSeries Navigator.

Ak chcete manuálne prispôsobiť nastavenia pamäte cache atribútov vo webovom administračnom nástroji, postupujte nasledovne.

1. V navigačnej oblasti webového administračného nástroja rozviňte kategóriu **Správa servera** a v pravom paneli vyberte záložku **Pamäť cache atribútov**.

   Poznámka: Ak chcete konfiguračné nastavenia servera zmeniť pomocou úloh z kategórie Správa servera vo webovom administračnom nástroji, musíte sa na server autentifikovať ako užívateľský profil i5/OS, ktorý má mimoriadne oprávnenia *ALLOBJ a IOSYSCFG. Docielite to autentifikáciou ako projektovaný užívateľ s heslom pre takýto profil. Ak chcete z webového administračného nástroja vytvoriť väzby ako projektovaný užívateľ, zadajte meno užívateľa vo forme os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, pričom reťazce MYUSERNAME a MYSYSTEM.COM budú nahradené názvom vášho užívateľského profilu a príponou projekcie nakonfigurovaného systému.
2. Zmeňte množstvo kilobajtov pamäte, ktoré sú dostupné pre pamäť cache adresárov. Predvolené nastavenie je 16 384 kilobajtov (16 MB).
3. Zmeňte množstvo kilobajtov pamäte, ktoré sú dostupné pre pamäť cache protokolu zmien. Predvolené nastavenie je 16 384 kilobajtov (16 MB).

   Poznámka: Tento výber bude zakázaný, ak nebol protokol zmien nakonfigurovaný. Ukladanie atribútov do pamäte cache pre protokol zmien by malo byť nastavené na hodnotu 0 a nemali by sa konfigurovať žiadne atribúty, pokiaľ nerobíte časté vyhľadávania v rámci protokolu zmien a vykonávanie týchto vyhľadávaní je životne dôležité.
4. Z ponuky **Dostupné atribúty** vyberte atribút, ktorý chcete uložiť do pamäte cache. V tejto ponuke sa zobrazujú iba tie atribúty, ktoré sa môžu uložiť do pamäte cache; napríklad sn.

   Poznámka: Atribút zostane v zozname dostupných atribútov, pokiaľ nebol umiestnený aj do kontajnera cn=directory aj do kontajnera cn=changelog.
5. Buď kliknite na **Pridať do cn=directory** alebo na **Pridať do cn=changelog**. Atribút sa zobrazí v príslušnom posuvnom zozname. Rovnaký atribút môžete uvádzať v zozname v obidvoch kontajneroch.

   Poznámka: Voľba **Pridať do cn=changelog** bude zakázaná, ak nebol protokol zmien nakonfigurovaný. Ukladanie atribútov do pamäte cache pre protokol zmien by malo byť nastavené na hodnotu 0 a nemali by sa konfigurovať žiadne atribúty, pokiaľ nerobíte časté vyhľadávania v rámci protokolu zmien a vykonávanie týchto vyhľadávaní je životne dôležité.
6. Opakujte tento postup pri každom atribúte, ktorý chcete pridať do pamäte cache atribútov.
7. Po dokončení kliknite na **OK**.

Ak chcete v aplikácii iSeries Navigator povoliť automatické ukladanie atribútov do pamäte cache, postupujte nasledovne:

1. V aplikácii iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte **Vlastnosti**.
5. Kliknite na záložku **Výkonnosť**.
6. Vyberte **Povoliť automatické ukladanie atribútov do pamäte cache** buď pre **Databázu** alebo pre **Protokol zmien** alebo pre obidva. Automatické ukladanie atribútov do pamäte cache pre protokol zmien by nemalo byť povolené, pokiaľ nerobíte časté vyhľadávania v rámci protokolu zmien a vykonávanie týchto vyhľadávaní je životne dôležité.
7. Špecifikujte **Čas spustenia** (v miestnom čase servera) a **Interval** pre každý typ ukladania do pamäte cache, ktorý chcete povoliť. Napríklad, ak povolíte ukladanie databázy do pamäte cache a čas spustenia nastavíte na 6:00 hod a interval na šesť hodín, pamäť cache sa automaticky upraví o 6:00, 12:00, 18:00 a o 24:00 bez ohľadu na to kedy bol server spustený alebo kedy bolo nakonfigurované automatické upravenie.

Poznámka: Automatické ukladanie atribútov do pamäte cache bude ukladať atribúty do pamäte cache, kým nedosiahne maximálne množstvo pamäte pre ukladanie do pamäte cache, ktoré je špecifikované vo webovom administračnom nástroji, podľa horeuvedeného popisu.

Tabuľka 4. Vzájomné pôsobenie nastavení pamäte cache atribútov

Činnosť	Čo sa udeje
Spúšťanie servera	Ak je aktuálne povolené automatické ukladanie atribútov do pamäte cache a automatické ukladanie do pamäte cache bolo povolené pri poslednom zastavení servera, rovnaké atribúty, ktoré boli uložené do pamäte cache pri zastavení servera, budú vytvorené pri reštarte servera. Ak je pre ukladanie atribútov do pamäte cache stále k dispozícii ďalšia pamäť, do pamäte cache sa budú ukladať aj atribúty, ktoré boli nakonfigurované manuálne. Ak je aktuálne povolené automatické ukladanie atribútov do pamäte cache, ale nebolo povolené pri poslednom zastavení servera, do pamäte cache sa budú ukladať atribúty, ktoré boli pre ukladanie do pamäte cache nakonfigurované manuálne. V obidvoch prípadoch bude server automaticky upravovať pamäte cache atribútov, podľa zadaného času spustenia a časového intervalu. Ak nie je povolené automatické ukladanie do pamäte cache, prejavia sa manuálne prispôsobené nastavenia pamäte cache.
Povolenie automatického ukladania atribútov do pamäte cache po spustení servera	Automatické ukladanie atribútov do pamäte cache sa udeje podľa popisu pre spúšťanie servera. Všetky manuálne nakonfigurované pamäte cache atribútov, ktoré sa nezmestia do množstva pamäte, nakonfigurovanej pre ukladanie atribútov do pamäte cache, budú vymazané.
Zakázanie automatického ukladania atribútov do pamäte cache po spustení servera	Do pamäte cache sa uložia iba atribúty, ktoré boli nakonfigurované manuálne.
Úprava atribútov manuálne vložených do pamäte cache, kým je povolené automatické ukladania do pamäte cache po spustení servera	Nič sa neudeje. Manuálna konfigurácia sa prejaví, keď bude zakázané automatické ukladanie do pamäte cache.
Úprava dostupného množstva pamäte pre ukladanie do pamäte cache po spustení servera	Ak je povolené automatické ukladanie do pamäte cache, server okamžite opakovane ukladá do pamäte cache podľa novej veľkosti. Ak je automatické ukladanie do pamäte cache zakázané, server bude ukladať do pamäte cache manuálne nakonfigurované atribúty podľa novej veľkosti.
Úprava času spustenia alebo intervalu po spustení servera	Ak je automatické ukladanie do pamäte cache povolené, nové nastavenia sa prejavia v špecifikovanom intervale alebo v čase spustenia. Ak je automatické ukladanie do pamäte cache zakázané, nastavenia sa uložia a prejavia sa keď bude automatické ukladanie do pamäte cache povolené.

Nastavenia konfigurácie transakcií

Ak chcete nastaviť nastavenia transakcií, postupujte nasledovne:

1. V navigačnej oblasti webového administračného nástroja rozviňte kategóriu **Riadiť vlastnosti servera** a v pravom paneli vyberte záložku **Transakcie**.
2. Ak chcete povoliť spracovanie transakcií, vyberte zaškrtávacie políčko**Povoliť spracovanie transakcií**. Ak je políčko**Povoliť spracovanie transakcií** zakázané, server bude všetky ostatné voľby na tomto paneli ignorovať.
3. Nastavte **Maximálny počet transakcií**. Buď kliknite na prepínač **Transakcie** alebo na prepínač **Neobmedzené**. Ak vyberiete**Transakcie**, zadajte maximálny počet transakcií. Maximálny počet transakcií je 2 147 483 647. Predvolené na stavenie je 20.
4. Nastavte **Maximálny počet operácií na transakciu**. Buď kliknite na prepínač **Operácie** alebo na prepínač **Neobmedzené**. Ak vyberiete **Operácie**, zadajte maximálny počet operácií, ktoré budú pre každú transakciu povolené. Maximálny počet operácií je 2 147 483 647. Čím je počet nižší, tým je výkon lepší. Predvolené nastavenie je 5 operácií.
5. Nastavte **Čakajúci časový limit**. Tento výber nastaví maximálnu hodnotu pre uplynutie vyhradeného času čakajúcej transakcie v sekundách. Buď kliknite na prepínač **Sekundy** alebo na prepínač **Neobmedzené**. Ak vyberiete**Sekundy**, zadajte maximálny počet sekúnd, ktoré sú pre každú transakciu povolené. Maximálny počet sekúnd je 2 147 483 647. Transakcie, ktoré zostanú nedokončené dlhšie ako je tento čas, budú zrušené (vrátené). Predvolené nastavenie je 300 sekúnd.
6. Po dokončení kliknite na **OK**.

7. Ak ste povolili podporu transakcií, musíte server reštartovať, aby sa zmeny prejavili. Ak ste upravovali iba nastavenia, server nemusíte reštartovať.

Riadenie replikácie

Ak chcete riadiť replikáciu, rozviňte kategóriu **Riadenie replikácie** webového administratívneho nástroja. Viac informácií o konceptoch replikácie obsahuje “Replikácia” na strane 36.

Viac informácií nájdete v týchto častiach:

- “Vytvorenie topológie hlavnej repliky”
- “Vytváranie topológie hlavného servera-odosielateľa-repliky” na strane 132
- “Prehľad vytvárania komplexnej topológie replikácie” na strane 134
- “Vytvorenie komplexnej topológie s partnerskou replikáciou” na strane 134
- “Nastavenie topológie brán” na strane 137
- “Riadenie topológií” na strane 138
- “Zmena vlastností replikácie” na strane 141
- “Vytvorenie replikačných plánov” na strane 142
- “Riadenie frontov” na strane 144
- “Nastavenie replikácie cez zabezpečené pripojenie” na strane 144

Vytvorenie topológie hlavnej repliky

Ak chcete definovať základnú topológiu hlavnej repliky:

1. Vytvorte hlavný server a definujte jeho obsah. Vyberte si podstrom, ktorý má byť replikovaný a zadajte server ako hlavný. Pozrite si “Vytvorenie hlavného servera (replikovaného podstromu)” na strane 128.
2. Vytvorte povoľovacie údaje, ktoré má použiť dodávateľ. Pozrite si “Vytvorenie povoľovacích údajov” na strane 128.
3. Vytvorte replikačný server. Pozrite si “Vytvorenie replikačného servera” na strane 130.
4. Vyexportujte topológiu z hlavného servera do repliky. Pozrite si “Kopírovanie údajov do repliky” na strane 131.
5. Zmeňte konfiguráciu repliky tak, aby identifikovala, kto má oprávnenie replikovať do nej zmeny a pridať odvolávku do hlavného servera. Pozrite si “Pridávanie informácií dodávateľa do repliky” na strane 131.

Poznámka:

Ak položka v koreni podstromu, ktorý chcete replikovať, nie je príponou v serveri, skôr než budete môcť použiť funkciu **Pridať podstrom**, musíte sa presvedčiť, či je jej ACL definovaný nasledovne:

Pre nefiltrované ACL:

```
ownersource: <rovnaký ako položka DN>
ownerpropagate: TRUE

aclsource: <rovnaký ako položka DN>
aclpropagate: TRUE
```

Pre filtrované ACL:

```
ibm-filteraclinherit: FALSE
```

Ak chcete splniť požiadavky ACL a ak položka nie je príponou v serveri, upravte ACL pre danú položku na paneli **Riadenie položiek**. Vyberte si položku a kliknite na **Upraviť ACL**. Ak chcete pridať nefiltrované zoznamy ACL, vyberte si záložku a potom zadajte v začiarkovacom políčku pre ACL aj majiteľov, či sú tieto ACL explicitné alebo nie. Skontrolujte, či sú začiarknuté políčka **Propagovať ACL** a **Propagovať majiteľa**. Ak chcete pridať filtrované ACL, vyberte si záložku a pridajte položku **cn=this** s rolou **access-id** pre ACL aj majiteľov. Skontrolujte, či je začiarknutie políčka **Akumulovať filtrované ACL** zrušené a či je začiarknuté políčko **Propagovať majiteľa**. Podrobnejšie informácie nájdete v časti “Manažovanie zoznamov riadenia prístupu (ACL)” na strane 179.

Objekt **ibm-replicagroup** vytvorený týmto procesom zdedí na začiatku ACL koreňovej položky pre replikovaný podstrom. Tieto ACL môžu byť na kontrolu prístupu do replikačných informácií v adresári nevhodné.

Vytvorenie hlavného servera (replikovaného podstromu)

Poznámka: Ak chcete vykonať túto úlohu, server musí byť spustený.

Táto úloha určí položku ako koreň nezávisle replikovaného podstromu a vytvorí **ibm-replicasubentry** reprezentujúci tento server ako jeden hlavný server pre podstrom. Ak chcete vytvoriť replikovaný podstrom, musíte určiť, ktorý podstrom má tento server replikovať.

Rozviňte kategóriu riadenia replikácie v navigačnej oblasti a kliknite na **Riadiť topológiu**.

1. Kliknite na **Pridať podstrom**.
2. Zadajte DN koreňovej položky podstromu, ktorý chcete replikovať alebo kliknutím na **Prehľadávať** expandujte položky; z nich si potom vyberte položku, ktorá má byť koreňom podstromu.
3. URL odvolávky hlavného servera sa zobrazí napríklad v tvare LDAP URL:
   `ldap://<myservername>.<mylocation>.<mycompany>.com`

   Poznámka: URL odvolávky hlavného servera je voliteľné a používa sa len vtedy:
   - Ak server obsahuje (alebo bude obsahovať) ľubovoľné podstromy určené len na čítanie.
   - Ak chcete definovať URL odvolávky, ktoré sa vráti pre aktualizácie do ľubovoľného podstromu určeného len na čítanie:
4. Kliknite na **OK**.
5. Nový server sa zobrazí na paneli riadenia topológie pod hlavičkou **Replikované podstromy**.

Vytvorenie povoľovacích údajov

Rozviňte kategóriu riadenia replikácie v navigačnej oblasti webového administratívneho nástroja a kliknite na **Riadiť povoľovacie údaje**

1. Vyberte si umiestnenie, ktoré chcete použiť na ukladanie povoľovacích údajov zo zoznamu podstromov. Webový administračný nástroj vám umožní definovať povoľovacie údaje na týchto miestach:
   - **cn=replication,cn=localhost**, ktoré udržiava povoľovacie údaje len na aktuálnom serveri.

     Poznámka: Vo väčšine replikačných prípadov sa uprednostňuje umiestnenie povoľovacích údajov v cn=replication,cn=localhost, pretože poskytuje väčšiu bezpečnosť než replikované povoľovacie údaje umiestnené v podstrome. Existujú však určité situácie, pri ktorých nie sú povoľovacie údaje umiestnené v cn=replication,cn=localhost dostupné.

     Ak sa snažíte pridať repliku pod server, napríklad serverA a ste pripojení k inému serveru s webovým administratívnym nástrojom, ktorým je serverB, pole **Vybrať povoľovacie údaje** nezobrazí voľbu **cn=replication,cn=localhost**. Je to preto, že nemôžete čítať alebo aktualizovať informácie pod **cn=localhost** serverA, ak ste pripojení k serveru s názvom serverB.

     Voľba cn=replication,cn=localhost je dostupná len vtedy, ak server, pod ktorý sa snažíte pridať repliku, je ten istý server, ku ktorému ste pripojení s webovým administratívnym nástrojom.
   - V rámci replikačného podstromu, kedy sú povoľovacie údaje replikované so zvyškom podstromu. Povoľovacie údaje umiestnené v replikačnom podstrome sú vytvorené pod položkou **ibm-replicagroup=default** pre daný podstrom.

     Poznámka: Ak nie sú zobrazené žiadne podstromy, choďte na “Vytvorenie hlavného servera (replikovaného podstromu)”, kde nájdete inštrukcie na vytvorenie podstromu, ktorý chcete replikovať.
2. Kliknite na **Pridať**.
3. Zadajte názov pre povoľovacie údaje, ktoré vytvárate, napríklad **mycreds**, cn= je v poli už pre vás vopred vyplnené.

4. Vyberte si typ autentifikačnej metódy, ktorú chcete použiť a kliknite na **Ďalej**.
   - Ak ste si vybrali jednu autentifikáciu vytváranie väzieb:
     a. Zadajte DN, ktoré server používa na vytvorenie väzby s replikou, napríklad cn=any
     b. Zadajte heslo, ktoré server používa, keď vytvára väzbu s replikou, napríklad secret.
     c. Opätovným zadaním hesla potvrďte, že nenastali žiadne typografické chyby.
     d. Podľa potreby zadajte stručný opis povoľovacích údajov.
     e. Kliknite na **Dokončiť**.

     Poznámka: Možno si chcete poznamenať DN povoľovacích údajov a heslo pre budúce potreby. Toto heslo budete potrebovať, keď budete vytvárať replikačnú zmluvu.
   - Ak ste si vybrali autentifikáciu Kerberos:
     a. Zadajte DN Kerberos.
     b. Zadajte názov súboru záložky kľúčov.
     c. Podľa potreby zadajte stručný opis povoľovacích údajov. Nie sú potrebné žiadne ďalšie informácie. Viac informácií nájdete v časti “Povolenie autentifikácie Kerberos na adresárovom serveri” na strane 151.
     d. Kliknite na **Dokončiť**.

| Panel **Pridať poverenia Kerberos** preberá voliteľné DN vytvárania väzieb vo forme ibm-kn=user@realm a voliteľný názov súboru záložky kľúčov (označovaný ako súbor kľúčov). Ak je špecifikované DN vytvárania väzieb, na autentifikáciu pre spotrebiteľský server bude server používať špecifikovaný názov principálu. Inak sa bude používať názov služby Kerberos servera (ldap/host-name@realm). Ak sa používa súbor záložky kľúčov, server ho použije na získanie poverení pre špecifikovaný názov principálu. Ak nie je špecifikovaný žiadny súbor záložky kľúčov, server použije súbor záložky kľúčov, ktorý je špecifikovaný v konfigurácii pre Kerberos servera. Ak existuje viac ako jeden dodávateľ, musíte zadať názov principálu a súbor záložky kľúčov, ktorý budú používať všetci dodávatelia.

Na serveri, na ktorom ste vytvorili povoľovacie údaje:

a. Rozviňte **Riadenie adresárov** a kliknite na **Riadiť položky**.
b. Vyberte si podstrom, v ktorom ste uložili povoľovacie údaje, napríklad **cn=localhost** a kliknite na **Rozvinúť**.
c. Vyberte si **cn=replication** a kliknite na **Rozvinúť**.
d. Vyberte si povoľovacie údaje Kerberos (ibm-replicationCredentialsKerberos) a kliknite na **Upraviť atribúty**.
e. Kliknite na záložku **Ostatné atribúty**.
f. Zadajte **replicaBindDN**, napríklad **ibm-kn=myprincipal@SOME.REALM**.
g. Zadajte **replicaCredentials**. Je to názov súboru záložky kľúčov, ktorý sa používa pre **myprincipal**.

   Poznámka: Tento principál a heslo by mali byť rovnaké ako principál a heslo, ktoré používate na spustenie **kinit** z príkazového riadka.

Na replike

a. V navigačnej oblasti kliknite na **Riadiť vlastnosti replikácie**.
b. Vyberte si dodávateľa z roletovej ponuky **Informácie o dodávateľovi** alebo zadajte názov replikovaného podstromu, pre ktorý chcete nakonfigurovať povoľovacie údaje dodávateľa.
c. Kliknite na **Úprava**.
d. Zadajte replikačný bindDN. V tomto príklade **ibm-kn=myprincipal@SOME.REALM**.
e. Zadajte a potvrďte **Heslo replikačnej väzby**. Toto je heslo KDC používané pre **myprincipal**.

   - Ak ste si vybrali SSL s autentifikáciou certifikátu a používate certifikát servera, nemusíte poskytovať ďalšie informácie. Ak si vyberiete použitie iného certifikátu než je certifikát servera:
     a. Zadajte názov súboru kľúčov.
     b. Zadajte heslo súboru kľúčov.

c. Opätovným zadaním hesla súboru kľúčov ho potvrďte.
d. Zadajte návestie kľúčov.
e. Podľa potreby zadajte stručný opis.
f. Kliknite na **Dokončiť**.

Viac informácií nájdete v časti “Povolenie SSL a TLS (Transport Layer Security) v adresárovom serveri” na strane 149.

5. Na serveri, na ktorom ste vytvorili povoľovacie údaje, nastavte systémovú hodnotu Povoliť uchovať bezpečnostné informácie servera (QRETSVRSEC) na 1 (uchovať údaje). Keďže replikačné povoľovacie údaje sú uložené v overovacom zozname, server ich môže z neho získať pri pripájaní k replike.

Vytvorenie replikačného servera

Poznámka: Ak chcete vykonať túto úlohu, server musí byť spustený.

Rozviňte kategóriu **Riadenie replikácie** v navigačnej oblasti a kliknite na **Riadiť topológiu**.

1. Vyberte si podstrom, ktorý chcete replikovať a kliknite na **Zobraziť topológiu**.
2. Kliknutím na šípku vedľa výberu **Topológia replikácie** rozviňte zoznam dodávateľských serverov.
3. Vyberte si dodávateľský server a kliknite na **Pridať repliku**.

Na záložke **Server** okna **Pridať repliku**:

- Zadajte hostiteľský názov a číslo portu pre repliku, ktorú vytvárate. Štandardný port je 636 pre SSL a 389 pre iné než SSL. Tieto polia sa vyžadujú.
- Vyberte si, či povoliť komunikácie SSL.
- Zadajte názov repliky alebo ponechajte toto pole prázdne, kedy sa použije hostiteľský názov.
- Zadajte ID repliky. Ak je spustený server, na ktorom vytvárate repliku, kliknite na **Získať ID repliky** a toto pole sa automaticky vyplní. Ak sa má pridávaný server stať partnerským serverom odosielajúceho servera, toto pole bude požadované. Odporúča sa, aby boli všetky servery v rovnakom vydaní.
- Zadajte opis replikačného servera.

Na záložke **Ďalšie**:

1. Uveďte povoľovacie údaje, ktoré replika používa na komunikáciu s hlavným serverom.

   Poznámka: Webový administratívny nástroj povoľuje definovanie povoľovacích údajov na týchto miestach:
   - **cn=replication,cn=localhost**, ktoré udržiava povoľovacie údaje len na serveri, ktorý ich používa
   - V rámci replikačného podstromu, kedy sú povoľovacie údaje replikované so zvyškom podstromu. Povoľovacie údaje umiestnené v replikačnom podstrome sú vytvorené pod položkou **ibm-replicagroup=default** pre daný podstrom.

   Umiestnenie povoľovacích údajov v cn=replication,cn=localhost sa považuje za bezpečnejšie.

   a. Kliknite na **Vybrať**.
   b. Vyberte si pre povoľovacie údaje umiestnenie, ktoré chcete použiť. Uprednostňuje sa cn=replication,cn=localhost.
   c. Kliknite na **Zobraziť povoľovacie údaje**.
   d. Rozviňte zoznam povoľovacích údajov a vyberte si tie, ktoré chcete použiť.
   e. Kliknite na **OK**.

   Viac informácií o povoľovacích údajoch zmluvy nájdete v časti “Vytvorenie povoľovacích údajov” na strane 128.
2. Z roletového zoznamu zadajte replikačný plán alebo ho vytvorte kliknutím na **Pridať**. Pozrite si “Vytvorenie replikačných plánov” na strane 142.
3. Na zozname schopností dodávateľa môžete zrušiť ktorúkoľvek schopnosť, ktorú nechcete u zákazníka replikovať.

Ak má vaša sieť rôzne servery v odlišných vydaniach, na novších vydaniach sa môžu nachádzať schopnosti, ktoré nenájdete v starších vydaniach. Niektoré schopnosti, napríklad ACL filtra a politika hesiel, používajú prevádzkové atribúty, ktoré sú replikované s inými zmenami. Ak sa tieto funkcie používajú, vo väčšine prípadov budete chcete, aby ich všetky servery používali. Ak danú schopnosť nepodporujú všetky servery, nebudete ju chcieť použiť. Napríklad nebudete chcieť pre každý server iný ACL. Môžu však nastať prípady, kedy budete chcieť použiť schopnosť na serveroch, ktoré ju podporujú a nebudete chcieť zmeny v súvislosti so schopnosťou replikovanou do serverov, ktoré túto schopnosť nepodporujú. V takých prípadoch môžete použiť zoznam schopností, na ktorom vyznačíte tie schopnosti, ktoré sa nemajú replikovať.

4. Ak chcete vytvoriť repliku, kliknite na **OK**.
5. Zobrazí sa správa, ktorá vám oznámi, že je potrebné vykonať ďalšie akcie. Kliknite na **OK**.

Poznámka: Ak pridávate viacero serverov ako ďalšie repliky alebo vytvárate komplexnú topológiu, nepokračujte s "Kopírovanie údajov do repliky" alebo "Pridávanie informácií dodávateľa do repliky", kým ste nedokončili definovanie topológie na hlavnom serveri. Ak vytvárate *masterfile.ldif* po dokončení topológie, tento bude obsahovať položky adresára hlavného servera a úplnú kópiu topologických zmlúv. Ak tento súbor zavediete na každý server, tieto servery budú mať potom rovnaké informácie.

Kopírovanie údajov do repliky

Po vytvorení repliky musíte vyexportovať topológiu z hlavného servera do repliky.

1. Na hlavnom serveri vytvorte súbor LDIF pre údaje. Ak chcete skopírovať všetky údaje nachádzajúce sa na hlavnom serveri, postupujte nasledovne:
   a. V iSeries Navigator rozviňte **Sieť**.
   b. Rozviňte **Servery**.
   c. Kliknite na **TCP/IP**.
   d. Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte **Nástroje**, a následne **Export súboru**.
   e. Uveďte názov súboru LDIF (napríklad masterfile.ldif), voliteľne uveďte podstrom, ktorý sa má exportovať (napríklad subtreeDN), a kliknite na **OK**.
2. Na počítači, na ktorom vytvárate repliku, postupujte nasledovne:
   a. Skontrolujte, či sú replikované prípony definované v konfigurácii replikačného servera.
   b. Zastavte replikačný server.
   c. Skopírujte súbor LDIF do repliky a postupujte nasledovne:
      1) V iSeries Navigator rozviňte **Sieť**.
      2) Rozviňte **Servery**.
      3) Kliknite na **TCP/IP**.
      4) Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte **Nástroje**, a následne **Import súboru**.
      5) Uveďte názov vstupného súboru LDIF (napríklad masterfile.ldif), voliteľne uveďte podľa potreby replikáciu údajov a kliknite na **OK**.

      Replikačné zmluvy, plány, povoľovacie údaje (ak sú uložené v replikovanom podstrome) a údaje položky sú zavedené na replike.
   d. Spustite server.

Pridávanie informácií dodávateľa do repliky

Musíte zmeniť konfiguráciu repliky, aby ste mohli zistiť, kto má oprávnenie replikovať do nej zmeny a pridať odvolávku do hlavného servera.

Na počítači, na ktorom vytvárate repliku:

1. V navigačnej oblasti rozviňte **Manažment replikácie** a kliknite na **Riadiť vlastnosti replikácie**.

   Poznámka: Do webového administračného nástroja sa musíte prihlásiť ako projektovaný užívateľ OS/400 s mimoriadnymi oprávneniami *ALLOBJ a *IOSYSCFG, aby ste mohli zmeniť nastavenia v paneloch **Riadiť vlastnosti replikácie**.
2. Kliknite na **Pridať**.

3. Z roletovej ponuky **Replikovaný podstrom** si vyberte dodávateľa alebo zadajte názov replikovaného podstromu, pre ktorý chcete nakonfigurovať povoľovacie údaje dodávateľa. Ak upravujete povoľovacie údaje dodávateľa, toto pole nebude možné upravovať.
4. Zadajte replikačný bindDN. V tomto príklade cn=any.

   Poznámka: V závislosti od situácie môžete použiť ktorúkoľvek z týchto dvoch volieb.

   - Pomocou 'štandardných prihlasovacích údajov a odvolávky' nastavte DN pripojenia replikácie (a heslo) a štandardnú odvolávku pre všetky podstromy replikované do servera. Toto možno použiť vtedy, keď sú všetky podstromy replikované z rovnakého dodávateľa.
   - Pridaním informácií pre každý podstrom nastavte replikačný bind DN a heslo nezávisle pre každý replikovaný podstrom. Toto možno použiť vtedy, keď má každý podstrom iného dodávateľa (to znamená iný hlavný server pre každý podstrom).
5. V závislosti od typu povoľovacích údajov zadajte a potvrďte ich heslo (ktoré ste si predtým poznamenali na budúce použitie.)
   - **Simple Bind** - Uveďte DN a heslo
   - **Kerberos** - Ak povoľovacie údaje na dodávateľovi neidentifikujú principála a heslo, čo znamená, že sa má použiť principál serverovej vlastnej služby, potom bind DN bude ibm-kn=ldap/<*yourservername@yourrealm*>. Ak majú povoľovacie údaje názov principála, napríklad <*myprincipal@myrealm*>, použite ho ako DN. V žiadnom z týchto dvoch prípadov sa heslo nevyžaduje.
   - **SSL w/ EXTERNAL bind** - Uveďte DN subjektu pre certifikát a neuvádzajte žiadne heslo

   Pozrite si "Vytvorenie povoľovacích údajov" na strane 128.
6. Kliknite na **OK**.
7. Ak majú zmeny nadobudnúť účinnosť, musíte reštartovať repliku.

Viac informácií nájdete v časti "Zmena vlastností replikácie" na strane 141.

Replika je v pozastavenom stave a nevykonáva sa žiadna replikácia. Keď dokončíte nastavovanie vašej replikačnej topológie, musíte kliknúť na **Riadiť fronty**, vybrať repliku a kliknúť na **Pozastaviť/pokračovať**, aby sa replikácia spustila. Podrobnejšie informácie nájdete v časti "Riadenie frontov" na strane 144. Replika teraz dostane aktualizácie z hlavného servera.

Vytváranie topológie hlavného servera-odosielateľa-repliky

Ak chcete definovať topológiu hlavný server-odosielateľ-replika, musíte:

1. Vytvoriť hlavný a replikačný server. Pozrite si "Vytvorenie topológie hlavnej repliky" na strane 127.
2. Pre pôvodnú repliku vytvorte nový replikačný server. Pozrite si "Vytvorenie nového replikačného servera".
3. Skopírujte údaje do replík. Pozrite si "Kopírovanie údajov do repliky" na strane 131.

Vytvorenie nového replikačného servera

Ak ste nastavili topológiu replikácie (pozri "Vytvorenie hlavného servera (replikovaného podstromu)" na strane 128) s hlavným serverom (server1) a replikou (server2), môžete zmeniť rolu servera s názvom server2 na odosielajúci server. Ak to chcete vykonať, musíte vytvoriť novú repliku (server3) pod serverom s názvom server2.

1. Pripojte webovú administráciu k hlavnému serveru (server1)
2. Rozviňte kategóriu riadenia replikácie v navigačnej oblasti a kliknite na **Riadiť topológiu**.
3. Vyberte si podstrom, ktorý chcete replikovať a kliknite na **Zobraziť topológiu**.
4. Kliknutím na šípku vedľa výberu **Topológia replikácie** rozviňte zoznam dodávateľských serverov.
5. Kliknutím na šípku vedľa výberu **server1** rozviňte zoznam serverov.
6. Vyberte si server2 a kliknite na **Pridať repliku**.
7. Na záložke **Server** okna **Pridať repliku**:
   - Zadajte hostiteľský názov a číslo portu pre repliku (server3), ktorú vytvárate. Štandardný port je 636 pre SSL a 389 pre iné než SSL. Tieto polia sa vyžadujú.

- Vyberte si, či povoliť komunikácie SSL.
- Zadajte názov repliky alebo ponechajte toto pole prázdne, kedy sa použije hostiteľský názov.
- Zadajte ID repliky. Ak je spustený server, na ktorom vytvárate repliku, kliknite na **Získať ID repliky** a toto pole sa automaticky vyplní. Ak sa má pridávaný server stať partnerským serverom odosielajúceho servera, toto pole bude požadované. Odporúča sa, aby boli všetky servery v rovnakom vydaní.
- Zadajte opis replikačného servera.

Na záložke **Ďalšie**:

a. Uveďte povoľovacie údaje, ktoré replika používa na komunikáciu s hlavným serverom.

Poznámka: Webový administratívny nástroj povoľuje definovanie povoľovacích údajov na týchto miestach:

- **cn=replication,cn=localhost**, ktoré udržiava povoľovacie údaje len na serveri, ktorý ich používa
- v rámci replikačného podstromu, kedy sú povoľovacie údaje replikované so zvyškom podstromu.

Umiestnenie povoľovacích údajov v cn=replication,cn=localhost sa považuje za bezpečnejšie. Povoľovacie údaje umiestnené v replikačnom podstrome sú vytvorené pod položkou **ibm-replicagroup=default** pre daný podstrom.

1) Kliknite na **Vybrať**.
2) Vyberte si pre povoľovacie údaje umiestnenie, ktoré chcete použiť. Uprednostňuje sa cn=replication,cn=localhost.
3) Kliknite na **Zobraziť povoľovacie údaje**.
4) Rozviňte zoznam povoľovacích údajov a vyberte si tie, ktoré chcete použiť.
5) Kliknite na **OK**.

Viac informácií o povoľovacích údajoch zmluvy nájdete v časti “Vytvorenie povoľovacích údajov” na strane 128.

b. Z roletového zoznamu zadajte replikačný plán alebo ho vytvorte kliknutím na **Pridať**. Pozrite si “Vytvorenie replikačných plánov” na strane 142.

c. Na zozname schopností dodávateľa môžete zrušiť ktorúkoľvek schopnosť, ktorú nechcete u zákazníka replikovať.

Ak má vaša sieť rôzne servery v odlišných vydaniach, na novších vydaniach sa môžu nachádzať schopnosti, ktoré nenájdete v starších vydaniach. Niektoré schopnosti, napríklad ACL filtra a politika hesiel, používajú prevádzkové atribúty, ktoré sú replikované s inými zmenami. Ak sa tieto funkcie používajú, vo väčšine prípadov budete chcete, aby ich všetky servery používali. Ak danú schopnosť nepodporujú všetky servery, nebudete ju chcieť použiť. Napríklad nebudete chcieť pre každý server iný ACL. Môžu však nastať prípady, kedy budete chcieť použiť schopnosť na serveroch, ktoré ju podporujú a nebudete chcieť zmeny v súvislosti so schopnosťou replikovanou do serverov, ktoré túto schopnosť nepodporujú. V takých prípadoch môžete použiť zoznam schopností, na ktorom vyznačíte tie schopnosti, ktoré sa nemajú replikovať.

d. Ak chcete vytvoriť repliku, kliknite na **OK**.

8. Skopírujte údaje zo servera s názvom server2 do nového replikačného servera s názvom server3. Ďalšie informácie nájdete v časti “Kopírovanie údajov do repliky” na strane 131.
9. Pridajte dodávateľskú zmluvu do servera s názvom server3, ktorý zo servera s názvom server2 urobí dodávateľa pre server3 a server3 bude zákazníkom servera s názvom server2. Viac informácií o spôsobe, akým to vykonáte, nájdete v časti “Pridávanie informácií dodávateľa do repliky” na strane 131.

Serverové roly sú reprezentované ikonami vo webovom administratívnom nástroji. Vaša topológia je teraz:

- server1 (hlavný server)
  - server2 (odosielateľ)
    - server3 (replika)

Prehľad vytvárania komplexnej topológie replikácie

Použite tento vysoko úrovňový prehľad ako sprievodcu nastavením komplexnej replikačnej topológie.

1. Spustite všetky partnerské servery alebo repliky. Vyžaduje si to webový administratívny nástroj na zhromažďovanie informácií zo serverov.
2. Ak chcete preskočiť všetko pre každý front, použite riadenie Spustite 'prvý' hlavný server a nakonfigurujte ho ako hlavný server pre kontext.
3. Ak ešte údaje nie sú zavedené, zaveďte ich pre podstrom s cieľom replikovať ich na 'prvom' hlavnom serveri.
4. Vyberte si podstrom, ktorý sa má replikovať.
5. Pridajte všetky potenciálne partnerské hlavné servery ako repliky 'prvého' hlavného servera.
6. Pridajte všetky ostatné repliky.
7. Presuňte ostatné partnerské hlavné servery s cieľom podporovať ich.
8. Pridajte replikačné zmluvy pre repliky každému z partnerských hlavných serverov.

   Poznámka: Ak sa majú vytvoriť povoľovacie údaje v **cn=replication,cn=localhost**, tieto musia byť vytvorené na každom serveri po ich reštartovaní. Replikácia partnerskými servermi zlyhá, kým sú vytvorené objekty povoľovacích údajov.
9. Ku každému partnerskému hlavnému serveru pridajte replikačné zmluvy pre ostatné hlavné servery. 'Prvý' hlavný server už tieto informácie má.
10. Uveďte replikovaný podstrom do stavu pokoja, čo zabráni aktualizácií počas kopírovania údajov do ostatných serverov.
11. Ak chcete všetko pre každý front preskočiť, použite riadenie frontu.
12. Vyexportujte údaje pre replikovaný podstrom z 'prvého' hlavného servera.
13. Aktivujte podstrom.
14. Zastavte replikačné servery a naimportujte údaje pre replikovaný podstrom na každej replike a partnerskom hlavnom serveri. Potom servery reštartujte.
15. Riaďte vlastnosti replikácie na každej replike a partnerskom hlavnom serveri s cieľom nastaviť povoľovacie údaje, ktoré budú používať dodávatelia.

Vytvorenie komplexnej topológie s partnerskou replikáciou

Partnerská replikácia je replikačná topológia, v ktorej sú hlavnými viaceré servery. Avšak na rozdiel od prostredia s viacerými hlavnými servermi, medzi partnerskými servermi sa nebudú rozlišovať konflikty. Servery LDAP akceptujú aktualizácie poskytované partnerskými servermi a aktualizujú svoje vlastné kópie údajov. Na poradie prijímania aktualizácií alebo na skutočnosť, či viaceré aktualizácie kolidujú, sa neberie ohľad.

Ak chcete pridať ďalšie hlavné servery (partnerské servery), najprv pridajte server ako repliku určenú len na čítanie existujúcich hlavných serverov (pozri "Vytvorenie replikačného servera" na strane 130), inicializujte adresárové údaje a potom povýšte server na hlavný server (pozri "Presun alebo povýšenie servera" na strane 139).

Objekt **ibm-replicagroup** vytvorený týmto procesom zdedí na začiatku ACL koreňovej položky pre replikovaný podstrom. Tieto ACL môžu byť na kontrolu prístupu do replikačných informácií v adresári nevhodné.

Aby bola operácia pridania podstromu úspešná, DN položky, ktorý pridávate, musí mať správne ACL, pokiaľ nie je príponou v serveri.

Pre nefiltrované ACL:

- ownersource : <*DN položky*>
- ownerpropagate : TRUE
- aclsource : <*DN položky*>
- aclpropagate: TRUE

Filtrované ACL:

- ownersource : *<DN položky>*
- ownerpropagate : TRUE
- ibm-filteraclinherit : FALSE
- ibm-filteraclentry : *<ľubovoľná hodnota>*

Použite funkciu **Upraviť ACL** webového administratívneho nástroja na nastavenie ACL pre replikačné informácie priradené k novo vytvorenému replikovanému podstromu (pozri "Úprava zoznamov riadenia prístupu" na strane 141).

Replika je v pozastavenom stave a nevykonáva sa žiadna replikácia. Keď dokončíte nastavovanie vašej replikačnej topológie, musíte kliknúť na **Riadiť fronty**, vybrať repliku a kliknúť na **Pozastaviť/pokračovať**, aby sa replikácia spustila. Podrobnejšie informácie nájdete v časti "Riadenie frontov" na strane 144. Replika teraz dostane aktualizácie z hlavného servera.

Replikáciu partnerského servera použite len v prostredí, v ktorom je vzor adresárových aktualizácií dobre známy. Aktualizácie určitých objektov v adresári musia byť vykonané len jedným partnerským serverom. Cieľom je zabrániť scenáru, kedy jeden server vymaže objekt, za ktorým nasleduje ďalší server, ktorý mení objekt. Tento scenár vytvára možnosť, že partnerský server dostane príkaz na vymazanie, za ktorým bude nasledovať príkaz na zmenu, pričom nastane konflikt.

Ak chcete definovať topológiu partnerský server-odosielateľ-replika pozostávajúcu z dvoch serverov partnerský-hlavný server, dvoch odosielajúcich serverov a štyroch replík:

1. Vytvoriť hlavný a replikačný server. Pozrite si "Vytvorenie topológie hlavnej repliky" na strane 127.
2. Vytvorte dva ďalšie replikačné servery pre hlavný server. Pozrite si "Vytvorenie replikačného servera" na strane 130.
3. Vytvorte dve repliky pod každým z dvoch novo vytvorených replikačných serverov.
4. Povýšte pôvodnú repliku na hlavný server. Pozrite si "Povýšenie servera na partnerský server".

   Poznámka: Server, ktorý chcete povýšiť na hlavný, musí byť replikou bez akýchkoľvek ďalších podriadených replík.
5. Skopírujte údaje z hlavného servera do nového hlavného servera a replík. Pozrite si "Kopírovanie údajov do repliky" na strane 131.

Povýšenie servera na partnerský server

Pomocou odosielateľskej topológie vytvorenej v časti "Vytváranie topológie hlavného servera-odosielateľa-repliky" na strane 132 môžete server povýšiť na partnerský server. V tomto príklade povýšite repliku (server3) na partnerský server hlavného servera (server1).

1. Pripojte webovú administráciu k hlavnému serveru (server1).
2. Rozviňte kategóriu riadenia replikácie v navigačnej oblasti a kliknite na **Riadiť topológiu**.
3. Vyberte si podstrom, ktorý chcete replikovať a kliknite na **Zobraziť topológiu**.
4. Kliknite na šípku vedľa výberu **Topológia replikácie** a rozviňte zoznam serverov.
5. Kliknutím na šípku vedľa výberu **server1** rozviňte zoznam serverov.
6. Kliknutím na šípku vedľa výberu **server2** rozviňte zoznam serverov.
7. Kliknite na **server1** a na **Pridať repliku**. Vytvorte server4. Pozrite si "Vytvorenie replikačného servera" na strane 130. Rovnakým spôsobom vytvorte server5. Serverové roly sú reprezentované ikonami vo webovom administratívnom nástroji. Vaša topológia je teraz:
   - server1 (hlavný server)
     - server2 (odosielateľ)
       - server3 (replika)
     - server4 (replika)
     - server5 (replika)
8. Kliknutím na **server2** a na **Pridať repliku** vytvorte server6.

9. Kliknutím na **server4** a na **Pridať repliku** vytvorte server7. Rovnakým spôsobom vytvorte server8. Vaša topológia je teraz:
   - server1 (hlavný server)
     - server2 (odosielateľ)
       - server3 (replika)
       - server6 (replika)
     - server4 (odosielateľ)
       - server7 (replika)
       - server8 (replika)
     - server5 (replika)
10. Vyberte si **server5** a kliknite na **Presunúť**.

    Poznámka: Server, ktorý chcete presunúť, musí byť replikou bez akýchkoľvek ďalších podriadených replík.
11. Výberom **Replikačnej topológie** povýšte repliku na hlavný server. Kliknite na **Presunúť**.
12. Zobrazí sa panel **Vytvorenie ďalších dodávateľských zmlúv**. Replikácia partnerského servera vyžaduje, aby bol každý hlavný server dodávateľom a zákazníkom každého z ostatných hlavných serverov v topológii a každej repliky z prvej úrovne replík, server2 a server4. Server5 je už zákazníkom servera s názvom server1 a teraz sa musí stať dodávateľom serverov server1, server2 a server4. Skontrolujte, či sú políčka dodávateľskej zmluvy začiarknuté pre:

Tabuľka 5.

	Dodávateľ	Zákazník
✓	server5	server1
✓	server5	server2
✓	server5	server4

Kliknite na **Pokračovať**.

Poznámka: V niektorých prípadoch bude panel výberu povoľovacích údajov požadovať povoľovacie údaje, ktoré sú umiestnené na inom mieste než cn=replication,cn=localhost. V takých situáciách musíte poskytnúť objekt povoľovacích údajov, ktorý je umiestnený na inom mieste než je cn=replication,cn=localhost. Z existujúcich sád povoľovacích údajov si vyberte povoľovacie údaje, ktoré sa podstrom chystá použiť alebo vytvorte nové povoľovacie údaje. Pozrite si “Vytvorenie povoľovacích údajov” na strane 128.

.

13. Kliknite na **OK**. Vaša topológia je teraz:
    - server1 (hlavný server)
      - server2 (odosielateľ)
        - server3 (replika)
        - server6 (replika)
      - server4 (odosielateľ)
        - server7 (replika)
        - server8 (replika)
      - server5 (hlavný server)
    - server5 (hlavný server)
      - server1 (hlavný server)
      - server2 (odosielateľ)
      - server4 (odosielateľ)

14. Skopírujte údaje zo server1 do všetkých serverov. Ďalšie informácie nájdete v časti “Kopírovanie údajov do repliky” na strane 131.

Nastavenie topológie brán

Skôr ako začnete nastavovať topológiu replikácie, vytvorte si záložnú kópiu vášho pôvodného súboru ibmslapd.conf. Túto záložnú kópiu môžete použiť na obnovu svojej pôvodnej konfigurácie, ak sa pri replikácii vyskytnú ťažkosti.

Ak chcete bránu nastaviť pomocou komplexnej topológie s replikáciou partnerských počítačov podľa procedúry v “Povýšenie servera na partnerský server” na strane 135, postupujte nasledovne:

- Skonvertujte existujúci partnerský server (partner 1) na server brány, aby sa vytvorila replikačná lokalita 1.
- Vytvorte nový server brány pre replikačnú lokalitu 2 a dohody s partnerom 1.
- Vytvorte topológiu pre replikačnú lokalitu 2 (v tomto príklade sa neuvádza).
- Skopírujte údaje z hlavného počítača do všetkých počítačov v topológii.

Skonvertujte existujúci partnerský server na server brány

1. Webový administračný nástroj použite na prihlásenie do hlavného počítača (server1).
2. Rozviňte kategóriu **Riadenie replikácie** v navigačnej oblasti a kliknite na **Riadiť topológiu**.
3. Vyberte si podstrom, ktorý chcete replikovať a kliknite na **Zobraziť topológiu**.
4. Kliknite na šípku vedľa výberu **Topológia replikácie** a rozviňte zoznam serverov.
5. Ak chcete existujúci server skonvertovať na server brány, vyberte **server1** alebo jeho partnera **server5**. V tomto príklade použijeme **server1**.
6. Kliknite na **Upraviť server**.
7. Skontrolujte, či je označené **Server je hlavný počítač**, a potom vyberte **Server je brána**.
8. Kliknite na **OK**.

Poznámka: Ak server, ktorý chcete používať ako bránu, ešte nie je hlavným počítačom, potom musí byť koncovou replikou bez podriadených replík, ktorú budete môcť najprv povýšiť na hlavný počítač a následne ju označiť ako bránu.

Vytvorte server brány a skopírujte údaje z hlavného počítača do všetkých počítačov v topológii

1. Vyberte **server1** a kliknite na **Pridať repliku**.
2. Vytvorte novú repliku **server9**. Informácie o tvorbe replík, pridávaní poverení a informáciách o dodávateľoch nájdete v “Vytvorenie replikačného servera” na strane 130.
3. Vyberte **server9** a kliknite na **Presunúť**.
4. Výberom **Replikačnej topológie** povýšte repliku na hlavný server. Kliknite na **Presunúť**.
5. Zobrazí sa panel **Vytvoriť ďalšie dodávateľské zmluvy**. V tomto paneli sa presvedčte, či sú políčka dodávateľských zmlúv označené len pre server1.

	Dodávateľ	Zákazník
✓	server9	server1
	server9	server2
	server9	server4
	server9	server5

Kliknite na **Pokračovať**.

Poznámka: Niekedy sa panel **Vybrať poverenia** zobrazí so žiadosťou o poverenie, ktoré sa nachádza mimo umiestnenia cn=replication,cn=localhost. V takých prípadoch musíte zadať objekt poverenia, ktoré sa

nachádza mimo umiestnenia cn=replication,cn=localhost. Vyberte poverenia, ktoré bude podstrom používať z existujúcich sád poverení alebo vytvorte nové poverenia. Pozrite si “Vytvorenie povoľovacích údajov” na strane 128.

6. Kliknite na **OK**.
7. Vyberte **server9** a kliknite na **Upraviť server**.
8. Skontrolujte, či je označené **Server je hlavný počítač**, a potom vyberte **Server je brána**.
9. Kliknite na **OK**. Serverové roly sú reprezentované ikonami vo webovom administratívnom nástroji. Vaša topológia je teraz:
   - server1 (hlavný počítač-brána pre replikačnú lokalitu1)
     - server2 (odosielateľ)
       - server3 (replika)
       - server6 (replika)
     - server4 (odosielateľ)
       - server7 (replika)
       - server8 (replika)
     - server5 (hlavný server)
     - server9 (hlavný počítač-brána pre replikačnú lokalitu 2)
   - server5 (hlavný server)
     - server1 (hlavný server)
     - server2 (odosielateľ)
     - server4 (odosielateľ)
   - server9 (hlavný počítač-brána)
     - server1 (hlavný server)
10. Pridajte replikačné servery na **server9**, aby sa vytvorila topológia pre replikačnú lokalitu 2.
11. Opakujte tento proces, ak chcete vytvoriť ďalšie replikačné lokality. Nezabudnite pre jednu replikačnú lokalitu vytvoriť iba jeden server brány.
12. Keď ste dokončili vytváranie topológie, skopírujte údaje zo servera server1 do všetkých nových serverov vo všetkých replikačných lokalitách a pridajte informácie o dodávateľoch do všetkých nových serverov. Informácie o tom ako to máte urobiť nájdete v “Kopírovanie údajov do repliky” na strane 131 a v “Pridávanie informácií dodávateľa do repliky” na strane 131.

Riadenie topológií

Topológie sú špecifické pre replikované podstromy.

Prezeranie topológie

Poznámka: Ak chcete vykonať túto úlohu, server musí byť spustený.

Rozviňte kategóriu **Riadenie replikácie** v navigačnej oblasti a kliknite na **Riadiť topológiu**.

1. Vyberte si podstrom, ktorý si chcete prezerať a kliknite na **Zobraziť topológiu**.

Topológia sa zobrazí na zozname replikačných topológií. Kliknutím na modré trojuholníčky rozviňte tieto topológie. Zo zoznamu môžete:

- Pridať repliku.
- Upraviť informácie o existujúcej replike.
- Zmeniť na iný dodávateľský server pre repliku alebo povýšiť repliku na hlavný server.
- Vymazať repliku.

Pridávanie repliky

Pozrite si “Vytvorenie replikačného servera” na strane 130.

Úprava zmluvy

Môžete zmeniť nasledujúce informácie pre repliku:

Na záložke **Server** môžete meniť len

- Hostiteľský názov
- Port
- Povolenie SSL
- Opis

Na záložke **Ďalšie** môžete zmeniť:

- Povoľovacie údaje - pozri “Vytvorenie povoľovacích údajov” na strane 128.
- Replikačné plány - pozri “Vytvorenie replikačných plánov” na strane 142.
- Zmeňte schopnosti replikované do repliky zákazníka. Na zozname schopností dodávateľa môžete zrušiť ktorúkoľvek schopnosť, ktorú nechcete u zákazníka replikovať.
- Po dokončení kliknite na **OK**.

Presun alebo povýšenie servera

1. Vyberte si potrebný server a kliknite na **Presunúť**.
2. Vyberte si server, do ktorého chcete presunúť repliku alebo si vyberte **Replikačnú topológiu**, aby ste mohli povýšiť repliku na hlavný server. Kliknite na **Presunúť**.
3. V niektorých prípadoch bude panel výberu povoľovacích údajov požadovať povoľovacie údaje, ktoré sú umiestnené na inom mieste než cn=replication,cn=localhost. V takých situáciách musíte poskytnúť objekt povoľovacích údajov, ktorý je umiestnený na inom mieste než je cn=replication,cn=localhost. Z existujúcich sád povoľovacích údajov si vyberte povoľovacie údaje, ktoré sa podstrom chystá použiť alebo vytvorte nové povoľovacie údaje. Pozrite si “Vytvorenie povoľovacích údajov” na strane 128.
4. Zobrazí sa panel **Vytvorenie ďalších dodávateľských zmlúv**. Vyberte si dodávateľské zmluvy vhodné pre rolu servera. Ak sa napríklad replikačný server povyšuje na partnerský server, musíte vytvoriť dodávateľské zmluvy so všetkými ostatnými servermi a ich replikami prvej úrovne. Tieto zmluvy umožňujú povýšenému serveru konať ako dodávateľ ostatných serverov a ich replík. Existujúce dodávateľské zmluvy z ostatných serverov do novo povýšeného servera sú stále v platnosti a nie je potrebné ich znova vytvárať.
5. Kliknite na **OK**.

Zmena v topologickom strome odráža presun servera.

Ďalšie informácie nájdete v časti “Vytvorenie komplexnej topológie s partnerskou replikáciou” na strane 134.

Degradovanie hlavného servera

Ak chcete zmeniť rolu hlavného servera na repliku, postupujte nasledovne:

1. Pripojte webový administratívny nástroj k serveru, ktorý chcete degradovať.
2. Kliknite na **Riadiť topológiu**.
3. Vyberte si podstrom a kliknite na **Zobraziť topológiu**.
4. Vymažte všetky zmluvy pre server, ktorý chcete degradovať.
5. Vyberte si server, ktorý degradujete a kliknite na **Presunúť**.
6. Vyberte si server, pod ktorý chcete umiestniť degradovaný server a kliknite na **Presunúť**.
7. Presne tak, ako by ste to urobili pre novú repliku, vytvorte nové dodávateľské zmluvy medzi degradovaným serverom a jeho dodávateľmi. Pokyny nájdete v časti “Vytvorenie replikačného servera” na strane 130.

Replikácia podstromu

Poznámka: Ak chcete vykonať túto úlohu, server musí byť spustený.

Rozviňte kategóriu **Riadenie replikácie** v navigačnej oblasti a kliknite na **Riadiť topológiu**.

- Kliknite na **Pridať podstrom**.
- Zadajte DN podstromu, ktorý chcete replikovať alebo kliknutím na **Prehľadávať** rozviňte položky; z nich si potom vyberte položku, ktorá sa má stať koreňom podstromu.
- Zadajte URL odvolávky hlavného servera, ktorá musí mať tvar LDAP URL, napríklad:
  `ldap://<myservername>.<mylocation>.<mycompany>.com`
- Kliknite na **OK**.
- Nový server sa zobrazí na paneli riadenia topológie pod hlavičkou **Replikované podstromy**.

Úprava podstromu

Túto voľbu použite na zmenu URL hlavného servera, do ktorého tento podstrom a jeho repliky zasielajú aktualizácie. Musíte to urobiť, keď zmeníte číslo portu alebo hostiteľský názov hlavného servera alebo keď meníte hlavný server na iný.

1. Vyberte si podstrom, ktorý chcete upravovať.
2. Kliknite na **Upraviť podstrom**.
3. Zadajte URL odvolávky hlavného servera, ktorá musí mať tvar LDAP URL, napríklad:
   `ldap://<mynewservername>.<mylocation>.<mycompany>.com`

V závislosti od roly, ktorú server zohráva v tomto podstrome (či už ide o hlavný server, repliku alebo odosielajúci server), sa na paneli objavia rôzne návestia a tlačidlá.

- Ak je rolou podstromu replika, zobrazí sa návestie označujúce, že server koná ako replika alebo odosielajúci server, spolu s tlačidlom **Povýšiť server na hlavný server**. Ak kliknete na toto tlačidlo, server, ku ktorému je webový administratívny nástroj pripojený, sa stáva hlavným serverom.
- Keď bude pridaním pomocnej triedy (nie je prítomná predvolená skupina a podpoložka) podstrom nakonfigurovaný iba pre replikáciu, potom sa pri tlačidle **Replikovať podstrom** zobrazí návestie **Tento podstrom nie je replikovaný**. Ak kliknete na toto tlačidlo, pridajú sa štandardná skupina a podpoložka, takže server, ku ktorému je pripojený webový administratívny nástroj, sa stáva hlavným serverom.
- Ak sa nenájdu žiadne podpoložky pre hlavné servery, zobrazí sa návestie **Pre tento podstrom nie je definovaný žiadny hlavný server** spolu s tlačidlom nazvaným **Povýšiť server na hlavný server**. Ak kliknete na toto tlačidlo, pridá sa chýbajúca podpoložka, takže server, ku ktorému je nástroj správy webu pripojený, sa stáva hlavným serverom.

Odstránenie podstromu

1. Vyberte si podstrom, ktorý chcete odstrániť.
2. Kliknite na **Vymazať podstrom**.
3. Po výzve na potvrdenie vymazania kliknite na **OK**.

Podstrom bude odstránený zo zoznamu **Replikovaného podstromu**.

Poznámka: Táto operácia bude úspešná len vtedy, ak bude položka ibm-replicaGroup=default prázdna.

Uvedenie podstromu do stavu pokoja

Táto funkcia sa vám zíde, keď budete chcieť vykonať údržbu alebo zmeny topológie. Táto funkcia minimalizuje počet aktualizácií, ktoré možno na serveri vykonať. Server uvedený do stavu pokoja neprijíma požiadavky klienta. Požiadavky prijíma pomocou riadenia správy servera len od administrátora.

Ide o boolovskú funkciu.

1. Kliknutím na **Uviesť do stavu pokoja/aktivovať** uveďte podstrom do stavu pokoja.
2. Po výzve na potvrdenie akcie kliknite na **OK**.
3. Kliknutím na **Uviesť do stavu pokoja/aktivovať** aktivujte podstrom..
4. Po výzve na potvrdenie akcie kliknite na **OK**.

Úprava zoznamov riadenia prístupu

Replikačné informácie (podpoložky repliky, replikačné zmluvy, plány, možné povoľovacie údaje) sú uložené pod špeciálnym objektom **ibm-replicagroup=default**. Objekt ibm-replicagroup je umiestnený hneď pod koreňovou položkou replikovaného podstromu. Štandardne tento podstrom zdedí ACL od koreňovej položky replikovaného podstromu. Tento ACL nemusí byť vhodný na riadenie prístupu k replikačným informáciám.

Požadované oprávnenia:

- Riadiť replikáciu - musíte mať prístup na písanie k objektu ibm-replicagroup=default (alebo byť majiteľom/administrátorom).
- Replikácia kaskádovej kontroly - musíte mať prístup na písanie k objektu ibm-replicagroup=default (alebo byť majiteľom/administrátorom).
- Riadiť front - musíte mať prístup na písanie k replikačnej zmluve.

Ak si chcete pozrieť vlastnosti ACL pomocou webového administratívneho nástroja a pracovať s ACL, pozrite si “Manažovanie zoznamov riadenia prístupu (ACL)” na strane 179.

Viac informácií nájdete v časti “Zoznamy riadenia prístupu” na strane 55.

Zmena vlastností replikácie

Rozviňte kategóriu **Riadenie replikácie** v navigačnej oblasti a kliknite na **Riadiť vlastnosti replikácie**. Do webového administračného nástroja sa musíte prihlásiť ako projektovaný užívateľ s mimoriadnymi oprávneniami *ALLOBJ a *IOSYSCFG, aby ste mohli zmeniť nastavenia v paneloch **Riadiť vlastnosti replikácie**.

Na tomto paneli môžete:

- Zmeniť maximálny počet nevybavených zmien, ktoré sa vrátia z dotazov o stave replikácie. Štandardnou hodnotou je 200.
- Pridávať, upravovať alebo vymazávať informácie dodávateľa.

  Poznámka: DN dodávateľa môže byť DN projektovaného užívateľského profilu i5/OS. Projektovaný užívateľský profil i5/OS nesmie mať administračné oprávnenie LDAP. Užívateľom nemôže byť užívateľ so špeciálnymi oprávneniami *ALLOBJ a *IOSYSCFG a nemôže mu byť dané administračné oprávnenie cez ID aplikácie administrátora adresárového servera.

Detailnejšie informácie obsahujú časti:

- “Pridávanie informácií dodávateľa” na strane 142
- “Úprava informácií o dodávateľovi” na strane 142
- “Odstránenie informácií o dodávateľovi” na strane 142

Pridávanie informácií dodávateľa

1. Kliknite na **Pridať**.
2. Vyberte si dodávateľa z roletovej ponuky alebo zadajte názov replikovaného podstromu, ktorý chcete pridať ako dodávateľa.
3. Zadajte replikačný bind DN pre povoľovacie údaje.

   Poznámka: V závislosti od situácie môžete použiť ktorúkoľvek z týchto dvoch volieb.
   - Pomocou 'štandardných prihlasovacích údajov a odvolávky' nastavte DN pripojenia replikácie (a heslo) a štandardnú odvolávku pre všetky podstromy replikované do servera. Toto možno použiť vtedy, keď sú všetky podstromy replikované z rovnakého dodávateľa.
   - Pridaním informácií pre každý podstrom nastavte replikačný bind DN a heslo nezávisle pre každý replikovaný podstrom. Toto možno použiť vtedy, keď má každý podstrom iného dodávateľa (to znamená iný hlavný server pre každý podstrom).
4. V závislosti od typu povoľovacích údajov zadajte a potvrďte ich heslo (ktoré ste si predtým poznamenali na budúce použitie.)
   - **Simple Bind** - uveďte DN a heslo
   - **Kerberos** - uveďte pseudo DN v tvare 'ibm-kn=LDAP-service-name@realm' bez hesla
   - **SSL w/ EXTERNAL bind** - uveďte DN subjektu pre certifikát a neuvádzajte žiadne heslo

   Pozrite si "Vytvorenie povoľovacích údajov" na strane 128.
5. Kliknite na **OK**.

Podstrom dodávateľa je pridaný na zoznam dodávateľových informácií.

Úprava informácií o dodávateľovi

1. Vyberte si dodávateľský podstrom, ktorý chcete upravovať.
2. Kliknite na **Úprava**.
3. Ak upravujete **Štandardné prihlasovacie údaje a odvolávku**, ktorý sa používa na vytvorenie položky servera cn=Master pod cn=configuration, zadajte URL servera, z ktorej klient chce prijímať replikačné aktualizácie do štandardného poľa dodávateľa LDAP URL. Musí to byť platná LDAP URL (ldap://). V opačnom prípade prejdite na 4. krok.
4. Zadajte replikačný bind DN pre nové povoľovacie údaje, ktoré chcete použiť.
5. Zadajte a potvrďte heslo povoľovacích údajov.
6. Kliknite na **OK**.

Odstránenie informácií o dodávateľovi

1. Vyberte si dodávateľský podstrom, ktorý chcete odstrániť.
2. Kliknite na **Vymazať**.
3. Po výzve na potvrdenie vymazania kliknite na **OK**.

Podstrom bude odstránený zo zoznamu informácií o dodávateľovi.

Vytvorenie replikačných plánov

Voliteľne môžete definovať replikačné plány s cieľom naplánovať replikáciu na určitý čas alebo aby sa v určitom čase replikácia nevykonávala. Ak nepoužívate plán, server naplánuje replikáciu pri vykonaní každej zmeny, čo je to ekvivalent k zadávaniu plánu s okamžitou replikáciou so začiatkom po všetky dni na poludnie o 12:00.

Rozviňte kategóriu **Riadenie replikácie** v navigačnej oblasti a kliknite na **Riadiť plány**.

Na záložke **Týždenný plán** si vyberte podstrom, pre ktorý chcete vytvoriť plán a kliknite na **Zobraziť plány**. Ak už plány existujú, zobrazia sa v políčku **Týždenné plány**. Ak chcete vytvoriť alebo pridať nový plán:

1. Kliknite na **Pridať**.
2. Zadajte názov pre plán, napríklad **schedule1**.
3. Pre každý deň od nedele do soboty je denný plán uvedený ako **Žiadny**. Znamená to, že nie sú naplánované žiadne udalosti aktualizácie replikácie. Posledná replikačná udalosť, pokiaľ bola zadaná, zostáva v platnosti. Keďže toto je nová replika a neexistujú žiadne predchádzajúce replikačné udalosti, plán sa štandardne nastaví na okamžitú replikáciu.
4. Môžete si vybrať deň a kliknutím na **Pridať denný plán** vytvoriť preň denný plán replikácie. Ak vytvárate denný plán, tento sa stane štandardným plánom pre každý deň v týždni. Môžete:
   - Ponechajte denný plán ako štandardnú hodnotu pre každý deň alebo si vyberte konkrétny deň a zmeňte plán späť na žiadny. Nezabudnite, že posledná udalosť replikácie je stále v platnosti pre deň, ktorý nemá naplánované žiadne udalosti replikácie.
   - Denný plán zmeníte tak, že vyberiete deň a kliknete na **Upraviť denný plán**. Nezabúdajte, že zmeny denného plánu nadobúdajú účinok pre všetky dni používajúce plán, a nie len pre vami vybraný deň.
   - Ak chcete vytvoriť iný denný plán, vyberte deň a kliknite na **Pridať denný plán**. Po vytvorení tohto plánu sa plán pridá do roletovej ponuky **Denný plán**. Tento plán vyberte pre každý deň, v ktorý chcete, aby sa plán použil.

   Viac informácií o nastavovaní denných plánov nájdete v časti “Vytvorenie denného plánu”.
5. Po dokončení kliknite na **OK**.

Vytvorenie denného plánu

Rozviňte kategóriu **Riadenie replikácie** v navigačnej oblasti a kliknite na **Riadiť plány**.

Na záložke **Denný plán** si vyberte podstrom, pre ktorý chcete vytvoriť plán a kliknite na **Zobraziť plány**. Ak už plány existujú, zobrazia sa v políčku **Denné plány**. Ak chcete vytvoriť alebo pridať nový plán:

1. Kliknite na **Pridať**.
2. Zadajte názov pre plán, napríklad **monday1**.
3. Vyberte si nastavenie časovej zóny na univerzálny alebo miestny čas.
4. Z roletovej ponuky si vyberte typ replikácie:

   Okamžite
   Vykoná všetky čakajúce aktualizácie položiek od poslednej udalosti replikácie a aktualizuje položky kontinuálne až do dosiahnutia nasledujúcej naplánovanej udalosti aktualizácie.

   Raz Vykoná všetky čakajúce aktualizácie pred časom spustenia. Všetky aktualizácie vykonané po čase spustenia budú čakať až do nasledujúcej naplánovanej udalosti replikácie.
5. Vyberte čas spustenia (v miestnom čase servera) pre udalosť replikácie.
6. Kliknite na **Pridať**. Zobrazia sa čas a typ udalosti replikácie.
7. Pridaním alebo odstránením udalostí dokončite svoj plán. Zoznam udalostí sa bude obnovovať v chronologickom poradí.
8. Po dokončení kliknite na **OK**.

Napríklad:

Tabuľka 6.

Typ replikácie	Čas spustenia
Okamžite	12:00
Raz	10:00
Raz	14:00
Okamžite	16:00
Raz	20:00

V tomto pláne sa vyskytne prvá udalosť replikácie o polnoci a zaktualizuje všetky čakajúce zmeny predchádzajúce

uvedenému času. Aktualizácie replikácie sa budú naďalej vykonávať až do 10:00. Aktualizácie medzi 10:00 a 14:00 budú čakať na replikáciu až do 14:00. Aktualizácie vykonané medzi 14:00 a 16:00 budú čakať na udalosť replikácie naplánovanú na 16:00, potom bude replikácia pokračovať až do nasledujúcej naplánovanej udalosti replikácie o 20:00. Všetky aktualizácie vykonané po 20:00 budú čakať až do nasledujúcej naplánovanej udalosti replikácie.

Poznámka: Ak sú udalosti replikácie naplánované veľmi tesne a ak stále prebiehajú aktualizácie z predchádzajúcej udalosti v čase, kedy je naplánovaná nasledujúca udalosť, môže nastať vynechanie udalosti replikácie.

Riadenie frontov

Táto úloha vám umožní monitorovať stav replikácie pre každú replikačnú zmluvu (front) používanú týmto serverom.

Rozviňte kategóriu **Riadenie replikácie** v navigačnej oblasti a kliknite na **Riadiť fronty**.

Vyberte si repliku, pre ktorú chcete riadiť front.

- V závislosti od stavu repliky môžete kliknutím na **Pozastaviť/pokračovať** zastaviť alebo spustiť replikáciu.
- Ak chcete replikovať všetky čakajúce zmeny bez ohľadu na čas, na ktorý je replikácia naplánovaná, kliknite na **Vynútiť replikáciu**.
- Kliknutím na **Podrobnosti frontu** získate bližšie informácie o fronte repliky. Front môžete riadiť aj z tohto výberu.
- Kliknutím na **Obnoviť** môžete aktualizovať fronty a vymazať správy servera.

Podrobnosti frontu

Ak kliknete na **Podrobnosti frontu** zobrazia sa tri záložky:

- Stav
- Posledný pokus o získanie detailov
- Čakajúce zmeny

Záložka **Stav** zobrazuje názov repliky, jej podstrom, jeho stav a záznam časov replikácie. Z tohto panelu môžete pozastaviť replikáciu alebo v nej pokračovať kliknutím na **Obnoviť**. Kliknutím na **Obnoviť** aktualizujte informácie o fronte.

Záložka **Posledný pokus o získanie detailov** poskytuje informácie o poslednom pokuse o aktualizáciu. Ak nie je možné položku zaviesť, stlačte **Preskočiť blokujúcu položku** a pokračujte v replikácii s nasledujúcou čakajúcou položkou. Kliknutím na **Obnoviť** aktualizujte informácie o fronte.

Záložka **Čakajúce zmeny** zobrazuje všetky čakajúce zmeny v replike. Ak je replikácia zablokovaná, kliknutím na **Preskočiť všetko** môžete vymazať všetky čakajúce zmeny. Kliknutím na **Obnoviť** aktualizujte zoznam čakajúcich zmien s cieľom odzrkadliť každú novú aktualizáciu alebo aktualizácie, ktoré boli spracované.

Poznámka: Ak sa rozhodnete preskočiť blokujúce zmeny, musíte skontrolovať, či je daný server zákazníka skutočne aktualizovaný. Ďalšie informácie nájdete v časti “ldapdiff” na strane 210.

Nastavenie replikácie cez zabezpečené pripojenie

Replikácia cez SSL by sa mala nastaviť po etapách, aby ste si počas celého procesu mohli všetko skontrolovať.

Skôr ako sa pokúsite nakonfigurovať replikáciu cez zabezpečené pripojenie, mali by ste vykonať nasledujúce úlohy (v ľubovoľnom poradí):

- Nakonfigurujte replikáciu cez nezabezpečené pripojenie.
- Nakonfigurujte server spotrebiteľa, aby akceptoval zabezpečené pripojenia cez zabezpečený port. Skontrolujte, či klient môže použiť zabezpečené pripojenie k serveru spotrebiteľa, napríklad použitím pomocného programu ldapsearch. Ak chcete, aby server dodávateľa používal na autentifikáciu certifikát, ako napríklad externé vytváranie väzieb SASL cez SSL, najprv by ste mali nastaviť autentifikáciu servera a potom autentifikáciu klienta a servera, pričom ″server″ je server spotrebiteľa a klient je server dodávateľa.

Poznámka: Keď je server nakonfigurovaný, aby používal autentifikáciu klienta a servera, všetci klienti, používajúci SSL, musia mať klientsky certifikát.

- Nakonfigurujte server dodávateľa, aby dôveroval certifikačnej autorite, ktorá vydala certifikát spotrebiteľa.

1. V kategórii **Riadenie replikácie** vo webovom administračnom nástroji kliknite na **Riadiť topológiu**.
2. Vyberte niektorú z existujúcich zmlúv, ktorú chcete mať zabezpečenú.
3. Vyberte **Upraviť zmluvu...** a vyberte používanie SSL, pričom skontrolujte, či sa bude používať správne číslo portu. 636 je číslo štandardného zabezpečeného portu.
4. Skontrolujte, či replikácia zmluvy funguje správne.

Ak sa snažíte replikáciu nastaviť len pre autentifikáciu cez zabezpečené pripojenie pomocou DN a hesla, vykonalo sa to už v predchádzajúcich krokoch. Autentifikácia s použitím klientskeho certifikátu si vyžaduje, aby server dodávateľa používal vo svojej zmluve iný objekt poverení, a tiež si vyžaduje nakonfigurovanie servera spotrebiteľa, aby akceptoval takýto certifikát ako server dodávateľa.

Riadenie vlastností zabezpečenia

Adresárový server má mnoho mechanizmov na zaručenie bezpečnosti vašich údajov. K nim patrí riadenie hesiel, šifrovanie pomocou SSL a TLS, autentifikácia Kerberos a autentifikácia DIGEST-MD5. Bližšie informácie o základných pojmoch zabezpečenia nájdete v “Bezpečnosť adresárového servera” na strane 46.

Viac informácií nájdete v týchto častiach:

- “Riadenie hesiel”
- “Povolenie SSL a TLS (Transport Layer Security) v adresárovom serveri” na strane 149
- “Povolenie autentifikácie Kerberos na adresárovom serveri” na strane 151
- “Konfigurácia autentifikácie DIGEST-MD5 na adresárovom serveri” na strane 151

Riadenie hesiel

Ak chcete riadiť heslá, v navigačnej oblasti webového administračného nástroja rozviňte kategóriu **Riadiť vlastnosti zabezpečenia** a vyberte záložku **Politika hesiel**.

Viac informácií nájdete v týchto častiach:

- “Nastavenie vlastností hesiel”
- “Tipy pre politiku hesiel” na strane 147

Nastavenie vlastností hesiel

Adresárový server poskytuje mnohé voľby hesiel, aby sa zaručilo, že prístup do adresára budú mať len autorizovaní užívatelia. Tieto voľby sú zoskupené pod politikou hesiel, blokovaním hesiel a overením platnosti hesiel.

Politika hesiel

Pri nastavovaní politiky hesiel postupujte nasledovne:

1. V navigačnej oblasti webového administračného nástroja rozviňte kategóriu **Riadiť vlastnosti zabezpečenia** a vyberte záložku **Politika hesiel**.Tento panel zobrazí pole bez možnosti úprav **Atribút hesla**, ktoré obsahuje názov atribútu, ktorý používa politika hesiel.
2. Zo sťahovacieho zoznamu vyberte typ šifrovania hesiel:

   Žiadne Bez šifrovania. Heslá sa uložia vo formáte čitateľného textu.

   crypt Predtým ako sa heslá uložia do adresára, budú zakódované pomocou kódovacieho algoritmu crypt systému UNIX.

   SHA-1 Predtým ako sa heslá uložia do adresára, budú zakódované pomocou kódovacieho algoritmu SHA-1.
3. Ak chcete povoliť politiku hesiel, vyberte zaškrtávacie políčko**Politika hesiel je povolená**.

Poznámka: Ak politika hesiel nie je povolená, žiadne ďalšie funkcie na tomto alebo na iných paneloch hesiel nebudú dostupné, kým nebude zaškrtávacie políčko povolené. Štandardne je politika hesiel zakázaná.

4. Ak chcete zadať, že užívateľ môže zmeniť heslo, vyberte zaškrtávacie políčko**Užívateľ môže zmeniť heslo**.
5. Ak chcete zadať, že užívateľ musí po prihlásení zmeniť heslo resetovaným heslom, vyberte zaškrtávacie políčko **Užívateľ musí zmeniť heslo po resete**.
6. Ak chcete zadať, že užívateľ musí po úvodnom prihlásení znovu zadať heslo, aby mohol toto heslo zmeniť, vyberte zaškrtávacie políčko **Užívateľ musí odoslať heslo pri zmene hesla** .
7. Nastavte limit pre uplynutie doby platnosti hesla. Kliknite na prepínač**Doba platnosti hesla nikdy neuplynie**, ak chcete špecifikovať, že heslo netreba zmeniť v špecifickom časovom intervale, alebo kliknite na prepínač **Dni** a v dňoch zadajte časový interval, kedy sa musí heslo resetovať.
8. Špecifikuje, či systém vydá varovanie o uplynutí doby platnosti hesla predtým ako doba platnosti hesla uplynie.

   Ak kliknete na prepínač**Nikdy nevarovať**, užívateľ nedostane varovanie pred uplynutím doby platnosti predchádzajúceho hesla. Užívateľ nemôže pristúpiť na adresár, kým administrátor nevytvorí nové heslo.

   Ak kliknete na prepínač **Dni pred uplynutím doby platnosti** a zadáte počet dní (n), užívateľ dostane varovnú výzvu na zmenu hesla, vždy keď sa prihlási. Táto výzva sa začne objavovať n dní pred uplynutím doby platnosti. Užívateľ môže naďalej pristupovať na adresár, až kým neuplynie doba platnosti hesla.
9. Zadajte koľkokrát, ak vôbec, sa bude môcť užívateľ prihlásiť po uplynutí doby platnosti hesla. Tento výber povolí užívateľovi pristúpiť na adresár s heslom po dobe platnosti.
10. Kliknite na **OK**.

Poznámka: Na nastavenie politiky hesiel môžete použiť aj pomocný program ldapmodify (pozri “ldapmodify a ldapadd” na strane 185).

Viac informácií o politike hesiel nájdete v časti “Politika hesiel” na strane 66.

Blokovanie hesiel

1. V navigačnej oblasti webového administračného nástroja rozviňte kategóriu **Riadiť vlastnosti zabezpečenia** a vyberte záložku **Blokovanie hesiel**.

   Poznámka: Ak na serveri nie je povolená politika hesiel, funkcie na tomto paneli nevstúpia do platnosti.
2. Zadajte počet sekúnd, minút, hodín alebo dní, ktoré musia uplynúť predtým, ako budete môcť heslo zmeniť.
3. Zadajte, či nesprávne prihlásenia zablokujú heslo.
   - Vyberte prepínač **Heslá nebudú nikdy zablokované**, ak chcete povoliť neobmedzený počet pokusov o prihlásenie. Tento výber zakáže funkciu blokovania hesiel.
   - Vyberte prepínač Pokusy a zadajte počet pokusov o prihlásenie, ktoré budú povolené pred zablokovaním hesla. Tento výber povoľuje funkciu blokovania hesiel.
4. Špecifikujte dĺžku trvania blokovania. Vyberte prepínač **Doba platnosti blokovania nikdy neuplynie**, ak chcete zadať, že správca systému musí resetovať heslo, alebo vyberte prepínač **Sekundy** a zadajte počet sekúnd, po ktorom doba platnosti blokovania uplynie a pokusy o prihlásenie môžu pokračovať.
5. Zadajte dobu ukončenia platnosti pre nesprávne prihlásenie. Kliknite na prepínač **Nesprávne prihlásenia sa odstránia iba správnym heslom**, ak chcete zadať, že nesprávne prihlásenia odstráni iba úspešné prihlásenie, alebo kliknite na prepínače **Sekundy**a zadajte počet sekúnd, po ktorých bude neúspešný pokus o prihlásenie odstránený z pamäte.

   Poznámka: Táto voľba funguje iba vtedy, ak nebolo heslo zablokované.
6. Ak už budete mať všetko hotové, kliknite na tlačidlo **Použiť** a zmeny sa uložia bez ukončenia panelu, alebo kliknite na tlačidlo **OK** a zmeny sa uložia aj s ukončením panelu, alebo kliknite na tlačidlo **Zrušiť** a tento panel sa ukončí bez vykonania zmien.

Overenie platnosti hesla

1. V navigačnej oblasti webového administračného nástroja rozviňte kategóriu **Riadiť vlastnosti zabezpečenia** a vyberte záložku **Overenie platnosti hesiel**.

   Poznámka: Ak na serveri nie je povolená politika hesiel, funkcie na tomto paneli nevstúpia do platnosti.
2. Nastavte počet hesiel, ktoré sa musia použiť, aby sa po nich mohlo heslo opätovne použiť. Zadajte číslo od 0 do 30. Ak zadáte nulu, heslo sa bude môcť opätovne použiť bez obmedzenia.
3. V sťahovacej ponuke vyberte, či sa bude kontrolovať syntax hesiel, ktoré sú definované v nasledujúcich poliach vstupu. Môžete vybrať:

   Nekontrolovať syntax
   Kontrola syntaxe sa nevykoná.

   Kontrolovať syntax (okrem šifrovaných)
   Kontrola syntaxe sa vykoná na všetkých nezašifrovaných heslách.

   Kontrolovať syntax
   Kontrola syntaxe sa vykoná na všetkých heslách.
4. Zadajte číselnú hodnotu pre nastavenie minimálnej dĺžky hesla. Ak je hodnota nastavená na nulu, kontrola syntaxe sa nevykoná.
   - Zadajte číselnú hodnotu pre nastavenie minimálneho počtu abecedných znakov, ktorý sa pre heslo vyžaduje.
   - Zadajte číselnú hodnotu pre nastavenie minimálneho počtu numerických a špeciálnych znakov, ktorý sa pre heslo vyžaduje.

   Poznámka: Súčet minimálneho počtu abecedných, numerických a špeciálnych znakov sa musí rovnať alebo musí byť menší ako číslo, zadané pre minimálnu dĺžku hesla.
5. Zadajte maximálny počet znakov, ktoré sa môžu v hesle opakovať. Táto voľba ohraničuje koľkokrát sa môže špecifický znak v hesle objaviť. Ak je hodnota nastavená na nulu, počet opakovania znakov sa nebude kontrolovať.
6. Zadajte minimálny počet znakov, ktoré sa musia odlišovať od predchádzajúceho hesla a od počtu predchádzajúcich hesiel, ktorý je zadaný v poli **Minimálny počet hesiel pred opätovným použitím**. Ak je hodnota nastavená na nulu, počet odlišných znakov sa nebude kontrolovať.
7. Ak už budete mať všetko hotové, kliknite na tlačidlo **Použiť** a zmeny sa uložia bez ukončenia panelu, alebo kliknite na tlačidlo **OK** a zmeny sa uložia aj s ukončením panelu, alebo kliknite na tlačidlo **Zrušiť** a tento panel sa ukončí bez vykonania zmien.

Tipy pre politiku hesiel

Dotazy politiky hesiel

Operačné atribúty politiky hesiel sa dajú použiť na zobrazenie stavu položky adresára alebo na dotazovanie položiek, ktoré sa zhodujú so zadanými kritériami. Operačné atribúty budú vrátené v požiadavke na vyhľadávanie, iba ak ich bude klient špecificky požadovať. Ak chcete tieto atribúty používať v operáciách vyhľadávania, musíte mať povolenie pre najdôležitejšie atribúty alebo povolenie pre použité špecifické atribúty.

Ak chcete zobraziť všetky atribúty politiky hesiel pre danú položku:

```
> ldapsearch -b "uid=user1,cn=users,o=ibm" -s base "(objectclass=*)"
 pwdChangedTime pwdAccountLockedTime pwdExpirationWarned
 pwdFailureTime pwdGraceUseTime pwdReset
```

Ak chcete dotazovať položky, ktorým takmer uplynula doba platnosti hesla, použite atribút pwdChangedTime. Napríklad, ak chcete nájsť heslá, ktorých platnosť skončí 26. augusta 2004, pričom politika pre ukončenie platnosti hesiel je 186 dní, dotazujte sa na položky, ktorým bolo heslo zmenené najmenej pred 186 dňami (22. februára 2004):

```
> ldapsearch -b "cn=users,o=ibm" -s sub
 "(!(pwdChangedTime>20040222000000Z))" 1.1
```

pričom filter je rovnocenný s pwdChangedTime polnoc, 22. februára 2004.

Ak chcete dotazovať uzamknuté kontá, použite atribút pwdAccountLockedTime:

```
> ldapsearch -b "cn=users,o=ibm" -s sub "(pwdAccountLockedTime=*)" 1.1
```

pričom ″1.1″ označuje, že sa vrátia iba DN položiek.

Ak chcete dotazovať kontá, pri ktorých sa musí heslo zmeniť, pretože bolo heslo resetované, použite atribút pwdReset:

```
> ldapsearch -b "cn=users,o=ibm" -s sub "(pwdReset=TRUE)" 1.1
```

Vyradenie politiky hesiel

Správca adresárov môže vyradiť normálne správanie politiky hesiel pre špecifické položky tak, že upraví operačné atribúty politiky hesiel a použije riadenie správy servera (voľba -k pomocných programov príkazového riadku LDAP).

Pri konkrétnom účte môžete zamedziť uplynutiu doby platnosti hesla tak, že pri nastavovaní atribútu userPassword nastavíte atribút pwdChangedTime na dátum v ďalekej budúcnosti. V nasledujúcom príklade bude čas nastavený na polnoc, 1. januára 2200.

```
> ldapmodify -D cn=root -w ? -k
dn: uid=wasadmin,cn=users,o=ibm
changetype: modify
replace: pwdChangedTime
pwdChangedTime: 22000101000000Z
```

Konto, ktoré bolo uzamknuté kvôli nadmernému počtu zlyhaní prihlásenia môžete odomknúť, keď odstránite atribúty pwdAccountLockedTime a pwdFailureTime:

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
delete: pwdAccountLockedTime
-
delete: pwdFailureTime
```

Konto po dobe platnosti môžete odomknúť, keď zmeníte atribút pwdChangedTime a vyčistíte atribúty pwdExpirationWarned a pwdGraceUseTime:

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: pwdChangedTime
pwdChangedTime: 20040826000000Z
-
delete: pwdExpirationWarned
-
delete: pwdGraceUseTime
```

Stav ″heslo sa musí zmeniť″ môžete odstrániť alebo nastaviť, keď nastavíte atribút pwdReset:

```
> 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
```

Konto sa dá administračne uzamknúť, keď nastavíte operačný atribút ibm-pwdAccountLocked na hodnotu TRUE. Konto sa dá odomknúť nastavením atribútu na hodnotu FALSE. Tento spôsob odomknutia konta nemá vplyv na stav konta ohľadne jeho uzamknutia kvôli nadmernému počtu zlyhania hesla alebo kvôli heslu s ukončenou platnosťou.

Užívateľ, ktorý nastavuje tento atribút musí mať povolenie na zápis do atribútu ibm-pwdAccountLocked, ktorý je definovaný, že sa nachádza v triede prístupu CRITICAL.

```
> ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: TRUE
```

Ak chcete konto odomknúť:

```
> ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: FALSE
```

Iné tipy pre politiku hesiel

Existujú dve oblasti, v ktorých sa implementácia politiky hesiel nemusí správať podľa očakávaní:

1. Ak bol atribút pwdReset nastavený pre položku, klient môže do nekonečna vytvárať väzby pomocou DN položky a resetovacieho hesla. V prítomnosti Riadenia požiadaviek na politiku hesiel bude výsledkom úspešné vytvorenie väzieb s varovaním v riadení odozvy. Ale ak klient nezadá riadenie požiadaviek, tento klient, ″vedomý si neexistencie politiky hesiel″, uvidí úspešné vytvorenie väzieb bez indikácie, že heslo sa musí zmeniť. Následné operácie pod týmto DN budú stále zlyhávať s chybou ″nie je žiaduce vykonať″; iba výsledok úvodného vytvorenia väzieb sa môže zdať zavádzajúci. Môže to byť problémom, ak sa vytvorenie väzieb uskutočnilo iba kvôli autentifikácii, čo môže byť prípad webovej aplikácie, ktorá používa adresár na autentifikáciu.
2. Politiky pwdSafeModify a pwdMustChange sa nesprávajú podľa vašich očakávaní pri aplikácii, ktorá mení heslá pod inou identitou ako je DN položky, pre ktorú sa mení heslo. V tomto scenári bude výsledkom zmeny bezpečného hesla, ktorá sa uskutoční napríklad, pod administračnou identitou, nastavenie atribútu pwdReset. Aplikácia, ktorá mení heslá, môže použiť konto administrátora a odstrániť atribút pwdReset podľa skôr uvedeného popisu.

Povolenie SSL a TLS (Transport Layer Security) v adresárovom serveri

SSL

Ak máte na vašom systéme nainštalovaný manažér digitálnych certifikátov, na ochranu prístupu k vášmu adresárovému serveru môžete použiť bezpečnosť SSL (Secure Sockets Layer). Pred povolením SSL na adresárovom serveri si prečítajte “Secure Sockets Layer (SSL) a Transport Layer Security (TLS) s adresárovým serverom” na strane 47.

Ak chcete povoliť SSL na vašom serveri LDAP, postupujte nasledovne:

1. **Priradenie certifikátu k adresárovému serveru**
   a. Ak chcete svoj adresárový server riadiť prostredníctvom SSL pripojenia z iSeries Navigator, pozrite si príručku iSeries Access for Windows User’s Guide (voliteľne sa nainštaluje na vaše PC počas inštalácie iSeries Navigator). Ak plánujete pre adresárový server povoliť aj SSL aj iné ako SSL pripojenia, môžete si zvoliť preskočenie tohto kroku.
   b. Spustite IBM Digital Certificate Manager. Viac informácií nájdete v téme Manažér digitálnych certifikátov v časti Spustiť manažéra digitálnych certifikátov.
   c. Ak si chcete zaobstarať alebo vytvoriť certifikáty alebo inak nastaviť či zmeniť váš certifikačný systém, urobte to teraz. Informácie o nastavení certifikačného systému nájdete v časti Manažér digitálnych certifikátov. K adresárovému serveru sú priradené dve serverové a jedna klientska aplikácia. Sú to:

      Aplikácia adresárového servera
      Aplikáciou adresárového servera je server samotný.

      Aplikácia publikovania adresárového servera
      Aplikácia publikovania adresárového servera identifikuje certifikát používaný publikovaním.

      Klientska aplikácia adresárového servera
      Klientska aplikácia adresárového servera identifikuje štandardný certifikát používaný aplikáciami, ktoré používajú rozhrania API ILE klienta LDAP.

d. Kliknite na tlačidlo **Vybrať sklad certifikátov**.
e. Vyberte si ***SYSTEM**. Kliknite na **Pokračovať**.
f. Zadajte správne heslo pre sklad certifikátov *SYSTEM. Kliknite na **Pokračovať**.
g. Keď sa znova zavedie ľavá navigačná ponuka, rozviňte **Riadiť aplikácie**.
h. Kliknite na **Aktualizovať priradenie certifikátu**.
i. Na ďalšej obrazovke si vyberte **serverovú** aplikáciu. Kliknite na **Pokračovať**.
j. Vyberte si **Adresárový server**.
k. Kliknutím na **Aktualizovať priradenie certifikátu** priraďte certifikát adresárovému serveru, ktorý ho použije na vytvorenie svojej identity pre klientov iSeries Access for Windows.

Poznámka: Ak si vyberiete certifikát z CA, ktorý sa nenachádza vo vašej klientskej databáze kľúčov iSeries Access for Windows, budete ho musieť pridať, aby ste mohli používať SSL. Skôr než začnete s uvedenou procedúrou, dokončite túto.

l. Vyberte si certifikát zo zoznamu, ktorý priradíte k serveru.
m. Kliknite na **Priradiť nový certifikát**.
n. DCM sa znova zavedie do stránky **Aktualizovať priradenie certifikátu** s potvrdzujúcou správou. Po dokončení nastavenia certifikátov pre adresárový server kliknite na **Vykonané**.

2. **Priradenie certifikátu pre publikovanie adresárového servera**. (voliteľný krok) Ak chcete povoliť publikovanie zo systému do adresárového servera prostredníctvom SSL pripojenia, možno budete chcieť priradiť aj certifikát k publikovaniu adresárového servera. To identifikuje štandardný certifikát a dôveryhodné CA pre aplikácie používajúce LDAP ILE API, ktoré neuvádzajú ID svojej vlastnej aplikácie alebo alternatívnu kľúčovú databázu.
   a. Spustite IBM Digital Certificate Manager.
   b. Kliknite na tlačidlo **Vybrať sklad certifikátov**.
   c. Vyberte si ***SYSTEM**. Kliknite na **Pokračovať**.
   d. Zadajte správne heslo pre sklad certifikátov *SYSTEM. Kliknite na **Pokračovať**.
   e. Keď sa znova zavedie ľavá navigačná ponuka, rozviňte **Riadiť aplikácie**.
   f. Kliknite na **Aktualizovať priradenie certifikátu**.
   g. Na ďalšej obrazovke si vyberte **klientsku** aplikáciu. Kliknite na **Pokračovať**.
   h. Vyberte si **Publikovanie adresárového servera**.
   i. Kliknutím na **Aktualizovať priradenie certifikátu** priraďte certifikát k publikovaniu adresárového servera, ktorý ho použije na vytvorenie svojej identity.
   j. Vyberte si certifikát zo zoznamu, ktorý priradíte k serveru.
   k. Kliknite na **Priradiť nový certifikát**.
   l. DCM sa znova zavedie do stránky **Aktualizovať priradenie certifikátu** s potvrdzujúcou správou.

   Poznámka: Tieto kroky predpokladajú, že už publikujete informácie do adresárového servera s pripojením, ktoré nie je SSL. Úplné informácie o nastavení publikovania nájdete v časti “Publikovanie informácií na adresárový server” na strane 90.

3. **Priradenie certifikátu klientovi adresárového servera**. (voliteľný krok) Ak aj iné aplikácie používajú SSL pripojenia k adresárovému serveru, musíte klientovi adresárového serveru priradiť aj certifikát.
   a. Spustite IBM Digital Certificate Manager.
   b. Kliknite na tlačidlo **Vybrať sklad certifikátov**.
   c. Vyberte si ***SYSTEM**. Kliknite na **Pokračovať**.
   d. Zadajte správne heslo pre sklad certifikátov *SYSTEM. Kliknite na **Pokračovať**.
   e. Keď sa znova zavedie ľavá navigačná ponuka, rozviňte **Riadiť aplikácie**.
   f. Kliknite na **Aktualizovať priradenie certifikátu**.
   g. Na ďalšej obrazovke si vyberte **klientsku** aplikáciu. Kliknite na **Pokračovať**.
   h. Vyberte si **klienta adresárového servera**.

i. Kliknutím na **Aktualizovať priradenie certifikátu** priraďte certifikát klientovi adresárového servera, ktorý si vytvorí svoju identitu.
j. Vyberte si certifikát zo zoznamu, ktorý priradíte k serveru.
k. Kliknite na **Priradiť nový certifikát**.
l. DCM sa znova zavedie do stránky **Aktualizovať priradenie certifikátu** s potvrdzujúcou správou.

Po povolení SSL môžete zmeniť port, ktorý adresárový server používa pre zabezpečené pripojenia.

TLS

Ak chcete používať SSL alebo TLS, musíte ho povoliť v aplikácii iSeries Navigator.
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
4. V záložke **Sieť** označte zaškrtávacie políčko vedľa voľby **Zabezpečiť**.

Môžete zadať aj číslo portu, ktorý chcete zabezpečiť. Kliknutie na zaškrtávacie políčko **Zabezpečiť** je označením toho, že aplikácia môže spustiť SSL alebo TLS pripojenie cez zabezpečený port. Je to tiež označením toho, že aplikácia dokáže zadať operáciu StartTLS, aby povolila TLS pripojenie cez nezabezpečený port. Alebo sa môže TLS vyvolať použitím voľby -Y z pomocného programu klientskeho príkazového riadku. Ak používate príkazový riadok, atribút ibm-slapdSecurity sa musí rovnať hodnote TLS alebo SSLTLS.

Bližšie informácie o SSL a TLS nájdete v “Secure Sockets Layer (SSL) a Transport Layer Security (TLS) s adresárovým serverom” na strane 47.

Povolenie autentifikácie Kerberos na adresárovom serveri

Ak máte vo vašom systéme nakonfigurovanú službu sieťovej autentifikácie, adresárový server môžete nakonfigurovať na používanie autentifikácie Kerberos. Autentifikácia Kerberos sa týka užívateľov a administrátora. Skôr ako na adresárovom serveri povolíte Kerberos, prečítajte si Prehľad o používaní služby Kerberos so Adresárový server.

Ak chcete umožniť autentifikáciu Kerberosom, postupujte takto:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **IBM Directory Server** a vyberte **Vlastnosti**.
5. Kliknite na zložku **Kerberos**.
6. Začiarknite **Umožniť autentifikáciu Kerberosom**.
7. Podľa vašej konkrétnej situácie špecifikujte ďalšie nastavenia na strane **Kerberos**. Informácie o jednotlivých poliach nájdete v online pomoci.

Konfigurácia autentifikácie DIGEST-MD5 na adresárovom serveri

DIGEST-MD5 je autentifikačný mechanizmus SASL. Keď klient používa DIGEST-MD5, heslo nebude vysielané ako zrozumiteľný text a protokol zamedzí náporom odpovedí. Na konfiguráciu DIGEST-MD5 sa používa webový administračný nástroj.
1. V navigačnej oblasti rozviňte pod **Správa servera** kategóriu **Riadiť vlastnosti zabezpečenia** a vyberte záložku **DIGEST-MD5**.

   Poznámka: Ak chcete konfiguračné nastavenia servera zmeniť pomocou úloh z kategórie Správa servera vo webovom administračnom nástroji, musíte sa na server autentifikovať ako užívateľský profil i5/OS, ktorý má mimoriadne oprávnenia *ALLOBJ a IOSYSCFG. Docielite to autentifikáciou ako projektovaný užívateľ s heslom pre takýto profil. Ak chcete z webového administračného nástroja vytvoriť väzby ako projektovaný užívateľ, zadajte meno užívateľa vo forme os400-

profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, pričom reťazce MYUSERNAME a MYSYSTEM.COM budú nahradené názvom vášho užívateľského profilu a príponou projekcie nakonfigurovaného systému.

2. Pod **Realm servera** použite predvybraté **Predvolené** nastavenie, ktoré je plne kvalifikovaným názvom hostiteľa servera, alebo môžete kliknúť na **Realm** a napísať názov realmu, ktorý chcete nakonfigurovať ako server. Tento názov realmu používa klient na zistenie toho, ktoré meno užívateľa a heslo má použiť. Keď používate replikáciu, budete chcieť mať všetky servery nakonfigurované s rovnakým realmom.
3. Pod atribútom **Meno užívateľa** použite predvybraté **Predvolené** nastavenie, ktoré je uid, alebo môžete kliknúť na **Atribút** a napísať názov atribútu, ktorý má server použiť na jedinečnú identifikáciu položky užívateľa počas vytvárania väzieb DIGEST-MD5 SASL.
4. Ak ste prihlásený ako správca adresárov, do poľa **Administrátorské meno užívateľa** napíšte administrátorské meno užívateľa. Toto pole nemôžu upravovať členovia administračnej skupiny. Ak sa meno užívateľa, zadané vo vytváraní väzieb DIGEST-MD5 SASL, zhoduje s týmto reťazcom, užívateľ je administrátor.

   Poznámka: V administrátorskom mene užívateľa sa rozlišuje veľkosť písmen.
5. Po dokončení kliknite na **OK**.

Manažovanie schémy

Viac informácií o schéme nájdete v časti “Schéma” na strane 15.

Schému je možné manažovať pomocou webového administratívneho nástroja alebo aplikácie LDAP, podobnej ldapmodify v kombinácii so súbormi LDIF. Keď prvýkrát definujete nové triedy objektov alebo atribúty, najvhodnejšie bude použiť webový administračný nástroj. Ak musíte skopírovať novú schému do ostatných serverov (hoci ako súčasť produktu alebo nástroja, ktorý rozmiestňujete), možno bude vhodnejší pomocný program ldapmodify. Bližšie informácie nájdete v “Kopírovanie schémy do iných serverov” na strane 161.

Viac informácií nájdete v týchto častiach:

Zobrazenie tried objektov

Triedy objektov v schéme môžete zobraziť pomocou webového administratívneho nástroja (preferovanej metódy) alebo pomocou príkazového riadka.

Webová správa

Rozviňte **Manažment schém** v navigačnej oblasti a kliknite na **Manažovať triedy objektov**. Zobrazí sa panel len na čítanie, ktorý vám dovoľuje zobraziť triedy objektov v schéme a ich charakteristiky. Triedy objektov sú zobrazené v abecednom poradí. Klikaním na tlačidlá Predošlá alebo Ďalšia sa môžete posúvať o stranu dozadu alebo dopredu. Pole vedľa týchto tlačidiel identifikuje stranu, na ktorej sa nachádzate. Môžete tiež použiť sťahovaciu ponuku v tomto poli a preskočiť na špecifickú stranu. Prvá uvedená trieda objektov na strane je zobrazená s číslom strany, čo pomáha pri hľadaní triedy objektov, ktorú chcete zobraziť. Napríklad, ak ste hľadali triedu objektov **person**, rozviňte sťahovaciu

ponuku a rolujte nadol, kým neuvidíte **Strana 14 zo 16 nsLiServer** a **Strana 15 zo 16 printerLPR**. Trieda person je abecedne medzi nsLiServer a printerLPR, vyberte stranu 14 a kliknite na **Prejsť**.

Triedy objektov tiež môžete zobraziť zoradené podľa typu. Vyberte **Typ** a kliknite na **Zoradiť**. Triedy objektov sa zoradia abecedne podľa ich typu, abstraktný, pomocný alebo štrukturálny. Podobne môžete otočiť zoznam výberom **Zostupne** a kliknutím na **Zoradiť**.

Po nájdení požadovanej triedy objektov môžete zobraziť jej typ, dedičnosť, povinné atribúty a voliteľné atribúty. Rozviňte sťahovacie ponuky pre dedičnosť, povinné atribúty a voliteľné atribúty, aby sa zobrazil úplný výpis každej charakteristiky.

Môžete vybrať operácie na vykonanie s triedou objektov z lišty nástrojov napravo:

- Pridať
- Upraviť
- Kopírovať
- Vymazať

Keď to dokončíte, kliknite na tlačidlo **Zatvoriť**, aby ste sa vrátili do **Uvítacieho** panelu pre IBM Directory Server.

Príkazový riadok

Ak chcete zmeniť triedy objektov obsiahnuté v schéme, zadajte príkaz:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Pridanie triedy objektov

Webová správa

Ak ste tak ešte nespravili, rozviňte **Manažment schém** v navigačnej oblasti a kliknite na **Manažovať triedy objektov**. Ak chcete vytvoriť novú triedu objektov:

1. Kliknite na **Pridať**.

   Poznámka: K tomuto panelu sa tiež dostanete rozvinutím **Manažmentu schém** v navigačnej oblasti a kliknutím na **Pridať triedu objektov**.

2. Na záložke **Všeobecné vlastnosti**:
   - Zadajte **Názov triedy objektov**. Toto je povinné pole a má opisovať funkciu triedy objektov. Napríklad **tempEmployee** pre triedu objektov, používanú na sledovanie dočasných zamestnancov.
   - Zadajte **Opis** triedy objektov, napríklad **Trieda objektov použitá pre dočasných zamestnancov**.
   - Zadajte **OID** pre triedu objektov. Toto je povinné pole. Pozrite si časť “Identifikátor objektov (OID)” na strane 26. Ak nemáte OID, môžete použiť **Názov triedy objektov** s pridaným **-oid**. Napríklad, ak názov triedy objektov je **tempEmployee**, potom OID je **tempEmployee-oid**. Hodnotu tohto poľa môžete meniť.
   - Vyberte **Nadradená trieda objektov** zo sťahovacieho zoznamu. Toto určuje triedu objektov, z ktorej sa dedia ostatné atribúty. Typicky, **Nadradená trieda objektov** je **top**, ale môže to byť aj iná trieda objektov. Napríklad nadradená trieda objektov pre **tempEmployee** môže byť **ePerson**.
   - Vyberte **Typ triedy objektov**. Pozrite si časť “Triedy objektov” na strane 18, kde nájdete viac informácií o typoch tried objektov.
   - Kliknite na záložku Atribúty, ak chcete zadať povinné a voliteľné atribúty pre triedu objektov a zobraziť zdedené atribúty, alebo kliknite na **OK**, ak chcete pridať novú triedu objektov, alebo kliknite na **Zrušiť**, ak sa chcete vrátiť do **Manažovať triedy objektov** bez vykonania zmien.
3. Na záložke **Atribúty**:
   - Vyberte atribút z abecedného zoznamu **Dostupné atribúty** a kliknite na **Pridať k povinným**, ak chcete spraviť atribút povinným, alebo kliknite na **Pridať k voliteľným**, ak chcete spraviť atribút voliteľným pre triedu objektov. Atribút sa zobrazí v príslušnom zozname vybratých atribútov.

- Tento proces zopakujte pre všetky atribúty, ktoré chcete vybrať.
- Atribút môžete presunúť z jedného zoznamu do druhého alebo vymazať atribút z vybratých zoznamov jeho výberom a kliknutím na tlačidlo **Presunúť do** alebo **Vymazať**.
- Môžete zobraziť zoznamy povinných a voliteľných zdedených atribútov. Zdedené atribúty sú založené na **Nadradenej triede objektov**, vybratej na záložke **Všeobecné**. Zdedené atribúty nemôžete meniť. Ak zmeníte **Nadradenú triedu objektov** na záložke **Všeobecné**, zobrazí sa iná množina zdedených atribútov.

4. Kliknite na tlačidlo **OK**, ak chcete pridať novú triedu objektov alebo kliknite na tlačidlo **Zrušiť**, ak sa chcete vrátiť do panelu **Riadiť triedy objektov** bez vykonania zmien.

Poznámka: Ak ste klikli na tlačidlo **OK** na záložke **Všeobecné** bez pridania atribútov, atribúty môžete pridať úpravou novej triedy objektov.

Príkazový riadok

Ak chcete pridať triedu objektov pomocou príkazového riadka, zadajte tento príkaz:

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

kde <*filename*> obsahuje:

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: ( <myobjectClass-oid> NAME
'<myObjectClass>' DESC '<An
object class
                I defined for my LDAP application>' SUP '<objectclassinheritance>'
                <objectclasstype> MAY (<attribute1> $ <attribute2>))
```

Úprava triedy objektov

Nie sú dovolené všetky zmeny schémy. Pozrite si časť “Nedovolené zmeny schémy” na strane 28, kde nájdete obmedzenie zmien.

Webová správa

Ak ste tak ešte nespravili, rozviňte **Manažment schém** v navigačnej oblasti a kliknite na **Manažovať triedy objektov**. Ak chcete upraviť triedu objektov:

1. Kliknite na rádiové tlačidlo vedľa triedy objektov, ktorú chcete upraviť.
2. Kliknite na tlačidlo **Upraviť**.
3. Vyberte záložku:
   - Záložku **Všeobecné** použite na:
     - Zmeňte **Popis**.
     - Zmenu **Nadradenej triedy objektov**. Vyberte nadradenú triedu objektov zo sťahovacieho zoznamu. Toto určuje triedu objektov, z ktorej sa dedia ostatné atribúty. Typicky, **Nadradená trieda objektov** je **top**, ale môže to byť aj iná trieda objektov. Napríklad nadradená trieda objektov pre **tempEmployee** môže byť **ePerson**.
     - Zmenu **Typu triedy objektov**. Vyberte typ triedy objektov. Pozrite si časť “Triedy objektov” na strane 18, kde nájdete viac informácií o typoch tried objektov.
     - Kliknite na záložku Atribúty, ak chcete zmeniť povinné a voliteľné atribúty pre triedu objektov a zobraziť zdedené atribúty, alebo kliknite na **OK**, ak chcete pridať novú triedu objektov, alebo kliknite na **Zrušiť**, ak sa chcete vrátiť do **Manažovať triedy objektov** bez vykonania zmien.
   - Záložku **Atribúty** použite na:

     Vyberte atribút z abecedného zoznamu **Dostupné atribúty** a kliknite na **Pridať k povinným**, ak chcete spraviť atribút povinným, alebo kliknite na **Pridať k voliteľným**, ak chcete spraviť atribút voliteľným pre triedu objektov. Atribút sa zobrazí v príslušnom zozname vybratých atribútov.

Tento proces zopakujte pre všetky atribúty, ktoré chcete vybrať.

Atribút môžete presunúť z jedného zoznamu do druhého alebo vymazať atribút z vybratých zoznamov jeho výberom a kliknutím na tlačidlo **Presunúť do** alebo **Vymazať**.

Môžete zobraziť zoznamy povinných a voliteľných zdedených atribútov. Zdedené atribúty sú založené na **Nadradenej triede objektov**, vybratej na záložke **Všeobecné**. Zdedené atribúty nemôžete meniť. Ak zmeníte **Nadradenú triedu objektov** na záložke **Všeobecné**, zobrazí sa iná množina zdedených atribútov.

4. Kliknite na tlačidlo **OK**, ak chcete aplikovať zmeny, alebo kliknite na tlačidlo **Zrušiť**, ak sa chcete vrátiť na **Manažovať triedy objektov** bez vykonania zmien.

Príkazový riadok

Ak chcete zobraziť triedy objektov, obsiahnuté v schéme, zadajte príkaz:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Ak chcete upraviť triedu objektov pomocou príkazového riadka, zadajte tento príkaz:

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

kde <*filename*> obsahuje:

```
dn:
cn=schema
changetype: modify
replace: objectclasses
objectclasses: ( <myobjectClass-oid> NAME
'<myObjectClass>' DESC '<An
object class
                I defined for my LDAP application>' SUP '<newsuperiorclassobject>'
                <newobjectclasstype> MAY (attribute1> $ <attribute2>
                 $ <newattribute3>) )
```

Kopírovanie triedy objektov

Webová správa

Ak ste tak ešte nespravili, rozviňte **Manažment schém** v navigačnej oblasti a kliknite na **Manažovať triedy objektov**. Ak chcete skopírovať triedu objektov:

1. Kliknite na rádiové tlačidlo vedľa triedy objektov, ktorú chcete skopírovať.
2. Kliknite na tlačidlo **Kopírovať**.
3. Vyberte záložku:
   - Záložku **Všeobecné** použite na:
     - Zmeňte **názov triedy objektov**. Predvolený názov je názov kopírovanej triedy objektov, rozšírený o slovo COPY. Napríklad **tempPerson** sa skopíruje ako **tempPersonCOPY**.
     - Zmeňte **Popis**.
     - Zmeňte **OID**. Predvolené OID sa skopíruje do OID triedy objektov, rozšíreného o slovo COPY. Napríklad **tempPerson-oid** sa skopíruje ako **tempPerson-oidCOPY**.
     - Zmenu **Nadradenej triedy objektov**. Vyberte nadradenú triedu objektov zo sťahovacieho zoznamu. Toto určuje triedu objektov, z ktorej sa dedia ostatné atribúty. Typicky, **Nadradená trieda objektov** je **top**, ale môže to byť aj iná trieda objektov. Napríklad nadradená trieda objektov pre **tempEmployeeCOPY** môže byť **ePerson**.
     - Zmenu **Typu triedy objektov**. Vyberte typ triedy objektov. Pozrite si časť “Triedy objektov” na strane 18, kde nájdete viac informácií o typoch tried objektov.
     - Kliknite na záložku **Atribúty**, ak chcete zmeniť povinné a voliteľné atribúty pre triedu objektov a zobraziť zdedené atribúty, alebo kliknite na **OK**, ak chcete pridať novú triedu objektov, alebo kliknite na **Zrušiť**, ak sa chcete vrátiť do **Manažovať triedy objektov** bez vykonania zmien.
   - Záložku **Atribúty** použite na:

Vyberte atribút z abecedného zoznamu **Dostupné atribúty** a kliknite na **Pridať k povinným**, ak chcete spraviť atribút povinným, alebo kliknite na **Pridať k voliteľným**, ak chcete spraviť atribút voliteľným pre triedu objektov. Atribút sa zobrazí v príslušnom zozname vybratých atribútov.

Tento proces zopakujte pre všetky atribúty, ktoré chcete vybrať.

Atribút môžete presunúť z jedného zoznamu do druhého alebo vymazať atribút z vybratých zoznamov jeho výberom a kliknutím na tlačidlo **Presunúť do** alebo **Vymazať**.

Môžete zobraziť zoznamy povinných a voliteľných zdedených atribútov. Zdedené atribúty sú založené na **Nadradenej triede objektov**, vybratej na záložke **Všeobecné**. Zdedené atribúty nemôžete meniť. Ak zmeníte **Nadradenú triedu objektov** na záložke **Všeobecné**, zobrazí sa iná množina zdedených atribútov.

4. Kliknite na tlačidlo **OK**, ak chcete aplikovať zmeny, alebo kliknite na tlačidlo **Zrušiť**, ak sa chcete vrátiť na **Manažovať triedy objektov** bez vykonania zmien.

Príkazový riadok

Ak chcete zobraziť triedy objektov, obsiahnuté v schéme, zadajte príkaz:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Vyberte triedu objektov, ktorú chcete skopírovať. Pomocou editora zmeňte potrebné informácie a uložte zmeny do <*filename*>. Zadajte nasledujúci príkaz:

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

kde <*filename*> obsahuje:

```
dn:
cn=schema
changetype: modify
add: objectclasses
objectclasses: ( <mynewobjectClass-oid> NAME '<mynewObjectClass>'
                 DESC '<A new object class
                   I copied for my LDAP application>'
                SUP '<superiorclassobject>'<objectclasstype> MAY (attribute1>
$ <attribute2> $ <attribute3>) )
```

Vymazanie triedy objektov

Nie sú dovolené všetky zmeny schémy. Pozrite si časť “Nedovolené zmeny schémy” na strane 28, kde nájdete obmedzenie zmien.

Webová správa

Ak ste tak ešte nespravili, rozviňte **Manažment schém** v navigačnej oblasti a kliknite na **Manažovať triedy objektov**. Ak chcete vymazať triedu objektov:

1. Kliknite na rádiové tlačidlo vedľa triedy objektov, ktorú chcete vymazať.
2. Kliknite na tlačidlo **Vymazať**.
3. Budete požiadaný o potvrdenie vymazania triedy objektov. Kliknite na tlačidlo **OK**, ak chcete vymazať triedu objektov, alebo kliknite na tlačidlo **Zrušiť**, ak sa chcete vrátiť na **Manažovať triedy objektov** bez vykonania zmien.

Príkazový riadok

Ak chcete zobraziť triedy objektov, obsiahnuté v schéme, zadajte príkaz:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Vyberte triedu objektov, ktorú chcete vymazať a zadajte tento príkaz:

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

kde <*filename*> obsahuje:

```
dn:
cn=schema
changetype: modify
delete: objectclasses
objectclasses: (<myobjectClass-oid>)
```

Zobrazenie atribútov

Atribúty v schéme môžete zobraziť pomocou webového administratívneho nástroja (preferovanej metódy) alebo pomocou príkazového riadka.

Webová správa

Rozviňte **Manažment schém** v navigačnej oblasti a kliknite na **Manažovať atribúty**. Zobrazí sa panel len na čítanie, ktorý vám dovoľuje zobraziť atribúty v schéme a ich charakteristiky. Atribúty sú zobrazené v abecednom poradí. Klikaním na tlačidlá Predošlá alebo Ďalšia sa môžete posúvať o stranu dozadu alebo dopredu. Pole vedľa týchto tlačidiel identifikuje stranu, na ktorej sa nachádzate. Môžete tiež použiť sťahovaciu ponuku v tomto poli a preskočiť na špecifickú stranu. Prvá uvedená trieda objektov na strane je zobrazená s číslom strany, čo pomáha pri hľadaní triedy objektov, ktorú chcete zobraziť. Napríklad, ak ste hľadali atribút **authenticationUserID**, rozviňte sťahovaciu ponuku a rolujte nadol, kým neuvidíte **Strana 3 zo 62 applSystemHint** a **Strana 4 zo 62 authorityRevocatonList**. Atribút authenticationUserID je abecedne medzi applSystemHint a authorityRevocatonList, vyberte stranu 3 a kliknite na **Prejsť**.

Atribúty tiež môžete zobraziť zoradené podľa syntaxe. Vyberte **Syntax** a kliknite na **Zoradiť**. Atribúty sa zoradia abecedne podľa ich syntaxe. Pozrite si časť “Syntax atribútov” na strane 24, kde nájdete zoznam typov syntaxe. Podobne môžete otočiť zoznam výberom **Zostupne** a kliknutím na **Zoradiť**.

Po nájdení požadovaného atribútu môžete zobraziť jeho syntax, či je viachodnotový a triedy objektov, ktoré obsahuje. Rozviňte sťahovaciu ponuku pre triedy objektov, aby ste zobrazili zoznam tried objektov pre daný atribút.

Keď to dokončíte, kliknite na tlačidlo **Zatvoriť**, aby ste sa vrátili do **Uvítacieho** panelu pre IBM Directory Server.

Príkazový riadok

Ak chcete zobraziť atribúty obsiahnuté v schéme, zadajte príkaz:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Pridanie atribútu

Nový atribút môžete vytvoriť jednou z týchto metód. Preferovanou metódou je webový administratívny nástroj.

Webová správa

Ak ste tak ešte nespravili, rozviňte **Manažment schém** v navigačnej oblasti a kliknite na **Manažovať atribúty**. Ak chcete vytvoriť nový atribút:

1. Kliknite na **Pridať**.

   Poznámka: K tomuto panelu sa dostanete tiež rozvinutím položky **Manažment schém** v navigačnej oblasti a kliknutím na **Pridať atribút**.
2. Zadajte **Názov atribútu**, napríklad **tempId**. Toto pole je povinné a musí sa začínať abecedným znakom.
3. Zadajte **Opis** atribútu, napríklad **Číslo identifikátora, priradené k dočasnému zamestnancovi**.
4. Zadajte **OID** pre atribút. Toto je povinné pole. Pozrite si časť “Identifikátor objektov (OID)” na strane 26. Ak nemáte OID, môžete použiť názov atribútu, ku ktorému pridáte -oid. Ak je názov atribútu napríklad **tempID**, potom predvolené OID je **tempID-oid**. Hodnotu tohto poľa môžete meniť.

5. Zo sťahovacieho zoznamu vyberte **Nadradený atribút**. Nadradený atribút určuje atribút, z ktorého sa dedia vlastnosti.
6. Zo sťahovacieho zoznamu vyberte **Syntax**. Viac informácií o syntaxi nájdete v časti “Syntax atribútov” na strane 24.
7. Zadajte hodnotu **Dĺžka atribútu**, určujúcu maximálnu dĺžku tohto atribútu. Dĺžka je vyjadrená ako počet bajtov.
8. Ak chcete, aby atribút mohol mať viac hodnôt, vyberte začiarkavacie políčko **Povoliť viac hodnôt**.
9. Vyberte porovnávacie pravidlo zo sťahovacích ponúk porovnávacích pravidiel pre rovnosť, zoradenie, a podreťazec. Úplný zoznam porovnávacích pravidiel nájdete v časti “Pravidlá zhody” na strane 22.
10. Kliknite na záložku **Rozšírenia IBM**, aby ste zadali ďalšie rozšírenia pre atribút, alebo kliknite na tlačidlo **OK**, ak chcete pridať nový atribút, alebo kliknite na tlačidlo **Zrušiť**, ak sa chcete vrátiť do panelu **Riadiť atribúty** bez vykonania zmien.
11. V záložke **Rozšírenia IBM**:
    - Zmeňte **Názov tabuľky DB2** . Ak necháte toto pole prázdne, názov tabuľky DB2 vygeneruje server. Ak zadáte názov tabuľky DB2, musíte zadať aj názov stĺpca DB2.
    - Zmeňte **Názov stĺpca DB2**. Ak necháte toto pole prázdne, názov stĺpca DB2 vygeneruje server. Ak zadáte názov stĺpca DB2, musíte zadať aj názov tabuľky DB2.
    - Výberom hodnoty **normálna**, **citlivá** alebo **kritická** zo sťahovacieho zoznamu nastavte **Triedu bezpečnosti**.
    - Výberom jedného alebo viacerých indexovacích pravidiel nastavte **Indexovacie pravidlá**. Viac informácií o indexovacích pravidlách nájdete v časti “Pravidlá indexovania” na strane 23.

    Poznámka: Odporúča sa nastaviť minimálne Indexovanie rovnosti pre všetky atribúty, ktoré sa budú používať vo vyhľadávacích filtroch.
12. Ak chcete pridať nový atribút, kliknite na **OK**, alebo ak sa chcete bez vykonania zmien vrátiť do časti **Manažovanie atribútov**, kliknite na **Zrušiť**.

Poznámka: Ak ste na záložke Všeobecné klikli na tlačidlo OK bez pridania rozšírení, môžete rozšírenia pridať úpravou nového atribútu.

Príkazový riadok

Tento príklad pridá definíciu typu atribútu pre atribút s názvom ″myAttribute″, so syntaxou Reťazec adresára (pozrite si časť “Syntax atribútov” na strane 24) a porovnávaním Zhoda s ignorovaním veľkosti písmen (pozrite si časť “Pravidlá zhody” na strane 22). Časť definície, špecifická pre IBM hovorí, že údaje atribútu sú uložené v stĺpci s názvom ″myAttrColumn″ v tabuľke s názvom ″myAttrTable″. Ak tieto názvy nie sú zadané, názov stĺpca aj tabuľky sa nastaví na predvolenú hodnotu ″myAttribute″. Atribút je priradený k triede prístupu ″normálna″ a hodnoty majú maximálnu dĺžku 200 bajtov.

```
ldapmodify -D < admindn> -w
<adminpw> -i myschema.ldif
```

Pričom súbor **myschema.ldif** obsahuje:

```
dn:
cn=schema
changetype: modify
add: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' )
                 DESC 'Atribút definovaný pre moju aplikáciu LDAP'
                 EQUALITY 2.5.13.2 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  USAGE userApplications )
-
add:ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                    ACCESS-CLASS normal LENGTH 200 )
```

Viac informácií o tomto príklade nájdete v časti “ldapmodify a ldapadd” na strane 185.

Úprava atribútu

Nie sú dovolené všetky zmeny schémy. Pozrite si časť “Nedovolené zmeny schémy” na strane 28, kde nájdete obmedzenie zmien.

Pred pridaním položiek využívajúcich daný atribút je možné zmeniť ľubovoľnú časť definície. Atribút môžete upraviť jednou z týchto metód. Preferovanou metódou je webový administratívny nástroj.

Webová správa

Ak ste tak ešte nespravili, rozviňte **Manažment schém** v navigačnej oblasti a kliknite na **Manažovať atribúty**. Ak chcete upraviť atribút:

1. Kliknite na rádiové tlačidlo vedľa atribútu, ktorý chcete upraviť.
2. Kliknite na tlačidlo **Upraviť**.
3. Vyberte záložku:
   - Záložku **Všeobecné** použite na:
     – Vyberte záložku:
       - **Všeobecné**, ak chcete:
         • Zmeniť **Popis**
         • Zmeniť **Syntax**
         • Nastaviť **Dĺžku atribútu**
         • Zmeniť nastavenia **Viac hodnôt**
         • Vybrať **Porovnávacie pravidlo**
         • Zmeniť **Nadradený atribút**
       - Kliknite na záložku **Rozšírenia IBM**, ak chcete upraviť rozšírenia pre atribút, alebo kliknite na tlačidlo **OK**, ak chcete svoje zmeny použiť alebo kliknite na tlačidlo **Zrušiť**, ak sa chcete vrátiť do panelu **Riadiť atribúty** bez vykonania zmien.
       - **Rozšírenia IBM**, ak používate IBM Directory Server na:
         • Zmeniť **Triedu bezpečnosti**
         • Zmeniť **Indexovacie pravidlá**
     – Ak chcete aplikovať vaše zmeny, kliknite na **OK**, alebo ak sa chcete bez vykonania zmien vrátiť do časti **Manažovanie atribútov**, kliknite na **Zrušiť**.
4. Ak chcete aplikovať zmeny, kliknite na **OK**, alebo ak sa chcete bez vykonania zmien vrátiť do časti **Manažovanie atribútov**, kliknite na **Zrušiť**.

Príkazový riadok

Tento príklad pridá indexovanie pre atribút, takže jeho vyhľadávanie bude rýchlejšie. Definíciu môžete zmeniť pomocou príkazu ldapmodify a súboru LDIF:

```
ldapmodify -D <admindn> -w <adminpw> -i myschemachange.ldif
```

Pričom súbor **myschemachange.ldif** obsahuje:

```
dn:
cn=schema
changetype: modify
replace: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' ) DESC 'Atribút
                 definovaný pre moju aplikáciu LDAP' EQUALITY 2.5.13.2
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
replace: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                  ACCESS-CLASS normal LENGTH 200 EQUALITY SUBSTR )
```

Poznámka: V operácii nahradenia musia byť zahrnuté obe časti definície (**attributetypes** a **ibmattributetypes**), aj keď sa mení len časť **ibmattributetypes**. Jedinou zmenou je pridanie ″EQUALITY SUBSTR″ na koniec definície, aby sa vyžadovali indexy pre porovnávanie rovnosti a podreťazcov.

Viac informácií o tomto príklade nájdete v časti “ldapmodify a ldapadd” na strane 185.

Kopírovanie atribútu

Atribút môžete skopírovať jednou z týchto metód. Preferovanou metódou je webový administratívny nástroj.

Webová správa

Ak ste tak ešte nespravili, rozviňte **Manažment schém** v navigačnej oblasti a kliknite na **Manažovať atribúty**. Ak chcete skopírovať atribút:

1. Kliknite na rádiové tlačidlo vedľa atribútu, ktorý chcete skopírovať.
2. Kliknite na tlačidlo **Kopírovať**.
3. Zmeňte **Názov atribútu**. Predvolený názov je skopírovaný názov atribútu s pridaným slovom COPY. Napríklad **tempID** sa skopíruje ako **tempIDCOPY**.
4. Zmeňte **Popis** atribútu, napríklad, **ID číslo priradené brigádnikovi**.
5. Zmeňte **OID**. Predvolené OID je OID skopírovaného atribútu s pridaným slovom COPYOID. Napríklad **tempID-oid** sa skopíruje ako **tempID-oidCOPYOID**.
6. Zo sťahovacieho zoznamu vyberte **Nadradený atribút**. Nadradený atribút určuje atribút, z ktorého sa dedia vlastnosti.
7. Zo sťahovacieho zoznamu vyberte **Syntax**. Viac informácií o syntaxi nájdete v časti “Syntax atribútov” na strane 24.
8. Zadajte hodnotu **Dĺžka atribútu**, určujúcu maximálnu dĺžku tohto atribútu. Dĺžka je vyjadrená ako počet bajtov.
9. Ak chcete, aby atribút mohol mať viac hodnôt, vyberte začiarkavacie políčko **Povoliť viac hodnôt**.
10. Vyberte porovnávacie pravidlo zo sťahovacích ponúk porovnávacích pravidiel pre rovnosť, zoradenie, a podreťazec. Úplný zoznam porovnávacích pravidiel nájdete v časti “Pravidlá zhody” na strane 22.
11. Kliknite na záložku **Rozšírenia IBM**, ak chcete zmeniť ďalšie rozšírenia pre atribút, alebo kliknite na tlačidlo **OK**, ak chcete použiť svoje zmeny, alebo kliknite na tlačidlo **Zrušiť**, ak sa chcete vrátiť do panelu **Riadiť atribúty** bez vykonania zmien.
12. V záložke **Rozšírenia IBM**:
    - Zmeňte **Názov tabuľky DB2** . Ak necháte toto pole prázdne, názov tabuľky DB2 vygeneruje server. Ak zadáte názov tabuľky DB2, musíte zadať aj názov stĺpca DB2.
    - Zmeňte **Názov stĺpca DB2**. Ak necháte toto pole prázdne, názov stĺpca DB2 vygeneruje server. Ak zadáte názov stĺpca DB2, musíte zadať aj názov tabuľky DB2.
    - Zmeňte **Triedu zabezpečenia** tak, že z roletového zoznamu vyberiete **normálne**, **citlivé** alebo **kritické**.
    - **Pravidlá indexovania** zmeníte výberom jedného alebo viacerých pravidiel indexovania. Viac informácií o indexovacích pravidlách nájdete v časti “Pravidlá indexovania” na strane 23.

      Poznámka: Odporúča sa nastaviť minimálne Indexovanie rovnosti pre všetky atribúty, ktoré sa budú používať vo vyhľadávacích filtroch.
13. Ak chcete aplikovať vaše zmeny, kliknite na **OK**, alebo ak sa chcete bez vykonania zmien vrátiť do časti **Manažovanie atribútov**, kliknite na **Zrušiť**.

Poznámka: Ak ste na záložke **Všeobecné** klikli na tlačidlo **OK** a nepridali ste žiadne rozšírenia, rozšírenia môžete pridať alebo zmeniť úpravou nového atribútu.

Príkazový riadok

Ak chcete zobraziť atribúty obsiahnuté v schéme, zadajte príkaz:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Vyberte atribút, ktorý chcete skopírovať. Pomocou editora zmeňte potrebné informácie a uložte zmeny do <*filename*>. Potom zadajte tento príkaz:

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

kde <*filename*> obsahuje:

```
dn:
cn=schema
changetype: modify
add: attributetypes
attributetypes: ( <mynewAttribute-oid> NAME '<mynewAttribute>' DESC '<Nový
                 skopírovaný atribút pre moju aplikáciu LDAP> EQUALITY 2.5.13.2
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
add:ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                    ACCESS-CLASS normal LENGTH 200 )
```

Vymazanie atribútu

Nie sú dovolené všetky zmeny schémy. Pozrite si časť “Nedovolené zmeny schémy” na strane 28, kde nájdete obmedzenie zmien.

Atribút môžete vymazať jednou z týchto metód. Preferovanou metódou je webový administratívny nástroj.

Webová správa

Ak ste tak ešte nespravili, rozviňte **Manažment schém** v navigačnej oblasti a kliknite na **Manažovať atribúty**. Ak chcete vymazať atribút:

1. Kliknite na rádiové tlačidlo vedľa atribútu, ktorý chcete vymazať.
2. Kliknite na tlačidlo **Vymazať**.
3. Budete požiadaný o potvrdenie vymazania atribútu. Ak chcete vymazať atribút, kliknite na **OK**, alebo ak sa chcete bez vykonania zmien vrátiť do časti **Manažovanie atribútov**, kliknite na **Zrušiť**.

Príkazový riadok

```
ldapmodify -D <admindn> -w <adminpw> -i myschemadelete.ldif
```

Pričom súbor **myschemadelete.ldif** zahŕňa:

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

Viac informácií o tomto príklade nájdete v časti “ldapmodify a ldapadd” na strane 185.

Kopírovanie schémy do iných serverov

Ak chcete skopírovať schému do iných serverov, vykonajte toto:

1. Pomocou nástroja ldapsearch skopírujte schému do súboru:

   ```
   ldapsearch -b cn=schema -L "(objectclass=*)" > schema.ldif
   ```

2. Súbor schémy bude obsahovať všetky triedy objektov a atribúty. Upravte súbor LDIF, ak chcete zahrnúť iba vami požadované prvky schémy, alebo budete môcť filtrovať výstup ldapsearch s požitím nástroja, ako napríklad grep. Skontrolujte, že ste umiestnili atribúty pred triedy objektov, ktoré sa na ne odvolávajú. Môžete získať napríklad takýto súbor (všimnite si, že každý riadok, na ktorý nadväzuje ďalší riadok má na konci jednu medzeru a nadväzujúci riadok má na začiatku aspoň jednu medzeru).

   ```
   attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Vhodné
     informácie.' 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 'Vhodné
  informácie.' 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 'Reprezentácia
  objektu.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

3. Vložením riadkov pred každý riadok typu objectclasses alebo attributetype vytvorte direktívy LDIF, na základe ktorých sa tieto hodnoty pridajú do položky cn=schema. Každú triedu objektov a atribút musíte pridať ako samostatnú modifikáciu.

```
dn:
cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Vhodné
  informácie.' 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 'Vhodné
  informácie.' 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 'Reprezentácia
  objektu.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

4. Pomocou nástroja ldapmodify načítajte túto schému do iných serverov:

```
ldapmodify -D cn=administrator -w <password> -f schema.ldif
```

Manažovanie položiek adresára

Ak chcete manažovať položky adresára, rozviňte kategóriu **Manažment adresárov** v navigačnej oblasti webového administratívneho nástroja.

Viac informácií nájdete v týchto častiach:

- “Prehľadanie stromu” na strane 163
- “Pridanie položky” na strane 163
- “Pridanie položky, ktorá obsahuje atribúty s označeniami jazyka” na strane 163
- “Kopírovanie užívateľov z validačného zoznamu servera HTTP na Adresárový server” na strane 92
- “Vymazanie položky” na strane 164
- “Úprava položky” na strane 164
- “Kopírovanie položky” na strane 165
- “Úprava zoznamov riadenia prístupu” na strane 165
- “Pridanie pomocnej triedy objektov” na strane 165
- “Vymazanie pomocnej triedy” na strane 166
- “Zmena členstva v skupine” na strane 166

- “Hľadanie položiek adresára” na strane 166
- “Zmena binárnych atribútov” na strane 168

Prehľadanie stromu

Ak ste tak ešte nespravili, rozviňte kategóriu **Manažment adresárov** v navigačnej oblasti a kliknite na **Manažovať položky**. Môžete rozvinúť rôzne podstromy a vybrať položku, s ktorou chcete pracovať. Z lišty nástrojov napravo môžete vybrať operáciu, ktorú chcete vykonať.

Pridanie položky

Ak ste tak ešte nespravili, rozviňte kategóriu **Manažment adresárov** v navigačnej oblasti.

1. Kliknite na **Pridať položku**.
2. Zo sťahovacieho zoznamu vyberte jednu **Štrukturálnu triedu objektov**.
3. Kliknite na tlačidlo **Ďalej**.
4. Z poľa Dostupné vyberte ľubovoľné **Pomocné triedy objektov**, ktoré chcete použiť a kliknite na **Pridať**. Opakujte tento proces pre každú pomocnú triedu objektov, ktorú chcete pridať. Z poľa Vybraté môžete odstrániť pomocnú triedu objektov tak, že ju vyberiete a kliknete na **Odstrániť**.
5. Kliknite na tlačidlo **Ďalej**.
6. V poli **Relatívne DN** zadajte relatívny rozlišovací názov (RDN) položky, ktorú pridávate, napríklad cn=John Doe.
7. V poli **Rodičovské DN** zadajte rozlišovací názov vybratej položky stromu, napríklad ou=Austin, o=IBM. Môžete tiež kliknúť na **Prehľadať** a vybrať Rodičovské DN zo zoznamu. Môžete tiež rozvinúť výber a zobraziť ostatné voľby hlbšie v strome. Zadajte vašu voľbu a kliknutím na **Vybrať** určite požadované Rodičovské DN. **Rodičovské DN** sa štandardne nastaví na vybratú položku v strome.

   Poznámka: Ak ste túto úlohu spustili z panelu **Manažment položiek**, toto pole je vopred vyplnené.
8. Na záložke **Povinné atribúty** zadajte hodnoty pre povinné atribúty. Ak chcete pre určitý atribút pridať viac ako jednu hodnotu, kliknite na **Viac hodnôt** a potom po jednej pridávajte hodnoty.
9. Kliknite na **Voliteľné atribúty**.
10. Na záložke **Voliteľné atribúty** zadajte vhodné hodnoty pre voliteľné atribúty. Informácie o pridávaní binárnych hodnôt nájdete v časti “Zmena binárnych atribútov” na strane 168. Ak chcete pre určitý atribút pridať viac ako jednu hodnotu, kliknite na **Viac hodnôt** a potom po jednej pridávajte hodnoty.
11. Kliknutím na OK vytvorte položku.
12. Kliknite na tlačidlo **ACL**, ak chcete zmeniť zoznam riadenia prístupu pre túto položku. Informácie o zoznamoch ACL nájdete v časti “Zoznamy riadenia prístupu” na strane 55.
13. Po vyplnení aspoň povinných polí pridajte novú položku kliknutím na **Pridať** alebo sa kliknutím na **Zrušiť** bez vykonania zmien vráťte do časti **Prehliadací strom**.

Pridanie položky, ktorá obsahuje atribúty s označeniami jazyka

Kódy jazyka môžete priradiť k hodnotám v adresári, aby ste klientom umožnili vyhľadávať v adresári hodnoty, ktoré spĺňajú určité jazykové požiadavky. Označenie jazyka je komponent popisu atribútu. Bližšie informácie o označeniach jazyka nájdete v “Jazykové značky” na strane 44.

Ak chcete povoliť označenia jazyka, postupujte nasledovne (predvolene sú zakázané):

1. Kliknite na **Riadiť vlastnosti servera** v kategórii **Správa servera** v navigačnej oblasti.

   Poznámka: Ak chcete konfiguračné nastavenia servera zmeniť pomocou úloh z kategórie Správa servera vo webovom administračnom nástroji, musíte sa na server autentifikovať ako užívateľský profil i5/OS, ktorý má mimoriadne oprávnenia *ALLOBJ a IOSYSCFG. Docielite to autentifikáciou ako projektovaný užívateľ s heslom pre takýto profil. Ak chcete z webového administračného nástroja vytvoriť väzby ako projektovaný užívateľ, zadajte meno užívateľa vo forme os400-

profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, pričom reťazce MYUSERNAME a MYSYSTEM.COM budú nahradené názvom vášho užívateľského profilu a príponou projekcie nakonfigurovaného systému.

2. Záložka Všeobecné je predvybratá. Kliknite na zaškrtávacie políčko**Povoliť podporu označenia jazyka**, ak ho chcete povoliť.

Poznámka: Keď povolíte funkciu označenia jazyka a ak priraďujete označenia jazyka k atribútom položky, server vráti položku s označeniami jazyka. Bude k tomu dochádzať aj keď neskôr zakážete funkciu označenia jazyka. Pretože server sa nemusí správať podľa očakávaní aplikácie, preto ak sa chcete vyhnúť možným problémom, nezakazujte funkciu označovania jazyka, keď ste ju povolili.

Ak chcete vytvoriť položku, ktorá bude obsahovať atribúty s označením jazyka:

1. V navigačnej oblasti v kategórii **Riadenie adresárov** kliknite na **Riadiť položky**.
2. Kliknite na tlačidlo **Upraviť atribúty**.
3. Vyberte atribút, pre ktorý chcete vytvoriť označenie jazyka.
4. Kliknite na tlačidlo **Hodnota označenia jazyka**, ak chcete pristúpiť na panel **Hodnoty označenia jazyka**.
5. Do poľa **Označenie jazyka** zadajte názov označenia, ktoré vytvárate. Označenie musí začínať príponou lang-.
6. Hodnotu pre označenie zadajte do poľa **Hodnota**.
7. Kliknite na **Pridať**.Označenie jazyka a jeho hodnota sa zobrazia v ponukovom zozname.
8. Ak chcete pre atribút vytvoriť ďalšie označenia jazyka, alebo ak mu chcete zmeniť existujúce označenia jazyka, zopakujte kroky 3, 4 a 5. Keď ste vytvorili vami požadované označenia jazyka, kliknite na tlačidlo **OK**.
9. Rozviňte ponuku **Zobraziť s označením jazyka** a vyberte označenie jazyka. Kliknite na **Zmeniť zobrazenie** a zobrazia sa hodnoty atribútu, ktoré ste zadali pre toto označenie jazyka. Všetky hodnoty, ktoré v tomto zobrazení pridáte alebo upravíte sa použijú len pre vybratý jazyk.
10. Keď to dokončíte, kliknite na tlačidlo **OK**.

Vymazanie položky

Ak ste tak ešte nespravili, rozviňte kategóriu **Manažment adresárov** v navigačnej oblasti a kliknite na **Manažovať položky**. Môžete rozvinúť rôzne podstromy a vybrať podstrom, príponu alebo položku, s ktorou chcete pracovať. Kliknite na tlačidlo **Vymazať** na lište nástrojov napravo.

- Budete požiadaný o potvrdenie vymazania. Kliknite na **OK**.
- Položka sa z adresára vymaže a vy sa vrátite do zoznamu položiek.

Úprava položky

Ak ste tak ešte nespravili, rozviňte kategóriu **Manažment adresárov** v navigačnej oblasti a kliknite na **Manažovať položky**. Môžete rozvinúť rôzne podstromy a vybrať položku, s ktorou chcete pracovať. Kliknite na tlačidlo **Upraviť atribúty** na lište nástrojov napravo.

1. Na záložke **Povinné atribúty** zadajte hodnoty pre povinné atribúty. Informácie o pridávaní binárnych hodnôt nájdete v časti “Zmena binárnych atribútov” na strane 168. Ak chcete pre určitý atribút pridať viac ako jednu hodnotu, kliknite na **Viac hodnôt** a potom po jednej pridávajte hodnoty.
2. Kliknite na **Voliteľné atribúty**.
3. Na záložke **Voliteľné atribúty** zadajte vhodné hodnoty pre voliteľné atribúty. Ak chcete pre určitý atribút pridať viac ako jednu hodnotu, kliknite na **Viac hodnôt** a potom po jednej pridávajte hodnoty.
4. Kliknite na **Členstvá**.
5. Ak ste vytvorili skupiny, na záložke **Členstvá**:
   - Z ponuky **Dostupné skupiny** vyberte skupinu a kliknite na **Pridať**, aby sa z položky stal člen vybratého **Členstva v statickej skupine**.
   - Z **Členstiev v statických skupinách** vyberte skupinu a kliknutím na **Odstrániť** odstráňte položku z vybratej skupiny.

6. Ak je položka položkou skupiny, je dostupná záložka **Členy**. Záložka **Členy** zobrazuje členy vybratej skupiny. Môžete pridávať a odstraňovať členy zo skupiny.
   - Ak chcete do skupiny pridať člen:
     a. Buď na záložke **Členy** kliknite na **Viac hodnôt** alebo na záložke **Členy** kliknite na **Členy**.
     b. V poli Člen zadajte DN položky, ktorú chcete pridať.
     c. Kliknite na **Pridať**.
     d. Kliknite na **OK**.
   - Ak chcete zo skupiny odstrániť člen:
     a. Buď kliknite na **Viacero hodnôt** na záložke **Členovia** alebo kliknite na záložku **Členovia** a kliknite na **Členovia**.
     b. Vyberte položku, ktorú chcete odstrániť.
     c. Kliknite na **Odstrániť**.
     d. Kliknite na **OK**.
   - Ak chcete obnoviť zoznam členov, kliknite na **Zaktualizovať**.
7. Ak chcete položku zmeniť, kliknite na tlačidlo **OK**.

Kopírovanie položky

Táto funkcia je užitočná pri vytváraní podobných položiek. Kópia zdedí všetky atribúty pôvodnej položky. Musíte vykonať niektoré úpravy a pomenovať novú položku.

Ak ste tak ešte nespravili, rozviňte kategóriu **Manažment adresárov** v navigačnej oblasti a kliknite na **Manažovať položky**. Môžete rozvinúť rôzne podstromy a vybrať položku, s ktorou chcete pracovať, napríklad Jon Doe. Kliknite na tlačidlo **Kopírovať** na lište nástrojov napravo.

- Zmeňte položku RDN v poli DN. Napríklad zmeňte cn=John Doe na cn=Jim Smith.
- Na záložke Povinné atribúty zmeňte položku cn na nové RDN. V tomto príklade na Jim Smith.
- Podľa potreby zmeňte ostatné povinné atribúty. V tomto príklade zmeňte atribút sn z Doe na Smith.
- Po vykonaní potrebných zmien vytvorte kliknutím na **OK** novú položku.
- Na koniec zoznamu sa pridá nová položka Jim Smith.

Poznámka: Táto procedúra skopíruje len atribúty položky. Členstvá v skupinách pôvodnej položky sa do novej položky nekopírujú. Členstvá pridajte pomocou funkcie Upraviť atribúty.

Úprava zoznamov riadenia prístupu

Ak chcete zobraziť vlastnosti ACL pomocou webového administratívneho nástroja a pracovať s zoznamami ACL, pozrite si časť “Manažovanie zoznamov riadenia prístupu (ACL)” na strane 179.

Viac informácií nájdete v časti “Zoznamy riadenia prístupu” na strane 55.

Pridanie pomocnej triedy objektov

Pomocnú triedu objektov môžete k existujúcej položke v adresárovom strome pridať pomocou tlačidla **Pridať pomocnú triedu** na lište nástrojov. Pomocná trieda objektov poskytuje ďalšie atribúty pre položku, ku ktorej je pridaná.

Ak ste tak ešte nespravili, rozviňte kategóriu **Manažment adresárov** v navigačnej oblasti a kliknite na **Manažovať položky**. Môžete rozvinúť rôzne podstromy a vybrať položku, s ktorou chcete pracovať, napríklad Jon Doe. Kliknite na tlačidlo **Pridať pomocnú triedu** na lište nástrojov napravo.

1. Z poľa Dostupné vyberte ľubovoľné **Pomocné triedy objektov**, ktoré chcete použiť a kliknite na **Pridať**. Opakujte tento proces pre každú pomocnú triedu objektov, ktorú chcete pridať. Z poľa Vybraté môžete odstrániť pomocnú triedu objektov tak, že ju vyberiete a kliknete na **Odstrániť**.
2. Na záložke **Povinné atribúty** zadajte hodnoty pre povinné atribúty. Ak chcete pre určitý atribút pridať viac ako jednu hodnotu, kliknite na **Viac hodnôt** a potom po jednej pridávajte hodnoty.

3. Kliknite na **Voliteľné atribúty**.
4. Na záložke **Voliteľné atribúty** zadajte vhodné hodnoty pre voliteľné atribúty. Ak chcete pre určitý atribút pridať viac ako jednu hodnotu, kliknite na **Viac hodnôt** a potom po jednej pridávajte hodnoty.
5. Kliknite na **Členstvá**.
6. Ak ste vytvorili skupiny, na záložke **Členstvá**:
   - Z ponuky **Dostupné skupiny** vyberte skupinu a kliknite na **Pridať**, aby sa z položky stal člen vybratého **Členstva v statickej skupine**.
   - Z **Členstiev v statických skupinách** vyberte skupinu a kliknutím na **Odstrániť** odstráňte položku z vybratej skupiny.
7. Ak chcete položku zmeniť, kliknite na tlačidlo **OK**.

Vymazanie pomocnej triedy

Aj keď môžete pomocnú triedu vymazať počas procedúry pridania pomocnej triedy, ak chcete z položky vymazať jednu pomocnú triedu, je jednoduchšie použiť funkciu vymazania pomocnej triedy. Ak však chcete z položky vymazať viac pomocných tried, môže byť pohodlnejšie použiť procedúru pridania pomocnej triedy.

1. Ak ste tak ešte nespravili, rozviňte kategóriu **Manažment adresárov** v navigačnej oblasti a kliknite na **Manažovať položky**. Môžete rozvinúť rôzne podstromy a vybrať položku, s ktorou chcete pracovať, napríklad Jon Doe. Kliknite na tlačidlo **Vymazať pomocnú triedu** na lište nástrojov napravo.
2. Zo zoznamu pomocných tried vyberte triedu, ktorú chcete vymazať a stlačte **OK**.
3. Po výzve na potvrdenie vymazania kliknite na **OK**.
4. Pomocná trieda sa vymaže z položky a vrátite sa do zoznamu položiek.

Opakujte tieto kroky pre každú pomocnú triedu, ktorú chcete vymazať.

Zmena členstva v skupine

Ak ste tak ešte nespravili, rozviňte kategóriu **Manažment adresárov** v navigačnej oblasti.

1. Kliknite na **Manažovať položky**.
2. Z adresárového stromu vyberte užívateľa a kliknite na tlačidlo **Upraviť atribúty** na lište nástrojov.
3. Kliknite na záložku **Členstvá**.
4. Ak chcete zmeniť užívateľovi členstvo. Panel **Zmena členstiev** zobrazuje **Dostupné skupiny**, do ktorých môžete pridať užívateľa, ako aj **Členstvá v statických skupinách** položky.
   - Z ponuky **Dostupné skupiny** vyberte skupinu a kliknite na **Pridať**, aby sa z položky stal člen vybratej skupiny.
   - Z **Členstiev v statických skupinách** vyberte skupinu a kliknutím na **Odstrániť** odstráňte položku z vybratej skupiny.
5. Ak chcete uložiť vaše zmeny, kliknite na **OK**, alebo ak sa chcete bez uloženia zmien vrátiť na predošlý panel, kliknite na **Zrušiť**.

Hľadanie položiek adresára

Existujú tri možnosti hľadania v adresárovom strome:

- Jednoduché hľadanie pomocou preddefinovanej množiny vyhľadávacích kritérií
- Rozšírené hľadanie pomocou užívateľom definovanej množiny vyhľadávacích kritérií
- Manuálne hľadanie

Voľby hľadania sú dostupné po rozvinutí kategórie **Manažment adresárov** v navigačnej oblasti a kliknutí na **Nájsť položky**. Vyberte záložku **Vyhľadávacie filtre** alebo **Možnosti**.

Poznámka: Nie je možné vyhľadávať binárne položky, napríklad heslá.

Vyhľadávacie filtre

Vyberte niektorý z nasledujúcich typov vyhľadávaní:

Jednoduché hľadanie

Jednoduché hľadanie používa predvolené vyhľadávacie kritérium:

- Základné DN je **Všetky prípony**
- Rozsah hľadania je **Podstrom**
- Veľkosť hľadania je **Neobmedzená**
- Časový limit je **Neobmedzený**
- Dereferencovanie aliasov je **nikdy**
- Sledovanie odvolávok nie je vybraté (je vypnuté)

Ak chcete vykonať jednoduché hľadanie:

1. Na záložke **Vyhľadávací filter** kliknite na **Jednoduché hľadanie**.
2. Z roletového zoznamu vyberte triedu objektov.
3. Pre vybratý typ položky vyberte špecifický atribút. Ak zvolíte hľadanie pre špecifický atribút, vyberte atribút zo sťahovacieho zoznamu a do okna **Je rovné** zadajte hodnotu atribútu. Ak nezadáte atribút, hľadanie vráti všetky položky adresára vybratého typu položky.

Rozšírené hľadanie

Rozšírené hľadanie vám umožňuje určiť obmedzenia vyhľadávania a povoliť vyhľadávacie filtre. Ak chcete použiť predvolené vyhľadávacie kritérium, použite Jednoduché hľadanie.

- Ak chcete vykonať rozšírené hľadanie:
  1. Na záložke **Vyhľadávací filter** kliknite na **Rozšírené hľadanie**.
  2. Zo sťahovacieho zoznamu vyberte **Atribút**.
  3. Vyberte operátor pre **Porovnávanie**
     - = Atribút je rovný hodnote.
     - ! Atribút nie je rovný hodnote.
     - < Atribút je menší alebo rovný hodnote.
     - > Atribút je väčší alebo rovný hodnote.
     - ~ Atribút je približne rovný hodnote.
  4. Zadajte **Hodnotu** pre porovnanie.
  5. Pre komplexné dotazy použite tlačidlá operátorov hľadania.
     - Ak ste už pridali aspoň jeden vyhľadávací filter, zadajte ďalšie kritérium a kliknite na **AND**. Príkaz **AND** vracia položky zodpovedajúce obom množinám vyhľadávacích kritérií.
     - Ak ste už pridali aspoň jeden vyhľadávací filter, zadajte ďalšie kritérium a kliknite na **OR**. Príkaz **OR** vracia položky zodpovedajúce niektorej z množín vyhľadávacích kritérií.
  6.
     - Ak chcete pridať kritérium vyhľadávacieho filtra do rozšíreného hľadania, kliknite na **Pridať**.
     - Ak chcete odstrániť kritérium vyhľadávacieho filtra z rozšíreného hľadania, kliknite na **Vymazať**.
     - Ak chcete vymazať všetky vyhľadávacie filtre, kliknite na **Reset**.

Manuálne hľadanie

Pomocou tejto metódy môžete vytvoriť vyhľadávací filter. Ak chcete napríklad hľadať priezviská, zadajte do poľa hodnotu sn=*. Ak vyhľadávate vo viacerých atribútoch, musíte použiť syntax vyhľadávacieho filtra. Ak chcete napríklad hľadať priezviská v určitom oddelení, zadajte:

```
(&(sn=*)(dept=<departmentname>))
```

Voľby

Na záložke **Možnosti**:

- **Základné DN pre hľadanie** - Ak chcete hľadať len v rámci určitej prípony, vyberte príponu zo sťahovacieho zoznamu.

  Poznámka: Ak ste spustili túto úlohu v paneli **Riadiť položky**, toto pole vám bude vyplnené. **Rodičovské DN** ste vybrali pred kliknutím na **Pridať** a spustením procesu pridania položky.

  Ak chcete hľadať v celom strome, môžete vybrať tiež **Všetky prípony**.

  Poznámka: Vyhľadávanie v podstrome s vybratou voľbou **Všetky prípony** nevráti informácie o schéme, informácie o protokole zmien ani nič zo systémovo projektovaného záložného procesu.
- **Rozsah hľadania**
  - Ak chcete hľadať len v rámci vybratého objektu, vyberte voľbu **Objekt**.
  - Ak chcete hľadať len v rámci najbližších potomkov vybratého objektu, vyberte voľbu **Jedna úroveň**.
  - Ak chcete hľadať vo všetkých potomkoch vybratej položky, vyberte voľbu **Podstrom**.
- **Limit veľkosti hľadania** - Zadajte maximálny počet položiek, ktoré sa budú hľadať alebo vyberte **Neobmedzené**.
- **Časový limit hľadania** - Zadajte maximálny počet sekúnd pre hľadanie alebo vyberte **Neobmedzené**.
- Zo sťahovacieho zoznamu vyberte typ **Dereferencovania aliasov**.
  - **Nikdy** - Ak je vybratou položkou alias, pre hľadanie sa nedereferencuje, teda hľadanie ignoruje referenciu na alias.
  - **Hľadať od aliasu** - Ak je vybratá položka alias, hľadanie dereferencuje alias a hľadá od umiestnenia aliasu.
  - **Dereferencovať pri hľadaní** - Vybratá položka sa nedereferencuje, ale všetky položky nájdené počas vyhľadávania sa dereferencujú.
  - **Vždy** - Všetky aliasy v hľadaní sa dereferencujú.
- Označte začiarkavacie políčko **Sledovať odvolávky**, ak chcete sledovať odvolávky do iného servera, ak vyhľadávanie vráti odvolávku. Ak odvolávka nasmeruje hľadanie do iného servera, na pripojenie k serveru sa použijú aktuálne prihlasovacie údaje. Ak ste prihlásený ako Anonymous, možno sa budete musieť prihlásiť do servera pomocou autentifikovaného DN.

Viac informácií o hľadaní nájdete v časti “Úprava nastavení hľadania” na strane 123.

Zmena binárnych atribútov

Ak atribút vyžaduje binárne údaje, zobrazí sa vedľa poľa atribútu tlačidlo **Binárne údaje**. Ak atribút nemá žiadne údaje, pole je prázdne. Ak atribút obsahuje binárne údaje, pole zobrazuje **Binárne údaje - 1**, pretože binárne atribúty sa nedajú zobraziť. Ak atribút obsahuje viac hodnôt, pole sa zobrazí ako sťahovací zoznam.

Ak chcete pracovať s binárnymi atribútmi, kliknite na tlačidlo **Binárne údaje**.

Binárne údaje môžete importovať, exportovať alebo vymazať.

Ak chcete do atribútu pridať binárne údaje:

1. Kliknite na tlačidlo **Binárne údaje**.
2. Kliknite na **Importovať**.
3. Môžete zadať názov cesty pre požadovaný súbor alebo kliknúť na **Prehľadať** a nájsť a vybrať binárny súbor.
4. Kliknite na **Predložiť súbor**. Zobrazí sa správa Súbor odoslaný.
5. Kliknite na tlačidlo **Zatvoriť**. Pod **Binárnymi údajovými položkami** sa teraz zobrazuje hodnota **Binárne údaje - 1**.
6. Opakujte proces importovania pre všetky binárne súbory, ktoré chcete pridať. Nasledujúce položky sa budú v zozname zobrazovať ako **Binárne údaje - 2**, **Binárne údaje - 3** a atď.

7. Po pridaní binárnych údajov kliknite na **OK**.

Ak chcete exportovať binárne údaje:

1. Kliknite na tlačidlo **Binárne údaje**.
2. Kliknite na **Exportovať**.
3. Kliknite na odkaz **Binárne údaje na stiahnutie**.
4. Postupujte podľa pokynov sprievodcu a buď zobrazte binárny súbor alebo ho uložte do nového umiestnenia.
5. Kliknite na tlačidlo **Zatvoriť**.
6. Proces exportovania opakujte pre toľko binárnych súborov, koľko chcete exportovať.
7. Po dokončení exportovania údajov kliknite na **OK**.

Ak chcete vymazať binárne údaje:

1. Kliknite na tlačidlo **Binárne údaje**.
2. Skontrolujte binárny údajový súbor, ktorý chcete vymazať. Môžete vybrať viac súborov.
3. Kliknite na **Vymazať**.
4. Po výzve na potvrdenie vymazania kliknite na **OK**. Binárne údaje označené na vymazanie sa odstránia zo zoznamu.
5. Po dokončení vymazávania údajov kliknite na **OK**.

Poznámka: V binárnych atribútoch sa dá vyhľadávať len to, či existujú.

Manažovanie užívateľov a skupín

Ak chcete manažovať užívateľov a skupiny, rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

Viac informácií nájdete v týchto častiach:

- “Manažovanie užívateľov”
- “Manažovanie skupín” na strane 170

Manažovanie užívateľov

Po nastavení vašich realmov a šablón ich môžete naplniť užívateľmi. Pozrite si tieto časti:

- “Pridanie užívateľov”
- “Vyhľadanie užívateľov v realme”
- “Úprava informácií o užívateľovi” na strane 170
- “Kopírovanie užívateľa” na strane 170
- “Odstránenie užívateľa” na strane 170

Pridanie užívateľov

Rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Pridať užívateľa** alebo kliknite na **Manažovanie užívateľov** a potom na **Pridať**.
2. Zo sťahovacieho zoznamu vyberte realm, do ktorého chcete pridať užívateľa.
3. Kliknite na tlačidlo **Ďalej**. Zobrazí sa šablóna priradená k danému realmu. Vyplňte povinné polia označené hviezdičkou (*) a ľubovoľné iné polia na záložkách. Ak ste už v realme vytvorili skupiny, môžete užívateľa tiež pridať do jednej alebo viacerých skupín.
4. Po dokončení kliknite na **Dokončiť**.

Vyhľadanie užívateľov v realme

Rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Nájsť užívateľa** alebo kliknite na **Manažovanie užívateľov** a potom na **Nájsť**.

2. V poli **Výber realmu** vyberte realm, v ktorom chcete hľadať.
3. Do poľa **Názvový atribút** zadajte hľadací reťazec. Sú podporované zástupné znaky, ak napríklad zadáte ***smith**, výsledkom budú všetky položky s názvovým atribútom končiacim na smith.
4. S vybratým užívateľom môžete vykonávať tieto operácie:
   - **Úprava** - Pozrite si časť “Úprava informácií o užívateľovi”.
   - **Kopírovanie** - Pozrite si časť “Kopírovanie užívateľa”.
   - **Vymazanie** - Pozrite si časť “Odstránenie užívateľa”.
5. Po dokončení kliknite na **OK**.

Úprava informácií o užívateľovi

Rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Manažovať užívateľov**.
2. Zo sťahovacej ponuky vyberte realm. Ak užívatelia ešte nie sú zobrazení v zozname **Užívatelia**, kliknite na **Zobraziť užívateľov**.
3. Vyberte užívateľa, ktorého chcete upraviť a kliknite na **Upraviť**.
4. Zmeňte informácie na záložkách, zmeňte členstvo v skupinách.
5. Po dokončení kliknite na **OK**.

Kopírovanie užívateľa

Ak potrebujete vytvoriť viacero užívateľov, ktorí majú väčšinu informácií zhodných, môžete ďalších užívateľov vytvoriť skopírovaním prvého užívateľa a upravením potrebných informácií.

Rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Manažovať užívateľov**.
2. Zo sťahovacej ponuky vyberte realm. Ak užívatelia ešte nie sú zobrazení v zozname **Užívatelia**, kliknite na **Zobraziť užívateľov**.
3. Vyberte užívateľa, ktorého chcete skopírovať a kliknite na **Kopírovať**.
4. Zmeňte príslušné informácie pre nového užívateľa, napríklad povinnú informáciu, ktorá identifikuje špecifického užívateľa, ako napríklad sn alebo cn. Informácie spoločné pre oboch užívateľov nie je nutné meniť.
5. Po dokončení kliknite na **OK**.

Odstránenie užívateľa

Rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Manažovať užívateľov**.
2. Zo sťahovacej ponuky vyberte realm. Ak užívatelia ešte nie sú zobrazení v zozname **Užívatelia**, kliknite na **Zobraziť užívateľov**.
3. Vyberte užívateľa, ktorého chcete odstrániť a kliknite na **Vymazať**.
4. Po výzve na potvrdenie vymazania kliknite na **OK**.
5. Užívateľ sa odstráni zo zoznamu užívateľov.

Manažovanie skupín

Po nastavení vašich realmov a šablón môžete vytvoriť skupiny. Pozrite si tieto časti:

- “Pridanie skupín” na strane 171
- “Vyhľadanie skupín v realme” na strane 171
- “Úprava informácií o skupine” na strane 171
- “Kopírovanie skupiny” na strane 171
- “Odstránenie skupiny” na strane 172

Pridanie skupín

Rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Pridať skupinu** alebo kliknite na **Manažovanie skupín** a potom na **Pridať**.
2. Zadajte názov skupiny, ktorú chcete vytvoriť.
3. Vyberte realm, do ktorého chcete pridať skupinu zo sťahovacej ponuky.
4. Kliknutím na **Dokončiť** vytvorte skupinu. Ak už máte v realme užívateľov, môžete kliknúť na **Ďalej** a vybrať užívateľov, ktorí sa pridajú do skupiny. Potom kliknite na **Dokončiť**.

Viac informácií nájdete v časti “Skupiny a roly” na strane 48.

Vyhľadanie skupín v realme

Rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Nájsť skupinu** alebo kliknite na **Manažovanie skupín** a potom na **Nájsť**.
2. V poli **Výber realmu** vyberte realm, v ktorom chcete hľadať.
3. Do poľa **Názvový atribút** zadajte hľadací reťazec. Sú podporované zástupné znaky, ak napríklad zadáte ***club**, výsledkom budú všetky skupiny s názvovým atribútom club, napríklad book club, chess club, garden club atď.
4. S vybratou skupinou môžete vykonávať tieto operácie:
   - **Úprava** - Pozrite si časť “Úprava informácií o skupine”.
   - **Kopírovanie** - Pozrite si časť “Kopírovanie skupiny”.
   - **Vymazanie** - Pozrite si časť “Odstránenie skupiny” na strane 172.
5. Po dokončení kliknite na **Zatvoriť**.

Úprava informácií o skupine

Rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Manažovať skupiny**.
2. Zo sťahovacej ponuky vyberte realm. Ak skupiny ešte nie sú zobrazené v zozname **Skupiny**, kliknite na **Zobraziť skupiny**.
3. Vyberte skupinu, ktorú chcete upraviť a kliknite na **Upraviť**.
4. Kliknutím na **Filtrovať** môžete obmedziť počet **Dostupných užívateľov**. Napríklad zadaním *smith do poľa pre priezvisko obmedzíte dostupných užívateľov na tých, ktorých meno sa končí na smith (Ann Smith, Bob Smith, Joe Goldsmith atď.)
5. Môžete pridávať a odstraňovať užívateľov zo skupiny.
6. Po dokončení kliknite na **OK**.

Kopírovanie skupiny

Ak potrebujete vytvoriť viacero skupín, ktoré majú väčšinu členov rovnakých, môžete ďalšie skupiny vytvoriť skopírovaním prvej skupiny a upravením potrebných informácií.

Rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Manažovať skupiny**.
2. Zo sťahovacej ponuky vyberte realm. Ak skupiny ešte nie sú zobrazené v zozname **Skupiny**, kliknite na **Zobraziť skupiny**.
3. Vyberte skupinu, ktorú chcete skopírovať a kliknite na **Kopírovať**.
4. V poli **Názov skupiny** zmeňte názov skupiny. Nová skupina má rovnakých členov ako pôvodná skupina.
5. Môžete zmeniť členov skupiny.
6. Po dokončení kliknite na **OK**. Vytvorí sa nová skupina obsahujúca rovnakých členov ako pôvodná skupina spolu s užívateľmi, ktorých ste pridali alebo odstránili počas procedúry kopírovania.

Odstránenie skupiny

Rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Manažovať skupiny**.
2. Zo sťahovacej ponuky vyberte realm. Ak skupiny ešte nie sú zobrazené v zozname **Skupiny**, kliknite na **Zobraziť skupiny**.
3. Vyberte skupinu, ktorú chcete odstrániť a kliknite na **Vymazať**.
4. Po výzve na potvrdenie vymazania kliknite na **OK**.
5. Skupina sa odstráni zo zoznamu skupín.

Manažovanie realmov a šablón užívateľov

Ak chcete manažovať realmy a šablóny užívateľov, kliknite na **Realmy a šablóny** v navigačnej oblasti webového administratívneho nástroja. Pomocou realmov a šablón užívateľov môžete iným zjednodušiť zadávanie údajov do adresára. Viac informácií o konceptoch realmov a šablón užívateľov nájdete v časti “Realmy a užívateľské šablóny” na strane 41.

Viac informácií nájdete v týchto častiach:

- “Vytvorenie realmu”
- “Vytvorenie administrátora realmu”
- “Vytvorenie šablóny” na strane 173
- “Pridanie šablóny do realmu” na strane 175
- “Vytvorenie skupín” na strane 175
- “Pridanie užívateľa do realmu” na strane 175
- “Manažovanie realmov” na strane 175
- “Manažovanie šablón” na strane 176

Vytvorenie realmu

Viac informácií o konceptoch realmov a šablón užívateľov nájdete v časti “Realmy a užívateľské šablóny” na strane 41.

Ak chcete vytvoriť realm, vykonajte toto:

1. Rozviňte kategóriu **Realmy a šablóny** v navigačnej oblasti webového administratívneho nástroja.
2. Kliknite na **Pridať realm**.
   - Zadajte názov realmu. Napríklad **realm1**.
   - Zadajte Rodičovské DN určujúce umiestnenie realmu. Táto položka má formu prípony, napríklad o=ibm,c=us. Táto položka môže byť prípona alebo položka inde v adresári. Môžete tiež kliknúť na **Prehľadať** a vybrať umiestnenie požadovaného podstromu.
3. Ak chcete pokračovať, kliknite na **Ďalej**, alebo kliknite na **Dokončiť**.
4. Ak ste klikli na **Ďalej**, skontrolujte informácie. Teraz ste ešte nevytvorili realm, takže môžete ignorovať položky **Šablóna užívateľov** a **Vyhľadávací filter užívateľov**.
5. Kliknutím na **Dokončiť** vytvorte realm.

Vytvorenie administrátora realmu

Ak chcete vytvoriť administrátora realmu, musíte najprv takto vytvoriť skupinu správy pre realm:

1. Vytvorte skupinu správy realmu.
   a. Rozviňte kategóriu **Manažment adresárov** v navigačnej oblasti webového administratívneho nástroja.
   b. Kliknite na **Manažovať položky**.
   c. Rozviňte strom a vyberte realm, ktorý ste práve vytvorili, **cn=realm1,o=ibm,c=us**.
   d. Kliknite na **Upraviť ACL**.

e. Kliknite na záložku **Vlastníci**.
f. Skontrolujte, že je začiarknuté políčko **Šíriť vlastníka**.
g. Zadajte DN pre realm, **cn=realm1,o=ibm,c=us**.
h. Zmeňte **Typ** na skupinu.
i. Kliknite na **Pridať**.

2. Vytvorte položku administrátora. Ak ešte nemáte položku užívateľa pre administrátora, musíte ju vytvoriť.
   a. Rozviňte kategóriu **Manažment adresárov** v navigačnej oblasti webového administratívneho nástroja.
   b. Kliknite na **Manažovať položky**.
   c. Rozviňte strom do miesta, kde chcete umiestniť položku administrátora.

      Poznámka: Umiestnenie položky administrátora mimo realmu spôsobí, administrátor nebude môcť omylom vymazať samého seba. V tomto príklade môže byť umiestnenie **o=ibm,c=us** .

   d. Kliknite na **Pridať**.
   e. Vyberte **Štrukturálnu triedu objektov**, napríklad **inetOrgPerson**.
   f. Kliknite na tlačidlo **Ďalej**.
   g. Vyberte všetky pomocné triedy objektov, ktoré chcete pridať.
   h. Kliknite na tlačidlo **Ďalej**.
   i. Zadajte povinné atribúty pre položku. Napríklad:
      - **RDN** cn=JohnDoe
      - **DN** o=ibm,c=us
      - **cn** John Doe
      - **sn** Doe
   j. Na záložke **Ostatné atribúty** skontrolujte, že ste priradili heslo.
   k. Po dokončení kliknite na **Dokončiť**.
3. Pridajte administrátora do skupiny správy.
   a. Rozviňte kategóriu **Manažment adresárov** v navigačnej oblasti webového administratívneho nástroja.
   b. Kliknite na **Manažovať položky**.
   c. Rozviňte strom a vyberte realm, ktorý ste práve vytvorili, **cn=realm1,o=ibm,c=us**.
   d. Kliknite na **Upraviť atribúty**.
   e. Kliknite na záložku **Členy**.
   f. Kliknite na **Členy**.
   g. V poli **Členy** zadajte DN administrátora, v tomto príklade **cn=John Doe,o=ibm,c=us**.
   h. Kliknite na **Pridať**. DN sa zobrazí v zozname **Členy**.
   i. Kliknite na **OK**.
   j. Kliknite na **Zaktualizovať**. DN sa zobrazí v zozname **Aktuálne členy**.
   k. Kliknite na **OK**.
4. Vytvorili ste administrátora, ktorý môže manažovať položky v realme.

Vytvorenie šablóny

Po vytvorení realmu je ďalším krokom vytvorenie šablóny užívateľov. Šablóna vám pomáha organizovať informácie, ktoré chcete zadať. Rozviňte kategóriu **Realmy a šablóny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Pridať šablónu užívateľov**.
   - Zadajte názov šablóny, napríklad **template1**.
   - Zadajte umiestnenie, kde sa bude nachádzať šablóna. Pre účely replikácie umiestnite šablónu do podstromu v realme, ktorý bude používať túto šablónu. Napríklad realm vytvorený v predošlých operáciách **cn=realm1,o=ibm,c=us**. Môžete tiež kliknúť na **Prehľadať** a vybrať pre umiestnenie šablóny iný podstrom.

2. Kliknite na tlačidlo **Ďalej**. Kliknutím na **Dokončiť** môžete vytvoriť prázdnu šablónu. Neskôr môžete do šablóny pridať informácie, pozrite si časť “Úprava šablóny” na strane 178.
3. Ak ste klikli na **Ďalej**, vyberte štrukturálnu triedu objektov pre šablónu, napríklad **inetOrgPerson**. Môžete pridať tiež ľubovoľné požadované pomocné triedy objektov.
4. Kliknite na tlačidlo **Ďalej**.
5. V šablóne sa vytvorila záložka **Povinné**. Môžete zmeniť informácie na tejto záložke.
   a. V ponuke záložiek vyberte **Povinné** a kliknite na **Upraviť**. Zobrazí sa panel **Upraviť záložku**. Vidíte názov záložky **Povinné** a vybraté atribúty, ktoré sú povinné pre triedu objektov **inetOrgPerson**:
      - *sn - priezvisko
      - *cn - bežné meno

      Poznámka: * označuje povinné informácie.
   b. Ak chcete do tejto záložky pridať ďalšie informácie, vyberte atribút z ponuky **Atribúty**. Vyberte napríklad **departmentNumber** a kliknite na **Pridať**. Vyberte **employeeNumber** a kliknite na **Pridať**. Vyberte **title** a kliknite na **Pridať**. Ponuka **Vybraté atribúty** teraz obsahuje:
      - title
      - employeeNumber
      - departmentNumber
      - *sn
      - *cn
   c. Spôsob, akým sa tieto polia zobrazujú v šablóne môžete zmeniť zvýraznením vybratého atribútu a kliknutím na **Presunúť nahor** alebo **Presunúť nadol**. Toto zmení umiestnenie atribútu o jednu pozíciu. Opakujte tento krok, kým nebudete mať atribúty v želanom poradí. Napríklad:
      - *sn
      - *cn
      - title
      - employeeNumber
      - departmentNumber
   d. Môžete zmeniť aj každý vybratý atribút.
      1) V zozname **Vybraté atribúty** zvýraznite atribút a kliknite na **Upraviť**.
      2) Môžete zmeniť zobrazovaný názov použitého poľa v šablóne. Ak napríklad chcete, aby sa atribút **departmentNumber** zobrazoval ako **Číslo oddelenia**, zadajte tento reťazec do poľa **Zobrazovaný názov**.
      3) Môžete tiež zadať predvolenú hodnotu, ktorá sa vopred vyplní do poľa atribútu v šablóne. Ak je napríklad väčšina pridávaných užívateľov členom oddelenia číslo 789, môžete zadať 789 ako predvolenú hodnotu. Do poľa v šablóne sa vopred vyplní hodnota 789. Pri pridávaní informácií o konkrétnom užívateľovi môžete túto hodnotu zmeniť.
      4) Kliknite na **OK**.
   e. Kliknite na **OK**.
6. Ak chcete vytvoriť ďalšiu kategóriu záložiek pre ostatné informácie, kliknite na **Pridať**.
   - Zadajte názov novej záložky. Napríklad Informácie o adrese.
   - Z ponuky **Atribúty** vyberte atribúty pre túto záložku. Vyberte napríklad **homePostalAddress** a kliknite na **Pridať**. Vyberte **postOfficeBox** a kliknite na **Pridať**. Vyberte **telephoneNumber** a kliknite na **Pridať**. Vyberte **homePhone** a kliknite na **Pridať**. Vyberte **facsimileTelephoneNumber** a kliknite na **Pridať**. Ponuka **Vybraté atribúty** teraz obsahuje:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone

- facsimileTelephoneNumber

- Spôsob, akým sa tieto polia zobrazujú v šablóne môžete zmeniť zvýraznením vybratého atribútu a kliknutím na **Presunúť nahor** alebo **Presunúť nadol**. Toto zmení umiestnenie atribútu o jednu pozíciu. Opakujte tento krok, kým nebudete mať atribúty v želanom poradí. Napríklad:
  - homePostalAddress
  - postOfficeBox
  - telephoneNumber
  - facsimileTelephoneNumber
  - homePhone
- Kliknite na **OK**.

7. Opakujte tento proces pre všetky záložky, ktoré chcete vytvoriť. Po dokončení vytvorte šablónu kliknutím na tlačidlo **Dokončiť**.

Pridanie šablóny do realmu

Po vytvorení realmu a šablóny musíte pridať šablónu do realmu. Rozviňte kategóriu **Realmy a šablóny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Manažovať realmy**.
2. Vyberte realm, do ktorého chcete pridať šablónu, v tomto príklade **cn=realm1,o=ibm,c=us** a kliknite na **Upraviť**.
3. Rolujte dole na položku **Šablóna užívateľov** a rozviňte sťahovaciu ponuku.
4. Vyberte šablónu, v tomto príklade **cn=template1,cn=realm1,o=ibm,c=us**.
5. Kliknite na **OK**.
6. Kliknite na tlačidlo **Zatvoriť**.

Vytvorenie skupín

Rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Pridať skupinu**.
2. Zadajte názov skupiny, ktorú chcete vytvoriť. Napríklad **group1**.
3. Zo sťahovacieho zoznamu vyberte realm, do ktorého chcete pridať užívateľa. V tomto príklade **realm1**.
4. Kliknutím na **Dokončiť** vytvorte skupinu. Ak už máte v realme užívateľov, môžete kliknúť na **Ďalej** a vybrať užívateľov, ktorí sa pridajú do skupiny group1. Potom kliknite na **Dokončiť**.

Viac informácií nájdete v časti “Skupiny a roly” na strane 48.

Pridanie užívateľa do realmu

Rozviňte kategóriu **Užívatelia a skupiny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Pridať užívateľa**.
2. Zo sťahovacieho zoznamu vyberte realm, do ktorého chcete pridať užívateľa. V tomto príklade **realm1**.
3. Kliknite na tlačidlo **Ďalej**. Zobrazí sa šablóna, ktorú ste práve vytvorili, template1. Vyplňte povinné polia označené hviezdičkou (*) a ľubovoľné iné polia na záložkách. Ak ste už v realme vytvorili skupiny, môžete užívateľa tiež pridať do jednej alebo viacerých skupín.
4. Po dokončení kliknite na **Dokončiť**.

Manažovanie realmov

Keď ste nastavili a naplnili svoj úvodný realm, môžete pridať ďalšie realmy alebo zmeniť existujúce realmy.

Rozviňte kategóriu **Realmy a šablóny** v navigačnej oblasti a kliknite na **Manažovať realmy**. Zobrazí sa zoznam existujúcich realmov. V tomto paneli môžete pridať, upraviť alebo odstrániť realm alebo upraviť zoznam riadenia prístupu (ACL) realmu. Viac informácií nájdete v nasledujúcich témach:

- “Prianie realmu” na strane 176

- "Úprava realmu"
- "Odstránenie realmu"
- "Úprava zoznamov ACL pre realm"

Prianie realmu

Rozviňte kategóriu **Realmy a šablóny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Pridať realm**.
   - Zadajte názov realmu. Napríklad **realm2**.
   - Ak už v systéme existujú realmy, napríklad **realm1**, môžete vybrať realm, z ktorého sa skopírujú nastavenia do vytváraného realmu.
   - Zadajte Rodičovské DN určujúce umiestnenie realmu. Táto položka má formu prípony, napríklad **o=ibm,c=us**. Môžete tiež kliknúť na **Prehľadať** a vybrať umiestnenie požadovaného podstromu.
2. Ak chcete pokračovať, kliknite na **Ďalej**, alebo kliknite na **Dokončiť**.
3. Ak ste klikli na **Ďalej**, skontrolujte informácie.
4. Zo sťahovacej ponuky vyberte **Šablónu užívateľov**. Ak ste skopírovali nastavenia z existujúceho realmu, je v tomto poli vopred vyplnená jeho šablóna.
5. Zadajte **Vyhľadávací filter užívateľov**.
6. Kliknutím na **Dokončiť** vytvorte realm.

Úprava realmu

Rozviňte kategóriu **Realmy a šablóny** v navigačnej oblasti webového administratívneho nástroja.

- Kliknite na **Manažovať realmy**.
- Zo zoznamu realmov vyberte realm, ktorý chcete upraviť.
- Kliknite na **Úprava**.
  - Pomocou tlačidiel **Prehľadať** môžete zmeniť:
    - Skupina administrátora
    - Kontajner skupín
    - Kontajner Užívateľov
  - Zo sťahovacej ponuky môžete vybrať inú šablónu.
  - Kliknite na **Upraviť**, ak chcete zmeniť **Filter vyhľadávania užívateľa**.
- Po dokončení kliknite na **OK**.

Odstránenie realmu

Rozviňte kategóriu **Realmy a šablóny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Manažovať realmy**.
2. Vyberte realm, ktorý chcete odstrániť.
3. Kliknite na **Vymazať**.
4. Po výzve na potvrdenie vymazania kliknite na **OK**.
5. Realm sa odstráni zo zoznamu realmov.

Úprava zoznamov ACL pre realm

Ak chcete zobraziť vlastnosti ACL pomocou webového administratívneho nástroja a pracovať s zoznamami ACL, pozrite si časť "Manažovanie zoznamov riadenia prístupu (ACL)" na strane 179.

Viac informácií nájdete v časti "Zoznamy riadenia prístupu" na strane 55.

Manažovanie šablón

Keď ste vytvorili svoju úvodnú šablónu, môžete pridať ďalšie šablóny alebo zmeniť existujúce šablóny.

Rozviňte kategóriu **Realmy a šablóny** v navigačnej oblasti a kliknite na **Manažovať šablóny**. Zobrazí sa zoznam existujúcich šablón. V tomto paneli môžete pridať, upraviť alebo odstrániť šablónu alebo upraviť zoznam riadenia prístupu (ACL) šablóny. Viac informácií nájdete v nasledujúcich témach:

- "Pridanie šablóny užívateľov"
- "Úprava šablóny" na strane 178
- "Odstránenie šablóny" na strane 178
- "Úprava zoznamov ACL pre šablónu" na strane 179

Pridanie šablóny užívateľov

Rozviňte kategóriu **Realmy a šablóny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Pridať šablónu užívateľov** alebo kliknite na **Manažovať šablóny užívateľov** a potom na **Pridať**.
   - Zadajte názov novej šablóny. Napríklad **template2**.
   - Ak už v systéme existujú šablóny, napríklad **template1**, môžete vybrať šablónu, z ktorej sa skopírujú nastavenia do vytváranej šablóny.
   - Zadajte Rodičovské DN určujúce umiestnenie šablóny. Táto položka má formu DN, napríklad **cn=realm1,o=ibm,c=us** . Môžete tiež kliknúť na **Prehľadať** a vybrať umiestnenie požadovaného podstromu.
2. Kliknite na tlačidlo **Ďalej**. Kliknutím na **Dokončiť** môžete vytvoriť prázdnu šablónu. Neskôr môžete do šablóny pridať informácie, pozrite si časť "Úprava šablóny" na strane 178.
3. Ak ste klikli na **Ďalej**, vyberte štrukturálnu triedu objektov pre šablónu, napríklad **inetOrgPerson**. Môžete pridať tiež ľubovoľné požadované pomocné triedy objektov.
4. Kliknite na tlačidlo **Ďalej**.
5. V šablóne sa vytvorila záložka **Povinné**. Môžete zmeniť informácie na tejto záložke.
   a. V ponuke záložiek vyberte **Povinné** a kliknite na **Upraviť**. Zobrazí sa panel **Upraviť záložku**. Vidíte názov záložky **Povinné** a vybraté atribúty, ktoré sú povinné pre triedu objektov **inetOrgPerson**:
      - *sn - priezvisko
      - *cn - bežné meno

      Poznámka: * označuje povinné informácie.
   b. Ak chcete do tejto záložky pridať ďalšie informácie, vyberte atribút z ponuky **Atribúty**. Vyberte napríklad **departmentNumber** a kliknite na **Pridať**. Vyberte **employeeNumber** a kliknite na **Pridať**. Vyberte **title** a kliknite na **Pridať**. Ponuka **Vybraté atribúty** teraz obsahuje:
      - title
      - employeeNumber
      - departmentNumber
      - *sn
      - *cn
   c. Spôsob, akým sa tieto polia zobrazujú v šablóne môžete zmeniť zvýraznením vybratého atribútu a kliknutím na **Presunúť nahor** alebo **Presunúť nadol**. Toto zmení umiestnenie atribútu o jednu pozíciu. Opakujte tento krok, kým nebudete mať atribúty v želanom poradí. Napríklad:
      - *sn
      - *cn
      - title
      - employeeNumber
      - departmentNumber
   d. Môžete zmeniť aj každý vybratý atribút.
      1) V zozname **Vybraté atribúty** zvýraznite atribút a kliknite na **Upraviť**.
      2) Môžete zmeniť zobrazovaný názov použitého poľa v šablóne. Ak napríklad chcete, aby sa atribút **departmentNumber** zobrazoval ako **Číslo oddelenia**, zadajte tento reťazec do poľa **Zobrazovaný názov**.

3) Môžete tiež zadať predvolenú hodnotu, ktorá sa vopred vyplní do poľa atribútu v šablóne. Ak je napríklad väčšina pridávaných užívateľov členom oddelenia číslo 789, môžete zadať 789 ako predvolenú hodnotu. Do poľa v šablóne sa vopred vyplní hodnota 789. Pri pridávaní informácií o konkrétnom užívateľovi môžete túto hodnotu zmeniť.

4) Kliknite na **OK**.

e. Kliknite na **OK**.

6. Ak chcete vytvoriť ďalšiu kategóriu záložiek pre ostatné informácie, kliknite na **Pridať**.
   - Zadajte názov novej záložky. Napríklad Informácie o adrese.
   - Z ponuky **Atribúty** vyberte atribúty pre túto záložku. Vyberte napríklad **homePostalAddress** a kliknite na **Pridať**. Vyberte **postOfficeBox** a kliknite na **Pridať**. Vyberte **telephoneNumber** a kliknite na **Pridať**. Vyberte **homePhone** a kliknite na **Pridať**. Vyberte **facsimileTelephoneNumber** a kliknite na **Pridať**. Ponuka **Vybraté atribúty** teraz obsahuje:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone
     – facsimileTelephoneNumber
   - Spôsob, akým sa tieto polia zobrazujú v šablóne môžete zmeniť zvýraznením vybratého atribútu a kliknutím na **Presunúť nahor** alebo **Presunúť nadol**. Toto zmení umiestnenie atribútu o jednu pozíciu. Opakujte tento krok, kým nebudete mať atribúty v želanom poradí. Napríklad:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – facsimileTelephoneNumber
     – homePhone
   - Kliknite na **OK**.
7. Opakujte tento proces pre všetky záložky, ktoré chcete vytvoriť. Po dokončení vytvorte šablónu kliknutím na tlačidlo **Dokončiť**.

Úprava šablóny

Rozviňte kategóriu **Realmy a šablóny** v navigačnej oblasti webového administratívneho nástroja.

- Kliknite na **Manažovať šablóny užívateľov**.
- Zo zoznamu realmov vyberte realm, ktorý chcete upraviť.
- Kliknite na **Úprava**.
- Ak už v systéme existujú šablóny, napríklad template1, môžete vybrať šablónu, z ktorej sa skopírujú nastavenia do vytváranej šablóny.
- Kliknite na tlačidlo **Ďalej**.
  – Pomocou sťahovacej ponuky môžete zmeniť štrukturálnu triedu objektov pre šablónu.
  – Môžete pridať alebo odstrániť pomocné triedy objektov.
- Kliknite na tlačidlo **Ďalej**.
- Môžete zmeniť záložky a atribúty v šablóne. Informácie o tom ako máte zmeniť záložky nájdete v 5 na strane 177.
- Po dokončení kliknite na **Dokončiť**.

Odstránenie šablóny

Rozviňte kategóriu **Realmy a šablóny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Manažovať šablóny užívateľov**.
2. Vyberte šablónu, ktorú chcete odstrániť.
3. Kliknite na **Vymazať**.

4. Po výzve na potvrdenie vymazania kliknite na **OK**.
5. Šablóna sa odstráni zo zoznamu šablón.

Úprava zoznamov ACL pre šablónu

Rozviňte kategóriu **Realmy a šablóny** v navigačnej oblasti webového administratívneho nástroja.

1. Kliknite na **Manažovať šablóny užívateľov**.
2. Vyberte šablónu, pre ktorú chcete upraviť zoznamy ACL.
3. Kliknite na **Upraviť ACL**.

Ak chcete zobraziť vlastnosti ACL pomocou webového administratívneho nástroja a pracovať s zoznamami ACL, pozrite si časť “Manažovanie zoznamov riadenia prístupu (ACL)”.

Viac informácií nájdete v časti “Zoznamy riadenia prístupu” na strane 55.

Manažovanie zoznamov riadenia prístupu (ACL)

Viac informácií o zoznamoch riadenia prístupu nájdete v časti “Zoznamy riadenia prístupu” na strane 55.

Ak si chcete pozrieť vlastnosti ACL pomocou webového administratívneho nástroja a pracovať s ACL, vykonajte toto:

1. Vyberte položku adresára. Napríklad cn=John Doe,ou=Advertising,o=ibm,c=US.
2. Kliknite na **Upraviť ACL**. Zobrazí sa panel Upraviť ACL s vopred vybratou záložkou **Efektívne zoznamy ACL**.

Tento panel má 5 záložiek:

- “Efektívne zoznamy ACL”
- “Efektívni vlastníci” na strane 180
- “Nefiltrované ACL” na strane 180
- “Filtrované ACL” na strane 181
- “Vlastníci” na strane 183

Záložky **Efektívne zoznamy ACL** a **Efektívni vlastníci** obsahujú informácie o zoznamoch ACL len na čítanie.

Efektívne zoznamy ACL

Efektívne zoznamy ACL sú explicitné a zdedené zoznamy ACL vybratej položky. Prístupové práva pre špecifické efektívne ACL môžete zobraziť, ak ho vyberiete a kliknete na **Zobraziť**. Zobrazí sa panel **Zobrazenie prístupových práv**.

Zobrazenie prístupových práv

- Časť **Práva** zobrazuje práva subjektu pre pridávanie a vymazávanie.
  - **Pridanie potomka** udeľuje alebo odoberá subjektu právo pridávať položku adresára pod vybratú položku.
  - **Vymazanie položky** udeľuje alebo odoberá subjektu právo vymazať vybratú položku.
- Časť **Trieda zabezpečenia** definuje povolenia pre triedy zabezpečenia. Atribúty sú zoskupené do tried bezpečnosti:
  - **Normálna** - Normálne triedy atribútov vyžadujú najnižšiu bezpečnosť, napríklad atribút commonName.
  - **Citlivá** - Citlivé triedy atribútov vyžadujú strednú úroveň bezpečnosti, napríklad homePhone.
  - **Kritická** - Kritické triedy bezpečnosti vyžadujú najvyššiu bezpečnosť, napríklad atribút userpassword.
  - **Systémová** - Systémové atribúty sú atribúty len na čítanie, ktoré udržuje server.
  - **Obmedzená** - Obmedzené atribúty sa používajú na definovanie riadenia prístupu.

  Ku každej triede bezpečnosti sú priradené oprávnenia.
  - **Čítanie** - subjekt môže čítať atribúty.
  - **Zápis** - subjekt môže zmeniť atribúty.
  - **Hľadanie** - subjekt môže vyhľadávať atribúty.

– **Porovnávanie** - subjekt môže porovnávať atribúty.

Ak sa chcete vrátiť na záložku Efektívne zoznamy ACL, kliknite na **OK**.

Ak sa chcete vrátiť na panel Úprava ACL, kliknite na **Zrušiť**.

Efektívni vlastníci

Efektívni vlastníci sú explicitní a zdedení vlastníci vybratej položky.

Nefiltrované ACL

K položke môžete pridať nové nefiltrované ACL alebo môžete upraviť existujúce nefiltrované ACL.

Nefiltrované zoznamy ACL sa môžu šíriť. To znamená, že informácie o riadení prístupu, definované pre jednu položku sa môžu aplikovať na všetky jej podriadené položky. Zdrojom ACL je zdroj aktuálneho ACL pre vybratú položku. Ak položka nemá ACL, zdedí ACL od rodičovských objektov na základe ich nastavení ACL.

Na záložke **Nefiltrované** zoznamy ACL zadajte tieto informácie:

- Šíriť zoznamy ACL - Výberom začiarkavacieho políčka **Šíriť** povolíte potomkom bez explicitne definovaného ACL zdediť ACL od tejto položky. Ak je vybraté toto začiarkavacie políčko, potomok zdedí zoznamy ACL od tejto položky a ak sa pre položku potomka explicitne definuje ACL, zdedené ACL od rodiča sa nahradí novým pridaným ACL. Ak toto začiarkavacie políčko nie je vybraté, položky potomkov bez explicitne definovaného ACL zdedia zoznamy ACL od rodiča tejto položky, ktorý má túto voľbu povolenú.
- Rozlišovací názov (DN) - Zadajte **Rozlišovací názov (DN)** entity požadujúcej prístup k vykonaniu operácií s vybratou položkou, napríklad cn=Marketing Group.
- Typ - Zadajte **Typ** rozlišovacieho názvu. Ak je DN napríklad užívateľ, vyberte access-id.

Pridávanie a upravovanie prístupových práv

Buď kliknite na tlačidlo **Pridať**, ak chcete DN pridať do poľa DN (Charakteristický názov) na zoznam ACL, alebo kliknite na tlačidlo Upraviť, ak chcete zmeniť ACL existujúceho DN.

Panely **Pridanie prístupových práv** a **Úprava prístupových práv** vám umožňujú nastaviť prístupové práva pre nové alebo existujúce zoznamy riadenia prístupu (ACL). Pole **Typ** sa štandardne nastaví na typ, ktorý ste vybrali v paneli **Úprava ACL**. Ak pridávate ACL, všetky ostatné polia sú štandardne prázdne. Ak upravujete ACL, polia obsahujú hodnoty nastavené pri poslednej úprave ACL.

Môžete:

- Nastaviť typ zoznamu ACL
- Nastaviť práva pre pridávanie a vymazávanie
- Nastaviť oprávnenia pre triedy bezpečnosti

Ak chcete nastaviť prístupové práva:

1. Vyberte **Typ** položky pre ACL. Ak je DN napríklad užívateľ, vyberte access-id.
2. Časť **Práva** zobrazuje práva subjektu pre pridávanie a vymazávanie.
   - **Pridanie potomka** udeľuje alebo odoberá subjektu právo pridávať položku adresára pod vybratú položku.
   - **Vymazanie položky** udeľuje alebo odoberá subjektu právo vymazať vybratú položku.
3. Sekcia **Trieda bezpečnosti** definuje oprávnenia pre triedy atribútov. Atribúty sú zoskupené do tried bezpečnosti:
   - **Normálna** - Normálne triedy atribútov vyžadujú najnižšiu bezpečnosť, napríklad atribút commonName.
   - **Citlivá** - Citlivé triedy atribútov vyžadujú strednú úroveň bezpečnosti, napríklad homePhone.
   - **Kritická** - Kritické triedy bezpečnosti vyžadujú najvyššiu bezpečnosť, napríklad atribút userpassword.
   - **Systémová** - Systémové atribúty sú atribúty len na čítanie, ktoré udržuje server.

- **Obmedzená** - Obmedzené atribúty sa používajú na definovanie riadenia prístupu.

Ku každej triede bezpečnosti sú priradené oprávnenia.

- Čítanie - subjekt môže čítať atribúty.
- Zápis - subjekt môže zmeniť atribúty.
- Hľadanie - subjekt môže vyhľadávať atribúty.
- Porovnávanie - subjekt môže porovnávať atribúty.

Okrem toho môžete povolenia zadávať na základe atribútu a nie na základe triedy zabezpečenia, do ktorej atribút patrí. Sekcia atribútov je zobrazená pod **Kritickou triedou bezpečnosti**.

- Zo sťahovacieho zoznamu **Definovanie atribútu** vyberte atribút.
- Kliknite na **Definovať**. Zobrazí sa atribút s tabuľkou oprávnení.
- Určite, či sa má udeliť alebo odobrať každé zo štyroch oprávnení triedy bezpečnosti priradených k atribútu.
- Túto procedúru môžete opakovať pre viac atribútov.
- Ak chcete odstrániť atribút, jednoducho vyberte atribút a kliknite na **Vymazať**.
- Po dokončení kliknite na **OK**.

Odstránenie zoznamov ACL

Zoznamy ACL môžete odstrániť dvoma spôsobmi:

- Vyberte rádiové tlačidlo vedľa zoznamu ACL, ktorý chcete vymazať. Kliknite na **Odstrániť**.
- Ak chcete zo zoznamu odstrániť všetky názvy DN, kliknite na **Odstrániť všetky**.

Filtrované ACL

K položke môžete pridať nové filtrované zoznamy ACL alebo môžete upraviť existujúce filtrované zoznamy ACL.

ACL založené na filtroch využívajú porovnávanie na základe filtrov, s použitím špecifikovaného filtra objektov, pre spárovanie cieľových objektov s efektívnym prístupom, ktorý sa pre ne používa.

Štandardným správaním ACL na báze filtrov je zhromažďovanie od najnižšej zahrnutej položky smerom nahor, pozdĺž reťaze rodičovských položiek, k najvyššej položke zahrnutej v DIT. Efektívny prístup sa vypočíta ako zjednotenie prístupových práv, ktoré povolili alebo zakázali ustanovujúce rodičovské položky. Existuje výnimka z tohto správania. Kvôli kompatibilite s funkciou replikácie podstromu a aby sa umožnilo väčšie administračné riadenie sa ako prostriedok na zastavenie hromadenia v položke používa atribút hornej hranice, ktorý sa v položke aj nachádza.

Na záložke Filtrované zoznamy ACL zadajte tieto informácie:

- Zhromažďovať filtrované zoznamy ACL -
  - Ak chcete z vybratej položky odstrániť atribút ibm-filterACLInherit, vyberte rádiové tlačidlo **Neurčené**.
  - Ak chcete umožniť zhromažďovanie zoznamov ACL pre túto položku smerom nahor od tejto položky, pozdĺž reťaze rodičovských položiek k najvyššej položke filtrovaného ACL zahrnutej v DIT, vyberte rádiové tlačidlo **Povolené**.
  - Ak chcete zastaviť zhromažďovanie filtrovaných zoznamov ACL pri vybratej položke, vyberte rádiové tlačidlo **Zakázané**.
- Rozlišovací názov (DN) - Zadajte **Rozlišovací názov (DN)** entity požadujúcej prístup k vykonaniu operácií s vybratou položkou, napríklad cn=Marketing Group.
- Typ - Zadajte **Typ** rozlišovacieho názvu. Ak je DN napríklad užívateľ, vyberte access-id.

Pridávanie a upravovanie prístupových práv

Buď kliknite na tlačidlo **Pridať**, ak chcete DN pridať do poľa DN (Charakteristický názov) na zoznam ACL, alebo kliknite na tlačidlo Upraviť, ak chcete zmeniť ACL existujúceho DN.

Panely **Pridanie prístupových práv** a **Úprava prístupových práv** vám umožňujú nastaviť prístupové práva pre nové alebo existujúce zoznamy riadenia prístupu (ACL). Pole Typ sa štandardne nastaví na typ, ktorý ste vybrali v paneli Úprava ACL. Ak pridávate ACL, všetky ostatné polia sú štandardne prázdne. Ak upravujete ACL, polia obsahujú hodnoty nastavené pri poslednej úprave ACL.

Môžete:

- Nastaviť typ zoznamu ACL
- Nastaviť práva pre pridávanie a vymazávanie
- Nastaviť filter objektov pre filtrované zoznamy ACL
- Nastaviť oprávnenia pre triedy bezpečnosti

Ak chcete nastaviť prístupové práva:

1. Vyberte **Typ** položky pre ACL. Ak je DN napríklad užívateľ, vyberte access-id.
2. Časť **Práva** zobrazuje práva subjektu pre pridávanie a vymazávanie.
   - **Pridanie potomka** udeľuje alebo odoberá subjektu právo pridávať položku adresára pod vybratú položku.
   - **Vymazanie položky** udeľuje alebo odoberá subjektu právo vymazať vybratú položku.
3. Nastavte filter objektov pre porovnávania založené na filtroch. V poli **Filter objektov** zadajte požadovaný filter objektov pre vybraté ACL. Po kliknutí na tlačidlo **Upraviť filter** získate asistenciu pri vytváraní reťazca vyhľadávacieho filtra. Aktuálne filtrované ACL sa šíri do všetkých objektov potomkov v priradenom podstrome, ktorý zodpovedá filtru v tomto poli.
4. Sekcia **Trieda bezpečnosti** definuje oprávnenia pre triedy atribútov. Atribúty sú zoskupené do tried bezpečnosti:
   - **Normálna** - Normálne triedy atribútov vyžadujú najnižšiu bezpečnosť, napríklad atribút commonName.
   - **Citlivá** - Citlivé triedy atribútov vyžadujú strednú úroveň bezpečnosti, napríklad homePhone.
   - **Kritická** - Kritické triedy bezpečnosti vyžadujú najvyššiu bezpečnosť, napríklad atribút userpassword.
   - **Systémová** - Systémové atribúty sú atribúty len na čítanie, ktoré udržuje server.
   - **Obmedzená** - Obmedzené atribúty sa používajú na definovanie riadenia prístupu.

   Ku každej triede bezpečnosti sú priradené oprávnenia.
   - Čítanie - subjekt môže čítať atribúty.
   - Zápis - subjekt môže zmeniť atribúty.
   - Hľadanie - subjekt môže vyhľadávať atribúty.
   - Porovnávanie - subjekt môže porovnávať atribúty.

   Okrem toho môžete povolenia zadávať na základe atribútu a nie na základe triedy zabezpečenia, do ktorej atribút patrí. Sekcia atribútov je zobrazená pod **Kritickou triedou bezpečnosti**.
   - Zo sťahovacieho zoznamu **Definovanie atribútu** vyberte atribút.
   - Kliknite na **Definovať**. Zobrazí sa atribút s tabuľkou oprávnení.
   - Určite, či sa má udeliť alebo odobrať každé zo štyroch oprávnení triedy bezpečnosti priradených k atribútu.
   - Túto procedúru môžete opakovať pre viac atribútov.
   - Ak chcete odstrániť atribút, jednoducho vyberte atribút a kliknite na **Vymazať**.
   - Po dokončení kliknite na **OK**.

Odstránenie zoznamov ACL

Zoznamy ACL môžete odstrániť dvoma spôsobmi:

- Vyberte rádiové tlačidlo vedľa zoznamu ACL, ktorý chcete vymazať. Kliknite na **Odstrániť**.
- Ak chcete zo zoznamu odstrániť všetky názvy DN, kliknite na **Odstrániť všetky**.

Vlastníci

Vlastníci položiek majú úplné oprávnenia na vykonávanie všetkých operácií na objekte. Vlastníci položiek môžu byť explicitní alebo rozšírení (zdedení).

Na záložke **Vlastníci** zadajte tieto informácie:

- Výberom začiarkavacieho políčka **Šíriť vlastníkov** povolíte potomkom bez explicitne definovaného vlastníka zdediť ho od tejto položky. Ak toto začiarkavacie políčko nie je vybraté, položky potomkov bez explicitne definovaného vlastníka zdedia vlastníka od rodiča tejto položky, ktorý má túto voľbu povolenú.
- Rozlišovací názov (DN) - Zadajte **Rozlišovací názov (DN)** entity požadujúcej prístup k vykonaniu operácií s vybratou položkou, napríklad cn=Marketing Group.

  Použitie cn=this s objektmi šíriacimi ich vlastníctvo na iné objekty zjednodušuje vytváranie podstromu adresára, v ktorom každý objekt vlastní sám seba.
- Typ - Zadajte **Typ** rozlišovacieho názvu. Ak je DN napríklad užívateľ, vyberte access-id.

Pridanie vlastníka

Kliknutím na **Pridať** pridajte DN z poľa **Rozlišovací názov (DN)** do zoznamu.

Odstránenie vlastníka

Vlastníka môžete odstrániť dvoma spôsobmi:

- Vyberte rádiové tlačidlo vedľa DN vlastníka, ktorého chcete vymazať. Kliknite na **Odstrániť**.
- Ak chcete zo zoznamu odstrániť všetky názvy DN vlastníkov, kliknite na **Odstrániť všetky**.

Kapitola 8. Referencie

Ďalšie referenčné informácie nájdete v týchto častiach:

- “Nástroje pre príkazový riadok”
- “Formát LDIF (LDAP data interchange format)” na strane 214
- “Schéma konfigurácie adresárového servera” na strane 216
- “Identifikátory objektov (OID)” na strane 254

Nástroje pre príkazový riadok

Táto časť popisuje pomocné programy, ktoré sa dajú spustiť z príkazového prostredia Qshell v i5/OS. Viac informácií nájdete v častiach opisujúcich tieto príkazy:

- “ldapmodify a ldapadd”
- “ldapdelete” na strane 189
- “ldapexop” na strane 192
- “ldapmodrdn” na strane 197
- “ldapsearch” na strane 200
- “ldapchangepwd” na strane 208
- “ldapdiff” na strane 210
- “Používanie SSL s pomocnými programami príkazového riadka LDAP” na strane 213

Všimnite si, že aby prostredie príkazov Qsehll správne spracovalo niektoré reťazce, musia byť uzavreté v úvodzovkách. Toto sa vo všeobecnosti týka reťazcov, ktoré tvoria názvy DN a vyhľadávacie filtre a zoznamov atribútov, ktoré má vrátiť príkaz ldapsearch. Tento zoznam obsahuje niekoľko príkladov:

- Reťazce obsahujúce medzery: "cn=John Smith,cn=users"
- Reťazce obsahujúce zástupné znaky: "*"
- Reťazce obsahujúce zátvorky: "(objectclass=person)"

Viac informácií o prostredí príkazov Qshell nájdete v téme “Qshell”.

ldapmodify a ldapadd

Nástroje pre modifikáciu položiek LDAP a pridávanie položiek LDAP

Prehľad

```
ldapmodify [-a] [-b] [-c] [-C charset] [-d debuglevel][-D binddn][-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][-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 rozhranie príkazového riadka k aplikačným programovým rozhraniam (API) ldap_modify, ldap_add, ldap_delete a ldap_modrdn. Príkaz **ldapadd** je implementovaný ako premenovaná verzia príkazu ldapmodify. Pri zavolaní ako ldapadd sa automaticky povolí prepínač **-a** (pridanie novej položky).

ldapmodify otvorí pripojenie k serveru LDAP a naviaže sa k serveru. **ldapmodify** môžete používať na zmenu alebo pridanie položiek. Informácie o položke sa čítajú zo štandardného vstupu alebo zo súboru pomocou voľby **-i**.

Ak chcete zobraziť pomoc k syntaxi pre **ldapmodify** alebo **ldapadd**, zadajte:

```
ldapmodify -?
```

alebo

```
ldapadd -?
```

Voľby

-a Pridanie nových položiek. Predvolená akcia pre **ldapmodify** je zmeniť existujúce položky. Ak sa príkaz zavolá ako **ldapadd**, tento prepínač sa vždy nastaví.

-b Predpokladajte, že všetky hodnoty začínajúce `/' sú binárne hodnoty a že skutočná hodnota sa nachádza v súbore, ktorého cesta je zadaná namiesto hodnoty.

-c Nepretržitý prevádzkový režim. Chyby sa nahlasujú, ale **ldapmodify** pokračuje s modifikáciou. V opačnom prípade je predvoleným správaním ukončenie po nahlásení chyby.

-C *charset*
Určuje, že reťazce zadané ako vstup pre nástroje **ldapmodify** a **ldapadd** sú reprezentované v lokálnej znakovej sade určenej hodnotou charset a musia sa konvertovať do UTF-8. Voľbu **-C** *charset* použite, ak je kódová stránka vstupného reťazca iná ako hodnota kódovej stránky úlohy. Podporované hodnoty znakovej sady nájdete v téme o API ldap_set_iconv_local_charset().

-d *debuglevel*
Nastaví úroveň ladenia LDAP na hodnotu debuglevel.

-D*binddn*
Na naviazanie k serveru LDAP sa použije hodnota ***binddn***. ***binddn*** je DN reprezentované reťazcom. Keď sa používa -m DIGEST-MD5, používa sa na špecifikáciu ID autorizácie. Môže to byť DN alebo reťazec authzId, ktorý sa začína na ″u:″ alebo ″dn:″.

-f *file* Prečítať informácie o modifikácii položky v súbore LDIF namiesto štandardného vstupu. Ak súbor LDIF nie je špecifikovaný, musíte použiť štandardný vstup na špecifikovanie aktualizovaných položiek vo formáte LDIF.

-F Prinúti aplikáciu na všetky zmeny bez ohľadu na obsah vstupných riadkov, ktoré sa začínajú na replica: (predvolene sa riadky replica: porovnajú s používaným hostiteľom a portom servera LDAP, aby sa mohlo rozhodnúť, či sa má skutočne použiť záznam protokolu replikácie).

-g Neodstráni koncové medzery v hodnotách atribútov.

–G Špecifikuje realm. Tento parameter je voliteľný. Keď sa používa s -m DIGEST-MD5, hodnota prejde do servera počas vytvárania väzieb.

-h*ldaphost*
Určenie alternatívneho hostiteľa, v ktorom je spustený server LDAP.

-i *file* Prečítať informácie o modifikácii položky v súbore LDIF namiesto štandardného vstupu. Ak súbor LDIF nie je špecifikovaný, musíte použiť štandardný vstup na špecifikovanie aktualizovaných položiek vo formáte LDIF.

-k Určuje použitie riadenia správy servera.

-K*keyfile*
Určuje názov databázového súboru kľúčov SSL s predvoleným rozšírením **kdb**. Ak databázový súbor kľúčov nie je v aktuálnom adresári, zadajte úplný názov databázového súboru kľúčov. Ak nezadáte názov

databázového súboru kľúčov, program najprv skontroluje, či existuje premenná prostredia SSL_KEYRING s daným názvom súboru. Ak nie je definovaná premenná prostredia SSL_KEYRING, použije sa systémový súbor kľúčov, ak existuje.

Tento parameter efektívne umožní prepínač **-Z**. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

-m *mechanism*
Pomocou hodnoty ***mechanism*** môžete určiť mechanizmus SASL, ktorý sa použije na naviazanie k serveru. Používa sa API ldap_sasl_bind_s(). Ak je zadané **-V 2**, ignoruje sa parameter **-m**. Ak nezadáte **-m**, použije sa jednoduchá autentifikácia. Platné mechanizmy sú:

- CRAM-MD5 - chráni heslo odosielané serveru.
- EXTERNAL - používa certifikát SSL. Vyžaduje -Z.
- GSSAPI - používa prihlasovacie údaje užívateľa Kerberos.
- DIGEST-MD5 - vyžaduje, aby klient odoslal hodnotu mena užívateľa do servera. Vyžaduje -U. Parameter -D (zvyčajne DN vytvárania väzieb) sa používa na zadanie ID autorizácie. Môže to byť DN alebo reťazec authzId, začínajúci na u: alebo dn:.
- OS400_PRFTKN - sa autentifikuje na lokálny server LDAP ako aktuálny užívateľ i5/OS s použitím DN užívateľa v systémom projektovanom záložnom procese. Parametre -D (DN vytvárania väzieb) a -w (heslo) by nemali byť zadané.

-M Spravovať objekty odvolávok ako štandardné záznamy.

-n Ukáže čo by sa urobilo, ale v skutočnosti položky neupraví. Je užitočný pre ladenie v spojitosti s parametrom -v.

-N*certificatename*
Zadajte návestie patriace klientskemu certifikátu v databázovom súbore kľúčov. Ak je server LDAP nakonfigurovaný, aby vykonával len autentifikáciu servera, nevyžaduje sa certifikát klienta. Ak je server LDAP nakonfigurovaný, aby vykonával autentifikáciu servera a klienta, môže sa vyžadovať certifikát klienta. Ak je pre databázový súbor kľúčov nastavený predvolený pár certifikát/súkromný kľúč, hodnota ***certificatename*** sa nevyžaduje. Podobne, ***certificatename*** nie je potrebné, ak v označenom súbore kľúčov databázy existuje jeden pár certifikát/súkromný kľúč. Ak nie je zadané **-Z** ani **-K**, tento parameter sa ignoruje. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

-O *maxhops*
Pomocou hodnoty ***maxhops*** môžete nastaviť maximálny počet skokov, ktoré vykoná klientska knižnica pri sledovaní odvolávok. Štandardný počet preskočení je 10.

-p *ldapport*
Určuje alternatívny port TCP, na ktorom počúva server LDAP. Štandardný port LDAP je 389. Ak nie za zadané **-p** a je zadané **-Z**, použije sa predvolený port 636 pre SSL LDAP.

-P*keyfilepw*
Zadajte heslo databázy kľúčov. Toto heslo sa vyžaduje na prístup k zašifrovaným informáciám v databázovom súbore kľúčov, ktorý môže obsahovať jeden alebo viac súkromných kľúčov. Ak je k databázovému súboru kľúčov priradený súbor hesiel, heslo sa získa zo súboru hesiel a parameter **-P** sa nevyžaduje. Ak nie je zadané **-Z** ani **-K**, tento parameter sa ignoruje.

-r Nahrádza existujúce hodnoty štandardnými.

-R Určuje, že odvolávky automaticky nenasledujú.

–U Špecifikuje meno užívateľa. Vyžaduje sa s -m DIGEST-MD5 a je ignorovaný s akýmkoľvek iným mechanizmom.

-v Použije sa viacslovný režim s veľkým množstvom diagnostík zapísaných do štandardného výstupu.

-V *version*
Určuje verziu LDAP, ktorú použije nástroj **ldapmodify** pri naviazaní k serveru LDAP. Štandardne sa vytvára pripojenie LDAP V3. Ak chcete explicitne vybrať LDAP V3, zadajte parameter **-V 3**. Ak chcete program spustiť ako aplikáciu LDAP V2, zadajte **-V 2**.

-w *passwd* **| ?**
Použiť ***passwd*** ako heslo pre autentifikáciu. Ak použijete hodnotu ?, vygeneruje sa výzva pre zadanie hesla.

-y *proxydn*
Nastaví ID z proxy servera pre voľbu autorizácie z proxy servera.

-Y Použije zabezpečené pripojenie LDAP (TLS).

-Z Na komunikáciu so serverom LDAP použije bezpečné spojenie SSL. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

Vstupný formát

Obsah súboru (alebo štandardného vstupu, ak na príkazovom riadku nie je zadaný prepínač **-i**) by mal spĺňať formát LDIF. Viac informácií o formáte LDIF nájdete v časti “Formát LDIF (LDAP data interchange format)” na strane 214.

Príklady

Predpokladáme, že existuje súbor /tmp/entrymods a má tento obsah:

```
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
-
```

príkaz:

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

nahradí v položke Modify Me obsah atribútu mail hodnotou modme@student.of.life.edu, pridá atribút title s hodnotou Grand Poobah, pridá obsah súboru /tmp/modme.jpeg ako jpegPhoto a úplne odstráni atribút description. Rovnaké úpravy môžete vykonať aj pomocou staršieho vstupného formátu nástroja ldapmodify:

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

a príkazu:

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

Predpokladáme, že existuje súbor /tmp/newentry a má tento obsah:

```
dn: cn=John Doe, o=University of Higher Learning, c=US
objectClass: person
      cn: John Doe
cn: Johnny
```

```
      sn: Doe
title: the world's most famous mythical person
mail: johndoe@student.of.life.edu
uid: jdoe
```

príkaz:

```
ldapadd -i /tmp/entrymods
```

pridá pre meno John Doe novú položku s použitím hodnôt zo súboru /tmp/newentry.

Poznámky

Ak nie je vstup zadaný pomocou voľby **-i** zo súboru, príkaz **ldapmodify** bude čakať na načítanie položiek zo štandardného vstupu.

Diagnostika

Ak nedôjde k chybe, bude stav ukončenia rovný 0. Chyba spôsobí stav ukončenia iný ako nula a na štandardný chybový výstup sa zapíše diagnostická správa.

ldapdelete

Nástroj na vymazávanie položiek LDAP

Prehľad

```
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 rozhranie príkazového riadka k aplikačnému programovému rozhraniu (API) ldap_delete.

ldapdelete otvorí pripojenie k serveru LDAP, vytvorí väzbu a vymaže jednu alebo viac položiek. Ak je zadaný jeden alebo viac rozlišovacích názvov (DN), vymažú sa položky s s týmito názvami DN. Každé DN je DN reprezentované reťazcom. Ak nie sú zadané žiadne argumenty DN, zoznam názvov DN sa číta zo štandardného vstupu alebo zo súboru, ak je použitý prepínač **-i**.

Ak chcete zobraziť pomoc k syntaxi pre **ldapdelete**, zadajte:

```
ldapdelete -?
```

Voľby

-c Nepretržitý prevádzkový režim. Chyby sa nahlasujú, ale **ldapdelete** pokračuje vo vymazávaní. V opačnom prípade je predvoleným správaním ukončenie po nahlásení chyby.

-C *charset*
Určuje, že názvy DN, zadané ako vstup pre nástroj **ldapdelete** sú reprezentované v lokálnej znakovej sade určenej hodnotou charset. Voľbu **-C** *charset* použite, ak je kódová stránka vstupného reťazca iná ako hodnota kódovej stránky úlohy. Podporované hodnoty znakovej sady nájdete v téme o API ldap_set_iconv_local_charset().

-d *debuglevel*
Nastaví úroveň ladenia LDAP na hodnotu debuglevel.

-D*binddn*

Na naviazanie k serveru LDAP sa použije hodnota ***binddn***. ***binddn*** je DN reprezentované reťazcom. Keď sa používa -m DIGEST-MD5, používa sa na špecifikáciu ID autorizácie. Môže to byť DN alebo reťazec authzId, ktorý sa začína na ″u:″ alebo ″dn:″.

-f *file* Načítanie postupnosti riadkov zo súboru a vymazanie jednej položky LDAP pre každý riadok v súbore. Každý riadok súboru by mal obsahovať jeden charakteristický názov (DN).

-G *realm*

Špecifikuje realm. Tento parameter je voliteľný. Keď sa používa s -m DIGEST-MD5, hodnota prejde do servera počas vytvárania väzieb.

-h*ldaphost*

Určite alternatívneho hostiteľa, na ktorom je spustený server LDAP.

-i *file* Načítanie postupnosti riadkov zo súboru a vymazanie jednej položky LDAP pre každý riadok v súbore. Každý riadok v súbore by mal obsahovať jeden rozlišovací názov.

-k Určuje použitie riadenia správy servera.

-K*keyfile*

Zadajte názov databázového súboru kľúčov SSL. Ak databázový súbor kľúčov nie je v aktuálnom adresári, zadajte úplný názov databázového súboru kľúčov.

Ak pomocný program nemôže lokalizovať databázu kľúčov, použije náročne kódovanú sadu štandardných dôveryhodných koreňov certifikačnej autority. Databázový súbor kľúčov zvyčajne obsahuje jeden alebo viac certifikátov z certifikačných autorít (CA), ktorým dôveruje klient. Tieto typy certifikátov X.509 sú tiež známe ako dôveryhodné zdroje.

Tento parameter efektívne umožní prepínač **-Z**. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

-m *mechanism*

Pomocou hodnoty ***mechanism*** môžete určiť mechanizmus SASL, ktorý sa použije na naviazanie k serveru. Používa sa API ldap_sasl_bind_s(). Ak je zadané **-V 2**, ignoruje sa parameter **-m**. Ak nezadáte **-m**, použije sa jednoduchá autentifikácia. Platné mechanizmy sú:

- CRAM-MD5 - chráni heslo odosielané serveru.
- EXTERNAL - používa certifikát SSL. Vyžaduje -Z.
- GSSAPI - používa prihlasovacie údaje užívateľa Kerberos.
- DIGEST-MD5 - vyžaduje, aby klient odoslal hodnotu mena užívateľa do servera. Vyžaduje -U. Parameter -D (zvyčajne DN vytvárania väzieb) sa používa na zadanie ID autorizácie. Môže to byť DN alebo reťazec authzId, začínajúci na u: alebo dn:.
- OS400_PRFTKN - sa autentifikuje na lokálny server LDAP ako aktuálny užívateľ i5/OS s použitím DN užívateľa v systémom projektovanom záložnom procese. Parametre -D (DN vytvárania väzieb) a -w (heslo) by nemali byť zadané.

-M Spravovať objekty odvolávok ako štandardné záznamy.

-n Ukáže čo by sa urobilo, ale v skutočnosti položky nezmení. Používa sa pri ladení spolu s **-v**.

-N*certificatename*

Zadajte návestie patriace klientskemu certifikátu v databázovom súbore kľúčov. Ak je server LDAP nakonfigurovaný, aby vykonával len autentifikáciu servera, nevyžaduje sa certifikát klienta. Ak je server LDAP nakonfigurovaný, aby vykonával autentifikáciu servera a klienta, môže sa vyžadovať certifikát klienta. ***Názov certifikátu*** sa nepožaduje, ak bol štandardný pár certifikát/privátny kľúč nastavený ako štandardný. Podobne, ***certificatename*** nie je potrebné, ak v označenom súbore kľúčov databázy existuje jeden pár certifikát/súkromný kľúč. Ak nie je zadané **-Z** ani **-K**, tento parameter sa ignoruje. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

-O *maxhops*
Pomocou hodnoty ***maxhops*** môžete nastaviť maximálny počet skokov, ktoré vykoná klientska knižnica pri sledovaní odvolávok. Štandardný počet preskočení je 10.

-p *ldapport*
Určuje alternatívny port TCP, na ktorom počúva server LDAP. Štandardný port LDAP je 389. Ak nie za zadané **-p** a je zadané **-Z**, použije sa predvolený port 636 pre SSL LDAP.

-P*keyfilepw*
Zadajte heslo databázy kľúčov. Toto heslo sa vyžaduje pre prístup k šifrovaným informáciám v súbore databázy kľúčov, ktorý môže obsahovať jeden alebo viaceré súkromné kľúče. Ak je k databázovému súboru kľúčov priradený súbor hesiel, heslo sa získa zo súboru hesiel a parameter **-P** sa nevyžaduje. Ak nie je zadané **-Z** ani **-K**, tento parameter sa ignoruje.

-R Určuje, že odvolávky automaticky nenasledujú.

-s Pomocou tejto voľby môžete vymazať podstrom s koreňom v zadanej položke.

–U *username*
Špecifikuje meno užívateľa. Vyžaduje sa s -m DIGEST-MD5 a je ignorovaný s akýmkoľvek iným mechanizmom.

-v Použije sa viacslovný režim s veľkým množstvom diagnostík zapísaných do štandardného výstupu.

-V *version*
Určuje verziu LDAP, ktorú použije nástroj **ldapdelete** pri naviazaní k serveru LDAP. Štandardne sa vytvára pripojenie LDAP V3. Ak chcete explicitne vybrať LDAP V3, zadajte parameter **-V 3**. Ak chcete program spustiť ako aplikáciu LDAP V2, zadajte **-V 2**.

-w *passwd* **| ?**
Použiť ***passwd*** ako heslo pre autentifikáciu. Ak použijete hodnotu ?, vygeneruje sa výzva pre zadanie hesla.

-y proxydn
Nastaví ID z proxy servera pre operáciu autorizácie z proxy servera.

–Y Použije zabezpečené pripojenie LDAP (TLS).

-Z Na komunikáciu so serverom LDAP použije bezpečné spojenie SSL. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

dn Určuje jeden alebo viac argumentov DN. Každé DN by malo byť DN reprezentované reťazcom.

Príklady

Príkaz

```
ldapdelete -D cn=administrator -w secret "cn=Delete Me, o=University of Life, c=US"
```

sa pokúsi vymazať položku s názvom commonName ″Delete Me″ priamo pod organizačnou položkou University of Life.

Poznámky

Ak nie sú zadané žiadne argumenty DN, príkaz **ldapdelete** čaká na načítanie zoznamu názvov DN zo štandardného vstupu.

Diagnostika

Ak nedôjde k chybe, bude stav ukončenia rovný 0. Chyba spôsobí stav ukončenia iný ako nula a na štandardný chybový výstup sa zapíše diagnostická správa.

ldapexop

Nástroj pre rozšírené operácie LDAP.

Prehľad

```
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

Nástroj **ldapexop** je rozhraním príkazového riadka poskytujúce možnosť naviazania k adresárovému serveru a odoslanie jednej rozšírenej operácie spolu s údajmi predstavujúcimi hodnotu rozšírenej operácie.

Nástroj **ldapexop** podporuje voľby pre štandardného hostiteľa, port, SSL a autentifikáciu, ktoré používajú všetky klientske nástroje LDAP. Okrem toho je definovaná množina volieb, pomocou ktorých určíte operáciu, ktorá sa má vykonať a argumenty pre každú rozšírenú operáciu.

Ak chcete zobraziť pomoc k syntaxi pre **ldapexop**, zadajte:

```
ldapexop -?
```

alebo

```
ldapexop -help
```

Voľby

Voľby pre príkaz ldapexop sú rozdelené do dvoch kategórií:

1. Všeobecné voľby určujúce spôsob pripojenia k adresárovému serveru. Tieto voľby musíte zadať pred voľbami špecifickými pre operáciu.
2. Voľba rozšírenej operácie, identifikujúca rozšírenú operáciu, ktorá sa má vykonať.

Všeobecné voľby

Tieto voľby určujú metódy pripojenia k serveru a musíte ich zadať pred voľbou **-op**.

-C *charset*
: Určuje, že názvy DN, zadané ako vstup pre nástroj **ldapexop** sú reprezentované v lokálnej znakovej sade určenej hodnotou charset. Voľbu **-C** *charset* použite, ak je kódová stránka vstupného reťazca iná ako hodnota kódovej stránky úlohy. Podporované hodnoty znakovej sady nájdete v téme o API ldap_set_iconv_local_charset().

-d *debuglevel*
: Nastaví úroveň ladenia LDAP na hodnotu debuglevel.

-D*binddn*
: Na naviazanie k serveru LDAP sa použije hodnota ***binddn***. ***binddn*** je DN reprezentované reťazcom. Keď sa používa -m DIGEST-MD5, používa sa na špecifikáciu ID autorizácie. Môže to byť DN alebo reťazec authzId, ktorý sa začína na ″u:″ alebo ″dn:″.

-e
: Zobrazenie informácií o verzii knižnice LDAP a ukončenie.

-G
: Špecifikuje realm. Tento parameter je voliteľný. Keď sa používa s -m DIGEST-MD5, hodnota prejde do servera počas vytvárania väzieb.

-h*ldaphost*
: Určite alternatívneho hostiteľa, na ktorom je spustený server LDAP.

-help
: Zobrazenie pomoci k syntaxi príkazu a informácií o použití.

-K*keyfile*

Zadajte názov databázového súboru kľúčov SSL. Ak databázový súbor kľúčov nie je v aktuálnom adresári, zadajte úplný názov databázového súboru kľúčov.

Ak program nemôže nájsť databázu kľúčov, použije sa systémová databáza kľúčov. Databázový súbor kľúčov zvyčajne obsahuje jeden alebo viac certifikátov z certifikačných autorít (CA), ktorým dôveruje klient. Tieto typy certifikátov X.509 sú tiež známe ako dôveryhodné zdroje.

Tento parameter efektívne umožní prepínač **-Z**. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

-m *mechanizmus*

Pomocou hodnoty ***mechanizmus*** môžete určiť mechanizmus SASL, ktorý sa použije na naviazanie k serveru. Používa sa API ldap_sasl_bind_s(). Ak je zadané **-V 2**, ignoruje sa parameter **-m**. Ak nezadáte **-m**, použije sa jednoduchá autentifikácia. Platné mechanizmy sú:

- CRAM-MD5 - chráni heslo odosielané serveru.
- EXTERNAL - používa certifikát SSL. Vyžaduje -Z.
- GSSAPI - používa prihlasovacie údaje užívateľa Kerberos.
- DIGEST-MD5 - vyžaduje, aby klient odoslal hodnotu mena užívateľa do servera. Vyžaduje -U. Parameter -D (zvyčajne DN vytvárania väzieb) sa používa na zadanie ID autorizácie. Môže to byť DN alebo reťazec authzId, začínajúci na u: alebo dn:.
- OS400_PRFTKN - sa autentifikuje na lokálny server LDAP ako aktuálny užívateľ i5/OS s použitím DN užívateľa v systémom projektovanom záložnom procese. Parametre -D (DN vytvárania väzieb) a -w (heslo) by nemali byť zadané.

-N*certificatename*

Zadajte návestie patriace klientskemu certifikátu v databázovom súbore kľúčov. Ak je server LDAP nakonfigurovaný, aby vykonával len autentifikáciu servera, nevyžaduje sa certifikát klienta. Ak je server LDAP nakonfigurovaný, aby vykonával autentifikáciu servera a klienta, môže sa vyžadovať certifikát klienta. ***Názov certifikátu*** sa nepožaduje, ak bol štandardný pár certifikát/privátny kľúč nastavený ako štandardný. Podobne, ***certificatename*** nie je potrebné, ak v označenom súbore kľúčov databázy existuje jeden pár certifikát/súkromný kľúč. Ak nie je zadané **-Z** ani **-K**, tento parameter sa ignoruje. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

-p *ldapport*

Určuje alternatívny port TCP, na ktorom počúva server LDAP. Štandardný port LDAP je 389. Ak nie za zadané **-p** a je zadané **-Z**, použije sa predvolený port 636 pre SSL LDAP.

-P*keyfilepw*

Zadajte heslo databázy kľúčov. Toto heslo sa vyžaduje pre prístup k šifrovaným informáciám v súbore databázy kľúčov, ktorý môže obsahovať jeden alebo viaceré súkromné kľúče. Ak je k databázovému súboru kľúčov priradený súbor hesiel, heslo sa získa zo súboru hesiel a parameter **-P** sa nevyžaduje. Ak nie je zadané **-Z** ani **-K**, tento parameter sa ignoruje.

-? Zobrazenie pomoci k syntaxi príkazu a informácií o použití.

–U Špecifikuje meno užívateľa. Vyžaduje sa s -m DIGEST-MD5 a je ignorovaný s akýmkoľvek iným mechanizmom.

-v Použije sa viacslovný režim s veľkým množstvom diagnostík zapísaných do štandardného výstupu.

-w *passwd* **| ?**

Použiť ***passwd*** ako heslo pre autentifikáciu. Ak použijete hodnotu ?, vygeneruje sa výzva pre zadanie hesla.

–Y Použije zabezpečené pripojenie LDAP (TLS).

-Z Na komunikáciu so serverom LDAP použije bezpečné spojenie SSL. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

Voľba rozšírenej operácie

Voľba rozšírenej operácie **-op** identifikuje rozšírenú operáciu, ktorá sa má vykonať. Pre rozšírenú operáciu môžete použiť jednu z týchto hodnôt:

- **cascrepl**: Rozšírená operácia replikácie s riadením kaskádovania. Požadovaná akcia sa aplikuje na zadaný server a odovzdá sa tiež všetkým replikám daného podstromu. Ak niektoré z týchto sú postupovacie repliky, odovzdajú tiež rozšírenú operáciu do ich replík. Operácia bude kaskáda na celej topológii replikácie.

  -action quiesce | unquiesce | replnow | wait
  Toto je povinný atribút určujúci akciu, ktorá sa vykoná.

  quiesce
  Nie sú povolené žiadne ďalšie aktualizácie okrem replikácie.

  unquiesce
  Obnovenie normálnej funkcie, aktualizácie od klientov sa akceptujú.

  replnow
  Replikácia všetkých zmien vo fronte do všetkých replikačných serverov hneď ako to bude možné, bez ohľadu na rozvrh.

  wait Čakanie na dokončenie replikácie všetkých aktualizácií do všetkých replík.

  -rc *contextDn*
  Toto je povinný atribút určujúci koreň podstromu.

  -timeout *secs*
  Toto je voliteľný atribút ktorý, ak je zadaný, určuje časový limit v sekundách. Ak nie je zadaný alebo je rovný 0, operácia čaká nekonečne dlho.

  Príklad:

  ```
  ldapexop -op cascrepl -action -quiesce -rc "o=acme,c=us" -timeout 60
  ```

- **controlqueue**: rozšírená operácia replikácie s frontom. Táto operácia vám umožňuje zo zoznamu zmien replikácie vymazať alebo odstrániť nevybavené zmeny, ktoré boli zaradené do frontu a nevykonali sa z dôvodu zlyhania replikácie. Táto operácia je užitočná pri manuálnom opravovaní údajov replikácie. V tom prípade by ste ju použili na vynechanie niektorých zlyhaní vo fronte.

  -skip all | change-id
  Toto je povinný atribút.
  - **-skip all**, indikuje vynechanie všetkých zmien v procese spracovania pre túto zmluvu.
  - **change-id** určuje jednu zmenu, ktorá sa vynechá. Ak server momentálne nevykonáva replikáciu tejto zmeny, požiadavka zlyhá.

  -ra *agreementDn*
  Toto je povinný atribút určujúci DN dohodnutia replikácie.

  Príklady:

  ```
  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**: rozšírená operácia riadenia replikácie

  -action suspend | resume | replnow
  Toto je povinný atribút určujúci akciu, ktorá sa vykoná.

-rc *contextDn* **| -ra** *agreementDn*

Názov **-rc** *contextDn* je názov DN kontextu replikácie. Akcia sa vykoná pre všetky dohodnutia pre tento kontext. **-ra** *agreementDn* je DN replikačnej zmluvy. Akcia sa vykoná pre zadané dohodnutie replikácie.

Príklad:

```
ldapexop -op controlrepl -action suspend -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"
```

- **getattributes -attrType**<*type*> **-matches bool**<*value*>

  -attrType {operational | language_tag | attribute_cache | unique | configuration}

  Je to povinný atribút, ktorý špecifikuje typ práve vyžadovaného atribútu.

  -matches bool {true | false}

  Špecifikuje, či sa vrátený zoznam atribútov zhoduje s typom atribútov, ktorý špecifikuje voľba -attrType<.

  Príklad

  ```
  ldapexop -op getattributes -attrType unique -matches bool true
  ```

  Vráti zoznam všetkých atribútov, ktoré boli označené ako jedinečné atribúty.

  ```
  ldapexop -op getattributes -attrType unique -matches bool false
  ```

  Vráti zoznam všetkých atribútov, ktoré neboli označené ako jedinečné atribúty.

- **getusertype:** požaduje rozšírenú operáciu typu užívateľa

  Táto rozšírená operácia vráti typ užívateľa na základe naviazaného DN.

  Príklad:

  ```
  ldapexop - D <AdminDN> -w <Adminpw> -op getusertype
  ```

  vráti:

  ```
  User : root_administrator
  Role(s) : server_config_administrator directory_administrator
  ```

- **quiesce**: rozšírená operácia uvedenia podstromu do do kľudového stavu alebo zrušenia kľudového stavu

  -rc *contextDn*

  Toto je povinný atribút, ktorý určuje DN kontextu replikácie (podstrom) na uvedenie do kľudového stavu alebo zrušenie kľudového stavu.

  -end Toto je voliteľný atribút a ak je prítomný, určuje ukončenie kľudového stavu podstromu. Ak nie je zadaný, predvolené nastavenie je uvedenie podstromu do kľudového stavu.

  Príklady:

  ```
  ldapexop -op quiesce -rc "o=acme,c=us"

  ldapexop -op quiesce -end -rc "o=ibm,c=us"
  ```

- **readconfig**: rozšírená operácia opätovného načítania konfiguračného súboru

  -scope entire | single<*entry DN***><***attribute***>**

  Toto je povinný atribút.

  - **entire** znamená, že sa znova načíta celý konfiguračný súbor.
  - **single** znamená, že sa načíta jedna zadaná položka a atribút.

  Príklady:

  ```
  ldapexop -op readconfig -scope entire

  ldapexop -op readconfig -scope single "cn=configuration" ibm-slapdAdminPW
  ```

  Poznámka: Tieto položky označené s:

  - [1] sa prejavia okamžite po readconfig
  - [2] nadobudnú účinnosť pri nových operáciách

– [3] nadobudnú účinnosť po zmene hesla (nevyžaduje sa operácia readconfig)

– [4] podporuje pomocný program príkazového riadku na i5/OS, ale nepodporuje ich adresárový 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]
```

- **unbind** {**-dn**<*specificDN*>| **-ip**<*sourceIP*> | **-dn**<*specificDN*> **-ip**<*sourceIP*> | **all**}:

  odpojí pripojenia podľa DN, IP, DN/IP alebo odpojí všetky pripojenia. Všetky pripojenia bez akýchkoľvek operácií a všetky pripojenia s operáciami vo fronte práce sa okamžite ukončia. Ak pracovník aktuálne pracuje na pripojení, pripojenie sa ukončí len čo pracovník túto operáciu dokončí.

  -dn<*specificDN*>
  Zadá požiadavku na ukončenie pripojenia len podľa DN. Výsledkom tejto požiadavky bude uvoľnenie všetkých pripojení, ktoré sú naviazané na špecifikované DN.

  -ip<*sourceIP*>
  Zadá požiadavku na ukončenie pripojenia len podľa IP. Výsledkom tejto požiadavky bude uvoľnenie všetkých pripojení zo špecifikovaného zdroja IP.

  -dn<*specificDN*> **-ip**<*sourceIP*>
  Zadá požiadavku na ukončenie pripojenia, stanoveného podľa páru DN/IP. Výsledkom tejto požiadavky bude uvoľnenie všetkých pripojení, naviazaných na špecifikované DN a zo špecifikovaného zdroja IP.

  -all Zadá požiadavku na ukončenie všetkých pripojení. Výsledkom tejto požiadavky bude uvoľnenie všetkých pripojení, okrem pripojenia, z ktorého táto požiadavka pochádza. Tento atribút sa nedá použiť s -D alebo -IP atribútmi

  Príklady:

```
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*>**:** identifikuje všetky nejedinečné hodnoty pre konkrétny atribút.

  -a <*attribute*>
  Špecifikuje atribút, pre ktorý sa vypíše zoznam všetkých konfliktných hodnôt.

  Poznámka: Nezobrazia sa duplicitné hodnoty pre binárne, operačné, konfiguračné atribúty a pre atribút objectclass. Tieto atribúty nie sú podporovanými rozšírenými operáciami pre jedinečné atribúty.

  Príklad:

  ```
  ldapexop -op uniqueattr -a "uid"
  ```

  Nasledujúci riadok bude pridaný do konfiguračného súboru pod položku ″cn=Directory,cn=RDBM Backends,cn=IBM Directory,cn=schema,cn=Configuration″ pre túto rozšírenú operáciu:

  ```
  ibm-slapdPlugin:extendedop /bin/libback-rdbm.dll initUniqueAttr
  ```

Diagnostika

Ak nedôjde k chybe, bude stav ukončenia rovný 0. Chyba spôsobí stav ukončenia iný ako nula a na štandardný chybový výstup sa zapíše diagnostická správa.

ldapmodrdn

Nástroj na modifikáciu RDN položiek LDAP

Prehľad

```
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 rozhranie príkazového riadka k aplikačnému programovému rozhraniu (API) ldap_modrdn.

ldapmodrdn otvorí pripojenie k serveru LDAP, vytvorí väzbu a upraví RDN položiek. Informácie o položkách sa čítajú zo štandardného vstupu, zo súboru pomocou voľby **-f** alebo z páru dn a rdn na príkazovom riadku.

Viac informácií o relatívnych rozlišovacích názvoch (RDN) a rozlišovacích názvoch (DN) nájdete v časti “Rozlišovacie názvy (DN)” na strane 11.

Ak chcete zobraziť pomoc k syntaxi pre **ldapmodrdn**, zadajte:

```
ldapmodrdn -?
```

Voľby

-c Nepretržitý prevádzkový režim. Chyby sa nahlasujú, ale **ldapmodrdn** pokračuje s modifikáciou. V opačnom prípade je predvoleným správaním ukončenie po nahlásení chyby.

-C *charset*
Určuje, že reťazce zadané ako vstup pre nástroj **ldapmodrdn** sú reprezentované v lokálnej znakovej sade určenej hodnotou charset. Voľbu **-C** *charset* použite, ak je kódová stránka vstupného reťazca iná ako hodnota kódovej stránky úlohy. Podporované hodnoty znakovej sady nájdete v téme o API ldap_set_iconv_local_charset(). Všimnite si, že podporované hodnoty pre parameter charset sú rovnaké ako podporované hodnoty pre značku charset, voliteľne definovanú v súboroch LDIF verzie 1.

-d *debuglevel*
Nastaví úroveň ladenia LDAP na hodnotu debuglevel.

-D*binddn*
Na naviazanie k serveru LDAP sa použije hodnota ***binddn***. ***binddn*** by malo byť DN zobrazené reťazcom. Pri použití s -m DIGEST-MD5 sa používa na zadanie ID autorizácie. Môže to byť DN alebo reťazec authzId, ktorý sa začína na ″u:″ alebo ″dn:″.

-f *file* Informácie o upravení položiek načíta zo súboru LDIF a nie zo štandardného vstupu ani z príkazového riadku (zadaním dn a nového rdn). Štandardný vstup sa môže dodať aj zo súboru (< file).

-G *realm*
Špecifikuje realm. Tento parameter je voliteľný. Keď sa používa s -m DIGEST-MD5, hodnota prejde do servera počas vytvárania väzieb.

-h*ldaphost*
Určenie alternatívneho hostiteľa, v ktorom je spustený server LDAP.

-i *file* Informácie pre modifikáciu položky sa načítajú zo súboru namiesto štandardného vstupu alebo príkazového riadka (určením hodnôt rdn and newrdn). Údaje štandardného súboru môžu byť tiež zo súboru (″< file″).

-k Určuje použitie riadenia správy servera.

-K*keyfile*
Zadajte názov databázového súboru kľúčov SSL. Ak databázový súbor kľúčov nie je v aktuálnom adresári, zadajte úplný názov databázového súboru kľúčov.

Ak pomocný program nemôže lokalizovať databázu kľúčov, použije náročne kódovanú sadu štandardných dôveryhodných koreňov certifikačnej autority. Databázový súbor kľúčov zvyčajne obsahuje jeden alebo viac certifikátov z certifikačných autorít (CA), ktorým dôveruje klient. Tieto typy certifikátov X.509 sú tiež známe ako dôveryhodné zdroje.

Tento parameter efektívne umožní prepínač **-Z**. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

-m *mechanizmus*
Pomocou hodnoty ***mechanizmus*** môžete určiť mechanizmus SASL, ktorý sa použije na naviazanie k serveru. Používa sa API ldap_sasl_bind_s(). Ak je zadané **-V 2**, ignoruje sa parameter **-m**. Ak nezadáte **-m**, použije sa jednoduchá autentifikácia. Platné mechanizmy sú:

- CRAM-MD5 - chráni heslo odosielané serveru.
- EXTERNAL - používa certifikát SSL. Vyžaduje -Z.
- GSSAPI - používa prihlasovacie údaje užívateľa Kerberos.
- DIGEST-MD5 - vyžaduje, aby klient odoslal hodnotu mena užívateľa do servera. Vyžaduje -U. Parameter -D (zvyčajne DN vytvárania väzieb) sa používa na zadanie ID autorizácie. Môže to byť DN alebo reťazec authzId, začínajúci na u: alebo dn:.
- OS400_PRFTKN - sa autentifikuje na lokálny server LDAP ako aktuálny užívateľ i5/OS s použitím DN užívateľa v systémom projektovanom záložnom procese. Parametre -D (DN vytvárania väzieb) a -w (heslo) by nemali byť zadané.

-M Spravovať objekty odvolávok ako štandardné záznamy.

-n Ukáže čo by sa urobilo, ale v skutočnosti položky nezmení. Používa sa pri ladení spolu s **-v**.

-N*certificatename*
Zadajte návestie patriace klientskemu certifikátu v databázovom súbore kľúčov. Všimnite si, že ak je server LDAP nakonfigurovaný, aby vykonával len autentifikáciu servera, nevyžaduje sa certifikát klienta. Ak je server LDAP nakonfigurovaný, aby vykonával autentifikáciu servera a klienta, môže sa vyžadovať certifikát klienta. ***Názov certifikátu*** sa nepožaduje, ak bol štandardný pár certifikát/privátny kľúč nastavený ako štandardný. Podobne, ***certificatename*** nie je potrebné, ak v označenom súbore kľúčov databázy existuje jeden

pár certifikát/súkromný kľúč. Ak nie je zadané **-Z** ani **-K**, tento parameter sa ignoruje. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

-O *hopcount*
Pomocou hodnoty ***hopcount*** môžete nastaviť maximálny počet skokov, ktoré vykoná klientska knižnica pri sledovaní odvolávok. Štandardný počet preskočení je 10.

-p *ldapport*
Určuje alternatívny port TCP, na ktorom počúva server LDAP. Štandardný port LDAP je 389. Ak nie voľba zadaní a je zadané -Z, použije sa predvolený port 636 pre SSL LDAP.

-P*keyfilepw*
Zadajte heslo databázy kľúčov. Toto heslo sa vyžaduje pre prístup k šifrovaným informáciám v súbore databázy kľúčov (ktorý môže obsahovať jeden alebo viaceré súkromné kľúče. Ak je k databázovému súboru kľúčov priradený súbor hesiel, heslo sa získa zo súboru hesiel a parameter **-P** sa nevyžaduje. Ak nie je zadané **-Z** ani **-K**, tento parameter sa ignoruje.

-r Odstránenie starých hodnôt RDN z položky. Predvolené správanie je ponechanie starých hodnôt.

-R Určuje, že odvolávky automaticky nenasledujú.

–U *username*
Špecifikuje meno užívateľa. Vyžaduje sa s -m DIGEST-MD5 a je ignorovaný s akýmkoľvek iným mechanizmom.

-v Použije sa viacslovný režim s veľkým množstvom diagnostík zapísaných do štandardného výstupu.

-V *version*
Určuje verziu LDAP, ktorú použije nástroj **ldapmodrdn** pri naviazaní k serveru LDAP. Štandardne sa vytvára pripojenie LDAP V3. Ak chcete explicitne vybrať LDAP V3, zadajte parameter **-V 3**. Ak chcete program spustiť ako aplikáciu LDAP V2, zadajte **-V 2**. Aplikácia, napríklad **ldapmodrdn** vyberá LDAP V3 ako preferovaný protokol pomocou ldap_init namiesto ldap_open.

-w *passwd* **| ?**
Použiť ***passwd*** ako heslo pre autentifikáciu. Ak použijete hodnotu ?, vygeneruje sa výzva pre zadanie hesla.

-y proxydn
Nastaví ID z proxy servera pre operáciu autorizácie z proxy servera.

–Y Použije zabezpečené pripojenie LDAP (TLS).

-Z Na komunikáciu so serverom LDAP použije bezpečné spojenie SSL. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

dn newrdn
Viac informácií nájdete v ďalšej časti, “Formát vstupu pre dn newrdn”.

Formát vstupu pre dn newrdn

Ak sú zadané argumenty príkazového riadka *dn* a *newrdn*, *newrdn* nahradí RDN položky určenej názvom DN, *dn*. V opačnom prípade pozostáva obsah súboru (alebo štandardného vstupu, ak nie je zadaný prepínač **-i**) z jednej alebo viacerých položiek:

```
Rozlišovací názov (DN)

Relatívny rozlišovací názov (RDN)
```

Na oddelenie každého páru DN a RDN sa môže použiť jeden alebo viaceré prázdne riadky.

Príklady

Predpokladáme, že existuje súbor /tmp/entrymods a má tento obsah:

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

príkaz:

```
ldapmodrdn -r -i /tmp/entrymods
```

zmení RDN položky Modify Me z Modify Me na The New Me a staré cn Modify Me sa odstráni.

Poznámky

Ak vstupná informácia nie je zadaná zo súboru pomocou voľby **-i** (alebo z páru *dn* a *rdn* príkazového riadku), príkaz **ldapmodrdn** počká na načítanie položiek zo štandardného vstupu.

Diagnostika

Ak nedôjde k chybe, bude stav ukončenia rovný 0. Chyba spôsobí stav ukončenia iný ako nula a na štandardný chybový výstup sa zapíše diagnostická správa.

ldapsearch

Nástroj na hľadanie položiek LDAP a vzorový program

Prehľad

```
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 rozhranie príkazového riadka k aplikačnému programovému rozhraniu (API) ldap_search.

ldapsearch otvorí pripojenie k serveru LDAP, vytvorí väzbu a vykoná hľadanie pomocou filtra. Filter by mal vyhovovať reprezentácii reťazcov pre filtre LDAP (viac informácií o filtroch nájdete v téme Rozhrania API adresárového servera).

Ak program **ldapsearch** nájde jednu alebo viac položiek, získajú sa atribúty zadané parametrom attrs a odošlú sa na štandardný výstup. Ak nie sú uvedené žiadne atribúty, vrátia sa všetky atribúty.

Ak chcete zobraziť pomoc k syntaxi pre **ldapsearch**, zadajte: ldapsearch -?.

Voľby

-a deref
: Špecifikuje, ako sa rušia referencie na alias. deref by malo byť jedno z never, always, search alebo find, aby určovalo, že aliasy sa nemajú nikdy dereferencovať, vždy dereferencovať, dereferencovať pri hľadaní alebo dereferencovať len pri hľadaní základného objektu pre hľadanie. Štandard je nikdy nerušiť referencie na alias.

-A
: Získava len atribúty (nie hodnoty). Možno ho použiť vtedy, keď sa chcete uistiť, či sa atribút v zázname nachádza, ale nezaujíma vás konkrétna hodnota.

-b searchbase
: Namiesto predvolenej hodnoty sa ako začiatočný bod použije hodnota searchbase. Ak nie je zadané **-b**, program sa pokúsi definíciu searchbase získať analýzou premennej prostredia LDAP_BASEDN. Ak nie je zadané ani jedno, začiatočný bod sa nastaví sa predvolenú hodnotu ″″.

-B Určuje, že sa nebude potláčať zobrazovanie hodnôt iných ako ASCII. Toto je užitočné pri spracúvaní hodnôt v alternatívnych znakových sadách, napríklad ISO-8859.1. Voľba **-L** implikuje túto voľbu.

-C charset

Určuje, že reťazce zadané ako vstup pre nástroj ldapsearch sú reprezentované v lokálnej znakovej sade (určenej hodnotou charset). Reťazcový vstup zahŕňa filter, DN pre väzbu a základné DN. Podobne aj pri zobrazovaní údajov **ldapsearch** konvertuje údaje prijaté zo servera LDAP do zadanej znakovej sady. Voľbu **-C** *charset* použite, ak je kódová stránka vstupného reťazca iná ako hodnota kódovej stránky úlohy. Podporované hodnoty znakovej sady nájdete v téme o API ldap_set_iconv_local_charset(). Ak sú zadané voľby **-C** aj **-L**, očakáva sa vstup v zadanej znakovej sade, ale výstup z programu **ldapsearch** sa vždy zachová v reprezentácii UTF-8 alebo v reprezentácii údajov zakódovanej vo formáte base-64, keď sa zistia netlačiteľné znaky. Je to preto, že štandardné súbory LDIF obsahujú len reprezentáciu reťazcových údajov vo formáte UTF-8 (alebo UTF-8 zakódovanom vo formáte base-64). Všimnite si, že podporované hodnoty pre parameter charset sú rovnaké ako podporované hodnoty pre značku charset, voliteľne definovanú v súboroch LDIF verzie 1.

-d debuglevel

Nastaví úroveň ladenia LDAP na hodnotu debuglevel.

-D binddn

Na naviazanie k serveru LDAP sa použije hodnota binddn. ***binddn*** by malo byť DN zobrazené reťazcom (pozrite si charakteristické názvy LDAP). Pri použití s -m DIGEST-MD5 sa používa na zadanie ID autorizácie. Môže to byť DN alebo reťazec authzId, ktorý sa začína na ″u:″ alebo ″dn:″.

-e Zobrazenie informácií o verzii knižnice LDAP a ukončenie.

-F sep Hodnota sep sa použije ako oddeľovač polí medzi názvami atribútov a hodnotami. Predvolený oddeľovač je `=', pokiaľ nie je zadaný prepínač **-L**, kedy sa ignoruje táto voľba.

-G *realm*

Špecifikuje realm. Tento parameter je voliteľný. Keď sa používa s -m DIGEST-MD5, hodnota prejde do servera počas vytvárania väzieb.

-h ldaphost

Určenie alternatívneho hostiteľa, v ktorom je spustený server LDAP.

-i file Načítanie postupnosti riadkov zo súboru a vykonanie jedného hľadania LDAP pre každý riadok. V tomto prípade sa filter zadaný na príkazovom riadku spracúva ako vzor, pričom prvý výskyt hodnoty %s sa nahradí riadkom zo súboru. Ak je hodnota file rovná jednému znaku ″-″, riadky sa čítajú zo štandardného vstupu.

-K keyfile

Zadajte názov databázového súboru kľúčov SSL. Ak databázový súbor kľúčov nie je v aktuálnom adresári, zadajte úplný názov databázového súboru kľúčov.

Ak pomocný program nemôže lokalizovať databázu kľúčov, použije náročne kódovanú sadu štandardných dôveryhodných koreňov certifikačnej autority. Databázový súbor kľúčov zvyčajne obsahuje jeden alebo viac certifikátov z certifikačných autorít (CA), ktorým dôveruje klient. Tieto typy certifikátov X.509 sú tiež známe ako dôveryhodné zdroje.

Tento parameter efektívne umožní prepínač **-Z**. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

-l timelimit

Hodnota timelimit určuje maximálny čas čakania na dokončenie hľadania.

-L Výsledky vyhľadávania zobrazí vo formáte LDIF. Táto voľba tiež zapína voľbu **-B** a zapríčiní ignorovanie voľby **-F**.

-m *mechanizmus*

Pomocou hodnoty ***mechanizmus*** môžete určiť mechanizmus SASL, ktorý sa použije na naviazanie k serveru. Používa sa API ldap_sasl_bind_s(). Ak je zadané **-V 2**, ignoruje sa parameter **-m**. Ak nezadáte **-m**, použije sa jednoduchá autentifikácia. Platné mechanizmy sú:

- CRAM-MD5 - chráni heslo odosielané serveru.

- EXTERNAL - používa certifikát SSL. Vyžaduje -Z.
- GSSAPI - používa prihlasovacie údaje užívateľa Kerberos.
- DIGEST-MD5 - vyžaduje, aby klient odoslal hodnotu mena užívateľa do servera. Vyžaduje -U. Parameter -D (zvyčajne DN vytvárania väzieb) sa používa na zadanie ID autorizácie. Môže to byť DN alebo reťazec authzId, začínajúci na u: alebo dn:.
- OS400_PRFTKN - sa autentifikuje na lokálny server LDAP ako aktuálny užívateľ i5/OS s použitím DN užívateľa v systémom projektovanom záložnom procese. Parametre -D (DN vytvárania väzieb) a -w (heslo) by nemali byť zadané.

-M Spravovať objekty odvolávok ako štandardné záznamy.

-n Ukáže čo by sa urobilo, ale v skutočnosti položky nezmení. Používa sa pri ladení spolu s **-v**.

-N certificatename
Zadajte návestie patriace klientskemu certifikátu v databázovom súbore kľúčov.

Poznámka: Ak je server LDAP nakonfigurovaný, aby vykonával len autentifikáciu servera, nevyžaduje sa certifikát klienta. Ak je server LDAP nakonfigurovaný, aby vykonával autentifikáciu servera a klienta, môže sa vyžadovať certifikát klienta. *Názov certifikátu* sa nepožaduje, ak bol štandardný pár certifikát/privátny kľúč nastavený ako štandardný. Podobne, *certificatename* nie je potrebné, ak v označenom súbore kľúčov databázy existuje jeden pár certifikát/súkromný kľúč. Ak nie je zadané **-Z** ani **-K**, tento parameter sa ignoruje.

Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

-o *attr_type*
Pomocou parametra -o (poradie) môžete určiť atribút, ktorý sa použije pre kritérium zoradenia výsledkov hľadania. Na ďalšie určenie poradia zoradenia môžete použiť viac parametrov -o. V tomto príklade sa výsledky hľadania zoradia podľa priezviska (sn), potom podľa krstného mena (givenname) zostupne, čo určuje predpona znaku mínus (-):

```
-o sn -o -givenname
```

Takže syntax parametra zoradenia je táto:

```
[-]<attribute name>[:<matching rule OID>]
```

kde

- attribute name je názov atribútu, podľa ktorého chcete zoradiť výsledky.
- OID porovnávacieho pravidla je voliteľné OID porovnávacieho pravidla, ktoré chcete použiť pre zoradenie. Adresárový server nepodporuje atribút OID porovnávacích pravidiel, ostatné servery LDAP však môžu tento atribút podporovať.
- Znak mínus (-) určuje, že výsledky musia byť zoradené v zostupnom poradí.
- Kritickosť je vždy critical.

Štandardným správaním je nezoraďovať vrátené výsledky.

-O maxhops
Pomocou hodnoty maxhops môžete nastaviť maximálny počet skokov, ktoré vykoná klientska knižnica pri sledovaní odvolávok. Štandardný počet preskočení je 10.

-p ldapport
Určuje alternatívny port TCP, na ktorom počúva server LDAP. Štandardný port LDAP je 389. Ak nie voľba zadaní a je zadané -Z, použije sa predvolený port 636 pre SSL LDAP.

-P keyfilepw
Zadajte heslo databázy kľúčov. Toto heslo sa vyžaduje pre prístup k šifrovaným informáciám v súbore databázy kľúčov (ktorý môže obsahovať jeden alebo viaceré súkromné kľúče. Ak je k databázovému súboru kľúčov priradený súbor hesiel, heslo sa získa zo súboru hesiel a parameter **-P** sa nevyžaduje. Ak nie je zadané **-Z** ani **-K**, tento parameter sa ignoruje.

-q *pagesize*

Na určenie stránkovania výsledkov hľadania, môžete použiť dva parametre: -q (veľkosť stránok dotazu) a -T (čas medzi hľadaniami v sekundách). V tomto príklade výsledky hľadania každých 15 sekúnd vrátia jednu stránku (25 položiek), až kým sa nevrátia všetky výsledky pre dané hľadanie. Klient ldapsearch riadi pokračovanie pripojenia pre každý požiadavku o stránkované výsledky počas celého trvania operácie hľadania.

Tieto parametre môžu byť užitočné, keď má klient obmedzené prostriedky alebo keď je pripojený cez pomalé pripojenie. Vo všeobecnosti vám umožňujú riadiť rýchlosť, akou sa vracajú údaje pre každú požiadavku o hľadanie. Namiesto súčasného prijatia všetkých výsledkov môžete vždy naraz získať niekoľko položiek (stránku). Okrem toho môžete riadiť dĺžku oneskoria medzi každou požiadavkou o stránku, čím poskytnete klientovi čas na spracovanie výsledkov.

```
-q 25  -T 15
```

Ak je zadaný parameter -v (verbose), ldapsearch po strane vrátených položiek zo servera zobrazí, koľko výsledkov sa už vrátilo, napríklad **Vrátilo sa celkovo 30 položiek.**

Je povolených viac parametrov -q, takže počas trvania jednej operácia hľadania môžete určiť rôzne veľkosti stránok. V tomto príklade je na prvej stránke 15 položiek, na druhej je 20 položiek a tretí parameter ukončuje operáciu stránkovaného hľadania.

```
-q 15 -q 20 -q 0
```

V tomto príklade je na prvej stránke 15 položiek a všetky ostatné stránky majú 20 položiek, pokračujúc s poslednou zadanou hodnotou **-q** až do konca operácie hľadania.

```
-q 15 -q 20
```

Štandardné správanie programu ldapsearch je vrátenie všetkých položiek v jednej požiadavke. Pri štandardnom správaní programu ldapsearch sa nevykonáva stránkovanie.

-R Určuje, že odvolávky automaticky nenasledujú.

-s scope

Špecifikuje rozsah hľadania. scope by malo byť jedno z base, one alebo sub, aby určovalo hľadanie základného objektu, jednej úrovne alebo podstromu. Predvolená hodnota je sub.

-t Získané hodnoty zapíše do niekoľkých dočasných súborov. Toto je užitočné pri spracúvaní hodnôt iných ako ASCII, napríklad jpegPhoto alebo audio.

-T *seconds*

Čas medzi hľadaním (v sekundách). Voľba **-T** je podporovaná, len keď je zadaná voľba **-q**.

–U *username*

Špecifikuje meno užívateľa. Vyžaduje sa s -m DIGEST-MD5 a je ignorovaný s akýmkoľvek iným mechanizmom.

-v Použije sa viacslovný režim s veľkým množstvom diagnostík zapísaných do štandardného výstupu.

-V Určuje verziu LDAP, ktorú použije nástroj ldapmodify pri naviazaní k serveru LDAP. Štandardne sa vytvára pripojenie LDAP V3. Ak chcete explicitne vybrať LDAP V3, zadajte parameter -V 3. Ak chcete program spustiť ako aplikáciu LDAP V2, zadajte ″-V 2″. Aplikácia, napríklad ldapmodify vyberá LDAP V3 ako preferovaný protokol pomocou ldap_init namiesto ldap_open.

-w *passwd* **| ?**

Použiť ***passwd*** ako heslo pre autentifikáciu. Ak použijete hodnotu ?, vygeneruje sa výzva pre zadanie hesla. .

-y proxydn

Nastaví ID z proxy servera pre operáciu autorizácie z proxy servera.

–Y Použije zabezpečené pripojenie LDAP (TLS).

-z sizelimit
Obmedzenie výsledkov hľadania na maximálny počet položiek sizelimit. Toto umožňuje nastaviť hornú hranicu pre počet vrátených položiek v jednej operácii hľadania.

-Z Na komunikáciu so serverom LDAP použije bezpečné spojenie SSL. Ak pri adresárovom serveri na i5/OS použijete -Z a nepoužijete -K alebo -N, použije sa certifikát, priradený k ID aplikácie Directory Services Client.

filter Určuje reťazcovú reprezentáciu filtra, ktorý sa má aplikovať v hľadaní. Jednoduché filtre môžete zadať vo formáte attributetype=attributevalue. Komplexnejšie filtre sa zadávajú pomocou notácie s predponami podľa tohto formátu BNR (Backus Naur Form):

```
<filter> ::='('<filtercomp>')'
<filtercomp> ::= <a>|<alebo>|<nie>|<simple>
<and> ::= '&' <filterlist>
<or> ::= '|' <filterlist>
<not> ::= '!' <filter>
<filterlist> ::= <filter>|<filter><filterlist>
<simple> ::= <attributetype><filtertype>
<attributevalue>
<filtertype> ::= '='|'~='|'<='|'>='
```

Konštrukcia '~=' sa používa na určenie približnej zhody. Reprezentácia pre <*typ atribútu*> a <*hodnotu atribútu*> je popísaná v ″RFC 2252, LDAP V3 Attribute Syntax Definitions″ . Okrem toho, ak je hodnota filtertype rovná '=', potom hodnota <*attributevalue*> môže byť jedna *, čím sa dosiahne test existencie atribútu, alebo môže obsahovať text a hviezdičky (*), čím sa dosiahne porovnávanie podreťazcov.

Napríklad filter ″mail=*″ nájde všetky položky, ktoré majú atribút mail. Filter ″mail=*@student.of.life.edu″ nájde všetky položky, ktorých atribút mail sa končí zadaným reťazcom. Ak chcete do filtra vložiť zátvorky, zadajte pred ne znak opačnej lomky (\).

Poznámka: Filter ako "cn=Bob *", kde je medzera medzi slovom Bob a hviezdičkou (*), porovnáva v IBM Directory ″Bob Carter″, ale nie ″Bobby Carter″. Medzera medzi slovom ″Bob″ a zástupným znakom (*) ovplyvňuje výsledok hľadania pomocou filtrov.

Pozrite si ″RFC 2254, Reprezentácia reťazca vyhľadávacích filtrov LDAP″ , kde nájdete úplný opis povolených filtrov.

Výstupný formát

Ak sa nájde jedna alebo viac položiek, každý položka sa zapíše na štandardný výstup vo formáte:

```
Rozlišovací názov (DN)

názov atribútu=hodnota

názov atribútu=hodnota

názov atribútu=hodnota

...
```

Viacnásobné položky sú oddelené jedným prázdnym riadkom. Ak je na určenie oddeľovacieho znaku použitá voľba **-F**, použije sa namiesto znaku `=’. Ak je použitá voľba **-t**, namiesto samotnej hodnoty sa použije názov dočasného súboru. Ak je zadaná hodnota **-A**, zapisuje sa len časť ″attributename″.

Príklady

Nasledujúci príkaz:

```
ldapsearch "cn=john doe" cn telephoneNumber
```

vyhľadá v podstrome (za použitia predvoleného základu hľadania) položky s atribútom commonName rovným ″john doe″. Získajú sa hodnoty commonName a telephoneNumber a odošlú sa na štandardný výstup. Ak sa nájdu dve položky, môže výstup vyzerať napríklad takto:

```
  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
```

Príkaz:

```
ldapsearch -t "uid=jed" jpegPhoto audio
```

vyhľadá v podstrome (za použitia predvoleného základu hľadania) položky s id užívateľa rovným ″jed″. Získajú sa hodnoty jpegPhoto a audio a zapíšu sa do dočasných súborov. Ak sa nájde jedna položka s jednou hodnotou pre každý z požadovaných atribútov, môže výstup vyzerať napríklad takto:

```
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
```

Príkaz:

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

vykoná hľadanie jednej úrovne na úrovni c=US a nájde všetky organizácie, ktorých atribút organizationName začína s ″university″. Výsledky hľadania sa zobrazia vo formáte LDIF (pozrite si LDAP Data Interchange Format). Získajú sa atribúty organizationName a description a odošlú sa na štandardný výstup, ktorý bude vyzerať napríklad takto:

```
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

...
```

Príkaz:

```
ldapsearch -b "c=US" -o ibm-slapdDN "objectclass=person" ibm-slapdDN
```

vykoná hľadanie v podstrome na úrovni c=US a vyhľadá všetky osoby. Keď sa tento špeciálny atribút (ibm-slapdDN) použije pri vyhľadávaní so zoradením, výsledky hľadania sa zoradia podľa reťazcovej reprezentácie rozlišovacieho názvu (DN). Výstup môže vyzerať napríklad takto:

```
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
```

Príkaz:

```
ldapsearch –h hostname –o sn –b "o=ibm,c=us" "title=engineer"
```

vracia všetky položky v adresári zamestnancov spoločnosti IBM, ktorých titul je ″inžinier″, s výsledkami triedenými podľa priezviska.

Príkaz:

```
ldapsearch –h hostname –o -sn –o cn –b "o=ibm,c=us" "title=engineer"
```

vracia všetky položky v adresári zamestnancov spoločnosti IBM, ktorých titul je ″inžinier″ s výsledkami triedenými podľa priezviska (v zostupnom poradí) a potom podľa mena (vo vzostupnom poradí).

Príkaz:

```
ldapsearch –h hostname –q 5 –T 3 –b o=ibm,c=us "title=engineer"
```

vracia päť položiek na stranu s oneskorením o 3 sekundy medzi jednotlivými stranami pre všetky položky v adresári zamestnancov spoločnosti IBM, ktorých titul je ″inžinier″.

Tento príkaz ukazuje vyhľadávania, keď sa týkajú objektu odvolávky. Ako už bolo spomenuté v “Odvolávky na adresár LDAP” na strane 45, Adresárový server adresáre LDAP môžu obsahovať objekty odkazov za predpokladu, že obsahujú len nasledovné:

- Rozoznaný názov (dn).
- Triedu objektov (objectClass).
- Atribút (ref) odvolávky.

Predpokladáme, že systém ’System_A’ uchováva položku odvolávky:

```
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
```

Všetky atribúty priradené k položke by sa mali nachádzať v systéme ’System_B’.

Systém_B obsahuje záznam:

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

Keď klient vydá požiadavku pre ’System_A’, server LDAP v systéme System_A odpovie klientovi pomocou URL:

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

Klient pomocou týchto informácií vydá požiadavku pre systém System_B. Ak položka v System_A obsahuje atribúty iné ako dn, objectclass a ref, server tieto atribúty ignoruje (pokiaľ pomocou prepínača **-R** neurčíte, aby sa nesledovali odvolávky).

Keď klient od servera získava odvolávkovú odpoveď, túto požiadavku vydá opäť serveru, na ktorý sa odvoláva vrátené URL. Nová požiadavka má rovnaký rozsah ako pôvodná požiadavka. Výsledky tohto vyhľadávania sa menia podľa hodnoty, ktorú špecifikujete pre rozsah vyhľadávania (**-b**).

Ak zadáte -s base, ako je ukázané tu:

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

hľadanie vráti všetky atribúty pre všetky položky s ’sn=Jensen’, ktoré sa náchádzajú v ’ou=Rochester, o=Big Company, c=US’ v systéme System_A aj System_B.

Ak špecifikujete -s sub, ako v tomto prípade:

```
ldapsearch -s sub "cn=John"
```

server by hľadal všetky prípony a vrátil by všetky položky s ″cn=John″. Toto sa volá podstromové vyhľadávanie na nulovej báze. Celý adresár sa prehľadáva jednou vyhľadávacou operáciou namiesto viacerých hľadaní, každé s inou príponou ako základom vyhľadávania. Tento typ vyhľadávacej operácie trvá dlhšie a spotrebuje viac systémových prostriedkov, pretože sa prehľadáva celý adresár (všetky prípony).

Poznámka: Podstromové vyhľadávanie na nulovej báze nevracia informácie o schéme, informácie o protokole zmien, ani nič zo systémom naprojektovaného backendu.

Ak špecifikujete -s sub, ako v tomto prípade:

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

hľadanie vráti všetky atribúty pre všetky položky s 'sn=Jensen', ktoré sa nachádzajú pod 'ou=Rochester, o=Big Company, c=US' v systéme System_A aj System_B.

Ak špecifikujete -s one, ako v tomto prípade:

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

vyhľadávanie nevráti položky ani z jedného systému. Namiesto toho server klientovi vráti odvolávku na URL:

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

Potom klient vydá požiadavku:

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

Toto tiež nevráti žiadne výsledky, pretože položka

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
```

je umiestnená v

```
ou=Rochester, o=Big Company, c=US
```

Hľadanie s parametrom -s one sa pokúsi nájsť položky v úrovni priamo pod

```
ou=Rochester, o=Big Company, c=US
```

Diagnostika

Ak nedôjde k chybe, bude stav ukončenia rovný 0. Chyba spôsobí stav ukončenia iný ako nula a na štandardný chybový výstup sa zapíše diagnostická správa.

ldapchangepwd

Nástroj pre modifikáciu hesiel LDAP.

Prehľad

```
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

Program odosiela do servera LDAP požiadavky o modifikáciu hesla. Umožňuje zmenu hesla pre položku adresára.

Voľby

-C *charset*
Určuje, že názvy DN, zadané ako vstup pre nástroj **ldapdelete** sú reprezentované v lokálnej znakovej sade určenej hodnotou charset. Voľbu **-C** *charset* použite, ak je kódová stránka vstupného reťazca iná ako hodnota kódovej stránky úlohy. Podporované hodnoty znakovej sady nájdete v téme o API ldap_set_iconv_local_charset().

-d *debuglevel*
Nastaví úroveň ladenia LDAP na hodnotu debuglevel.

-D*binddn*
Na naviazanie k serveru LDAP sa použije hodnota ***binddn***. ***binddn*** je DN reprezentované reťazcom. Ak sa použije s -m DIGEST-MD5, použije sa na zadanie ID autorizácie. Môže to byť buď DN, alebo reťazec authzId začínajúci sa na ″u:″ alebo ″dn:″.

–G *realm*
Zadajte realm. Tento parameter je voliteľný. Ak sa použije s -m DIGEST-MD5, hodnota sa odovzdá serveru počas vytvárania väzby.

-h*ldaphost*
Určenie alternatívneho hostiteľa, v ktorom je spustený server LDAP.

-K*keyfile*
Zadajte názov databázového súboru kľúčov SSL. Ak databázový súbor kľúčov nie je v aktuálnom adresári, zadajte úplný názov databázového súboru kľúčov.

Ak pomocný program nemôže lokalizovať databázu kľúčov, použije náročne kódovanú sadu štandardných dôveryhodných koreňov certifikačnej autority. Databázový súbor kľúčov zvyčajne obsahuje jeden alebo viac certifikátov z certifikačných autorít (CA), ktorým dôveruje klient. Tieto typy certifikátov X.509 sú tiež známe ako dôveryhodné zdroje.

Tento parameter efektívne umožní prepínač **-Z**. Ak na adresárovom serveri na i5/OS použijete parameter -Z a nepoužijete -K alebo -N, použije sa certifikát priradený k ID aplikácie Directory Services Client.

-m *mechanism*
Pomocou hodnoty ***mechanism*** môžete určiť mechanizmus SASL, ktorý sa použije na naviazanie k serveru. Používa sa API ldap_sasl_bind_s(). Ak je zadané **-V 2**, ignoruje sa parameter **-m**. Ak nezadáte **-m**, použije sa jednoduchá autentifikácia. Platné mechanizmy sú:

- CRAM-MD5 - chráni heslo odosielané serveru.
- EXTERNAL - používa certifikát SSL. Vyžaduje -Z.
- GSSAPI - používa prihlasovacie údaje užívateľa Kerberos.
- DIGEST-MD5 - vyžaduje, aby klient zaslal na server hodnotu mena užívateľa. Vyžaduje -U. Parameter -D (častejšie väzba DN) sa používa na zadanie ID autorizácie. Môže to byť DN, alebo reťazec authzId začínajúci sa na u: alebo dn:.

-M Spravovať objekty odvolávok ako štandardné záznamy.

-n *newpassword* **| ?**
Určuje nové heslo. Ak použijete hodnotu ?, vygeneruje sa výzva pre zadanie hesla.

-N*certificatename*
Zadajte návestie patriace klientskemu certifikátu v databázovom súbore kľúčov. Ak je server LDAP nakonfigurovaný, aby vykonával len autentifikáciu servera, nevyžaduje sa certifikát klienta. Ak je server LDAP nakonfigurovaný, aby vykonával autentifikáciu servera a klienta, môže sa vyžadovať certifikát klienta. ***Názov certifikátu*** sa nepožaduje, ak bol štandardný pár certifikát/privátny kľúč nastavený ako štandardný. Podobne, ***certificatename*** nie je potrebné, ak v označenom súbore kľúčov databázy existuje jeden pár

certifikát/súkromný kľúč. Ak nie je zadané **-Z** ani **-K**, tento parameter sa ignoruje. Ak na adresárovom serveri na i5/OS použijete parameter -Z a nepoužijete -K alebo -N, použije sa certifikát priradený k ID aplikácie Directory Services Client.

-O *maxhops*
Pomocou hodnoty ***maxhops*** môžete nastaviť maximálny počet skokov, ktoré vykoná klientska knižnica pri sledovaní odvolávok. Štandardný počet preskočení je 10.

-p *ldapport*
Určuje alternatívny port TCP, na ktorom počúva server LDAP. Štandardný port LDAP je 389. Ak nie za zadané **-p** a je zadané **-Z**, použije sa predvolený port 636 pre SSL LDAP.

-P*keyfilepw*
Zadajte heslo databázy kľúčov. Toto heslo sa vyžaduje na prístup k zašifrovaným informáciám v súbore databázy kľúčov, ktorý môže obsahovať jeden alebo viac súkromných kľúčov. Ak je k databázovému súboru kľúčov priradený súbor hesiel, heslo sa získa zo súboru hesiel a parameter **-P** sa nevyžaduje. Ak nie je zadané **-Z** ani **-K**, tento parameter sa ignoruje.

-R Určuje, že odvolávky automaticky nenasledujú.

-U *meno užívateľa*
Zadajte meno užívateľa. Vyžaduje sa pri -m DIGEST-MD5 a ignoruje sa pri všetkých ostatných mechanizmoch.

-v Použije sa viacslovný režim s veľkým množstvom diagnostík zapísaných do štandardného výstupu.

-V *version*
Určuje verziu LDAP, ktorú použije nástroj **ldapdchangepwd** pri naviazaní k serveru LDAP. Štandardne sa vytvára pripojenie LDAP V3. Ak chcete explicitne vybrať LDAP V3, zadajte parameter **-V 3**. Ak chcete program spustiť ako aplikáciu LDAP V2, zadajte **-V 2**. Aplikácia, napríklad **ldapdchangepwd** vyberá LDAP V3 ako preferovaný protokol pomocou ldap_init namiesto ldap_open.

-w *passwd* **| ?**
Použiť ***passwd*** ako heslo pre autentifikáciu. Ak použijete hodnotu ?, vygeneruje sa výzva pre zadanie hesla.

-y proxydn
Vytvorí náhradné ID pre zástupnú autorizačnú operáciu.

–Y Použiť bezpečné LDAP pripojenie (TLS).

-Z Na komunikáciu so serverom LDAP použije bezpečné spojenie SSL. Ak na Adresárovom serveri na i5/OS použijete parameter -Z a nepoužijete -K alebo -N, použije sa certifikát priradený k ID aplikácie Directory Services Client.

-? Zobrazenie pomoci k syntaxi príkazu ldapchangepwd.

Príklady

Príkaz

```
ldapchangepwd -D cn=John Doe -w a1b2c3d4 -n wxyz9876
```

zmení heslo pre položku s atribútom commonName rovným ″John Doe″ z a1b2c3d4 na wxyz9876

Diagnostika

Ak nedôjde k chybe, bude stav ukončenia rovný 0. Chyba spôsobí stav ukončenia iný ako nula a na štandardný chybový výstup sa zapíše diagnostická správa.

ldapdiff

Nástroj pre synchronizáciu repík LDAP.

Poznámka: V závislosti od počtu replikovaných položiek (a atribútov týchto položiek) sa môže tento príkaz vykonávať dlho.

Prehľad

(Porovnanie a synchronizácia údajových položiek medzi dvoma servermi v rámci prostredia replikácie.)

```
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]
```

alebo

(Porovnanie schémy medzi dvoma servermi.)

```
 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

Tento nástroj synchronizuje replikačný server s hlavným serverom. Ak chcete zobraziť pomoc k syntaxi pre **ldapdiff**, zadajte:

```
ldapdiff -?
```

Voľby

Tieto voľby sú platné pre príkaz **ldapdiff**. Sú rozdelené na dve skupiny platné špecificky pre dodávateľský server alebo spotrebiteľský server.

-a Určuje použitie riadenia správy servera pre zápisy do repliky len na čítanie.

-b *baseDN*
Namiesto predvolenej hodnoty sa ako začiatočný bod použije hodnota searchbase. Ak nie je zadané **-b**, program sa pokúsi definíciu searchbase získať analýzou premennej prostredia LDAP_BASEDN.

-C *countnumber*
Počítanie opravovaných položiek. Ak sa nájde viac ako tento počet nezhôd, nástroj sa ukončí.

-F Toto je voľba pre opravu. Ak je zadaná, obsah spotrebiteľského servera sa upraví, aby zodpovedal obsahu dodávateľského servera. Toto nie je možné použiť, ak je zadaná aj voľba **-S**.

-L Ak nie je zadaná voľba **-F**, môžete pomocou tejto voľby pre výstup vygenerovať súbor LDIF. Súbor LDIF môžete použiť na aktualizáciu spotrebiteľa a odstránenie rozdielov.

-S Určuje porovnávanie schémy v oboch serveroch.

-v Použije sa viacslovný režim s veľkým množstvom diagnostík zapísaných do štandardného výstupu.

Voľby pre dodávateľa replikácie

Tieto voľby sú platné pre spotrebiteľský server a sú označené počiatočným znakom ’s’ v názve voľby.

-sD *dn* Na naviazanie k serveru LDAP sa použije hodnota ***dn***. ***dn*** je DN reprezentované reťazcom.

-sh *host*
Určuje názov hostiteľa.

-sK *keyStore*
Určuje názov databázového súboru kľúčov SSL s predvoleným rozšírením **kdb**. Ak tento parameter nie je

zadaný alebo hodnota je prázdny reťazec (-sK″″) použije sa systémový úložný priestor kľúčov. Ak databázový súbor kľúčov nie je v aktuálnom adresári, zadajte úplný názov databázového súboru kľúčov.

-sN *keyLabel*
Zadajte návestie patriace klientskemu certifikátu v databázovom súbore kľúčov. Ak je návestie zadané bez určenia úložného priestoru kľúčov, návestie je identifikátor aplikácie v správcovi digitálnych certifikátov (DCM). Predvolené označenie (id aplikácie) je QIBM_GLD_DIRSRV_CLIENT. Ak je server LDAP nakonfigurovaný, aby vykonával len autentifikáciu servera, nevyžaduje sa certifikát klienta. Ak je server LDAP nakonfigurovaný, aby vykonával autentifikáciu servera a klienta, vyžaduje sa certifikát klienta. Ak je vytvorený predvolený pár certifikát/súkromný kľúč, hodnota ***keyLabel*** sa nevyžaduje. Podobne, ak vo vytvorenom databázovom súbore kľúčov existuje len jeden pár certifikát/súkromný kľúč, hodnota ***keyLabel*** sa nevyžaduje. Ak nie je zadané **-sZ** ani **-sK**, tento parameter sa ignoruje.

-sp *ldapport*
Určuje alternatívny port TCP, na ktorom počúva server LDAP. Štandardný port LDAP je 389. Ak nie je zadané **-sp** a je zadané **-sZ** použije sa predvolený port 636 pre SSL LDAP.

-sP *keyStorePwd*
Zadajte heslo databázy kľúčov. Toto heslo sa vyžaduje na prístup k zašifrovaným informáciám v súbore databázy kľúčov, ktorý môže obsahovať jeden alebo viac súkromných kľúčov. Ak je k databázovému súboru kľúčov priradený súbor hesiel, heslo sa získa zo súboru hesiel a parameter **-sP** sa nevyžaduje. Ak nie je zadané **-sZ** ani **-sK**, tento parameter sa ignoruje. Heslo sa nepoužije, ak pre použitý úložný priestor kľúčov existuje skrytý súbor.

-st *trustStoreType*
Zadajte návestie patriace klientskemu certifikátu v databázovom súbore dôveryhodných položiek. Ak je server LDAP nakonfigurovaný, aby vykonával len autentifikáciu servera, nevyžaduje sa certifikát klienta. Ak je server LDAP nakonfigurovaný, aby vykonával autentifikáciu servera a klienta, môže sa vyžadovať certifikát klienta. Ak je vytvorený predvolený pár certifikát/súkromný kľúč, hodnota ***trustStoreType*** sa nevyžaduje. Podobne, ak vo vytvorenom databázovom súbore kľúčov existuje len jeden pár certifikát/súkromný kľúč, hodnota ***trustStoreType*** sa nevyžaduje. Ak nie je zadané **-sZ** ani **-sT**, tento parameter sa ignoruje.

-sZ Na komunikáciu so serverom LDAP použije bezpečné spojenie SSL.

Voľby pre spotrebiteľa replikácie

Tieto voľby sú platné pre spotrebiteľský server a sú označené počiatočným znakom ’c’ v názve voľby. Ak je zadané -cZ bez zadania is hodnôt pre -cK, -cN alebo -cP, použijú tieto hodnoty rovnakú hodnotu, ako bola zadaná pre voľby SSL dodávateľa. Ak chcete nahradiť voľby dodávateľa a použiť predvolené nastavenie, zadajte -cK ″″ -cN ″″ -cP ″″.

-cD *dn* Na naviazanie k serveru LDAP sa použije hodnota ***dn***. ***dn*** je DN reprezentované reťazcom.

-ch *host*
Určuje názov hostiteľa.

-cK *keyStore*
Určuje názov databázového súboru kľúčov SSL s predvoleným rozšírením kdb. Ak je hodnota prázdny reťazec (-sK″″) použije sa systémový úložný priestor kľúčov. Ak databázový súbor kľúčov nie je v aktuálnom adresári, zadajte úplný názov databázového súboru kľúčov.

-cN *keyLabel*
Zadajte návestie patriace klientskemu certifikátu v databázovom súbore kľúčov. Ak je server LDAP nakonfigurovaný, aby vykonával len autentifikáciu servera, nevyžaduje sa certifikát klienta. Ak je návestie zadané bez určenia úložného priestoru kľúčov, návestie je identifikátor aplikácie v správcovi digitálnych certifikátov (DCM). Predvolené označenie (id aplikácie) je QIBM_GLD_DIRSRV_CLIENT. Ak je server LDAP nakonfigurovaný, aby vykonával autentifikáciu servera a klienta, vyžaduje sa certifikát klienta. Ak je vytvorený predvolený pár certifikát/súkromný kľúč, hodnota ***keyLabel*** sa nevyžaduje. Podobne, ak vo vytvorenom databázovom súbore kľúčov existuje len jeden pár certifikát/súkromný kľúč, hodnota ***keyLabel*** sa nevyžaduje. Tento parameter sa ignoruje, ak nie je zadané **-cZ** ani **-cK**.

-cp *ldapport*
Určuje alternatívny port TCP, na ktorom počúva server LDAP. Štandardný port LDAP je 389. Ak nie za zadané **-cp** a je zadané **-cZ**, použije sa predvolený port 636 pre SSL LDAP.

-cP *keyStorePwd*
Zadajte heslo databázy kľúčov. Toto heslo sa vyžaduje na prístup k zašifrovaným informáciám v súbore databázy kľúčov, ktorý môže obsahovať jeden alebo viacero súkromných kľúčov. Ak je k databázovému súboru kľúčov priradený súbor hesiel, heslo sa získa zo súboru hesiel a parameter **-cP** sa nevyžaduje. Ak nie je zadané **-cZ** ani **-cK**, tento parameter sa ignoruje.

-cw *password* **| ?**
Pre autentifikáciu sa použije heslo ***password***. Ak použijete hodnotu ?, vygeneruje sa výzva pre zadanie hesla.

-cZ Na komunikáciu so serverom LDAP použije bezpečné spojenie SSL.

Príklady

```
ldapdiff -b <baseDN> -sh <supplierhostname> -ch <consumerhostname> []
```

alebo

```
ldapdiff -S  -sh <supplierhostname> -ch <consumerhostname> [možnosti]
```

Diagnostika

Ak nedôjde k chybe, bude stav ukončenia rovný 0. Chyba spôsobí stav ukončenia iný ako nula a na štandardný chybový výstup sa zapíše diagnostická správa.

Používanie SSL s pomocnými programami príkazového riadka LDAP

“Secure Sockets Layer (SSL) a Transport Layer Security (TLS) s adresárovým serverom” na strane 47 sa zaoberá použitím SSL s adresárovým serverom LDAP. Tieto informácie zahŕňajú riadenie a vytváranie dôveryhodných certifikačných autorít manažérom digitálnych certifikátov.

Niektoré servery LDAP, do ktorých vstupujú klienti, používajú len autentifikáciu servera. Pre tieto servery musíte definovať jeden alebo viac dôveryhodných zdrojových certifikátov v pamäti certifikátov. Ak je použitá autentifikácia servera, je klientovi jasné, že cieľovému serveru LDAP bol certifikát vydaný jednou z dôveryhodných Certifikačných autorít (CA). Aj všetky transakcie LDAP, ktoré tečú ponad spojenie SSL so serverom, sú zakódované. Medzi tieto procesy patria aj povoľovacie údaje LDAP, dodávané v aplikačných programových rozhraniach (API), ktoré sa používajú na väzbu s adresárovým serverom. Napríklad, ak server LDAP používa vysoko spoľahlivý certifikát Verisign, mali by ste urobiť nasledujúce:

1. Od Verisign získať certifikát CA.
2. Na jeho importovanie do vašej pamäte certifikátov použite DCM.
3. Na jeho označenie za dôveryhodný certifikát použite DCM.

Ak server LDAP používa súkromne vydaný certifikát servera, administrátor serverov vám môže dodať kópiu súboru požiadaviek certifikátu serverov. Certifikát požadovaného súboru importujte do vašej pamäti certifikátov a označte ho ako dôveryhodný.

Ak používate na prístup k serverom LDAP funkcie shell, ktoré používajú autentifikáciu klienta aj autentifikáciu servera, musíte urobiť nasledujúce:

- Definujte jeden alebo viacej dôveryhodných zdrojov certifikátov v systémovej pamäti certifikátov. Toto umožňuje klientovi mať istotu, že cieľovému serveru LDAP bol certifikát vydaný jednou z dôveryhodných CA. Aj všetky transakcie LDAP, ktoré tečú ponad spojenie SSL so serverom, sú zakódované. Medzi tieto procesy patria aj povoľovacie údaje LDAP, dodávané v aplikačných programových rozhraniach (API), ktoré sa používajú na väzbu s adresárovým serverom.
- Vytvorte kľúčový pár a od CA vyžiadajte klientsky certifikát. Po prijatí podpísaného certifikátu od CA certifikát umiestnite do súboru kľúčov klienta.

Formát LDIF (LDAP data interchange format)

Táto dokumentácia opisuje LDIF (formát výmeny údajov) LDAP, aký sa používa v pomocných programoch ldapmodify, ldapsearch a ldapadd. Tu uvedený formát LDIF tiež podporujú pomocné programy servera poskytované spolu s IBM Directory.

Formát LDIF sa používa na reprezentáciu položiek LDAP v textovej forme. Základný formát položky LDIF je:

```
dn: <distinguished name>
<attrtype> : <attrvalue>
<attrtype> : <attrvalue>
...
```

Riadok môže pokračovať tak, že nasledujúci riadok sa bude začínať jednou medzerou alebo znakom tabulátora, napríklad:

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

Viac hodnôt sa zadáva na samostatných riadkoch, napríklad:

```
      cn: John E Doe
cn: John Doe
```

Ak <*attrvalue*> obsahuje znak iný ako US-ASCII alebo začína medzerou alebo dvojbodkou ':', <*attrtype*> je nasledované dvoma dvojbodkami a hodnota je kódovaná v notácii base-64. Napríklad hodnota ″ začína medzerou″ by bola kódovaná takto:

```
cn:: IGJlZ2lucyB3aXRoIGEgc3BhY2U=
```

Viacero položiek v rovnakom súbore LDIF je oddelených prázdnym riadkom. Viacero prázdnych riadkov sa považuje za koniec sú boru.

Viac informácií nájdete v nasledujúcich témach:

- "Príklad: LDIF"
- "Podpora LDIF verzie 1" na strane 215
- "Príklady: Verzia 1 LDIF" na strane 215

Príklad: LDIF

Nasleduje príklad súboru LDIF s tromi položkami.

```
dn: cn=John E Doe, o=University of High
 er Learning, c=US
cn: John E Doe
cn: John Doe
objectclass: person
sn: Doe

dn: cn=Bjorn L Doe, o=University of High
 er Learning, c=US
cn: Bjorn L Doe
cn: Bjorn Doe
objectclass: person
sn: Doe

dn: cn=Jennifer K. Doe, o=University of High
 er Learning, c=US
cn: Jennifer K. Doe
cn: Jennifer Doe
objectclass: person
sn: Doe
```

```
jpegPhoto:: /9j/4AAQSkZJRgABAAAAAQABAAD/2wBDABALD
 A4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQ
 ERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARESEhgVG
...
```

Atribút jpegPhoto v položke Jennifer Jensen je kódovaný pomocou base-64. Textové hodnoty atribútov je tiež možné zadať vo formáte base-64. V tomto prípade však musí byť kódovanie base-64 v kódovej stránke základného formátu pre protokol (pre LDAP V2 to je znaková sada IA5 a pre protokol LDAP V3 to je kódovanie UTF-8).

Podpora LDIF verzie 1

Nástroje klienta (ldapmodify a ldapadd) boli rozšírené na rozpoznanie poslednej verzie LDIF, ktorá je identifikovaná prítomnosťou značky ″version: 1″ v hlavičke súboru. Na rozdiel od originálnej verzie LDIF, novšia verzia LDIF podporuje hodnoty atribútov, reprezentované v UTF-8 (namiesto US-ASCII s množstvom obmedzení).

Manuálne vytvorenie súboru LDIF obsahujúceho hodnoty UTF-8 však môže byť zložité. Na zjednodušenie tohto procesu je k dispozícii podpora rozšírenia znakovej sady na formát LDIF. Toto rozšírenie dovoľuje zadať názov znakovej sady IANA v hlavičke súboru LDIF (spolu s číslom verzie). Je podporovaná obmedzená množina znakových sád IANA.

Formát LDIF verzie 1 tiež podporuje odkazy URL na súbory. Toto poskytuje pružnosť pri definovaní špecifikácie súboru. Odkazy URL na súbory používajú tento formát:

```
      attribute:< file:///path          (syntax pre path
závisí na platforme)
```

Nasleduje príklad platných vzorových webových adries súborov:

```
      jpegphoto:<
file:///d:\temp\photos\myphoto.jpg    (cesta v štýle DOS/Windows)
      jpegphoto:< file:///etc/temp/photos/myphoto.jpg   (cesta v štýle Unix)
```

Poznámka: Pomocné programy IBM Directory podporujú nový aj starý (″jpegphoto: /etc/temp/myphoto″) spôsob špecifikácie URL súboru bez ohľadu na špecifikáciu verzie. Inými slovami, nový formát URL súboru sa môže používať bez pridania značky version do vašich súborov LDIF.

Príklady: Verzia 1 LDIF

Môžete použiť voliteľnú značku charset, aby nástroje automaticky vykonali konverziu zo zadanej znakovej sady na UTF-8 ako v tomto príklade:

```
  version: 1
 charset: ISO-8859-1

 dn: cn=Juan Griego, o=University of New Mexico, c=US
 cn: Juan Griego
 sn: Griego
 description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd
 title: Associate Dean
 title: [nadpis v španielčine]
 jpegPhoto:> file:///usr/local/photos/jgriego.jpg
```

V tomto príklade sa všetky hodnoty za názvom atribútu a jednou dvojbodkou preložia zo znakovej sady ISO-8859-1 na UTF-8. Hodnoty za názvom atribútu a dvojitou dvojbodkou (napríklad description:: V2hhdCBhIGNhcm...) musia byť kódované v base-64 a očakáva sa, že budú binárne alebo znakové reťazce UTF-8. Očakáva sa tiež, že hodnoty prečítané zo súboru, napríklad atribút jpegPhoto, určený webovou adresou v predošlom príklade, budú tiež binárne alebo UTF-8. Pre tieto hodnoty sa nevykoná žiadny preklad zo zadaného ″charset″ na UTF-8.

V tomto príklade súboru LDIF bez značky charset sa očakáva, že obsah bude kódovaný ako UTF-8 alebo UTF-8 kódované cez base-64 alebo ako binárne údaje kódované v base-64:

```
# IBM Directorysample LDIF file
 #
 # The suffix "o=IBM, c=US" should be defined before attempting to load
 # this data.

 version: 1

 dn: o=IBM, c=US
 objectclass: top
 objectclass: organization
 o: IBM

 dn: ou=Austin, o=IBM, c=US
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

Tento istý súbor by mohol byť použitý bez informácie záhlavia o verzii: 1 tak, ako v predchádzajúcich vydaniach IBM Directory:

```
 # IBM Directorysample LDIF file
 #
 # The suffix "o=IBM, c=US" should be defined before attempting to load
 # this data.

 dn: o=IBM, c=US
 objectclass: top
 objectclass: organization
 o: IBM

 dn: ou=Austin, o=IBM, c=US
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

Poznámka: Textové hodnoty atribútov je možné zadať vo formáte base-64.

Schéma konfigurácie adresárového servera

Tieto informácie opisujú DIT (Directory Information Tree) a atribúty používané na konfiguráciu súboru ibmslapd.conf. V predchádzajúcich vydaniach sa konfiguračné nastavenia adresárov ukladali do konfiguračného súboru vo vlastnom formáte. Nastavenia adresára sa teraz ukladajú v konfiguračných súboroch pomocou formátu LDIF.

Konfiguračný súbor má názov ibmslapd.conf. Je tiež k dispozícii schéma používaná konfiguračným súborom. Typy atribútov môžete nájsť v súbore v3.config.at a triedy objektov sú v súbore v3.config.oc. Atribúty je možné upravovať pomocou príkazu ldapmodify. Viac informácií o príkaze ldapmodify nájdete v časti “ldapmodify a ldapadd” na strane 185.

- “Strom informácií v adresári”
- “Atribúty” na strane 225

Strom informácií v adresári

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 Toto je položka na najvyššej úrovni v konfigurácii DIT. Obsahuje údaje, ktoré sú pre server globálne, hoci v praxi môže tiež obsahovať rôzne položky. Každý atribút v tejto položke sa stane prvou časťou (odsek global) súboru ibmslapd.conf.

Počet 1 (vyžadované)

Trieda objektov
ibm-slapdTop

Povinné atribúty

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

Voliteľné atribúty

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (Deprecated)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion

cn=Admin

DN cn=Admin, cn=Configuration

Opis Globálne konfiguračné nastavenia pre IBM démona admin

Počet 1 (vyžadované)

Trieda objektov
ibm-slapdAdmin

Povinné atribúty

- cn
- ibm-slapdErrorLog
- ibm-slapdPort

Voliteľné atribúty

- ibm-slapdSecurePort

cn=Event Notification

DN cn=Event Notification, cn=Configuration

Opis Globálne nastavenia pre notifikáciu na udalosti pre adresárový server

Počet 0 alebo 1 (voliteľné, potrebné len v prípade, ak chcete povoliť notifikáciu na udalosti)

Trieda objektov
ibm-slapdEventNotification

Povinné atribúty

- cn
- ibm-slapdEnableEventNotification
- objectClass

Voliteľné atribúty

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

cn=Front End

DN cn=Front End, cn=Configuration

Opis Globálne nastavenia prostredia, ktoré server aplikuje pri spúšťaní.

Počet 0 alebo 1 (voliteľné)

Trieda objektov
ibm-slapdFrontEnd

Povinné atribúty

- cn
- objectClass

Voliteľné atribúty

- 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 Globálne nastavenia autentifikácie Kerberos pre adresárový server.

Počet 0 alebo 1 (voliteľné)

Trieda objektov
ibm-slapdKerberos

Povinné atribúty

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

Voliteľné atribúty

- Žiadne

cn=Master Server

DN cn=Master Server, cn=Configuration

Opis Pri konfigurácii repliky táto položka obsahuje prihlasovacie údaje pre pripojenie a URL odvolávky hlavného servera.

Počet 0 alebo 1 (voliteľné)

Trieda objektov
ibm-slapdReplication

Povinné atribúty

- cn
- ibm-slapdMasterPW (Povinné, ak sa nepoužíva autentifikácia Kerberos.)

Voliteľné atribúty

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Voliteľné, ak sa používa autentifikácia Kerberos.)
- ibm-slapdMasterReferral
- objectClass

cn=Referral

DN cn=Referral, cn=Configuration

Opis Táto položka obsahuje všetky položky odvolávok z prvej časti (odsek global) súboru ibmslapd.conf. Ak neexistujú odvolávky (predvolené nastavenie), táto položka je voliteľná.

Počet 0 alebo 1 (voliteľné)

Trieda objektov
ibm-slapdReferral

Povinné atribúty

- cn
- ibm-slapdReferral
- objectClass

Voliteľné atribúty

- Žiadne

cn=Schemas

DN cn=Schemas, cn=Configuration

Opis Táto položka slúži ako kontajner pre schémy. Táto položka nie je v skutočnosti potrebná, pretože schémy môžu byť rozlíšené pomocou triedy objektov ibm-slapdSchema. Je k dispozícii kvôli lepšej čitateľnosti DIT.

V súčasnosti je dovolená len jedna položka schémy: cn=IBM Directory.

Počet 1 (vyžadované)

Trieda objektov
Kontajner

Povinné atribúty

- cn
- objectClass

Voliteľné atribúty

- Žiadne

cn=IBM Directory

DN cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Táto položka obsahuje všetky konfiguračné údaje schémy z prvej sekcie (odsek global) súboru ibmslapd.conf. Slúži tiež ako kontajner pre všetky ukončenia, ktoré používajú danú schému. V súčasnosti nie je podporovaných viacero schém, ale keby boli, jedna schéma môže používať jednu položku ibm-slapdSchema. Nezabudnite, že viacero schém sa považuje za nekompatibilné. Z tohto dôvodu môže byť ukončenie priradené len k jednej schéme.

Počet 1 (vyžadované)

Trieda objektov
ibm-slapdSchema

Povinné atribúty

- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

Voliteľné atribúty

- ibm-slapdSchemaAdditions

cn=Config Backends

DN cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Táto položka slúži ako kontajner pre ukončenia Config.

Počet 1 (vyžadované)

Trieda objektov
Kontajner

Povinné atribúty

- cn

- objectClass

Voliteľné atribúty
Žiadne

cn=ConfigDB

DN cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Backend pre konfiguráciu servera IBM Directory

Počet 0 - n (voliteľné)

Trieda objektov
ibm-slapdConfigBackend

Povinné atribúty

- ibm-slapdSuffix
- ibm-slapdPlugin

Voliteľné atribúty

- ibm-slapdReadOnly

cn=RDBM Backends

DN cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Táto položka slúži ako kontajner pre ukončenia RDBM. a účinne nahrádza riadok databázy rdbm z ibmslapd.conf identifikovaním všetkých podpoložiek ako backendov DB2. Táto položka nie je v skutočnosti potrebná, pretože ukončenia RDBM môžu byť rozšlíšené pomocou triedy objektov ibm-slapdRdbmBackend. Je k dispozícii kvôli lepšej čitateľnosti DIT.

Počet 0 alebo 1 (voliteľné)

Trieda objektov
Kontajner

Povinné atribúty

- cn
- objectClass

Voliteľné atribúty

- Žiadne

cn=Directory

DN cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Táto položka obsahuje všetky konfiguračné nastavenia databázy pre predovlené ukončenie databázy RDBM.

Hoci možno vytvoriť viaceré backendy s ľubovoľnými názvami, správa servera predpokladá, že ″cn=Directory″ je backendom hlavného adresára a ″cn=ChangeLog″ je voliteľným backendom protokolu zmien. Len prípony zobrazené v ″cn=Directory″ možno nakonfigurovať prostredníctvom správy servera (s výnimkou prípony protokolu zmien, ktorá sa nastavuje transparentne zapnutím protokolu zmien).

Počet 0 - n (voliteľné)

Trieda objektov
ibm-slapdRdbmBackend

Povinné atribúty

- cn

- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Voliteľné atribúty

- 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

  Poznámka: Ak používate **ibm-slapdUseProcessIdPw**, schému musíte zmeniť tak, aby **ibm-slapdDbUserPW** bol voliteľný.

cn=Change Log

DN cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Táto položka obsahuje všetky konfiguračné nastavenia databázy pre ukončenie protokolu zmien.

Počet 0 - n (voliteľné)

Trieda objektov
ibm-slapdRdbmBackend

Povinné atribúty

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Voliteľné atribúty

- 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

Poznámka: Ak používate **ibm-slapdUseProcessIdPw**, schému musíte zmeniť tak, aby **ibm-slapdDbUserPW** bol voliteľný.

cn=LDCF Backends

DN cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Táto položka slúži ako kontajner pre ukončenia LDCF. Účinne nahrádza riadok databázy ldcf z ibmslapd.conf tým, že identifikuje všetky podpoložky ako ukončenia LDCF. Táto položka nie je v skutočnosti potrebná, pretože ukončenia LDCF môžu byť rozlíšené pomocou triedy objektov ibm-slapdLdcfBackend. Je k dispozícii kvôli lepšej čitateľnosti DIT.

Počet 1 (vyžadované)

Trieda objektov
Kontajner

Povinné atribúty
- cn
- objectClass

Voliteľné atribúty
- ibm-slapdPlugin

cn=SchemaDB

DN cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Opis Táto položka obsahuje všetky konfiguračné údaje databázy z časti ldcf database súboru ibmslapd.conf.

Počet 1 (vyžadované)

Trieda objektov
ibm-slapdLdcfBackend

Povinné atribúty
- cn
- objectClass

Voliteľné atribúty
- ibm-slapdPlugin
- ibm-slapdSuffix

cn=SSL

DN cn=SSL, cn=Configuration

Opis Globálne nastavenia pripojenia SSL pre adresárový server.

Počet 0 alebo 1 (voliteľné)

Trieda objektov
ibm-slapdSSL

Povinné atribúty

- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

Voliteľné atribúty

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

  Poznámka: **ibm-slapdSslCipherSpecs** je teraz nedovolené. Namiesto toho použite **ibm-slapdSslCipherSpec**. Ak používate **ibm-slapdSslCipherSpecs**, server spraví konverziu na podporovaný atribút.
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW

cn=CRL

DN cn=CRL, cn=SSL, cn=Configuration

Opis Táto položka obsahuje údaje zoznamu zrušených certifikátov z prvej sekcie (odsek global) súboru ibmslapd.conf. Je to potrebné len v prípade, ak ″ibm-slapdSslAuth = serverclientauth″ v položke cn=SSL a na validáciu cez CRL boli poskytnuté certifikáty klienta.

Počet 0 alebo 1 (voliteľné)

Trieda objektov
ibm-slapdCRL

Povinné atribúty

- cn
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPort
- objectClass

Voliteľné atribúty

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword

cn=Transaction

DN cn = Transaction, cn = Configuration

Opis Určuje globálne nastavenia podpory transakcií. Podpora transakcií je poskytovaná ako doplnkový komponent:

```
extendedop /QSYS.LIB/QGLDTRANEX.SRVPGM tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

Server (**slapd**) zavedie tento doplnkový komponent automaticky, ak **ibm-slapdTransactionEnable = TRUE**. Tento doplnkový komponent nie je potrebné explicitne pridávať do **ibmslapd.conf**.

Počet 0 alebo 1 (voliteľné; vyžadované len v prípade, ak chcete používať transakcie.)

Trieda objektov
ibm-slapdTransaction

Povinné atribúty

- cn
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

Voliteľné atribúty

- Žiadne

Atribúty

- 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 Toto je atribút bežného názvu X.500, ktorý obsahuje názov objektu.

Syntax Reťazec adresára

Maximálna dĺžka
256

Hodnota
Viac hodnôt

ibm-slapdACIMechanism

Opis Určuje, ktorý model ACL používa server. (Podporuje sa len na platformách i5/OS a OS/400 v3.2 a ignoruje sa na ostatných platformách.)

- 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

Predvolená hodnota
1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL model

Syntax Reťazec adresára

Maximálna dĺžka
256

Hodnota
Viac hodnôt.

ibm-slapdACLAccess

Opis Riadi, či je povolený prístup k zoznamom ACL. Ak je nastavený na TRUE, prístup k zoznamom ACL je povolený. Ak je nastavený na FALSE, prístup k zoznamom ACL je zakázaný.

Predvolená hodnota
TRUE

Syntax Boolean

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdACLCache

Opis Riadi, či server ukladá informácie ACL do vyrovnávacej pamäte.

- Ak je nastavený na TRUE, server ukladá informácie ACL do vyrovnávacej pamäte.
- Ak je nastavený na FALSE, server neukladá informácie ACL do vyrovnávacej pamäte.

Predvolená hodnota
TRUE

Syntax Boolean

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdACLCacheSize

Opis Maximálny počet položiek na uchovanie vo vyrovnávacej pamäti ACL.

Predvolená hodnota
25000

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdAdminDN

Opis DN pripojenia administrátora pre adresárový server.

Predvolená hodnota
cn=root

Syntax DN

Maximálna dĺžka
Neobmedzené

Hodnota
Jedna hodnota

ibm-slapdAdminGroupEnabled

Opis Uvádza, či je administratívna skupina momentálne zapnutá. Ak je nastavená na TRUE, server umožní prihlásiť sa užívateľom v administratívnej skupine.

Predvolená hodnota
FALSE

Syntax Boolean

Maximálna dĺžka
128

Hodnota
Jedna hodnota

ibm-slapdAdminPW

Opis Heslo pripojenia administrátora pre adresárový server.

Predvolená hodnota
secret

Syntax Binary

Maximálna dĺžka
128

Hodnota
Jedna hodnota

ibm-slapdAllowAnon

Opis Uvádza, či je povolené vytváranie anonymných väzieb.

Predvolená hodnota
True

Syntax Boolean

Maximálna dĺžka
128

Hodnota
Jedna hodnota

ibm-slapdAllReapingThreshold

Opis Uvádza, aký počet pripojení sa má ponechať na serveri pred aktiváciou manažmentu pripojení.

Predvolená hodnota
1200

Syntax Reťazec adresára zohľadňujúci veľkosť písmen.

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdAnonReapingThreshold

Opis Uvádza, aký počet pripojení sa má ponechať na serveri pred aktiváciou manažmentu anonymných pripojení.

Predvolená hodnota
0

Syntax Reťazec adresára zohľadňujúci veľkosť písmen.

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdBoundReapingThreshold

Opis Uvádza, aký počet pripojení sa má ponechať na serveri pred aktiváciou manažmentu anonymných a viazaných pripojení.

Predvolená hodnota
1100

Syntax Reťazec adresára zohľadňujúci veľkosť písmen.

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdBulkloadErrors

Opis Cesta k súboru alebo zariadeniu v hostiteľskom počítači ibmslapd, kam sa zapíšu chybové správy bulkload.

Predvolená hodnota
/var/bulkload.log

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdCachedAttribute

Opis Obsahuje názvy atribútov, ktoré majú byť uložené do vyrovnávacej pamäte atribútov; na jednu hodnotu jeden názov atribútu.

Predvolená hodnota
Žiadne

Syntax Reťazec adresára

Maximálna dĺžka
256

Hodnota
Viac hodnôt

ibm-slapdCachedAttributeAutoAdjust

Opis Kontroluje, či server automaticky nastaví vyrovnávacie pamäte atribútov v nakonfigurovaných časových intervaloch definovaných v ibm-slapdCachedAttributeAutoAdjustTime a ibm-slapdCachedAttributeAutoAdjustTimeInterval.

Predvolená hodnota
FALSE

Syntax Boolean

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdCachedAttributeAutoAdjustTime

Opis Keď je ibm-slapdCachedAttributeAutoAdjust nastavený na TRUE, kontroluje čas, kedy server začne automaticky upravovať vyrovnávacie pamäte atribútov.

```
Minimum = T000000
Maximum = T235959
```

Predvolená hodnota
T000000

Syntax Vojenský čas

Maximálna dĺžka
7

Hodnota
Jedna hodnota

ibm-slapdCachedAttributeAutoAdjustTimeInterval

Opis Keď je ibm-slapdCachedAttributeAutoAdjust nastavený na TRUE, kontroluje časový interval medzi automatickými úpravami vyrovnávacej pamäte atribútov.

```
Minimum = 1
Maximum = 24
```

Predvolená hodnota
2

Syntax Integer

Maximálna dĺžka
2

Hodnota
Jedna hodnota

ibm-slapdCachedAttributeSize

Opis Objem pamäte v bajtoch, ktorý môže vyrovnávacia pamäť atribútov použiť. Hodnota 0 znamená nepoužitie vyrovnávacej pamäte atribútov.

Predvolená hodnota
0

Syntax Integer

Maximálna dĺžka
11

Hodnota
S jednou hodnotou.

ibm-slapdChangeLogMaxEntries

Opis Tento atribút sa použije pri zapojení protokolu zmien na zadanie maximálneho počtu položiek protokolu zmien povoleného v databáze RDBM. Každý protokol zmien má vlastný atribút changeLogMaxEntries.

```
Minimum = 0
(neobmedzené)
Maximum = 2,147,483,647 (32-bitové celé číslo so znamienkom)
```

Predvolená hodnota
0

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdCLIErrors

Opis Cesta k súboru alebo zariadeniu v hostiteľskom počítači ibmslapd, kam sa zapíšu chybové správy CLI.

Predvolená hodnota
/var/db2cli.log

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdConcurrentRW

Opis Nastavenie hodnoty TRUE dovoľuje vykonávanie hľadania súčasne a aktualizáciou. Dovoľuje ’nekonzistenené čítania’, teda výsledky nemusia byť konzistentné s potvrdeným stavom databázy.

Upozornenie: Tento atribút nie je dovolený.

Predvolená hodnota
FALSE

Syntax Boolean

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdDB2CP

Opis Určuje kódovú stránku adresárovej databázy. 1208 je kódová stránka pre databázy UTF-8.

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdDBAlias

Opis Alias databázy DB2.

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
8

Hodnota
Jedna hodnota

ibm-slapdDbConnections

Opis Uvádza počet pripojení DB2, ktoré server vyhradí backendu DB2. Táto hodnota musí byť medzi 5 a 50 (vrátane).

Poznámka: Premenná prostredia ODBCCONS nahrádza hodnotu tejto direktívy.
Ak je ibm-slapdDbConnections (alebo ODBCCONS) menšie ako 5, respektíve väčšie ako 50, server použije hodnotu 5, respektíve 50. 1 dodatočné pripojenie sa vytvorí pre replikáciu (ak keď nie je definovaná replikácia). 2 dodatočné pripojenia sa vytvoria pre protokol zmien (ak je protokol zmien povolený).

Predvolená hodnota
15

Syntax Integer

Maximálna dĺžka
50

Hodnota
Jedna hodnota

ibm-slapdDbInstance

Opis Uvádza príklad databázy DB2 pre tento backend.

Predvolená hodnota
ldapdb2

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
8

Hodnota
Jedna hodnota

Poznámka: Všetky objekty ibm-slapdRdbmBackend musia používať rovnakú sadu znakov ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW a DB2.

ibm-slapdDbLocation

Opis Cesta v súborovom systéme, kde sa nachádza koncová databáza.

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdDbName

Opis Uvádza názov databázy DB2 pre tento backend.

Predvolená hodnota
ldapdb2

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
8

Hodnota
Jedna hodnota

ibm-slapdDbUserID

Opis Uvádza meno užívateľa, s ktorým sa má vytvoriť väzba na databázu DB2 pre tento backend.

Predvolená hodnota
ldapdb2

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
8

Hodnota
Jedna hodnota

Poznámka: Všetky objekty ibm-slapdRdbmBackend musia používať rovnakú sadu znakov ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW a DB2.

ibm-slapdDerefAliases

Opis Maximálna úroveň dereferencovania aliasu v požiadavke vyhľadávania, bez ohľadu na akýkoľvek derefAliases, ktoré mohli byť špecifikované v klientskej požiadavke. Povolené hodnoty sú **nikdy**, **nájsť**, **vyhľadávať** a **vždy**.

Predvolená hodnota
vždy

Syntax Reťazec adresára

Maximálna dĺžka
6

Hodnota
Jedna hodnota

ibm-slapdDbUserPW

Opis Určuje užívateľské heslo na ktoré má byť viazaná databáza DB2 pre toto zálohovanie. Heslo môže byť normálny text alebo byť zašifrovaný pomocou imask.

Predvolená hodnota
ldapdb2

Syntax Binary

Maximálna dĺžka
128

Hodnota
Jedna hodnota

Poznámka: Všetky objekty ibm-slapdRdbmBackend musia používať rovnakú sadu znakov ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW a DB2.

ibm-slapdDigestAdminUser

Opis Uvádza meno užívateľa Digest MD5 administrátora LDAP alebo člena administratívnej skupiny. Používa sa pri použití autentifikácie MD5 Digest na autentifikáciu administrátora.

Predvolená hodnota
Žiadne

Syntax Reťazec adresára

Maximálna dĺžka
512

Hodnota
Jedna hodnota

ibm-slapdDigestAttr

Opis Nahrádza predvolený atribút mena užívateľa DIGEST-MD5. Názov atribútu, ktorý sa má použiť na vyhľadanie mena užívateľa pre väzbu DIGEST-MD5 SASL. Ak hodnota nie je zadaná, server použije uid.

Predvolená hodnota
Ak nie je zadaná, server použije uid.

Syntax Reťazec adresára.

Maximálna dĺžka
64

Hodnota
Jedna hodnota

ibm-slapdDigestRealm

Opis Nahrádza predvolenú realm DIGEST-MD5. Reťazec, ktorý môže užívateľom pomôcť zistiť, aké užívateľské meno a heslo použiť v prípade, že sa tieto pre rôzne servery líšia. Čo sa týka pojmov, ide o názov kolekcie kont, ktoré môžu zahŕňať aj užívateľské konto. Tento reťazec by mal obsahovať minimálne meno hostiteľa vykonávajúceho autentifikáciu a môže tiež znamenať kolekciu užívateľov s prístupom. Ako príklad môže slúžiť registered_users@gotham.news.example.com. Ak nie je atribút zadaný, server použije plne kvalifikované hostiteľské meno servera.

Predvolená hodnota
Plne kvalifikované hostiteľské meno servera

Syntax Reťazec adresára.

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdEnableEventNotification

Opis Určuje, či sa má povoliť podpora notifikácie. Musí byť nastavený na TRUE alebo FALSE.

Ak je nastavený na FALSE, server odmietne všetky požiadavky klientov o registráciu notifikácií na udalosti s rozšíreným výsledkom LDAP_UNWILLING_TO_PERFORM.

Predvolená hodnota
TRUE

Syntax Boolean

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdEntryCacheSize

Opis Maximálny počet položiek na uchovanie vo vyrovnávacej pamäti položiek.

Predvolená hodnota
25000

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdErrorLog

Opis Určuje cestu k súboru alebo zariadeniu v počítači adresárového servera, kam sa zapíšu chybové správy.

Predvolená hodnota
/var/ibmslapd.log

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdESizeThreshold

Opis Uvádza počet pracovných položiek v pracovnom fronte pred aktiváciou núdzového vlákna.

Predvolená hodnota
50

Syntax Integer

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdEThreadActivate

Opis Uvádza, za akých podmienok sa aktivuje núdzové vlákno. Musí byť nastavený na jednu z nasledujúcich hodnôt:

S Len veľkosť

T Len čas

SOT Veľkosť alebo čas

SAT Veľkosť a čas

Predvolená hodnota
SAT

Syntax Reťazec

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdEThreadEnable

Opis Uvádza, či je núdzové vlákno zapnuté.

Predvolená hodnota
True

Syntax Boolean

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdETimeThreshold

Opis Uvádza časový úsek v minútach medzi odstránením položiek z pracovného frontu pred aktivovaním núdzového vlákna.

Predvolená hodnota
5

Syntax Integer

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdFilterCacheBypassLimit

Opis Do vyrovnávacej pamäte vyhľadávacích filtrov sa nepridajú vyhľadávacie filtre, ktoré nájdu viac ako tento počet položiek. Zoznam identifikátorov položiek, nájdených filtrom sa zahrnie do tejto vyrovnávacej pamäte, preto toto nastavenie pomáha obmedziť použitie pamäte. Hodnota 0 označuje žiadny limit.

Predvolená hodnota
100

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdFilterCacheSize

Opis Určuje maximálny počet položiek na uchovanie vo vyrovnávacej pamäti vyhľadávacieho filtra.

Predvolená hodnota
25000

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdIdleTimeOut

Opis Maximálny čas udržiavania pripojenia LDAP v otvorenom stave, ak je pripojenie neaktívne. Čas nečinnosti pre pripojenie LDAP je čas (v sekundách) medzi poslednou aktivitou na pripojení a aktuálnym časom. Ak pripojenie exspiruje, pretože čas nečinnosti je väčší ako hodnota tohto atribútu, server LDAP vyčistí a ukončí dané pripojenie LDAP, čím ho sprístupní pre iné prichádzajúce požiadavky.

Predvolená hodnota
300

Syntax Integer

Dĺžka 11

Počet Jeden

Použitie
Operácia na adresári

Upraviteľné užívateľom
Yes

Trieda prístupu
Kritická

Vyžadované
Nie

ibm-slapdIncludeSchema

Opis Určuje cestu k súboru v počítači adresárového servera, ktorý obsahuje definície schém.

Predvolená hodnota
/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

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
1024

Hodnota
Viac hodnôt

ibm-slapdKrbAdminDN

Opis Určuje ID Kerberos administrátora LDAP (napríklad ibm-kn=admin1@realm1). Používa sa pri použití autentifikácie Kerberos na autentifikáciu administrátora pri prihlásení do rozhrania Správa servera. Môže to byť zadané ako náhrada alebo doplnok k adminDN a adminPW.

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
128

Hodnota
Jedna hodnota

ibm-slapdKrbEnable

Opis Určuje, či server podporuje Kerberos. Musí byť zadaný ako TRUE alebo FALSE.

Predvolená hodnota
TRUE

Syntax Boolean

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdKrbIdentityMap

Opis Určuje, či sa má používať mapovanie identity Kerberos. Musí byť nastavený na TRUE alebo FALSE. Ak je nastavený na TRUE a klient je autentifikovaný s ID Kerberos, server pohľadá všetkých lokálnych užívateľov s vyhovujúcimi prihlasovacími údajmi Kerberos a dané rozlišovacie mená týchto užívateľov pridá k prihlasovacím údajom viazania pre pripojenie. Toto dovoľuje používať zoznamy ACL, založené na rozlišovacích menách užívateľov LDAP.

Predvolená hodnota
FALSE

Syntax Boolean

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdKrbKeyTab

Opis Určuje súbor kľúčov Kerberos servera LDAP. Tento súbor obsahuje súkromný kľúč servera LDAP, ktorý je priradený k jeho kontu Kerberos. Tento súbor je potrebné chrániť (podobne, ako databázový súbor kľúčov SSL).

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdKrbRealm

Opis Určuje realm Kerberos servera LDAP. Používa sa na zverejnenie atribútu ldapservicename v rodičovskom DSE. Nezabudnite, že server LDAP môže vystupovať ako archív informácií o kontách pre viacero centier KDC (a realmov), ale server LDAP, ako server s Kerberos, môže byť členom jedného realmu.

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax Reťazec adresára, nezohľadňujúci veľkosť písmen

Maximálna dĺžka
256

Hodnota
Jedna hodnota

ibm-slapdLanguageTagsEnabled

Opis Či má server povoliť jazykové označenia alebo nie. Hodnota prečítaná zo súboru ibmslapd.conf pre tento atribút je FALSE, ale možno je nastaviť na TRUE.

Predvolená hodnota
FALSE

Syntax Boolean

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdLdapCrlHost

Opis Určuje názov hostiteľa servera LDAP, ktorý obsahuje zoznamy zrušených certifikátov (CRL) pre validáciu certifikátov x.509v3 klienta. Tento parameter je potrebný v prípade, ak pre validáciu CRL bolo poskytnuté ibm-slapdSslAuth=serverclientauth a certifikáty klienta.

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax Reťazec adresára, nezohľadňujúci veľkosť písmen

Maximálna dĺžka
256

Hodnota
Jedna hodnota

ibm-slapdLdapCrlPassword

Opis Určuje heslo, ktoré používa SSL na strane servera na naviazanie k serveru LDAP, ktorý obsahuje zoznamy zrušených certifikátov (CRL) pre validáciu certifikátov x.509v3 klienta. Tento parameter môže byť potrebný v prípade, ak pre validáciu CRL bolo poskytnuté ibm-slapdSslAuth=serverclientauth a certifikáty klienta.

Poznámka: Ak server LDAP, obsahujúci zoznamy CRL povoľuje neautentifikovaný prístup k zoznamom CRL (nazývaný anonymný prístup), nevyžaduje sa ibm-slapdLdapCrlPassword.

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax Binary

Maximálna dĺžka
128

Hodnota
Jedna hodnota

ibm-slapdLdapCrlPort

Opis Určuje port na použitie na pripojenie k serveru LDAP, ktorý obsahuje zoznamy zrušených certifikátov (CRL) pre validáciu certifikátov x.509v3 klienta. Tento parameter je potrebný v prípade, ak pre validáciu CRL bolo poskytnuté ibm-slapdSslAuth=serverclientauth a certifikáty klienta. (Porty IP sú 16-bitové celé čísla bez znamienka, z rozsahu 1 - 65535.)

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdLdapCrlUser

Opis Určuje bindDN, ktoré používa SSL na strane servera na naviazanie k serveru LDAP, ktorý obsahuje zoznamy zrušených certifikátov (CRL) pre validáciu certifikátov x.509v3 klienta. Tento parameter môže byť potrebný v prípade, ak pre validáciu CRL bolo poskytnuté ibm-slapdSslAuth=serverclientauth a certifikáty klienta.

Poznámka: Ak server LDAP, obsahujúci zoznamy CRL povoľuje neautentifikovaný prístup k zoznamom CRL (nazývaný anonymný prístup), nevyžaduje sa ibm-slapdLdapCrlUser.

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax DN

Maximálna dĺžka
1000

Hodnota
Jedna hodnota

ibm-slapdMasterDN

Opis Určuje DN pripojenia hlavného servera. Táto hodnota sa musí zhodovať s replicaBindDN v replicaObject definovanom pre hlavný server. Keď sa na autentifikáciu pre repliku používa Kerberos, ibm-slapdMasterDN musí určovať ID Kerberos v tvare DN (napríklad ibm-kn=freddy@realm1). Keď sa používa Kerberos, ignoruje sa MasterServerPW.

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax DN

Maximálna dĺžka
1000

Hodnota
Jedna hodnota

ibm-slapdMasterPW

Opis Určuje heslo pripojenia hlavného replikačného servera. Táto hodnota sa musí zhodovať s replicaBindDN v replicaObject definovanom pre hlavný server. Keď sa na autentifikáciu pre repliku používa Kerberos, ibm-slapdMasterDN musí určovať ID Kerberos v tvare DN (napríklad ibm-kn=freddy@realm1). Keď sa používa Kerberos, ignoruje sa MasterServerPW.

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax Binary

Maximálna dĺžka
128

Hodnota
Jedna hodnota

ibm-slapdMasterReferral

Opis Určuje URL hlavného replikačného servera. Napríklad:

```
ldap://master.us.ibm.com
```

Ak je bezpečnosť nastavená len na použitie SSL:

```
ldaps://master.us.ibm.com:636
```

Ak je bezpečnosť nastavená na none a používa sa neštandardný port:

```
ldap://master.us.ibm.com:1389
```

Predvolená hodnota
none

Syntax Reťazec adresára, nezohľadňujúci veľkosť písmen

Maximálna dĺžka
256

Hodnota
Jedna hodnota

ibm-slapdMaxEventsPerConnection

Opis Určuje maximálny počet notifikácií na udalosti, ktoré môžu byť zaregistrované pre pripojenie.

```
Minimum = 0
(neobmedzené)
Maximum = 2,147,483,647
```

Predvolená hodnota
100

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdMaxEventsTotal

Opis Určuje maximálny celkový počet notifikácií na udalosti, ktoré môžu byť zaregistrované pre všetky pripojenia.

```
Minimum = 0
(neobmedzené)
Maximum = 2,147,483,647
```

Predvolená hodnota
0

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdMaxNumOfTransactions

Opis Určuje maximálny počet transakcií pre server.

```
Minimum = 0
(neobmedzené)
Maximum = 2,147,483,647
```

Predvolená hodnota
20

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdMaxOpPerTransaction

Opis Určuje maximálny počet operácií pre transakciu.

```
Minimum = 0
(neobmedzené)
Maximum = 2,147,483,647
```

Predvolená hodnota
5

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdMaxPendingChangesDisplayed

Opis Maximálny počet čakajúcich zmien na zobrazenie.

Predvolená hodnota
200

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdMaxTimeLimitOfTransactions

Opis Určuje hodnotu maximálneho časového limitu nevybavenej transakcie v sekundách.

```
Minimum = 0
(neobmedzené)
Maximum = 2,147,483,647
```

Predvolená hodnota
300

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdPagedResAllowNonAdmin

Opis Určuje, či má server povoliť viazanie iné ako Administrátor pre požiadavky o stránkované výsledky v požiadavke o hľadanie. Ak hodnota prečítaná zo súboru ibmslapd.conf je FALSE, server spracuje len tie požiadavky klienta, ktoré predložil užívateľ s oprávnením administrátor. Ak klient požaduje stránkované výsledky pre operáciu vyhľadávania a nemá oprávnenie Administrátor a hodnota prečítaná zo súboru ibmslapd.conf pre tento atribút je FALSE, server vráti klientovi návratový kód insufficientAccessRights; nevykoná sa žiadne vyhľadávanie ani stránkovanie.

Predvolená hodnota
FALSE

Syntax Boolean

Dĺžka 5

Počet Jeden

Použitie
directoryOperation

Upraviteľné užívateľom
Áno

Trieda prístupu
kritická

Objectclass
ibm-slapdRdbmBackend

Vyžadované
Nie

ibm-slapdPagedResLmt

Opis Maximálny počet nevybavených požiadaviek o vyhľadávanie so stránkovanými výsledkami, ktoré môžu byť aktívne súčasne. Rozsah = 0.... Ak klient požiada o operáciu so stránkovanými výsledkami a je práve aktívny maximálny počet nevybavených stránkovaných výsledkov, server vráti klientovi návratový kód zaneprázdnený; nevykoná sa žiadne vyhľadávanie ani stránkovanie.

Predvolená hodnota
3

Syntax Integer

Dĺžka 11

Počet Jeden

Použitie
directoryOperation

Upraviteľné užívateľom
Áno

Trieda prístupu
kritická

Vyžadované
Nie

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPageSizeLmt

Opis Maximálny počet položiek na vrátenie z vyhľadávania pre jednu stranu, keď sa používajú stránkované výsledky, bez ohľadu na veľkosť strany, ktorá mohla byť zadaná v požiadavke klienta o vyhľadávanie. Rozsah = 0.... Ak klient poskytol veľkosť strany, použije sa menšia hodnota spomedzi hodnoty klienta a hodnoty prečítanej zo súboru ibmslapd.conf.

Predvolená hodnota
50

Syntax Integer

Dĺžka 11

Počet Jeden

Použitie
directoryOperation

Upraviteľné užívateľom
Áno

Trieda prístupu
kritická

Vyžadované
Nie

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPlugin

Opis Doplnkový komponent je dynamicky zavedená knižnica, ktorá rozširuje schopnosti servera. Atribút ibm-slapdPlugin hovorí serveru, ako má zaviesť a inicializovať knižnicu doplnkového komponentu. Syntax:

```
názov súbor kľúčových slov init_function [args...]
```

Syntax sa mierne odlišuje pre každú platformu kvôli názvovým konvenciám knižníc.

Väčšina doplnkových komponentov je voliteľná, ale doplnkový komponent ukončenia RDBM je vyžadovaný pre všetky ukončenia RDBM.

Predvolená hodnota
database /bin/libback-rdbm.dll rdbm_backend_init

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
2000

Hodnota
Viac hodnôt

ibm-slapdPort

Opis Určuje port TCP/IP, používaný pre pripojenia iné ako SSL. Nemôže mať rovnakú hodnotu ako ibm-slapdSecurePort. (Porty IP sú 16-bitové celé čísla bez znamienka, z rozsahu 1 - 65535.)

Predvolená hodnota
389

Syntax Integer

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdPWEncryption

Opis Určuje mechanizmus kódovania pre heslá užívateľov pred ich uložením do adresára. Musí byť zadaný ako none, imask, crypt alebo sha (ak chcete používať kódovanie SHA-1, musíte použiť kľúčové slovo **sha**). Pre viazania SASL a cram-md5 musí byť hodnota nastavená na none.

Predvolená hodnota
none

Syntax Reťazec adresára, nezohľadňujúci veľkosť písmen

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdReadOnly

Opis Tento atribút sa zvyčajne aplikuje len na ukončenie databázy. Určuje, či sa dá zapisovať do ukončenia. Musí byť zadaný ako TRUE alebo FALSE. Ak nie je zadaný, použije sa predvolená hodnota FALSE. Ak je nastavený na TRUE, server vráti LDAP_UNWILLING_TO_PERFORM (0x35) v odpovedi na každú požiadavku klienta, ktorá mení údaje v databáze readOnly.

Predvolená hodnota
FALSE

Syntax Boolean

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdReferral

Opis Určuje URL odvolávky LDAP na vrátenie, keď sa lokálne prípony nezhodujú s požiadavkou. Používa sa pre nadradenú odvolávku (prípona nie je v názvovom kontexte servera).

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
32700

Hodnota
Viac hodnôt

ibm-slapdReplDbConns

Opis Maximálny počet pripojení k databáze pre použitie replikáciou.

Predvolená hodnota
4

Syntax Integer

Maximálna dĺžka
11

Hodnota
Jedna hodnota

ibm-slapdReplicaSubtree

Opis Identifikuje DN replikovaného podstromu

Syntax DN

Maximálna dĺžka
1000

Hodnota
Jedna hodnota

ibm-slapdSchemaAdditions

Opis Atribút ibm-slapdSchemaAdditions sa používa na explicitnú identifikáciu súboru, ktorý obsahuje nové položky schémy. Predvolene to je /etc/V3.modifiedschema. Ak tento atribút nie je definovaný, server použije posledný súbor ibm-slapdIncludeSchema, ako v predošlých vydaniach.

Pred verziou 3.2, posledná položka includeSchema v **slapd.conf** bol súbor, do ktorého server pridával nové položky schémy, ak prijal požiadavku od klienta. Posledné includeSchema je zvyčajne súbor V3.modifiedschema, čo je prázdny súbor nainštalovaný práve na tento účel.

Poznámka: Názov modified je zavádzajúci, pretože súbor obsahuje len nové položky. Zmeny v existujúcich položkách schémy sa robia v ich originálnych súboroch.

Predvolená hodnota
/etc/V3.modifiedschema

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdSchemaCheck

Opis Určuje mechanizmus kontroly schémy pre operáciu pridania/modifikácie/vymazania. Musí byť zadaný ako V2, V3 alebo V3_lenient.

- V2 - Zachovať kontrolu v2 a v2.1. Odporúčané pre migráciu.
- V3 - Vykonať kontrolu v3.
- V3_lenient - Nie sú potrebné všetky rodičovské triedy objektov. Pri pridávaní položiek je potrebná len priama trieda objektov.

Predvolená hodnota
V3_lenient

Syntax Reťazec adresára, nezohľadňujúci veľkosť písmen

Maximálna dĺžka
10

Hodnota
Jedna hodnota

ibm-slapdSecurePort

Opis Určuje port TCP/IP, používaný pre pripojenia SSL. Nemôže mať rovnakú hodnotu ako ibm-slapdPort. (Porty IP sú 16-bitové celé čísla bez znamienka, z rozsahu 1 - 65535.)

Predvolená hodnota
636

Syntax Integer

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdSecurity

Opis Povoľuje pripojenia SSL a TLS. Musí byť žiadne, SSL, SSLOnly, TLS alebo SSLTLS.

- žiadne - server počúva len na nechránenom porte.
- SSL - server počúva na portoch SSL a tých, ktoré nie sú SSL. Použitie chráneného portu predstavuje jediný spôsob použitia bezpečného pripojenia.
- SSLOnly - server počúva len na porte SSL.
- TLS - server počúva len na nechránenom porte. Použitie rozšírenej prevádzky StartTLS predstavuje jediný spôsob používania bezpečného pripojenia.
- SSLTLS - server počúva na predvolenom aj chránenom porte. Na nadviazanie bezpečného pripojenia cez predvolený port sa môže použiť rozšírená operácia StartTLS alebo má klient možnosť využiť priamo chránený port. Ak pošlete StartTLS prostredníctvom chráneného portu, vráti sa správa LDAP_OPERATIONS_ERROR.

Predvolená hodnota
none

Syntax Reťazec adresára, nezohľadňujúci veľkosť písmen

Maximálna dĺžka
7

Hodnota
Jedna hodnota

ibm-slapdServerId

Opis Identifikuje server na použitie v replikácii.

Syntax Reťazec IA5, zohľadňujúci veľkosť písmen

Maximálna dĺžka
240

Hodnota
Jedna hodnota

ibm-slapdSetenv

Opis Aby sa mohlo zmeniť prevádzkové prostredie, server spustí **putenv()** pre všetky hodnoty ibm-slapdSetenv pri spustení. Premenné shellu (napríklad %PATH% alebo $LANG) sa nerozvíjajú.

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
2000

Hodnota
Viac hodnôt

ibm-slapdSizeLimit

Opis Určuje maximálny počet položiek na vrátenie z vyhľadávania, bez ohľadu na limit veľkosti, ktorý môže byť zadaný v požiadavke klienta o vyhľadávanie (Rozsah = 0...). Ak klient poskytol limit, použije sa menšia hodnota spomedzi hodnôt klienta a hodnoty prečítanej zo súboru **ibmslapd.conf**. Ak klient neposkytol limit a je naviazaný s DN administrátora, za limit sa považuje ″neobmedzené″. Ak klient neposkytol limit a nie je naviazaný s DN administrátora, ako limit sa použije hodnota prečítaná zo súboru **ibmslapd.conf**. 0 = neobmedzené.

Predvolená hodnota
500

Syntax Integer

Maximálna dĺžka
12

Hodnota
Jedna hodnota

ibm-slapdSortKeyLimit

Opis Maximálny počet podmienok zoradenia (kľúčov), ktorý je možné zadať v jednej požiadavke o vyhľadávanie. Rozsah = 0.... Ak klient zadal operáciu vyhľadávania s viac zoraďovacími kľúčmi ako dovoľuje limit a kritickosť riadenia vyhľadávania so zoradením je FALSE, server použije hodnotu prečítanú zo súboru ibmslapd.conf a inogruje všetky zoraďovacie kľúče nájdené po dosiahnutí limitu - vykoná sa vyhľadávanie a zoradenie. Ak klient zadal operáciu vyhľadávania s viacerými kľúčmi ako dovoľuje limit a kritickosť riadenia triedeného vyhľadávania je TRUE, server zašle klientovi správu **adminLimitExceeded** - vyhľadávanie alebo triedenie sa nezrealizuje.

Predvolená hodnota
3

Syntax cis

Dĺžka 11

Počet Jeden

Použitie
directoryOperation

Upraviteľné užívateľom
Yes

Trieda prístupu
kritická

Objectclass
ibm-slapdRdbmBackend

Vyžadované
Nie

ibm-slapdSortSrchAllowNonAdmin

Opis Určuje, či má server povoliť viazanie iné ako Administrátor pre požiadavky o zoradenie v požiadavke o hľadanie. Ak hodnota prečítaná zo súboru ibmslapd.conf je FALSE, server spracuje len tie požiadavky klienta, ktoré predložil užívateľ s oprávnením administrátor. Ak klient požaduje zoradenie pre operáciu vyhľadávania a nemá oprávnenie Administrátor a hodnota prečítaná zo súboru ibmslapd.conf pre tento atribút je FALSE, server vráti klientovi návratový kód insufficientAccessRights - nevykoná sa žiadne vyhľadávanie ani zoradenie.

Predvolená hodnota
FALSE

Syntax Boolean

Dĺžka 5

Počet Jeden

Použitie
directoryOperation

Upraviteľné užívateľom
Áno

Trieda prístupu
kritická

Objectclass
ibm-slapdRdbmBackend

Vyžadované
Nie

ibm-slapdSslAuth

Opis Určuje typ autentifikácie pre pripojenie ssl, buď serverauth, alebo serverclientauth.

- serverauth - podporuje autentifikáciu servera v klientovi. Toto je predvolené nastavenie.
- serverclientauth - podporuje autentifikáciu servera aj klienta.

Predvolená hodnota
serverauth

Syntax Reťazec adresára, nezohľadňujúci veľkosť písmen

Maximálna dĺžka
16

Hodnota
Jedna hodnota

ibm-slapdSslCertificate

Opis Určuje návestie, ktoré identifikuje osobný certifikát servera v databázovom súbore kľúčov. Toto návestie sa zadáva pri vytvorení súkromného kľúča a certifikátu servera aplikáciou **gsk4ikm**. Ak ibm-slapdSslCertificate nie je definované, server LDAP použije pre pripojenia SSL predvolený súkromný kľúč z databázového súboru kľúčov.

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
128

Hodnota
Jedna hodnota

ibm-slapdSslCipherSpec

Určuje metódu šifrovania SSL pre klientov pristupujúcich k serveru. Musí byť jedno z tohto:

Tabuľka 7. Metódy šifrovania SSL

Atribút	Úroveň šifrovania
TripleDES-168	Šifrovanie Triple DES so 168-bitovým kľúčom a SHA-1 MAC
DES-56	Šifrovanie DES s 56-bitovým kľúčom a SHA-1 MAC
RC4-128-SHA	Šifrovanie RC4 so 128-bitovým kľúčom a SHA-1 MAC
RC4-128-MD5	Šifrovanie RC4 so 128-bitovým kľúčom a MD5 MAC
RC2-40-MD5	Šifrovanie RC4 so 40-bitovým kľúčom a MD5 MAC
RC4-40-MD5	Šifrovanie RC4 so 40-bitovým kľúčom a MD5 MAC
AES	Šifrovanie AES

Syntax Reťazec IA5

Maximálna dĺžka
30

ibm-slapdSslKeyDatabase

Opis Určuje cestu k súboru pre databázový súbor kľúčov SSL servera LDAP. Tento databázový súbor kľúčov sa používa na obsluhu pripojení SSL od klientov LDAP, ako aj na vytváranie bezpečných pripojení SSL k replikačným serverom LDAP.

Predvolená hodnota
/etc/key.kdb

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdSslKeyDatabasePW

Opis Určuje heslo priradené k databázovému súboru kľúčov SSL servera LDAP, určenému parametrom ibm-slapdSslKeyDatabase. Ak má databázový súbor kľúčov servera LDAP priradený súbor hesiel, parameter ibm-slapdSslKeyDatabasePW môžete vynechať alebo nastaviť na none.

Poznámka: Súbor hesiel sa musí nachádzať v rovnakom adresári ako databázový súbor kľúčov a musí mať rovnaký názov ako databázový súbor kľúčov, ale s rozšírením .sth namiesto .kbd.

Predvolená hodnota
none

Syntax Binary

Maximálna dĺžka
128

Hodnota
Jedna hodnota

ibm-slapdSslKeyRingFile

Opis Cesta k databázovému súboru kľúčov SSL servera LDAP. Tento databázový súbor kľúčov sa používa na obsluhu pripojení SSL od klientov LDAP, ako aj na vytváranie bezpečných pripojení SSL k replikačným serverom LDAP.

Predvolená hodnota
key.kdb

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

ibm-slapdSuffix

Opis Určuje názvový kontext na uloženie v tomto ukončení.

Poznámka: Toto je rovnaký názov ako má trieda objektov.

Predvolená hodnota
Nie je definovaná žiadna predvolená hodnota.

Syntax DN

Maximálna dĺžka
1000

Hodnota
Viac hodnôt

ibm-slapdSupportedWebAdmVersion

Opis Tento atribút definuje najstaršiu verziu webového administratívneho nástroja, ktorá podporuje tento server cn=configuration.

Predvolená hodnota

Syntax Reťazec adresára

Maximálna dĺžka

Hodnota
Jedna hodnota

ibm-slapdSysLogLevel

Opis Určuje úroveň, na ktorej sa do súboru slapd.errors protokoluje štatistika ladenia a operácie. Musí byť určená ako l, m alebo h.

- h - vysoká úroveň (high), poskytuje najviac informácií
- m - stredná úroveň (medium), predvolená
- l - nízka úroveň (low), poskytuje najmenej informácií

Predvolená hodnota
m

Syntax Reťazec adresára, nezohľadňujúci veľkosť písmen

Maximálna dĺžka
1

Hodnota
Jedna hodnota

ibm-slapdTimeLimit

Opis Určuje maximálny počet sekúnd pre trvanie požiadavky o hľadanie, bez ohľadu na časový limit, ktorý môže byť zadaný v požiadavke klienta. Ak klient poskytol limit, použije sa menšia hodnota spomedzi hodnôt klienta a hodnoty prečítanej zo súboru **ibmslapd.conf**. Ak klient neposkytol limit a je naviazaný s DN administrátora, za limit sa považuje ″neobmedzené″. Ak klient neposkytol limit a nie je naviazaný s DN administrátora, ako limit sa použije hodnota prečítaná zo súboru **ibmslapd.conf**. 0 = neobmedzené.

Predvolená hodnota
900

Syntax Integer

Maximálna dĺžka

Hodnota
Jedna hodnota

ibm-slapdTransactionEnable

Opis Ak je zavedený doplnkový komponent transakcií, ale ibm-slapdTransactionEnable je nastavené na FALSE, server odmietne všetky požiadavky StartTransaction s odpoveďou LDAP_UNWILLING_TO_PERFORM.

Predvolená hodnota
TRUE

Syntax Boolean

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdUseProcessIdPw

Opis V prípade nastavenia na TRUE bude server ignorovať atribúty ibm-slapdDbUserID a ibm-slapdDbUserPW a použije na autentifikáciu do DB2 svoje vlastné povoľovacie údaje.

Predvolená hodnota
FALSE

Syntax Boolean

Maximálna dĺžka
5

Hodnota
Jedna hodnota

ibm-slapdVersion

Opis Číslo verzie IBM Slapd

Predvolená hodnota

Syntax Reťazec adresára, zohľadňujúci veľkosť písmen

Maximálna dĺžka

Hodnota
Jedna hodnota

ibm-slapdWriteTimeout

Opis Uvádza hodnotu uplynutia vyhradeného času v sekundách pre blokované zápisy. Po dosiahnutí limitu sa pripojenie preruší.

Predvolená hodnota
120

Syntax Integer

Maximálna dĺžka
1024

Hodnota
Jedna hodnota

objectClass

Opis Hodnoty atribútu objectClass opisujú druh objektu, ktorý reprezentuje položka.

Syntax Reťazec adresára

Maximálna dĺžka
128

Hodnota
Viac hodnôt

Identifikátory objektov (OID)

Identifikátory OID zobrazené v nasledujúcich tabuľkách sa používajú v adresárovom serveri. Tieto OID sa nachádzajú v kmeňovom DSE. Položka v kmeňovom DSE obsahuje informácie o samotnom serveri.

Kontroly

Tabuľka 8. Podporované ovládacie prvky adresárového servera

Názov	OID	Najstaršie vydanie alebo vydanie i5/OS či OS/400	Najstaršia verzia IBM Directory Server	Opis
Manage DSA IT	2.16.840.1.1137.30.3.4.2	V4R5	V3.2	Spracovať položky odvolávok ako normálne položky.
"Transakcie" na strane 46	1.3.18.0.2.10.5	V4R5	V3.2	Označiť operáciu ako súčasť transakcie.
os400-dltusrprf-ownobjopt	1.3.18.0.2.10.8	V5R2		Vymazať voľbu užívateľského profilu pre majiteľa objektu. Pozrite si detaily v časti "Projektované pozadie operačného systému" na strane 73.

Tabuľka 8. Podporované ovládacie prvky adresárového servera (pokračovanie)

Názov	OID	Najstaršie vydanie alebo vydanie i5/OS či OS/400	Najstaršia verzia IBM Directory Server	Opis
os400-dltusrprf-pgpopt	1.3.18.0.2.10.9	V5R2		Vymazať možnosť užívateľského profilu pre primárnu skupinu. Pozrite si detaily v časti "Projektované pozadie operačného systému" na strane 73.
Sorted search	1.2.840.113556.1.4.473 (požiadavka) a 1.2.840.113556.1.4.474 (odpoveď)	V5R2 s PTF	V4.1	Triediť výsledky vyhľadávania pred vrátením položiek klientovi.Pozrite si "Parametre vyhľadávania" na strane 42.
Paged search	1.2.840.113556.1.4.319	V5R2 s PTF	V4.1	Vrátiť klientovi výsledky vyhľadávania v stránkach namiesto všetkého naraz.Pozrite si "Parametre vyhľadávania" na strane 42.
Tree Delete control	1.2.840.113556.1.4.805	V5R3	V5.1	Táto kontrola je pripojená k požiadavke o vymazanie, aby hlásila že špecifikovaná položka a všetky podriadené položky budú vymazané. Užívateľ musí byť administrátor adresára. Položka na vymazanie nemôže byť kontextom replikácie.
"Politika hesiel" na strane 66	1.3.6.1.4.1.42.2.27.8.5.1	V5R3	V5.1	Vrátiť klientovi extra chybové informácie politiky hesiel.
Server administration	1.3.18.0.2.10.15	V5R3	V5.1	Umožniť administrátorovi vykonať opravné operácie, ktoré by normálne boli zamietnuté (napríklad: aktualizovať repliku určenú iba na čítanie, aktualizovať server v kľudovom stave alebo nastaviť určité prevádzkové atribúty).
"Autorizácia proxy" na strane 54	2.16.840.1.113730.3.4.18	V5R4	V5.2	Aplikácia klienta sa môže viazať na adresár so svojou vlastnou identitou, ale operácie môže vykonávať v mene inej.

Tabuľka 8. Podporované ovládacie prvky adresárového servera (pokračovanie)

Názov	OID	Najstaršie vydanie alebo vydanie i5/OS či OS/400	Najstaršia verzia IBM Directory Server	Opis
Ovládanie replikácie dodávateľských väzieb	1.3.18.0.2.10.18	V5R3	V5.2	Toto ovládanie pridal dodávateľ, ak dodávateľom je server gateway.

Rozšírené operácie

Tabuľka 9. Identifikátory OID pre rozšírené operácie

Názov	OID	Najstaršie vydanie i5/OS alebo OS/400	Najstaršia verzia IBM Directory Server	Opis
Register for events	1.3.18.0.2.12.1	V4R5	V3.2	Požadovať registráciu pre udalosti v SecureWay V3.2 Event Support
Unregister for events	1.3.18.0.2.12.3	V4R5	V3.2	Zrušiť registráciu udalostí registrovaných pre použitie Event Registration Request.
Begin transaction	1.3.18.0.2.12.5	V4R5	V3.2	Spustiť Transactional context pre SecureWay V3.2
End transaction	1.3.18.0.2.12.6	V4R5	V3.2	Ukončiť Transactional context (commit/rollback) pre SecureWay V3.2
DN normalize request	1.3.18.0.2.12.30	V5R3	V5.1	Požadovať normalizáciu DN alebo sekvencie DN.
StartTLS	1.3.6.1.4.1.1466.20037	V5R4	V5.2	Požadovať spustenie Transport Layer Security.

Sú definované dodatočné rozšírené operácie, ktoré nie sú určené na spúšťanie klientom. Tieto operácie sa používajú prostredníctvom pomocného programu ldapexop alebo operácií vykonaných pomocou nástroja správy webu. Tieto operácie a oprávnenia potrebné na ich spustenie, sú uvedené ďalej:

Tabuľka 10. Ďalšie rozšírené operácie

Názov	OID	Najstaršie vydanie i5/OS	Najstaršia verzia IBM Directory Server	Opis
Control replication	1.3.18.0.2.12.16	V5R3	V5.1	Táto operácia vykonáva požadovanú akciu na serveri, kde je spustená a postupne volá všetkých zákazníkov, ktorých má pod sebou v replikačnej topológii. Klient musí byť administrátorom adresára alebo musí mať oprávnenie na zápis do objektu ibm-replicagroup=default pre priradený replikačný kontext.

Tabuľka 10. Ďalšie rozšírené operácie (pokračovanie)

Názov	OID	Najstaršie vydanie i5/OS	Najstaršia verzia IBM Directory Server	Opis
Control replication queue	1.3.18.0.2.12.17	V5R3	V5.1	Táto operácia označuje položky ako už replikované pre špecifikovanú zmluvu. Táto operácia je povolená, len keď má klient oprávnenie na zápis do replikačnej zmluvy.
Quiesce or unquiesce	1.3.18.0.2.12.19	V5R3	V5.1	Táto operácia uvedie podstrom do stavu, kde nebude akceptovať aktualizáciu klienta (alebo ukončí tento stav), okrem tých z klientov, ktorí sú autentifikovaní ako administrátori adresára, kde sa vykonáva kontrola administrácie servera. Klient musí byť autentifikovaný ako administrátor adresára alebo musí mať oprávnenie na zápis do objektu ibm-replicagroup=default pre priradený replikačný kontext.
Cascading control replication	1.3.18.0.2.12.15	V5R3	V5.1	Táto operácia vykonáva požadovanú akciu na serveri, kde je spustená a postupne volá všetkých zákazníkov, ktorých má pod sebou v replikačnej topológii. Klient musí byť administrátorom adresára alebo musí mať oprávnenie na zápis do objektu ibm-replicagroup=default pre priradený replikačný kontext.
Update configuration	1.3.18.0.2.12.28	V5R3	V5.1	Táto operácia sa používa, aby server opakovane načítal špecifikované nastavenia zo svojej konfigurácie. Táto operácia je povolená, len keď je klient administrátorom adresára.
Kill Connection Request	1.3.18.0.2.12.35	V5R4	V5.2	Požiadavka zrušiť pripojenia na serveri.
Unique attribute request	1.3.18.0.2.12.44	V5R4	V5.2	Požiada server, aby vrátil zoznam všetkých nejedinečných hodnôt pre daný názov atribútu. Pozri “ldapexop” na strane 192 -op uniqueattr.
Attribute type request	1.3.18.0.2.12.46	V5R4	V5.2	Požiada server, aby vrátil zoznam názvov atribútov s určitou charakteristikou. Pozri “ldapexop” na strane 192 -op getattributes
Control server tracing	1.3.18.0.2.12.40	V5R3	V5.2	Aktivovať alebo deaktivovať sledovanie v IBM Directory Server.
User type request	1.3.18.0.2.12.37	V5R3	V5.2	Žiadosť o získanie typu viazaného užívateľa.

Podporované a povolené schopnosti

Nasledujúca tabuľka zobrazuje identifikátory OID pre podporované a povolené schopnosti. Pomocou týchto OID môžete zistiť, či daný server tieto funkcie podporuje.

Tabuľka 11. Identifikátory OID pre podporované a povolené schopnosti

Názov	OID	Opis
Rozšírený replikačný model	1.3.18.0.2.32.1	Identifikuje replikačný model zavedený v IBM Directory Server v5.1 vrátane podstromu a kaskádovej replikácie.
Kontrolný súčet položky	1.3.18.0.2.32.2	Znamená, že tento server podporuje vlastnosti ibm-entrychecksum a ibm-entrychecksumop.
UUID položky	1.3.18.0.2.32.3	Znamená, že tento server podporuje operačný atribút ibm-entryuuid.
Filter ACLs	1.3.18.0.2.32.4	Znamená, že tento server podporuje model ACL používajúci filtre IBM.
Heslová politika	1.3.18.0.2.32.5	Znamená, že tento server podporuje politiku hesiel
Triedenie podľa DN	1.3.18.0.2.32.6	Znamená, že tento server podporuje používanie atribútu ibm-slapdDn na triedenie podľa DN.
Delegovanie administratívnej skupiny	1.3.18.0.2.32.8	Server podporuje delegovanie administrácie servera na skupinu administrátorov zadaných v backende konfigurácie.
Odmietnutie servisnej prevencie	1.3.18.0.2.32.9	Server podporuje vlastnosť odmietnutia servisnej prevencie vrátane časových limitov na čítanie/zápis a núdzového vlákna.
Dynamické aktualizácie položiek a podstromov	1.3.18.0.2.32.15	Server podporuje dynamické konfiguračné aktualizácie na položkách a podstromoch
Voľba nepriameho aliasu	1.3.18.0.2.32.10	Server štandardne nepodporuje voľbu nepriamych aliasov
Limity vyhľadávania špecifické pre skupinu	1.3.18.0.2.32.17	Voľba Limity vyhľadávania špecifické pre skupinu podporuje limity rozšíreného vyhľadávania pre skupinu ľudí
Dynamické sledovanie	1.3.18.0.2.32.14	Server podporuje aktívne sledovanie pre server s rozšírenou prevádzkou LDAP.
Schopnosti TLS	1.3.18.0.2.32.28	Uvádza, že server je naozaj schopný vykonávať TLS.
Audit démona admin	1.3.18.0.2.32.11	Server podporuje audit démona admin.
Schopnosti Kerberos	1.3.18.0.2.32.30	Uvádza, že server je naozaj schopný vykonávať Kerberos.
Neblokujúca replikácia	1.3.18.0.2.32.29	Dodávateľ nie vždy zopakuje pokus zaslať aktualizáciu, ak príjemca ohlási chybu.
Operačné atribúty ibm-allMembers a ibm-allGroups	1.3.18.0.2.32.31	Backend podporuje statické, dynamické a vložené skupinové vyhľadávanie prostredníctvom operačných atribútov ibm-allMembers a ibm-allGroups. Člena statickej, dynamickej a/alebo vloženej skupiny možno získať vyhľadaním v operačnom atribúte ibm-allMembers. Statická, dynamická a/alebo vložená skupina, do ktorej patrí DN člena, možno získať vyhľadaním v operačnom atribúte ibm-allGroups.
Globálne jedinečné atribúty	1.3.18.0.2.32.16	Funkcia servera na vynútenie hodnôt globálne jedinečných atribútov.
Monitorovať počty operácií	1.3.18.0.2.32.24	Server monitoruje počty operácií pre iniciované a ukončené typy operácií.
Monitorovať protokolovacie počty	1.3.18.0.2.32.20	Server monitoruje protokolovacie počty pre správy pridané do súborov protokolu auditu, servera a CLI.
Monitorovať počty typov pripojenia	1.3.18.0.2.32.22	Server monitoruje počty typov pripojenia pre pripojenia SSL a TLS.
Monitorovať informácie o aktívnych pracovníkoch	1.3.18.0.2.32.21	Server monitoruje informácie pre aktívnych pracovníkov (cn=workers,cn=monitor).
Monitorovať informácie o pripojeniach	1.3.18.0.2.32.23	Server monitoruje informácie pre pripojenia podľa IP adresy, a nie podľa ID pripojenia (cn=connections, cn=monitor).

Tabuľka 11. Identifikátory OID pre podporované a povolené schopnosti (pokračovanie)

Názov	OID	Opis
Monitorovať informácie o sledovaní	1.3.18.0.2.32.25	Server monitoruje informácie o práve používaných voľbách sledovania.
Ukladanie atribútov do pamäte cache pre rozlíšenie vyhľadávacích filtrov	1.3.18.0.2.32.13	Server podporuje ukladanie atribútov do pamäte cache pre rozlíšenie vyhľadávacích filtrov.
Autorizácia proxy	1.3.18.0.2.32.27	Server podporuje autorizáciu proxy pre skupinu užívateľov.
Podpora voľby jazykových označení	1.3.6.1.4.1.4203.1.5.4	Znamená, že server podporuje jazykové označenia podľa definície v RFC 2596.
Položky protokolu zmien podľa maximálneho veku	1.3.18.0.2.32.19	Uvádza, že server je schopný uchovávať položky protokolu zmien podľa ich veku.
Podstrom replikácie IBMpolicies	1.3.18.0.2.32.18	Server podporuje replikáciu podstromu cn=IBMpolicies.
Podstromové vyhľadávanie na nulovej (NULL) báze	1.3.18.0.2.32.26	Server umožňuje podstromové vyhľadávanie na nulovej báze, ktoré prehľadáva celý DIT definovaný na serveri.
autonómne ukladanie atribútov do pamäte cache	1.3.18.0.2.32.50	Podporuje autonómne ukladanie atribútov do pamäte cache
ibm-entrychecksumop	1.3.18.0.2.32.56	Funkčnosť 6.0 IDS ibm-entrychecksumop

Identifikátory OID pre mechanizmy ACL

Nasledujúca tabuľka zobrazuje identifikátory OID pre mechanizmy ACL.

Tabuľka 12. OID pre ACL mechanizmy

Názov	OID	Opis
Model IBM SecureWay V3.2 ACL	1.3.18.0.2.26.2	Znamená, že server LDAP podporuje model IBM SecureWay V3.2 ACL
Mechanizmus ACL používajúci filter IBM	1.3.18.0.2.26.3	Znamená, že server LDAP podporuje zoznamy ACL používajúce filter IBM Directory Server v5.1.
Systémom obmedzená podpora ACL	1.3.18.0.2.26.4	Znamená, že server podporuje systémovú a obmedzenú prístupovú triedu v položkách ACL.

Kapitola 9. Odstraňovanie problémov adresárového servera

Nanešťastie aj spoľahlivé servery ako adresárový server majú niekedy problémy. Keď má váš adresárový server problémy, tieto informácie vám môžu pomôcť zistiť, kde je chyba a odstrániť ju.

Spätné kódy chýb LDAP sa nachádzajú v súbore ldap.h, ktorý je umiestnený na vašom systéme v QSYSINC/H.LDAP.

“Monitorovanie chýb a prístupu pomocou protokolu úloh adresárového servera” na strane 262
Keď dôjde vo vašom adresárovom serveri k chybe a chcete získať viac detailov, ďalšou akciou, ktorú môžete vykonať je zobrazenie protokolu úlohy QDIRSRV.

“Použitie TRCTCPAPP na pomoc pri vyhľadávaní problémov” na strane 262
Pre zopakovateľné chyby môžete pomocou príkazu TRCTCPAPP APP(*DIRSRV) (Trace TCP/IP Application) spustiť sledovanie chýb.

“Použitie voľby LDAP_OPT_DEBUG na sledovanie chýb” na strane 263
Sledovanie chýb klientov používajúcich rozhrania API LDAP C.

“Obvyklé chyby klienta LDAP” na strane 266
Poznanie príčin obvyklých problémov klientov LDAP vám pomôže vyriešiť problémy s vaším serverom.

“Chyby týkajúce sa politiky hesiel” na strane 268
Zapnutie heslovej politiky môže občas spôsobiť nečakané chyby.

“Odstraňovanie problémov QGLDCPYVL API” na strane 268
Použitie pomocného programu User Trace môže vysvetliť chybu alebo určiť, či je nutný servis.

Viac informácií o bežných problémoch adresárového servera nájdete na domovskej stránke adresárového servera (www.iseries.ibm.com/ldap).

Adresárový server používa niekoľko serverov SQL (Structured Query Language), ktoré sú úlohami iSeries QSQSRVR. Keď nastane chyba SQL, protokol úlohy QDIRSRV obyčajne obsahuje nasledujúcu správu:

```
Nastala chyba SQL -1
```

V týchto príkladoch vás bude protokol úlohy QDISRV odkazovať na protokoly úlohy servera SQL. V niektorých prípadoch však QDIRSRV nemusí obsahovať túto správu a odkaz, aj keď príčinou problému je server SQL. V týchto prípadoch vám pomôže, ak budete vedieť, ktoré úlohy serverov SQL spustil server, takže budete vedieť, v ktorých protokoloch úloh QSQSRVR máte hľadať ďalšie chyby.

Keď sa adresárový server spustí normálne, generuje správy podobné tejto:

```
                                                    Systém: MYISERIES
 Úloha . . :   QDIRSRV       Užívateľ . . :   QDIRSRV       Číslo .
. . :   174440

  >> CALL PGM(QSYS/QGLDSVR)
     Úloha 057448/QUSER/QSQSRVR používaná pre spracovanie v režime
SQL servera.
     Úloha 057340/QUSER/QSQSRVR používaná pre spracovanie v režime
SQL servera.
     Úloha 057448/QUSER/QSQSRVR používaná pre spracovanie v režime
SQL servera.
     Úloha 057166/QUSER/QSQSRVR používaná pre spracovanie v režime
```

```
SQL servera.
     Úloha 057279/QUSER/QSQSRVR používaná pre spracovanie v režime
   Úloha 057288/QUSER/QSQSRVR používaná na spracovanie režimu servera SQL.
     Adresárový server sa úspešne spustil.
```

Správy odkazujú na úlohy QSQSRVR, spustené pre server. Počet správ na vašom serveri sa môže líšiť v závislosti od konfigurácie a počtu úloh QSQSRVR potrebných na dokončenie spustenia servera.

Na stránke Vlastnosti **databázy/prípon** adresárových serverov v iSeries Navigator uvádzate celkový počet serverov SQL, ktoré používa adresárový server pre operácie adresára po spustení servera. Pre účely replikácie sa spustia ďalšie servery SQL.

Monitorovanie chýb a prístupu pomocou protokolu úloh adresárového servera

Zobrazenie protokolu úlohy pre váš adresárový server vás môže upozorniť na chyby a pomôcť vám pri monitorovaní prístupu k serveru. Protokol úlohy obsahuje:

- Správy o práci servera a všetkých problémoch v serveri, napríklad zlyhania úloh servera SQL alebo replikácie.
- Správy súvisiace s bezpečnosťou, týkajúce sa operácií klientov, napríklad nesprávne heslá.
- Správy poskytujúce detaily o chybách klientov, napríklad chýbajúce povinné atribúty.

Pokiaľ nevykonávate ladenie problémov klienta, nie je potrebné protokolovať jeho chyby. Protokolovanie chýb klienta môžete kontrolovať na záložke vlastností **Všeobecné** adresárového servera v iSeries Navigator.

Ak je server naštartovaný, prezrite si protokol úlohy QDIRSRV:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom myši na **IBM Directory Server** a vyberte **Úlohy servera.**.
5. Z menu **File** vyberte **Protokol úlohy**.

Ak je server zastavený, prezrite si protokol úlohy QDIRSRV:
1. V iSeries Navigator rozviňte **Základné operácie**.
2. Kliknite na **Výstup na tlačiareň**.
3. QDIRSRV sa objaví v stĺpci **Užívateľ** iSeries Navigators pravého panelu. Ak si chcete prezerať protokol úloh, kliknite dvakrát na **Qpjoblog** v tom istom riadku vľavo od QDIRSRV.

   Poznámka: iSeries Navigator môže byť nakonfigurované len na zobrazovanie spoolových súborov. Ak sa QDIRSRV na zozname neobjaví, kliknite na **Výstup tlačiarne** a potom si vyberte **Zahrnúť** z ponuky **Voľby**. V poli **Užívateľ** špecifikujte **Všetko** Potom kliknite na **OK**.

Poznámka: Adresárový server používa na vykonanie niektorých úloh iné systémové prostriedky. Ak chyba nastane na jednom z týchto prostriedkov, protokol úlohy označí, kde nájdete potrebné informácie. V niektorých prípadoch nemusí byť Adresárový server schopný určiť, kam sa pozrieť. V takýchto prípadoch si pozrite protokol úloh serverov SQL (Structured Query Language) a zistite, či sa problém týkal serverov SQL.

Použitie TRCTCPAPP na pomoc pri vyhľadávaní problémov

Váš server poskytuje sledovanie komunikácie a zhromažďuje údaje o komunikačnej linke, napríklad rozhranie LAN (local area network) alebo WAN (wide area network). Priemerný užívateľ nemusí rozumieť celému obsahu údajov sledovania. Tieto položky sledovania však môže použiť na to, aby určil, či sa skutočne bude konať výmena údajov medzi dvoma bodmi.

Príkaz TRCTCPAPP (Trace TCP/IP Application) s voľbou *DIRSRV vám môže v adresárovom serveri pomôcť pri hľadaní problémov klientov alebo aplikácií.

Viac detailných informácií o použití príkazu TRCTCPAPP s LDAP ako aj o obmedzeniach požadovaných oprávnení nájdete v časti Opis príkazu TRCTCPAPP (Trace TCP/IP Application).

Všeobecné informácie o používaní sledovania komunikácie nájdete v časti Sledovanie komunikácie.

Použitie voľby LDAP_OPT_DEBUG na sledovanie chýb

Na sledovanie problémov klientov používajúcich rozhrania API LDAP C môžete použiť voľbu LDAP_OPT_DEBUG rozhrania API **ldap_set_option()**. Voľba ladenia má nastavenie viacerých úrovní ladenia, ktoré môžete použiť na pomoc pri odstraňovaní problémov s týmito aplikáciami.

Nasleduje príklad povolenia klientskej voľby ladenia sledovania.

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

Iným spôsobom nastavenia úrovne ladenia je nakonfigurovať numerickú hodnotu premennej prostredia LDAP_DEBUG pre úlohu, v ktorej je spustená klientska aplikácia na rovnakú numerickú hodnotu, ktorou by debugvalue bola, ak by sa použilo API **ldap_set_option()** .

Nasleduje príklad povolenia sledovania klienta pomocou premennej prostredia LDAP_DEBUG:

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

Po spustení klienta, ktorý spôsobuje váš problém, napíšte do iSeries tento text:

```
DMPUSRTRC ClientJobNumber
```

kde ClientJobNumber je číslo úlohy klienta.

Na interaktívne zobrazenie týchto informácií, napíšte do iSeries tento text:

```
DSPPFM QAP0ZDMP QP0Znnnnnn
```

, kde QAP0ZDMP obsahuje nulu a nnnnnn je číslo úlohy.

Ak chcete uložiť tieto informácie s cieľom odoslať ich do servisu, postupujte takto:

1. Pomocou príkazu CRTSAVF (Create SAVF) vytvorte súbor SAVF.
2. Do príkazovej výzvy iSeries napíšte nasledujúce:

   ```
   SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
   ```

   , kde QAP0ZDMP obsahuje nulu a *xxx* je názov, ktorý ste zadali pre súbor SAVF.

Identifikátory správ GLEnnnn

Identifikátory správ majú tvar GLEnnnn, kde nnnn je číslo decimálnej chyby. Napríklad opis návratového kódu 50 (0x32) si možno prezerať zadaním príkazu:

```
DSPMSGD MSGID(GLE0050) MSGF(QGLDMSG)
```

Uvedené poskytuje opis pre LDAP_INSUFFICIENT_ACCESS.

Nasledujúca tabuľka zobrazuje identifikátory správ GLE a ich opisy.

Identifikátor správy	Opis
GLE0000	Žiadosť bola úspešná (LDAP_SUCCESS)
GLE0001	Chyba operácie (LDAP_OPERATIONS_ERROR)
GLE0002	Chyba protokolu (LDAP_PROTOCOL_ERROR)
GLE0003	Prekročený časový limit (LDAP_TIMELIMIT_EXCEEDED)
GLE0004	Prekročený limit veľkosti (LDAP_SIZELIMIT_EXCEEDED)
GLE0005	Porovnávaný typ a hodnota neexistujú v položke (LDAP_COMPARE_FALSE)
GLE0006	Porovnávaný typ a hodnota existujú v položke (LDAP_COMPARE_TRUE)
GLE0007	Nepodporovaná metóda autentifikácie (LDAP_AUTH_METHOD_NOT_SUPPORTED)
GLE0008	Vyžaduje sa silná autentifikácia (LDAP_STRONG_AUTH_REQUIRED)
GLE0009	Prijaté boli čiastkové výsledky a odkaz (LDAP_PARTIAL_RESULTS)
GLE0010	Vrátený odkaz (LDAP_REFERRAL)
GLE0011	Prekročený administratívny limit (LDAP_ADMIN_LIMIT_EXCEEDED)
GLE0012	Nepodporované kritické rozšírenie (LDAP_UNAVAILABLE_CRITICAL_EXTENSION)
GLE0013	Vyžaduje sa dôvernosť (LDAP_CONFIDENTIALITY_REQUIRED)
GLE0014	Prebieha vytváranie väzby SASL (LDAP_SASLBIND_IN_PROGRESS)
GLE0016	Neexistujúci atribút (LDAP_NO_SUCH_ATTRIBUTE)
GLE0017	Nedefinovaný typ atribútu (LDAP_UNDEFINED_TYPE)
GLE0018	Nevhodné porovnávanie (LDAP_INAPPROPRIATE_MATCHING)
GLE0019	Porušenie obmedzenia (LDAP_CONSTRAINT_VIOLATION)
GLE0020	Typ alebo hodnota existuje (LDAP_TYPE_OR_VALUE_EXISTS)
GLE0021	Neplatná syntax (LDAP_INVALID_SYNTAX)
GLE0032	Neexistujúci objekt (LDAP_NO_SUCH_OBJECT)
GLE0033	Problém aliasu (LDAP_ALIAS_PROBLEM)
GLE0034	Neplatná syntax DN (LDAP_INVALID_DN_SYNTAX)
GLE0035	Objektom je list (LDAP_IS_LEAF)
GLE0036	Problém nepriameho odkazu na alias (LDAP_ALIAS_DEREF_PROBLEM)
GLE0048	Nevhodná autentifikácia (LDAP_INAPPROPRIATE_AUTH)
GLE0049	Neplatné povoľovacie údaje (LDAP_INVALID_CREDENTIALS)
GLE0050	Nedostatočný prístup (LDAP_INSUFFICIENT_ACCESS)
GLE0051	Adresárový server je zaneprázdnený (LDAP_BUSY)

Identifikátor správy	Opis
GLE0052	Agent adresárových služieb je nedostupný (LDAP_UNAVAILABLE)
GLE0053	Adresárový server odmieta vykonať požadovanú operáciu (LDAP_UNWILLING_TO_PERFORM)
GLE0054	Bola zistená slučka (LDAP_LOOP_DETECT)
LE0064	Porušenie pomenúvania (LDAP_NAMING_VIOLATION)
LE0065	Porušenie triedy objektu (LDAP_OBJECT_CLASS_VIOLATION)
GLE0066	Operácia nie je povolená v nelistovej položke (LDAP_NOT_ALLOWED_ON_NONLEAF)
GLE0067	Nepovolená operácia pre relatívny charakteristický názov (LDAP_NOT_ALLOWED_ON_RDN)
GLE0068	Už existuje (LDAP_ALREADY_EXISTS)
GLE0069	Triedu objektu nemožno zmeniť (LDAP_NO_OBJECT_CLASS_MODS)
GLE0070	Výsledky sú príliš veľké (LDAP_RESULTS_TOO_LARGE)
GLE0071	Ovplyvňuje viacero serverov. (LDAP_AFFECTS_MULTIPLE_DSAS)
GLE0080	Neznáma chyba (LDAP_OTHER)
GLE0081	LDAP server nemožno kontaktovať (LDAP_SERVER_DOWN)
GLE0082	Lokálna chyba (LDAP_LOCAL_ERROR)
GLE0083	Chyba kódovania (LDAP_ENCODING_ERROR)
GLE0084	Chyba dekódovania (LDAP_DECODING_ERROR)
GLE0085	Uplynul stanovený čas požiadavky (LDAP_TIMEOUT)
GLE0086	Neznáma metóda autentifikácie (LDAP_AUTH_UNKNOWN)
GLE0087	Nesprávny vyhľadávací filter (LDAP_FILTER_ERROR)
GLE0088	Užívateľ zrušil operáciu (LDAP_USER_CANCELLED)
GLE0089	Nesprávny parameter pre rutinu LDAP (LDAP_PARAM_ERROR)
GLE0090	Nedostatok pamäte (LDAP_NO_MEMORY)
GLE0091	Chyba pripojenia (LDAP_CONNECT_ERROR)
GLE0092	Vlastnosť nie je podporovaná (LDAP_NOT_SUPPORTED)
GLE0093	Nenašiel sa ovládač (LDAP_CONTROL_NOT_FOUND)
GLE0094	Nevrátili sa žiadne výsledky (LDAP_NO_RESULTS_RETURNED)
GLE0095	Vrátiť sa má viac výsledkov (LDAP_MORE_RESULTS_TO_RETURN)
GLE0096	URL nepatrí do LDAP (LDAP_URL_ERR_NOTLDAP)
GLE0097	URL nemá žiadne DN (LDAP_URL_ERR_NODN)
GLE0098	Hodnota rozsahu URL je neplatná (LDAP_URL_ERR_BADSCOPE)
GLE0099	Chyba alokácie pamäte (LDAP_URL_ERR_MEM)
GLE0100	Slučka u klienta (LDAP_CLIENT_LOOP)

Identifikátor správy	Opis
GLE0101	Prekročený limit odkazov (LDAP_REFERRAL_LIMIT_EXCEEDED)
GLE0112	Prostredie SSL už bolo inicializované (LDAP_SSL_ALREADY_INITIALIZED)
GLE0113	Inicializačné volanie zlyhalo (LDAP_SSL_INITIALIZE_FAILED)
GLE0114	Prostredie SSL nebolo inicializované (LDAP_SSL_CLIENT_INIT_NOT_CALLED)
GLE0115	Zadali ste neplatnú hodnotu parametra SSL (LDAP_SSL_PARAM_ERROR)
GLE0116	Dohodnutie bezpečného pripojenia bolo neúspešné (LDAP_SSL_HANDSHAKE_FAILED)
GLE0118	Knižnicu SSL nemožno lokalizovať (LDAP_SSL_NOT_AVAILABLE)
GLE0128	Nenašiel sa konkrétny vlastník (LDAP_NO_EXPLICIT_OWNER)
GLE0129	Nemožno získať zámok na požadovaný prostriedok (LDAP_NO_LOCK)
GLE0133	V DNS sa nenašli žiadne servery LDAP (LDAP_DNS_NO_SERVERS)
GLE0134	Skrátené výsledky DNS (LDAP_DNS_TRUNCATED)
GLE0135	Údaje DNS nemožno analyzovať (LDAP_DNS_INVALID_DATA)
GLE0136	Doménu alebo názvový server nemožno rozlíšiť (LDAP_DNS_RESOLVE_ERROR)
GLE0137	Chyba konfiguračného súboru DNS (LDAP_DNS_CONF_FILE_ERROR)
GLE0160	Pretečenie výstupu vo vyrovnávacej pamäti (LDAP_XLATE_E2BIG)
GLE0161	Vstup do vyrovnávacej pamäte bol skrátený (LDAP_XLATE_EINVAL)
GLE0162	Nepoužiteľný vstupný znak (LDAP_XLATE_EILSEQ)
GLE0163	Znak nemapuje do bodu kódovej sady (LDAP_XLATE_NO_ENTRY)

Obvyklé chyby klienta LDAP

Poznanie príčin obvyklých problémov klientov LDAP vám pomôže vyriešiť problémy s vaším serverom. Úplný zoznam chybových stavov klientov LDAP nájdete v téme “Rozhrania API adresárového servera” pod časťou Programovanie v iSeries Information Center.

Chybové správy klienta majú nasledujúci formát:

```
[Zlyhanie operácie LDAP]:[chybový stav API klienta LDAP]
```

Poznámka: Z vysvetlenia týchto chýb vyplýva, že klient komunikuje so serverom LDAP na i5/OS. Klient komunikujúci so serverom na inej platforme sa môže stretnúť s podobnými chybami, ale príčiny a ich náprava budú pravdepodobne odlišné.

Bežné správy majú nasledujúci obsah:

- “ldap_search: Timelimit exceeded”
- “[Failing LDAP operation]: Operations error”
- “ldap_bind: No such object”
- “ldap_bind: Inappropriate authentication”
- “[Failing LDAP operation]: Insufficient access”
- “[Failing LDAP operation]: Cannot contact LDAP server”
- “[Failing LDAP operation]: Failed to connect to SSL server” na strane 268

ldap_search: Timelimit exceeded

Táto chyba nastane pri pomalom vykonávaní Idapsearch. Môžete ju opraviť týmito činnosťami:

- Zvýšte časový limit hľadania pre adresárový server. Viac informácie nájdete v časti “Úprava nastavení výkonu” na strane 124.
- Znížte aktivitu na vašom systéme. Môžete znížiť aj počet aktívnych spustených úloh klienta LDAP.

[Failing LDAP operation]: Operations error

Túto chybu môže spôsobiť viacero príčin. Ak chcete získať informácie o príčine tejto chyby pre konkrétny prípad, pozrite si protokoly úlohy QDIRSRV (ako je opísané v časti “Monitorovanie chýb a prístupu pomocou protokolu úloh adresárového servera” na strane 262) a protokoly úlohy servera SQL (Structured Query Language) (ako je opísané v časti Kapitola 9, “Odstraňovanie problémov adresárového servera”, na strane 261).

ldap_bind: No such object

Bežnou príčinou tejto chyby je, že keď užívateľ vykonáva operáciu, urobí chybu pri písaní. Ďalšou bežnou príčinou býva, keď sa klient LDAP pokúsi o väzbu s DN, ktorý neexistuje, čo sa často stáva, keď užívateľ zadá čosi, o čom sa chybne domnieva, že ide o administrátora DN. Užívateľ môže napríklad zadať QSECOFR alebo Administrator, keď aktuálny DN administrátora môže byť podobný cn=Administrator.

Detaily o tejto chybe nájdete v protokole úlohy QDIRSRV, ako je opísané v časti “Monitorovanie chýb a prístupu pomocou protokolu úloh adresárového servera” na strane 262.

ldap_bind: Inappropriate authentication

Keď je heslo alebo DN vytvorenia väzby nesprávny, server vráti neplatné oprávnenia. Server vracia nevhodnú autentifikáciu, keď sa klient pokúša vytvoriť väzbu buď ako:

- Položka, ktorá nemá atribút userpassword
- Položka reprezentujúca užívateľa i5/OS s atribútom UID a bez atribútu userpassword. Zapríčiní to porovnávanie medzi zadaným heslom a heslom užívateľa i5/OS, ktoré sa nezhodujú.
- Položka, ktorá predstavuje projektovaného užívateľa a inú metódu pripojenia, než bola požadovaná.

Táto chyba sa vyskytne vtedy, keď sa klient pokúša pripojiť použitím hesla, ktoré nie je platné. Ak potrebujete informácie o tejto chybe, pozrite sa do protokolu úlohy QDIRSRV, ako je opísané v časti “Monitorovanie chýb a prístupu pomocou protokolu úloh adresárového servera” na strane 262.

[Failing LDAP operation]: Insufficient access

Táto chyba sa zvyčajne vyskytne vtedy, keď pripájané DN nemá oprávnenie na vykonanie operácie (napríklad pridať alebo vymazať), ktorú klient požaduje. Ak potrebujete informáciu o tejto chybe, pozrite sa do protokolu úlohy QDIRSRV, ako sa uvádza v časti “Monitorovanie chýb a prístupu pomocou protokolu úloh adresárového servera” na strane 262.

[Failing LDAP operation]: Cannot contact LDAP server

Najčastejšie príčiny tejto chyby sú nasledujúce:

- LDAP klient zadá požiadavku predtým, než je server LDAP na danom systéme pripravený a v režime očakávania výberov.
- Užívateľ špecifikuje číslo portu, ktoré je neplatné. Napríklad: server je pripravený na porte 386, ale požiadavka klienta smeruje na port 387.

Ak potrebujete informáciu o tejto chybe, pozrite sa do protokolu úlohy QDIRSRV, ako sa uvádza v časti “Monitorovanie chýb a prístupu pomocou protokolu úloh adresárového servera” na strane 262. Ak sa adresárový server úspešne spustil, v protokole úlohy QDIRSRV bude správa Adresárový server sa úspešne spustil.

[Failing LDAP operation]: Failed to connect to SSL server

Táto chyba sa vyskytuje vtedy, keď server LDAP odmietne spojenie s klientom preto, lebo sa nedá nastaviť zásuvka bezpečného spojenia. Môže to byť spôsobené jednou z nasledujúcich príčin:

- Podpora riadenia certifikátov odmietne pokus klienta o pripojenie sa k serveru. Pomocou Správcu digitálnych certifikátov skontrolujte, že sú vaše certifikáty správne nastavené, potom reštartujte server a zopakujte požiadavku.
- Užívateľ možno neprečítal prístup do skladu certifikátov *SYSTEM (štandardne /QIBM/userdata/ICSS/Cert/Server/default.kdb).

Pre aplikácie i5/OS C sú k dispozícii ďalšie informácie o chybe SSL. Detaily nájdete v časti “Rozhrania API adresárového servera” v téme Programovanie.

Chyby týkajúce sa politiky hesiel

Povolenie určitých politík hesiel môže spôsobiť neobvyklé zlyhania. V nasledujúcej časti nájdete pomoc pri odstraňovaní chýb týkajúcich sa politiky hesiel.

Vytvorenie väzby so správnym heslom zlyháva s ″neplatnými povoľovacími údajmi″: Heslu mohla skončiť platnosť alebo mohlo byť zamknuté konto. Pozrite si atribúty pwdchangedtime a pwdaccountlockedtime položky podľa opisu v “Tipy pre politiku hesiel” na strane 147.

Požiadavky boli neúspešné s ″neochotou vykonať″ po úspešnom vytvorení väzieb: Heslo mohlo byť resetované. V takom prípade bude vytvorenie väzby úspešné, ale jedinou operáciou, ktorú server užívateľovi povolí, bude zmeniť jeho heslo. Ostatné požiadavky budú až do zmeny hesla neúspešné s ″neochotou vykonať″.

Autentifikácia s resetovaným heslom má neočakávané správanie: Ak bolo heslo resetované, požiadavka na vytvorenie väzby bude podľa vyššie uvedeného opisu úspešná. Znamená to, že užívateľ sa snáď bude môcť autentifikovať natrvalo pomocou resetovaného hesla.

Odstraňovanie problémov QGLDCPYVL API

Rozhranie API používa zariadenie User Trace na zaznamenanie svojej prevádzky. Ak sa vyskytnú chyby alebo vznikne podozrenie, sledovanie môže vysvetliť zrejmú chybu alebo určiť, či je potrebný servis. Sledovanie možno získať takto:

```
STRTRC SSNID(COPYVLDL) JOBTRCTYPE(*TRCTYPE) TRCTYPE((*DIRSRV *INFO))
CALL QGLDCPYVL PARM(...)
ENDTRC SSNID(COPYVLDL) DTALIB(QTEMP) PRTTRC(*YES)
```

Ak chcete uložiť tieto informácie s cieľom odoslať ich do servisu, postupujte takto:

1. Pomocou príkazu CRTSAVF (Create SAVF) vytvorte súbor SAVF.
2. Do príkazovej výzvy iSeries napíšte nasledujúce:

   SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(*xxx*)

   , kde QAP0ZDMP obsahuje nulu a *xxx* je názov, ktorý ste zadali pre súbor SAVF.

Kapitola 10. Súvisiace informácie

Dole sú uvedené dokumenty Témy IBM Redbooks (vo formáte PDF), webových stránok a informačného centra týkajúce sa témy adresárového servera. Každý dokument typu PDF môžete vytlačiť.

Redbooks (www.redbooks.ibm.com)

- Understanding LDAP, SG24-4986 .
- Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino, SG24-6163 .
- Implementation and Practical Use of LDAP on the iSeries Server, SG24-6193 .

Webové lokality

- IBM Directory Server for iSeries Web site (www.ibm.com/servers/eserver/iseries/ldap)
- The Java Naming and Directory Interface (JNDI) Tutorial Web site (java.sun.com/products/jndi/tutorial/)

Ostatné informácie

“API adresárového servera” v kategórii Programovanie.

Príloha. Poznámky

Tieto informácie boli vyvinuté pre produkty a služby ponúkané v USA.

Spoločnosť IBM nemusí v iných krajinách ponúkať produkty, služby alebo vlastnosti preberané v tomto dokumente. Informácie o produktoch a službách momentálne ponúkaných vo vašej krajine poskytuje miestny zástupca spoločnosti IBM. Odkazy na produkty, programy alebo služby spoločnosti IBM neznamenajú ani nenaznačujú, že tieto sú jediné, ktoré možno použiť. Namiesto nich možno použiť ľubovoľné, funkčne ekvivalentné produkty, programy alebo služby, ktoré neporušujú duševné vlastníctvo spoločnosti IBM. Vyhodnotenie a kontrola činnosti produktu, programu alebo služby inej ako od IBM je však na zodpovednosti užívateľa.

Spoločnosť IBM môže vlastniť patenty alebo nevybavené žiadosti o patenty zaoberajúce sa predmetnou záležitosťou opisovanou v tomto dokumente. Predloženie tohto dokumentu vám neudeľuje žiadni licenciu na tieto patenty. Žiadosti o licencie môžete zasielať písomne na:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

V prípade otázok na licencie týkajúcich sa dvojbajtových informácií (DBCS), kontaktujte Oddelenie duševného vlastníctva spoločnosti IBM vo vašej krajine alebo ich zašlite písomne na adresu:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Nasledujúci odsek sa netýka Veľkej Británie ani žiadnej inej krajiny, kde sú takéto vyhlásenia nezlučiteľné s lokálnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU "TAK AKO JE" BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO MLČKY PREDPOKLADANEJ, VRÁTANE (ALE NEOBMEDZENE) MLČKY PREDPOKLADANÝCH ZÁRUK NEPOŠKODENIA, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. Niektoré štáty nedovoľujú zrieknutie sa vyjadrených alebo mlčky predpokladaných záruk v určitých transakciách, preto sa vás toto vyhlásenie nemusí týkať.

Tieto informácie môžu obsahovať technické nepresnosti alebo typografické chyby. Tieto informácie sa periodicky menia; tieto zmeny budú začlenené do nových vydaní publikácie. Spoločnosť IBM môže kedykoľvek a bez oznámenia vykonať zlepšenia a/alebo zmeny v produkte(och) a/alebo programe(och) opisovaných v tejto publikácii.

Všetky odkazy v týchto informáciách na webové lokality iné ako od IBM sú poskytnuté len pre pohodlie a v žiadnom prípade neslúžia ako potvrdenie obsahu týchto webových lokalít. Materiály na uvedených webových stránkach nie sú súčasťou dokumentácie pre tento produkt IBM a riziko za ich používanie znáša zákazník.

Spoločnosť IBM môže použiť alebo distribuovať informácie poskytnuté zákazníkom ľubovoľným a vhodným spôsobom bez toho, aby jej voči zákazníkovi vznikol nejaký záväzok.

Vlastníci licencií na tento program, ktorí chcú o ňom získať informácie za účelom povolenia: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (vrátane tohto) a (ii) vzájomného použitia vymieňaných informácií by mali kontaktovať:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Takéto informácie môžu byť dostupné, môžu byť predmetom príslušných pojmov a podmienok a v niektorých prípadoch sú dostupné za poplatok.

Spoločnosť IBM poskytuje licenčný program opisovaný v týchto informáciách a všetky príslušné licenčné materiály na základe podmienok Zákazníckej zmluvy IBM, Medzinárodnej programovej licenčnej zmluvy IBM, Licenčnej zmluvy IBM pre strojový kód alebo ľubovoľnej rovnocennej zmluvy medzi oboma zmluvnými stranami.

Všetky údaje o výkone, uvádzané v tomto dokumente boli získané v riadenom prostredí. Výsledky získané v iných prevádzkových prostrediach sa môžu podstatne odlišovať. Niektoré merania boli vykonané v systémoch vývojovej úrovne a nie je žiadna záruka, že tieto merania budú rovnaké vo všeobecne dostupných systémoch. Okrem toho, niektoré výsledky boli odhadnuté extrapoláciou. Skutočné výsledky sa môžu odlišovať. Užívatelia tohto dokumentu by si mali overiť použiteľnosť týchto údajov pre svoje špecifické prostredie.

Informácie o produktoch iných ako od IBM boli získané od poskytovateľov týchto produktov, z ich zverejnených oznámení alebo z iných, verejne dostupných zdrojov. Spoločnosť IBM tieto produkty neodskúšala a nemôže potvrdiť presnosť výkonu, kompatibilitu alebo iné požiadavky týkajúce sa produktov nepochádzajúcich od IBM. Otázky k schopnostiam produktov iných ako od IBM by ste mali adresovať poskytovateľom týchto produktov.

Všetky vyhlásenia týkajúce sa budúceho smerovania alebo úmyslov IBM sú predmetom zmeny alebo zrušenia bez ohlásenia a vyjadrujú len zámery a ciele.

Všetky ceny uvedené spoločnosťou IBM sú momentálne platnými odporúčanými maloobchodnými cenami IBM a tieto sa môžu bez oznámenia zmeniť. Dílerské ceny sa môžu líšiť.

Tieto informácie sú len pre účely plánovania. Tu uvedené informácie sú predmetom zmeny, predtým ako budú opisované produkty dostupné.

Tieto informácie obsahujú príklady údajov a hlásení používaných v každodenných firemných operáciách. Kvôli ich čo najlepšej ilustrácii obsahujú tieto príklady mená osôb, názvy spoločností, pobočiek a produktov. Všetky tieto mená a názvy sú vymyslené a akákoľvek podobnosť s menami, názvami a adresami používanými skutočnými osobami a spoločnosťami je čisto náhodná.

LICENCIA AUTORSKÝCH PRÁV:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom jazyku, ktoré ilustrujú programovacie techniky na rôznych operačných platformách. Zákazník môže tieto vzorové programy kopírovať, modifikovať a distribuovať v ľubovoľnej forme bez poplatku spoločnosti IBM na účely vývoja, použitia, marketingu alebo distribúcie aplikačných programov vyhovujúcich aplikačnému programovému rozhraniu pre operačnú platformu, pre ktorú boli vzorové programy napísané. Tieto príklady neboli dôkladne testované pre všetky podmienky. Spoločnosť IBM preto nemôže zaručiť ani predpokladať ich spoľahlivosť, použiteľnosť alebo funkčnosť.

Ak si prezeráte elektronickú kópiu týchto informácií, nemusia byť zobrazené fotografie ani farebné ilustrácie.

Ochranné známky

Nasledujúce pojmy sú ochranné známky spoločnosti International Business Machines v USA alebo v iných krajinách:

Application System/400
AS/400
DB2
e(logo)server
eServer
i5/OS

IBM
iSeries
Lotus
Lotus Notes
Operating System/400
OS/400
Redbooks
SecureWay
WebSphere
400

Microsoft, Windows, Windows NT a logo Windows sú ochranné známky spoločnosti Microsoft Corporation v Spojených štátoch alebo iných krajinách.

Java a všetky ochranné známky založené na Java, sú ochranné známky spoločnosti Sun Microsystems, Inc. v Spojených štátoch alebo iných krajinách.

UNIX je registrovaná ochranná známka spoločnosti The Open Group v Spojených štátoch a iných krajinách.

Názvy iných spoločností, produktov a služieb môžu byť obchodnými alebo servisnými značkami iných subjektov.

Podmienky

Povolenie na používanie týchto publikácií sa udeľuje za týchto podmienok.

Osobné použitie: Zákazník smie reprodukovať tieto publikácie na svoje osobné, nekomerčné použitie za predpokladu zachovania všetkých oznamov o vlastníctve. Bez výslovného súhlasu spoločnosti IBM nesmie zákazník distribuovať, zobrazovať ani vytvárať odvodené práce z týchto publikácií ani žiadnej ich časti.

Komerčné použitie: Zákazník smie reprodukovať, distribuovať a zobrazovať tieto publikácie výlučne len vo svojom podniku a za predpokladu zachovania všetkých oznamov o vlastníctve. Bez výslovného súhlasu spoločnosti IBM nesmie zákazník vytvárať odvodené práce z týchto publikácií ani reprodukovať, distribuovať, či zobrazovať tieto publikácie ani žiadne ich časti mimo svojho podniku.

S výnimkou toho, čo sa výslovne udeľuje týmto povolením, sa na publikácie ani informácie, údaje, softvér alebo iné duševné vlastníctvo, ktoré sa v nich nachádza, neudeľujú žiadne iné povolenia, licencie ani práva, či už vyjadrené alebo predpokladané .

Spoločnosť IBM si vyhradzuje právo odňať povolenia udelené týmto dokumentom vždy, keď usúdi, že používanie publikácií škodí jej záujmom alebo sa podľa nej nedodržiavajú vyššie uvedené pokyny.

Stiahnuť, exportovať a re-exportovať môžete tieto informácie len v tom prípade, ak vyhovujú všetkým platným zákonom a predpisom, vrátane zákonov a predpisov USA týkajúcich sa exportu.

SPOLOČNOŤ IBM NEPOSKYTUJE ŽIADNE ZÁRUKY TÝKAJÚCE SA OBSAHU TÝCHTO PUBLIKÁCIÍ, KTORÉ SA POSKYTUJÚ ″TAK AKO SÚ″ BEZ ZÁRUK AKÉHOKOĽVEK DRUHU, ČI UŽ VYJADRENÝCH ALEBO MLČKY PREDPOKLADANÝCH, VRÁTANE, AVŠAK BEZ OBMEDZENIA LEN NA ZÁRUKY PREDAJNOSTI, DODRŽIAVANIA AUTORSKÝCH PRÁV A VHODNOSTI NA URČITÝ ÚČEL.

Vytlačené v USA