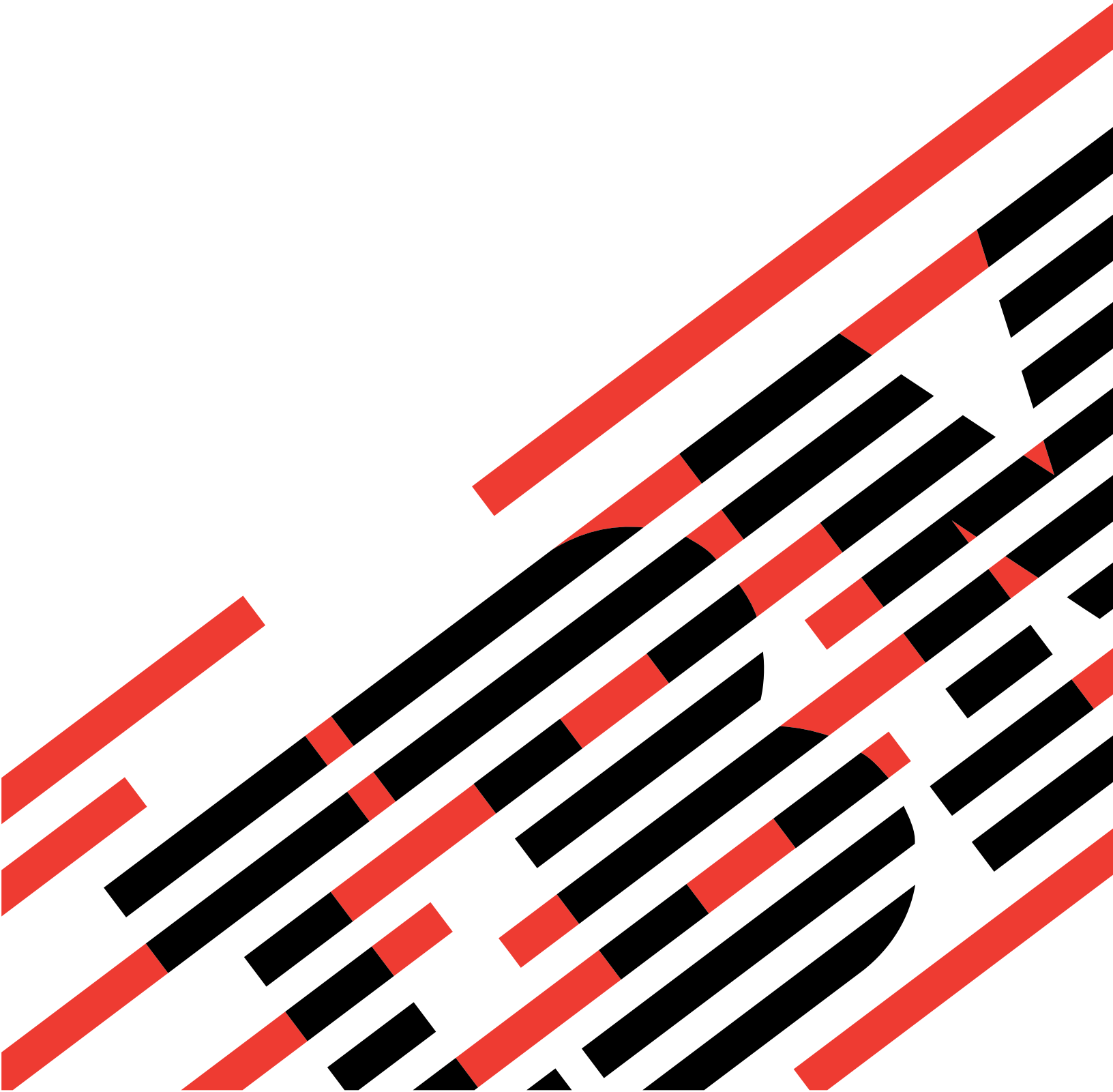
IBM

eserver

iSeries

IBM Directory Server (LDAP)

Versiunea 5 Ediţia 3



IBM

@server

iSeries

IBM Directory Server (LDAP)

Versiunea 5 Ediţia 3

Notă

Înainte să folosiţi aceste informaţii şi produsul pe care îl însoţesc citiţi informaţiile din “Observaţii”, la pagina 225.

Ediţia a şaptea (august 2005)

Această ediţie este valabilă pentru IBM Operating System/400 (număr produs 5722–SS1) Versiunea 5, Ediţia 3, Modificarea 2 şi pentru toate ediţiile şi modificările următoare, până când se specifică altceva în noile ediţii. Această versiune nu rulează pe toate modelele de calculatoare cu set de instrucţiuni reduse (RISC) şi nici pe modelele CISC.

Cuprins

Capitolul 1. IBM Directory Server pentru iSeries (LDAP)

IBM Directory Server pentru iSeries (se referă la el ca Directory Server) furnizează un server Lightweight Directory Access Protocol (LDAP) pe serverul iSeries. LDAP rulează peste Transmission Control Protocol/Internet Protocol (TCP/IP) şi este popular ca un serviciu de directore pentru aplicaţiile Internet şi non-Internet.

Următoarele subiecte vă furnizează informaţii pentru a vă ajuta să înţelegeţi şi să folosiţi Directory Server pe serverul dumneavoastră iSeries:

Capitolul 2. Ce este nou pentru V5R3

Directory Server pentru iSeries (cunoscut anterior ca IBM Directory Server pentru iSeries) are următoarele îmbunătăţiri şi caracteristici noi pentru V5R3:

- **Accesibilitate administrare şi utilizator:** Noul IBM Directory Server Web Administration Tool înlocuieşte IBM Directory Management Tool. Unealta de administrare Web include funcţia de administrare a intrărilor utilizatorului, a proceselor Directory Server şi a arborelui de directoare dintr-o interfaţă Web comună. Protocolul LDAP este acum folosit pentru interogarea şi actualizarea opţiunilor de configurare a Directory Server.
- **Grupuri dinamice:** Grupurile dinamice permit unui grup să fie creat unde membrii sunt intrări care se potrivesc unui filtru de căutare.
- **Grupuri imbricate:** Grupurile imbricate permit să fie creat un grup al cărui membri includ toţi membrii celorlalte grupuri.
- **Poliţă de parolă:** Directory Server suportă acum o politică de parolă care include reguli de sintaxă a parolei, istorie a parolei şi intrări de dezactivare după prea multe încercări pentru a folosi parole incorecte.
- **Controale de acces bazate pe filtru** Autorizarea intrărilor poate fi specificată acum folosind control de acces bazat pe filtru. De exemplu, puteţi specifica permisiuni la intrări cu numărul de departament 'abc sau puteţi acorda acces la diferite tipuri specifice de intrări.
- **Replicare:** Îmbunătăţirile de replicare includ abilitatea de a avea servere master multiple (servere peer), replicare a subarborilor, planificare şi control a replicării îmbunătăţite, monitorizare îmbunătăţită şi mai multe funcţii de replicare.
- **Căutare sortată:** Controlul căutării sortare permite unui client să primească rezultate ale căutării sortate bazându-se pe o listă de criterii unde fiecare criteriu reprezintă o cheie de sortare. Aceasta mută responsabilitatea de sortare de la aplicaţia clientului la serverul unde poate fi făcută mai eficient. Comanda de căutare LDAP a fost îmbunătăţită cu noi parametri pentru a permite rezultatelor căutării să fie sortate. Există de asemenea noi API-uri LDAP pentru sortarea rezultatelor căutării.
- **Căutare paginată:** Controlul rezultatelor paginate vă permite să gestionaţi cantitatea de date returnate de o cerere de căutare. Puteţi cere un subset de intrări în loc să primiţi toate rezultatele o dată. Cererile de căutare următoare afişează următoarea pagină de rezultate până când este anulată operaţia sau este returnat ultimul rezultat. Comanda de căutare LDAP a fost îmbunătăţită cu noi parametri pentru a permite rezultatelor căutării să fie paginate. Există de asemenea noi API-uri LDAP pentru paginarea rezultatelor căutării.
- **Utilităţi ale liniei de comandă:** Următoarele utilităţi ale liniei de comandă sunt noi:
  - ldapexop - furnizează capabilitatea de legare la un director şi de a emite o singură operaţie extinsă împreună cu orice date care formează valoarea de operaţii extinse.
  - ldapdiff - sincronizează un server replică cu masterul său.
  - ldapchangepwd - trimite cereri de modificare a parolei la un server LDAP.
- **Performanţă:** Performanţa este îmbunătăţită pentru toate operaţiile. În plus, toate operaţiile sunt acum permise să fie realizate simultan de către clienţi multipli.
- **Caracterele speciale în Numele distinctive (DN):** Un DN poate să conţină acum următoarele caractere speciale: virgulă, egal, plus, mai mic, mai mare, liră sterlină, punct şi virgulă, backslash şi ghilimele.
- **Reguli de potrivire pentru atribute de şiruri:** Dacă un atribut este definit cu una din cele două sintaxe de şir, Directory String IA5 String, serverul va onora comportamentul care se potriveşte specificat în schema atributului, corectând astfel o eroare din ediţiile anterioare. Puteţi defini un atribut să fie sensibil la majuscule sau să ignore majusculele când se potrivesc. Anterior, serverul permitea să fie definită o regulă de potrivire, dar o ignore. Intern serverul trata IA5 String ca fiind sensibil la majuscule, iar Directory String ca fiind insensibil la majuscule. Dacă serverul dumneavoastă a definit atribute ca IA5 String cu caseIgnoreMatch sau DirectoryString cu caseExactMatch, serverul se va comporta corect pentru acele atribute.

Capitolul 3. PDF tipăribil

Pentru a vizualiza sau descărca versiunea PDF a acestui document, selectaţi Directory Server (LDAP) (aprox. 2700 KB).

Alte informaţii

Pentru a vizualiza sau tipări PDF-uri ale manualelor înrudite şi Redbooks, vedeţi Capitolul 10, “Informaţii înrudite”, la pagina 223.

Salvarea fişierelor PDF

Pentru a salva un fişier PDF pe staţia de lucru proprie pentru vizualizare sau tipărire:

1. Faceţi clic dreapta pe fişierul PDF în browserul dumneavoastră (clic dreapta pe legătura de mai sus).
2. Faceţi clic pe opţiunea care salvează fişierul PDF local.
3. Navigaţi până la directorul unde vreţi să salvaţi fişierul PDF.
4. Faceţi clic pe **Save**.

Descărcarea programului Adobe Reader

Aveţi nevoie de Adobe Reader pentru a vizualiza sau tipări aceste PDF-uri. Puteţi descărca gratis o copie de la situl Web Adobe (www.adobe.com/products/acrobat/readstep.html) .

Capitolul 4. Concepte Directory Server

Directory Server implementează specificaţiile Internet Engineering Task Force (IETF) LDAP V3. Include de asemenea îmbunătăţiri adăugate de IBM în zone de funcţionalitate şi performanţă. Această versiune foloseşte IBM DB2 ca memorare de siguranţă pentru a furniza operaţiei LDAP integritate de tranzacţie, operaţii de performanţă ridicată, copie de siguranţă online şi capabilitate de restaurare. Interferează cu clienţii de bază IETF LDAP V3. Pentru concepte şi consideraţii înrudite cu Directory Server, vedeţi următoarele:

Directoare

Directory Server permite accesul la un tip de bază de date care păstrează informaţiile într-o structură similară cu modul în care este organizat sistemul de fişiere integrat i5/OS.

Dacă este cunoscut numele unui obiect, pot fi extrase caracteristicele sale. Dacă este cunoscut numele unui obiect individual particular, directorul poate fi căutat pentru o listă de obiecte care îndeplinesc o anumită cerinţă. Directoarele pot fi căutate de obicei de criterii specifice, nu doar de un set predefinit de categorii.

Un director este o bază de date specializată care are caracteristici ce o deosebesc de bazele de date relaţionale cu scop general. O caracteristică a unui director este că acesta este accesat (citit sau căutat) mult mai des decât este actualizat (scris. Deoarece directoarele trebuie să poată să suporte volume mari de cereri de citire, ele sunt optimizate tipic pentru acces de citire. Deoarece directoarele nu au scopul de a furniza la fel de multe funcţii ca bazele de date cu scop general, ele pot fi optimizate pentru a furniza economic mai multe aplicaţii cu acces rapid la datele de directoare din medii mari de distribuţie.

Un director poate fi centralizat sau distribuit. Dacă un director este centralizat, există un server de directoare (sau un cluster server) la o locaţie care furnizează acces la director. Dacă directorul este distribuit, există servere multiple, de obicei dispersate geografic, care furnizează acces la director.

Când este distribuit un director, informaţiile stocate în director pot fi partiţionate sau replicate. Când informaţiile sunt partiţionate, fiecare server de directoare memorează un subset unic şi non-overlapping de informaţii. Adică, fiecare intrare de director este memorată de către un singur server. Tehnica de partiţionare a directorului este de a folosi referalii LDAP. Referalii LDAP permit utilizatorului să trimită cererile Lightweight Directory Access Protocol (LDAP)

la spaţii de nume diferite sau la fel într-un server diferit. Când sunt replicate informaţiile, aceeaşi intrare de director este memorată de mai mult de un server. Într-un director distribuit, unele informaţii pot fi partiţionate şi unele informaţii pot fi replicate.

Modelul serverului de directoare LDAP se bazează pe intrări (la care se face referire tot ca obiecte). Fiecare intrare conţine unul sau mai multe atribute, cum ar fi un nume sau o adresă şi un tip. Tipurile conţin în mod tipic şiruri mnemonice, cum ar fi cn pentru nume comun sau poştă pentru adresa poştii electronice.

Directorul de exemplu din Figura 1 la pagina 9 arată o intrare pentru Tim Jones care include atribute ale poştei şi ale numărului de telefon. Alte posibile atribute includ fax, titlu şi poză jpeg.

Fiecare director are o schemă, care este un set de reguli care determină structura şi conţinutul directorului. Puteţi vizualiza schema folosind unealta de administrare Web. Pentru informaţii suplimentare despre schemă, vedeţi “Schema” la pagina 15.

Fiecare intrare de director are un atribut special numit objectClass. Acest atribut controlează care atribute sunt necesare şi permise într-o intrare. Cu alte cuvinte, valorile atributului objectClass determină regulile schemă pe care intrarea trebuie să le îndeplinească.

În plus faţă de atributele definite de schemă, intrările au de asemenea un set de atribute care sunt menţinute de server. Aceste atribute, cunoscute ca atribute operaţionale, includ asemenea lucruri ca atunci când a fost creată intrarea şi informaţiile de control al accesului. Pentru informaţii suplimentare despre atribute operaţionale, vedeţi “Atribute operaţionale” la pagina 71.

Tradiţional, intrările director LDAP sunt aranjate într-o structură ierarhică care reflectă graniţa politicală, geografică sau organizaţională (consultaţi Figura 1 la pagina 9). Intrările care reprezintă ţări sau regiuni apar la începutul ierarhiei. Intrările ce reprezintă stări sau organizaţii naţionale ocupă al doilea nivel jos în ierarhie. Intrările de jos care pot reprezenta persoane, unităţi organizaţionale, imprimante, documente sau alte elemente.

LDAP se referă la intrări cu DN-uri (Distinguished Names). Numele distinctive consistă din numele intrării înseşi precum şi numele, în ordinea de jos în sus, a obiectelor de peste el din director. De exemplu, DN-ul complet pentru intrarea din colţul stânga jos a Figura 1 la pagina 9 este cn=Tim Jones, o=IBM, c=US. Fiecare intrare are cel puţin un atribut care este folosit pentru a numi intrarea. Acest atribut de numire este numit Nume distinctiv relativ (Relative Distinguished Name - RDN) al intrării. Intrarea de deasupra unui RDN dat, se numeşte Numele distinctiv părinte. În exemplul de mai sus, cn=Tim Jones numeşte intrarea, deci este RDN. o=IBM, c=US este DN-ul părinte pentru cn=Tim Jones. Pentru informaţii suplimentare despre DN-uri, vedeţi “Nume distinctive (DN-uri)” la pagina 11.

Pentru a da unui server LDAP capabilitatea de a gestiona o parte a unui director LDAP, specificaţi numele distinctive părinte de cel mai înalt nivel în configuraţia serverului. Aceste nume distinctive se numesc sufixe. Serverul poate accesa toate obiectele din director care sunt sub sufixul specificat în ierarhia directorului. De exemplu, dacă un server LDAP conţinea directorul arătat în Figura 1 la pagina 9, ar fi trebuit să aibă sufixul o=ibm, c=us specificat în configuraţia sa pentru a putea răspunde interogărilor clientului cu privire la Tim Jones.

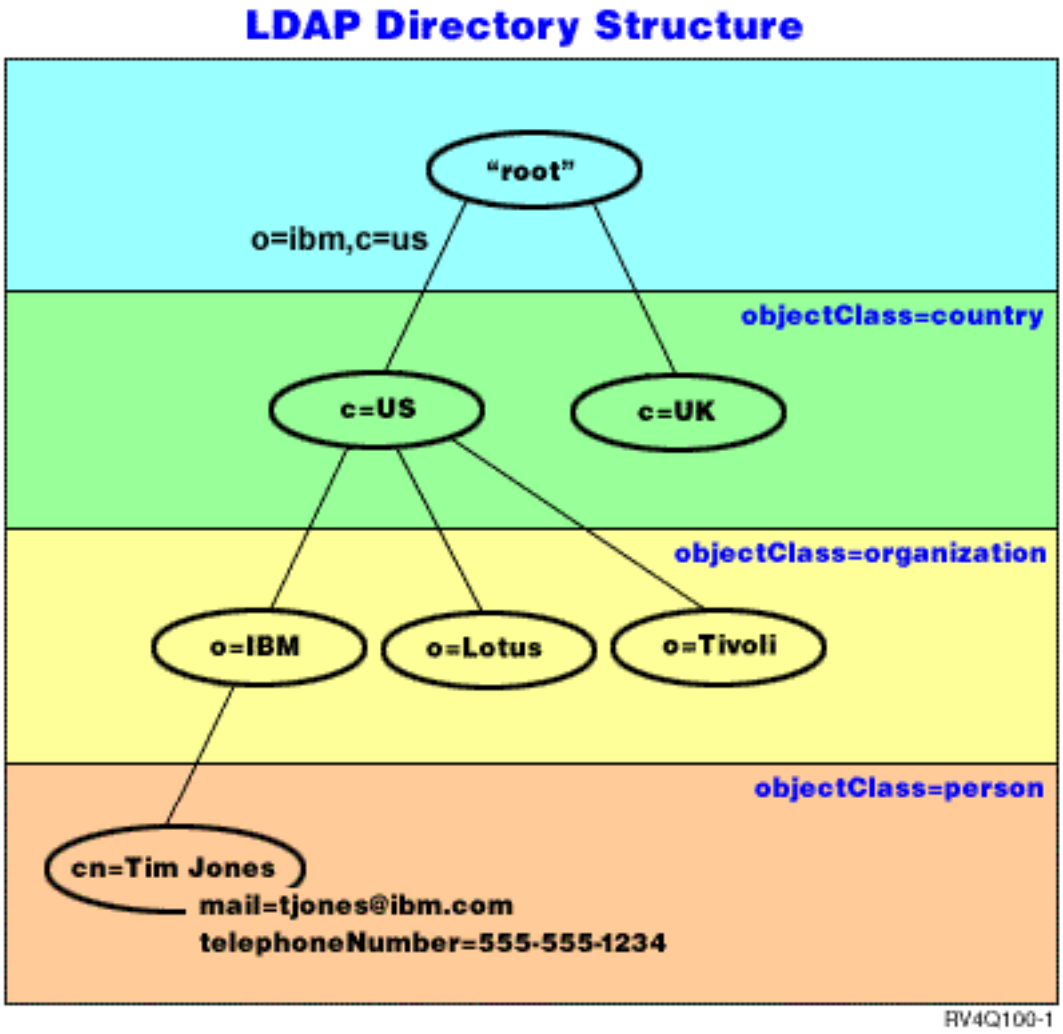


Figura 1. Structura directorului LDAP

Nu sunteţi limitat la ierarhia tradiţională când vă structuraţi directorul. Structura componentelor domeniului, de exemplu, câştigă teren. Cu această structură, intrările sunt compuse din părţi ale numelor domeniilor TCP/IP. De exemplu, dc=ibm,dc=com poate fi preferabilă în loc de o=ibm,c=us.

Să spunem că aţi vrea să creaţi un director folosind structura componentă a domeniului care va conţine date despre angajaţi cum ar fi nume, numere de telefon şi adrese de e-mail. Folosiţi sufixul sau contextul de numire bazat pe domeniul TCP/IP. Acest director poate fi vizualizat ca ceva similar cu ceea ce urmează:

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

Când sunt introduse în Directory Server aceste date pot arăta similar cu următoarele:

```
# 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
```

Veţi observa că fiecare intrare conţine valori de atribute numite clasă obiect. Valorile clasă obiect definesc ce atribute sunt permise în intrare, cum ar fi numărul de telefon sau numele de naştere. Clasele obiect permise sunt definite în schemă. Schema este un set de reguli care definesc tipurile de intrări permise în baza de date.

Clienţi şi servere de directoare

Directoarele sunt accesate de obicei folosind modelul de comunicare client-server. Procesele client şi server pot fi sau nu pe aceeaşi maşină. Un server este capabil să servească mai mulţi clienţi. O aplicaţie care vrea să citească sau să scrie informaţii într-un director nu accesează directorul direct. În schimb, apelează o funcţie sau o interfaţă de programare a aplicaţiei (API) care trimite un mesaj la un alt proces. Acest proces secund accesează informaţiile din director în numele aplicaţiei de cerere. Rezultatele citirii sau scrierii sunt atunci returnate la aplicaţia de cerere.

Un API defineşte o interfaţă de programare pe care un limbaj de programare particular o foloseşte pentru a accesa un serviciu. Formatul şi conţinutul mesajelor schimbate între client şi server trebuie să adere la o înţelegere de protocol. LDAP defineşte un protocol de mesaj folosit de clienţi şi servere de directoare. Există de asemenea un API LDAP asociat pentru limbajul C şi moduri de acces la director de la o aplicaţie Java folosind JNDI (Java Naming and Directory Interface).

Securitate director

Un director trebuie să suporte capabilităţile de bază necesare pentru a implementa o politică de securitate. Directorul poate să nu furnizeze direct capabilităţile de securitate necesare, dar poate fi integrat cu un serviciu de securitate de reţea de încredere care furnizează serviciile de securitate de bază. Mai întâi, este necesară o metodă pentru a autentifica utilizatorii. Autentificarea verifică ca utilizatorii să fie cine pretind a fi. Un nume de utilizator şi o parolă sunt schema de bază de autentificare. După ce sunt autentificaţi utilizatorii, trebuie determinat dacă au autorizarea sau permisiunea de a realiza operaţia cerută pe obiectul specific.

Autorizarea este deseori bazată pe liste de control de acces (ACL-uri). Un ACL este o listă de autorizări care pot fi ataşate la obiecte şi atribute din director. Un ACL listează ce tip de acces este permis sau refuzat fiecărui utilizator sau grup de utilizator. Pentru a face ACL mai scurt şi mai manevrabil, utilizatorii cu aceleaşi drepturi de acces sunt deseori puşi în grupuri.

Nume distinctive (DN-uri)

Fiecare intrare din director are un nume distinctiv (DN). DN este numele care identifică în mod unic o intrare din director. Un DN este alcătuit dintr-un atribut=perechi de valori, separate de virgule, de exemplu:

```
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
```

Oricare din atributele definite în schema directorului poate fi folosit pentru a alcătui un DN. Ordinea perechilor de valori ale atributului component este importantă. DN conţine o componentă pentru fiecare nivel al ierarhiei de directoare de la rădăcină la nivelul unde se află intrarea. LDAP DN-uri încep cu cel mai specific atribut (de obicei un model de nume) şi continuă progresiv cu atribute mai apropiate, terminând de obicei cu atributul ţară. Prima componentă a DN se numeşte Relative Distinguished Name (RDN). Identifică o intrare diferită de orice altă intrare care are acelaşi părinte. În exemplul de mai sus, RDN ″cn=Ben Gray″ separă prima intrare de de-a doua, (cu RDN ″cn=Lucille White″). Aceste două exemple de DN sunt altfel echivalente. Atributul=pereche valori care alcătuieşte RDN pentru o intrare trebuie să fie de asemenea prezent în intrare. (Aceasta nu este valabilă şi pentru celelalte componente ale DN.)

Urmăriţi acest exemplu pentru a crea o intrare pentru o persoană:

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

Reguli escape pentru DN

Unele caractere au un înţeles special într-un DN. De exemplu, = (egal) separă un nume şi-o valoare de atribut, iar , (virgulă) separă atribut=perechi de valori. Caracterele speciale sunt **,** (virgula), **=** (egal), **+** (plus), **<** (mai mic), **>** (mai mare), # (semnul numărului), **;** (punct şi virgulă), \ (backslash) şi **"** (ghilimele, ASCII 34).

Un caracter special poate fi scăpat într-o valoare atribut pentru a înlătura înţelesul special. Pentru a scăpa aceste caractere speciale sau alte caractere într-o valoare atribut dintr-un şir DN, folosiţi următoarele metode:

1. Dacă un caracter de scăpat este unul din caracterele speciale, precedaţi-l de un backslash (’\’ ASCII 92). Acest exemplu arată o metodă de plasare a unei virgule într-un nume de organizaţie:

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

   Aceasta este metoda de preferat.
2. Altfel înlocuiţi caracterul de plasat cu un backslash şi doi digiţi zecimali, care formează un singur octet în codul caracterului. Codul caracterului **trebuie** să fie în setul de coduri UTF-8.

   ```
   CN=L. Eagle,O=Sue\2C Grabbit and Runn,C=GB
   ```
3. Încadraţi întrega valoare atribut de**""** (ghilimele) (ASCII 34), care nu sunt parte a valorii. Între perechea de ghilimele, toate caracterele sunt preluate aşa cum sunt, cu excepţia \ (backslash). \ (backslash) poate fi folosit pentru

a plasa un backslash (ASCII 92) sau ghilimele (ASCII 34), oricare dintre caracterele menţionate anterior sau perechi zecimale ca în metoda 2. De exemplu, pentru a scăpa ghilimelele din cn=xyz"qrs"abc, devine cn=xyz\"qrs\"abc sau pentru a scăpa \ :

```
"trebuie saă scapaţi un singur backslash astfel
\\"
```

Alt exemplu, "\Zoo" este ilegal, deoarece 'Z' nu poate fi sărit în acest context.

Pseudo DNs

Pseudo DNs sunt folosite în definiţii şi evaluări ale controlului de acces. Directorul LDAP suportă mai multe DNs (de exemplu, ″group:CN=THIS″ şi ″access-id:CN=ANYBODY″), care sunt folosite pentru a se referi la numere mari de DN-uri care împart o caracteristică comună, în relaţie fie cu operaţia ce este realizată, fie cu obiectul pe care este realizată operaţia. Pentru informaţii suplimentare de spre controlul de acces, vedeţi "Securitate Directory Server" la pagina 40.

Trei pseudo DN-uri sunt suportate de Directory Server:

- access-id: CN=THIS

  Când este specificat ca parte a unui ACL, acest DN se referă la bindDN, care se potriveşte cu DN pe care este realizată operaţia. De exemplu, dacă o operaţie este realizată pe obiectul ″cn=personA, ou=IBM, c=US″ şi bindDn este ″cn=personA, ou=IBM, c=US″, permisiunile acordate sunt o combinaţie a celor date la ″CN=THIS″ şi a celor date la ″cn=personA, ou=IBM, c=US″.
- grup: CN=ANYBODY

  Când este specificat ca parte a unui ACL, acest DN se referă la toţi utilizatorii, chiar şi la cei care nu sunt autentificaţi. Utilizatorii nu pot fi înlăturaţi din acest grup, iar acest grup nu poate fi înlăturat din baza de date.
- grup: CN=AUTHENTICATED

  Acest DN se referă la orice DN care a fost autentificat de către director. Metoda de autentificare nu este considerată.

  Notă: ″CN=AUTHENTICATED″ se referă la un DN care a fost autentificat oriunde pe server, indifirent de locul unde se află obiectul ce reprezintă DN. Totuşi ar trebui folosit cu atenţie. De exemplu, sub un sufix, ″cn=Secret″ poate fi un nod numit ″cn=Confidential Material″ care are o intrare ACL a ″group:CN=AUTHENTICATED:normal:rsc″. Sub un alt sufix, ″cn=Common″ poate fi nodul ″cn=Public Material″. Dacă aceşti doi arbori se află pe acelaşi server, o legare la ″cn=Public Material″ va fi considerată autentificată şi va primi permisiunea la clasa normală din obiectul ″cn= Confidential Material″.

Unele exemple de pseudo DNs:

Exemplu 1

Consideraţi următorul ACL ca obiect: cn=personA, c=US

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

Legare utilizator ca	Va primi
cn=personA, c=US	normal:rsc:sensitive:rcs:critical:rwsc
cn=personB, c=US	normal:rsc:sensitive:rsc
Anonymous	normal:rsc

În acest exemplu, persoana A primeşte permisiuni acordate la ″CN=THIS″ ID şi permisiuni date ambelor grupuri de pseudo DN ″CN=ANYBODY″, ″CN=AUTHENTICATED″.

Exemplu 2

Consideraţi următorul ACL ca obiect: 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
```

Pentru o operaţie realizată pe on cn=personA, c=US:

Legare utilizator ca	Va primi
cn=personA, c=US	object:ad:critical:rwsc
cn=personB, c=US	normal:rsc:sensitive:rsc
Anonymous	normal:rsc

În acest exemplu, persoana A primeşte permisiuni acordate la ″CN=THIS″ ID şi pe cele date la DN însuşi ″cn=personA, c=US″. A lua la cunoştinţă că permisiunile de grup nu sunt date deoarece există o intrare acl mai specifică (″access-id:cn=personA, c=US″) pentru legarea DN (″cn=personA, c=US″).

Procesare îmbunătăţită DN

Un RDN compus al DN poate conţine componente multiple conectate de către operatorii '+'. Serverul îmbunătăţeşte suportul pentru căutările intrărilor ce au un astfel de DN. Un RDN compus poate fi specificat în orice ordine ca bază pentru operaţia de căutare.

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

Serverul suportă o operaţie extinsă de nominalizare DN. Operaţiile extinse de nominalizare DN normalizează DN-urile folosind schema serverului. Această operaţie extinsă poate fi de folos aplicaţiilor care folosesc DN-uri. Pentru informaţii suplimentare despre operaţii extinse, vedeţi “Controale şi operaţii extinse” la pagina 72.

Sintaxă nume distinctiv

Sintaxa normală pentru un nume distinctiv (DN) se bazează pe RFC 2253. Sintaxa Backus Naur Form (BNF) este definită după cum urmează:

```
<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> ::= orice caracter cu excepţia <special> sau "\" sau '"'


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

Un caracter punct şi virgulă (;) poate fi folosit pentru a separa RDN-uri dintr-un nume distinctiv, deşi caracterul virgulă (,) este notaţia tipică.

Caracterele spaţiu (spaţii) pot fi prezente pe fiecare parte a virgulei sau a punct şi virgulei. Caracetrele spaţiu sunt ignorate, iar punctul şi virgula este înlocuit cu virgula.

În plus, caracterele spaţiu (’ ’ ASCII 32) pot fi prezente fie înainte, fie după un ’+’ sau ’=’. Aceste caractere spaţiu sunt ignorate la parsare.

Următorul exemplu este un nume distinctiv scris folosind o notaţie care este proiectată să fie comodă formelor comune de nume. Primul este un nume ce conţine trei componente. Prima componentă este un RDN compus. Un RDN compus conţine mai multe de un atribut:pereche valoare şi poate fi folosit pentru a identifica distinctiv o intrare specifică în cazuri în care o simplă valoare CN poate fi ambiguă.

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

Sufix (context de numire)

Un sufix (cunoscut de asemenea ca, context de numire) este un DN care identifică cea mai de sus intrare dintr-o ierarhie de directoare conţinută local. Datorită schemei de numire relativă folosită în LDAP, acest DN este de asemenea sufixul oricărei alte intrări din acea ierarhie de directoare. Un server de directoare poate avea sufixe multiple, fiecare identificând o ierarhie de directoare conţinută local, de exemplu, o=ibm,c=us.

Intrarea specifică care se potriveşte sufixului trebuie adăugată directorului. Intrarea pe care o creaţi trebuie să folosească o clasă obiect care conţine atributul de numire folosit. Puteţi folosi unealta de administrare Web sau utilitarul Qshell ldapadd pentru a crea intrarea corespunzătoare acestui sufix. Pentru informaţii suplimentare vedeţi “Gestionarea intrărilor în director” la pagina 131 sau “ldapmodify şi ldapadd” la pagina 159.

Conceptual, există un spaţiu nume LDAP global. În spaţiul nume LDAP global aţi putea vedea DN-urile ca:

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

Sufixul ″o=IBM″ spune serverului că doar primul DN este într-un spaţiu de nume conţinut de server. Încearcă să facă referire la obiecte care nu sunt într-unul din rezultatele sufix, în nici o eroare de obiect de acest gen sau într-un referal la un alt server de directoare.

Un server poate avea sufixe multiple. Directory Server are mai multe sufixe predefinite care păstrează date specifice implementării noastre:

- cn=schema conţine reprezentarea accesibilă LDAP a schemei
- cn=changelog păstrează istoricul de modificare al serverului, dacă este activat
- cn=localhost conţine informaţii nereplicate care controlează câteva aspecte ale operaţiei serverului, de exemplu, obiecte de configurare ale replicării
- cn=pwdpolicy conţine politica de parolă a serverului
- Sufixul ″os400-sys=system-name.mydomain.com″ face LDAP accesibil la obiecte i5/OS, limitat momentan la profiluri şi grupuri de utilizator

Directory Server vine pre-configurat cu un sufix implicit, dc=system-name,dc=domain-name, pentru a fi mai uşoară pornirea serverului. Nu este necesar să folosiţi acel sufix. Puteţi adăuga propriile dumneavoastră sufixe şi să ştergeţi sufixul pre-configurat.

Există două convenţii comune de numire a sufixilui. Una se bazează pe domeniul TCP/IP pentru organizaţia dumneavoastră. Cealaltă se bazează pe locaţia şi numele organizaţiei.

De exemplu, fiind dat un domeniu TCP/IP al mycompany.com, puteţi alege un sufix ca dc=mycompany,dc=com, unde atributul dc se referă la domeniul component. În acest caz intrarea cu nivelul cel mai de sus pe care aţi creat-o în director poate arăta după cum urmează (folosind LDIF, un format de fişier text pentru reprezentarea intrărilor LDAP):

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

Clasa obiect domain are de asemenea câteva atribute opţionale pe care le-aţi putea folosi. Vizualizaţi schema sau editaţi intrarea pe care aţi creat-o folosind unealta de administrare Web pentru a vedea atributele suplimentare pe care le puteţi folosi. Pentru informaţii suplimentare vedeţi, “Gestionarea schemei” la pagina 121.

Dacă numele companiei dumneavoastră este My Company şi este localizată în Statele Unite, puteţi alege un sufix cum ar fi cele care urmează:

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

Unde ou este numele pentru clasa de obiecte a unităţii organizaţionale, o este numele organizaţiei pentru clasa de obiecte a organizaţiei, iar c este o abreviere de două litere standard de ţară folosită pentru a numi clasa obiect ţară. În acest caz intrarea de nivel cel mai sus pe care aţi creat-o poate arăta astfel:

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

Aplicaţiile pe care le folosiţi pot necesita ca anumite sufixe specifice să fie definite sau să fie folosită o convenţie de numire specifică. De exemplu, dacă directorul dumneavoastră este folosit pentru a gestiona certificate digitale, aţi putea fi nevoit să structuraţi o parte a directorului pentru ca numele de intrare să se potrivească cu subiectul DN al certificatelor pe care le deţine.

Intrările de adăugat la director trebuie să aibă un sufix care se potriveşte cu valoarea DN, precum ou=Marketing,o=ibm,c=us. Dacă o interogare conţine un sufix care nu se potriveşte cu nici un alt sufix configurat pentru baza de date locală, interogarea se referă la serverul LDAP care este identificat de către referalul implicit. Dacă nu este specificată nici un referal implicit LDAP, este returnat un rezultat de obiect care nu există.

Pentru informaţii suplimentare despre cum să adăugaţi sau să înlăturaţi un sufix, vedeţi “Adăugarea şi ştergerea sufixelor Directory Server” la pagina 100.

Schema

O schemă este un set de reguli care controlează modalitatea prin care datele pot fi stocate în director. Schema defineşte tipul de intrări permise, structura atributelor lor şi sintaxa atributelor.

Datele sunt stocate în director folosind intrări ale directorului. O intrare conţine o clasă obiect, care este necesară şi atributele sale. Atributele pot fi necesare sau opţionale. Clasa obiectului specifică felul de informaţii descrise de intrare şi defineşte setul de atribute pe care le conţine. Fiecare atribut are una sau mai multe valori asociate. Vedeţi “Gestionarea intrărilor în director” la pagina 131 pentru informaţii suplimentare despre gestionarea intrărilor.

Pentru informaţii suplimentare înrudite cu schema, vedeţi următoarele:

- “Schema IBM Directory Server” la pagina 16

Schema IBM Directory Server

Schema pentru Directory Server este predefinită, totuşi, puteţi modifica schema, dacă aveţi cerinţe suplimentare. Pentru detalii suplimentare despre cum să modificaţi schema, vedeţi “Gestionarea schemei” la pagina 121.

Directory Server include suport dinamic de schemă. Schema este publicată ca parte a informaţiilor directorului şi este dispo nibilă în intrarea subschemă (DN=″cn=schema″). Puteţi interoga schema folosind API-ul ldap_search() şi puteţi s-o modificaţi folosind ldap_modify(). Vedeţi subiectul “API-uri Directory Server” pentru informaţii suplimentare despre aceste API-uri.

Schema are mai multe informaţii de configurare decât cele incluse în RFC-urile (Request For Comments) LDAP Versiunea 3 sau în specificaţiile standard. De exemplu, pentru un atribut dat, puteţi alege care indecşi trebuie menţinuţi. Aceste informaţii suplimentare de configurare sunt menţinute corespunzător în intrarea subschemă. Este definită o clasă obiect suplimentară pentru intrarea subschemă IBMsubschema, care are atribute ″MAY″ care conţin informaţii despre schema extinsă.

Directory Server defineşte o singură schemă pentru întregul server, accesibil printr-o intrare specială de director, ″cn=schema″. Intrarea conţine toată schema definită pentru server. Pentru a extrage informaţii despre schemă, puteţi realiza o căutare ldap folosind următoarea:

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

Schema furnizează valori pentru următoarele tipuri de atribute:

- objectClasses (Pentru informaţii suplimentare despre objectClasses, vedeţi “Clase obiect” la pagina 18.)
- attributeTypes (Pentru informaţii suplimentare despre attributeTypes, vedeţi “Atribute” la pagina 19.)
- IBMAttributeTypes (Pentru informaţii suplimentare despre IBMAttributeTypes, vedeţi “Atributul IBMAttributeTypes” la pagina 22.)
- reguli de potrivire (Pentru informaţii suplimentare despre reguli de potrivire, vedeţi “Reguli de potrivire” la pagina 23).
- reguli de potrivire (Pentru informaţii suplimentare despre reguli de potrivire, vedeţi “Sintaxă atribut” la pagina 25).

Sintaxa acestor definiţii de schemă este bazată pe RFC-urile LDAP Versiunea 3.

Un exemplu de intrare de schemă poate conţine:

```
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 )
```

Informaţiile schemei pot fi modificate prin API-ul ldap_modify. Consultaţi subiectul “API-uri Directory Server” pentru informaţii suplimentare. Cu DN ″cn=schema″ puteţi adăuga, şterge sau înlocui un tip de atribut sau o clasă obiect. Vedeţi “Schema dinamică” la pagina 27 şi “Gestionarea schemei” la pagina 121 pentru informaţii suplimentare. Puteţi furniza de asemenea o descriere plină. Puteţi adăuga sau înlocui o intrare de schemă cu definiţia LDAP Versiunea 3 sau cu definiţia extensiei atributului IBM sau cu ambele definiţii.

Suport schemă obişnuită

Directorul IBM suportă schema standard de director definită după cum urmează:

- Internet Engineering Task Force (IETF)  RFC-uri LDAP Versiunea 3, precum RFC 2252 şi 2256.
- Directory Enabled Network (DEN) 
- Common Information Model (CIM) din Desktop Management Task Force (DMTF) 
- Lightweight Internet Person Schema (LIPS) din Network Application Consortium 

Această versiune a LDAP include schema definită LDAP Versiunea 3 din configuraţia implicită a schemei. Include de asemenea definiţiile schemei DEN.

IBM furnizează de asemenea un set de definiţii de scheme obişnuite extinse pe care alte produse IBM le partajează când exploatează directorul LDAP. Ele includ:

- Obiecte pentru aplicaţii de pagini albe precum persoană, grup, ţară, organizaţie, unitate şi rol de organizaţie, localitate, stare şi tot aşa
- Obiectele pentru alte subsisteme precum conturi, servicii şi puncte de acces, autorizare, autentificare, politică de securitate şi tot aşa.

Clase obiect

O clasă obiect specifică un set de atribute folosite pentru a descrie un obiect. De exemplu, dacă aţi creat clasa obiect **tempEmployee**, poate conţine atribute asociate cu un angajat temporar precum, **idNumber**, **dateOfHire** sau **assignmentLength**. Puteţi adăuga clase obiect personalizate pentru a servi necesităţile organizaţiei dumneavoastră. Schema IBM Directory Server furnizează unele tipuri de bază de clase obiect, incluzând:

- Grupuri
- Locaţii
- Organizaţii
- Persoane

Notă: Clasele obiect care sunt specifice pentru Directory Server au prefixul ’ibm-’.

Clasele obiect sunt definite de caracteristicile tipului, moştenirii şi atributelor.

Tip clasă obiect

O clasă obiect poate fi de trei tipuri:

Structurală:
Fiecare intrare trebuie să aparţină unei singure clase obiect structurală, care defineşte conţinutul de bază al intrării. Această clasă obiect reprezintă un obiect din lumea reală. Deoarece toatre intrările trebuie să aparţină unei clase obiect structurală, acesta este cel mai comun tip de clasă obiect.

Abstractă:
Acest tip este folosit ca o superclasă sau şablon pentru alte clase obiect structurale. Defineşte un set de atribute care sunt comune cu un set de clase obiect structurale. Aceste clase obiect, dacă sunt definite ca superclase sau clase abstracte, moştenesc atributele definite. Atributele nu trebuie să fie definite pentru fiecare dintre clasele obiect subordonate.

Auxiliară:
Acest tip indică atribute suplimentare care pot fi asociate cu o intrare aparţinând unei anumite clase obiect structurală. Deşi o intrare poate aparţine unei singure clase obiect structurală, poate aparţine unor multiple clase obiect auxiliare.

Moştenire clasă obiect

Această versiune Directory Server suportă moştenire obiect pentru clasa obiect şi pentru definiţiile atributului. Poate fi definită o nouă clasă obiect cu clase părinte şi cu atribute suplimentare sau modificate.

Fiecare intrare este alocată unei singure clase obiect structurală. Toate clasele obiect moştenesc de la clasa obiect abstractă **top**. Pot moşteni de asemenea de la la alte clase obiect. Structura clasei obiect determină lista de atribute necesare şi permise pentru o anumită intrare. Moştenirea clasei obiect depinde de secvenţa definiţiei clasei obiect. O clasă obiect poate moşteni doar de la clase obiect ce o preced. De exemplu, structura clasei obiect pentru intrarea unei persoane poate fi definită în fişierul LDIF ca:

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

În această structură, organizationalPerson moşteneşte de la clasele person şi top, în timp ce clasa obiect person moşteneşte doar de la clasa obiect top. De aceea, când alocaţi unei intrări clasa obiect organizationalPerson, moşteneşte automat atributele nesesare şi permise de la clasa obiect superioară (în acest caz, clasa de obiect person).

Operaţiile de actualizare schemă sunt verificate împotriva ierarhiei clasei schemă pentru consistenţă înainte de a fi procesate şi comise.

Atribute

Orice clasă obiect include un număr de atribute necesare şi opţionale. Atributele necesare sunt atributele care trebuie să fie prezente în intrări folosind clasa obiect. Atributele necesare sunt atributele care pot să fie prezente în intrări folosind clasa obiect.

Atribute

Fiecare intrare de director are un set de atribute asociate ei prin clasa sa obiect. În timp ce clasa obiect descrie tipul de informaţii pe care le conţine o intrare, datele reale sunt conţinute în atribute. Un atribut este reprezentat de una sau mai multe perechi de valori de nume care conţin anumite elemente de date cum ar fi un nume, o adresă sau un număr de telefon. Directory Server reprezintă datele ca perechi de valori de nume, un atrbut descriptiv, precum commonName (cn) şi o anumită informaţie, precum John Doe.

De exemplu, intrarea pentru John Doe poate conţine mai multe atribute perechi de valori nume.

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

În timp ce atributele standard sunt deja definite în schemă, puteţi crea, edita, copia sau şterge definiţii de atribute pentru a servi necesităţilor organizaţiei dumneavoastră.

Atributele pot fi definite ca valori singulare sau multiple. Atributele cu valori multiple nu sunt ordonate, deci în aplicaţie nu ar trebui să depindă de setul de valori pentru un atribut dat ce este returnat într-o anumită ordine. Dacă aveţi nevoie de un set de valori ordonate, încercaţi să puneţi lista de valori într-o singură valoare de atribut:

```
preferences: 1 pref 2-a pref 3-a pref
```

Sau încercaţi să includeţi informaţii despre ordine în valoare:

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

Atributele cu valori multiple sunt folositoare când o intrare este cunoscută după mai multe nume. De exemplu, cn (nume comun) este multi-valoric. O intrare ar putea fi definită ca:

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

Aceasta permite cererilor pentru John Smith şi Jack Smith să întoarcă aceleaşi informaţii.

Atributele binare conţin un şir arbitrar de octeţi, de exemplu o poză JPEG şi nu pot fi folosite pentru a căuta intrări.

Atibutele buleane conţin şirurule TRUE sau FALSE.

Atributele DN conţin nume distinctive LDAP. Valorile nu trebuie să fie DN-urile pentru intrările existente, dar trebuie să aibă o sintaxă DN validă.

Atributele şir director conţin un şir text folosind caractere UTF-8. Atributul poate ţine cont de majuscule sau nu, respectând valorile folosite în filtre de căutare (bazate pe regula de potrivire definită pentru atribut), deşi valoarea este întotdeauna returnată cum a fost introdusă original.

Atributele Generalized Time conţin o reprezentare sigură pentru anul 2000 sub formă de şir a datei şi orei folosind timpi GMT cu un offset de fus orar GMT opţional. Vedeţi “Timp generalizat şi UTC” la pagina 32 pentru informaţii suplimentare despre sintaxa acestor valori.

Atributele şir IA5 conţin un şir text folosind setul de caractere IA5 (7-bit US ASCII. Atributul poate ţine cont de majuscule sau nu, respectând valorile folosite în filtre de căutare (bazate pe regula de potrivire definită pentru atribut), deşi valoarea este întotdeauna returnată cum a fost introdusă original. Şirul IA5 permite de asemnea folosirea unui caracter card sălbatic pentru căutările subşirurilor.

Atributele întregi conţin reprezentarea şirului text a valorii. De exemplu, 0 sau 1000.

Atributele numere de telefon conţin o reprezentare text a unui număr de telefon. Directory Server nu impune o anumită sintaxă pentru aceste valori. Următoarele sunt valori valide: (555)555-5555, 555.555.5555 şi +1 43 555 555 5555.

Atributele timp UTC folosesc un format de şir mai vechi, fără an 2000 sigur, pentru a reprezenta data şi timpul. Vedeţi “Timp generalizat şi UTC” la pagina 32 pentru informaţii suplimentare.

Pentru informaţii suplimentare, vedeţi următoarele:
- “Elementele subschemei obişnuite”
- “Atributul objectclass” la pagina 21
- “Atributul attributetypes” la pagina 21
- “Atributul IBMAttributeTypes” la pagina 22
- “Reguli de potrivire” la pagina 23
- “Reguli de indexare” la pagina 24
- “Sintaxă atribut” la pagina 25

Elementele subschemei obişnuite

Următoarele elemente sunt folosite pentru a defini gramatica valorilor atributelor subschemei:
- 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 ; set de oid-uri de orice formă (OID-uri numerice sau nume)
- oids = woid / (″(″ oidlist ″)″)

- oidlist = woid *(″$″ woid) ; descriptori de obiecte folosiţi ca nume de elemente ale schemei
- qdescrs = qdescr / (whsp ″(″ qdescrlist ″)″ whsp)
- qdescrlist = [qdescr *(qdescr)]
- whsp ″'″ descr ″'″ whsp

Atributul objectclass

Atributul objectclass listează clasele obiect suportate de către server. Fiecare valoare a acestui atribut reprezintă o definiţie separată de clasă obiect. Definiţiile clasei obiect pot fi adăugate, şterse sau modificate de modificări corespunzătaore a le atributului clase obiect a cn=intrare schemă. Valorile atributului objectclass au următoarea gramatică, definită de 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 ")"
```

De exemplu, definiţia clasei obiect person este:

(2.5.6.6 NAME 'person' DESC 'Defineşte intrări care reprezintă în general persoane. ' STRUCTURAL SUP top MUST (cn $ sn) MAY (userPassword $ telephoneNumber $ seeAlso $ description))

- OID pentru această clasă este 2.5.6.6
- Numele este ″person″
- Este o clasă obiect structurală
- Moşteneşte de la clasa obiect ″top″
- Următoarele atribute sunt necesare: cn, sn
- Următoarele atribute sunt opţionale: userPassword, telephoneNumber, seeAlso, description

Pentru informaţii suplimentare despre cum se modifică clasele obiect suportate de server, vedeţi “Gestionarea schemei” la pagina 121.

Atributul attributetypes

Atributul attributetypes tipăreşte atributul suportat de server. Fiecare valoare a acestui atribut reprezintă o definiţie de atribut separată. Definiţiile clasei obiect pot fi adăugate, şterse sau modificate de modificări corespunzătoare ale atributului attributetypes a intrării cn=schema. Valorile atributului attributetypes au următoarea gramatică, definită de RFC 2252:

```
AttributeTypeDescription = "(" whsp
        numericoid whsp ; AttributeType identifier
        [ "NAME" qdescrs ] ; nume folosit în AttributeType
        [ "DESC" qdstring ] ; descriere
        [ "OBSOLETE" whsp ]
        [ "SUP" woid ] ; derivat din celălalt AttributeType
        [ "EQUALITY" woid ; Nume regulă de potrivire
        [ "ORDERING" woid ; Nume regulă de potrivire
        [ "SUBSTR" woid   ; Nume regulă de potrivire
        [ "SYNTAX" whsp noidlen whsp ]
        [ "SINGLE-VALUE" whsp ] ; valoare multiplă implicită
        [ "COLLECTIVE" whsp ] ; implicit not collective
        [ "NO-USER-MODIFICATION" whsp ]; implicit modificabil de utilizator
        [ "USAGE" whsp AttributeUsage ]; implicit userApplications
         whsp ")"

AttributeUsage =
        "userApplications" /
```

```
        "directoryOperation" /
        "distributedOperation" / ; DSA-shared
        "dSAOperation" ; DSA-specific, valoarea depinde de server
```

Regulile de potrivire şi valorile sintaxei trebuie să fie aibă din valorile definite în continuare:

- “Reguli de potrivire” la pagina 23
- “Sintaxă atribut” la pagina 25

Doar atributele ″userApplications″ pot fi definite sau modificate în schemă. Atributele ″directoryOperation″, ″distributedOperation″ şi ″dSAOperation″ sunt definite de server şi au un anumit înţeles pentru operaţia serverului.

De exemplu, atributul ″description″ are următoare definiţie:

(2.5.4.13 NAME ’description’ DESC ’Atribut comun pentru scheme CIM şi LDAP pentru a furniza descrieri de lungime a unei intrări de obiect director. ’ EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications)

- OID-ul său este 2.5.4.13
- Numele său este ″description″
- Sintaxa sa este 1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Pentru informaţii suplimentare despre cum se modifică tipurile de atribute suportate de server, vedeţi “Gestionarea schemei” la pagina 121.

Atributul IBMAttributeTypes

Atributul IBMAttributeTypes poate fi folosit pentru a defini informaţii de schemă care nu sunt acoperite de standardul LDAP Versiunea 3 pentru atribute. Valorile IBMAttributeTypes trebuie să respecte următoarea gramatică:

```
IBMAttributeTypesDescription = "(" whsp
        numericoid whsp
      [ "DBNAME"   qdescrs ]            ; cel mult 2 nume (tabel, coloană)
      [ "ACCESS-CLASS" whsp IBMAccessClass whsp ]
      [ "LENGTH" wlen whsp ]            ; lungimea maximă a atributului
      [ "EQUALITY" [ IBMwlen ] whsp ]   ; creează index pentru regula de potrivire
      [ "ORDERING" [ IBMwlen ] whsp ]   ; creează index pentru regula de potrivire
      [ "APPROX"   [ IBMwlen ] whsp ]   ; creează index pentru regula de potrivire
      [ "SUBSTR"   [ IBMwlen ] whsp ]   ; creează index pentru regula de potrivire
      [ "REVERSE"  [ IBMwlen ] whsp ]   ; index invers pentru subşir
      whsp ")"

   IBMAccessClass =
      "NORMAL"           / ; acesta este implicit
      "SENSITIVE"        /
      "CRITICAL"         /
      "RESTRICTED"       /
      "SYSTEM"           /
      "OBJECT"

   IBMwlen = whsp len
```

Numericoid
Folosit pentru a corela valoarea din attributetypes cu valoarea din IBMAttributeTypes.

DBNAME
Puteţi furniza cel mult 2 nume, dacă sunt într-adevăr 2 nume date. Primul este numele de tabelă folosit pentru acest atribut. Al doilea este numele coloanei folosit pentru valoarea normalizată total a atributului din tabel. Dacă furnizaţi un singur nume, este folosit şi pentru numele tabelului şi pentru numele coloanei. Dacă nu furnizaţi nici un DBNAME, atunci este folosit numele atributului scurt (din attributetypes).

ACCESS-CLASS
Clasificarea accesului pentru acest tip de atribut. Dcaă ACCESS-CLASS este omisă, este pus implicit pe normal.

LENGTH

Lungimea maximă a acestui atribut. Lungimea este exprimată ca numărul de octeţi. Directory Server are o prevedere pentru specificarea lungimii unui atribut. În valoarea attributetypes, şirul:

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

poate fi folosit pentru a indica că attributetype cu oid attr-oid are o lungime maximă.

EQUALITY, ORDERING, APPROX, SUBSTR, REVERSE

Dacă oricare din aceste atribute este folosit, este creat un index pentru regula de potrivire corespunzătoare. Lungimea opţională specifică lăţimea coloanei indexate. Este folosit un singur index pentru a implementa multiple reguli de potrivire. Directory Server alocă o lungime de 500 când nu este una furnizată de utilizator. Serverul poate de asemenea să folosească o lungime mai scurtă decât cea cerută de utilizator când are rost s-o facă. De exemplu, când lungimea indexului depăşeşte lungimea maximă a atributului, lungimea indexului este ignorată.

Reguli de potrivire

O regulă de potrivire furnizează linii de ghidare pentru compararea şirului în timpul unei operaţii de căutare. Aceste reguli sunt împărţite în trei categorii:

- Egalitate
- Ordonare
- Subşir

Reguli de potrivire ale egalării		
Regulă de potrivire	**OID**	**Sintaxă**
caseExactIA5Match	1.3.6.1.4.1.1466.109.114.1	Sintaxă şir director
caseExactMatch	2.5.13.5 IA5	Sintaxă şir
caseIgnoreIA5Match	1.3.6.1.4.1.1466.109.114.2	Sintaxă şir IA5
caseIgnoreMatch	2.5.13.2	Sintaxă şir director
distinguishedNameMatch	2.5.13.1	DN - nume distinctiv
generalizedTimeMatch	2.5.13.27	Sintaxă Generalized Time
ibm-entryUuidMatch	1.3.18.0.2.22.2	Sintaxă şir director
integerFirstComponentMatch	2.5.13.29	Sintaxă Integer - număr intreg
integerMatch	2.5.13.14	Sintaxă Integer - număr intreg
objectIdentifierFirstComponentMatch	2.5.13.30	Şir pentru conţinerea OID-urilor. OID este un şir care conţine digiţi (0-9) şi puncte zecimale (.).
objectIdentifierMatch	2.5.13.0	Şir pentru conţinerea OID-urilor. OID este un şir care conţine digiţi (0-9) şi puncte zecimale (.)
octetStringMatch	2.5.13.17	Sintaxă şir director
telephoneNumberMatch	2.5.13.20	Sintaxă număr telefon
uTCTimeMatch	2.5.13.25	Sintaxă UTC Time

Reguli de potrivire ale sortării		
Regulă de potrivire	**OID**	**Sintaxă**
caseExactOrderingMatch	2.5.13.6	Sintaxă şir director
caseIgnoreOrderingMatch	2.5.13.3	Sintaxă Directory String
distinguishedNameOrderingMatch	1.3.18.0.2.4.405	DN - nume distinctiv

Reguli de potrivire ale sortării		
Regulă de potrivire	**OID**	**Sintaxă**
generalizedTimeOrderingMatch	2.5.13.28	Sintaxă Generalized Time

Reguli de potrivire ale subşirului		
Regulă de potrivire	**OID**	**Sintaxă**
caseExactSubstringsMatch	2.5.13.7	Sintaxă şir director
caseIgnoreSubstringsMatch	2.5.13.4	Sintaxă şir director
telephoneNumberSubstringsMatch	2.5.13.21	Sintaxă număr telefon

Notă: UTC-Time este formatul şirului timp definit de standardele ASN.1. Vedeţi ISO 8601 şi X680. Folosiţi această sintaxă pentru a stoca valorile timp în format UTC-Time. Vedeţi “Timp generalizat şi UTC” la pagina 32.

Reguli de indexare

Reguli de indexare ataşate atributelor fac posibilă extragerea mai rapidă a informaţiilor. Dacă este dat doar atributul, nu se menţine nici un index. Directory Server furnizează următoarele reguli de indexare:

- Egalitate
- Ordonare
- Aproximare
- Subşir
- Inversare

Specificaţiile regulilor de indexare pentru atribute: Specificând o regulă de indexare pentru un atribut se controlează crearea şi menţinerea unor indecşi speciali ai valorilor atributului. Aceasta îmbunătăţeşte timpul de răspundere pentru căutările cu filtru care includ acele atribute. Cele cinci tipuri posibile de reguli de indexare sunt înrudite cu operaţiile aplicate în filtru de căutare.

Egalitate

Se aplică următoarelor operaţii de căutare:

- equalityMatch ’=’

De exemplu:

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

Ordonare

Se aplică următoarelor operaţii de căutare:

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

De exemplu:

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

Aproximare

Se aplică următoarelor operaţii de căutare:

- approxMatch ’~=’

De exemplu:

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

Subşir Se aplică următoarelor operaţii de căutare:

- substring ’*’

De exemplu:

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

Inversare

Se aplică următoarelor operaţii de căutare:

- '*' substring

De exemplu:

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

Ca minim, este recomandabil să specificaţi indexare egală pe orice atribut care va fi folosit în filtrele de căutare.

Sintaxă atribut

O sintaxă de atribut defineşte valorile permise pentru un atribut. Serverul foloseşte definiţia sintaxei pentru un atribut pentru a valida date şi pentru a determina cum să potrivească valori. De exemplu, un atribut ″Boolean″ poate avea doar valorile ″TRUE″ şi ″FALSE″..

Sintaxă	OID
Sintaxă Attribute Type Description	1.3.6.1.4.1.1466.115.121.1.3
Binary - şir de octeţi	1.3.6.1.4.1.1466.115.121.1.5
Boolean - TRUE/FALSE	1.3.6.1.4.1.1466.115.121.1.7
Sintaxă Directory String	1.3.6.1.4.1.1466.115.121.1.15
Sintaxă DIT Content Rule Description	1.3.6.1.4.1.1466.115.121.1.16
Sintaxă DITStructure Rule Description	1.3.6.1.4.1.1466.115.121.1.17
DN - nume distinctiv	1.3.6.1.4.1.1466.115.121.1.12
Sintaxă Generalized Time	1.3.6.1.4.1.1466.115.121.1.24
Sintaxă IA5 String	1.3.6.1.4.1.1466.115.121.1.26
IBM Attribute Type Description	1.3.18.0.2.8.1
Sintaxă Integer - număr intreg	1.3.6.1.4.1.1466.115.121.1.27
Sintaxă LDAP Syntax Description	1.3.6.1.4.1.1466.115.121.1.54
Matching Rule Description	1.3.6.1.4.1.1466.115.121.1.30
Matching Rule Use Description	1.3.6.1.4.1.1466.115.121.1.31
Name Form Description	1.3.6.1.4.1.1466.115.121.1.35
Sintaxă Object Class Description	1.3.6.1.4.1.1466.115.121.1.37
Şir care conţine OID-uri. OID este un şir care conţine digiţi (0-9) şi puncte zecimale (.). Vedeţi “Identificator obiect (OID)”.	1.3.6.1.4.1.1466.115.121.1.38
Sintaxă Telephone Number	1.3.6.1.4.1.1466.115.121.1.50
Sintaxă UTC Time. UTC-Time este formatul şirului timp definit de standardele ASN.1. Vedeţi ISO 8601 şi X680. Folosiţi această sintaxă pentru a stoca valorile timp în format UTC-Time. Vedeţi “Timp generalizat şi UTC” la pagina 32.	1.3.6.1.4.1.1466.115.121.1.53

Identificator obiect (OID)

Un identificator obiect (OID) este un şir, de numere zecimale, care identifică în mod unic un obiect. Aceste obiecte sunt în mod obişnuit o clasă obiect sau un atribut.

Dacă nu aveţi un OID, puteţi specifica numele clasei obiect sau al atributului la care adăugaţi **-oid**. De exemplu, dacă creaţi atributul tempID, puteţi specifica OID ca **tempID-oid** .

Este absolut important ca OID-urile private să fie obţinute din autorizări legitime. Există două startegii de bază pentru obţinerea OID-urilor legale:

- Înregistraţi obiectele cu o autorizare. Această strategie poate fi convenabilă, de exemplu, dacă aveţi nevoie de un număr mic de OID-uri.
- Obţineţi un arc (un arc este un subarbore individual al arborelui OID) dintr-o autoritate şi alocaţi-vă propriile OID-uri după necesitate. Această strategie este de preferat dacă sunt necesare multe OID-uri sau dacă asignările OID nu sunt stabile.

American National Standards Institute (ANSI) este autoritatea de înregistrare pentru numele de organizaţii din Statele Unite sub procesul global de înregistrare stabilit de International Standards Organization (ISO) şi International Telecommunication Union (ITU). Informaţii suplimentare despre înregistrarea numelui pot fi găsite pe site-ul Web ANSi * (www.ansi.org). Arcul ANSI OID pentru organizaţii este 2.16.840.1. ANSI va aloca un număr (NEWNUM), creând un nou arc OID: 2.16.840.1.NEWNUM.

În majoritatea ţărilor şi regiunilor asociaţia naţională de standarde menţine un registru OID. Ca şi cu arcul ANSI, acestea sunt în general arce alocate sub OID 2.16. Ar putea fi nevoie de investigare pentru a găsi autoritatea OID pentru o anumită ţară sau regiune. Organizaţia naţională de standarde pentru ţara sau regiunea dumneavoastră poate fi un membru ISO. Numele şi informaţiile de contact ale membrilor ISO pot fi găsite pe situl ISO Web (www.iso.ch).

Internet Assigned Numbers Authority (IANA) alocă numere private pentru întreprinderi, care sunt OID-uri, în arcul 1.3.6.1.4.1. IANA va aloca un număr (NEWNUM) pentru ca noul arc OID să fie 1.3.6.1.4.1.NEWNUM. Aceste numere pot fi obţinute de pe site-ul IANA Web (www.iana.org).

O dată ce organizaţiei dumneavoastre i-a fost alocat un OID, puteţi defini propriile OID-uri adăugând la sfârşitul OID-ului. De exemplu, presupunem că organizaţiei dumneavoastre i-a fost alocat OID 1.1.1. Nici unei alte organizaţii nu i se va aloca un OID care începe cu ″1.1.1″. Puteţi crea un interval pentru LDAP adăugând ″.1″ la forma 1.1.1.1. Puteţi în continuare să-l subdivizaţi în intervale pentru for clase obiect (1.1.1.1.1), tipuri de atribute (1.1.1.1.2) şi tot aşa şi puteţi să alocaţi un OID 1.1.1.1.2.34 la atributul ″foo″.

Intrările subschemei

Nu există nici o intrare de subschemă pentru server. Toate intrările din director au un tip implicit de atribut subschemaSubentry. Valoarea tipul atributului subschemaSubentry este DN al intrării subschemei care corespunde intrării. Toate intrările de sub acelaşi server împart aceeaşi intrare de subschemă, iar tipul atributului subschemaSubentry are aceeaşi valoare. Intrarea subschemei are codat DN ’cn=schema’.

Intrarea subschemei aparţine claselor obiect ’top’, ’subschema’ şi ’IBMsubschema’. Clasa obiect ’IBMsubschema’ nu are atribute MUST şi are un tip de atribut MAY (’IBMattributeTypes’).

Clasa obiect IBMsubschema

Clasa obiect IBMsubschema este folosită în intrarea subschemei după cum urmează:

```
( 1.3.18.0.2.6.174
NAME 'ibmSubSchema'
DESC 'IBM clasă obiect specifică care stochează toate atributele şi clasele obiect pentru un director dat
 server.'
SUP 'subschema'
STRUCTURAL MAY ( IBMAttributeTypes ) )
```

Interogări schemă

API-ul ldap_search() poate fi folosit pentru a interoga intrarea subschema, aşa cum este arătat în exemplul următor:

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

Acest exemplu extrage întreaga schemă. Pentru a extrage toate valorile tipurilor de atribute selectate, folosiţi parametrul attrs în ldap_search. Nu puteţi extrage doar o anumită valoare a unui tip de atribut specific.

Vedeţi subiectul “API-uri Directory Server” pentru informaţii suplimentare despre API-ul ldap_search.

Schema dinamică

Pentru a realiza o modificare de schemă dinamică, folosiţi API-ul ldap_modify cu un DN de ″cn=schema″. Este permis să adăugaţi, ştergeţi sau să modificaţi doar o entitate a schemei (de exemplu, un tip de atribut sau o clasă obiect) la un moment dat.

Pentru a şterge o intrare a schemei, specificaţi atributul schemei care defineşte intrarea schemei (objectclasses sau attributetypes), iar pentru valoare sa, OID în paranteze. De exemplu, pentru a şterge atributul cu OID <attr-oid>:

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

Puteţi de asemenea furniza o descriere plină. În orice caz, regula de potrivire folosită pentru a găsi entitatea schemei de şters este objectIdentifierFirstComponentMatch.

Pentru a adăuga sau înlocui o entitate a schemei, trebuie să furnizaţi o definiţie LDAP Versiunea 3 şi puteţi furniza definiţia IBM. În toate cazurile, trebuie să furnizaţi doar definiţia sau definiţiile entităţii schemei pe care vreţi să o afectaţi.

De exemplu, pentru a şterge tipul atributul ’cn’ (its OID is 2.5.4.3), folosiţi ldap_modify() cu:

```
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);
```

Pentru a adăuga o nouă bară tip de atribut cu OID 20.20.20 care moşteneşte de la atributul ″name″ şi are o lungime de 20 caractere:

```
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);
```

Versiunea LDIF a celor de mai sus ar fi:

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

Controale de acces

Modificările schemei dinamice pot fi realizate doar de un furnizor de replicare sau de administratorul DN.

Replicare

Când se realizează o modificare de schemă dinamică, aceasta este replicată.

Modificări de schemă nepermise

Nu sunt permise toate modificările de schemă. Restricţiile de modificare includ următoarele:

- Orice modificare a schemei trebuie să lase schema într-o stare consistentă.
- Un tip de atribut care este un supertip al unui alt tip de atribut nu poate fi şters. Un tip de atribut care este un tip de atribut ″MAY″ sau un ″MUST″ al unei clase obiect nu poate fi şters.
- O clasă obiect care este o superclasă al alteia nu poate fi ştearsă.
- Tipurile de atribute sau clasele obiect care se referă la entităţi inexistente (de exemplu, sintaxe sau clase obiect) nu pot fi adăugate.
- Tipurile de atribute sau clasele obiect nu pot fi modificate în aşa fel încât să ajungă să se refere la entităţi inexistente (de exemplu, sintaxe sau clase obiect).

Modificările unei scheme care afectează operaţia serverului nu sunt permise. Următoarele definiţii de schemă sunt necesare pentru serverul de directoare. Nu trebuie să fie modificate.

Clase obiect:

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

Atribute:

- 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

Sintaxe:
All

Reguli de potrivire:
All

Verificare schemă

Când serverul este iniţializat, fişierele schemei sunt citite şi verificate pentru consistenţă şi corectitudine. Dacă verificările eşuează, serverul eşuează să iniţializeze şi emite un mesaj de eroare. În timpul oricărei modificări de schemă dinamică, schema rezultată este de asemenea verificată pentru consistenţă şi corectitudine. Dacă verificările eşuează, se returnează o eroare, iar modificarea eşuează. Unele verificări sunt părţi ale gramaticii (de exemplu, un tip de atribut poate avea cel mult un supertip sau o clasă obiect poate avea orice număr de supercalse).

Următoarele elemente sunt verificate pentru tipuri de atribute:

- Două tipuri diferite de atribute nu pot avea acelaşi nume sau OID.
- Ierarhia moştenită a tipurilor de atribut nu are cicluri.
- Supertipul unui tip de atribut trebuie de asemenea definit, deşi definiţia sa poate fi afişată mai târziu sau într-un fişier separat.
- Dacă un tip de atribut este un subtip al altuia, amândoi au acelaşi USAGE.
- Toate tipurile de atribute au o sintaxă direct definită sau moştenită.

- Doar atributele operaţionale pot fi marcate ca NO-USER-MODIFICATION.

Următoarele articole sunt verificate pentru clase obiect:

- Două tipuri diferite de clase obiect nu pot avea acelaşi nume sau OID.
- Ierarhia moştenită a claselor obiect nu are cicluri.
- Supertipul unei clase obiect trebuie de asemenea definit, deşi definiţia sa poate fi afişată mai târziu sau într-un fişier separat.
- Tipurile de atribut ″MUST″ şi ″MAY″ ale unei clase obiect trebuie să fie de asemenea definite, deşi definiţia sa poate fi afişată mai târziu sau într-un fişier separat.
- Orice clasă obiect structurală este o subclasă directă sau indirectă de sus.
- Dacă o clasă obiect abstractă are superclase, acestea trebuie să fie de asemenea abstracte.

Verificând o intrare împotriva schemei

Când o intrare este adăugată sau modificată printr-o operaţie LDAP, intrarea este verificată împotriva schemei. Implicit, sunt realizate toate verificările afişate în această secţiune. Totuşi puteţi dezactiva selectiv unele din verificările schemei modificând nivelul de verificare al schemei. Aceasta se face prin Navigator iSeries modificând valoarea câmpului **Verificare schemă** din pagina **Bază de date/Sufixe** a proprietăţilor Directory Server. Vedeţi “Schema de configurare Directory Server” la pagina 186 pentru informaţii despre atributele de configurare a schemei.

Pentru a se conforma schemei, o intrare este verificată pentru următoarele condiţii:

Cu respect pentru clasele obiect:

- Trebuie să aibă cel puţin o valoare de tip de atribut ″objectClass″.
- Poate avea orice număr de clase obiect, inclusiv zero. Aceasta nu este o verificare, doar o clarificare. Nu există opţiuni pentru a dezactiva aceasta.
- Poate avea orice număr de clase obiect abstracte, dar doar ca rezultat al unei moşteniri de clasă. Aceasta înseamnă că pentru fiecare clasă obiect abstractă avută de intrare, are de asemenea şi-o clasă obiect structurală sau auxiliară care moşteneşte direct sau indirect de la clasa obiect abstarctă.
- Trebuie să aibă cel puţin o clasă obiect structurală.
- Trebuie să aibă exact o clasă obiect structurală imediată sau de bază. Asta înseamnă că dintre toate clasele obiect structurale furnizate cu intrarea, toate trebuie să fie superclase exact a uneia dintre ele. Cea mai derivată clasă obiect este numită clasa obiect ″imediată″ sau ″structurală de bază″ a intrării sau simplu clasa obiect ″structurală″ a intrării.
- Nu se poate modifica clasa obiect structurală imediată (pe ldap_modify).
- Pentru fiecare clasă obiect furnizată cu intrarea, se calculează setul tuturor superclaselor directe şi indirecte; dacă oricare dintre acele superclase nu este furnizată cu intrarea, atunci este adăugată automat.
- Dacă nivelul de verificare al schemei este setat pe **Versiunea 3 (strict)** toate superclasele structurale trebuie să fie furnizate. De exemplu, pentru a crea o intrare cu objectclass inetorgperson, trebuie specificate următoarele objectclasses: person, organizationalperson şi inetorgperson.

Validitatea tipurilor de atribute pentru o intrare este determinată după cum urmează:

- Setul de tipuri de atribute MUST pentru intrare este calculat ca uniune de seturi de tipuri de atribute MUST a tuturor claselor sale obiect, inclusiv clasele obiect moştenite implicit. Dacă setul de tipuri de atribute MUST pentru intrare nu este un subset al setului de tipuri de atribute conţinut de intrare, atunci intrarea este respinsă.
- Setul de tipuri de atribute MAY pentru intrare este calculat ca uniune de seturi de tipuri de atribute MAY a tuturor claselor sale obiect, inclusiv clasele obiect moştenite implicit. Dacă setul de tipuri de atribute conţinut de intrare nu este un subset al uniunii de seturi de tipuri de atribute MUST şi MAY pentru intrare, atunci intrarea este respinsă.
- Dacă oricare dintre tipurile de atribute definite pentru intrare sunt marcate ca NO-USER-MODIFICATION, atunci intrarea este respinsă.

Validitatea valorilor tipurilor de atribute pentru o intrare este determinată după cum urmează:

- Pentru fiecare tip de atribut conţinut de intrare, dacă tipul atributului este de valoare singulară şi intrarea are mai mult de-o valoare, atunci intrarea este respinsă.
- Pentru fiecare valoare de atribut a fiecărui tip de atribut conţinut de intrare, dacă sintaxa sa nu respectă rutina de verificare a sintaxei pentru sintaxa acelui atribut, atunci intrarea este respinsă.
- Pentru fiecare valoare de atribut a fiecărui tip de atribut conţinut de intrare, dacă lungimea sa este mai mare decât lungimea maximă alocată acelui tip de atribut, atunci intrarea este respinsă.

Validitatea DN-ului este verificată după cum urmează:

- Sintaxa este verificată pentru compatibilitate cu BNF pentru DistinguishedNames. Dacă nu este compatibilă, intrarea este respinsă.
- Este verificat că RDN este făcut doar cu tipuri de atribute care sunt valide pentru acea intrare.
- Este verificat că valorile pentru tipurile de atribute folosite în RDN apar în intrare.

Compatibilitate iPlanet

Analizorul folosit de Directory Server permite valorilor atributului ale tipurilor de atribute schemă (objectClasses şi attributeTypes) să fie specificate folosind gramatica iPlanet. De exemplu, descrs şi numeric-oids pot fi specificate între apostroafe (ca şi cum ar fi qdescrs). Totuşi, informaţiile schemei sunt disponibile tot timpul prin ldap_search. Imediat ce este realizată o singură modificare dinamică (folosind ldap_modify) pe o valoare de atribut dintr-un fişier, întregul fişier este înlocuit cu unul în care toate valorile de atribut urmează specificaţiile Directory Server. Deoarece analizorul folosit pe fişiere şi pe cererile ldap_modify este acelaşi, un ldap_modify care foloseşte gramatica iPlanet pentru valori de atribute este de asemenea tratat corect.

Când este făcută o interogare pe intrarea subschemei a serverului iPlanet, intrarea rezultată poate avea mai mult de o valoare pentru un OID dat. De exemplu, dacă un anumit tip de atribut are două nume (cum ar fi ’cn’ şi ’commonName’), atunci descrierea acelui tip de atribut este furnizată de două ori, o dată pentru fiecare nume. Directory Server poate analiza o schemă unde descrierea unui singur tip de atribut sau a unei clase obiect apare de mai multe ori cu aceeaşi descriere (mai puţin pentru NAME şi DESCR). Totuşi, când Directory Server publică schema, furnizează o singură descriere de un asemenea tip de atribut cu toate numele (numele scurt vine primul). De exemplu, uitaţi cum iPlanet descrie atributul nume comun:

```
( 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' )
```

Astfel o descrie Directory Server:

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

Directory Server suportă subtipuri. Dacă nu vreţi ca ’cn’ să fie un subtip de nume (care derivă de la standard), puteţi declara următoarele:

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

Primul nume (’cn’) este luat ca cel preferat sau ca nume scurt şi toate celelalte nume de după ’cn’ sunt luate ca nume alternative. Din acest punct înainte, şirurile ’2.3.4.3’, ’cn’ şi ’commonName’ (ca şi echivalentele lor insensibile la majusculă) pot fi folosite interschimbabil în schemă sau pentru intrări adăugate pentru director.

Timp generalizat şi UTC

Există notaţii diferite folosite pentru a desemna data şi ora şi alte informaţii despre timp. De exemplu, a patra zi din februarie a anului 1999 poate fi scrisă ca:

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

la fel ca şi multe alte notaţii.

Directory Server standardizează reprezentarea amprentei de timp impunând serverelor LDAP să suporte două sintaxe:

- Sintaxa Timp Generalizat, care ia forma:
  `YYYYMMDDHHMMSS[.|,fraction][(+|-HHMM)|Z]`

  Există 4 digiţi pentru an, 2 digiţi fiecare pentru lună, zi, oră, minut şi secundă şi o fracţiune opţională a unei secunde. Fără alte adăugări viitoare, o dată şi-o oră este asumată să fie într-un fus orar local. Pentru a indica că un timp este măsurat în Timp Coordonat Universal, adăugaţi o literă mare Z unei diferenţe de timp local. De exemplu:

  ```
  "19991106210627.3"
  ```

  care în timp local este 6 minute, 27,3 secunde după 9 p.m. pe 6 Noiembrie 1999.

  ```
  "19991106210627.3Z"
  ```

  care este timpul universal coordonat.

  ```
  "19991106210627.3-0500"
  ```

  care este timpul local ca în primul exemplu, cu o diferenţă de 5 ore în relaţie cu timpul universal coordonat.

  Dacă desemnaţi o fracţiune de secundă opţională, este necesar un punct sau o virgulă. Pentru diferenţierile de timp local, un '+' sau un '-' trebuie să preceadă valoarea oră:minute
- Sintaxa timpului universal, care ia forma:
  `YYMMDDHHMM[SS][(+ | -)HHMM)|Z]`

  Există 2 digiţi fiecare pentru an, lună, zi, oră, minut şi câmpuri opţionale pentru secundă. Ca şi în GeneralizedTime, poate fi specificată o diferenţă de timp opţională. De exemplu, dacă timpul local este a.m. pe 2 ianuarie 1999 şi timpul universal coordonat este 12 amiaza pe 2 ianuarie 1999, valoarea UTCTime ester:

  ```
  "9901021200Z"
       sau
  "9901020700-0500"
  ```

  De exemplu, dacă timpul local este a.m. pe 2 ianuarie 2001 şi timpul universal coordonat este 12 amiaza pe 2 ianuarie 2001, valoarea UTCTime ester:

  ```
  "0101021200Z"
       sau
  "0101020700-0500"
  ```

  UTCTime permite doar 2 digiţi pentru valoarea anului, de aceea nu se recomandă folosirea.

Regulile de potrivire suportate sunt generalizedTimeMatch pentru egalitate şi generalizedTimeOrderingMatch pentru inegalitate. Nu este permisă căutarea subşirului. De exemplu, sunt valide următoarele filtre:

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

Următoarele filtre nu sunt valide:

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

Publicare

i5/OS furnizează abilitatea ca sistemul să publice anumite informaţii la un director LDAP. Adică, sistemul va crea şi actualiza intrări LDAP reprezentând tipuri diferite de date.

i5/OS are suport încorporat pentru a publica următoarele informaţii pe un server LDAP:

Utilizatori

Când configuraţi i5/OS să publice informaţii tip Utilizatori la Directory Server, se exportă automat intrări din directorul de distribuţie al sistemului la Directory Server. Foloseşte API-ul QGLDSSDD pentru a face asta. Aceasta păstrează de asemenea directorul LDAP sincronizat cu modificările care sunt făcute în directorul de distribuţie sistem. Pentru informaţii despre API-ul QGLDSSDD, vedeţi "API-uri Directory Server" din subiectul Programare.

Publicarea utilizatorilor este de folos pentru furnizarea căutării LDAP accesului la informaţiile din directorul de distribuţia al sistemului (de exemplu pentru a furniza cărţii de adrese LDAP acces la clienţii de mail LDAP-activat POP3 cum ar fi Netscape Communicator sau Microsoft Outlook Express).

Utilizatorii publicaţi pot fi de asemenea folosiţi pentru a suporta autentificare LDAP cu alţi utilizatori publicaţi din directorul de distribuţie al sistemului şi cu alţi utilizatori adăugaţi la director din alte motive. Un utilizator publicat are un atribut uid care numeşte profilul utilizatorului şi nu are nici un atribut userPassword. Când se primeşte o cerere de legare pentru o intrare ca aceasta, serverul apelează securitatea i5/OS pentru a valida uid şi parola ca pe un profil utilizator şi parolă valide pentru acel profil. Dacă doriţi să folosiţi autentificarea LDAP şi aţi vrea ca utilizatorii existenţi i5/OS să fie capabili să se autentifice utilizându-şi parolele i5/OS, în timp ce utilizatorii non-i5/OS sunt adăugaţi în director manual, ar trebui să luaţi în considerare această caracteristică.

Informaţii sistem

Când configuraţi i5/OS pentru a publica informaţiile tip Sistem în Directory Server, următoarele tipuri de informaţii sunt publicate:

- Informaţii de bază despre această maşină şi despre ediţia sistemului de operare.
- Opţional, puteţi alege una sau mai multe imprimante pentru a publica, caz în care sistemul va păstra automat directorul LDAP sincronizat cu modificări care sunt făcute la acele imprimante pe sistem.

Informaţiile despre imprimantă care pot fi publicate includ:

- Locaţia
- Viteza în pagini pe minut
- Suport pentru duplex şi culoare
- Tip şi model
- Descriere

Această informaţie vine din descrierea imprimantei pe sistemul ce este publicat. Într-un mediu reţea, utilizatorii pot folosi această informaţie pentru a selecta o imprimantă. Informaţiile sunt mai întâi publicate când este selectată o imprimantă de publicat şi sunt actualizate când este oprit sau pornit un scriitor de imprimantă sau când se modifică descrierea unui dispozitiv imprimantă.

Partajări imprimantă

Când configuraţi i5/OS să publice partajări imprimantă, informaţiile despre partajările imprimantă Netserver iSeries selectate sunt publicate la serverul configurat Active Directory. Publicarea de partajări imprimantă la un Active Directory permite utilizatorilor să adauge imprimante iSeries la desktop-ul Windows 2000 cu vrăjitorul

Add Printer din Windows. Pentru a face asta în vrăjitorul Add Printer, specificaţi că doriţi să găsiţi o imprimantă în Windows 2000 Active Directory. Trebuie să publicaţi partajările imprimantă pe un server de directoare care suportă schema Microsoft's Active Directory.

Calitate a serviciului TCP/IP (QoS TCP/IP)

Serverul QoS TCP/IP poate fi configurat să folosească o politică partajată QoS definită într-un director LDAP folosind o schemă definită IBM. Agentul de publicare TCP/IP QoS este folosit de serverul QOS pentru a citi informaţiile politicii; defineşte serverul, informaţiile de autentificare şi unde în director sunt memorate informaţiile politicii.

Puteţi de asemenea crea o aplicaţie de a publica sau căuta alte tipuri de informaţii dintr-un director LDAP folosind acest cadru de lucru definind agenţi publicare suplimentari şi folosindu-vă de API-urile publicare ale directorului. Pentru informaţii suplimenater, vedeţi "API-uri Directory Server" din subiectul Programare

Replicare

Replicarea este o tehnică folosită de serverele de directoare pentru a îmbunătăţi performanţa şi încrederea. Procesul de replicare ţine datele în directoare multiple sincronizate.

Pentru informaţii despre cum se gestionează replicarea vedeţi "Gestionarea replicării" la pagina 103. Pentru informaţii suplimentare despre replicare vedeţi următoarele:

- "Privire generală replicare"
- "Terminologia replicării" la pagina 36
- "Acorduri de replicare" la pagina 37
- "Cum sunt memorate în server informaţiile de replicare" la pagina 38
- "Considerente de securitate pentru informaţii de replicare" la pagina 38

Privire generală replicare

Replicarea furnizează două mari avantaje:

- Redundanţă a informaţiilor - replicele fac copie de siguranţă a serverelor furnizoare.
- Căutări mai rapide - cererile de căutare pot fi împrăştiate de-a lungul mai multor servere diferite, toate având acelaşi conţinut, în loc de un singur server. Aceasta îmbunătăţeşte timpul de răspuns pentru completarea cererii.

Anumite intrări din director sunt identificate ca rădăcini a subarborilor replicaţi, adăugându-le ibm-replicationContext objectclass. Fiecare subarbore este replicat independent. Subarborele continuă în jos prin arborele de informaţii al directorului (DIT) până ce ajunge la intrările frunze (leaf) sau la alţi subarbori replicaţi. Intrările sunt adăugate sub rădăcina subarborelui replicat pentru a conţine informaţiile topologiei de replicare. Aceste intrări sunt una sau mai multe intrări grup de replicare, sub care sunt create subintrări de replicare. Asociate cu fiecare subintrare replică sunt înţelegerile de replicare care identifică serverele care sunt livrate (replicate la) de fiecare server, la fel ca şi definirea acreditărilor şi informaţiilor de planificare.

Prin replicare, o modificare făcută la un director este propagată la unul sau mai multe directoare suplimentare. Ca efect, o modificare la un director apare pe diferite directoare multiple. Directorul IBM suportă un model extins de replicare master-subordonat. Topologiile de replicare sunt expendate pentru a include:

- Replicarea subarborilor Arborelui de informaţii director (Directory Information Tree - DIT) la anumite servere
- O topologie multi-tier care mai este numită şi replicarea în cascadă
- Asignarea rolului server (master sau replică) de către subarbore.
- Mai multe servere master, care mai sunt numite şi replicarea peer la peer.

Avantajul replicării subarborilor este că o replică nu trebuie să replice întregul director. Poate fi replica unei părţi sau unui subarbore al directorului.

Modelul expandat modifică conceptul de master şi replică. Aceşti termeni nu se mai aplică pentru servere, ci mai degrabă pentru roluri avute de server cu privire la un anumit subarbore replicat. Un server poate acţiona ca master pentru unii subarbori şi ca replică pentru alţii. Termenul, master, este folosit pentru un server care acceptă actualizări de client pentru un subarbore replicat. Termenul, replică, este folosit pentru un server care acceptă doar actualizări de la alte servere desemnate ca furnizoare pentru subarborele replicat.

Există trei tipuri de directoare definite de funcţia: *master/peer*, *cascading* şi *read-only*.

Tabela 1. Roluri server

Directory	**Descriere**
Master/peer	Serverul master/peer conţine informaţiile de director master de unde actualizările sunt propagate la replici. Toate modificările sunt făcute şi apar pe serverul master, iar master-ul este responsabil pentru propagarea acestor modificări la replici. Pot exista mai multe servere care acţionează ca master pentru informaţiile director, cu fiecare master responsabil pentru actualizarea altor servere master şi replică. Acesteia i se mai spune şi replicarea peer. Replicarea peer poate îmbunătăţi performanţa şi încrederea. Performaţa este îmbunătăţită furnizând un server local să trateze actualizările dintr-o reţea distribuită larg. Încrederea este îmbunătăţită furnizând un server master copie de siguranţă gata să preia controlul imediat dacă eşuează master-ul principal. **Note:** 1. Serverele master replichează toate actualizările clientului, dar nu replichează actualizări primite de la alţi masteri. 2. Actualizările la aceeaşi intrare făcute de servere multiple poate cauza inconsistenţe în datele din director deoarece nu există o rezoluţie conflict.
Cascadare (înaintare)	Un server de cascadare este un server replică care replichează toate modificările trimise la el. Acesta contrastează cu un server master/peer deoarece un server master/peer replichează doar modificările care sunt făcute de clienţi conectaţi la acel server. Un server de cascadare poate elibera încărcătura de lucru de replicare din serverele master dintr-o reţea care conţine multe replici dispersate.
Replică (numai citire)	Un server suplimentar care conţine o copie a informaţiilor director. Replicele sunt copii ale master-ului (sau ale subarborelui a cărui replică este). Replica furnizează o copie de siguranţă a subarborelui replicat.

Dacă replicarea eşuează, este repetată chiar dacă masterul este repornit. Fereastra Gestionare cozi (Manage Queues) din unealta de administrare Web poate fi folosită pentru a verifica dacă există replicări eşuate.

Puteţi solicita actualizări pe un server replică, dar actualizarea este de fapt înaintată la serverul master prin returnarea unui referal clientului. Dacă actualizarea este un succes, serverul master trimite apoi actualizarea la replici. Până când masterul n-a terminat replicarea actualizării, modificarea nu este reflectată pe serverul replică unde a fost cerută iniţial. Modificările sunt replicate în ordinea în care sunt făcute pe master.

Dacă nu mai folosiţi o replică, trebuie să înlăturaţi acordul de replicare de la furnizor. Părăsind definiţia face ca serverul să pună în coadă toate actualizările şi să folosească spaţiul nenecesar din director. De asemenea, furnizorul continuă să încerce să contacteze consumatorul lipsă pentru a reîncerca să trimită datele.

Terminologia replicării

Unele terminologii folosite în descriere replicării:

Cascadare replicare
: O topologie de replicare în care există multiple nivele (tier) de servere. Un server peer/master replichează la un set de servere numai citire (înaintare) care în schimb replichează la alte servere. O astfel de topologie descarcă lucrul de replicare din serverele master.

Server consumator
: Un server care primeşte modificări prin replicare de la un alt server (furnizor).

Acreditări
Identifică metoda şi informaţiile necesare pe care le foloseşte furnizorul în legarea cu consumatorul. Pentru asocieri simple, aceasta include DN-ul şi parola. Acreditările sunt memorate într-o intrare DN despre care se specifică în acordul de replicare.

Server înaintare
Un server numai citire care replichează toate modificările trimise la el de un master sau peer. Cererile de actualizare client sunt transmise la serverul master sau peer.

Server master
Un server care este inscriptibil (poate fi actualizat) pentru un subarbore dat.

Subarbore imbricat
Un subarbore dintr-un subarbore replicat al directorului.

Server peer
Termenul folosit pentru un server master când există mai multe server master pentru un subarbore dat.

Acord replicare
Informaţii conţinute în directorul care defineşte ’connection’ sau ’replication path’ între două servere. Un server este numit furnizorul (cel care trimite modificările) şi celălalt este consumatorul (cel care primeşte modificările). Acordul conţine toate informaţiile necesare pentru realizarea unei conexiuni de la furnizor la consumator şi planificarea replicării.

Context replicare
Identifică rădăcina unui subarbore replicat. Clasa obiect auxiliară ibm-replicationContext poate fi adăugată unei intrări pentru a o marca ca rădăcina unei zone replicate. Informaţiile înrudite despre topologia replicării sunt menţinute într-un set de intrări create sub un context de replicare.

Grup replică
Prima intrare creată sub un context de replicare are objectclass ibm-replicaGroup şi reprezintă o colecţie de servere participante la replicare. Furnizează o locaţie de dorit pentru setarea ACL’s pentru protejarea informaţiiilor topologiei de replicare. Uneltele de administrare suportă]n mod curent un grup replică sub fiecare conţinut de replicare, numit **ibm-replicagroup=default**.

Subintrare replică
Sub o intrare de grup replică, una sau mai multe intrări cu objectclass ibm-replicaSubentry pot fi create; una pentru fiecare server care participă în replicare ca furnizor. Subintrarea replică identifică rolul pe care îl joacă serverul în replicare: master sau numai citire. Un server numai citire ar putea, în schimb, să aibă acorduri de replicare pentru a suporta replicarea în cascadă.

Subarbore replicat
O porţiune a DIT care este replicată de pe un server pe altul. În acest proiect, un subarbore dat poate fi replicat pe unele servere şi nu pe altele. Un subarbore poate fi inscriptibil pe un serber dat, în timp ce alţi subarbori pot fi numai citire.

Planificare
Replicarea poate fi planificată să aibă loc la anumite momente de timp, cu schimbările asupra furnizorului acumulate şi trimise într-un batch. Acordul de replicare conţine DN-ul pentru intrarea care furnizează planificarea.

Server furnizor
Un server care trimite modificări unui alt (consumator) server.

Acorduri de replicare

Un acord de replicare este o intrare în directorul cu clasa obiect **ibm-replicationAgreement** creată sub o subintrare replică pentru a defini replicarea de la server reprezentată de către subintrare la un alt server. Aceste obiecte sunt similare cu intrările replicaObject folosite de versiunile de dinainte Directory Server. Acordul de replicare conţine următoarele elemente:

- Un nume de utilizator prietenos, folosit ca atribut de numire pentru acord.

- Un URL LDAP specificând serverul, număr port şi dacă SSL trebuie folosit.
- ID-ul server consumator, dacă este cunoscut. Serverele de directoare dinainte de V5R3 nu au un ID server.
- DN-ul unui obiect conţinând acreditările folosite de furnizator pentru a-l lega de consumator.
- Un pointer DN opţional conţinând informaţiile de planificare pentru replicare. Dacă atributul nu este prezent, modificările sunt replicate imediat.

Numele prietenos al utilizatorului poate fi numele server al consumatorului sau un alt şir descriptiv.

ID-ul serverului consumator este folosit de GUI adiministrativ pentru a traversa topologia. Fiind dat ID-ul server al consumatorului, GUI poate găsi subintrarea corespunzătoare şi acordurile sale. Pentru a ajuta la impunerea corectidunii datelor, când furnizorul se leagă de consumator, extrage ID-ul server din rădăcina DSE şi o compară cu valoarea din acord. Se înregistrează o avertizare în istoric dacă ID-urile server nu se potrivesc.

Deoarece acordul de replicare poate fi replicat, se foloseşte un DN la obiectul de acreditări. Aceasta permite acreditărilor să fie memorate într-o zonă nereplicată a directorului. Replicarea obiectelor acreditări (din care trebuie să fie posibil de obţinut acreditările 'clear text') reprezintă o potenţială expunere de securitate. Sufixul cn=localhost este o locaţie implicită corespunzătoare pentru a crea obiecte de acreditări.

Clasele obiect sunt definite pentru fiecare dintre metodele de autentificare suportate:
- legătură simplă
- SASL
- mecanism EXTERN cu SSL
- Autentificare Kerberos

Puteţi desemna partea unui subarbore replicat care să nu fie replicată adăugând clasa auxiliară ibm-replicationContext la rădăcina subarborelui, fără să definiţi vreo subintrare replică

Notă: Unealta de administrare Web se referă de asemenea la acorduri ca 'queues' când se referă la setul de modificări care aşteaptă să fie replicate sub un acord dat.

Cum sunt memorate în server informaţiile de replicare

Informaţiile de replicare sunt memorate în director în trei locuri:
- Configuraţia serverului, care conţine informaţii despre cum se pot autentifica alte servere la acest server pentru a realiza replicarea (de exemplu, cui îi permite acest server să se comporte ca un furnizor).
- În director în vârful unui subarbore replicat. Dacă ″o=my company″ este vârfului unui subarbore replicat, un obiect numit ″ibm-replicagroup=default″ va fi creat direct sub el (ibm-replicagroup=default,o=my company). Sub obiectul ″ibm-replicagroup=default″ vor fi obiecte suplimentare care descriu replicele reţinute de servere ale subarborelui şi acordurile dintre servere.
- Un obiect numit ″cn=replication,cn=localhost″ este folosit pentru a conţine informaţii de replicare care sunt folosite de către un singur server. De exemplu, obiectul care conţine acreditările folosite de un server furnizor sunt necesare doar serverului furnizor. Acreditările pot fi puse sub ″cn=replication,cn=localhost″ făcându-le accesibile doar acelui server.

Considerente de securitate pentru informaţii de replicare

Revedeţi considerentele de securitate pentru următoarele obiecte:
- ibm-replicagroup=default: Accesul controlează pe acest control al obiectului cine poate vizualiza sau modifica informaţiile de replicare memorate aici. Implicit, acest obiect moşteneşte controlul accesului de la părintele său. Ar trebui să consideraţi setarea controlului de acces pe acest obiect pentru a restricţiona accesul la informaţiile de replicare. De exemplu, puteţi defini un grup care conţine utilizatori care vor gestiona replicarea. Acest grup poate fi făcut proprietarul obiectului ″ibm-replicagroup=default″ şi altor utilizatori cărora nu li s-a dat acces la obiect.
- cn=replication,cn=localhost: Există două considerente de securitate pentru acest obiect:

– Controlul accesului pe acest obiect controlează cine are permisiunea de a vizualiza sau actualiza obiectele memorate aici. Controlul de acces implicit permite utilizatorilor anonimi să citească majoritatea informaţiilor cu excepţia parolelor şi necesită autoritate de administrator pentru a adăuga, modifica sau şterge obiecte.
– Obiectele memorate în ″cn=localhost″ nusunt niciodată replicate pe alte servere. Puteţi pune acreditările de replicare în acest container de pe serverul care foloseşte acreditările şi ele nu vor fi accesibile altor servere. Alternativ, puteţi alege să puneţi acreditările sub obiectul ″ibm-replicagroup=default″ pentru ca serverele multiple să împartă aceleaşi acreditări.

Regiuni şi şabloane utilizator

Regiunea şi obiectele şablon găsite în unealta de administrare Web sunt folosite pentru a scuti utilizatorul de nevoia de a înţelege unele probleme LDAP.

O regiune identifică o colecţie de utilizatori şi grupuri. Specifică informaţii, într-o structură neierarhică de directoare, cum ar fi unde sunt utilizatorii şi unde se află şi grupurile. O regiune defineşte o locaţie pentru utilizatori (de exemplu, ″cn=users,o=acme,c=us″) şi creează utilizatori ca subordonaţi direcţi ai acelei intrări (de exemplu John Doe este creat ca ″cn=John Doe,cn=users,o=acme,c=us″). Puteţi defini regiuni multiple şi să le daţi nume familiare (de exemplu Utilizatori Web). Numele familiar poate fi folosit de către persoanele care creează şi menţin utilizatorii.

un şablon descrie cum arată un utilizator. Specifică clasele obiect care sunt folosite când se creează utilizatori (clasa obiect structurală şi clase auxiliare pe care le doriţi). Un şablon specifică de asemenea dispunerea panourilor folosite pentru a crea sau edita utilizatori (de exemplu, nume de fişe, valori implicite şi atribute de apărut pe fiecare fişă).

Când adăugaţi o nouă regiune, creaţi un obiect ibm-realm în director. Obiectele ibm-realm păstrează urma proprietăţilor regiunii cum ar fi unde sunt definiţi utilizatori şi grupuri şi ce şablon trebuie folosit. Obiectul ibm-realm poate indica o intrare de director existent care este părintele utilizatorilor sau poate indica spre sine (implicit), făcându-l containerul pentru noii utilizatori. De exemplu, puteţi avea un container existent cn=users,o=acme,c=us şi creaţi o regiune numită users în altă parte în director (poate un obiect container numit cn=realms,cn=admin stuff,o=acme,c=us) care identifică cn=users,o=acme,c=us ca locaţie pentru utilizatori şi grupuri. Aceasta creează un obiect 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
```

Sau, dacă nu a existat cn=users,o=acme,c=us object, puteţi crea regiunea users sub o=acme,c=us care să indice spre sine.

Administratorul directorului este responsabil pentru gestionarea şabloanelor utilizatorului, regiunilor şi grupurilor de administrare a regiunii. După ce este creat o regiune, membrii grupului de administrare a acelei regiuni sunt responsabili cu gestionarea utilizatorilor şi grupurilor din acea regiune.

Pentru informaţii suplimentare despre gestionarea regiunilor şi a şabloanelor utilizatorilor, vedeţi “Regiuni şi şabloane utilizator” la pagina 140.

Consideraţii suport limbă naţională (NLS)

Fiţi conştienţi de următoarele considerente NLS:
- Datele sunt transferate între serverele LDAP şi clienţii în format UTF-8. Toate caracterele ISO 10646 sunt permise.
- Directory Server foloseşte metoda de mapare UTF-16 pentru a memora date în baza de date.
- Serverul şi clientul fac comparaţii de şiruri ţinând cont de majuscule. Algoritmii majuscule nu vor fi corecţi pentru toate limbile (Locale-urile).

Pentru informaţii suplimentare despre UCS-2, vedeţi “Globalization ” din subiectul Planificare.

Referalii directorului LDAP

Referalii permit mai multor Directory Server să lucreze în echipe. Dacă DN-ul pe care un client îl cere nu este într-un director, serverul poate trimite automat cererea la orice alt server LDAP.

Directory Server vă permite să folosiţi două tipuri diferite de referali. Puteţi specifica servere referal implicite, unde serverul LDAP va trimite clienţii de câte ori un DN nu este în director. Puteţi folosi de asemenea clientul dumneavoastră LDAP pentru a adăuga intrări la serverul de directoare care are referral ca objectClass. Aceasta vă permite să specificaţi referali bazaţi pe acel DN specific cerut de client.

Notă: Cu Directory Server, obiectele referal trebuie să conţină doar un nume distinctiv (dn), un objectClass (objectClass) şi un atribut referal (ref). Vedeţi “ldapsearch” la pagina 171 pentru un exemplu care ilustrează această restricţie.

Serverele referal sunt înrudite îndeaproape de serverele replică. Deoarece datele pe serverele replică nu pot fi modificate de clienţi, replica trimite orice cereri de a schimba datele director la serverul master.

Tranzacţii

Puteţi configura Directory Server pentru a pemite clienţilor să folosească tranzacţii. (Pentru informaţii suplimentare despre configurarea setărilor de tranzacţie, vedeţi “Specificarea setărilor de tranzacţie” la pagina 97.) O tranzacţie este un grup de operaţii director LDAP care sunt tratate ca o unitate. Nici una din operaţiile individuale LDAP care alcătuiesc o tranzacţie nu sunt permanente până când toate operaţiile din tranzacţie s-au terminat cu succes şi tranzacţia a fost comisă. Dacă vreo operaţie a eşuat sau tranzacţia este oprită, cealalte operaţii sunt refăcute. Această capabilitate poate ajuta utilizatorii să pastreze operaţiile LDAP organizate. De exemplu, un utilizator poate seta o tranzacţie pe clientul său care va şterge mai multe intrări director. Dacă clientul îşi pierde conexiunea la server în timpul tranzacţiei, nici una din intrări nu este ştearsă. Astfel, utilizatorul poate porni simplu tranzacţia din nou decât să trebuiască să verifice care intrări au fost şterse cu succes.

Următoarele operaţii LDAP pot fi parte a unei tranzacţii:

- adăugare
- modificare
- modificare RDN
- ştergere

Notă: Nu includeţi în tranzacţii modificări la schema directorului (sufixul cn=schema). Deşi este posibil să le includeţi, nu pot fi retrase dacă tranzacţia eşuează. Aceasta poate cauza ca serverul de directoare să întâmpine probleme impredictibile.

Securitate Directory Server

Vedeţi următoarele pentru informaţii suplimentare despre securitatea Directory Server:

- “Auditare” la pagina 41
- “SSL (Secure Sockets Layer) şi TLS (Transport Layer Security) cu Directory Server” la pagina 41
- “Autentificare Kerberos cu Directory Server” la pagina 41)
- “Grupuri şi roluri” la pagina 42
- “Liste de control al accesului” la pagina 48
- “Drept de proprietate a obiectelor directorului LDAP” la pagina 59
- “Politică parolă” la pagina 59
- “Autentificare” la pagina 63

Auditare

Directory Server suportă auditare de securitate OS/400. Elementele care pot fi auditate includ următoarele:

- Legări şi dezlegări de la serverul de directoare.
- Modificări la permisiunile obiectelor directorelor LDAP.
- Modificări la proprietatea obiectelor directoarelor.
- Crearea, ştergerea, căutarea şi modificarea obiectelor directoarelor LDAP.
- Modificări la parola de administrator şi actualizarea numelor distinctive (DN)
- Modificări ale parolelor utilizatorilor.
- Importări şi exportări de fişiere.

Puteţi avea nevoie să faceţi modificări la setările de auditare ale i5/OS înainte ca auditarea intrărilor de directoare să funcţioneze. Dacă variabila sistem QAUDCTL are specificat *OBJAUD, puteţi activa auditarea obiectelor prin

Navigator iSeries. Pentru informaţii suplimentare despre auditare, vedeţi legătura *Security - Reference*  sau la subiectul " Security auditing".

SSL (Secure Sockets Layer) şi TLS (Transport Layer Security) cu Directory Server

Pentru a comunica cu Directory Server mai în siguranţă. Directory Server poate folosi securitatea SSL.

Pentru a folosi SSL cu Directory Server, trebuie să aveţi unul din produsele Cryptographic Access Provider (5722-ACx) instalate pe sistemul dumneavoastră. Dacă vreţi să folosiţi SSL de la Navigator iSeries, trebuie să aveţi unul din produsele Client Encryption (5722-CEx) instalate pe PC-ul dumneavoastră. Aveţi nevoie de acest software dacă vreţi să faceţi una din următoarele:

- Să configuraţi şi să administraţi Directory Server de la staţia dumneavoastră de lucru folosind o conexiune SSL. Aceasta include operaţiile care le realizaţi de la Navigator iSeries.
- Pentru a folosi o conexiune SSL cu aplicaţii pe care le creaţi cu API-uri clientului LDAP.

SSL este standardul pentru securitatea Internet. Puteţi folosi SSL pentru a comunica cu clienţi LDAP la fel şi cu servere replică LDAP. Puteţi folosi autentificarea client în plus la autentificarea server pentru a furniza securitate suplimentară la conexiunile dumneavoastră SSL. Autentificarea client cere ca clientul LDAP să prezinte un certificat digital care confirmă clienţii identitatea la server înainte ca o conexiune să fie stabilită.

Pentru a folosi SSL, trebuie să aveţi opţiunea Digital Certificate Manager (DCM), opţiunea 34 din i5/OS, instalată pe sistemul dumneavoastră. DCM furnizează o interfaţă pentru ca să creaţi şi să gestionaţi certificatele digitale şi memorările de certificate. Vedeţi subiectul "Digital Certificate Manager" pentru informaţii despre certificate digitale şi folosind DCM. Pentru informaţii despre SSL pe iSeries, vedeţi subiectul "SSL (Secure Sockets Layer)". Pentru informaţii despre TLS pe serverul iSeries, consultaţi Protocoale SSL şi Transport Layer Security (TLS) suportate.

Autentificare Kerberos cu Directory Server

Directory Server vă permite să folosiţi autentificarea Kerberos. Kerberos este un protocol de autentificare în reţea care foloseşte chei criptografice pentru a furniza o autentificare puternică aplicaţiilor client/server.

Pentru a activa autentificarea Kerberos, trebuie să aveţi unul din produsele Cryptographic Service Provider (5722AC2 sau 5722AC3) instalat pe sitemul dumneavoastră. Trebuie să aveţi de asemenea serviciul de autentificare al reţelei configurat.

Suportul Kerberos al Directory Server furnizează suport pentru mecanismul GSSAPI SASL. Aceasta activează clienţii Directory Server şi Windows 2000 LDAP să folosească autentificarea Kerberos cu Directory Server.

Numele de principal Kerberos pe care îl foloseşte serverul are următoarea formă:

```
nume-serviciu/nume-gazdă@realm
```

nume-service este ldap (ldap trebuie să fie cu litere mici), nume-gazdă este numele TCP/IP complet calificat al sistemului, iar regiune este regiunea implicită specificată în configuraţia sistemului Kerberos.

De exemplu, pentru un sistem numit my-as400 în domeniul TCP/IP acme.com , cu o regiune Kerberos implicită ACME.COM, numele Kerberos principal al serverului LDAP ar fi ldap/my-as400.acme.com@ACME.COM . Domeniul implicit Kerberos este specificat în fişierul de configurarea Kerberos (implicit, /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) cu directiva default_realm (default_realm = ACME.COM). Serverul de directoare nu poate fi configurat să folosească autentificarea Kerberos dacă nu a fost configurat nici un domeniu implicit.

Când este folosită autentificarea Kerberos, Directory Server asociază un nume distinctiv (DN) cu conexiunea care determină accesul la datele directorului. Puteţi alege să aveţi asociat DN-ul serverului cu una din următoarele metode:

- Serverul poate crea un DN pe baza ID-ului Kerberos. Când alegeţi această opţiune o identitate Kerberos de forma principal@realm generează un DN de forma ibm-kn=principal@realm. ibm-kn= este echivalent cu ibm-kerberosName=.
- Serverul poate căuta directorul pentru un nume distinctiv (DN) care conţine o intrare pentru principalul şi domeniul Kerberos. Când alegeţi această opţiune, serverul caută în director o intrare care specifică această identitate Kerberos.

Trebuie să aveţi un fişier tabelă de chei (keytab) care conţine o cheie pentru principalul serviciului LDAP. Consultaţi subiectul Centru de informare Serviciul de autentificare în reţea din Securitate, pentru mai multe informaţii despre Kerberos pe pe serverul iSeries. Secţiunea Configurarea serviciului autentificare în reţea conţine informaţii despre adăugarea informaţiilor în fişiere tabelă de chei.

Grupuri şi roluri

Un grup este o listă, o collcţie de nume. Un grup poate fi folosit în atributele **aclentry**, **ibm-fliterAclEntry** şi **entryowner** pentru a controla accesul sau în anumite folosiri de aplicaţii cum ar fi trmimiterea prin poştă a unei liste; vedeţi “Liste de control al accesului” la pagina 48. Grupurile pot fi definite ca statice, dinamice sau imbricate. Pentru informaţii despre cum să lucraţi cu grupuri, vedeţi “Gestionarea utilizatorilor şi grupurilor” la pagina 137.

Rolurile sunt similare grupurilor prin faptul că sunt reprezentate în director de un obiect. Suplimentar, rolurile conţin un grup de DN-uri.

Vedeţi următoarele pentru informaţii suplimentare:

- “Grupuri statice”
- “Grupuri dinamice” la pagina 43
- “Grupuri imbricate” la pagina 44
- “Grupuri hibride” la pagina 44
- “Determinarea apartenenţei la grup” la pagina 44
- “Clase obiecte grup pentru grupuri imbricate şi dinamice” la pagina 46
- “Tipuri atribut grup” la pagina 47
- “Roluri” la pagina 47

Grupuri statice

Un grup static defineşte fiecare membru individual folosind clasa obiect structurală **groupOfNames**, **groupOfUniqueNames**, **accessGroup** sau **accessRole**; sau clasa obiect auxiliară **ibm-staticgroup**. Aceste clase obiect necesită atributul **membru** (sau uniqueMember în cazul groupOfUniqueNames). Un grup static folosind clasele obiect structurale **groupOfNames** sau **groupOfUniqueNames** trebuie să aibă cel puţin un membru. Un grup folosind clasele obiect structurael **accessGroup** sau **accessRole** poate fi gol. Un grup static poate fi de asemenea definit folosind clasa obiect auxiliară: **ibm-staticGroup**, care nu necesită atributul **member** şi de aceea poate fi gol.

O intrare grup tipică este:

```
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
```

Fiecare obiect grup conţine un atribut multivaloric conţinând DN-uri membri.

Asupra ştergerii unui grup de acces, acesta este de asemenea şters din toate ACL-urile în care a fost aplicat.

Grupuri dinamice

Un grup defineşte membrii săi diferit de un grup static. În loc să le asculte individual, intrările grupului dinamic îşi definesc membrii folosind o căutare LDAP. Grupul dinamic foloseşte clasa obiect structurală **groupOfURLs** (sau clasa obiect auxiliară **ibm-dynamicGroup**) şi atributul, **memberURL** pentru a defini căutarea folosind o sintaxă LDAP URL simplificată.

```
 ldap:///< DN
de bază al căutării> ? ? <scopul căutării> ?
<filtru de căutare>
```

Notă: Aşa cum ilustrează exemplul, numele gazdă nu trebuie să fie prezent în sintaxă. Parametrii rămaşi sunt ca o sintaxă LDAP URL normală. Fiecare câmp parametru trebuie să fie separat de un ?, chiar dacă nu este specificat nici un parametru. Normal, o listă de atribute de returnat ar fi inclusă între DN-ul de bază şi scopul căutării. Acest parametru nu este folosit de asemenea de către server când se determină apartenenţa dinamică, şi astfel poate fi omis, totuşi, separatorul **?** trebuie să fie prezent încă.

unde:

DN de bază al căutării
Este punctul din care începe căutarea în director. Poate fi sufixul sau rădăcina directorului cum ar fi **ou=Austin**. Acest parametru este necesar.

scopul căutării
Specifică extensia căutării. Scopul implicit este baza.

- **bază** Întoarce informaţii doar despre DN-ul bazei specificat în URL
- **unul** Întoarce informaţii despre intrări de pe nivelul de sub DN-ul bază specificat în URL. Nu include intrarea bazei.
- **sub** Întoarce informaţii despre intrări la toate nivelele de mai jos şi include DN-ul bazei.

filtru căutare
Este filtru pe care doriţi să-l aplicaţi intrărilor din scopul căutării. Vedeţi “opţiunea de filtrare ldapsearch” la pagina 174 pentru informaţii despre sintaxa filtrului de căutare. Implicit este objectclass=*

Căutarea de membri dinamici este întotdeauna internă pentru server, deci spre deosebire de un LDAP URL întreg, un nume gazdă şi un număr de port nu este niciodată specificat şi protocolul este întotdeauna **ldap** (niciodată **ldaps**). Atributul **memberURL** poate conţine orice fel de URL, dar serverul foloseşte doar **memberURL**s începând cu **ldap:///** pentru a determina apartenenţă dinamică.

Exemple

O singură intrare în care scopul este implicit bază iar filtrul este implicit objectclass=*:

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

Toate intrările care sunt cu un nivel sub cn=Employees şi filtrul este implicit objectclass=*:

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

Toate intrările care sunt sub o-Acme cu objectclass=person:

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

În funcţie de clasele de obiecte pe care le folosiţi pentru a defini intrări utilizator, acele intrări ar putea să nu conţină atribute care sunt corespunzătaore pentru determinarea apartenenţei la un grup. Puteţi folosi clasa de obiecte auxiliară, **ibm-dynamicMember**, pentru a extinde intrările dumneavoastră utilizator ca să includă atributul **ibm-group** . Acest atribut vă permite să adăugaţi valori arbitrare la intrările dvs. utilizator pentru a servi ca destinaţii pentru filtrele grupurilor dvs. dinamice. De exemplu:

Membrii acestui grup dinamic sunt intrări aflate direct sub intrarea cn=users,ou=Austin care au atributul ibm-group al GROUP1:

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

Iată un exemplu de membru al 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
```

Grupuri imbricate

Imbricarea grupurilor permite crearea de relaţii ierarhice care pot fi folosite pentru a defini apartenenţa de grup moştenită. Un grup imbricat este definit ca o intrare grup fiu al cărei DN este referit de un atribut conţinut într-o intrare de grup părinte. Un grup părinte este creat prin extinderea uneia dintre clasele de obiecte grup structurală (**groupOfNames**, **groupOfUniqueNames**, **accessGroup**, **accessRole** sau **groupOfURLs**) cu adăugarea clasei de obiecte auxiliară **ibm-nestedGroup**. După extinderea grupului imbricat, pot fi adăugate zero sau mai multe atribute **ibm-memberGroup** , cu valorile lor setate la DN-urile grupurile fii imbricate. De exemplu:

```
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
```

Introducerea de cicli în ierarhia de grupuri imbricate nu este permisă. Dacă se detrmină că o operaţie de grup imbricat produce o referinţă ciclică, ori în mod direct ori prin moştenire, este considerată o violare a unei restricţii şi de aceea actualizarea intrării eşuează.

Grupuri hibride

Oricare dintre clasele de obiecte grup structurale poate fi extinsă astfel încât apartenenţa la un grup să fie descrisă printr-o combinaţie de tipuri de membru static, dinamic şi imbricat. De exemplu:

```
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
```

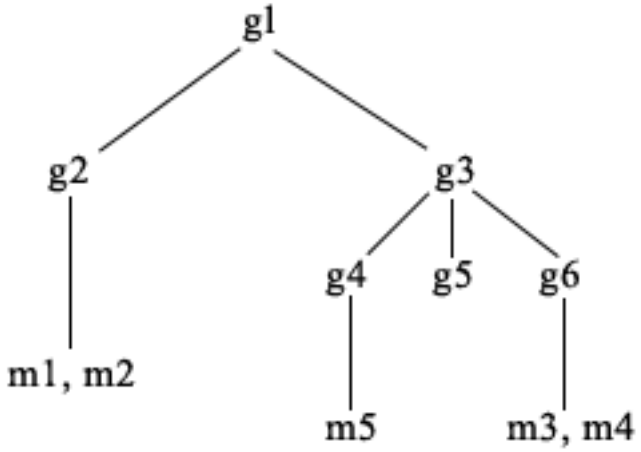
Determinarea apartenenţei la grup

Pot fi folosite două atribute operaţionale pentru a interoga apartenenţa la un grup agregat. Pentru o intrare grup dată, atributul operaţional **ibm-allMembers** enumerează setul agregat al apartenenţei grup, inclusiv membri statici, dinamici

şi imbricaţi, aşa cum este descris de ierarhia de grup imbricat. Pentru o intrare utilizator dată, atributul operaţional **ibm-allGroups** enumerează setul agregat al grupurilor, inclusiv grupurile strămoş, de care aparţine utilizatorul.

Un solicitant poate primi doar un subset al datelor totale cerute, în funţie de modul în care au fost setate ACL-urile pentru date. Oricine poate cere atributele operaţionale **ibm-allMembers** şi **ibm-allGroups**, dar setul de date întors conţine date doar pentru intrările LDAP şi atributele pentru care solicitantul are drepturi de acces. Utilizatorul care cere atributul **ibm-allMembers** sau **ibm-allGroups** trebuie să aibă acces la valorile atributelor **member** sau **uniquemember** pentru grupul şi pentru grupurile imbricate pentru a putea vedea membrii statici şi trebuie să poată efectua căutările specificate în valorile atributului **memberURL** pentru a putea vedea membrii dinamici. De exemplu:

Exemple ierarhie



Pentru acest exemplu, **m1** şi **m2** sunt în atributul membru al **g2**. ACL-ul pentru **g2** pemite **user1** să citească atributul de membru, dar **user 2** nu are acces la atributul membru. Intrarea LDIF pentru intrarea **g2** este următoarea:

```
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
```

Intrarea **g4** foloseşte intrarea ACL implicită, care permite atât lui **user1** şi **user2** să citească atributul membrului său. LDIF-ul pentru intrarea **g4** este după cum urmează:

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

Intrarea **g5** este un grup dinamic, care îşi obţine membrii din atributul memberURL. LDIF-ul pentru intrarea **g5** este următorul:

```
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))
```

Intrările **m3** şi **m4** sunt membri ai grupului **g5** deoarece ei corespund cu **memberURL**. ACL-ul pentru intrarea **m3** permite atât lui **user1** cât şi lui **user2** să o caute. ACL-ul pentru intrările **m4** nu permite lui **user2** să o caute. LDIF-ul pentru **m4** este următorul:

```
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
```

Exemplu 1:

Utilizatorul 1 face o căutare pentru a obţine toţi membrii grupului **g1**. Utilizatorul 1 are acces la toţi membrii, astfel că toţi vor fi returnaţi.

```
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
```

Exemplul 2:

Utilizatorul 2 face o căutare pentru a obţine toţi membrii grupului **g1**. Utilizatorul 2 nu are acces la membrii **m1** sau **m2** deoarece ei nu au acces la atributul membru pentru grupul **g2**. Utilizatorul 2 are acces la atributul membru pentru **g4** şi de aceea are acces la membrul **m5**. Utilizatorul 2 poate efectua căutarea în grupul **g5** memberURL pentru intrarea **m3**, pentru ca membrii să fie menţionaţi, dar nu poate efectua căutarea lui **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
```

Exemplu 3:

Utilizatorul 2 face o căutare pentru a vedea dacă **m3** este un membru al grupului **g1**. Utilizatorul 2 are acces pentru a face această căutare, deci căutarea arată că **m3** este un membru al grupului **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
```

Exemplu 4:

Utilizatorul 2 face o căutare pentru a vedea dacă **m1** este un membru al grupului **g1**. Utilizatorul 2 nu are acces la atributul membru, deci căutarea nu arată că **m1** este un membru al grupului **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
```

Clase obiecte grup pentru grupuri imbricate şi dinamice

ibm-dynamicGroup

Această clasă auxiliară permite atributul opţional **memberURL**. Folosiţi-o cu o clasă structurală precum **groupOfNames** pentru a crea un grup hibrid atât cu membri statici cât şi dinamici.

ibm-dynamicMember

Această clasă auxiliară permite atributul opţional **ibm-group**. Folosiţi-o ca un atribut filtru pnetru grupurile dinamice.

ibm-nestedGroup

Această clasă auxiliară permite atributul opţional **ibm-memberGroup** . Folosiţi-o cu o clasă structurală precum **groupOfNames** pentru a permite sub-grupurilor să fie imbricate în cadrul grupului părinte.

ibm-staticGroup

Această clasă auxiliară permite atributul opţional **member**. Folosiţi-o cu o clasă structurală precum **groupOfURLs** pentru a crea un grup hibrid atât cu membri statici cât şi dinamici.

Notă: **ibm-staticGroup** este singura clasă pentru care **member** este *optional*, toate celelalte clase având **member** să necesite cel puţin un membru.

Tipuri atribut grup

ibm-allGroups

Arată toate grupurile cărora le aparţine o intrare. O intrare poate fi un membru direct prin atributele **member**, **uniqueMember** sau **memberURL** sau indirect prin atributul **ibm-memberGroup**. Acest atribut operaţional **Read-only** nu este permis într-un filtru de căutare. Atributul **ibm-allGroups** poate fi folosit într-o cerere de comparaţie pentru a determoina dacă o intrare este membru al grupului dat. De exemplu, pentru a determina dacă ″cn=john smith,cn=users,o=my company″ este membru al grupului ″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

Arată toţi membrii unui grup. O intrare poate fi un membru direct prin atributele **member**, **uniqueMember** sau **memberURL** sau indirect prin atributul **ibm-memberGroup** . Acest atribut operaţional **Read-only** nu este permis într-un filtru de căutare. Atributul **ibm-allMembers** poate fi folosit într-o cerere de comparaţie pentru a determoina dacă un DN este membru al grupului dat. De exemplu, pentru a determina dacă ″cn=john smith,cn=users,o=my company″ este membru al grupului ″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

Este un atribut pe care îl are clasa auxiliară **ibm-dynamicMember** . Folosiţi-l pentru a defini valori arbitrare pentru a controla aparteneţa intrării la grupuri dinamice. De exemplu, adăugaţi valoarea ″Bowling Team″ pentru a include intrarea în orice **memberURL** care are filtrul ″ibm-group=Bowling Team″.

ibm-memberGroup

Este un atribut pe care îl are clasa auxiliară **ibm-nestedGroup** . Identifică subgrupurile unei intrări grup părinte. Membrii tuturor astfel de subgrupuri sunt consideraţi membri ai grupului părinte când sunt prelucrate ACL-urile sau atributele operaţionale **ibm-allMembers** şi **ibm-allGroups** . Intrările subgrup *nu* sunt ele însele membri . Apartenenţa imbricată este recursivă.

member

Identifică numele distinctive pentru fiecare membru al grupului. De exemplu: member: cn=John Smith, dc=ibm, dc=com.

memberURL

Identifică un URL asociat cu fiecare membru al unui grup. Poate fi folosit orice tip de URL etichetat. De exemplu: memberURL: ldap:///cn=jsmith,dc=ibm,dc=com .

uniquemember

Identifică un grup de nume asociate cu o intrare în care fiecărui nume i-a fost acordat un uniqueIdentifier pentru a-i asigura unicitatea. O valoare pentru atributul uniqueMember este un DN urmat de uniqueIdentifier. De exemplu: uniqueMember: cn=John Smith, dc=ibm, dc=com 17.

Roluri

Autorizarea bazată pe roluri este un complement conceptual al autorizării bazate pe grup şi este folositoare în unele cazuri. Ca membru al unui rol, aveţi autoritatea să faceţi tot ce este necesar pentru rol pentru a realiza sarcina. Spre

deosebire de un grup, un rol vine cu un set implicit de permisiuni. Nu există vreo presupunere încorporată legată de permisiunile care sunt obţinute (sau pierdute) prin apartenenţa la un grup.

Rolurile sunt similare grupurilor prin faptul că sunt reprezentate în director de un obiect. Suplimentar, rolurile conţin un grup de DN-uri. Rolurile care urmează să fie folosite pentru controlul accesului trebuie să aibe objectclass 'AccessRole'. Clasa de obiecte 'Accessrole' este o subclasă a clasei de obiecte 'GroupOfNames'.

De exemplu, dacă avem o colecţie de DN-uri precum 'sys admin', prima dvs. reacţie ar fi să vă gândiţi la ele ca 'grupul sys admin' (deoarece grupurile şi utilizatorii sunt cele mai familiare tipuri de atribute de privilegiu). Oricum, deoarece există un set de permisiuni pe care vă aşteptaţi să le primiţi ca membru al 'sys admin', colecţia de DN-uri poate fi definită mai precis ca 'rolul sys admin'.

Liste de control al accesului

Listele de control al accesului (Access control list - ACL) oferă un mijloc de a proteja informaţiile stocate într-un director LDAP. Administratorii folosesc ACL-urile pentru a restricţiona accesul la diverse porţiuni ale directorului sau la anumite intrări din director. Schimbările făcute asupra fiecărei intrări sau atribut din director pot fi controlate prin folosirea ACL-urilor. Un ACL pentru o intrare sau un atribut date pot fi moştenite de la intrarea ei părinte sau pot fi definite în mod explicit.

Este cel mai bine să proiectaţi strategia de control al accesului prin crearea grupurilor de utilizatori pe care le veţi folosi când setaţi accesul pentru obiecte şi atribute. Setaţi apartenenţa şi accesul la cel mai înalt nivel posibil din arbore şi lăsaţi controalele să fie moştenite în jos în arbore.

Atributele operaţionale asociate cu controlul accesului, precum entryOwner, ownerSource, ownerPropagate, aclEntry, aclSource şi aclPropagate sunt neobişnuite prin faptul că sunt asociate logic cu fiecare obiect, dar pot avea valori care depind de alte obiecte de mai sus din arbore. În funcţie de cum sunt stabilite, valorile acestor atribut pot fi explicite pentru un obiect sau pot fi moştenite de la un strămoş.

Modelul de control al accesului defineşte două seturi de atribute: informaţiile de control al accesului (Access Control Information - ACI) şi informaţiile entryOwner. ACI defineşte drepturile de acces acordate unui subiect specificat referitor la operaţiile pe care le pot efectua pe obiectele pentru care se aplică. Atributele aclEntry şi aclPropagate se aplică la definiţia ACI. Informaţia entryOwner defineşte ce subiecte pot defini ACI-ul pentru obiectul intrare asociat. Atributele entryOwner şi ownerPropagate se aplică la definiţia entryOwner.

Sunt două tipuri de liste de control al accesului din care puteţi alege: ACL-uri bazate pe filtru şi ACL-uri non-filtrate. ACL-urile non-filtrate se aplică explicit asupra intrării director care le conţine, dar pot fi propagate la nici una sau la toate intrările ei descendente. ACL-urile bazate pe filtru diferă prin aceea că ele implică o comparaţie bazată pe filtru, folosind un filtru de obiect specificat, pentru a corespunde cu obiectele destinaţie cu accesul efectiv care le se aplică.

Folosind ACL-uri, administratorii pot restricţiona accesul la diverse porţiuni ale directorului, la anumite intrări director şi, în funcţie de numele atributului sau de clasa de acces la atribut, atributele conţinute în intrări. Fiecare intrare din directorul LDAP are un set de ACI-uri asociate. În conformitate cu modelul LDAP, informaţiile de ACI şi entryOwner sunt reprezentate ca perechi atribut-valoare. Mai mult, este folosită sintaxa LDIF pentru a administra aceste valori. Atributele sunt:

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

Pentru informaţii despre cum să lucraţi cu ACL-uri, vedeţi "Gestionarea listelor de control al accesului (ACL-uri)" la pagina 147. Pentru informaţii suplimentare, vedeţi următoarele:

- "ACL-uri filtrate" la pagina 49

ACL-uri filtrate

ACL-urile bazate pe filtru implică o comparaţie bazată pe filtru, folosind un filtru de obiect specificat, pentru a corespunde cu obiectele destinaţie cu accesul efectiv care le se aplică.

ACL-urile bazate pe filtru se propagă în mod inerent asupra oricăror obiecte care corespund în urma comparaţiei din subarborele asociat. Din acest motiv, atributul aclPropagate, care este folosit pentru a opri propagarea ACL-urilor non-filtru, nu se aplică la noile ACL-uri bazate pe filtru.

Comportamentul implicit al ACL-urilor bazate pe filtru este să se acumuleze de la intrarea container cea mai de jos, în sus de-a lungul lanţului de intrări strămoş, până la intrarea container cea mai de sus din DIT. Accesul efectiv este calculat ca reuniune a drepturilor de acces acordate sau negate, de către intrările strămoş constituente. Există totuşi o excepţie de la acest comportament. Pentru compatibilitatea cu facilitatea de replicare a subarborelui şi pentru a permite un control administrativ mai mare, este folosit un atribut plafon ca mijloc de a opri acumularea la intrarea în care este conţinut.

Este folosit un set nou de atribute de control al accesului, special pentru suportul ACL bazat pe filtre, în loc de a îmbina caracteristicile bazate pe filtre în ACL-urile existente nebazate pe filtru. Atributele sunt:

- ibm-filterAclEntry
- ibm-filterAclInherit

Atributul ibm-filterAclEntry are acelaşi format ca şi aclEntry, cu adăugarea unei componente filtru de obiecte. Atributul plafon asociat este ibm-filterAclInherit. În mod implicit, el este setat pe true. Când este setat la false, el termină acumularea.

Sintaxa atributului de control acces

Fiecare dintre aceste atribute pot fi administrate folosind notaţia LDIF. Sintaxa pentru noile atribute ACL bazate pe filtre sunt versiuni modificate ale atributelor ACL curente, nebazate pe filtre. Următoarele definesc sintaxa pentru atributele ACI şi entryOwner folosind 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> ::= nume distinctiv descris ca în RFC 2251, secţiunea 4.1.3.

<pseudoDn> ::= "group:cn=anybody" | "group:cn=authenticated" |
                       "access-id:cn=this"
<object filter> ::= filtru căutare şir definit ca în RFC 2254, secţiunea 4
                                (potrivire extensibilă nu este suportată).
<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> ::= nume attributeType descris ca în RFC 2251, secţiunea 4.1.4.
                       (OID sau şir alpha-numeric cu conducere
                        alfabet, "-" and ";" permis)

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

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

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

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

AclEntry şi ibm-filterAclEntry

Subiect: Un subiect (entitatea care solicită acces pentru a opera asupra unui obiect) constă dintr-o combinaţie de tip DN (Distinguished Name - nume distinctiv) şi un DN. Tipurile DN valide sunt: access-id, Group şi Role.

DN-ul identifică un access-id, rol sau grop particular. De exemplu, un subiect poate fi access-id: cn=personA, o=IBM sau group: cn=deptXYZ, o=IBM.

Deoarece delimitatorul de câmp este ″două puncte″ (:), un DN care conţine ″două puncte″ trebuie să fie înconjurat de caractere ghilimele duble (“”). Dacă un DN conţine deja caractere cu marcaje ghilimele duble, aceste caractere trebuie însoţite de un backslash (\).

Toate grupurile director pot fi folosite în controlul accesului.

Notă: Orice grup cu clasa de obiect structurală **AccessGroup**, **GroupOfNames**, **GroupofUniqueNames** sau **groupOfURLs** sau cu clasa de obiect auxiliară **ibm-dynamicGroup**, **ibm-staticGroup** poate fi folosit pentru controlul accesului.

Alt tip DN folosit în cadrul modelului de control al accesului este rolul. Deşi rolurile şi grupurile sunt similare ca implementare, conceptual ele sunt diferite. Când un utilizator este asignat unui rol, este de aşteptat în mod implicit că autoritatea necesară a fost deja setată pentru a efectua jobul asociat cu acel rol. Cu apartenenţa la un grup, nu există presupunerea implicită despre ce permisiuni sunt obţinute (sau negate) prin a fi membru al acelui grup.

Rolurile sunt similare grupurilor prin faptul că sunt reprezentate în director de un obiect. Suplimentar, rolurile conţin un grup de DN-uri. Rolurile care sunt folosite pentru controlul accesului trebuie să aibe objectclass-ul **AccessRole**.

Pseudo DN: Directorul LDAP conţine mai multe pseudo DN-uri. Acestea sunt folosite pentru a referirea la un număr mare de DN-uri care la momentul legării partajează o caracteristică comună, în relaţie ori cu operaţia care este efectuată, ori cu obiectul destinaţie asupra căreia este efectuată operaţia.

În prezent, sunt definite trei pseudo DN-uri:

group:cn=anybody
Se referă la toţi subiecţii, inclusiv la cei care sunt neautentificaţi. Toţi utilizatorii aparţin acestui grup în mod automat.

group:cn=authenticated
Se referă la orice DN care a fost autentificat la director. Metoda de autentificare nu este considerată.

access-id:cn=this
Se referă la DN-ul legat care corespunde cu DN-ul obiectului destinaţie asupra căruia este efectuată operaţia.

Filtru de obiecte: Acest parametru se aplică doar la ACL-uri filtrate. Filtrul de căutare şir aşa cum este definit în RFC 2254, este folosit ca format al filtrului obiect. Deoarece obiectul destinaţie este deja cunoscut, şirul nu este folosit pentru a realiza o căutare efectivă. În schimb, este realizată o comparaţie bazată pe filtru pe obiectul destinaţie în cauză pentru a determina dacă un set dat de valori ibm-filterAclEntry se aplică.

Drepturi: Drepturile de acces se pot aplica la un obiect întreg sau la atributele obiectului. Drepturile de acces LDAP sunt discrete. Un drept nu implică alt drept. Drepturile pot fi combinate pentru a furniza lista cu drepturile dorite urmată de un set de reguli discutate mai târziu. Drepturile pot fi o valoare nespecificată, care indică faptul că nu este acordat nici un drept subiectului de pe obiectul destinaţie. Drepturile conţin trei părţi:

Acţiune:
Valorile definite sunt **acordate** sau **refuzate**. Dacă acest câmp nu este prezent, valoarea implicită este setată pe **acordat**.

Permisiune:
Sunt şase operaţii de bază care pot fi executate pe un obiect director. Din aceste operaţii, este preluat setul de bază de pemisiuni ACI. Acestea sunt: adăugare intrare, ştergere intrare, citire valoare atribut, scriere valoare atribut, căutare atribut şi comparare valoare atribut.

Permisiunile de atribut posibile sunt: citire (r), scriere (w), căutare (s) şi comparare (c). În plus, permisiunile de obiect se aplică intrării ca un întreg. Aceste permisiuni sunt adăugare intrări fiu (a) şi ştergere intrare (d).

Următoarea tabelă rezumă permisiunile necesare pentru a realiza fiecare din operaţiile LDAP.

Operaţie	**Permisiune Necesară**
ldapadd	add (pe părinte)
ldapdelete	delete (pe obiect)
ldapmodify	write (pe atribute ce sunt modificate)
ldapsearch	• search, read (pe atribute în RDN) • search (pe atribute specificate în filtru de căutare) • search (pe atribute returnate cu nume doar) • search, read (pe atribute returnate cu valori)
ldapmodrdn	write (pe atribute RDN)
ldapcompare	compare (pe atribute comparate)

Notă: Pentru operaţiile de căutare, subiectului i se cere să aibă acces de căutare (s) la toate atributele din filtrul de căutare sau nu este întoarsă nici o intrare. Pentru intrările întoarse dintr-o căutare, subiectul trebuie să aibă acces de căutare (s) şi citire (r) la toate atributele din RDN ale intrărilor întoarse sau aceste intrări nu sunt întoarse.

Destinaţie acces:

Aceste pemisiuni pot fi aplicate întregului obiect (adăugare intrare copil, ştergere intrare), unui atribut individual din cadrul intrării sau poate fi aplicat grupurilor de atribute (Clase de acces atribut) descrise în continuare.

Atributele care necesită permisiuni similare de acces sunt grupate în clase. Atributele sunt mapate către clasele lot de atribut ăn fişierul schemă director. Aceste clase sunt discrete; accesul la o clasă nu implică accesul la altă clasă. Permisiunile sunt setate cu privire la clasa de acces a atributului ca un întreg. Setul de permisiuni dintr-o clasă de atribute specifică se aplică la toate atributel din acea clasă de acces dacă nu sunt specificate permisiunile de acces atribut individual.

IBM defineşte trei clase de atribut care sunt folosite în evaluarea accesului la atributele utilizator: **normal**, **sensibil** şi **critic**. De exemplu, atributul **commonName** intră într-o clasă normală şi atributul parolă utilizator aparţine clasei critice. Atributele definite de utilizator aparţin clasei de acces normal doar dacă nu s-a specificat altfel.

De asemenea, mai sunt definite două alte clase de acces: sistem şi restricţionat. Atributele clasei sistem sunt:

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

Acestea sunt atribute păstrate de câtre serverul LDAP şi sunt numai-citire pentru utilizatorii directorului. **OwnerSource** şi **aclSource** sunt descrise în secţiunea Propagare (vedeţi“Propagare” la pagina 53).

Clasa de atribute restricţionate care definesc controlul accesului sunt:

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

Toţi utilizatorii au acces de citire la atributele restricţionate dar numai **entryOwners** pot crea, modifica şi şterge aceste atribute.

Notă: Atributul **ibm-effectiveAcl** este numai-citire.

EntryOwner

Proprietarii intrării au permisiuni complete pentru a efectua orice operaţie asupra obiectului indiferent de aclEntry. În plus, proprietarii intrării sunt singurii cărora le este permis să administreze aclEntries pentru acel obiect. EntryOwner este un subiect de control acces, el poate fi definit ca indivizi, grupuri sau roluri.

Notă: Administratorul directorului este în mod implicit unul dintre proprietarii intrării (entryOwners) pentru toate obiectele din director şi dreptul de proprieate (entryOwnership) al administratorului directorului nu poate fi şters de la nici un obiect.

Propagare

Intrările asupra cărora a fost plasată o aclEntry sunt considerate a avea o **aclEntry** explicită. În mod similar, dacă **entryOwner** a fost setat pentru o intrare particulară, acea intrare are un proprietar explicit. Cele două nu sunt intersectate, o intrare cu un proprietar explicit poate sau nu poate să aibă o **aclEntry** explicită şi o intrare cu o **aclEntry** explicită ar putea avea un proprietar explicit. Dacă oricare dintre aceste valori nu este prezentă în mod explicit pentru o intrare, valoarea lipsă este moştenită de la un nod strămoş din arborele directorului.

Fiecare **aclEntry** sau **entryOwner** explicit se aplică la acea intrare asupra căreia este setat. În plus, valoarea s-ar putea aplica asupra tuturor descendenţilor care nu au o valoare explicită setată. Aceste valori se consideră a fi propagate; valorile lor se propagă prin arborele director. Propagarea unei valori particulare continuă până când altă este atinsă altă valoare de propagare.

Notă: ACL-urile bazate pe filtru nu se propagă în acelaşi mod în care se propagă ACL-urile care nu sunt bazate pe filtru. Ele se propagă asupra oricăror obiecte care corespund în urma comparaţiei din subarborele asociat. Vedeţi “ACL-uri filtrate” la pagina 49 pentru mai multe informaţii despre diferenţe.

AclEntry şi **entryOwner** pot fi setate să se aplice doar la o intrare particulară cu valoarea de propagare setată pe ″fals″ sau la o intrare şi subarborele lor cu valoarea de propagare setată pe ″adevărat″. Deşi atât **aclEntry** cât şi **entryOwner** se pot propaga, propagarea lor nu este legată în nici un fel.

Atributele **aclEntry** şi **entryOwner** permit valori multiple, dar oricum, atributele de propagare (**aclPropagate** şi **ownerPropagate**) pot avea o singură valoare pentru toate valorile atributelor **aclEntry** sau **entryOwner** din cadrul aceleiaşi intrări.

Atributele sistem **aclSource** şi **ownerSource** conţin DN-ul nodului efectiv din care sunt evaluate **aclEntry** sau **entryOwner**, respectiv. Dacă nu există un astfel de nod, este atribuită valoarea **default**.

Definiţiile de control acces efectiv al unui obiect pot fi derivate de următoarea logică:

- Dacă există un set de atribute de control explicit al accesului pentru obiect, atunci aceea este definiţia de control al accesului obiectului.
- Dacă nu există atribute de control al accesului explicit definite atunci traversaţi arborele director în sus până când se ajunge la un nod strămoş cu un set de atribute de control al accesului care se propagă.
- Dacă nu este găsit un astfel de nod strămoş, accesul implicit descris mai jos este acordat subiectului.

Administratorul directorului este proprietarul intrării. Pseudo grupul cn=anybody (toţi utilizatorii) primeşte acces de citire, căutare şi comparaţie pentru atributle din clasa de acces normal.

Evaluarea accesului

Accesul la o operaţie particulară este acordat sau respins pe baza DN-ului de legare al subiectului pentru acea operaţie asupra obiectului ţintă. Procesarea se opreşte atunci când dreptul de acces poate fi determinat.

Verificările de acces sunt făcute găsind mai întâi definiţia efectivă pentru **entryOwnership** şi **ACI**, verificarea dreptului de proprietate asupra intrării şi apoi prin evaluarea valorilor ACI ale obiectului.

ACL-urilor bazate pe filtru se acumulează de la intrare container cea mai de jos, în sus de-a lungul lanţului de strămoşi ai intrării, până la cea mai de sus intrare container din DIT. Accesul efectiv este calculat ca reuniune a drepturilor de acces acordate sau negate, de către intrările strămoş constituente. Setul existent de reguli de specificitate şi combinatorii este folosit pentru a evalua accesul efectiv pentru ACL-uri bazate pe filtru.

Atributele bazate pe filtru şi nebazate pe filtru sunt mutual exclusive în cadrul unei singure intrări director container. Plasarea ambelor tipuri de atribute în aceeaşi intrare nu este permisă şi este considerată o violare de restricţie. Operaţiile asociate cu crearea sau actualizarea, unei intrări director eşuează dacă este detectată această condiţie.

Când se calculează accesul efectiv, primul tip de ACL care va fi detectat în lanţul de strămoşi al intrării obiectului ţintă setează modul de calcul. În modul bazat pe filtru, ACL-urile nebazate pe filtru sunt ignorate la calculul accesului efectiv. La fel, în modul nebazat pe filtru, ACL-urile bazate pe filtru sunt ignorate la calculul accesului efectiv.

Pentru a limita acumularea de ACL-uri bazate pe filtru la calculul accesului efectiv, un atribut **ibm-filterAclInherit** setat la valoarea ″fals″ poate fi plasat în orice intrare dintre cea mai mare şi cea mai mică apariţie a **ibm-filterAclEntry** într-un subarbore dat. Aceasta face ca subsetul de atribute **ibm-filterAclEntry** de deasupra lui în lanţul de strămoşi al obiectului ţintă să fie ignorat.

În modul bazat pe filtru, dacă nu se aplică nici un ACL bazat pe filtru, atunci se aplică ACL-ul implicit (cn=anybody primeşte drept de acces de citire, căutare şi comparaţie la atribute din clasa de acces normal). Această situaţie poate apare când intrarea care este accesată nu corespunde cu nici unul dintre filtrele specificate în valorile **ibm-filterAclEntry**. Poate doriţi să specificaţi un filtru ACL implicit cum este următorul dacă nu doriţi ca acest control de acces implicit să se aplice:

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

Acest exemplu nu acordă nici un acces. Modificaţi-l pentru a furniza accesul pe care îl doriţi aplicat.

Implicit, administratorul directorului şi serverul master sau serverul peer (pentru replicare) obţin drepturi de acces depline la toate obiectele din director cu excepţia accesului de scriere la atributele sistem. Alte **entryOwners** obţin drepturi de acces depline la obiectele de sub dreptul lor de proprietate cu excepţia accesului de scriere la atributele sistemului. Toţi utilizatorii au drepturi de acces citire la atributele restricţionate şi sistem. Aceste drepturi predefinite nu pot fi modificate. Dacă subiectul care face cererea are **entryOwnership**, accesul este determinat de setările implicite de mai sus şi procesarea accesului se opreşte.

Dacă subiectul care face cererea nu este un entryOwner, atunci sunt verificate valorile ACI pentru intrările obiect. Drepturile de acces aşa cum sunt definite în ACI-uri pentru obiectul destinaţie sunt calculate prin reguli de specificitate şi combinatorii.

Regulă specificitate

Cele mai specifice definiţii aclEntry sunt cele folosite în evaluarea permisiunilor acordate/respinse unui utilizator. Nivelele de specificitate sunt:

- ID-acces este mai specific decât grup sau rol. Grupurile şi rolurile sunt pe acelaşi nivel.
- În acelaşi nivel **dnType**, permisiunile de nivel atribut individuale sunt mai specifice decât permisiunile nivelului clasă atribut.
- În acelaşi nivel atribut sau clasă atribut, **refuzare** este mai specific decât **acordare**.

Regulă combinatorie

Permisiunile acordate subiecţilor cu specificitate egală sunt combinate. Dacă accesul nu poate fi determinat în cadrul aceluiaşi nivel de specificiate, sunt folosite definiţiile de acces cu nivelul specific mai mic. Dacă accesul nu este determinat după ce toate ACI-urile definite sunt aplicate, accesul este refuzat.

Notă: După ce o intrare **aclEntry** de nivel id-acces care se potriveşte este găsită în evaluarea accesului, intrările aclEntries de nivel grup nu sunt incluse în calcularea accesului. Excepţia este aceea că intrările **aclEntries** de nivel id-acces care se potrivesc sunt toate definite sub cn=this, atunci toate intrările **aclEntries** de nivel grup care se potrivesc sunt de asemenea combinate în evaluare.

Cu alte cuvinte, în cadrul intrării obiect, dacă o intrare ACI definită conţine un DN subiect id-acces care se potriveşte cu DN de legare, atunci permisiunile sunt întâi evaluate pe baza acelei intrări aclEntry. Sub acelaşi DN subiect, dacă sunt definite permisiunile de nivel atribut care se potrivesc, ele înlocuiesc orice permisiune definită sub clasele de atribut. Sub aceeaşi definiţie de nivel atribut sau clasă atribut, dacă sunt prezente permisiuni care dau conflict, permisiunile refuzate suprascriu permisiunile acordate.

Notă: O permisiune definită cu valoare nulă împiedică includerea definiţiilor cu permisiune mai puţin specifică.

Dacă accesul încă nu poate fi determinat şi toate intrările aclEntries găsite care se potrivesc sunt definite sub ″cn=this″, apoi apartenenţa grupului este evaluată. Dacă un utilizator aparţine mai multor grupuri, utilizatorul primeşte permisiunile combinate de la aceste grupuri. În plus, utilizatorul aparţine automat grupului cn=Anybody şi posibil grupului cn=Authenticated dacă utilizatorul a făcut o legare autentificată. Dacă sunt definite permisiuni pentru aceste grupuri, utilizatorul primeşte permisiunile specificate.

Notă: Apartenenţa grup şi rol este determinată la momentul legării şi durează până când are loc altă legare sau până când este primită o cerere de dezlegare. Roluri şi grupuri imbricate, adică un grup sau rol definit ca un membru al altui grup sau rol, nu sunt rezolvate în determinarea apartenenţei şi nici în evaluarea accesului.

De exemplu, să presupunem atribute1 este în clasa de atribut sensibilă şi utilizatorul cn=Person A, o=IBM aparţine atât grupului group1 cât şi grupului group2 cu următoarele intrări aclEntries definite:

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

Acest utilizator obţine:

- Acces pentru ’rsc’ la atribut1, (din 1. Definiţia de nivel atribut înlocuieşte definiţia de nivel clasă atribut).
- Nici un acces la alte atribute de clasă sensibilă din obiectul destinaţie, (din 1).
- Nici un alt drept nu este acordat (2 şi 3 NU sunt incluse în evaluarea de acces).

Alt exemplu, cu următoarele aclEntries:

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

Utilizatorul are:

- nici un acces la atributele de clasă sensibilă, (din 1. Valoare nulă definită sub id-acces împiedică includerea permisiunilor la atributelor de clasă sensibilă din grup1).
- şi acces ’rsc’ la atributele de clasă normală (din 2).

Definire ACI-uri şi proprietari intrare

Următoarele două exemple arată un subdomeniu administrativ fiind stabilit. Primul exemplu arată un singur utilizator fiind asignat ca entryOwner pentru întregul domeniu. Al doilea exemplu arată un grup asignat ca entryOwner.

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

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

Următorul exemplu arată cum unui id-access ″cn=Person 1, o=IBM″ îi este dată permisiunea de citire, căutare şi comparare atribut1. Permisiunea se aplică la orice nod din întregul subarbore, la sau sub nodul care conţine acest ACI, care se potriveşte cu filtrul de comparare ″(objectclass=groupOfNames)″. Acumularea de atribute ibm-filteraclentry care se potrivesc în oricare nod strămoş a fost terminată la această intrare prin setarea atributului ibm-filterAclInherit la ″fals″.

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

ibm-filterAclInherit: false
```

Următorul exemplu arată cum unui grup ″cn=Dept XYZ, o=IBM″ îi este dată permisiunea de citire, căutare şi comparare atribut1. Permisiunea se aplică la întregul subarbore de sub nodul care conţine acest ACI.

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

Următorul exemplu arată cum unui rol ″cn=System Admins,o=IBM″ îi este dată permisiunea de adăugare obiecte sub acest nod şi citire, căutare şi comparare atribut2 şi clasă de atribut critic. Permisiunea se aplică doar la nodul care conţine acest ACI.

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

Modificare valori ACI şi proprietar intrare

Modificare-înlocuire

Modificare-înlocuire funcţionează în acelaşi mod ca toate celelalte atribute. Dacă valoarea atributului nu există, se creează valoarea. Dacă valoarea atributului există, se înlocuieşte valoarea.

Date fiind următoarele ACI-uri pentru o intrare:

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

realizaţi următoarea modificare:

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

ACI-ul rezultat este:

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

Valorile ACI pentru Dept ABC se pierd prin înlocuire.

Date fiind următoarele ACI-uri pentru o intrare:

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

realizaţi următoarele modificări:

```
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
```

ACI-ul rezultat este:

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

Valorile ACI pentru Dept ABC se pierd prin înlocuire.

Modificare-adăugare

În timpul unei adăugări ldapmodify-add, dacă ACI-ul sau entryOwner nu există, este creat ACI sau entryOwner cu valorile specifice. Dacă ACI sau entryOwner există, atunci adăugaţi valorile specificate la ACI-ul sau entryOwner date. De exemplu, fiind dat ACI-ul:

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

cu o modificare:

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

ar oferi o aclEntry multi-valoare de:

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

De exemplu, fiind dat ACI-ul:

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

cu o modificare:

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

ar oferi o aclEntry multi-valoare de:

```
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
```

Permisiunile de sub acelaşi atribut sau clasă de atribut sunt considerate ca fiind blocurile de bază şi acţiunile sunt considerate ca fiind calificative. Dacă este adăugată aceeaşi valoare de permisiune de mai multe ori, doar o valoare este stocată. Dacă aceeaşi valoare de permisiune este adăugată de mai multe ori cu diverse valori de acţiune, este folosită ultima valoare de acţiune. În cazul în care câmpul cu permisiunea rezultată este gol(″″), această valoare de permisiune este setată nulă şi valoarea acţiunii este setată pe **acordare** .

De exemplu, fiind dat următorul ACI:

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

cu o modificare:

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

furnizează o aclEntry de:

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

De exemplu, fiind dat următorul ACI:

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

cu o modificare:

```
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
```

furnizează o aclEntry de:

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

Modificare-ştergere

Pentru a şterge o anumită valoare ACI, folosiţi sintaxa normală ldapmodify-delete.

Fie dat un ACI de:

```
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
```

furnizează un ACI care rămâne pe server de:

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

Fie dat un ACI de:

```
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
```

furnizează un ACI care rămâne pe server de:

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

Ştergerea unei valori entryOwner sau ACI care nu există are ca rezultat un ACI nemodificat sau entryOwner şi un cod retur care specifică faptul că valoarea atributului nu există.

Ştergerea valorilor ACI/proprietar intrare

Cu operaţia ldapmodify-delete, entryOwner poate fi ştearsă prin specificarea

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

În acest caz, intrarea nu ar avea un entryOwner explicit. OwnerPropagate este de asemenea şters automat. Această intrare ar moşteni entryOwner de la nodul strămoş din arborele director care urmează regulii de propagare.

Acelaşi lucru poate fi făcut pentru a şterge aclEntry complet:

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

Ştergerea ultimei valori ACI sau entryOwner de la o intrare nu este la fel ca ştergerea ACI sau entryOwner. Este posibil pentru o intrare să conţină un ACI entryOwner fără valori. În acest caz, nimic nu este returnat clientului când interogarea ACI sau entryOwner şi setarea se propagă nodurilor descendente până este suprascrisă. Pentru a împiedica amestecarea intrărilor pe care nimeni nu le poate accesa, administratorul director are întotdeauna acces deplin la o intrare chiar dacă intrarea are o valoare ACI sau entryOwner nulă.

Extragere valori ACI/proprietar intrare

Valorile ACI sauentryOwner efective pot fi extrase prin specificarea atributelor ACL sau entryOwner într-o căutare, de exemplu,

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

returnează toate informaţiile ACL sau entryOwner care sunt folosite într-o evaluare de acces asupra obiectului A. Luaţi aminte că valorile returnate s-ar putea să nu arate exact la fel cum sunt definite ele iniţial. Valorile sunt echivalentul formei originale.

Căutarea doar pe atributul ibm-filterAclEntry întoarce valori corespunzătoare intrării care le conţine.

Un atribut operaţional numai citire, ibm-effectiveAcl, este folosit pentru a arăta accesul efectiv acumulat. O cerere de căutare pentru ibm-effectiveAcl întoarce accesul efectiv care se aplică la obiectul destinaţie pe baza: ACL-uri non-filtru sau ACL-uri filtru, în funcţie de modul în care au fost distribuite in DIT.

Deoarece ACL-urile bazate pe filtru pot veni din mai multe surse strămoş, o căutare pe atributul aclSource produce o listă de surse asociate.

Considerente de replicare subarbore

Pentru ca accesul bazat pe filtru să fie inclus în replicarea de subarbore, orice atribut ibm-filterAclEntry trebuie să se afle la sau sub intrarea ibm-replicationContext asociată.

Deoarece accesul efectiv nu poate fi acumulat dintr-o intrare strămoş de deasupra unui subarbore replicat, atributul ibm-filterAclInherit trebuie să fie setat la o valoare **fals** şi să se afle la intrarea ibm-replicationContext asociată.

Drept de proprietate a obiectelor directorului LDAP

Fiecare obiect din directorul dumneavoastră LDAP are el puţin un proprietar. Proprietării de obiecte au puterea de a şterge obiectul. Proprietarii şi administratorii de server sunt singurii utilizatori care pot modifica proprietăţile dreptului de proprietate şi lista de control acces (ACL) atributele unui obiect. Dreptul de proprietate a obiectelor poate fi moştenit sau explicit. Deci, pentru a asigna dreptul de proprietate puteţi face una din următoarele:

- Setaţi explicit dreptul de proprietate pentru un obiect specific.
- Specifică dacă obiectele moştenite de la obiecte de mai sus din ierarhia de directoare LDAP.

Directory Server vă permite să specificaţi proprietari multipli pentru acelaşi obiect. Puteţi de asemenea specifica dacă un obiect se deţine. Pentru a face asta includeţi DN-ul special cn=this în lista de proprietari de obiecte. De exemplu, asumaţi că obiectul cn=A are proprietarul cn=this. Orice utilizator are acces de proprietar la obiectul cn=A dacă se conectează la server ca cn=A.

Pentru mai multe informaţii despre cum să lucraţi cu proprietăţile dreptului de proprietate, vedeţi “Gestionarea intrărilor în director” la pagina 131.

Politică parolă

Cu folosirea serverelor LDAP pentru autentificare, este important ca un server LDAP să suporte politici cu privire la expirarea parolei, încercările de înregistrare eşuate şi reguli de parolă. Directory Server furnizează suport configurabil pentru toate cele trei tipuri de politici. Această politică este aplicată la toate intrările director care au un atribut userPassword. Nu puteţi defini o politică pentru un set de utilizatori şi politici diferite pentru alte seturi de utilizatori. Directory Server furnizează de asemenea un mecanism pentru ca clienţii să fie informaţi de condiţiile înrudite cu

politica de parolă (parola expiră în trei zile) şi un set de atribute operaţionale pe care un administrator îl poate folosi pentru a căuta lucruri precum utilizatori cu parole expirate sau conturi blocate.

Pentru mai multe informaţii despre cum să lucraţi cu proprietăţile politicii de parolă, vedeţi “Setarea politicii pentru parole” la pagina 98.

Configurare

Puteţi configura comportamentul serverului ţinând cont de parolele din următoarele zone:

- Un comutator ″on/off″ global pentru activarea sau dezactivarea politicii de parolă
- Reguli pentru schimbarea parolelor, inclusiv:
  - Utilizatorii îşi pot schimba propriile parole. Ţineţi cont că această politică se aplică în plus faţă de orice control de acces. Adică, controlul de acces trebuie să dea unui utilizator autorizarea de modificare a atributului userPassword, cât şi politica de parolă care permite utilizatorilor să-şi schimbe parola. Dacă această politică este dezactivată, utilizatorii nu îşi pot schimba parola. Doar un administrator sau alt utilizator cu atorizare de schimbare a atributului userPassword poate schimba parola pentru o intrare.
  - Parolele trebuie să fie schimbate după reset. Dacă această politică este activată, când o parolă este schimbată de oricine altcineva decât acel utilizator, parola este marcată ca reset şi trebuie să fie schimbată de utilizator ănainte de a putea realiza alte operaţii director. O cerere de legare cu o parolă reset este realizată cu succes. Pentru a fi notificată de faptul că parola trebuie resetată, aplicaţia trebuie să fie conştientă de politica de parolă.
  - Utilizatorii trebuie să trimită parolele vechi la schimbarea parolei. Dacă această politică este activată, o parolă poate fi schimbată doar prin cerere de modificare care include o ştergere a atributului userPassword (cu valoarea veche) şi o adăugare a noii valori userPassword. Aceasta asigură că doar cine îşi cunoaşte parola o poate modifica. Administratorul sau alţi utilizatori autorizaţi să schimbe atributul userPassword pot întotdeauna seta parola.
- Regulile pentru expirarea parolei includ:
  - Parolele nu expiră niciodată sau parolele expiră după un timp configurabil după ce au schimbate ultima dată.
  - Nu se atenţionează utilizatorii când expiră o parolă sau se atenţionează utilizatorii înainte de expirarea parolei cu o perioadă de timp configurabilă. Pentru a fi atenţionată de apropierea expirării parolei, aplicaţia trebuie să fie conştientă de politica de parolă.
  - Permiterea unui număr configurabil de înregistrări de graţie după ce parola utilizatorului a expirat. O aplicaţie conşientă de politica de parolă va fi notificată de numărul de înregistrări de graţie rămase. Dacă nu sunt permise înregistrări de graţie, un utilizator nu poate autentifica sau schimba parola după ce a expirat.
- Reguli pentru validarea parolei, inclusiv:
  - O dimensiune istorie de parolă configurabilă, care spune serverului să ţină o istorie a ultimelor N parole şi să refuze parolele care au fost folosite anterior.
  - Verificarea sintaxei parolei, inclusiv o setare pentru cum ar trebui să se comporte serverul când parolele sunt hashed. Această setare afectează dacă serverul ar trebui să ignore politica în una din următoarele condiţii:
    - Serverul stochează parolele hash.
    - Un client prezintă o parolă hash serverului (aceasta se poate întâmpla la transferarea intrărilor între servere via un fişier LDIF dacă serverul sursă stochează parole hash).

    În oricare din aceste cazuri, serverul s-ar putea să nu poată aplica toate regulile de sintaxă. Următoarele reguli de sintaxă sunt suportate: lungime minimă, număr minim de caractere alfabetice, număr minim de caractere speciale sau numerice, număr de caractere repetate şi număr de caractere în care parola trebuie să difere de parola anterioară.
- Reguli pentru înregistrări eşuate, inclusiv:
  - Un timp minim permis între schimbarea parolei, care împiedică utilizatorii de la ciclarea rapidă printr-un set de parole pentru a ajunge înapoi la parola originală.
  - Un număr maxim de încercări de înregistrare eşuate înainte de blocarea contului.
  - O durată de blocare parolă configurabilă. După acest timp, un cont blocat anterior poate fi folosit. Aceasta poate ajuta la blocarea unui hacker care încearcă să spargă o parolă, în timp ce ajută un utilizator care şi-a uitat parola.

– Un timp configurabil pentru care serverul ţine evidenţa încercărilor de înregistrare eşuate. Dacă numărul maxim de încercări de înregistrare eşuate apare în această perioadă, contul este blocat. După ce acest timp a expirat, serverul renunţă la informaţiile despre încercările de înregistrare eşuate anterioare pentru cont.

Setările politicii de parolă pentru serverul de directoare sunt stocate în obiectul ″cn=pwdpolicy″, care arată:

```
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
```

Aplicaţii conştiente de politica de parolă

Suportul politicii de parolă Directory Server for iSeries include un set de controale LDAP care pot fi foosite de către o aplicaţie conşientă de politica de parolă pentru a primi notificări ale condiţiilor înrudite cu politica de parolă adiţionale.

O aplicaţie poate fi informată de următoarele condiţii de avertizare:

- Timp rămas înainte de expirarea parolei
- Număr de înregistrări de graţie rămase după ce parola a expirat

O aplicaţie poate fi de asemenea informată de următoarele condiţii de eroare:

- Parola a expirat
- Contul este blocat
- Parola a fost resetată şi trebuie schimbată
- Utilizatorul nu are permisiunea de a-şi schimba parola
- Vechea parolă trebuie să fie furnizată la schimbarea parolei.
- Noua parolă violează regulile de sintaxă
- Noua parolă este prea scurtă
- Parola a fost schimbată prea recent
- Noua parolă este în istorie

Două controale sunt folosite. Un control de cerere politică parolă este folosit pentru a informa serverul că aplicaţia doreşte să fie informată de condiţiile înrudite cu politica de parolă. Acest control trebuie să fie specificat de aplicaţie pe toate operaţiile pentru care este interesat, tipic cererea de legare iniţială şi orice cerere de schimbare parolă. Dacă controlul de cerere politică parolă este prezent, un control de răspuns politică parolă este returnat de server când oricare din condiţiile de eroare de mai sus este prezentă.

API-urile client Directory Server includ un set de API-uri care pot fi folosite de aplicaţii C pentru a lucra cu aceste controale. Aceste API-uri sunt:

- ldap_parse_pwdpolicy_response
- ldap_pwdpolicy_err2string

Pentru aplicaţii care nu folosesc aceste API-uri, controalele sunt definite mai jos. Trebuie să folosiţi capabilităţile furnizate de API-urile client LDAP care sunt folozite pentru a procesa controalele. De exemplu, JNDI (Java Naming and Directory Interface) are suport încorporat pentru unele controale cunoscute şi, de asemenea, furnizează un cadru de lucru pentru controalele suportate pe care JNDI nu le recunoaşte.

Control cerere politică parolă

```
Nume control: 1.3.6.1.4.1.42.2.27.8.5.1
Criticalitate control: FALSE
Valoare control: nici una
```

Control răspuns politică parolă

```
Nume control: 1.3.6.1.4.1.42.2.27.8.5.1 (la fel ca şi control cerere)
Criticalitate control: FALSE
Valoare control: O valoare codată BER definită în ASN.1 după cum urmează:
  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) } }
```

Ca şi alte elemente protocol LDAP, codarea BER foloseşte etichetare implicită.

Atribute operaţionale politică parolă

Directory Server menţine un set de atribute operaţionale pentru fiecare intrare care are un atribut userPassword. Aceste atribute pot fi căutate de utilizatorii autorizaţi, folosite în filtre de căutare sau returnate de cererea de căutare. Aceste atribute sunt:

- pwdChangedTime - Un atribut GeneralizedTime care conţine timpul la care a fost schimbată parola ultima dată.
- pwdAccountLockedTime - Un atribut GeneralizedTime care conţine timpul la care a fost blocat contul Dacă contul nu este blocat, acest atribut nu este prezent.
- pwdExpirationWarned - Un atribut GeneralizedTime care conţine timpul la care avertizarea de expirare parolă a fost trimisă prima dată la client.
- pwdFailureTime - Un atribut GeneralizedTime multi valoare care conţine timpii eşecurilor de înregistrare consecutivă anterioare. Dacă ultima înregistrare a fost realizată cu succes, acest atribut nu este prezent.
- pwdGraceUseTime - Un atribut GeneralizedTime multi valoare care conţine timpii înregistrărilor de graţie anterioare.
- pwdReset - Un atribut boolean care conţine valoarea TRUE dacă parola a fost resetată şi trebuie schimbată de utilizator.

Replicarea politicii de parolă

Informaţiile politicii de parolă sunt replicate de serverele furnizor consumatorilor. Modificările intrării cn=pwdpolicy sunt replicate ca modificări globale, cum sunt modificările schemei. Informaţiile de stare politică parolă pentru intrările

individuale sunt de asemenea replicate, astfel încât, de exemplu, dacă o intrare este blocată pe un server furnizor, acea acţiune va fi replicată la orice consumator. Modificările stării politicii de parolă de pe o replică numai citire nu se replică pe nici un alt server.

Autentificare

Controlul de acces din cadrul Directory Server se bazează pe numele distinctiv (DN) asociat cu o conexiune dată. Acel DN este stabilit ca rezultat al unei legări la (înregistrare în) Directory Server.

Când Directory Server este configurat prima dată, următoarele identităţi pot fi folosite pentru a autentifica serverul:

- anonymous
- administratorul directorului (cn=administrator implicit)
- un profil utilizator i5/OS proiectat (vedeţi “Backend proiectat pe sistemul de operare” la pagina 65)

Este o idee bună să creaţi utilizatori adiţionali care pot primi autorizare de gestionare a diferitelor părţi din director fără a vă cere să partajaţi identitatea administratorului de director.

Dintr-o perspectivă LDAP, există două cadre de lucru pentru autentificarea la LDAP:

- Legarea simplă, în care o aplicaţie furnizează un DN şi parola text pentru acel DN.
- Nivelul Securitate şi autentificare simplă (SASL - Simple Authentication and Security Layer), care furnizează câteva metode de autentificare adiţionale, inclusiv CRAM-MD5, EXTERNAL, GSSAPI şi OS400-PRFTKN.

Legare simplă (şi CRAM-MD5)

Pentru a folosi o legare simplă, clientul trebuie să furnizeze DN-ul unei intrări LDAP existente şi o parolă care se potriveşte cu atributul userPassword pentru acea intrare. De exemplu, puteţi crea o intrare pentru John Smith după cum urmează:

```
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
```

Puteţi acum folosi DN-ul ″cn=John Smith,cn=users,o=acme,c=us″ din controlul de acces sau să îl faceţi un membru al grupului folosit în controlul de acces.

Câteva clase obiect predefinite permit ca userPassword să fie specificat, inclusiv (dar nu limitat la): person, organizationalperson, inetorgperson, organization, organizationalunit şi altele.

Parolele Directory Server sunt sensibile la majuscule. Dacă creaţi o intrare cu valoarea userPassword secret, o legare care specifică parola SECRET va eşua.

Când folosiţi o legare simplă, clientul trimite parola text la server ca parte a cererii de legare. Aceasta face parola susceptibilă la snooping la nivel de protocol. O conexiune SSL ar putea fi folosită pentru a proteja parola (toate informaţiile trimise printr-o conexiune SSL sunt criptate). Sau poate fi folosită metoda CRAM-MD5 SASL.

Metoda CRAM-MD5 necesită ca serverul să aibă acces la parola text (protecţia parolei este setată pe nici una, ceea ce înseamnă că parola este stocată în formă decriptabilă şi returnată ca text simplu la căutări). Clientul trimite DN-ul către server. Serverul primeşte valoarea userPassword pentru intrare şi generează un şir de caractere aleator. Şirul de caractere aleator este trimis către client. Atât clientul cât şi serverul dispersează (hash) şirul aleator folosind parola drept cheie şi clientul trimite rezultatul către server. Dacă cele două şiruri hashed se potrivesc, cererea de legare are succes şi parola nu a fost trimisă niciodată la server.

Pentru a folosi CRAM-MD5 serverul trebuie să fie configurat pentru ca protecţia parolei să fie Fără (None) şi valoarea sistem QRETSVRSEC (Reţinere date de securitate server) trebuie să fie 1 (Reţinere date).

Legarea ca un utilizator public

Directory Server oferă un mijloc de a avea o intrare LDAP a cărei parolă este cea a unui profil de utilizator i5/OS de pe acelaşi sistem. Pentru a face aceasta, intrarea trebuie să:

- aibă un atribut UID, a cărei valoare este numele unui profil de utilizator i5/OS
- să nu aibă un atribut userPassword

Când serverul primeşte o cerere pentru o intrare care are o valoare UID dar nu are userPassword, serverul apelează securitatea i5/OS pentru a valida că UID-ul este un nume valid de profil de utilizator şi că parola specificată este parola corectă pentru acel profil de utilizator. O astfel de intrare este numită utilizator publicat în legătură cu publicarea directorului de distribuţie sistem (SDD - system distribution directory) la LDAP, care creează astfel de intrări.

Legarea ca un utilizator proiectat

O intrare LDAP care reprezintă un profil de utilizator i5/OS este denumit utilizator proiectat. Puteţi folosi DN-ul unui utilizator proiectat împreună cu parola corectă pentru acel profil de utilizator dintr-o legare simplă. De exemplu, DN-ul pentru utilizatorul JSMITH de pe sistemul my-system.acme.com ar fi:

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

Legarea SASL EXTERNAL

Dacă este folosită o conexiune SSL sau TLS pentru autentificarea clientului (de exemplu, clientul are un certificat privat), atunci poate fi folosită metoda SASL EXTERNAL. Această metodă spune serverului să preia identitatea clientului de la o sursă externă, în acest caz conexiunea SSL. Serverul obţine porţiunea publică a certificatului client (trimis către server ca parte a stabilirii conexiunii SSL) şi extrage DN-ul subiect. Acel DN este atribuit conexiunii de către serverul LDAP.

De exemplu, fiind dat un certificat asignat lui:

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

DN-ul subiect ar fi:

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

Notaţi că elementele cn, ou, o, l, st şi c sunt folosite în ordinea arătată pentru a genera DN-ul subiect.

Legarea SASL GSSAPI

Mecanismul de legare SASL GSSAPI este folosit pentru autentificarea la server folosind un tichet Kerberos. Acest lucru este de folos atunci când clientul a făcut un KINIT sau altă formă de autentificare Kerberos (de exemplu, login la un domeniu Windows 2000). În acest caz, serverul validează tichetul clientului şi obţine numele de Kerberos principal şi de regiune; de exemplu, principalul jsmith din regiunea acme.com, exprimată normal ca jsmith@acme.com. Serverul poate fi configurat pentru a asocia această identitate cu un DN în unul din două moduri:

- Generează un pseudo DN de forma ibm-kn=jsmith@acme.com
- Caută o intrare care are clasa auxiliară ibm-securityidentities şi o valoare altsecurityidenties de forma KERBEROS:<principal>@<realm>.

O intrare care ar putea fi folosită pentru jsmith@acme.com ar putea arăta astfel:

```
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
```

Pentru informaţii despre cum să activaţi autentificarea Kerberos, vedeţi “Activarea autentificării Kerberos pe Directory Server” la pagina 121.

Legarea OS400-PRFTKN

Mecanismul de legare OS400-PRFTKN SASL este folosit pentru autentificarea la server folosind un jeton de profil (vedeţi API-ul Generate Profile Token). Când este folosit acest mecanism, serverul validează jetonul de profil şi asociază DN-ul profilului de utilizator proiectat cu conexiunea (de exemplu, os400-profile=JSMITH,cn=accounts,os400-system=my-as400.mycompany.com). Dacă aplicaţia are deja un jeton de profil, acest mecanism evită nevoia de a obţine numele profilului de utilizator şi parola pentru a efectua o legare simplă. Pentru a folosi acest mecanism, folosiţi API-ul ldap_sasl_bind s, specificând un DN nul, OS400-PRFTKN pentru mecanism şi un berval (date binare care sunt codificate folosind regulile de codificare de bază simplificate) care conţin jetonul de profil pe 32 de octeţi pentru acreditări.

LDAP ca un serviciu de autentificare

LDAP este folosit de obicei pentru a oferi un serviciu de autentificare. Puteţi configura un server Web pentru autentificarea la LDAP. Prin setarea mai multor servere Web (sau alte aplicaţii) pentru autentificarea la LDAP, puteţi stabili un singur registru de utilizator pentru acele aplicaţii, decât să definiţi utilizatori din noi şi din nou pentru fiecare aplicaţie sau instanţă a serverului Web.

Cum funcţionează aceasta? Pe scurt, serverul Web îi cere utilizatorului un nume de utilizator şi o parolă. Serverul Web preia aceste informaţii şi apoi face o căutare în directorul LDAP pentru o intrare cu acel nume de utilizator (de exemplu, puteţi configura serverul Web să asocieze numele de utilizator ci atributele LDAP ’uid’ sau ’mail’). Dacă găseşte exact o intrare, serverul Web trimite apoi o cerere de legare către server folosind DN-ul intrării pe care tocmai a găsit-o şi parola furnizată de utilizator. Dacă legarea are succes, utilizatorul este acum autentificat. Conexiunile SSL pot fi folosite pentru a proteja informaţiile de parolă de snooping la nivel de protocol.

Serverul Web poate de asemenea păstra evidenţa DN-ului care a fost folosit astfel încât o aplicaţie dată poate folosi acel DN, poate prin stocarea datelor de personalizare din acea intrare, o altă intrare asociată cu ele sau într-o bază de date separată folosind DN-ul drept cheie pentru a găsi informaţiile.

O alternativă comună la folosirea unei cereri de legare este să folosiţi operaţia de comparaţie LDAP. De exemplu ldap_compare(ldap_session, dn, "userPassword", enteredPassword). Aceasta permite aplicaţiei să folosească o singură sesiune LDAP, în loc de a porni şi termina sesiuni pentru fiecare cerere de autentificarea.

Backend proiectat pe sistemul de operare

Backend-ul proiectat pe sistem are abilitatea de a mapa obiecte i5/OS ca intrări în arborele de directoare accesibil LDAP. Obiectele proiectate sunt reprezentări LDAP ale obiectelor i5/OS în locul intrărilor reale memorate în baza de date a serverului LDAP. Profilele de utilizator sunt singurele obiecte care sunt asociate sau proiectate ca intrări în cadrul arborelui director. Maparea obiectelor profil de utilizator este referită ca backend-ul proiectat al utilizatorului i5/OS.

Operaţiile LDAP sunt mapate în obiectele de bază i5/OS şi operaţiile LDAP realizează funcţii sistem de operare pentru a accesa aceste obiecte. Toate operaţiile LDAP realizate pe profilele utilizator sunt făcute sub autoritatea profilului utilizator asociat cu conexiunea client.

Pentru informaţii mai detaliate despre backend-ul proiectat pe sistemul de operare, vedeţi următoarele:

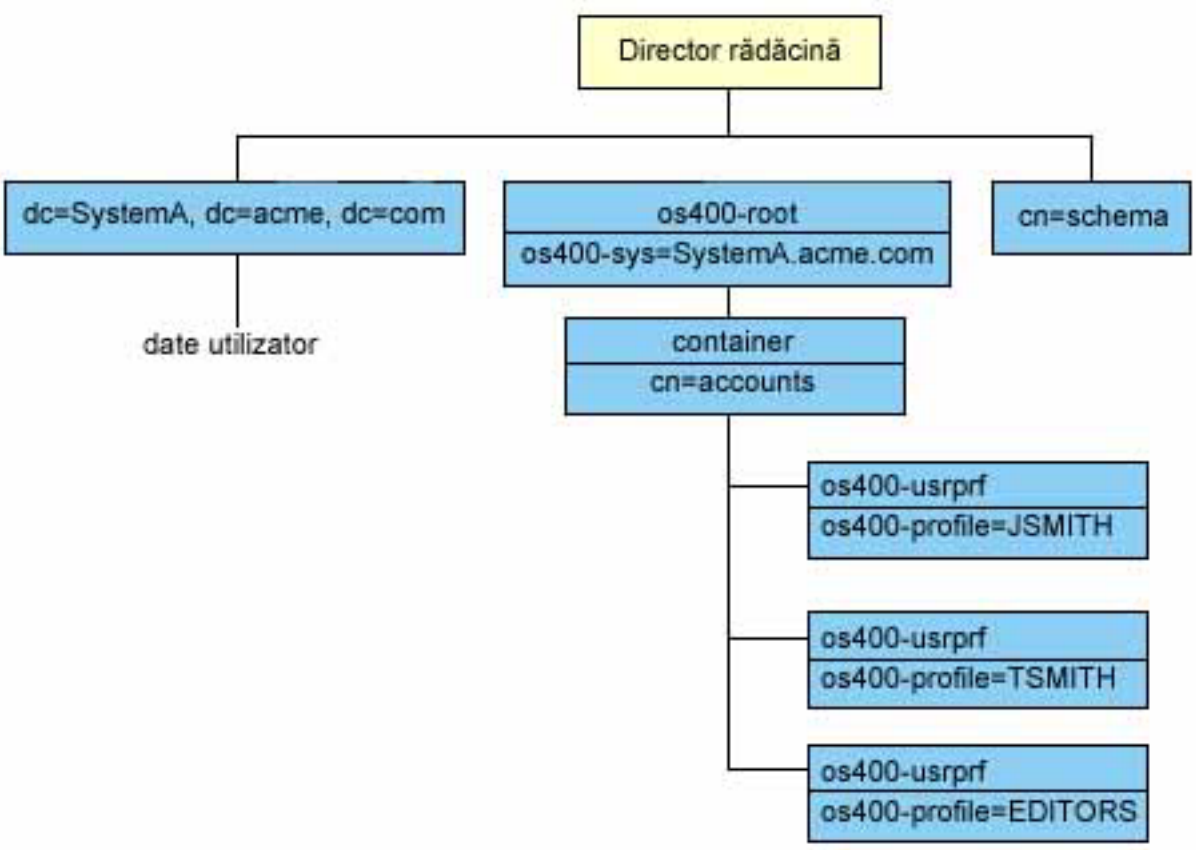
- “Arborele de informaţii director proiectat al utilizatorului i5/OS” la pagina 66

- “Operaţii LDAP” la pagina 67
- “DN-uri legate administrator şi replică” la pagina 70
- “Schema proiectată-utilizator i5/OS” la pagina 70

Arborele de informaţii director proiectat al utilizatorului i5/OS

Figura de mai jos prezintă un arbore de informaţii director (DIT) exemplu pentru backend-ul proiectat utilizator. Figura prezintă atât profilele individuale şi pe cele de grup. În figură, JSMITH şi TSMITH sunt profile utilizator, care este indicat intern de identificatorul de grup (GID), GID=*NONE (sau 0); EDITORS este un profil de grup, care este indicat intern de un GID diferit de zero.

Sufixul dc=SystemA,dc=acme,dc=com este inclus în figură pentru referinţă. Acest sufix reprezintă backend-ulcurent al bazei de date care gestionează alte intrări LDAP. Sufixul cn=schema este schema întinsă a serverului care este folosită curent.



Rădăcina arborelui este un sufix, care este implicit os400-sys=*SystemA.acme.com*, unde *SystemA.acme.com* este numele sistemului dumneavoastră. Objectclass este os400-root. Deşi DIT nu poate fi modificat sau şters, puteţi reconfigura sufixul obiectelor sistem. Oricum, trebuie să vă asiguraţi că sufixul curent nu este folosit în ACL-uri sau în altă parte în sistem unde ar trebui să fie modificate intrările dacă sufixul se schimbă.

În figura anterioară, containerul, cn=accounts, este afişat sub rădăcină. Acest obiect nu poate fi modificat. Un container este plasat la acest nivel în anticipaţia altor feluri de informaţii sau obiecte ce ar putea fi proiectate in viitor de sistemul de operare. Mai jos, în containerul cn=accounts sunt profilele utilizator care sunt proiectate ca objectclass=os400-usrprf. Profilele utilizator sunt referite ca profile de utilizator proiectate şi sunt cunoscute la LDAP în forma os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com.

Operaţii LDAP

Următoarele sunt operaţiile LDAP ce pot fi realizate folosind profilele de utilizator proiectate.

Legare

Un client LDAP se poate lega (autentifica) la serverul LDAP folosind un profil de utilizator proiectat. Aceasta este realizată prin specificarea numelui distinctiv (distinguished name - DN) al profilului de utilizator proiectat pentru DN-ul de legare şi parola corectă a profilului de utilizator i5/OS pentru autentificare. Un exemplu de DN folosit într-o cerere de legare este os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com.

Un client trebuie să se lege ca un utilizator proiectat pentru a accesa informaţii în backend-ul proiectat în sistem.

Sunt disponibile două mecanisme suplimentare pentru autentificarea la serverul de directoare ca un utilizator i5/OS:

- Legarea GSSAPI SASL. Dacă i5/OS este configurat să folosească Enterprise Identity Mapping (EIM), serverul de directoare interoghează EIM pentru a determina dacă există o legare cu un profil de utilizator i5/OS local din identitatea Kerberos iniţială. Dacă există o astfel de asociere, serverul va asocia profilul de utilizator cu conexiunea şi poate fi folosit pentru a accesa backend-ul proiecţiei sistem. Pentru mai multe informaţii despre EIM, vedeţi capitolul EIM .
- Legarea OS400-PRFTKN SASL. Un jeton de profil poate fi folosit pentru autentificarea la serverul de directoare. Serverul asociază profilul de utilizator al jetonului de profil cu conexiunea.

Serverul realizează toate operaţiile folosind autorizarea acelui profil de utilizator. Profilul de utilizator proiectat DN poate fi de asemenea în ACL-urile LDAP ca alte DN-uri intrări LDAP. Metoda simplă de legare este singura metodă de legare care este permisă când într-o cerere de legare este specificat un profil de utilizator proiectat.

Căutare

Backend-ul proiectat în sistem suportă unele filtre elementare de căutare. Puteţi specifica atributele objectclass, os400-profile şi os400-gid în filtrele de căutare. Atributul os400-profile suportă înlocuitori generici. Atributul os400-gid este limitat la specificarea (os400-gid=0), care este un profil de utilizator individual sau !(os400-gid=0), care este un profil de grup. Puteţi extrage toate atributele unui profil de utilizator exceptând parola şi atributele similare.

Pentru anumite filtre, sunt întoarse doar valorile DN objectclass şi os400-profile. Totuşi, căutările repetate pot conduce la întoarcerea unor informaţii mai detailate.

Următorul tabel descrie comportamentul sistemului proiectat backend pentru asemenea operaţii.

Tabela 2. Comportamentul backend-ului proiectat sistem pentru operaţii de căutare

Cerere de căutare	Baza de căutare	Scopul de căutare	Filtrul de căutare	Comentarii
Întoarce informaţii pentru os400-sys=SystemA, (opţional) pentru containerele de sub acesta şi (opţional) pentru obiectele din acele containere.	os400-sys=SystemA.acme.com	base, sub sau one	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	Întoarce atributele corespunzătoare şi valorile lor pe baza scopului şi filtrului specificat. Atributele codate hardware şi valorile lor sunt întoarse pentru sufixele obiectelor sistem şi pentru containerul de sub acesta.

Tabela 2. Comportamentul backend-ului proiectat sistem pentru operaţii de căutare (continuare)

Cerere de căutare	Baza de căutare	Scopul de căutare	Filtrul de căutare	Comentarii
Returnarea tuturor profilelor de utilizator.	cn=accounts, os400-sys=SystemA.acme.com	one sau sub	os400-gid=0	Doar valorile nume distinctiv (DN), objectclass şi profil-os400 sunt returnate pentru profile utilizator proiectate. Dacă este specificat un filtru, LDAP_UNWILLING_ Este întors TO_PERFORM.
Returnarea tuturor profilelor de grup.	cn=accounts, os400-sys=SystemA.acme.com	one sau sub	(!(os400-gid=0))	Doar valorile nume distinctiv (DN), objectclass şi profil-os400 sunt returnate pentru profile utilizator proiectate. Dacă este specificat un filtru, LDAP_UNWILLING_ Este întors TO_PERFORM.
Returnarea tuturor profilelor de utilizator şi de grup.	cn=accounts, os400-sys=SystemA.acme.com	one sau sub	os400-profile=*	Doar valorile nume distinctiv (DN), objectclass şi profil-os400 sunt returnate pentru profile utilizator proiectate. Dacă este specificat un filtru, LDAP_UNWILLING_ Este întors TO_PERFORM.
Returnează informaţii pentru un anumit profil de utilizator sau de grup cum ar fi profilul utilizator JSMITH.	cn=accounts, os400-sys=SystemA.acme.com	one sau sub	os400-profile=JSMITH	Pot fi specificate alte atribute care să fie întoarse.
Returnează informaţii pentru un anumit profil de utilizator sau de grup cum ar fi profilul utilizator JSMITH.	os400-profile=JSMITH, cn=accounts, os400-sys=SystemA.acme.com	bas, sub sau one	objectclass=os400-usrprf objectclass=* os400-profile=JSMITH	Pot fi specificate alte atribute care să fie întoarse. Deşi poate fi specificat un scop de un nivel, rezultatele căutării nu vor întoarce valori, deoarece nu este nimic sub profilul utilizator JSMITH din DIT.
Returnarea tuturor profilelor de utilizator şi de grup care încep cu A.	cn=accounts, os400-sys=SystemA.acme.com	one sau sub	os400-profile=A*	Doar valorile nume distinctiv (DN), objectclass şi profil-os400 sunt returnate pentru profile utilizator proiectate. Dacă este specificat un filtru, LDAP_UNWILLING_ Este întors TO_PERFORM.

Tabela 2. Comportamentul backend-ului proiectat sistem pentru operaţii de căutare (continuare)

Cerere de căutare	Baza de căutare	Scopul de căutare	Filtrul de căutare	Comentarii
Returnarea tuturor profilelor de grup care încep cu G.	cn=accounts, os400-sys=SystemA.acme.com	one sau sub	(&(!(os400-gid=0)) (os400-profile=G*))	Doar valorile nume distinctiv (DN), objectclass şi profil-os400 sunt returnate pentru profile utilizator proiectate. Dacă este specificat un filtru, LDAP_UNWILLING_ Este întors TO_PERFORM.
Returnarea tuturor profilelor de utilizator care încep cu A.	cn=accounts, os400-sys=SystemA.acme.com	one sau sub	(&(os400-gid=0) (os400-profile=A*))	Doar valorile nume distinctiv (DN), objectclass şi profil-os400 sunt returnate pentru profile utilizator proiectate. Dacă este specificat un filtru, LDAP_UNWILLING_ Este întors TO_PERFORM.

Comparare

Operaţia de comparare LDAP poate fi folosită pentru a compara o valoarea de atribut a unui profil de utilizator proiectat. Atributele os400-aut şi os400-docpwd nu pot fi comparate.

Adăugare şi modificare

Puteţi crea profile utilizator folosind operaţia de adăugare LDAP şi puteţi de asemenea modifica profile utilizator folosind operaţia de modificare LDAP.

Ştergere

Profilele utilizator pot fi şterse folosind operaţia de ştergere LDAP. Penru a specifica comportamentul parametrilor DLTUSRPRF OWNOBJOPT şi PGPOPT, sunt furnizate acum două controale server LDAP. Aceste controale pot fi specificate la operaţia de ştergere LDAP. Vedeţi comanda DLTUSRPRF (Delete User Profile - Ştergere profil de utilizator) pentru mai multe informaţii despre comportamentul acestor parametri.

Următoarele sunt controale şi identificatorii lor obiect (OID) care pot fi specificaţi la operaţia de ştergere client LDAP.

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  Valoarea de control este un şir de caractere de forma următoare:

  – controlValue::= ownObjOpt [newOwner]
  – ownObjOpt::= *NODLT / *DLT / *CHGOWN

  Valoarea de control ownObjOpt specifică acţiunea care trebuie realizată dacă profilul utilizator deţine vreun obiect. Valoarea *NODLT indică să nu se şteargă profilul utilizator dacă profilul utilizator deţine vreun obiect. Valorea *DLT indică să se şteargă obiectele deţinute, iar valoarea *CHGOWN indică să se transfere dreptul de proprietate la alt profil.

  Valoarea newOwner specifică profilul cărui îi este transferat dreptul de proprietate. Această valoare este cerută când ownObjOpt este setat la *CHGOWN.

  Exemple ale valorilor de control sunt următoarele:

  – *NODLT: specifică faptul că profilul nu poate fi şters dacă deţine vreun obiect
  – *CHGOWN SMITH: specifică că se transfere dreptul de proprietate al oricărui obiect la profilul de utilizator SMITH.

- Identificatorul obiect (OID) este definit în ldap.h as LDAP_OS400_OWNOBJOPT_CONTROL_OID.
  - os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

    Valoarea de control este definită ca un şir de caractere de forma următoare:

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

    Valoarea pgpOpt specifică acţiunea de efectuat dacă profilul care este şters este grupul primar pentru orice obiecte. Dacă este specificat *CHGPGP, newPgp trebuie de asemenea specificat. Valoarea newPgp specifică numele profilului de grup primar sau *NONE. Dacă este specificat un nou profil de grup primar, valoarea newPgpAut poate fi de asemenea specificată. Valoarea newPgpAut specifică autorizarea asupra obiectelor care îi este dată noului grup primar.

  Exemple de valoarilor de control sunt următoarele:
  - *NOCHG: specifică faptul că profilul nu poate fi şters dacă este grupul primar pentru orice obiect.
  - *CHGPGP *NONE: specifică să se înlăture grupul primar pentru obiecte.
  - *CHGPGP SMITH *USE: specifică să se modifice grupul primar la profilul utilizator SMITH şi de a acorda autorizarea *USE grupului primar.

  Dacă vreunul din aceste controale nu este specificat la ştergere, sunt utilizate valorile implicite pentru comanda QSYS/DLTUSRPRF.

ModRDN

Nu puteţi redenumi profilele utilizator proiectate deoarece aceasta nu este suportată de sistemul de operare.

Importarea şi exportarea API-urilor

Api-urile QgldImportLdif şi QgldExportLdif nu suportă importarea sau exportarea datelor din cadrul bechend-ului proiectat în sistem.

DN-uri legate administrator şi replică

Puteţi specifica un profil de utilizator proiectat ca DN-ul de legare configurat administrator sau replică. Este utilizată parola profilului utilizator. Profilele utilizator proiectate pot deveni de asemenea administratori LDAP dacă sunt autorizate la identificatorul funcţiei Directory Server Administrator (QIBM_DIRSRV_ADMIN). Profilelor multiple de utilizator le pot fi acordate acces de administrator.

Pentru informaţii suplimnetare consultaţi “Lucrul cu accesul administrativ pentru utilizatori autorizaţi” la pagina 101.

Schema proiectată-utilizator i5/OS

Clasele de obiecte şi atributele de la backend-ul proiectat pot fi găsite în schema de întindere server. Numele atributelor LDAP sunt în formatul os400–*nnn*, unde *nnn* este în mod tipic cuvântul cheie al unui atribut al comenzilor profilului de utilizator. De exemplu, atributul os400-usrcls corespunde cu parametrul USRCLS al comenzii CRTUSRPRF. Valorile atributelor corespund cu valorile parametrilor acceptate de către comenzile CRTUSRPRF şi CHGUSRPRF sau cu valorile afişate la afişarea unui profil de utilizator. Folosiţi unealta de administrare Web sau altă aplicaţie pentru a vedea definiţiile clasei de obiect (objectclass) os400-usrprf şi atributele os400-xxx asociate.

Directory Server şi suportul de jurnalizare i5/OS

Directory Server foloseşte suportul bază de date i5/OS pentru a memora informaţii director. Directory Server foloseşte controlul comiterii pentru a memora intrările director în baza de date. Acesta necesită suportul de jurnalizare i5/OS.

Când serverul sau unealta de importare LDIF este pornită pentru prima oară, sunt construite următoarele:

- Un jurnal
- Un receptor jurnal
- Orice bază de date necesară iniţial

Juranlul QSQJRN este construit în biblioteca bazei de date car aţi configurat-o. Receptorul jurnal QSQJRN0001 este creat iniţial în biblioteca bazei de date care aţi configurat-o.

Mediul dumneavoastră, mărimea şi structura directorului sau strategia de salvare şi restaurare poate dicta unele diferenţe de la implicit, incluzând cum aceste obiecte sunt gestionate şi starea threshold-ului folosit. Puteţi modifica parametrii comenzii de jurnalizare dacă este necesar. Jurnalizarea LDAP este setată implicit entru a şterge receptorii vechi. Dacă comanda de modificare jurnal este configurată şi vreţi să păstraţi receptorii vechi, executaţi următoarea comandă de la o linie de comandă i5/OS:

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

Dacă istoricul de modificări este configurat, puteţi şterge vechii receptori de jurnal cu următoarea comandă:

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

Pentru informaţii despre comenzile de jurnalizare, vedeţi “ Comenzile OS/400” în capitolul Programare.

Atribute operaţionale

Există mai multe atribute care au o semnificaţie specială pentru Directory Server cunoscute ca atribute operaţionale. Acestea sunt atribute care sunt menţinute de către server şi ori reflectă informaţiile pe care serverul le administrează legate de o intrare, ori afectează operarea serverului. Aceste atribute au caracteristici speciale:

- Atributele nu sunt returnate de o operaţie de căutare decât dacă ele sunt cerute în mod special (după nume) în cererea de căutare
- Atributele nu fac parte din nici o clasă de obiect. Serverul controlează ce intrări au atributele.

Următoarele seturi de atribute operaţionale sunt suportate de către Directory Server:

- creatorsName, createTimestamp, modifiersName, modifyTimestamp. Prezente la fiecare intrare. Aceste atribute arată DN-ul şi momentul legării când o intrare a fost creată sau modificată ultima dată. Puteţi folosi aceste atribute în filtre de căutare, de exemplu, pentru a găsi toate intrările modificate după un moment de timp specificat. Aceste atribute nu pot fi modificate de nici un utilizator.
- ibm-entryuuid. Prezent la fiecare intrare care este creată când serverul este la V5R3 sau ulterior. Acest atribut este un identificator şir de caractere unic universal asignat fiecărei intrări de către server când este creată o intrare. Este folositor pentru aplicaţiile care trebuie să distingă între intrări cu acelaşi nume de pe servere diferite. Atributul foloseşte algoritmul DCE UUID pentru a genera un ID care este unic peste toate intrările de pe toate serverele folosind o amprentă de timp, adresă de adaptor şi alte informaţii.
- entryowner, ownersource, ownerpropagate, aclentry, aclsource, aclpropagate, ibm-filteracl, ibm-filteraclinherit, ibm-effectiveAcl. Pentru informaţii suplimnetare consultaţi “Liste de control al accesului” la pagina 48.
- hasSubordinates. Prezent la fiecare intrare şi are valoarea TRUE dacă intrarea are subordonări.
- numSubordinates. Prezent la fiecare intrare şi conţine numărul de intrări care sunt fii ai acestei intrări.
- pwdChangedTime, pwdAccountLockedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdReset, pwdHistory. (atribute de politică parolă).

- subschemasubentry - Prezent la fiecare intrare şi identifică locaţia schemei pentru acea parte a arborelui. Acesta este util pentru serverele cu mai multe scheme dacă vreţi să găsiţi schema pe care vreţi să o folosiţi în acea parte a arborelui.

Controale şi operaţii extinse

Controale

Controalele oferă informaţii suplimentare către server pentru a controla cum interpretează el o cerere dată. De exemplu, un control ştergere subarbore poate fi specificat într-o cerere de ştergere LDAP, indicând că serverul ar trebui să şteargă intrarea şi toate intrările ei subordonate, în loc de a şterge doar intrarea specificată. Un control constă din trei părţi:

- Tipul de control, care este un OID care identifică controlul.
- Un indicator de criticalitate, care specifică cum ar trebui serverul să se comporte dacă nu suportă controlul. Aceasta este o valoare Boolean. FALSE indică faptul că controlul nu este critic şi serverul ar trebui să îl ignore dacă nu îl suportă. TRUE indică faptul că controlul este critic şi întreaga cerere ar trebui să eşueze (cu o eroare de extensie critică nesuportată) dacă serverul nu poate onora controlul.
- O valoare de control opţională, care conţine alte informaţii specifice controlului. Conţinutul valorii de control este specificat folosind notaţia ASN.1. Valoarea însăşi este codificarea BER a datelor de control.

Următoarele controale sunt suportate de către Directory Server:

Nume	OID	Cea mai veche ediţie OS/400	Cea mai veche ediţie IBM Directory Server	Descriere
Manage DSA IT	2.16.840.1.1137.30.3.4.2	V4R5	V3.2	Tratează intrările trimitere ca intrări obişnuite.
Tranzacţie	1.3.18.0.2.10.5	V4R5	V3.2	Marchează o operaţie ca parte a tranzacţiei.
OS/400 DLTUSRPRF OWNOBJOPT	1.3.18.0.2.10.8	V5R2		Opţiune de ştergere profil de utilizator OS/400 pentru proprietarul obiectului. Vedeţi “Backend proiectat pe sistemul de operare” la pagina 65 pentru detalii.
OS/400 DLTUSRPRF PGPOPT	1.3.18.0.2.10.9	V5R2		Opţiune de ştergere profil de utilizator OS/400 pentru grupul primar. Vedeţi “Backend proiectat pe sistemul de operare” la pagina 65 pentru detalii.
Căutare sortată	1.2.840.113556.1.4.473 (cerere) şi 1.2.840.113556.1.4.474 (răspuns)	V5R2 cu PTF	V4.1	Sortare rezultate căutare înainte de a întoarce intrările către client.

Nume	OID	Cea mai veche ediţie OS/400	Cea mai veche ediţie IBM Directory Server	Descriere
Căutare paginată	1.2.840.113556.1.4.319	V5R2 cu PTF	V4.1	Întoarce către client rezultatele căutării în pagini în loc de a le întoarce pe toate deodată.
Control ştergere arbore	1.2.840.113556.1.4.805	V5R3	V5.1	Acest control este ataşat unei cereri de Ştergere pentru a indica că intrarea specificată şi toate intrările descendente vor fi şterse. Utilizatorul trebuie să fie un administrator al directorului. Intrarea care va fi ştearsă nu poate fi un context de replicare.
Politică parolă	1.3.6.1.4.1.42.2.27.8.5.1	V5R3	V5.1	Întoarce către client informaţiile suplimentare de eroare de politică parolă.
Administrare server	1.3.18.0.2.10.15	V5R3	V5.1	Permite administratorului să efectueze operaţii de reparare care ar fi în mod normal refuzate (de exemplu: actualizarea unei replici numai-citire, actualizarea unui server liniştit sau setarea anumitor atribute operaţionale).

Operaţii extinse

Operaţiile extinse sunt folosite pentru a porni operaţii suplimentare dincolo de operaţiile LDAP de bază. De exemplu, operaţiile extinse au fost definite pentru a grupa un set de operaţii într-o singură tranzacţie. O operaţie extinsă constă din:

- Numele cererii, un OID care identifică operaţia respectivă.
- O valoare de cerere opţională, care conţine alte informaţii specifice operaţiei. Conţinutul valorii de cerere este specificat folosind notaţia ASN.1. Valoarea însăşi este codificarea BER a datelor de cerere.

Operaţiile extinse au în mod tipic un răspuns extins. Răspunsul constă din:

- Componentele rezultatului LDAP standard (codul de eroare, DN-ul potrivit şi mesajul de eroare)
- Numele răspunsului, un OID care identifică tipul de răspuns
- O valoare opţională, care conţine alte informaţii specifice răspunsului. Conţinutul valorii de răspuns este specificat folosind notaţia ASN.1. Valoarea însăşi este codificarea BER a datelor de răspuns.

Următoarele cereri extinse sunt suportate de către Directory Server:

Nume	OID	Cea mai veche ediţie OS/400	Cea mai mică ediţie IBM Directory Server	Descriere
Înregistrare pentru evenimente	1.3.18.0.2.12.1	V4R5	V3.2	
Dezînregistrare pentru evenimente	1.3.18.0.2.12.3	V4R5	V3.2	
Începere tranzacţie	1.3.18.0.2.12.5	V4R5	V3.2	
Terminare tranzacţie	1.3.18.0.2.12.6	V4R5	V3.2	
Cerere normalizare DN	1.3.18.0.2.12.30	V5R3	V5.1	

Sunt definite operaţii extinse suplimentare care nu sunt intenţionate a fi pornite de către un client. Aceste operaţii sunt folosite prin intermediul utilitarului ldapexop sau prin operaţii efectuate de către unealta de Administrare Web. Aceste operaţii şi autoritatea necesară pentru a le porni, sunt listate mai jos:

Nume	OID	Cea mai veche ediţie OS/400	Cea mai mică ediţie IBM Directory Server	Descriere
Replicare control	1.3.18.0.2.12.16	V5R3	V5.1	Această operaţie efectuează acţiunea cerută pe serverul pe care a fost lansată şi cascadează apelul către toţi consumatorii de sub el din topologia de replicare. Clientul trebuie să fie administratorul directorului sau să aibă autorizare de scriere pentru obiectul ibm-replicagroup=default pentru contextul de replicare asociat.
Coada de replicare control	1.3.18.0.2.12.17	V5R3	V5.1	Această operaţie marchează elementele ca deja replicate pentru o înţelegere specificată. Această operaţie este permisă doar când clientul are autoritate de scriere pentru acordul (agreement) de replicare.

Nume	OID	Cea mai veche ediţie OS/400	Cea mai mică ediţie IBM Directory Server	Descriere
Liniştire (quiesce) sau trezire (unquiesce)	1.3.18.0.2.12.17	V5R3	V5.1	Această operaţie pune subarborele într-o stare în care el nu acceptă actualizări client (sau termină această stare), cu excepţia acelora de la clienţi autentificaţi ca administrator al directorului în care este prezent controlul de Administrare Server. Clientul trebuie să fie autentificat ca administratorul directorului sau să aibă autoritate de scriere pentru obiectul ibm-replicagroup=default pentru contextul de replicare asociat.
Terminare tranzacţie	1.3.18.0.2.12.19	V5R3	V5.1	
Cascadarea replicării controlului	1.3.18.0.2.12.15	V5R3	V5.1	Această operaţie efectuează acţiunea cerută pe server şi este emisă către şi cascadează apelul către toţi consumatorii de sub el din topologia de replicare. Clientul trebuie să fie administratorul directorului sau să aibă autorizare de scriere pentru obiectul ibm-replicagroup=default pentru contextul de replicare asociat.
Actualizare configuraţie	1.3.18.0.2.12.28	V5R3	V5.1	Această operaţie este folosită pentru a face ca serverul să recitească setările specificate din configuraţia lui. Operaţia este permisă doar când clientul este administratorul directorului.

Capitolul 5. Iniţierea cu Directory Server

Directory Server este instalat automat când instalaţi i5/OS. Directory Server include o configuraţie implicită. Pentru a începe lucrul cu Directory Server, faceţi următoarele:

1. Dacă instalaţi V5R3 şi aţi folosit Directory Server pe o ediţie anterioară, atunci revedeţi considerentele legate de migrare. Pentru informaţii suplimentare consultaţi “Considerente de migrare”.
2. Planificaţi-vă Directory Server. Pentru informaţii suplimentare consultaţi “Planificarea Directory Server” la pagina 81.
3. Pentru a personaliza setările Directory Server, rulaţi vrăjitorul de configurare Directory Server. Pentru mai multe informaţii vedeţi “Configurarea Directory Server” la pagina 82.
4. Porniţi serverul. Pentru informaţii suplimentare consultaţi “Pornirea Directory Server” la pagina 96
5. Folosiţi unealta de administrare Web pentru a crea sau edita directoarele LDAP. Pentru mai multe informaţii vedeţi “Administrarea Web” la pagina 83.
6. Citiţi informaţiile din secţiunea Capitolul 7, “Administrarea Directory Server”, la pagina 95 pentru a găsi mai multe informaţii despre cum să efectuaţi diverse operaţii asupra serverului Directory Server.

Considerente de migrare

Directory Server este instalat automat când instalaţi i5/OS. Prima dată când serverul este pornit, el migrează automat orice configuraţii şi date existente. Aceasta poate produce o întârziere mare înainte ca serverul să fie pornit prima dată.

Dacă aveţi un Directory Server care rulează pe V5R2 sau V5R1, vedeţi “Migrarea la V5R3 de la V5R2 sau V5R1”.

Dacă aveţi un Directory Server care rulează pe V4R3, V4R4 sau V4R5, puteţi migra datele dvs. la V5R3. Pentru informaţii suplimentare consultaţi “Migrarea datelor de la V4R3, V4R4 sau V4R5” la pagina 78.

Dacă aveţi o reţea de servere de replicare, vedeţi “Migrarea unei reţele de servere de replicare” la pagina 79 pentru mai multe informaţii.

Dacă folosiţi Kerberos, vedeţi “Modificarea numelui serviciului Kerberos” la pagina 81.

Migrarea la V5R3 de la V5R2 sau V5R1

V5R3 a OS/400 introduce noi caracteristici şi capabilităţi la Directory Server. Aceste modificări afectează şi serverul de directoare LDAP şi interfaţa grafică utilizator (GUI) a Navigator iSeries. Pentru a beneficia de avantajele noilor caracteristici GUI, trebuie să instalaţi Navigator iSeries pe un PC care poate comunica peste TCP/IP la serverul iSeries. Navigator iSeries este o componentă a iSeries Access pentru Windows. Dacă aveţi instalată o versiune anterioară a Navigator iSeries, ar trebui să faceţi o modernizare la V5R3.

V5R3 a OS/400 suportă modernizări de la V5R1 şi V5R2. Când modernizaţi la V5R3 a OS/400, atât datele directorului LDAP şi fişierele schemei director sunt migrate automat pentru a se conforma la formatele V5R3.

Când modernizaţi la V5R3 a OS/400, ar trebui să fiţi conştient de unele probleme de migrare:

- Când modernizaţi la V5R3, Directory Server migrează automat fişierele schemă la V5R3 şi şterge vechile fişiere schemă. Totuşi, dacă aţi şters sau redenumit fişierele schemă, Directory Server nu le poate migra. Puteţi primi o eroare sau Directory Server poate asuma că fişierele au fost deja migrate.
- Directory Server migrează datele director la formatul V5R3 prima dată când porniţi serverul sau importaţi un fişier LDIF. Planificaţi să alocaţi ceva timp pentru ca această migrare să fie completă.

  După ce modernizaţi la V5R3, ar trebui să porniţi serverul o dată pentru a migra datele existente înainte de a importa noile date. Dacă încercaţi să importaţi date înainte de a porni serverul o dată şi nu aveţi suficientă autoritate, importul poate eşua.

- Urmând migrarea, serverul de directoare LDAP va porni automat când porneşte TCP/IP. Dacă nu vreţi ca serverul de directoare să pornească automat, folosiţi Navigator iSeries pentru a schimba setarea.

Migrarea datelor de la V4R3, V4R4 sau V4R5

OS/400 V5R3 nu suportă modernizări directe de la V4R3, V4R4 sau V4R5. Dacă vreţi să migraţi Directory Server V4R3, V4R4 sau V4R5 la V5R3, puteţi urma oricare dintre următoarele proceduri:

- "Modernizarea OS/400 de la V4R3, V4R4 sau V4R5 la o ediţie interimară"
- "Salvarea bibliotecii bază de date şi instalarea V5R3" la pagina 79

Înainte de a porni, citiţi următoarele:

- Când modernizaţi de la V4R3 la orice ediţie posterioară, trebuie să ştiţi următoarele probleme:
  - **Migrarea fişierului inel de chei la o bază de date de chei:**

    Serverul de directoare LDAP foloseşte de asemnea ca şi fişier inel de chei propria conexiune SSL în V4R3. Începând cu V4R4 acesta foloseşte memorarea certificatelor sistem. Dacă serverul dumneavoastră a fost setat să folosească SSL în V4R3, conţinutul fişierul inel de chei va fi migrat la memoria certificatului sistem.
  - **Două fişiere şir au fost înlăturate:**

    Următoarele fişiere folosite de Directory Server în V4R3 nu mai sunt necesare şi sunt înlăturate când instalaţi o ediţie posterioară:

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

    Nu trebuie să luaţi vreo acţiune cu aceste fişiere. Aceasta este menţionată doar dacă nu sunteţi îngrijorat dacă observaţi că nu mai sunt prezente pe sistemul dumneavoastră.
- V4R4 şi ediţiile anterioare ale Directory Server nu ţin cont de fusurile orare când creează intrări amprentă de timp. Începând cu V4R5, fusul orar este folosit în toate adăugările şi modificările la director. De aceea, dacă modernizaţi datele de la V4R4 sau anterior, Directory Server adjustează atributele existente createtimestamp şi modifytimestamp pentru a reflecta fusul orar corect. Face asta prin extragerea fusului orar care este definit curent pe sistemul iSeries din amprentele de timp care sunt memorate în director. Notaţi că dacă fusul orar curent nu este aceelaşi fus orar care a fost activ când intrările au fost create sau modificate original, noile valori amprentă de timp nu vor reflecta fusul orar original.
- Dacă modernizaţi datele de la V4R4 sau anterior, fiţi conştient că datele director vor necesita aproximativ de două ori mai mult spaţiu de stocare decât necesita anterior. Aceasta se întâmplă deoarece în V4R4 sau versiunile anterioare, Directory Server suporta doar setul de caractere IA5 şi salva date în ccsid 37 (format octet singur). Directory Server suportă setul complet de caractere ISO 10646. După ce modernizaţi, ar trebui să porniţi serverul o dată pentru a migra datele existente înainte de a importa noile date. Dacă încercaţi să importaţi date înainte de a porni serverul o dată şi nu aveţi suficientă autoritate, importul poate eşua.
- De asemenea fiţi conştient că pot fi şi alte probleme asociate cu trecerea la ediţia curentă de la alte ediţii.

Modernizarea OS/400 de la V4R3, V4R4 sau V4R5 la o ediţie interimară

Prin modernizări de la V4R3, V4R4 şi V4R5 ale OS/400 la V5R3 nu sunt suportate, sunt suportate următoarele modernizări:

- V4R3 şi V4R4 modernizate la V4R5
- V4R4 şi V4R5 modernizate la V5R1
- V4R5 şi V5R1 modernizate la V5R2
- V5R1 şi V5R2 modernizate la V5R3

Un mod de a migra serverul dvs. Directory Server este de a moderniza la o ediţie interimară (V5R1 sau V5R2), apoi la V5R3. Pentru informaţii detaliate despre procedurile de instalare OS/400, vedeţi *Instalarea Software*  . Urmaţi aceşti paşi generali pentru a realiza migrarea:

1. Notaţi orice modificare care aţi făcut-o la fişierele schemă din directorul /QIBM/UserData/OS400/DirSrv. Fişierele schemă sunt migrate automat.
2. Pentru V5R3, faceţi instalarea lui V4R5.

3. Pentru V4R4 sau V4R5, faceţi instalarea lui V5R1 sau V5R2.
4. Faceţi instalarea lui V5R3.
5. Porniţi Directory Server dacă nu este deja pornit.
6. Folosiţi unealta de administrare Web pentru a modifica fişierele schemă pentru orice modificări utilizatori pe care le-aţi notat în pasul 1 la pagina 78.
7. Reporniţi Directory Server.

Salvarea bibliotecii bază de date şi instalarea V5R3

Puteţi migra serverul Directory Server prin salvarea bibliotecii bază de date pe care Directory Server o foloseşte în V4R3, V4R4 sau V4R5 şi apoi restaurarea ei după instalarea V5R3. Această vă scuteşte de pasul de instalare a unei ediţii interimare. Oricum, setările serverului nu sunt migrate, astfel că trebuie să reconfiguraţi setările serverului. Pentru informaţii detaliate despre procedurile de instalare OS/400, vedeţi *Instalarea Software* . Urmaţi aceşti paşi generali pentru a realiza migrarea:

1. Notaţi orice modoficare care aţi făcut-o la fişierele schemă din directorul /QIBM/UserData/OS400/DirSrv. Fişierele schemă nu sunt migrate automatic, aşa încât dacă vreţi să vă păstraţi schimbările va trebui să le implementaţi manual din nou.
2. Notaţi diversele setări de configurare din proprietăţile Directory Server, inclusiv numele bibliotecii bază de date.
3. Salvaţi biblioteca bază de date care este specificată în configuraţia Directory Server. Dacă aţi configurat istoricul de modificări, atunci va trebui de asemenea să salvaţi biblioteca QUSRDIRCL.
4. Notaţi configuraţia de publicare.
5. Instalaţi V5R3 a OS/400 de pe sistem.
6. Folosiţi EZ-Setup pentru a configura Directory Server.
7. Restauraţi biblioteca bazei de date pe care aţi salvat-o în pasul 3. Dacă aţi salvat biblioteca QUSRDIRCL în pasul 3, restauraţi-o acum.
8. Folosiţi unealta de administrare Web pentru a modifica fişierele schemă pentru orice modificări utilizatori pe care le-aţi notat în pasul 1.
9. Folosiţi Navigator iSeries pentru a reconfigura Directory Server. Specificaţi biblioteca bază de date care a fost configurată anterior şi care a fost salvată şi restaurată în paşii anteriori
10. Folosiţi Navigator iSeries pentru a reconfigura publicarea.
11. Reporniţi Directory Server.

Migrarea unei reţele de servere de replicare

Prima dată când este pornit serverul master, acesta migrează informaţiile din directorul care controlează replicarea. Intrările cu objectclass replicaObject de sub cn=localhost sunt înlocuite cu intrări folosite de către modelul de replicare (pentru mai multe informaţii, vedeţi “Replicare” la pagina 35). Serverul master este configurat să replice toate sufixele din director. Intrările de acord (agreement) sunt create cu atributul ibm-replicationOnHold setat la valoarea adevărat. Aceasta permite ca actualizările făcute la master să fie acumulate pentru replică până când replica este gata.

Aceste intrări sunt denumite topologia de replicare. Noul master poate fi folosit cu replici care rulează versiuni anterioare; datele legate de noile facilităţi nu vor fi replicate către serverele de pe nivelul anterior. Este necesar să exportaţi intrările topologiei de replicare de la master şi să le adăugaţi la fiecare replică după ce serverul replică a fost migrat. Pentru a exporta intrările, folosiţi unealta din linia de comandă Qshell “ldapsearch” la pagina 171 şi salvaţi ieşirea într-un fişier. Comanda de căutare este similară cu următoarea:

```
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
```

Această comandă creează un fişier LDIF de ieşire numit replication.topology.ldif în directorul de lucru curent. Fişierul conţine doar noile intrări.

Notă: Nu includeţi următoarele sufixe:

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

Includeţi doar sufixele create de utilizator.

Repetaţi comanda pentru fiecare intrare sufix de pe master, dar înlocuiţi ">" cu ">>" pentru a adăuga datele la sfârşitul fişierului de ieşire pentru căutări ulterioare. După ce fişierul este complet, copiaţi-l la serverele replică.

Adăugaţi fişierul la serverele replica după ce au fost migrate cu succes; nu adăugaţi fişierul la serverele care rulează versiuni anterioare ale serverului de directoare. Trebuie să porniţi şi să opriţi serverul înainte de a adăuga fişierul.

Pentru a porni serverul, folosiţi opţiunea **Pornire** din Navigator iSeries. Pentru informaţii suplimentare consultaţi "Pornirea Directory Server" la pagina 96.

Pentru a opri serverul, folosiţi opţiunea **Oprire** din Navigator iSeries. Pentru informaţii suplimentare vedeţi, "Oprirea Directory Server" la pagina 96.

Când adăugaţi fişierul la un server replică, asiguraţi-vă că serverul replică nu este pornit. Pentru a adăuga datele, folosiţi opţiunea **Importare fişier** din Navigator iSeries.

După ce intrările topologiei de replicare sunt încărcate, porniţi serverul şi reluaţi aplicaţia. Puteţi relua aplicaţia în una din următoarele moduri:

- Pe serverul master, folosiţi **Gestionare cozi din management replicare** din unealta de administrare Web.
- Folosiţi utilitarul linie de comandă **ldapexop**. De exemplu:

  ```
  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
  ```

  Această comandă reia aplicaţia pentru serverul definit în intrarea cu DN-ul specificat.

Pentru a determina care DN de acord replicare corespunde cu un server de replicare, verificaţi în fişierul replication.topology.ldif. Serverul master va înregistra în istoric un mesaj că replicarea a început pentru acea replică şi un avertisment că ID-ul serverului replică din acord nu se potriveşte cu ID-ul serverului replică. Pentru a actualiza acordul replică să folosească ID-ul serverului corect, folosiţi **Management replicare** din unealta de administrare Web sau unealta linie de comandă **ldapmodify**. De exemplu:

```
ldapmodify -c -h master-server-host-name -p master-server-port \
 -D master-server-admin-DN -w master-server-admin-password
dn: replica-agreement-DN
changetype: modify
replace: ibm-replicaConsumerID
ibm-replicaConsumerID: replica-server-ID
```

Puteţi introduce aceste comenzi direct în linia de comandă sau puteţi salva comenzile într-un fişier LDIF şi furnizaţi-le comenzii cu opţiunea **-i** *file*. Folosiţi **Terminare cerere anterioară** pentru a opri comanda.

Migrarea pentru această replică este încheiată.

Pentru a continua să folosiţi o replică care rulează o versiune anterioară, este încă necesar să reluaţi replicarea folosind unealta linie de comandă **ldapexop** sau **Management replicare** din unealta de administrare Web pentru acea replică. Dacă o replică ce rulează o versiune anterioară este migrată mai târziu, folosiţi unealta linie de comandă **ldapdiff** pentru a sincroniza datele director. Aceasta va asigura că intrările sau atributele care nu au fost replicate sunt actualizate pe replică.

Modificarea numelui serviciului Kerberos

În V5R3, numele serviciului folosit de serverul de directoare şi API-urile client pentru autentificare GSSAPI (Kerberos) sunt modificate. Această modificare este incompatibilă cu numele de serviciu folosit înainte de V5R3 (V5R2M0 PTF 5722SS1-SI08487 include aceeaşi modificare).

Anterior acestei ediţii, serverul de directoare i5/OS şi API-urile client au folosit un nume serviciu de forma LDAP/dns-host-name@Kerberos-realm când mecanismul GSSAPI (Kerberos) este folosit pentru autentificare. Acest nume nu se conformează cu standardele care definesc autentificarea GSSAPI, care spun că numele principal ar trebui să înceapă cu literele mici ″ldap″. Drept urmare, atât serverul de directoare i5/OS cât şi API-urile client ar putea să nu interopereze cu produsele altor vânzători. Aceasta este adevărat în special dacă centrul de distribuţie chei Kerberos (KDC) are nume de principali sensibile la majuscule. Furnizorul de servicii LDAP pentru JNDI, un API client Java LDAP folosit în mod curent, este un exemplu de client inclus cu i5/OS care foloseşte numele de serviciu corect.

V5R3M0 schimbă numele de serviciu ca să se conformeze cu standardele. Aceasta introduce oricum propriile probleme de compatibilitate.

- Un server de directoare configurat să folosească autentificarea GSSAPI nu va începe să instaleze această ediţie. Aceasta deoarece fişierul keytab folosit de către server are acreditări care folosesc nume vechi de serviciu (LDAP/mysys.ibm.com@IBM.COM), în timp ce serverul caută acreditări care folosesc noul nume de serviciu (ldap/mysys.ibm.com@IBM.COM).
- Un server de directoare sau aplicaţia LDAP care foloseşte API-uri LDAP la V5R3M0 ar putea să nu reuşească autentificarea cu servere sau clienţi i5/OS mai vechi. Pentru a corecta aceasta, ar trebui să faceţi următoarele:
  1. Dacă KDC foloseşte nume principal sensibile la majuscule, creaţi un cont care foloseşte numele service corect (ldap/mysys.ibm.com@IBM.COM).
  2. Actualizaţi fişierul keytab folosit de i5/OS Directory Server pentru a conţine acreditări pentru noul nume de service. Aţi putea dori să ştergeţi vechile acreditări. Puteţi folosi utilitarul Qshell keytab pentru a actualiza fişierul keytab. Implicit, serverul de directoare foloseşte fişierul /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab. Vrăjitorul NAS (Network Authentication Service) V5R3M0 (Kerberos) din Navigator iSeries creează de asemenea intrări keytab care folosesc noul nume de serviciu.
  3. Actualizaţi sistemele i5/OS V5R2M0, unde GSSAPI este folosit prin aplicarea PTF 5722SS1-SI08487.

Alternativ, puteţi alege să aveţi serverul de directoare şi API-urile client să continue să folosească numele de service vechi. Aceasta ar putea fi de dorit când folosiţi autentificare Kerberos într-o reţea mixtă de sisteme care rulează cu şi fără PTF-uri. Pentru a face aceasta, setaţi variabila de mediu LDAP_KRB_SERVICE_NAME. Puteţi seta aceasta pentru întregul sistem (necesat pentru a seta numele de service pentru server) folosind următoarea comandă:

```
ADDENVVAR ENVVAR(LDAP_KRB_SERVICE_NAME)
```

sau în QSH (pentru a afecta utilitarele LDAP rulate din această sesiune QSH):

```
export LDAP_KRB_SERVICE_NAME=1
```

Planificarea Directory Server

Înainte de a instala Directory Server şi a începe să vă configuraţi directorul LDAP, ar trebui să luaţi câteva minute pentru a planifica directorul. Lucrurile importante de considerat le includ pe următoarele:

- **Organizarea directorului**. Planificarea structurii directorului dumneavoastră şi să determinaţi ce sufixe şi atribute va necesita serverul dumneavoastră. Pentru mai multe informaţii, vedeţi “Directoare” la pagina 7, “Sufix (context de numire)” la pagina 14 şi “Atribute” la pagina 19.
- **Decideţi cât de mare va fi directorul dumneavoastră va fi**. Puteţi apoi estima de cât spaţiu de memorare aveţi nevoie. Mărimea directorului depinde de următoarele:
  - Numărul de atribute din schema serverului.
  - Numărul de intrări pe server.
  - Tipul de informaţii care le memoraţi pe server.

De exemplu, directorul gol care foloseşte Directory Server schema implicită necesită aproximativ 10 MB de spaţiu de memorare. Un director care foloseşte schema implicită şi care conţine 1000 de intrări de informaţii tipice angajat necesită aproximativ 30 MB de spaţiu de memorare. Acest nunmăr va varia depinzând de atributele exacte care le-aţi folosit. Se va mări de asemenea considerabil dacă aţi memorat obiecte mari, cum ar fi imagini, în director.

- **Decideţi ce măsuri de securitate veţi lua**.

  Directory Server vă permite să aplicaţi o politică de parolă pentru a asigura că utilizatorii îşi schimbă parolele periodic şi că parolele întrunesc cerinţele sintactice de parolă ale organizaţiei.

  Directory Server suportă folosirea Secure Sockets Layer (SSL) şi Certificate digitale ca şi Transport Layer Security (TLS) pentru securitatea comunicaţiilor. De asemenea este suportată şi autentificarea Kerberos.

  Directory Server vă permite să controlaţi accesul la obiectele director cu liste de control acces (ACL-uri). Puteţi de asemenea folosi auditarea securităţii i5/OS pentru a proteja directorul.

  În plus decideţi ce politică de parolă să aplicaţi.
- **Alegeţi un DN administrator şi o parolă**. DN-ul administrator implicit este cn=administrator. Acesta este singura identitate care are autorizarea să creeze sau modifice intrările director când serverul este configurat iniţial. Puteţi de asemenea folosi DN-ul administrator implicit sau să selectaţi un alt DN. De asemenea trebuie să creaţi o parolă pentru DN-ul administrator.
- **Instalare software preliminar pentru unealta de administrare Web pentru Directory Server**. Pentru a folosi unealta de administrare web pentru Directory Server, următoarele produse preliminare trebuie să fie instalate pe serverul iSeries.
  - IBM HTTP Server for iSeries (5722-DG1)
  - IBM WebSphere Application Server - Express (5722-IWE Base and Option 2)

  Vedeţi subiectul IBM HTTP Server pentru mai multe informaţii despre IBM HTTP Server for iSeries şi IBM WebSphere Application Server - Express.

Configurarea Directory Server

1. Dacă sistemul nu a fost configurat pentru publicarea informaţiilor către alt server LDAP şi nu sunt cunoscute servere LDAP de către serverul TCP/IP DNS, atunci Directory Server este instalat automat cu o configuraţie implicită limitată. Consultaţi “Configuraţie implicită pentru Directory Server” la pagina 83 pentru informaţii suplimentare. Directory Server oferă un vrăjitor care să vă asiste la configurarea Directory Server pentru nevoile dumneavoastră specifice. Puteţi rula acest vrăjitor ca parte a EZ-Setup sau să rulaţi vrăjitorul mai târziu din Navigator iSeries. Folosiţi acest vrăjitor când configuraţi iniţial serverul de directoare. Puteţi de asemenea să folosiţi vrăjitorul pentru a reconfigura serverul de directoare.

   Notă: Când folosiţi vrăitorul pentru a reconfigura serverul de directoare, porniţi configurarea de la schiţă. Configuraţia originală este ştersă ami degrabă, decât schimbată. Totuşi, datele director nu sunt şterse, ci rămân stocate în biblioteca pe care aţi selectat-o la instalare (implicit QUSRDIRDB). Jurnalul de modificări rămâne de asemenea intact, implicit în biblioteca QUSRDIRCL.

   Dacă vreţi să porniţi complet de la schiţă, ştergeţi cele două biblioteci înainte de a porni vrăjitorul.

   Dacă vreţi să modificaţi configuraţia serverului de directoare, dar să nu o ştergeţi complet, faceţi clic dreapta pe **Director** şi selectaţi **Proprietăţi**. Aceasta nu şterge configuraţia iniţială.

   Pentru a configura serverul trebuie să aveţi autorizările speciale *ALLOBJ şi *IOSYSCFG. Dacă vreţi să configuraţi auditarea securităţii OS/400, trebuie să aveţi autorizarea specială *AUDIT.
2. Pentru a porni Directory Server Vrăjitorul de configurare, urmaţi aceşti paşi:
   a. În Navigator iSeries, expandaţi **Reţea**.
   b. Expandaţi **Servere**.
   c. Apăsaţi **TCP/IP**.
   d. Faceţi clic-dreapta pe **Director** şi selectaţi **Configurare**.

   Notă: Dacă aţi configurat deja serverul de directoare, apăsaţi **Reconfigurare** mai degrabă decât **Configurare**.
3. Urmaţi instrucţiunile din vrăjitorul de configurare Directory Server pentru a configura Directory Server.

Notă: Puteţi dori de asemenea să puneţi biblioteca ce memorează datele directoarelor într-un pool de memorie auxiliar (ASP) mai degrabă decât în ASP-ul sistem. Totuşi, această bibliotecă nu poate fi memorată într-un ASP independent şi orice încercare de configurare, reconfigurare sau pornire a serverului cu o bibliotecă care există într-un ASP independent va eşua.

4. Când vrăjitorul s-a încheiat, Directory Server are o configuraţie de bază. Dacă rulaţi Lotus Domino pe sistem, atunci portul 389 (portul implicit pentru serverul LDAP) poate fi deja folosit de către funcţia LDAP Domino. Trebuie să faceţi una din următoarele:
   - Schimbaţi portul pe care îl foloseşte Lotus Domino. Vedeţi " Host Domino LDAP şi Directory Server de pe acelaşi iSeries " din subiectul E-mail pentru mai multe informaţii.
   - Schimbaţi portul pe care îl foloseşte Directory Server. Consultaţi "Schimbarea portului sau a adresei IP" la pagina 98 pentru mai multe informaţii.
   - Folosiţi adrese IP specifice. Consultaţi "Schimbarea portului sau a adresei IP" la pagina 98 pentru informaţii suplimentare.
5. Creaţi intrări corespunzătoare pentru sufixul sau sufixele pe care le-aţi configurat. Pentru informaţii suplimentare consultaţi "Adăugarea şi ştergerea sufixelor Directory Server" la pagina 100.

S-ar putea să vreţi să faceţi unele sau toate dintre următoarele înainte de a continua:
- Importaţi date către server, vedeţi "Importarea unui fişier LDIF" la pagina 99.
- Activaţi securitatea Secure Sockets Layer (SSL), vedeţi "Activarea SSL în Directory Server" la pagina 119.
- Activaţi autentificarea Kerberos, vedeţi "Activarea autentificării Kerberos pe Directory Server" la pagina 121.
- Setaţi un referal, vedeţi "Specificarea unui server pentru referalii directorului" la pagina 99.

Configuraţie implicită pentru Directory Server

Directory Server este instalat automat când instalaţi OS/400. Această instalare include o configuraţie implicită. Serverul de directoare foloseşte configuraţie impplicită când toate cele următoare sunt adevărate:
- Administratorii nu rulează Directory Server Vrăjitorul de configurare sau au modificat setăriel directoarelor cu paginile de proprietăţi.
- Publicarea Directory Server nu este configurată.
- Directory Server nu poate găsi nici o informaţie LDAP DNS.

Dacă Directory Server foloseşte configuraţia implicită, atunci se întâmplă următoarele:
- Directory Server porneşte automat când porneşte TCP/IP.
- Sistemul creează un administrator implicit, cn=Administrator. Generează de asemenea o parolă care este folosită intern. Dacă vreţi să folosiţi o parolă de administrator mai târziu, puteţi seta una nouă din Directory Server pagina de proprietăţi.
- Este creat un sufix implicit care se bazează pe numele IP al sistemului. Un sufix de obiecte ssitem este de asemenea creat bazat pe numele sistemului. De exemplu, dacă numele IP al sistemului dvs. este mary.acme.com, sufixul este dc=mary,dc=acme,dc=com.
- Directory Server foloseşte biblioteca de date implicită QUSRDIRDB. Sistemul o creează în ASP-ul sistem.
- Serverul foloseşte portul 389 pentru comunicaţii nesigure. Dacă un certificat digital a fost configurat pentru LDAP, SSL este activat şi portul 636 este folosit pentru comunicaţii sigure.

Administrarea Web

Unul sau mai multe servere de directoare pot fi administrate prin intermediul consolei de administrare Web. Consola de administrare Web vă permite să:
- Adăugaţi sau modificaţi lista de servere de directoare care pot fi administrate.
- Administraţi un Directory Server folosind unealta de administrare Web.
- Schimbaţi atributele consolei de administrare Web.

Pentru a folosi consola de administrare Web, faceţi următoarele:

1. Dacă aceasta este prima dată când folosiţi administrarea Web pentru Directory Server, trebuie să setaţi întâi administrarea Web (vedeţi “Setarea administrării web pentru prima dată”) şi apoi continuaţi cu pasul următor.
2. Înregistraţi-vă la administrarea Web pentru Directory Server făcând unul din următoarele lucruri:
   - Din Navigator iSeries, selectaţi serverul şi apăsaţi **Reţea > Servere > TCP/IP**, faceţi clic-dreapta pe **Director** şi apăsaţi **Administrare server**.
   - Din pagina Task-uri iSeries (http://*serverul_dvs* :2001) apăsaţi **IBM Directory Server**.
3. Dacă doriţi să administraţi un Directory Server, faceţi următoarele:
   a. Selectaţi Directory Server pe care vreţi să îl administraţi în câmpul **Nume gazdă LDAP** .
   b. Introduceţi DN-ul de înregistrare administrator pe care îl folosiţi să vă legaţi la serverul de directoare.
   c. Introduceţi parola de administrator.
   d. Apăsaţi **Înregistrare**. Este afişată pagina IBM Directory Server Web Administration Tool. Pentru mai multe informaţii despre pagina IBM Directory Server Web Administration Tool, vedeţi “Unealta de administrare web” la pagina 86.
4. Dacă vreţi să adăugaţi sau să modificaţi lista de servere de directoare care pot fi administrate sau să modificaţi atributele consolei de administrare web, faceţi următoarele:
   a. Selectaţi **Console Admin** în câmpul **Nume gazdă LDAP**.
   b. Introduceţi login-ul de administrator consolă.
   c. Introduceţi parola de administrator consolă.
   d. Apăsaţi **Înregistrare**. Este afişată pagina IBM Directory Server Web Administration Tool. Pentru mai multe informaţii despre pagina IBM Directory Server Web Administration Tool, vedeţi “Unealta de administrare web” la pagina 86.
   e. Apăsaţi **Administrare consolă** şi apoi selectaţi una din următoarele:
      - **Schimbare login administrator consolă** pentru a schimba numele login-ului de administrator consolă.
      - **Schimbare parolă administrator consolă** pentru a schimba parola administratorului de consolă.
      - **Gestionare servere consolă** pentru a schimba ce server de directoare pot fi administrate de către consola de administrare web.
      - **Gestionare proprietăţi consolă** pentru a schimba proprietăţile consolei de administrare web.

Setarea administrării web pentru prima dată

Faceţi următoarele pentru a seta Directory Server Web Administration Tool pentru prima dată.

1. Instalaţi IBM WebSphere Application Server - Express (5722-IWE Base and Option 2) şi software-ul preliminar asociat dacă nu sunt deja instalate. Vedeţi subiectul IBM HTTP Server pentru mai multe informaţii.
2. Activaţi instanţa server a aplicaţiei sistem în serverul HTTP ADMIN.
   a. Porniţi instanţa de server HTTP ADMIN, făcând una din următoarele:
      - În Navigator iSeries, apăsaţi **Reţea -> Servere -> TCP/IP** şi faceţi clic dreapta pe **Administrare HTTP**. Apoi faceţi clic pe **Pornire**.
      - Pe o linie de comandă i5/OS tastaţi STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).
   b. Înregistraţi-vă la IBM Web Administration for iSeries. Folosiţi un profil de utilizator i5/OS şi parola pentru logarea în pagina Task-uri iSeries (http://*serverul_dv*:2001), apoi faceţi clic pe **IBM Web Administration pentru iSeries**.
   c. Din pagina *serverului_dumneavoastră* Administrare server HTTP, faceţi clic pe fişa **Gestionare** şi apoi faceţi clic pe fişa **Servere HTTP**. Asiguraţi-vă că este selectat în lista derulantă Servere, **ADMIN – Apache**. Din opţiunile din panoul din stânga paginii, faceţi clic pe **Configuraţii generale server**.

      Notă: S-ar putea să fie nevoie să expandaţi secţiunea **Proprietăţi server** pentru a vedea opţiunea **Configuraţii generale server**.
   d. Setaţi **Pornire instanţă de server de aplicaţii sistem la pornirea serverului ’Admin’** la **Da**.
   e. Selectaţi **OK**.

3. Setaţi WebSphere Application Server să folosească SYSINST.
   a. Faceţi clic pe **WebSphere Application Server** din opţiunile panoului din stânga.
   b. Selectaţi **WebSphere Application Server – Express 5.0**.
   c. Din lista derulantă cu **instanţe WebSphere**, selectaţi **SYSINST**.

      Notă: Dacă nu există SYSINST în lista derulantă, reporniţi serverul ADMIN.
   d. Din lista derulantă **Pornire toate serverele de aplicaţii WebSphere ...**, selectaţi **Da** .
   e. Din lista derulantă **Oprire toate serverele de aplicaţii WebSphere...**, selectaţi **Da**.
   f. Selectaţi **OK**.
4. Reporniţi instanţa de server HTTP ADMIN, făcând clic pe butonul de repornire (al doilea buton de sub fişa **Servere HTTP**). Puteţi opri şi porni instanţa de server HTTP ADMIN folosind Navigator iSeries sau o linie de comandă i5/OS.

   Puteţi opri instanţa serverului HTTP ADMIN, făcând una din următoarele:
   - În Navigator iSeries apăsaţi **Reţea -> Servere -> TCP/IP** şi faceţi clic-dreapta pe **Administrare HTTP**. Apoi faceţi clic pe **Oprire**.
   - Pe o linie de comandă i5/OS tastaţi ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN) .

   Puteţi porni instanţa serverului HTTP ADMIN, făcând una din următoarele:
   - În Navigator iSeries apăsaţi **Reţea -> Servere -> TCP/IP** şi faceţi clic-dreapta pe **Administrare HTTP**. Apoi faceţi clic pe **Pornire**.
   - În linia de comandă i5/OS tastaţi STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN) .

   Vedeţi subiectul IBM HTTP Server pentru mai multe informaţii.
5. Logaţi-vă la Directory Server Web Administration Tool.
   a. Aduceţi la vedere **pagina Logare**, făcând una din următoarele:
      - Din Navigator iSeries, selectaţi serverul dumneavoastră şi apăsaţi **Reţea > Servere > TCP/IP**, faceţi clic dreapta pe **IBM Directory Server** şi faceţi clic pe **Administrare server**.
      - Din pagina Task-uri iSeries (http://*serverul_dv*:2001) faceţi clic pe **IBM Directory Server pentru iSeries**.
   b. Selectaţi **Console Admin** în câmpul **Nume gazdă LDAP**.
   c. Introduceţi superadmin în câmpul **Nume utilizator**.
   d. Tastaţi secret în câmpul **Parolă** .
   e. Apăsaţi **Înregistrare**. Este afişată pagina IBM Directory Server Web Administration Tool.
6. Schimbaţi login administrator consolă.
   a. Faceţi clic pe **Administrare consolă** în panoul din stânga pentru a extinde secţiunea, apoi faceţi clic pe **Modificare consolă pentru logare administrator**.
   b. Tastaţi un nou nume de login administrare parolă în câmpul **Login administrator consolă**.
   c. Tastaţi parola curentă (secret) în câmpul **Parola curent**.
   d. Selectaţi **OK**.
7. Schimbaţi parola de administrare consolă. Faceţi clic pe **Modificare parolă administrator consolă** din panoul din stânga.
8. Adăugaţi Directory Server pe care vreţi să îl administraţi. Faceţi clic pe **Gestionare servere consolă** din panoul din stânga.

   Notă: Când adăugaţi un Directory Server i5/OS, **Portul de administrare** nu este folosit şi va fi ignorat.
9. Dacă doriţi să modificaţi proprietăţile consolei. Faceţi clic pe **Gestionare proprietăţi consolă** din panoul din stânga.
10. Apăsaţi **Logout**. Când apare ecranul de succes al delogării, apăsaţi legătura **aici** pentru a reveni la pagina de logare administrare web.

După ce aţi configurat consola pentru prima dată, puteţi reveni la consolă în orice moment pentru a realiza:

- Schimbare login şi parola administratorului de consolă.
- Schimbare serverului de directoare care poate fi administrat de unealta de administrare web.
- Schimbare proprietăţi consolă.

Unealta de administrare web

O dată ce v-aţi înregistrat pe unealta de administrare web, veţi găsi o fereastră aplicaţie care conţine cinci părţi:

Zona de banner
Zona de banner se află în partea de sus a panoului şi conţine numele aplicaţiei şi logo-ul IBM.

Zona de navigare
Zona de navigare, aflată în stânga panoului, afişează categoriile expandabile pentru diverse task-uri conţinut de servere cum sunt:

Proprietăţi utilizator
Acest task că permite să schimbaţi parola utilizatorului curent.

Management schemă
Acest task vă permite să lucraţi cu clase obiect, atribute, reguli de potrivire şi sintaxe.

Management director
Acest task că permite să lucraţi cu intrările director.

Management replicare
Acest task vă permite să lucraţi cu acreditări, topologie, planificări şi cozi.

Regiuni şi şabloane
Acest task vă permite să lucraţi cu şabloane utilizator şi regiuni.

Utilizatori şi grupuri
Acest task vă permite să lucraţi cu utilizatori şi grupuri din regiunile definite. De exemplu, dacă doriţi să creaţi un nou utilizator Web, task-ul **Utilizatori şi grupuri** funcţionează cu un singur grup objectclass, groupOfNames. Puteţi ajusta suportul de grup.

Zona de lucru
Zona de lucru afişează task-urile asociate cu task-ul selectat din zona de navigaţie. De exemplu, dacă este selectată Gestionarea securităţii serverului în zona de navigare, zona de lucru afişează pagina Securitate server şi fişele care conţin task-urile înrudite cu setarea securităţii serverului.

Zona stare server
Zona de stare server, se află în partea de sus a zonei de lucru. Pictograma din partea stângă a zonei de stare server indică starea curentă a serverului. Lângă pictogramă este numele serverului care este administrat. Pictograma din partea dreaptă a zonei de stare server furnizează un link la ajutorul online.

Zona de stare task
Zona task, se află sub zona de lucru şi afişează starea task-ului curent.

Capitolul 6. Scenariu: MyCo, Inc. setează un Directory Server

Situaţie

Ca administrator al sistemelor de calculatoare ale companiei dvs., v-ar plăcea să plasaţi informaţiile despre angajaţi cum sunt numerele de telefon şi adresele de e-mail pentru organizaţia dvs. într-o magazie LDAP centrală.

Obiective

În acest scenariu, MyCo, Inc. doreşte să configureze un Directory Server şi să creeze o bază de date director care conţine informaţii despre angajaţi cum sunt numele, adresa e-mail şi numărul de telefon.

Obiectivele acestui scenariu sunt după cum urmează:

- Pentru a face informaţiile despre angajaţi disponibile oriunde în reţeaua companiei folosind un client de poştă Lotus Notes sau Microsoft Outlook Express.
- Pentru a permite managerilor să schimbe datele angajaţilor în baza de date director, în timp ce nu permiteţi celorlalţi să schimbe datele despre angajaţi.
- Pentru a permite serverului iSeries să poată publica date despre angajaţi în baza de date director.

Detalii

Directory Server va rula pe serverul iSeries numit myiSeries.

Următorul exemplu ilustrează informaţiile pe care MyCo, Inc. doreşte să le includă în baza sa de date director pentru fiecare angajat.

```
Name: Jose Alvirez
Department: DEPTA
Telephone number: 999 999 9999
Email address: jalvirez@my_co.com
```

Structura de directoare pentru acest scenariu poate fi vizualizată ca ceva similar cu următoarele:

```
/
|
+- my_co.com
   |
   +- employees
      |
      +- Jose Alvirez
      |  DEPTA
      |  999-555-1234
      |  jalvirez@my_co.com
      |
      +- John Smith
      |  DEPTA
      |  999-555-1235
      |  jsmith@my_co.com
      |
      +  Managers group
         Jose Alvirez
         myiSeries.my_co.com
.
.
.
```

Toţi angajaţii (manageri şi non-manageri) există în arborele director cu angajaţi. Managerii aparţin de asemenea şi grupului manageri. Membrii grupului manageri au autorizare să schimbe datele despre angajaţi.

Serverul iSeries (myiSeries) are nevoie de asemenea să aibă autorizare să modifice datele angajaţilor. În acest scenariu, serverul iSeries este plasat în arborele director angajaţi şi este făcut membru al grupului manageri.

Dacă doriţi să ţineţi intrările despre anagajaţi separat de intrarea server iSeries, puteţi crea alt arbore director (de exemplu: computere) şi adăugaţi serverul iSeries acolo. Serverul iSeries va trebui să aibă aceeaşi autorizarea ca managerii.

Cerinţe preliminare şi supoziţii

Unealta de administrare Web este configurată şi rulează corespunzător. Consultaţi “Administrarea Web” la pagina 83 pentru informaţii suplimentare.

Paşi de setare

Completaţi următoarele task-uri:
1. “Detalii scenariu: Setarea Directory Server”.
2. “Detalii scenariu: Crearea bazei de date director” la pagina 89.
3. “Detalii scenariu: Publicarea datelor iSeries în baza de date director” la pagina 91.
4. “Detalii scenariu: Introducerea informaţiilor în baza de date director” la pagina 92.
5. “Detalii scenariu: Testarea bazei de date director” la pagina 93.

Detalii scenariu: Setarea Directory Server

Pas 1: Configurare Directory Server

Notă: Pentru a configura serverul trebuie să aveţi autorizările speciale *ALLOBJ şi *IOSYSCFG.

1. În Navigator iSeries apăsaţi **Reţea —> Servere —> TCP/IP**.
2. Apăsaţi **Configurare sistem ca Directory Server** în fereastra **Task-uri de configurare server** în partea din dreapta jos a Navigatorului iSeries.
3. Va apărea **Vrăjitorul de configurare Directory Server**.
4. Apăsaţi **Configurare server de directoare LDAP local** în fereastra **Vrăjitor de configurare IBM Directory Server - Bun venit**.
5. Apăsaţi **Următor** în fereastra **Vrăjitor de configurare IBM Directory Server - Bun venit**.
6. Selectaţi **Nu** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare setări**. Aceasta vă permite să configuraţi serverul LDAP fără setările implicite.
7. Apăsaţi **Următor** în fereastra **Vrăjitor configurare IBM Directory Server - Specificare setări**.
8. Deselectaţi **Generat de sistem** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare administrator** şi introduceţi următoarele:

DN Administrator	cn=administrator
Parolă	secret
Confirmare parolă	secret

Notă: Oricare şi toate parolele specificate în acest scenariu sunt doar pentru exemplificare. Pentru a împiedica o compromitere a securităţii sistemului sau reţelei dvs., nu ar trebui să folosiţi niciodată aceste parole ca parte a propriilor dvs. configuraţii.

9. Apăsaţi **Următor** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare DN administrator**.
10. Tastaţi dc=my_co,dc=com în câmpul **Sufix** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare sufixe**.
11. Apăsaţi **Adăugare** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare sufixe**.
12. Apăsaţi **Următor** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare sufixe**.

13. Selectaţi **Da, foloseşte toate adresele IP** în fereastra **Vrăjitor de configurare IBM Directory Server - Selectare adrese IP**.
14. Apăsaţi **Următor** în fereastra **Vrăjitor de configurare IBM Directory Server - Selectare adrese IP**.
15. Selectaţi **Da** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare preferinţă TCP/IP**.
16. Apăsaţi **Următor** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare preferinţă TCP/IP**.
17. Apăsaţi **Sfârşit** în fereastra **Vrăjitor de configurare IBM Directory Server - Rezumat**.
18. Faceţi clic dreapta pe **IBM Directory Server** şi apăsaţi **Pornire**.

Pas 2: Configurare unealtă de administrare web Directory Server

1. Îndreptaţi-vă browserul la http://*myiSeries.my_co.com*:9080/IDSWebApp/IDSjsp/Login.jsp, unde *myiSeries.my_co.com* este serverul dvs. iSeries .
2. Ar trebui să apară o pagină de login. Apăsaţi pe lista **Nume gazdă LDAP** şi selectaţi **Admin consolă**. Tastaţi superadmin pentru numele de utilizator şi secret pentru parolă. Apăsaţi **Logon**.
3. Configuraţi unealta de administrare web să se conecteze la serverul LDAP de pe iSeries-ul dvs. Selectaţi **Administrare consolă—> Gestionare servere consolă** în navigarea din stânga.
4. Selectaţi **Adăugare**.
5. În câmpul **Adăugare server**, tastaţi myiSeries.my_co.com.
6. Clic **Ok**. Noul server va apărea în lista de sub **Gestionare servere consolă**.
7. Apăsaţi **delogare** în cadrul de navigare din stânga.
8. În pagina de logare din unealta de administrare Web apăsaţi pe lista **Nume gazdă LDAP** şi selectaţi serverul pe care tocmai l-aţi configurat (**myiSeries.my_co.com**).
9. În câmpul **Nume utilizator** tastaţi cn=administrator şi în câmpul **Parolă** tastaţi secret. Apăsaţi **Înregistrare**. Ar trebui să vedeţi pagina principală a uneltei de administrare web a serverului IBM Directory Server.

Detalii scenariu: Crearea bazei de date director

Înainte de a putea începe să introduceţi date, trebuie să creaţi un loc pentru ca datele să fie stocate.

Pas 1: Creaţi un obiect DN de bază

1. Apăsaţi **Management director—> Gestionare intrări**. Vedeţi o listă de obiecte în nivelul de bază al directorului. Deoarece serverul este nou, vedeţi doar obiectele structurale care conţin informaţiile de configurare.
2. Doriţi să adăugaţi un nou obiect să conţină datele MyCo, Inc. Întâi apăsaţi **Adăugare...** în partea dreaptă a ferestrei. În fereastra următoare, căutaţi în lista de **Clase obiect** pentru a selecta **domeniul** şi apăsaţi **Următor**.
3. Nu doriţi să adăugaţi nici o clasă obiect auxiliară, aşa că apăsaţi din nou **Următor**.
4. În fereastra **Introduceţi atributele**, introduceţi datele care corespund cu sufixul pe care l-aţi creat mai devreme în vrăjitor. Lăsaţi lista derulantă **Clasă obiect** pe **domeniu**. Tastaţi dc=my_co în câmpul **DN relativ**. Tastaţi dc=com în câmpul **DN părinte**. Tastaţi Type my_co în câmpul **dc**.
5. Apăsaţi **Sfârşit** în josul ferestrei. Înapoi în nivelul de bază ar trebui să vedeţi noul DN de bază.

Pas 2: Creare şablon utilizator

Veţi crea un şablon utilizator ca un ajutor la adăugarea datelor despre angajaţi ai MyCo, Inc.

1. Apăsaţi **Regiuni şi şabloane—> Adăugare şablon utilizator**.
2. În câmpul **Nume şablon utilizator**, tastaţiAngajat.
3. Apăsaţi pe butonul **Răsfoire...** de lângă câmpul **DN părinte**. Apăsaţi pe DN-ul de bază pe care l-aţi creat în secţiunea anterioară, **dc=my_co,dc=com** şi apăsaţi **Selectare** în dreapta ferestrei.
4. Apăsaţi **Următor**
5. În lista derulantă **Clasă obiect structural**
6. alegeţi **inetOrgPerson** şi apăsaţi **Următor**.

7. În lista derulantă **Atribut de numire**, selectaţi **cn**.
8. În lista **Fişe**, selectaţi **Necesar** şi apăsaţi **Editare**.
9. Fereastra **Editare fişă** este unde alegeţi care câmpuri să fie incluse în şablonul utilizator. **sn** şi **cn** sunt necesare.
10. În lista **Atribute**, selectaţi **departmentNumber** şi apăsaţi **Adăugare >>>**.
11. Selectaţi **telephoneNumber** şi apăsaţi **Adăugare >>>**.
12. Selectaţi **mail** şi apăsaţi **Adăugare >>>**.
13. Selectaţi **userPassword** şi apăsaţi **Adăugare >>>**.
14. Apăsaţi **OK** şi apoi **Sfârşit** pentru a crea şablonul utilizator.

Pas 3: Creare regiune

1. În unealta de administrare Web, apăsaţi **Regiuni şi şabloane —> Adăugare regiune**.
2. În câmpul **Nume regiune**, tastaţi angajaţi.
3. Apăsaţi **Răsfoire...** în dreapta câmpului **DN părinte**.
4. Selectaţi DN-ul părinte pe care l-aţi creat, **dc=my_co,dc=com** şi apăsaţi **Selectare** în partea dreaptă a ferestrei.
5. Apăsaţi **Continuare**.
6. În următoarea fereastră trebuie doar să schimbaţi lista derulantă **Şablon utilizator**. Selectaţi şablonul utilizator pe care l-aţi creat, **cn=employees,dc=my_co,dc=com**.
7. Clic **Sfârşit**.

Pas 4: Creare grup manager

1. Creare grup manager.
   a. Apăsaţi **Utilizatori şi grupuri—> Adăugare grup**.
   b. În câmpul **Nume grup**, tastaţi manageri.
   c. Asiguraţi-vă că **angajaţi** este selectat în lista derulantă **Regiune**.
   d. Clic **Sfârşit**.
2. Configurare administrator grup manager pentru regiunea **angajaţi**.
   a. Apăsaţi **Regiuni şi şabloane—> Gestionare regiuni**.
   b. Selectaţi regiunea pe care aţi creat-o, **cn=employees,dc=my_co,dc=com** şi apăsaţi **Editare**.
   c. În dreapta câmpului **Grup administrator**, apăsaţi **Răsfoire...**.
   d. Selectaţi **dc=my_co,dc=com** şi apăsaţi **Expandare**.
   e. Selectaţi **cn=employees** şi apăsaţi **Expandare**.
   f. Selectaţi **cn=managers** şi apăsaţi **Selectare**.
   g. În fereastra **Editare regiune**, apăsaţi **OK**.
3. Daţi-i grupului de manageri autorizare pentru sufixul **dc=my_co,dc=com**.
   a. Apăsaţi **Management director—> Gestionare intrări**.
   b. Selectaţi **dc=my_co,dc=com** şi apăsaţi **Editare ACL...**.
   c. În fereastra **Editare ACL**, apăsaţi pe fişa **Proprietari**.
   d. Selectaţi căsuţa de bifare **Propagare proprietar**. Oricine este membru al grupului de manageri va fi făcut proprietar al arborelui de date **dc=my_co,dc=com**.
   e. În lista derulantă **Tip**, selectaţi **Grup**.
   f. În câmpul **DN (Distinguished name)**, tastaţi cn=managers,cn=employees,dc=my_co,dc=com.
   g. Selectaţi **Adăugare**.
   h. Apăsaţi **Ok**.

Pasul:5 Adăugaţi un utilizator ca manager

1. În unealta de Administrare Web, apăsaţi **Utilizatori şi grupuri —> Adăugare utilizator**.

2. Selectaţi regiunea pe care aţi creat-o, **employees**, în meniul derulant **Regiune** şi apăsaţi **Continuare**.
3. În câmpul **cn**, tastaţi Jose Alvirez.
4. În câmpul ***sn** (surname - prenume) tastaţi Alvirez.
5. În câmpul ***cn** (complete name - nume complet), tastaţi Jose Alvirez. cn este folosit pentru a crea DN-ul intrării. *cn este un atribut al obiectului.
6. În câmpul **telephoneNumber** tastaţi 999 555 1234.
7. În câmpul **departmentNumber** tastaţi DEPTA.
8. În câmpul **mail** tastaţi jalvirez@my_co.com.
9. În câmpul **userPassword** tastaţi secret.
10. Apăsaţi fişa **Grupuri utilizator**.
11. În lista **Gruprui disponibile**, selectaţi **manageri** şi apăsaţi **Adăugare—>**.
12. La baza ferestrei apăsaţi **Sfârşit**.
13. Log out din unealta de administrare web apăsând pe **Log out** în partea stângă de navigare.

Detalii scenariu: Publicarea datelor iSeries în baza de date director

Configuraţi publicarea pentru a permite serverului dvs. iSeries să introducă în mod automat informaţiile utilizator în directorul LDAP. Informaţiile utilizator din directorul de distribuţie sistem sunt publicate în directorul LDAP.

Notă: Utilizatorii creaţi cu Navigator iSeries primesc atât un profil de utilizator cât şi o intrare utilizator director de distribuţie sistem. Dacă folosiţi comenzi CL pentru a crea utilizatori, trebuie să creaţi atât un profil de utilizator (**CRTUSRPRF**) cât şi o intrare utilizator director de distribuţie sistem (**WRKDIRE**). Dacă utilizatorii dvs. există doar ca profile de utilizator şi vreţi ca ei să fie publicaţi în directorul LDAP, trebuie să creaţi intrări utilizator director distribuţie sistem pentru ei.

Pasul:1 Creaţi serverul iSeries ca utilizator Directory Server

1. Logaţi-vă în unealta de Administrare Web (http://**myiSeries.my_co.com**:9080/IDSWebApp/IDSjsp/Login.jsp) ca administrator.
   a. Selectaţi **myiSeries.my_co.com** din lista **Nume gazdă LDAP**.
   b. Tastaţi cn=administrator în câmpul **Username**
   c. Tastaţi secret în câmpul **Parolă**.
   d. Apăsaţi **Înregistrare**.
2. Selectaţi **Utilizatori şi grupuri —> Adăugare utilizator**.
3. Selectaţi **employees** din lista **Regiune**.
4. Apăsaţi **Continuare**.
5. Tastaţi myiSeries.my_co.com în câmpul **cn**.
6. Tastaţi myiSeries.my_co.com în câmpul ***sn**.
7. Tastaţi myiSeries.my_co.com în câmpul ***cn**.
8. Tastaţi secret în câmpul **Parolă utilizator**.
9. Apăsaţi fişa **Grupuri utilizator**.
10. Selectaţi grupul **manageri**.
11. Apăsaţi **Adăugare —>**.
12. Clic **Sfârşit**.

Pasul:2 Configuraţi serverul iSeries ca să publice date

1. În Navigator iSeries, faceţi clic-dreapta pe iSeries-ul dvs. în fereastra de navigare din partea stângă şi selectaţi **Proprietăţi**.
2. În fereastra de dialog **Proprietăţi**, alegeţi fişa **Directory Server**.

3. Selectaţi **Utilizatori** şi apăsaţi **Detalii**.
4. Selectaţi căsuţa de bifare **Publicare informaţii utilizator**.
5. În secţiunea **Unde să se publice**, apăsaţi butonul **Editare**. Apare o fereastră.
6. Tastaţi myiSeries.my_co.com.
7. În câmpul **Sub DN**, tastaţi cn=employees,dc=my_co,dc=com.
8. În secţiunea **Conexiune server**, asiguraţi-vă că este introdus numărul de port implicit, **389**, în câmpul **Port**. În lista derulantă **Metoda de autentificare**, alegeţi **Nume distinctiv** şi introduceţi cn=myiSeries,cn=employees,dc=my_co,dc=com în câmpul **Nume distinctiv**.
9. Apăsaţi **Parola**.
10. Tastaţi secret în câmpul **Parolă** .
11. Tastaţi secret în câmpul **Confirmare parolă** .
12. Selectaţi **OK**.
13. Apăsaţi pe butonul **Verificare**. Aceasta asigură că aţi introdus toate informaţiile corect şi că serverul iSeries se poate conecta la directorul LDAP.
14. Selectaţi **OK**.
15. Selectaţi **OK**.

Detalii scenariu: Introducerea informaţiilor în baza de date director

Ca manager, Jose Alvirez adaugă acum şi actualizează datele pentru indivizii din departmentul lui. El trebuie să adauge unele informaţii adiţionale despre Jane Doe. Jane Doe este un utilizator de pe serverul iSeries şi informaţiile ei au fost publicate. Jose Alvirez trebuie de asemenea să adauge informaţii despre John Smith. John Smith nu este un utilizator de pe serverul iSeries. Jose Alvirez face următoarele:

Pasul 1: Se înregistrează la unealta de Administrare Web

Se înregistrează în unealta de Administrare Web. (http://**myiSeries.my_co.com**:9080/IDSWebApp/IDSjsp/Login.) făcând următoarele:

1. Selectează **myiSeries.my_co.com**, din lista **Nume gazdă LDAP**.
2. Tastează cn=Jose Alvirez,cn=myco employees,dc=my_co,dc=com în câmpul Username.
3. Tastează secret în câmpul parolă.
4. Apăsaţi **Logon**.

Pasul 2: Modifică datele despre angajat

1. Apasă **Utilizatori şi grupuri —> Gestiune utilizatori**.
2. Selectează **employees** din lista **Regiune** şi apasă **Vizualizare utilizatori**.
3. Selectează **Jane Doe** din lista de utilizatori şi apasă **Editare**.
4. Tastează DEPTA în câmpul **departmentNumber** .
5. Selectaţi **OK**.
6. Apăsaţi **Închidere**.

Pasul 3: Adăugare date despre angajat

1. Apăsaţi **Utilizatori şi grupuri—> Adăugare utilizator**.
2. Selectaţi **employees** din meniul derulant **Regiune** şi apăsaţi **Continuare**.
3. În câmpul **cn**, tastaţi John Smith.
4. În câmpul ***sn** tastaţi Smith.
5. În câmpul ***cn**, tastaţi John Smith.
6. În câmpul **telephoneNumber** tastaţi 999 555 1235.
7. În câmpul **departmentNumber** tastaţi DEPTA.

8. În câmpul **mail** tastaţi jsmith@my_co.com.
9. Apăsaţi **Sfârşit** în partea de jos a ferestrei.

Detalii scenariu: Testarea bazei de date director

După ce aţi introdus datele despre angajat în baza de date director, testaţi baza de date director şi Directory Server făcând una din următoarele:

Căutaţi în baza de date director folosind cartea dvs. de adrese e-mail

Informaţiile dintr-un director LDAP pot fi căutate cu uşurinţă cu programe cu posibilităţi LDAP. Mulţi clienţi de e-mail pot căuta în servere directoare LDAP ca parte a funcţiei lor de carte de adrese. Următoarele sunt exemple de proceduri de configurare a Lotus Notes 6 şi Microsoft Outlook Express 6. Procedura pentru mulţi alţi clienţi de e-mail va fi similară.

Lotus Notes

1. Deschideţi cartea dvs. de adrese.
2. Apăsaţi **Acţiuni —> Nou —> Cont**.
3. Tastaţi myiSeries în câmpul **Nume cont**.
4. Tastaţi myiSeries.my_co.com în câmpul **Nume server cont**.
5. Selectaţi **LDAP** în câmpul **Protocol**.
6. Apăsaţi pe fişa **Configuraţie Protocol**.
7. Tastaţi dc=my_co,dc=com în câmpul **Bază de căutare**.
8. Apăsaţi **Salvează şi închide**.
9. Apăsaţi **Creare —> Mail —> Memo**.
10. Apăsaţi **Adresă...**.
11. Selectaţi myiSeries în câmpul **Alegere carte de adrese**.
12. Tastaţi Alvirez în câmpul **Caută pentru** .
13. Apăsaţi **Căutare**. Apar datele pentru Jose Alvirez

Microsoft Outlook Express

1. Apăsaţi **Unelte —> Conturi**.
2. Apăsaţi **Adăugare —> Directory Service**.
3. Tastaţi adresa Web a serverului iSeries în câmpul **Internet Directory (LDAP) server** (myiSeries.my_co.com).
4. Deselectaţi căsuţa de bifare **Serverul meu LDAP îmi cere să mă înregistrez**
5. Apăsaţi **Continuare**.
6. Apăsaţi **Continuare**.
7. Clic **Sfârşit**.
8. Selectaţi myiSeries.my_co.com (serviciul director pe care tocmai l-aţi configurat) şi apăsaţi **Proprietăţi**.
9. Apăsaţi **Avansat**.
10. Tastaţi dc=my_co,dc=com în câmpul **Search base**.
11. Clic **Ok**.
12. Apăsaţi **Închidere**.
13. Tastaţi Ctrl+E pentru a deschide fereastra **Căutare persoană**.
14. Selectaţi myiSeries.my_co.com din lista **Căutare în**.
15. Tastaţi Alvirez în câmpul **Nume**.
16. Clic **Găsire acum**. Apar datele pentru Jose Alvirez.

Căutarea în baza de date director folosind comanda din linia de comandă ldapsearch

1. În interfaţa bazată pe caractere introduceţi comanda CL **QSH** pentru a deschide o sesiune Qshell.
2. Introduceţi următoarele pentru a obţine o listă a tuturor intrărilor LDAP din baza de date.

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

   Unde:

   –h este numele maşinii gazdă care rulează serverul LDAP.

   –b este DN-ul de bază sub care se caută.

   objectclass=*
   întoarce toate intrările din director.

   Această comandă întoarce ceva de forma următoare:

   ```
   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

   .
   .
   .
   ```

   Prima linie a fiecărei intrări este denumită numele distinctiv (distinguished name - DN). DN-urile sunt precum numele de fişier complet al fiecărei intrări. Unele din intrări nu conţin date şi sunt doar structurale. Acelea cu linia **objectclass=inetOrgPerson** corespund cu intrările pe care le-aţi creat pentru oameni. Jose Alvirez’s DN is **cn=Jose Alvirez,cn=MyCo Employees,dc=my_co,dc=com**.

Capitolul 7. Administrarea Directory Server

Pentru a administra Directory Server, trebuie să aveţi următoarele seturi de autorizări:

- Pentru a configura serverul sau pentru a modifica configuraţia serverului: autorizările speciale All Object (*ALLOBJ) şi I/O System Configuration (*IOSYSCFG)
- Pentru a porni sau opri serverul: autorizarea Job Control (*JOBCTL) şi autorizarea pentru obiect la comenzile End TCP/IP (ENDTCP), Start TCP/IP (STRTCP), Start TCP/IP Server (STRTCPSVR) şi End TCP/IP Server (ENDTCPSVR)
- Pentru a seta comportamentul de auditare pentru serverul de directoare: autorizarea specială Audit (*AUDIT)
- Pentru a vedea istoricul de joburi al serverului: autorizarea specială Spool Control (*SPLCTL)

Pentru a gestiona obiectele directoarelor (inclusiv listele de control, proprietatea obiectelor şi replicarea), conectaţi-vă la director fie cu DN de administrator DN fie cu un alt DN care are autorizarea corespunzătoare LDAP. Dacă integrarea autorizării este folosită, un administrator poate fi de asemenea un utilizator proiectat (vedeţi “Backend proiectat pe sistemul de operare” la pagina 65) care are autorizarea pentru ID-ul funcţiei Directory Server Administrator, vedeţi “Lucrul cu accesul administrativ pentru utilizatori autorizaţi” la pagina 101).

Task-uri de administrare generale

Task-uri de conţinut director

- “Gestionarea listelor de control al accesului (ACL-uri)” la pagina 147

Task-uri de publicare

- “Publicarea informaţiilor pe serverul de directoare” la pagina 151

Pornirea Directory Server

Pentru a porni Directory Server, faceţi paşii următori:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Pornire**.

   Serverul de directoare poate avea nevoie de mai multe minute pentru a porni depinde de viteza serverului dumneavoastră şi de cantitatea de memorie disponibilă. Prima dată când porniţi serverul de directoare poate lua cu câteva minute mai mult decât de obicei deoarece serverul trebuie să creeze noi fişiere. Similar, când porniţi serverul de directoare pentru prima dată după ce modernizaţi de la o ediţie anterioară a Directory Server, poate dura câteva minute mai mult decât de obicei deoarece trebuie să migreze fişierele. Puteţi verifica starea serverului periodic (vedeţi “Verificarea stării serverului de directoare” la pagina 97) pentru a vedea dacă a pornit deja.

Serverul de directoare poate de asemenea să fie pornit din interfaţa bazată pe caractere prin introducerea comenzii STRTCPSVR *DIRSRV. În plus, dacă aveţi serverul de directoare configurat să pornească când TCP/IP porneşte, puteţi de asemenea să-l porniţi prin introducerea comenzii STRTCP.

Modul doar configurare

Serverul de directoare poate fi pornit în modul doar configurare din interfaţa caracter prin introducerea comenzii TRCTCPAPP APP(*DIRSRV) ARGLIST(SAFEMODE).

Modul doar configurare porneşte serverul doar cu sufixul cn=configuration activ şi nu depinde de iniţializarea cu succes a backend-urilor bazei de date.

Oprirea Directory Server

Oprirea serverului de directoare afectează toate aplicaţiile ce folosesc serverul când acesta este oprit. Aceasta include aplicaţiile Enterprise Identity Mapping (EIM) care folosesc curent serverul de directoare pentru operaţii EIM. Toate aplicaţiile sunt deconectate de la serverul de directoare, totuşi, nu sunt prevenite de la încercarea de a se reconecta la server.

Pentru a opri Directory Server, faceţi paşii următori:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Oprire**.

   Serverul de directoare poate avea nevoie de mai multe minute pentru a se opri depinde de viteza serverului dumneavoastră, de cantitatea de activitate a serverului şi de cantitatea de memorie disponibilă. Puteţi verifica starea serverului periodic (vedeţi “Verificarea stării serverului de directoare” la pagina 97) pentru a vedea dacă a pornit deja.

Notă: Serverul de directoare poate fi de asemenea oprit de la o sesiune 5250 prin introducerea comenilor ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL sau ENDTCP. ENDTCPSVR *ALL şi ENDTCP afectează de asemena orice alte servere TCP/IP care rulează pe sistemul dumneavoastră. ENDTCP va opri de asemenea TCP/IP.

Verificarea stării serverului de directoare

Navigator iSeries afişează starea serverului de directoare în coloana **Stare** din cadrul din dreapta.

Pentru a verifica starea serverului de directoare, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**. Navigator iSeries afişează starea tuturor serverelor TCP/IP, incluzând serverul de directoare, în coloana **Stare**. Pentru a actualiza starea serverelor, apăsaţi meniul **View** şi selectaţi **Reîmprospătare**.
4. Pentru a vizualiza mai multe informaţii despre starea serverului de directoare, faceţi clic-dreapta pe **Director** şi selectaţi **Stare**. Aceasta va afişa numărul de conexiuni active, la fel şi alte informaţii cum ar fi nivelurile trecute şi curente de activitate.

   Pe lângă furnizarea de informaţii suplimentare, vizualizarea stării prin această opţiune poate salva timp. Puteţi reîmprospăta starea serverului de directoare fără să folosiţi timpul suplimentar cerut pentru a verifica starea celorlalte servere TCP/IP.

Verificarea joburilor de pe Directory Server

Uneori puteţi dori să monitorizaţi anumite joburi de pe Directory Server. Pentru a verifica job-urile server, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Joburi server**.

Activarea notificării de evenimente

Directory Server suportă notificarea de evenimente, care permite clienţilor să se înregistreze cu serverul LDAP pentru a fi notificaţi la un eveniment specificat, cum ar fi la adăugarea unui obiect în director.

Pentru a activa notificarea de evenimente pentru serverul dumneavoastră, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
5. Apăsaţi **Evenimente**.
6. Selectaţi **Permitere clienţi să se înregistreze pentru notificare de evenimente**.

Puteţi de asemenea specifica înregistrările maxime permise pentru fiecare conexiune şi totalul maxim de înregistrări pe care le permite serverul.

Pentru informaţii suplimentare despre notificarea evenimentelor, vedeţi secţiunea Notificare eveniomente din IBM Directory Server Version 5.1 Programming Reference .

Specificarea setărilor de tranzacţie

Directory Server suportă tranzacţii, ceea ce permite ca un grup de operaţii director LDAP să fie tratat ca o singură unitate. Pentru informaţii suplimentare consultaţi “Tranzacţii” la pagina 40.

Pentru a configura setările de tranzacţii ale serverului dumneavoastră, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
5. Apăsaţi **Tranzacţii**.

6. Specificaţi setările de tranzacţie.

   Notă: Setările de tranzacţie pot avea impact asupra performanţei serverului dumneavoastră LDAP, prin urmare, puteţi dori să experimentaţi diferite setări.

Schimbarea portului sau a adresei IP

Directory Server foloseşte următoarele porturi implicite:
- 389 pentru conexiuni nesecurizate.
- 636 pentru conexiuni securizate (dacă aţi folosit Digital Certificate Manager pentru a activa Directory Server ca o aplicaţie care poate folosi un port securizat).

Notă: Implicit, toate adresele IP definite pe sistemul local sunt legate la server.

Dacă folosiţi deja aceste porturi pentru altă aplicaţie, puteţi asigna un port diferit pentru Directory Server sau puteţi folosi adrese IP diferite pentru cele două servere, dacă aplicaţiile suportă legarea la o animită adresă IP.

Pentru un exemplu cu un server Domino LDAP care este în conflict cu Directory Server, vedeţi Host Domino LDAP şi Directory Server de pe acelaşi iSeries

Pentru a schimba porturile pe care le foloseşte Directory Server, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
5. Apăsaţi pe fişa **Reţea**.
6. Introduceţi numerele corespunzătoare porturilor, apoi apăsaţi **OK**.

Pentru a modifica adresa IP pe care serverul de directoare acceptă conexiuni, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
5. Apăsaţi pe fişa **Reţea**.
6. Apăsaţi butonul **Adrese IP...**.
7. Selectaţi **Utilizare adrese IP selectate** şi selectaţi adresele IP care să fie utilizate de server pentru acceptarea conexiunilor.

Setarea politicii pentru parole

Pentru a seta politica de parolă, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
5. Apăsaţi pe fişa **Parolă**.
6. Introduceţi informaţia despre politica de parolă. Opţional apăsaţi **Validare parolă şi blocare** pentru a specifica informaţii suplimentare despre politica de parolă, apoi apăsaţi **OK**.
7. Selectaţi **OK**.

Notă: Puteţi de asemenea folosi utilitarul ldapmodify (vedeţi “ldapmodify şi ldapadd” la pagina 159) pentru a seta politica de parolă.

Pentru mai multe informaţii despre politica de parolă, vedeţi “Politică parolă” la pagina 59.

Importarea unui fişier LDIF

Puteţi transfera informaţii între diferite servere de directoare prin folosirea fişierelor LDAP Data Interchange Format (LDIF). Consultaţi “LDIF (LDAP Data Interchange Format)” la pagina 184 pentru informaţii suplimentare. Înainte de a începe această procedură, transferaţi fişierul LDIF la serrverul dumneavoastră iSeries ca un fişier şir.

Pentru importa un fişier LDIF în Directory Server, urmaţi aceşti paşi:
1. Dacă serverul de directoare este pornit, opriţi-l. Vedeţi “Oprirea Directory Server” la pagina 96 pentru informaţii despre oprirea serverului de directoare.
2. În Navigator iSeries, expandaţi **Reţea**.
3. Expandaţi **Servere**.
4. Apăsaţi **TCP/IP**.
5. Faceţi clic-dreapta pe **Director** şi selectaţi **Unelte**, apoi **Importare fişier**.

   Opţional puteţi face ca serverul să replice noile date importate când este pornit următoarea dată prin selectarea **Replicare date importate**. Aceasta este de folos când adăugaţi noi intrări la un arbore director existent pe un server master. Dacă importaţi date pentru a iniţializa un server replică (sau peer), în mod normal nu aţi dori să fie replicate datele, deoarece ar putea exista deja pe serverele pentru care acest server este furnizor.

Notă: Puteţi de asemenea folosi utilitarul ldapadd (vedeţi “ldapmodify şi ldapadd” la pagina 159) pentru a importa fişierele LDIF.

Exportarea unui fişier LDIF

Puteţi transfera informaţii între diferite servere de directoare prin folosirea fişierelor LDIF (LDAP Data Interchange Format), vedeţi “LDIF (LDAP Data Interchange Format)” la pagina 184. Puteţi exporta toate sau părţi ale directorului LDAP la un fişier LDIF.

Pentru a exporta un fişier LDIF din serverul de directoare, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Unelte**, apoi **Exportare fişier**.

   Notă: Dacă nu specificaţi o cale complet calificată pentru fişierul LDIF pentru a exporta datele în el, fişierul va fi creat în directorul home din profilul dumneavoastră de utilizator i5/OS.

Note:
1. Asiguraţi-vă că setaţi authoritatea fişierului LDIF pentru a preveni accesul neautorizat la datele directorului. Pentru a face asta, faceţi clic-dreapta pe fişierul din Navigator iSeries, apoi selectaţi **Permissions**.
2. Puteţi crea un fişier plin sau parţial LDIF cu utilitarul ldapsearch, consultaţi “ldapsearch” la pagina 171. Folosiţi opţiunea -L şi redirectaţi ieşirea într-un fişier.

Specificarea unui server pentru referalii directorului

Pentru a asigna servere referal pentru serverul dumneavoastră de directoare, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
5. Selectaţi pagina de proprietăţi **General**.
6. În câmpul **Referal nou**, specificaţi URL-ul serverului referal.
7. La prompt, specificaţi numele serverului referal în format URL. Următoarele sunt exemple de LDAP URL acceptabile:

- ldap://test.server.com
- ldap://test.server.com:400
- ldap://9.9.99.255

Notă: Dacă serverul referal nu foloseşte portul implicit, specificaţi numărul de port corect ca parte a URL-ului, aşa cum este specificat portul 400 în exemplul al doilea de mai sus.

8. Selectaţi **Adăugare**.
9. Selectaţi **OK**.

Adăugarea şi ştergerea sufixelor Directory Server

Adăugarea unui sufix la Directory Server permite serverului să gestioneze acea parte a arborelui director.

Notă: Nu puteţi adăuga un sufix care este sub un alt sufix aflat deja pe server. De exemplu, dacă o=ibm, c=us erau sufixe pe serverul dumneavoastră, nu puteţi adăuga ou=rochester, o=ibm, c=us.

Pentru a adăuga un sufix la serverul de directoare, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
5. Apăsaţi fişa **Bază de date/Sufixe**.
6. În câmpul **Sufix nou**, introduceţi numele noului sufix.
7. Selectaţi **Adăugare**.
8. Selectaţi **OK**.

Notă: Adăugarea unui sufix indică serverului o secţiune a directorului, dar nu creează obiecte. Dacă un obiect care corespunde noului sufix nu exista anterior, trebuie să îl creaţi la fel ca pe orice alt obiect.

Pentru a şterge un sufix din Directory Server, urmaţi aceşi paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
5. Apăsaţi fişa **Bază de date/Sufixe**.
6. Apăsaţi pe sufixul care vreţi să-l înlăturaţi pentru a-l selecta.
7. Apăsaţi **Înlăturare**.

Notă: Puteţi alege să ştergeţi un sufix fără să ştergeţi obiectele directorului de sub el. Aceasta face datele inaccesibile din serverul de directoare. Totuşi, puteţi mai târziu recăpăta acces la date prin adăugarea înapoi a sufixului.

Salvarea şi restaurarea informaţiilor Directory Server

Directory Server memorează informaţii în următoarele locaţii:

- Biblioteca de baze de date (implicit QUSRDIRDB), care conţine conţinutul serverelor de directoare.
- Biblioteca QDIRSRV2, care este folosită pentru a memora informaţii de publicare.
- Biblioteca QUSRSYS, care memorează numeroase elemente începând cu QGLD (specificaţi QUSRSYS/QGLD* pentru a le salva).
- Dacă configuraţi serverul de directoare pentru a înregistra modificări ale directoarelor,este utilizată o bază de date numită QUSRDIRCL pentru înregistra modificările.

Dacă conţinutul directorului se schimbă regulat, ar trebui să vă salvaţi regulat biblioteca de baze de date şi obiectele din aceasta. Datele de configurare sunt de asemenes memorate în următorul director:

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

De asemenea, ar trebui să salvaţi fişierele în acel director de fiecare dată când modificaţi configuraţia sau aplicaţi PTF-uri.

Vedeţi Backup şi recuperare, SC41-5304  pentru informaţii despre salvarea şi restaurarea datelor OS/400.

Lucrul cu accesul administrativ pentru utilizatori autorizaţi

Puteţi acorda acces de administrator pentru profilele utilizator care au primit acces la identificatorul funcţiei Directory Server Administrator (QIBM_DIRSRV_ADMIN).

De exemplu, dacă profilul de utilizator JOHNSMITH primeşte acces la identificatorul funcţiei Directory Server Administrator şi este selectată opţiunea Acordare acces administrator la utilizatorii autorizaţi din dialogul Proprietăţi director, profilul JOHNSMITH are atunci autorizarea de administrator LDAP. Când acest profil este folosit pentru a lega la serverul de directoare folosind următorul DN, os400-profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com, utilizatorul are autoritate de administrator. Sufixul obiectului sistem din acest exemplu este os400-sys=systemA.acme.com. Pentru informaţii suplimentare despre utilizatorii proiectaţi, vedeţi“Backend proiectat pe sistemul de operare” la pagina 65.

Pentru a selecta această opţiune, urmaţi aceşti paşi:

1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
4. La fişa **General** sub **Informaţii administrator** , selectaţi opţiunea **Acordare de acces administrator utilizatorilor autorizaţi**.

Pentru a seta identificatorul de funcţie de autorizare Directory Server Administrator într-un profil de utilizator, urmaţi aceşti paşi:

1. În Navigator iSeries, faceţi clic-dreapta pe numele sistemului şi selectaţi **Administrare aplicaţii**.
2. Apăsaţi fişa **Aplicaţii gazdă**.
3. Expandaţi **Operating System/400**.
4. Apăsaţi **Administrator Directory Server** pentru a evidenţia această opţiune.
5. Apsaţi butonul **Personalizare**.
6. Expandaţi **Utilizatori**, **Grupuri** sau **Utilizatori care nu sunt într-un grup**, care este corespunzător pentru utilizatorul care-l vreţi.
7. Selectaţi un utilizator sau grup să fie adăugat la lista **Acces permis**.
8. Apăsaţi butonul **Adăugare**.
9. Apăsaţi **OK** pentru a salva.
10. Apsaţi **OK** pe dialogul **Administrare aplicaţii**.

Urmărirea accesului şi a modificărilor la directorul LDAP

Vreţi să urmăriţi accesul şi modificările la directorul dumneavoastră LDAP. Puteţi folosi instoricul de modificări a directoarelor LDAP pentru a păstra evidenţa schimbărilor din director. Jurnalul de modificări este localizat sub sufixul special cn=changelog. Este memorat în biblioteca QUSRDIRCL.

Pentru a activa istoricul de modificări, urmaţi aceşti paşi:

1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
5. Apăsaţi pe fişa **Istoric de modificări**.
6. Selectaţi **Înregistrare modificări directoare**.

7. (opţional) În câmpul **Număr maxim de intrări** specificaţi numărul maxim de intrări pe care le va păstra istoricul de modificări. În câmpul **Vârsta maximă** specificaţi cât timp sunt păstrate intrările în istoricul de modificări.

   Notă: Deşi aceşti parametri sunt opţionali, ar trebui să luaţi în considerare specificarea ori a unui număr maxim de intrări, ori a vârstei maxime. Dacă nu specificaţi nici una, istoricul de modificări va păstra toate intrările şi poate deveni foarte mare.

Clasa de obiecte changeLogEntry este folosită pentru a reprezenta modificările aplicate serverului de directoare. Setul de modificări este dat de setul ordonat al tuturor intrărilor din containerul changelog, cum este definit de changeNumber. Informaţiile istoricului de modificări sunt numai pentru citire.

Orice utilizator care se află în lista de control a accesului pentru sufixul cn=changelog poate căuta intrările din istoricul de modificări. Ar trebui să executaţi căutări doar pentru sufixul istoricului de modificări, cn=changelog. Nu încercaţi să adăugaţi, să modificaţi sau să ştergeţi sufixul istoricului de modificări, chiar dacă aveţi această autorizare. Aceasta va cauza rezultate imprevizibile.

Exemplu:

Următorul exemplu foloseşte utilitarul în linie de comandă ldapsearch pentru a extrage toate intrările din istoricul de modificări înregistrate pe server:

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

Activarea auditării obiectelor pentru Directory Server

Directory Server suportă OS/400 auditarea securităţii. Dacă variabila de sistem QAUDCTL are specificat *OBJAUD, puteţi activa auditarea obiectului prin Navigator iSeries.

Pentru a activa auditarea obiecului pentru Directory Server, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
5. Apăsaţi fişa **Auditare**.
6. Selectaţi setarea de auditare pe care vreţi s-o folosiţi pentru serverul dumneavoastră.

Modificările în setările de auditare vor avea efect de îndată ce apăsaţi **OK**. Nu este nevoie să reporniţi Directory Server. Pentru informaţii suplimentare consultaţi “Securitate Directory Server” la pagina 40

Ajustarea setărilor de căutare

Puteţi seta parametrii de căutare pentru a controla capabilităţile de căutare ale utilizatorilor, cum sunt căutarea paginată şi sortată.

Rezultatele paginate vă permit să gestionaţi cantitatea de date returnate de o cerere de căutare. Puteţi cere un subset de intrări în loc să primiţi toate rezultatele o dată. Cererile de căutare următoare afişează următoarea pagină de rezultate până când este anulată operaţia sau este returnat ultimul rezultat.

Căutarea sortată permite unui client să primească rezultate ale căutării sortate bazându-se pe o listă de criterii unde fiecare criteriu reprezintă o cheie de sortare. Aceasta mută responsabilitatea de sortare de la aplicaţia clientului la serverul.

Pentru a ajusta valorile de căutare ale serverului de directoare, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.

5. Apăsaţi pe fişa **Căutare**.

Ajustarea setărilor de performanţă

Puteţi ajusta setările de performanţă ale Serverului dvs. Director prin modificarea oricăror dintre următoarele:
- Dimensiunea cache-ului ACL, dimensiunea cache-ului de intrări, numărul maxim de căutări de stocat în cache-ul de filtru şi cea mai mare căutare de memorat în cache-ul de filtru.
- Setările de tranzacţie server
- Numărul de conexiuni la baza de date şi threaduri server

Pentru a ajusta valorile de cache pentru serverul de directoare, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
5. Apăsaţi fişa **Performanţă**.

Pentru a ajusta valorile de tranzacţie pentru serverul de directoare, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
5. Apăsaţi pe fişa **Tranzacţie**.

Puteţi de asemenea ajusta performanţa serverului de directoare prin modificarea numărului de conexiuni baze de date şi fire de execuţie server pe care le foloseşte serverul. Pentru a modifica această valoare, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
5. Apăsaţi fişa **Bază de date/Sufixe**.

Gestionarea replicării

Pentru a gestiona replicarea, expandaţi categoria **Gestiune replicare** din unealta de administrare web. Pentru informaţii suplimentare despre conceptele de replicare, vedeţi“Replicare” la pagina 35.

Vedeţi următoarele pentru informaţii suplimentare:
- “Crearea topologiei master-replică”
- “Crearea unei topologii master-forwarder-replica” la pagina 108
- “Privire generală asupra creării unei topologii complexe de replicare” la pagina 110
- “Crearea topologiei complexe cu replicare peer” la pagina 110
- “Gestionarea topologiilor” la pagina 113
- “Modificare proprietăţi de replicare” la pagina 115
- “Crearea planificării de replicare” la pagina 117
- “Gestionarea cozilor” la pagina 118

Crearea topologiei master-replică

Pentru a defini o topologie de bază master-replică trebuie să:
1. Creaţi un server master şi să definiţi ce conţine el. Selectaţi subarborele care vreţi să fie replicat şi să specificaţi serverul ca master. Vedeţi “Crearea serverului master (subarbore replicat)” la pagina 104.
2. Creaţi acreditări de folosit de către furnizor. Vedeţi “Crearea acreditărilor” la pagina 105.
3. Creaţi un server replică. Vedeţi “Crearea serverului replică” la pagina 106.

4. Exportaţi topologia de la master către replică. Vedeţi “Copierea datelor la replică” la pagina 107.
5. Modificaţi configuraţia replicii pentru a identifica cine este autorizat să replice modificările făcute asupra ei şi adăugaţi un referal la un master. Vedeţi “Adăugarea informaţiilor furnizorului la replică” la pagina 108.

Notă:

Dacă intrarea de la rădăcina subarborelui care vreţi să fie replicat nu este un sufix în server, înainte de a putea folosi funcţia **Adăugare subarbore**, trebuie să vă asiguraţi că ACL-urile lui sunt definite după cum urmează:

Pentru ACL-uri nefiltrate:

```
ownersource: <same as the entry DN>
ownerpropagate: TRUE

aclsource: <same as the entry DN>
aclpropagate: TRUE
```

Pentru ACL-uri filtrate:

```
ibm-filteraclinherit: FALSE
```

Pentru a satisface cerinţele de ACL, dacă intrarea nu este un sufix în server, editaţi ACL-ul pentru acea intrare în panoul **Gestiune intrări**. Selectaţi intrarea şi apăsaţi **Editare ACL**. Dacă vreţi să adăugaţi ACL-uri nefiltrate selectaţi acea fişă şi selectaţi căsuţa de bifare pentru a specifica dacă ACL-urile sunt explicite sau nu, atât pentru ACL-uri, cât şi pentru proprietari. Asiguraţi-vă că **Propagare ACL-uri** şi **Propagare proprietar** sunt bifate. Dacă vreţi să adăugaţi ACL-uri filtrate, selectaţi acea fişa şi adăugaţi o intrare **cn=this** cu rolul **access-id** pentru ACL-uri şi proprietari. Asiguraţi-vă că **Acumulare ACL-uri filtrate** este nebifat şi că **Propagare proprietar** este bifat. Vedeţi “Gestionarea listelor de control al accesului (ACL-uri)” la pagina 147 pentru informaţii mai detaliate.

Iniţial, obiectul **ibm-replicagroup** creat de acest proces moşteneşte ACL-ul intrării rădăcină pentru subarborele replicat. Aceste ACL-uri ar putea să nu fie potrivite pentru controlul accesului la informaţiile de replicare din director.

Crearea serverului master (subarbore replicat)

Notă: Serverul trebuie să ruleze pentru a efectua această operaţie.

Această operaţie desemnează o intrare ca rădăcină a unui subarbore replicat în mod independent şi creează un **ibm-replicasubentry** care reprezintă acest server drept singurul master pentru subarbore. Pentru a crea un subarbore replicat, trebuie să desemnaţi subarborele pe care vreţi să îl replice serverul.

Expandaţi categoria Gestiune replicare din zona de navigare şi apăsaţi **Gestiune topologie**.

1. Apăsaţi **Adăugare subarbore**.
2. Introduceţi DN-ul intrării rădăcină a subarborelui pe care vreţi să îl replicaţi sau apăsaţi **Răsfoire** pentru a expanda intrările pentru a selecta intrarea care va fi rădăcina subarborelui.
3. URL-ul referal al serverului master este afişat în forma unui URL LDAP, de exemplu:
   `ldap://<myservername>.<mylocation>.<mycompany>.com`

   Notă: URl-ul referal al serverului master este opţional. Este folosit doar:
   - Dacă serverul conţine (sau va conţine) orice subarbore numai citire.
   - Pentru a defini un URL referal care este returnat pentru actualizări la orice subarbore numai citire de pe server.
4. Selectaţi **OK**.
5. Noul server este afişat în panoul Gestiune topologie sub antetul **Subarbori replicaţi**.

Crearea acreditărilor

Expandaţi categoria Gestiune replicare din zona de navigare a uneltei de administrare web şi apăsaţi **Gestiune acreditări**

1. Selectaţi locaţia pe care vreţi să o folosiţi pentru a stoca acreditările din lista de subarbori. Unealta de administrare web vă permite să definiţi acreditări în aceste locaţii:
   - **cn=replication,cn=localhost**, care păstrează acreditările doar pe serverul curent.

     Notă: În majoritatea cazurilor de replicare, este preferată localizarea acreditărilor în cn=replication,cn=localhost deoarece oferă o securitate mai mare decât acreditările localizate în subarbore. Oricum, există anumite situaţii în care acreditările localizate în cn=replication,cn=localhost nu sunt disponibile.

     Dacă încercaţi să adăugaţi o replică sub un server, de exemplu, serverA şi sunteţi conectat la un alt server cu unealta de administrare web, serverB, câmpul **Selectare acreditări** nu afişează opţiunea **cn=replication,cn=localhost**. Aceasta deoarece nu poate citi informaţiile sau actualiza vreo informaţie de sub **cn=localhost** de pe serverA când sunteţi conectat la serverB.

     Opţiunea cn=replication,cn=localhost este disponibilă doar când serverul sub care încercaţi să adăugaţi o replică este acelaşi server la care sunteţi conectat cu unealta de administrare web.
   - În subarborele replicat, caz în care acreditările sunt replicate cu restul subarborelui. Acreditările plasate în subarborele replicat sunt create sub intrarea **ibm-replicagroup=default** pentru acel subarbore.

     Notă: Dacă nu este afişat nici un subarbore mergeţi la “Crearea serverului master (subarbore replicat)” la pagina 104 pentru instrucţiuni despre crearea subarborelui pe care vreţi să îl replicaţi.
2. Selectaţi **Adăugare**.
3. Introduceţi numele pentru acreditările pe care le creaţi, de exemplu **mycreds**, cn= este completat dinainte pentru dvs.
4. Selectaţi tipul de metodă de autentificare pe care vreţi să o folosiţi şi apăsaţi **Următor**.
   - Dacă aţi selectat autentificarea cu legare simplă:
     a. Introduceţi DN-ul pe care îl foloseşte serverul pentru a se lega la replică, de exemplu cn=any
     b. Introduceţi parola pe care serverul o foloseşte când se leagă la replică, de exemplu secret.
     c. Introduceţi parola din nou pentru a confirma că nu există erori tipografice.
     d. Dacă vreţi, introduceţi o descriere scurtă a acreditărilor.
     e. Clic **Sfârşit**.

     Notă: Aţi putea dori să înregistraţi DN-ul de legare a acreditării şi parola pentru referiri ulterioare. Vă va trebui această parolă când creaţi acordul de replică.
   - Dacă aţi selectat autentificarea Kerberos:
     a. Introduceţi DN-ul de legare Kerberos.
     b. Introduceţi parola de legare.
     c. Reintroduceţi parola de legare pentru a o confirma.
     d. Dacă vreţi, introduceţi o descriere scurtă a acreditărilor. Nu sunt necesare alte informaţii. Vedeţi “Activarea autentificării Kerberos pe Directory Server” la pagina 121 pentru informaţii suplimentare.
     e. Clic **Sfârşit**.

     Implicit, furnizorul foloseşte propriul principal de serviciu pentru a se lega la consumator. De exemplu, dacă furnizorul este denumit master.our.org.com şi regiunea este SOME.REALM, DN-ul este **ibm-Kn=ldap/master.our.org.com@SOME.REALM**. Valoarea regiunii nu este sensibilă la majuscule. Dacă există mai mult de un furnizor, trebuie să specificaţi principalul şi parola care vor fi folosite de către toţi furnizorii.

     Pe serverul pe care aţi creat acreditările:

     a. Expandaţi **Management director** şi faceţi clic pe **Gestionare intrări**.

b. Selectaţi subarborele unde aţi stocat acreditările, de exemplu **cn=localhost** şi apăsaţi **Expandare**.
c. Selectaţi **cn=replication** şi apăsaţi **Expandare**.
d. Selectaţi acreditările Kerberos (ibm-replicationCredentialsKerberos) şi apăsaţi **Editare atribute**.
e. Apăsaţi pe fişa **Alte atribute**.
f. Introduceţi **replicaBindDN**, de exemplu, **ibm-kn=myprincipal@SOME.REALM**.
g. Introduceţi **replicaCredentials**. Aceasta este parola KDC folosită pentru **myprincipal**.

Notă: Acest principal şi parolă ar trebui să fie aceleaşi cu cele folosite pentru a rula **kinit** de la linia de comandă.

Pe replică

a. Apăsaţi pe **Gestiune proprietăţi de replicare** în zona de navigare.
b. Selectaţi un furnizor din meniul derulant **Informaţii despre furnizor** sau introduceţi numele subarborelui replicat pentru care vreţi să configuraţi acreditările de furnizor.
c. Apăsaţi **Editare**.
d. Introduceţi DN-ul de legare de replicare. În acest exemplu, **ibm-kn=myprincipal@SOME.REALM**.
e. Introduceţi şi confirmaţi **Parola de legare replicare**. Aceasta este parola KDC folosită pentru **myprincipal**.

- Dacă aţi selectat SSL cu autentificare cu certificat nu este nevoie să furnizaţi vreo informaţie suplimentară, dacă folosiţi certificatul serverului. Dacă alegeţi să folosiţi un certificat diferit de cel al serverului:
  a. Introduceţi numele fişierului cheie.
  b. Introduceţi parola fişierului cheie.
  c. Reintroduceţi parola fişierului cheie pentru a o confirma.
  d. Introuceţi eticheta cheii.
  e. Dacă doriţi, introduceţi o scurtă descriere.
  f. Clic **Sfârşit**.

  Vedeţi “Activarea SSL în Directory Server” la pagina 119 pentru informaţii suplimentare.

5. Pe serverul unde aţi creat acreditările, setaţi valoarea sistem Permite reţinerea informaţiilor de securitate server (QRETSVRSEC) la 1 (reţinere date). Deoarece acreditările de replicare sunt stocate într-o listă de validare, aceasta permite serverului să extragă acreditările din lista de validare când se conectează la replică.

Crearea serverului replică

Notă: Serverul trebuie să ruleze pentru a efectua această operaţie.

Expandaţi categoria **Gestiune replicare** din zona de navigare şi apăsaţi **Gestiune topologie**.

1. Selectaţi subarborele pe care vreţi să îl replicaţi şi apăsaţi **Arată topologie**.
2. Apăsaţi săgeata de lângă selecţia **Topologie de replicare** pentru a expanda lista de servere furnizor.
3. Selectaţi serverul furnizor şi apăsaţi **Adăugare replică**.

În fişa **Server** din fereastra **Adăugare replică**:

- Introduceţi numele gazdă şi numărul de port pentru replica pe care o creaţi. Portul implicit este 389 pentru non-SSL şi 636 pentru SSL. Acestea sunt câmpuri necesare.
- Selectaţi dacă să activaţi comunicaţiile SSL.
- Introduceţi numele replicii sau lăsaţi acest câmp gol pentru a folosi numele gazdă.
- Introduceţi ID replică. Dacă serverul pe care creaţi replica rulează, apăsaţi **Obţinere ID replică** pentru a completa automat acest câmp. Acesta este un câmp obligatoriu, dacă serverul pe care îl adăugaţi va fi server peer sau de înaintare (forwarding). Este recomandat ca toate serverele să aibă aceeaşi ediţie.
- Introduceţi o descriere a serverului replică.

În fişa **Adiţional**:

1. Specificaţi acreditările pe care le foloseşte replica pentru a comunica cu masterul.

   Notă: Unealta de administrare web vă permite să definiţi acreditări în aceste locuri:
   - **cn=replication,cn=localhost**, care păstrează acreditările doar pe serverul care le foloseşte.
   - În subarborele replicat, caz în care acreditările sunt replicate cu restul subarborelui. Acreditările plasate în subarborele replicat sunt create sub intrarea **ibm-replicagroup=default** pentru acel subarbore.

   Plasarea acreditărilor în cn=replication,cn=localhost este considerată mai sigură.

   a. Apăsaţi **Selectare**.
   b. Selectaţi locaţia pentru acreditările pe care vreţi să le folosiţi. Preferabil aceasta este cn=replication,cn=localhost.
   c. Apăsaţi **Arată acreditări**.
   d. Expandaţi lista de acreditări şi selectaţi-o pe aceea pe care vreţi să o folosiţi.
   e. Selectaţi **OK**.

   Vedeţi “Crearea acreditărilor” la pagina 105 pentru informaţii suplimentare despre acreditări de acord.
2. Specificaţi o planificare de replicare din meniul derulant sau apăsaţi **Adăugare** pentru a crea una. Vedeţi “Crearea planificării de replicare” la pagina 117
3. Din lista de capabilităţi furnizor puteţi deselecta orice capabilităţi pe care nu vreţi să le replicaţi la consumator.

   Dacă reţeaua dvs. are un amestec de servere la diferite ediţii, sunt disponibile capabilităţi pe ediţii ulterioare care nu sunt disponibile pe ediţii mai vechi. Unele capabilităţi, precum ACL-uri filtrate şi politica de parolă, folosesc atribute operaţionale care sunt replicate cu alte modificări. În majoritatea cazurilor, dacă sunt folosite aceste facilităţi, doriţi ca toate serverele să le suporte. Dacă toate serverele nu suportă capabilitatea, atunci nu vreţi să o folosiţi. De exemplu, nu aţi dori ACL-uri diferite care să fie active pe fiecare server. Oricum, ar putea fi cazuri în care aţi dori să folosiţi o capabilitate de pe serverele care o suportă şi modificările legate de această capabilitate să nu fie replicate la serverele care nu suportă capabilitatea. În astfel de cazuri, puteţi folosi lista de capabilităţi pentru a marca anumite capabilităţi care să nu fie replicate.
4. Apăsaţi **OK** pentru a crea replica.
5. Este afişat un mesaj care spune că trebuie făcute acţiuni suplimentare. Selectaţi **OK**.

Notă: Dacă adăugaţi mai multe servere ca replici suplimentare sau dacă creaţi o topologie complexă, nu continuaţi cu “Copierea datelor la replică” sau “Adăugarea informaţiilor furnizorului la replică” la pagina 108până ce nu aţi terminat definirea topologiei pe serverul master. Dacă creaţi *masterfile.ldif* după ce aţi încheiat topologia, aceasta conţine intrările director ale serverului master şi o copie completă a acordurilor de topologie. Când încărcaţi acest fişier pe fiecare din servere, fiecare server are aceeaşi informaţie.

Copierea datelor la replică

După ce creaţi replica, trebuie să exportaţi topologia de la master către replică.

1. Pe serverul master creaţi un fişier LDIF pentru date. Pentru a copia toate datele conţinute pe serverul master, faceţi următoarele:
   a. În Navigator iSeries, expandaţi **Reţea**.
   b. Expandaţi **Servere**.
   c. Apăsaţi **TCP/IP**.
   d. Faceţi clic-dreapta pe **Director** şi selectaţi **Unelte**, apoi **Exportare fişier**.
   e. Specificaţi numele fişierului de ieşire LDIF (de exemplu masterfile.ldif), opţional specificaţi un subarbore pentru a exporta (de exemplu subtreeDN) şi apăsaţi **OK**.
2. Pe maşina unde creaţi replica, faceţi următoarele:
   a. Asiguraţi-vă că sufixele replicate sunt definite în configuraţia serverului replică.
   b. Opriţi serverul replică.
   c. Copiaţi fişierul LDIF pe replică şi faceţi următoarele:
      1) În Navigator iSeries, expandaţi **Reţea**.
      2) Expandaţi **Servere**.

3) Apăsaţi **TCP/IP**.
4) Faceţi clic-dreapta pe **Director** şi selectaţi **Unelte**, apoi **Importare fişier**.
5) Specificaţi numele fişierului de intrare LDIF (de exemplu masterfile.ldif), opţional specificaţi dacă vreţi să replicaţi datele şi apăsaţi **OK**.

Acordurile de replicare, planificările, acreditările (dacă sunt stocate în subarborele replicat) şi datele intrării sunt încărcate pe replică.

d. Porniţi serverul.

Adăugarea informaţiilor furnizorului la replică

Trebuie să modificaţi configuraţia replicii pentru a identifica cine este autorizat să replice modificările făcute asupra ei şi adăugaţi un referal la un master.

Pe maşina unde creaţi replica:

1. Expandaţi **Gestiune replicare** din zona de navigare şi apăsaţi **Gestiune proprietăţi de replicare**.
2. Selectaţi **Adăugare**.
3. Selectaţi un furnizor din meniul derulant **Subarbore replicat** sau introduceţi numele subarborelui replicat pentru care vreţi să configuraţi acreditările de furnizor. Dacă editaţi acreditările de furnizor, acest câmp nu este editabil.
4. Introduceţi DN-ul de legare de replicare. În acest exemplu, cn=any.

   Notă: Puteţi folosi oricare dintre aceste două opţiuni, în funcţie de situaţia dvs.
   - Setaţi DN-ul de legare replicare (şi parola) şi un referal implicit pentru toate subarborele replicate pe un server folosind 'referalul şi acreditările implicite'. Acestea ar putea fi folosite când toţi subarborii sunt replicaţi de la acelaşi furnizor.
   - Setaţi DN-ul de legare replicare şi parola independent pentru fiecare subarbore replicat prin adăugarea informaţiilor despre furnizor pentru fiecare subarbore. Acesta ar putea fi folosit când fiecare subarbore are alt furnizor (adică un server master diferit pentru fiecare subarbore).
5. În funcţie de tipul de acreditare, introduceţi şi confirmaţi parola acreditării. (Aţi înregistrat aceasta anterior pentru folosiri ulterioare.)
   - **Legare simplă** - Specificaţi DN-ul şi parola
   - **Kerberos** - Dacă acreditările de la furnizor nu identifică principalul şi parola, adică, dacă va fi folosit propriul principal de serviciu al serverului, atunci DN-ul de legare este ibm-kn=ldap/<*numele_serverului@regiunea_dvs*>. Dacă acreditările au un nume de principal precum <*myprincipal@myrealm*>, folosiţi-l pe acela ca DN. În orice caz, nu este necesară o parolă.
   - **SSL w/ EXTERNAL bind** - Specificaţi DN-ul subiect pentru certificat şi nici o parolă

   Vedeţi "Crearea acreditărilor" la pagina 105.
6. Selectaţi **OK**.
7. Trebuie să reporniţi replica pentru ca schimbările să aibe efect.

Vedeţi "Modificare proprietăţi de replicare" la pagina 115 pentru informaţii suplimentare.

Replica este într-o stare suspendată şi nu apare nici o replicare. După ce aţi terminat de setat topologia dvs. de replicare, trebuie să apăsaţi pe **Gestionare cozi**, să selectaţi replica şi să apăsaţi **Pornire/reluare** pentru a porni replicarea. Vedeţi "Gestionarea cozilor" la pagina 118 pentru informaţii mai detaliate. Replica primeşte acum actualizări de la master.

Crearea unei topologii master-forwarder-replica

Pentru a defini o topologie master-forwarder-replica, trebuie să:

1. Creaţi un server master şi un server replică. Vedeţi "Crearea topologiei master-replică" la pagina 103.
2. Creaţi un nou server replică pentru replica originală. Vedeţi "Crearea unui nou server replică" la pagina 109.
3. Copiaţi datele la replici. Vedeţi "Copierea datelor la replică" la pagina 107.

Crearea unui nou server replică

Dacă aţi setat o topologie de replicare (vedeţi “Crearea serverului master (subarbore replicat)” la pagina 104) cu un master (server1) şi o replică (server2), puteţi schimba rolul lui server2 în cel al unui server de înaintare (forwarding). Pentru a face aceasta trebuie să creaţi o nouă replică (server3) sub server2.

1. Conectaţi Administrarea Web la master (server1)
2. Expandaţi categoria Gestiune replicare din zona de navigare şi apăsaţi **Gestiune topologie**.
3. Selectaţi subarborele pe care vreţi să îl replicaţi şi apăsaţi **Arată topologie**.
4. Apăsaţi săgeata de lângă selecţia **Topologie de replicare** pentru a expanda lista de servere furnizor.
5. Apăsaţi săgeata de lângă selecţia **server1** pentru a expanda lista de servere.
6. Selectaţi server2 şi apăsaţi **Adăugare replică**.
7. În fişa **Server** din fereastra **Adăugare replică**:
   - Introduceţi numele gazdă şi numărul de port pentru replica (server3) pe care o creaţi. Portul implicit este 389 pentru non-SSL şi 636 pentru SSL. Acestea sunt câmpuri necesare.
   - Selectaţi dacă să activaţi comunicaţiile SSL.
   - Introduceţi numele replicii sau lăsaţi acest câmp gol pentru a folosi numele gazdă.
   - Introduceţi ID replică. Dacă serverul pe care creaţi replica rulează, apăsaţi **Obţinere ID replică** pentru a completa automat acest câmp. Acesta este un câmp obligatoriu, dacă serverul pe care îl adăugaţi va fi server peer sau de înaintare (forwarding). Este recomandat ca toate serverele să aibă aceeaşi ediţie.
   - Introduceţi o descriere a serverului replică.

   În fişa **Adiţional**:

   a. Specificaţi acreditările pe care le foloseşte replica pentru a comunica cu masterul.

      Notă: Unealta de administrare web vă permite să definiţi acreditări în două locuri:
      - **cn=replication,cn=localhost**, care păstrează acreditările doar pe serverul care le foloseşte.
      - În subarborele replicat, caz în care acreditările sunt replicate cu restul subarborelui.

      Plasarea acreditărilor în cn=replication,cn=localhost este considerată mai sigură. Acreditările plasate în subarborele replicat sunt create sub intrarea **ibm-replicagroup=default** pentru acel subarbore.

      1) Apăsaţi **Selectare**.
      2) Selectaţi locaţia pentru acreditările pe care vreţi să le folosiţi. De preferat aceasta este cn=replication,cn=localhost.
      3) Apăsaţi **Arată acreditări**.
      4) Expandaţi lista de acreditări şi selectaţi-o pe aceea pe care vreţi să o folosiţi.
      5) Selectaţi **OK**.

      Vedeţi “Crearea acreditărilor” la pagina 105 pentru informaţii suplimentare despre acreditări de acord.

   b. Specificaţi o planificare de replicare din meniul derulant sau apăsaţi **Adăugare** pentru a crea una. Vedeţi “Crearea planificării de replicare” la pagina 117.

   c. Din lista de capabilităţi furnizor puteţi deselecta orice capabilităţi pe care nu vreţi să le replicaţi la consumator.

      Dacă reţeaua dvs. are un amestec de servere la diferite ediţii, sunt disponibile capabilităţi pe ediţii ulterioare care nu sunt disponibile pe ediţii mai vechi. Unele capabilităţi, precum ACL-uri filtrate şi politica de parolă, folosesc atribute operaţionale care sunt replicate cu alte modificări. În majoritatea cazurilor, dacă sunt folosite aceste facilităţi, doriţi ca toate serverele să le suporte. Dacă toate serverele nu suportă capabilitatea, atunci nu vreţi să o folosiţi. De exemplu, nu aţi dori ACL-uri diferite care să fie active pe fiecare server. Oricum, ar putea fi cazuri în care aţi dori să folosiţi o capabilitate de pe serverele care o suportă şi modificările legate de această capabilitate să nu fie replicate la serverele care nu suportă capabilitatea. În astfel de cazuri, puteţi folosi lista de capabilităţi pentru a marca anumite capabilităţi care să nu fie replicate.

   d. Apăsaţi **OK** pentru a crea replica.

8. Copie date de la server2 la noua replică server3. Vedeţi “Copierea datelor la replică” la pagina 107 pentru informaţii despre cum să faceţi aceasta.

9. Adăugaţi acordul furnizorului la server3 care face server2 ca furnizor pentru server 3 şi server 3 drept consumator pentru server2. Vedeţi “Adăugarea informaţiilor furnizorului la replică” la pagina 108 pentru informaţii despre cum să faceţi aceasta.

Rolurile serverelor sunt reprezentate de iconuri în unealta de administrare Web. Topologia dvs. este acum:

- server1 (master)
  - server2 (forwarder)
    - server3 (replica)

Privire generală asupra creării unei topologii complexe de replicare

Folosiţi această privire de ansamblu de nivel înalt ca un ghid pentru setarea unei topologii complexe de replicare.

1. Porniţi toate serverele peer sau viitoare replici. Acest lucru este necesar pentru unealta de administrare Web pentru a culege informaţii de la servere.
2. Porniţi ’primul’ master şi configuraţi-l ca master pentru context.
3. Încărcaţi datele pentru subarborele de replicat pe ’primul’ master, dacă datele nu sunt deja încărcate.
4. Selectaţi subarborele care va fi replicat.
5. Adăugaţi toate potenţialele servere master peer ca replici ale ’primului’ master.
6. Adăugaţi toate celelalte replici.
7. Mutaţi celelalte servere master peer pentru a le promova.
8. Adăugaţi acorduri replică pentru replicile către fiecare masteri de peer.

   Notă: Dacă acreditările urmează să fie create în **cn=replication,cn=localhost**, atunci acreditările trebuie să fie create pe fiecare server după ce ele sunt restartate. Replicarea de către perechi eşuează până când sunt create obiectele de acreditare.
9. Adăugaţi acorduri replică pentru alţi masteri către fiecare masteri de peer. ’Primul’ master are deja acele informaţii.
10. Dezactivaţi subarborele replicat. Aceasta împiedică efectuarea de actualizări în timp ce se copiază date către celelalte servere.
11. Folosiţi Gestionare cozi pentru a sări peste toate pentru fiecare coadă.
12. Exportaţi datele pentru subarborele replicat de la ’primul’ master.
13. Activaţi subarborele.
14. Opriţi serverele replică şi importaţi datele pentru subarborele replicat de pe fiecare replică şi master peer. Apoi reporniţi serverele.
15. Gestionaţi proprietăţile de replicare de pe fiecare replică şi master peer pentru a seta acreditările care vor fi folosite de furnizori.

Crearea topologiei complexe cu replicare peer

Replicarea peer este o topologie de replicare în care mai multe servere sunt masteri. Totuşi, spre deosebire de un mediu multi-master, nu este făcută rezoluţie de conflicte între serverele peer. Serverele LDAP acceptă actualizările furnizate de serverele peer şi actualizează propriile copii ale datelor. Nu este ţinut cont de ordinea în care sunt primite actualizările sau dacă mai multe actualizări intră în conflict.

Pentru a adăuga masteri (peer) suplimentari, trebuie întâi să adăugaţi serverul ca o replică numai citire a masterilor existenţi (vedeţi “Crearea serverului replică” la pagina 106), să iniţializaţi datele director şi apoi să promovaţi serverul să fie master (vedeţi “Mutarea sau promovarea unui server” la pagina 113).

Iniţial, obiectul **ibm-replicagroup** creat de acest proces moşteneşte ACL-ul intrării rădăcină pentru subarborele replicat. Aceste ACL-uri ar putea să nu fie potrivite pentru controlul accesului la informaţiile de replicare din director.

Pentru ca operaţia Adăugare subarbore să aibă succes, intrarea DN pe careo adăugaţi trebuie să aibă ACL-uri corecte, dacă nu este un sufix în server.

Pentru ACL-uri nefiltrate:

- ownersource : <*the entry DN*>
- ownerpropagate : TRUE
- aclsource : <*the entry DN*>
- aclpropagate: TRUE

ACL-uri filtrate:

- ownersource : <*the entry DN*>
- ownerpropagate : TRUE
- ibm-filteraclinherit : FALSE
- ibm-filteraclentry : <*any value*>

Folosiţi funcţia **Editare ACL-uri** din unealta de administrare web pentru a seta ACL-urile pentru informaţiile de replicare asociate cu subarborele de replicare nou creat (vedeţi “Editarea listelor de control al accesului” la pagina 115).

Replica este într-o stare suspendată şi nu apare nici o replicare. După ce aţi terminat de setat topologia dvs. de replicare, trebuie să apăsaţi pe **Gestiune cozi**, să selectaţi replica şi să apăsaţi **Pornire/reluare** pentru a porni replicarea. Vedeţi “Gestionarea cozilor” la pagina 118 pentru informaţii mai detaliate. Replica primeşte acum actualizări de la master.

Folosiţi replicarea peer doar în mediile unde şablonul de actualizări director este bine cunoscut. Actualizările la obiecte particulare din cadrul directorului trebuie să fie făcute doar de către un server peer. Acesta are scopul de a împiedica scenariul în care un server şterge un obiect, după care alt server modifică obiectul. Acest scenariu creează posibilitatea ca un server peer să primească o comandă de ştergere urmată de o comandă de modificare, ceea ce creează un conflict.

Pentru a defini o topologie peer-forwarder-replica, constând în două servere peer-master, două servere forwarding şi patru replici trebuie să:

1. Creaţi un server master şi un server replică. Vedeţi “Crearea topologiei master-replică” la pagina 103.
2. Creaţi două servere replică suplimentare pentru serverul master. Vedeţi “Crearea serverului replică” la pagina 106.
3. Creaţi două replici sub fiecare din cele două servere replică nou create.
4. Promovaţi replica originală la un master. Vedeţi “Promovarea unui server să fie peer”.

   Notă: Serverul pe care vreţi să îl promovaţi la master trebuie să fie o replică frunză fără nici o replică subordonată.
5. Copiaţi datele de la master la noul master şi noile replici. Vedeţi “Copierea datelor la replică” la pagina 107.

Promovarea unui server să fie peer

Folosind topologia de forwarding creată în “Crearea unei topologii master-forwarder-replica” la pagina 108, puteţi promova un server să fie peer. În acest exemplu, veţi promova replica (server3) să fie peer pentru serverul master (server1).

1. Conectaţi Administrarea Web la master (server1).
2. Expandaţi categoria Gestiune replicare din zona de navigare şi apăsaţi **Gestiune topologie**.
3. Selectaţi subarborele pe care vreţi să îl replicaţi şi apăsaţi **Arată topologie**.
4. Apăsaţi săgeata de lângă selecţia **Topologie de replicare** pentru a expanda lista de servere.
5. Apăsaţi săgeata de lângă selecţia **server1** pentru a expanda lista de servere.
6. Apăsaţi săgeata de lângă selecţia **server2** pentru a expanda lista de servere.
7. Apăsaţi **server1** şi apăsaţi **Adăugare replică**. Creaţi server4. Vedeţi “Crearea serverului replică” la pagina 106. Urmaţi aceeaşi procedură pentru a crea server5. Rolurile serverelor sunt reprezentate de iconuri în unealta de administrare Web. Topologia dvs. este acum:
   - server1 (master)
     - server2 (forwarder)
       - server3 (replica)
     - server4 (replica)

- server5 (replica)

8. Apăsaţi **server2** şi apăsaţi **Adăugare replică** pentru a crea server6.
9. Apăsaţi **server4** şi apăsaţi **Adăugare replică** pentru a crea server7. Urmaţi aceeaşi procedură pentru a crea server8. Topologia dvs. este acum:
   - server1 (master)
     - server2 (forwarder)
       - server3 (replica)
       - server6 (replica)
     - server4 (forwarder)
       - server7 (replica)
       - server8 (replica)
     - server5 (replica)
10. Selectaţi **server5** şi daţi clic **Mutare**.

    Notă: Serverul pe care vreţi să îl mutaţi trebuie să fie o replică frunză fără nici o replică subordonată.
11. Selectaţi **Topologie de replicare** pentru a promova replica la un master. Clic **Mutare**.
12. Este afişat panoul **Creare acorduri furnizor suplimentare**. Replicarea peer necesită ca fiecare master să fie un furnizor şi consumator pentru fiecare din ceilalţi masteri din topologie şi pentru fiecare din replicile de pe primul nivel, server2 şi server 4. Server5 este deja un consumator al server1, el are acum nevoie să devină furnizor pentru server1, server2 şi server4. Asiguraţi-vă că casetele de acord furnizor sunt bifate pentru:

Tabela 3.

	Furnizor	Consumator
✓	server5	server1
✓	server5	server2
✓	server5	server4

Apăsaţi **Continuare**.

Notă: În unele cazuri va apare panoul Selectare acreditări care să vă ceară o acreditare care se află în alt loc decât cn=replication,cn=localhost. În astfel de situaţii trebuie să furnizaţi un obiect de acreditare care se află în alt loc decât cn=replication,cn=localhost. Selectaţi acreditările pe care subarborele urmează să le folosească din setul existent de acreditări sau creaţi noi acreditări. Vedeţi “Crearea acreditărilor” la pagina 105

.

13. Selectaţi **OK**. Topologia dvs. este acum:
    - server1 (master)
      - server2 (forwarder)
        - server3 (replica)
        - server6 (replica)
      - server4 (forwarder)
        - server7 (replica)
        - server8 (replica)
      - server5 (master)
    - server5 (master)
      - server1 (master)
      - server2 (forwarder)
      - server4 (forwarder)

14. Copie date de la server1 la toate serverele. Vedeţi “Copierea datelor la replică” la pagina 107 pentru informaţii despre cum să faceţi aceasta.

Gestionarea topologiilor

Topologiile sunt specifice pentru subarborii replicaţi.

- “Vizualizarea topologiei”
- “Adăugarea unei replici”
- “Editarea unui acord”
- “Mutarea sau promovarea unui server”
- “Retrogradarea unui master” la pagina 114
- “Replicarea subarborelui” la pagina 114
- “Editarea subarborelui” la pagina 114
- “Ştergerea subarborelui” la pagina 115
- “Dezactivarea subarborelui” la pagina 115
- “Editarea listelor de control al accesului” la pagina 115

Vizualizarea topologiei

Notă: Serverul trebuie să ruleze pentru a efectua această operaţie.

Expandaţi categoria **Gestiune replicare** din zona de navigare şi apăsaţi **Gestiune topologie**.

1. Selectaţi subarborele pe care vreţi să îl vizualizaţi şi apăsaţi **Arată topologie**.

Topologia este afişată în lista de Replicare topologie. Expandaţi topologiile apăsând pe triunghiurile albastre. Din această listă puteţi să:

- Adăugaţi o replică.
- Editaţi informaţiile de pe o replică existentă.
- Treceţi la un alt server furnizor pentru replică sau promovaţi replica la un server master.
- Ştergeţi o replică.

Adăugarea unei replici

Vedeţi “Crearea serverului replică” la pagina 106.

Editarea unui acord

Puteţi modifica următoarele informaţii pentru replică:

În fişa **Server** puteţi schimba doar:

- Nume gazdă
- Port
- Activare SSL
- Descriere

În fişa **Adiţional** puteţi schimba:

- Acreditări - vedeţi “Crearea acreditărilor” la pagina 105.
- Planificări replicare - vedeţi “Crearea planificării de replicare” la pagina 117.
- Schimbaţi capabilităţile replicate la replica consumator. Din lista de capabilităţi furnizor puteţi deselecta orice capabilităţi pe care nu vreţi să le replicaţi la consumator.
- Când terminaţi, apăsaţi **OK**.

Mutarea sau promovarea unui server

1. Selectaţi serverul dorit şi apăsaţi **Mutare**.

2. Selectaţi serverul pe care vreţi să mutaţi replica sau selectaţi **Topologie de replicare** pentru a promova replica la un master. Clic **Mutare**.
3. În unele cazuri va apare panoul Selectare acreditări care să vă ceară o acreditare care se află în alt loc decât cn=replication,cn=localhost. În astfel de situaţii trebuie să furnizaţi un obiect de acreditare care se află în alt loc decât cn=replication,cn=localhost. Selectaţi acreditările pe care subarborele urmează să le folosească din setul existent de acreditări sau creaţi noi acreditări. Vedeţi “Crearea acreditărilor” la pagina 105.
4. Este afişat **Creare acorduri furnizor suplimentare**. Selectaţi acordurile de furnizor corespunzătoare pentru rolul serverului. De exemplu, dacă un server replică este promovat să fie un server peer, trebuie să selectaţi să creaţi acorduri furnizor cu toate celelalte servere şi cu replicile lor de pe primul nivel. Aceste acorduri permit serverului promovat să funcţioneze ca furnizor pentru celelalte servere şi pentru replicile lor. Acordurile de furnizor existente de la celelalte servere către serverul nou promovat au încă efect şi nu trebuie să fie recreate.
5. Selectaţi **OK**.

Modificarea din arborele topologiei reflectă mutarea serverului.

Consultaţi “Crearea topologiei complexe cu replicare peer” la pagina 110 pentru informaţii suplimentare.

Retrogradarea unui master

Pentru a schimba rolul unui server de la master la replică faceţi următoarele:

1. Conectaţi unealta de administrare web la serverul pe care vreţi să îl retrogradaţi.
2. Apăsaţi **Gestiune topologie**.
3. Selectaţi subarborele şi apăsaţi **Arată topologie**.
4. Ştergeţi toate acordurile pentru serverul pe care vreţi să îl retrogradaţi.
5. Selectaţi serverul pe care îl retrogradaţi şi apăsaţi **Mutare**.
6. Selectaţi serverul sub care veţi plasa serverul retrogradat şi apăsaţi **Mutare**.
7. La fel ca pentru o replică nouă, creaţi noi acorduri de furnizor între serverul retrogradat şi furnizorul lui. Vedeţi “Crearea serverului replică” la pagina 106 pentru instrucţiuni.

Replicarea subarborelui

Notă: Serverul trebuie să ruleze pentru a efectua această operaţie.

Expandaţi categoria **Gestiune replicare** din zona de navigare şi apăsaţi **Gestiune topologie**.

- Apăsaţi **Adăugare subarbore**.
- Introduceţi DN-ul subarborelui pe care vreţi să îl replicaţi sau apăsaţi **Răsfoire** pentru a expanda intrările pentru a selecta intrarea care va fi rădăcina subarborelui.
- Introduceţi URL-ul referal al serverului master. Acesta trebuie să fie în forma unui URL LDAP, de exemplu:
  `ldap://<myservername>.<mylocation>.<mycompany>.com`
- Selectaţi **OK**.
- Noul server este afişat în panoul Gestiune topologie sub antetul **Subarbori replicaţi**.

Editarea subarborelui

Folosiţi această opţiune pentru a schimba URL-ul serverului master către care trmite actualizări acest subarbore şi replicile lui. Trebuie să faceţi acest lucru dacă schimbaţi numărul portului sau numele gazdă al serverului master, dacă schimbaţi masterul la un alt server.

1. Selectaţi subarborele pe care vreţi să îl editaţi.
2. Apăsaţi **Editare subarbore**.
3. Introduceţi URL-ul referal al serverului master. Acesta trebuie să fie în forma unui URL LDAP, de exemplu:
   `ldap://<mynewservername>.<mylocation>.<mycompany>.com`

În funcţie de rolul jucat de către server în acest subarbore (indiferent dacă este master, replică sau forwarding), vor apărea etichete şi butoane diferite în panou.

- Când rolul subarborelui este replică, este afişată o etichetă care indică cum că serverul funcţionează ca replică sau forwarder împreună cu butonul **Faceţi serverul master**. Dacă se apasă pe acest buton atunci serverul la care este conectată unealta de administrare web devine un master.
- Când subarborele este configurat doar pentru replicare prin adăugarea clasei auxiliare (nu există nici un grup şi subintrare implicite), atunci eticheta **Acest subarbore nu este replicat** este afişată împreună cu butonul **Replicare subarbore**. Dacă se apasă pe acest buton sunt adăugate grupul şi subintrarea implicite, astfel încât serverul cu care este conectată unealta de administrare web devine un master.
- Dacă nu sunt găsite subintrări pentru serverele master, atunci este afişată eticheta **Nu este definit nici un server master pentru acest subarbore** împreună cu butonul **Faceţi serverul master**. Dacă se apasă pe acest buton, este adăugată subintrarea lipsă astfel încât serverul cu care este conectată unealta de administrare web devine un master.

Ştergerea subarborelui

1. Selectaţi subarborele pe care vreţi să îl ştergeţi.
2. Apăsaţi **Ştergere subarbore**.
3. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**.

Subarborele este şters din lista **Subarbore replicat**.

Notă: Această operaţie are succes doar dacă intrarea ibm-replicaGroup=default este goală.

Dezactivarea subarborelui

Această funcţie este folositoare când doriţi să realizaţi mentenanţă sau să schimbaţi topologia. Minimizează numărul de actualizări care pot fi făcute la server. Un server activat nu acceptă cereri client. El acceptă cereri doar de la un administrator care foloseşte controlul Administrare server.

Această funcţie este Boolean.

1. Apăsaţi **Quiesce/Unquiesce** pentru a dezactiva subarborele.
2. Când vi se cere să confirmaţi acţiunea, apăsaţi **OK**.
3. Apăsaţi **Quiesce/Unquiesce** pentru a reactiva subarborele.
4. Când vi se cere să confirmaţi acţiunea, apăsaţi **OK**.

Editarea listelor de control al accesului

Informaţiile de replicare (subintrări replică, acorduri de replicare, planificări, posibile acreditări) sunt stocate sub un obiect special, **ibm-replicagroup=default**. Obiectul ibm-replicagroup se află imediat sub intrarea rădăcină a subarborelui replicat. Implicit, acest subarbore moşteneşte ACL-ul de la intrarea rădăcină a subarborelui replicat. Acest ACL ar putea să nu fie potrivit pentru controlul accesului la informaţiile de replicare.

Autorizări necesare:

- Replicare control - Trebuie să aveţi acces de scriere la obiectul ibm-replicagroup=default (sau să fiţi proprietar/administrator).
- Cascadare replicare control - Trebuie să aveţi acces de scriere la obiectul ibm-replicagroup=default (sau să fiţi proprietar/administrator).
- Coadă de control - Trebuie să aveţi acces de scriere la acordul de replicare.

Pentru a vedea proprietăţile ACL folosind unealta de administrare Web şi să lucraţi cu ACL-uri, vedeţi “Gestionarea listelor de control al accesului (ACL-uri)” la pagina 147.

Vedeţi “Liste de control al accesului” la pagina 48 pentru informaţii suplimentare.

Modificare proprietăţi de replicare

Expandaţi categoria **Gestiune replicare** din zona de navigare şi apăsaţi **Gestiune proprietăţi replicare**. Trebuie să vă înregistraţi la unealta de administrare Web ca un utilizator i5/OS proiectat cu autorizările speciale *ALLOBJ şi *IOSYSCFG pentru ca Gestiune proprietăţi de replicare să fie arătat.

În acest panou puteţi:

- Schimba numărul maxim de modificări în aşteptare care vor fi întoarse de interogările de stare replicare. Implicit este 200.
- Adăugaţi, editaţi sau ştergeţi informaţiile de furnizor.

Notă: DN-ul furnizor poate fi DN-ul unui profil de utilizator i5/OS proiectat. Profilul de utilizator i5/OS proiectat nu trebuie să aibă autoritate administrativă LDAP. Utilizatorul nu poate fi un utilizator cu autorizările speciale *ALLOBJ şi *IOSYSCFG şi nu poate să îi fi fost acordată autoritate administrativă prin ID-ul de aplicaţie administrator server de directoare.

Pentru informaţii suplimentare, vedeţi următoarele:

- "Adăugarea informaţiilor de furnizor"
- "Editarea informaţiilor de furnizor"
- "Ştergerea informaţiilor de furnizor" la pagina 117

Adăugarea informaţiilor de furnizor

1. Selectaţi **Adăugare**.
2. Selectaţi un furnizor din meniul derulant sau introduceţi numele subarborelui replicat pe care vreţi să îl adăugaţi ca furnizor .
3. Introduceţi DN-ul de legare de replicare pentru acreditări.

   Notă: Puteţi folosi oricare dintre aceste două opţiuni, în funcţie de situaţia dvs.
   - Setaţi DN-ul de legare replicare (şi parola) şi un referal implicit pentru toate subarborele replicate pe un server folosind 'acreditările şi referalul implicite'. Acestea ar putea fi folosite când toţi subarborii sunt replicaţi de la acelaşi furnizor.
   - Setaţi DN-ul de legare replicare şi parola independent pentru fiecare subarbore replicat prin adăugarea informaţiilor despre furnizor pentru fiecare subarbore. Acesta ar putea fi folosit când fiecare subarbore are alt furnizor (adică un server master diferit pentru fiecare subarbore).
4. În funcţie de tipul de acreditare, introduceţi şi confirmaţi parola acreditării. (Aţi înregistrat aceasta anterior pentru folosiri ulterioare.)
   - **Legare simplă** - specificaţi DN-ul şi parola
   - **Kerberos** - specificaţi un pseudo DN de forma 'ibm-kn=LDAP-service-name@realm' fără o parolă
   - **SSL w/ EXTERNAL bind** - specificaţi DN-ul subiect pentru certificat şi nici o parolă

   Vedeţi "Crearea acreditărilor" la pagina 105.
5. Selectaţi **OK**.

Subarborele furnizorului este adăugat la lista cu informaţii despre furnizor.

Editarea informaţiilor de furnizor

1. Selectaţi subarborele furnizor pe care vreţi să îl editaţi.
2. Apăsaţi **Editare**.
3. Dacă editaţi **Referal şi acreditări implicite**, care sunt folosite pentru a crea intrarea cn=Master Server sub cn=configuration, introduceţi URL-ul serverului de la care clientul vrea să primească actualizări replică în câmpul URL LDAP al Furnizorului implicit. Acesta trebuie să fie un URL LDAP valid (ldap://). Altfel, săriţi la pasul 4.
4. Introduceţi DN-ul de legare de replicare pentru noile acreditări pe care vreţi să le folosiţi.
5. Introduceţi şi confirmaţi parola de acreditare.
6. Selectaţi **OK**.

Ştergerea informaţiilor de furnizor

1. Selectaţi subarborele furnizor pe care vreţi să îl ştergeţi.
2. Apăsaţi **Ştergere**.
3. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**.

Subarborele este şters din lista Informaţii furnizor.

Crearea planificării de replicare

Puteţi defini opţional planificări pentru a planifica replicarea la anumite momente de timp sau să nu se facă replicarea la anumite momente de timp. Dacă nu folosiţi o planificare, serverul planifică replicarea oricând se face o schimbare. Aceasta este echivalentă cu specificarea unei planificări cu replicare imediată începând la 12:00 AM în toate zilele.

Expandaţi categoria **Gestiune replicare** din zona de navigare şi apăsaţi **Gestiune planificări**.

În fişa **Planificare săptămânală**, selectaţi subarborele pentru care vreţi să creaţi planificarea şi apăsaţi **Arată planificări**. Dacă există vreo planificare, ele sunt afişate în căsuţa **Planificări săptămânale**. Pentru a crea sau adăuga o nouă planificare:

1. Selectaţi **Adăugare**.
2. Introduceţi un nume pentru planificare. De exemplu **schedule1**.
3. Pentru fiecare zi, planificarea zilnică este specificată ca **Nici una**. Aceasta înseamnă că nu este planificat nici un eveniment de replicare. Ultimul eveniment de replicare, dacă există, are încă efect. Deoarece aceasta este o replică nouă, nu există evenimente de replicare anterioare, de aceea, planificarea este implicit pe replicare imediată.
4. Puteţi selecta o zi şi să apăsaţi **Adăugare planificare zilnică** pentru a crea o planificare de replicare zilnică pentru ea. Dacă creaţi o planificare zilnică aceasta devine planificarea implicită pentru fiecare zi a săptămânii. Puteţi să:
   - Păstraţi planificarea zilnică ca cea implicită pentru fiecare zi sau să selectaţi o anumită zi şi să modificaţi planificarea la Nici una. Ţineţi minte că ultimul eveniment de replicare care a apărut are încă efect pentru o zi care nu are planificate evenimente de replicare.
   - Modificaţi planificarea zilnică prin selectarea unei zile şi apăsarea pe **Editare planificare zilnică**. Reţineţi că schimbările la o planificare zilnică afectează toate zilele care folosesc acea planificare, nu doar ziua pe care aţi selectat-o.
   - Creaţi o altă planificare zilnică prin selectarea unei zile şi apăsarea pe **Adăugare planificare zilnică**. După ce aţi creat această planificare, ea este adăugată la meniul derulant **Planificare zilnică**. Trebuie să selectaţi această planificare pentru fiecare zi pentru care vreţi să fie folosită planificarea.

   Vedeţi “Crearea planificării zilnice” pentru mai multe informaţii despre setarea planificărilor zilnice.
5. Când terminaţi, apăsaţi **OK**.

Crearea planificării zilnice

Expandaţi categoria **Gestiune replicare** din zona de navigare şi apăsaţi **Gestiune planificări**.

În fişa **Planificare zilnică**, selectaţi subarborele pentru care vreţi să creaţi planificarea şi apăsaţi **Arată planificări**. Dacă există vreo planificare, ele sunt afişate în căsuţa **Planificări zilnice**. Pentru a crea sau adăuga o nouă planificare:

1. Selectaţi **Adăugare**.
2. Introduceţi un nume pentru planificare. De exemplu, **monday1**.
3. Selectaţi setarea de fus orar, fie UTC sau local.
4. Selectaţi un tip de replicare din meniul derulant.

   Imediat
   Realizează orice actualizări de intrare în aşteptare de la ultimul eveniment de replicare şi apoi actualizează intrările în mod continuu până când apare următorul eveniment de actualizare planificat.

   O dată Realizează toate actualizările în aşteptare anterioare momentului de start. Orice actualizări făcute după momentul de start, aşteaptă până la următorul eveniment de replicare planificat.

5. Selectaţi un moment de start pentru evenimentul de replicare.
6. Selectaţi **Adăugare**. Sunt afişate tipul evenimentului de replicare şi timpul.
7. Adăugaţi sau ştergeţi evenimente pentru a completa planificarea. Lista de evenimente este reîmprospătată în ordine cronologică.
8. Când terminaţi, apăsaţi **OK**.

De exemplu:

Tabela 4.

Tip replicare	Oră pornire
Imediat	12:00 AM
O dată	10:00 AM
O dată	2:00 PM
Imediat	4:00 PM
O dată	8:00 PM

În această planificare, primul eveniment de replicare apare la miezul nopţii şi actualizează orice modificări în aşteptare anterioare acelui moment. Actualizările de replicare continuă să fie făcute până la 10:00 AM. Actualizările făcute între 10:00 AM şi 2:00 PM aşteaptă până la 2:00 PM pentru a fi replicate. Orice actualizări făcute între 2:00 PM şi 4:00 PM aşteaptă evenimentul de replicare planificat la 4:00 PM, după care actualizările de replicare continuă până la următorul eveniment de replicare planificat la 8:00 PM. Orice actualizări făcute după 8:00 PM, aşteaptă până la următorul eveniment de replicare planificat.

Notă: Dacă evenimentele de replicare sunt planificate prea apropiate unele de altele, un eveniment de replicare ar putea fi sărit dacă actualizările de la evenimentul anterior sunt încă în desfăşurare când este planificat următorul eveniment.

Gestionarea cozilor

Acest task vă permite să monitorizaţi starea replicării pentru fiecare acord (coadă) de replicare folosit de acest server.

Expandaţi categoria **Gestiune replicare** din zona de navigare şi apăsaţi **Gestiune cozi**.

Selectaţi replica pentru care vreţi să gestionaţi coada.

- În funcţie de starea replicii, puteţi apăsa pe **Suspendare/reluare** pentru a opri sau porni replicarea.
- Apăsaţi **Forţare replicare** pentru a replica toate modificările în aşteptare indiferent de când este planificată următoarea replicare.
- Apăsaţi **Detalii coadă**, pentru informaţii mai complete despre coada replicii. Puteţi de asemenea gestiona coada de la această selecţie.
- Apăsaţi **Reîmprospătare** pentru a actualiza cozile şi pentru a şterge mesajele serverului.

Detalii coadă

Dacă aţi apăsat **Detalii coadă**, sunt afişate trei fişe:

- Stare
- Ultimele detalii încercate
- Schimbări în aşteptare

Fişa **Stare** afişează numele replicii, subarborele ei, starea ei şi o înregistrare a momentelor de replicare. Din acest panou puteţi suspenda sau relua replicarea apăsând pe **Reluare**. Apăsaţi **Reîmprospătare** pentru a actualiza informaţiile despre coadă.

Fişa **Ultimele detalii încercate** oferă informaţii despre ultima încercare de actualizare. Dacă nu poate fi încărcată o intrare apăsaţi **Sărire intrare blocantă** pentru a continua replicarea cu următoarea intrare în aşteptare. Apăsaţi **Reîmprospătare** pentru a actualiza informaţiile despre coadă.

Fişa **Schimbări în aşteptare** arată toate schimbările la replică în aşteptare. Dacă replicarea este blocată puteţi şterge toate schimbările în aşteptare apăsând pe **Sărire toate**. Apăsaţi pe **Reîmprospătare** pentru a actualiza lista de schimbări în aşteptare ca să reflecte orice noi actualizări sau actualizări care au fost procesate.

Notă: Dacă alegeţi să săriţi modificările blocante, trebuie să vă asiguraţi că serverul consumator este în cele din urmă actualizat. Consultaţi “ldapdiff” la pagina 180 pentru informaţii suplimentare.

Activarea SSL în Directory Server

Dacă aveţi instalat Digital Certificate Manager pe sistemul dvs., puteţi folosi securitatea Secure Sockets Layer (SSL) pentru a proteja accesul la serverul dvs. director. Înainte de a activa SSL pe serverul de directoare, puteţi găsi util să citiţi “SSL (Secure Sockets Layer) şi TLS (Transport Layer Security) cu Directory Server” la pagina 41.

Pentru a folosi o conexiune SSL când administraţi Directory Server din Navigator iSeries sau să folosiţi SSL cu clientul Windows LDAP, trebuie să aveţi unul din produsele Client Encryption (5722CE2 sau 5722CE3) instalate pe PC.

Pentru a activa SSL pe serverul LDAP, faceţi următoarele:

1. **Asociaţi un certificat cu Directory Server**
   a. Dacă vreţi să gestionaţi Directory Server printr-o conexiune SSL de la Navigator iSeries, vedeţi Ghidul utilizatorului iSeries Access pentru Windows (este instalat opţional pe PC, când aţi instalat Navigator iSeries). Dacă intenţionaţi să permiteţi atât conexiuni SSL cât şi non SSL către serverul de directoare, puteţi alege să săriţi peste acest pas.
   b. Porniţi IBM Digital Certificate Manager. Vedeţi Pornire Digital Certificate Manager din subiectul Digital Certificate Manager pentru mai multe informaţii.
   c. Dacă trebuie să obţineţi sau să creaţi certificate sau să setaţi altfel sau să modificaţi sistemul de certificate, faceţi aceasta acum. Vedeţi Digital Certificate Manager pentru informaţii despre setarea unui sistem de certificate. Sunt două aplicaţii server şi o aplicaţie client asociate cu Directory Server. Acestea sunt:

      Aplicaţia Directory Server
      Aplicaţia Directory Server este serverul însuşi.

      Aplicaţia de publicare Directory Server
      Aplicaţia de publicare Directory Server identifică certificatul folosit prin publicare.

      Aplicaţia client Directory Server
      Aplicaţia client Directory Server identifică certificatul implicit folosit de aplicaţiile care folosesc API-urile ILE client LDAP.

   d. Apăsaţi **Selectare depozit de certificate**.
   e. Selectaţi ***SYSTEM**. Apăsaţi **Continuare** .
   f. Introduceţi parola corespunzătoare pentru depozitul de certificate *SYSTEM. Apăsaţi **Continuare**.
   g. Când meniul de navigare din stânga se reîncarcă, expandaţi **Gestiune aplicaţii**.
   h. Apăsaţi **Actualizare asignare certificat**.
   i. În ecranul următor, selectaţi aplicaţia **Server**. Apăsaţi **Continuare**.
   j. Selectaţi **serverul de directoare**.
   k. Apăsaţi **Actualizare asignare certificat** pentru a asigna un certificat la Directory Server ca să îl folosească pentru a stabili identitatea sa către clienţii iSeries Access pentru Windows.

      Notă: Dacă alegeţi un certificat de la o CA ale cărei certificate CA nu este în baza de date de chei a clientului dvs. iSeries Access pentru Windows, va trebui să o adăugaţi pentru a putea folosi SSL. Terminaţi această procedură înainte de a o începe pe aceea.

l. Selectaţi un certificat din listă pentru a îl asigna la server.

m. Apăsaţi **Asignare certificat nou**.

n. DCM se reîncarcă în pagina **Actualizare asignare certificat** cu un mesaj de confirmare. Când aţi terminat să setaţi certificatele pentru Directory Server, apăsaţi **Gata**.

2. **Asociaţi un certificat pentru publicarea Directory Server**. (pas opţional) Dacă vreţi de asemenea să permiteţi publicarea de la sistem către un Directory Server printr-o conexiune SSL, aţi putea dori să asociaţi de asemenea un certificat cu publicarea Directory Server. Aceasta identifică certificatul implicit şi CA-urile de încredere pentru aplicaţiile care folosesc API-urile ILE LDAP care nu specifică propriul ID aplicaţie sau o altă bază de date de chei.

   a. Porniţi IBM Digital Certificate Manager.

   b. Apăsaţi **Selectare depozit de certificate**.

   c. Selectaţi ***SYSTEM**. Apăsaţi **Continuare** .

   d. Introduceţi parola corespunzătoare pentru depozitul de certificate *SYSTEM. Apăsaţi **Continuare**.

   e. Când meniul de navigare din stânga se reîncarcă, expandaţi **Gestiune aplicaţii**.

   f. Apăsaţi **Actualizare asignare certificat**.

   g. În ecranul următor, selectaţi aplicaţia **Client**. Apăsaţi **Continuare**.

   h. Selectaţi **Publicarea Directory Server**.

   i. Apăsaţi **Actualizare asignare certificat** pentru a asigna un certificat la publicarea Directory Server care îşi va stabili identitatea.

   j. Selectaţi un certificat din listă pentru a îl asigna la server.

   k. Apăsaţi **Asignare certificat nou**.

   l. DCM se reîncarcă în pagina **Actualizare asignare certificat** cu un mesaj de confirmare.

   Notă: Aceşti paşi presupun că publicaţi deja informaţii la Directory Server cu o conexiune non-SSL. Vedeţi “Publicarea informaţiilor pe serverul de directoare” la pagina 151 pentru informaţii complete despre setarea unei publicări.

3. **Asocierea unui certificat pentru clientul Directory Server**. (pas opţional) Dacă aveţi alte aplicaţii care folosesc conexiuni SSL către un Directory Server, trebuie să asociaţi de asemenea un certificat cu un client Directory Server.

   a. Porniţi IBM Digital Certificate Manager.

   b. Apăsaţi **Selectare depozit de certificate**.

   c. Selectaţi ***SYSTEM**. Apăsaţi **Continuare** .

   d. Introduceţi parola corespunzătoare pentru depozitul de certificate *SYSTEM. Apăsaţi **Continuare**.

   e. Când meniul de navigare din stânga se reîncarcă, expandaţi **Gestiune aplicaţii**.

   f. Apăsaţi **Actualizare asignare certificat**.

   g. În ecranul următor, selectaţi aplicaţia **Client**. Apăsaţi **Continuare**.

   h. Selectaţi **Clientul Directory Server**.

   i. Apăsaţi **Actualizare asignare certificat** pentru a asigna un certificat pentru clientul Directory Server care îşi va stabili identitatea.

   j. Selectaţi un certificat din listă pentru a îl asigna la server.

   k. Apăsaţi **Asignare certificat nou**.

   l. DCM se reîncarcă în pagina **Actualizare asignare certificat** cu un mesaj de confirmare.

După ce SSL este activat, puteţi schimba portul pe care îl foloseşte Directory Server pentru conexiuni securizate.

Activarea autentificării Kerberos pe Directory Server

Dacă aveţi Network Authentication Service configurat pe sistemul dvs., puteţi seta Directory Server să folosească autentificarea Kerberos. Autentificarea Kerberos se aplică la utilizatori şi la administrator. Înainte de activarea Kerberos pe serverul de directoare, puteţi găsi de folos să citiţi o privire generală despre folosirea Kerberos cu Directory Server.

Pentru a activa autentificarea Kerberos, urmaţi aceşti paşi:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
5. Apăsaţi fişa **Kerberos**.
6. Bifaţi **Activare autentificare Kerberos** .
7. Specificaţi alte setări din pagina **Kerberos** corespunzător cu situaţia dumneavoastră. Vedeţi ajutorul online al paginii pentru informaţii despre câmpurile individuale.

Gestionarea schemei

Pentru mai multe informaţii despre schemă, vedeţi “Schema” la pagina 15.

Schema poate fi gestionată folosind unealta de adminstrare web sau o aplicaţie LDAP precum ldapmodify în combinaţie cu fişierele LDIF. Când definiţi pentru prima dată noi clase de obiecte sau atribute, poate fi mai convenabil să folosiţi unealta de administrare web. Dacă trebuie să copiaţi noua schemă pe alte servere (poate ca parte a unui produs sau unealtă pe care le dispuneţi), utilitarul ldapmodify poate fi mai folositor, vedeţi “Copierea schemei la alte servere” la pagina 130 pentru mai multe informaţii.

Vedeţi următoarele pentru informaţii suplimentare:
- “Vizualizarea claselor de obiecte”
- “Adăugarea unei clase de obiect” la pagina 122
- “Editarea clasei de obiecte” la pagina 123
- “Copierea unei clase de obiecte” la pagina 124
- “Ştergerea unei clase de obiecte” la pagina 125
- “Vizualizarea atributelor” la pagina 126
- “Adăugarea unui atribut” la pagina 126
- “Editarea unui atribut” la pagina 127
- “Copierea unui atribut” la pagina 128
- “Ştergerea unui atribut” la pagina 130

Vizualizarea claselor de obiecte

Puteţi vizualiza clasele de obiecte din schemă folosind ori unealta de administrare web, metoda preferată sau folosind linia de comandă.

Administrare Web

Expandaţi **Gestiune schema** în zona de navigare şi apăsaţi pe **Gestiune clase obiect**. Este afişat un panou numai citire care vă permite să vedeţi clasele de obiecte din schemă şi caracteristicile lor. Clasele de obiecte sunt afişate în ordine alfabetică. Vă puteţi deplasa o pagină înapoi sau înainte apăsând pe Anterior sau Următor. Câmpul de lângă aceste butoane identifică pagina la care sunteţi. Puteţi de asemenea folosi meniul derulant al acestui câmp pentru a sări la o anumită pagină. Prima clasă de obiecte listată pe pagină este afişată cu numărul de pagină pentru a vă ajuta să localizaţi clasa de obiecte pe care vreţi să o vizualizaţi. De exemplu, dacă vreţi să căutaţi clasa de obiecte **person**, expandaţi meniul derulant şi căutaţi în jos până vedeţi **Page 14 of 16 nsLiServer** şi **Page 15 of 16 printerLPR**. Deoarece person se află alfabetic între nsLiServer şi printerLPR, selectaţi Page 14 şi apăsaţi **start**.

Puteţi de asemenea afişa clasele de obiecte sortate după tip. Selectaţi **Tip** şi apăsaţi **Sortare**. Clasele de obiecte sunt sortate alfabetic în interiorul tipului lor, Abstract, Auxiliar sau Structural. Similar, puteţi inversa ordinea listei prin selectarea **Descendent** şi apăsarea pe **Sortare**.

După ce aţi localizat clasa de obiect pe care o vreţi, puteţi să îi vedeţi tipul, moştenirea, atributele necesare şi atributele opţionale. Expandaţi meniurile derulante pentru moştenire, atribute necesare şi atribute opţionale pentru a vedea listingurile complete pentru fiecare caracteristică.

Puteţi alege operaţiile de clase de obiecte pe care vreţi să le efectuaţi din bara de unelte din partea dreaptă, precum:

- Adăugare
- Editare
- Copiere
- Ştergere

Când aţi terminat apăsaţi pe **Închidere** pentru a reveni la panoul IBM Directory Server **Welcome**.

Linie de comandă

Pentru a vedea clasele de obiecte conţinute în schemă lansaţi comanda:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Adăugarea unei clase de obiect

Administrare Web

Dacă nu aţi făcut asta deja, expandaţi **Gestiune schema** în zona de navigare, apoi apăsaţi pe **Gestiune clase obiect**. Pentru a crea o nouă clasă obiect:

1. Selectaţi **Adăugare**.

   Notă: De asemnea puteţi accesa acest panou prin expandara **Gestiune schemă** în zona de navigare, apoi apăsaţi pe **Adăugare clasă de obiecte**.
2. În fişa **Proprietăţi generale**:
   - Introduceţi **Nume clasă obiect**. Acesta este un câmp obligatoriu şi este descriptiv pentru funcţia clasei de obiecte. De exemplu, **tempEmployee** pentru o clasă de obiect folosită pentru urmări angajaţii temporari.
   - Introduceţi o **Descriere** a clasei de obiecte, de exemplu **Clasa de obiecte folosită pentru angajaţi temporari**.
   - Introduceţi **OID** pentru clasa de obiecte. Acesta este un câmp obligatoriu. Vedeţi “Identificator obiect (OID)” la pagina 25. Dacă nu aveţi un OID, puteţi folosi **Nume clasă obiect** ataşat cu **-oid**. De exemplu, dacă numele clasei de obiect este **tempEmployee**, atunci OID este **tempEmployee-oid**. Puteţi schimba valoarea acestui câmp.
   - Selectaţi o **Clasă superioară de obiecte** din lista derulantă. Aceasta determină clasa de obiecte din care sunt moştenite atributele. În mod normal, **Clasa superioară de obiecte** este **top**, totuşi, ea poate fi altă clasă de obiecte. De exemplu, o clasă superioară de obiecte pentru **tempEmployee** ar putea fi **ePerson**.
   - Selectaţi un **Tip clasă de obiect**. Vedeţi “Clase obiect” la pagina 18 pentru informaţii suplimentare despre tipurile de clase de obiecte.
   - Apăsaţi pe fişa Atribute pentru a specifica atributele obligatorii şi cele opţionale pentru clasa de obiecte şi pentru a vizualiza atributele moştenite sau apăsaţi **OK** pentru a adăuga noua clasă de obiecte sau apăsaţi **Anulare** pentru a reveni la **Gestiune clase de obiecte** fără a face vreo schimbare.
3. În fişa **Atribute**:
   - Selectaţi un atribut din lista alfabetică de **Atribute disponibile** şi apăsaţi **Adăugare la obligatorii** pentru a face atributul obligatoriu sau apăsaţi **Adăugare la opţionale** pentru a face atributul opţional pentru clasa de obiecte. Atributul este afişat în lista corespunzătoare de atribute selectate.
   - Repetaţi acest proces pentru toate atributele pe care vreţi să le selectaţi.

- Puteţi muta un atribut de la o listă la alta sau să ştergeţi atributul din listele selectate prin selectarea lui şi apăsarea pe butonul corespunzător **Mutare la** sau **Ştergere**.
- Puteţi vedea lista de atribute obligatorii şi opţionale moştenite. Atributele moştenite se bazează pe **Clasa superioară de obiecte** selectată în fişa **General**. Nu puteţi schimba atributele moştenite. Totuşi, dacă schimbaţi **Clasa superioară de obiecte** din fişa **General**, este afişat un alt set de atribute moştenite.

4. Apăsaţi **OK** pentru a adăuga noua clasă de obiecte sau apăsaţi **Anulare** pentru a reveni la **Gestiune clase de obiecte** fără a face vreo modificare.

Notă: Dacă aţi apăsat **OK** în fişa **General** fără a adăuga vreun atribut, puteţi adăuga atribute prin editarea noii clase de obiecte.

Linie de comandă

Pentru a adăuga o clasă de obiecte folosind linia de comandă, lansaţi comanda următoare:

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

unde <*filename*>conţine:

```
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>))
```

Editarea clasei de obiecte

Nu sunt permise toate modificările de schemă. Vedeţi “Modificări de schemă nepermise” la pagina 28 pentru restricţii de modificare.

Administrare Web

Dacă nu aţi făcut asta deja, expandaţi **Gestiune schema** în zona de navigare, apoi apăsaţi pe **Gestiune clase obiect**. Pentru a edita o clasă de obiecte:

1. Apăsaţi butonul radio de lângă clasa de obiecte pe care vreţi să o editaţi.
2. Apăsaţi **Editare** .
3. Selectaţi o fişă:
   - Folosiţi fişa **General** pentru:
     - Modificaţi **Descriere**.
     - Modificaţi **Clasă superioară de obiecte**. Selectaţi o clasă superioară de obiecte din lista derulantă. Aceasta determină clasa de obiecte din care sunt moştenite atributele. În mod normal, **Clasa superioară de obiecte** este **top**, totuşi, ea poate fi altă clasă de obiecte. De exemplu, o clasă superioară de obiecte pentru **tempEmployee** ar putea fi **ePerson**.
     - Modificaţi **Tipul clasei de obiecte**. Selectaţi un tip de clasă de obiecte. Vedeţi “Clase obiect” la pagina 18 pentru informaţii suplimentare despre tipurile de clase de obiecte.
     - Apăsaţi pe fişa Atribute pentru a modifica atributele obligatorii şi cele opţionale pentru clasa de obiecte şi pentru a vizualiza atributele moştenite sau apăsaţi **OK** pentru a aplica modificările sau apăsaţi **Anulare** pentru a reveni la **Gestiune clase de obiecte** fără a face vreo schimbare.
   - Folosiţi fişa **Atribute** pentru :

     Selectaţi un atribut din lista alfabetică de **Atribute disponibile** şi apăsaţi **Adăugare la obligatorii** pentru a face atributul obligatoriu sau apăsaţi **Adăugare la opţionale** pentru a face atributul opţional pentru clasa de obiecte. Atributul este afişat în lista corespunzătoare de atribute selectate.

     Repetaţi acest proces pentru toate atributele pe care vreţi să le selectaţi.

     Puteţi muta un atribut de la o listă la alta sau să ştergeţi atributul din listele selectate prin selectarea lui şi apăsarea pe butonul corespunzător **Mutare la** sau **Ştergere**.

Puteţi vedea lista de atribute obligatorii şi opţionale moştenite. Atributele moştenite se bazează pe **Clasa superioară de obiecte** selectată în fişa **General**. Nu puteţi schimba atributele moştenite. Totuşi, dacă schimbaţi **Clasa superioară de obiecte** din fişa **General**, este afişat un alt set de atribute moştenite.

4. Apăsaţi **OK** pentru a aplica modificările sau apăsaţi **Anulare** pentru a reveni la **Gestiune clase de obiecte** fără a face vreo schimbare.

Linie de comandă

Vizualizare clase de obiecte conţinute în schemă lansaţi comanda:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Pentru a edita o clasă de obiecte folosind linia de comandă, lansaţi comanda următoare:

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

unde <*filename*>conţine:

```
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>) )
```

Copierea unei clase de obiecte

Administrare Web

Dacă nu aţi făcut asta deja, expandaţi **Gestiune schema** în zona de navigare, apoi apăsaţi pe **Gestiune clase obiect**. Pentru a copia o clasă de obiecte:

1. Apăsaţi butonul radio de lângă clasa de obiecte pe care vreţi să o copiaţi.
2. Apăsaţi **Copiere**.
3. Selectaţi o fişă:
   - Folosiţi fişa **General** pentru:
     - Modificaţi **numele clasei de obiecte**. Numele implicit este numele clasei de obiecte copiate ataşat cu cuvântul COPY. De exemplu, **tempPerson** este copiat ca **tempPersonCOPY**.
     - Modificaţi **Descriere**.
     - Modificaţi **OID**. OID-ul implicit este OID-ul clasei de obiecte copiate ataşat cu cuvântul COPY. De exemplu, **tempPerson-oid** este copiat ca **tempPerson-oidCOPY** .
     - Modificaţi **Clasă superioară de obiecte**. Selectaţi o clasă superioară de obiecte din lista derulantă. Aceasta determină clasa de obiecte din care sunt moştenite atributele. În mod normal, **Clasa superioară de obiecte** este **top**, totuşi, ea poate fi altă clasă de obiecte. De exemplu, o clasă superioară de obiecte pentru **tempEmployeeCOPY** ar putea fi **ePerson**.
     - Modificaţi **Tipul clasei de obiecte**. Selectaţi un tip de clasă de obiecte. Vedeţi “Clase obiect” la pagina 18 pentru informaţii suplimentare despre tipurile de clase de obiecte.
     - Apăsaţi pe fişa **Atribute** pentru a modifica atributele obligatorii şi cele opţionale pentru clasa de obiecte şi pentru a vizualiza atributele moştenite sau apăsaţi **OK** pentru a aplica modificările sau apăsaţi **Anulare** pentru a reveni la **Gestiune clase de obiecte** fără a face vreo schimbare.
   - Folosiţi fişa **Atribute** pentru :

     Selectaţi un atribut din lista alfabetică de **Atribute disponibile** şi apăsaţi **Adăugare la obligatorii** pentru a face atributul obligatoriu sau apăsaţi **Adăugare la opţionale** pentru a face atributul opţional pentru clasa de obiecte. Atributul este afişat în lista corespunzătoare de atribute selectate.

     Repetaţi acest proces pentru toate atributele pe care vreţi să le selectaţi.

Puteţi muta un atribut de la o listă la alta sau să ştergeţi atributul din listele selectate prin selectarea lui şi apăsarea pe butonul corespunzător **Mutare la** sau **Ştergere**.

Puteţi vedea lista de atribute obligatorii şi opţionale moştenite. Atributele moştenite se bazează pe **Clasa superioară de obiecte** selectată în fişa **General**. Nu puteţi schimba atributele moştenite. Totuşi, dacă schimbaţi **Clasa superioară de obiecte** din fişa **General**, este afişat un alt set de atribute moştenite.

4. Apăsaţi **OK** pentru a aplica modificările sau apăsaţi **Anulare** pentru a reveni la **Gestiune clase de obiecte** fără a face vreo schimbare.

Linie de comandă

Vizualizare clase de obiecte conţinute în schemă lansaţi comanda:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Selectaţi clasa de obiecte pe care vreţi să o copiaţi. Folosiţi un editor pentru a schimba informaţiile corespunzătoare şi salvaţi modificările în <*filename*>. Apoi lansaţi următoarea comandă:

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

unde <*filename*>conţine:

```
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>) )
```

Ştergerea unei clase de obiecte

Nu sunt permise toate modificările de schemă. Vedeţi “Modificări de schemă nepermise” la pagina 28 pentru restricţii de modificare.

Administrare Web

Dacă nu aţi făcut asta deja, expandaţi **Gestiune schema** în zona de navigare, apoi apăsaţi pe **Gestiune clase obiect**. Pentru a şterge o clasă de obiecte:

1. Apăsaţi butonul radio de lângă clasa de obiecte pe care vreţi să o ştergeţi.
2. Apăsaţi **Ştergere**.
3. Vi se va cere să confirmaţi ştergerea clasei de obiecte. Apăsaţi **OK** pentru a şterge clasa de obiecte sau apăsaţi **Anulare** pentru a reveni la **Gestiune clase de obiecte** fără a face vreo modificare.

Linie de comandă

Vizualizare clase de obiecte conţinute în schemă lansaţi comanda:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Selectaţi clasa de obiecte pe care vreţi să o ştergeţi şi lansaţi următoarea comandă:

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

unde <*filename*>conţine:

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: (<myobjectClass-oid>)
```

Vizualizarea atributelor

Puteţi vizualiza atributele din schemă folosind ori unealta de administrare web, metoda preferată sau folosind linia de comandă.

Administrare Web

Expandaţi **Gestiune schema** în zona de navigare şi apăsaţi pe **Gestiune atribute**. Este afişat un panou numai citire care vă permite să vedeţi atributele din schemă şi caracteristicile lor. Atributele sunt afişate în ordine alfabetică. Vă puteţi deplasa o pagină înapoi sau înainte apăsând pe Anterior sau Următor. Câmpul de lângă aceste butoane identifică pagina la care sunteţi. Puteţi de asemenea folosi meniul derulant al acestui câmp pentru a sări la o anumită pagină. Prima clasă de obiecte listată pe pagină este afişată cu numărul de pagină pentru a vă ajuta să localizaţi clasa de obiecte pe care vreţi să o vizualizaţi. De exemplu, dacă vreţi să căutaţi atributul **authenticationUserID**, expandaţi meniul derulant şi căutaţi în jos până vedeţi **Page 3 of 62 applSystemHint** şi **Page 4 of 62 authorityRevocatonList**. Deoarece authenticationUserID se află alfabetic între applSystemHint şi authorityRevocatonList, selectaţi Page 3 şi apăsaţi **start**.

Puteţi de asemenea afişa atributele sortate după sintaxă. Selectaţi **Sintaxă** şi apăsaţi **Sortare**. Atributele sunt sortate alfabetic în cadrul sintaxei lor. Vedeţi “Sintaxă atribut” la pagina 25 pentru o listă a tipurilor de sintaxă. Similar, puteţi inversa ordinea listei prin selectarea **Descendent** şi apăsarea pe **Sortare**.

După ce aţi localizat atributul dorit, puteţi să îi vedeţi sintaxa, dacă este multi-valoare şi clasa de obiecte care îl conţine. Expandaţi meniul derulant pentru clasele de obiect pentru a vedea lista de clase de obiect pentru atribut.

Când aţi terminat apăsaţi pe **Închidere** pentru a reveni la panoul IBM Directory Server **Welcome**.

Linie de comandă

Pentru a vedea atributele conţinute în schemă lansaţi comanda:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes
IBMAttributeTypes
```

Adăugarea unui atribut

Folosiţi una din următoarele metode pentru a crea un atribut. Unealta de administrare web este metoda preferată.

Administrare Web

Dacă nu aţi făcut asta deja, expandaţi **Gestiune schema** în zona de navigare, apoi apăsaţi pe **Gestiune atribute**. Pentru a crea un nou atribut:

1. Selectaţi **Adăugare**.

   Notă: De asemnea puteţi accesa acest panou prin expandara **Gestiune schemă** în zona de navigare, apoi apăsaţi pe **Adăugare atribut**.
2. Introduceţi **Nume atribut**, de exemplu, **tempId**. Acesta este un câmp obligatoriu şi trebuie să înceapă cu un caracter alfabetic.
3. Introduceţi o **Descriere** a atributului, de exemplu **Numărul ID asignat unui angajat temporar**.
4. Introduceţi **OID** pentru atribut. Acesta este un câmp obligatoriu. Vedeţi “Identificator obiect (OID)” la pagina 25. Dacă nu aveţi un OID, puteţi folosi numele atributului ataşat cu -oid. De exemplu, dacă numele atributului este **tempID**, atunci OIDul implicit este **tempID-oid**. Puteţi schimba valoarea acestui câmp.
5. Selectaţi o **Atribut superior** din lista derulantă. Atributul superior determină atributul din care sunt moştenite proprietăţile.
6. Selectaţi o **Sintaxă** din lista derulantă. Vedeţi “Sintaxă atribut” la pagina 25 pentru informaţii suplimentare despre sintaxă.
7. Introduceţi **Lungime atribut** care specifică lungimea maximă a acestui atribut. Lungimea este exprimată ca numărul de octeţi.

8. Selectaţi căsuţa de bifare **Permite valori multiple** pentru a permite ca atributul să aibă valori multiple.
9. Selectaţi o regulă corespunzătoare din fiecare din meniurile derulante pentru regulile de egalitate, ordonare şi asemănare subşir. Vedeţi “Reguli de potrivire” la pagina 23 pentru o listă completă de reguli de potrivire.
10. Apăsaţi pe fişa **Extensii IBM** pentru a specifica extensii suplimentare pentru atribut sau apăsaţi **OK** pentru a adăuga noul atribut sau apăsaţi **Anulare** pentru a reveni la **Gestiune atribute** fără a face vreo modificare.
11. În fişa **Extensii IBM**:
    - Modificaţi **numele tabelei DB2**. Serverul generează numele tabelei DB2 dacă acest câmp este lăsat gol. Dacă introduceţi un nume de tabelă DB2, trebuie de asemenea să introduceţi un nume coloană DB2.
    - Modificaţi **numele coloană DB2**. Serverul generează numele coloanei DB2 dacă acest câmp este lăsat gol. Dacă introduceţi un nume de coloană DB2, trebuie de asemenea să introduceţi un nume tabelă DB2.
    - Setaţi **Clasă de securitate** selectând **normal**, **sensibil** sau **critic** din lista derulantă.
    - Setaţi **Reguli de indexare** selectând una din următoarele reguli de indexare. Vedeţi “Reguli de indexare” la pagina 24 pentru informaţii suplimentare despre reguli de indexrare.

      Notă: Ca minim, este recomandabil să specificaţi Indexare de egalitate pe orice atribut care va fi folosit în filtrele de căutare.
12. Apăsaţi **OK** pentru a adăuga noua atribut sau apăsaţi **Anulare** pentru a reveni la **Gestiune atribute** fără a face vreo modificare.

Notă: Dacă aţi apăsat OK în fişa General fără a adăuga vreo extensie, puteţi adăuga extensii editând noul atribut.

Linie de comandă

Următorul exemplu adaugă o definiţie de tip de atribut pentru un atribut numit ″myAttribute″, cu sintaxa Directory String (vedeţi “Sintaxă atribut” la pagina 25) şi Case Ignore Equality matching (vedeţi “Reguli de potrivire” la pagina 23). Partea specifică IBM a definiţiei spune că datele atributului sunt stocate într-o coloană denumită ″myAttrColumn″ dintr-o tabelă denumită ″myAttrTable″. Dacă aceste nume nu erau specificate, numele coloanei şi tabelei ar fi avut valoarea implicită ″myAttribute″. Atributul este asignat clasei de acces ″normal″ şi valorile au o lungime maximă de 200 octeţi.

```
ldapmodify -D <admindn> -w <adminpw> -i myschema.ldif
```

unde fişierul **myschema.ldif** conţine:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' )
                  DESC 'An attribute I defined for my LDAP application'
                  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 )
```

Vedeţi “ldapmodify şi ldapadd” la pagina 159 pentru mai multe informaţii despre această comandă.

Editarea unui atribut

Nu sunt permise toate modificările de schemă. Vedeţi “Modificări de schemă nepermise” la pagina 28 pentru restricţii de modificare.

Orice parte a definiţiei poate fi modificată înainte să adăugaţi intrări care folosesc atributul. Folosiţi una din următoarele metode pentru a edita un atribut. Unealta de administrare web este metoda preferată.

Administrare Web

Dacă nu aţi făcut asta deja, expandaţi **Gestiune schema** în zona de navigare, apoi apăsaţi pe **Gestiune atribute**. Pentru a edita un atribut:

1. Apăsaţi butonul radio de lângă atributul pe care vreţi să o editaţi.
2. Apăsaţi **Editare** .
3. Selectaţi o fişă:
   - Folosiţi fişa **General** pentru:
     – Selectaţi o fişă:
       - **General** pentru a:
         - Modificaţi **Descriere**
         - Schimbaţi **Sintaxa**
         - Setaţi **Lungimea atributului**
         - Schimbaţi setările **Valori multiple**
         - Selectaţi o **Regulă de potrivire**
         - Schimbaţi **Atributul superior**
       - Apăsaţi pe fişa **Extensii IBM** pentru a edita extensii suplimentare pentru atribut sau apăsaţi **OK** pentru a aplica schimbările sau apăsaţi **Anulare** pentru a reveni la **Gestiune atribute** fără a face vreo modificare.
       - **Extensii IBM**, dacă folosiţi IBM Directory Server, pentru:
         - Modificaţi **Clasa de securitate**
         - Modificaţi **Regulile de indexare**
     – Apăsaţi **OK** pentru a aplica modificările sau apăsaţi **Anulare** pentru a reveni la **Gestiune atribute** fără a face vreo schimbare.
4. Apăsaţi **OK** pentru a aplica modificările sau apăsaţi **Anulare** pentru a reveni la **Gestiune atribute** fără a face vreo schimbare.

Linie de comandă

Acest exemplu adaugă indexarea atributului, astfel încât căutarea este mai rapidă. Folosiţi comanda ldapmodify şi fişierul LDIF pentru a modifica definiţia:

```
ldapmodify -D <admindn> -w <adminpw> -i myschemachange.ldif
```

unde fişierul **myschemachange.ldif** conţine:

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' ) DESC 'An attribute
                 I defined for my LDAP application' 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 )
```

Notă: Ambele porţiuni ale definiţiei (**attributetypes** şi **ibmattributetypes**) trebuie să fie incluse în operaţia de înlocuire, chiar dacă se modifică doar secţiunea **ibmattributetypes**. Singura modificare este adăugarea ″EQUALITY SUBSTR″ la sfârşitul definiţiei pentru a cere indexarea pentru potrivirea de egalitate şi de subşir.

Vedeţi “ldapmodify şi ldapadd” la pagina 159 pentru mai multe informaţii despre această comandă.

Copierea unui atribut

Folosiţi una din următoarele metode pentru a copia un atribut. Unealta de administrare web este metoda preferată.

Administrare Web

Dacă nu aţi făcut asta deja, expandaţi **Gestiune schema** în zona de navigare, apoi apăsaţi pe **Gestiune atribute**. Pentru a copia un atribut:

1. Apăsaţi butonul radio de lângă atributul pe care vreţi să îl copiaţi.
2. Apăsaţi **Copiere**.
3. Modificaţi **Nume atribut**. Numele implicit este numele atributului copiat ataşat cu cuvântul COPY. De exemplu, **tempID** este copiat ca **tempIDCOPY** .
4. Modificaţi o **Descriere** a atributului, de exemplu **Numărul ID asignat unui angajat temporar**.
5. Modificaţi **OID**. OID-ul implicit este OID-ul atributului copiat ataşat cu cuvântul COPYOID. De exemplu, **tempID-oid** este copiat ca **tempID-oidCOPYOID** .
6. Selectaţi o **Atribut superior** din lista derulantă. Atributul superior determină atributul din care sunt moştenite proprietăţile.
7. Selectaţi o **Sintaxă** din lista derulantă. Vedeţi “Sintaxă atribut” la pagina 25 pentru informaţii suplimentare despre sintaxă.
8. Introduceţi **Lungime atribut** care specifică lungimea maximă a acestui atribut. Lungimea este exprimată ca numărul de octeţi.
9. Selectaţi căsuţa de bifare **Permite valori multiple** pentru a permite ca atributul să aibă valori multiple.
10. Selectaţi o regulă corespunzătoare din fiecare din meniurile derulante pentru regulile de egalitate, ordonare şi asemănare subşir. Vedeţi “Reguli de potrivire” la pagina 23 pentru o listă completă de reguli de potrivire.
11. Apăsaţi pe fişa **Extensii IBM** pentru a modifica extensii suplimentare pentru atribut sau apăsaţi **OK** pentru a aplica schimbările sau apăsaţi **Anulare** pentru a reveni la **Gestiune atribute** fără a face vreo modificare.
12. În fişa **Extensii IBM**:
    - Modificaţi **numele tabelei DB2**. Serverul generează numele tabelei DB2 dacă acest câmp este lăsat gol. Dacă introduceţi un nume de tabelă DB2, trebuie de asemenea să introduceţi un nume coloană DB2.
    - Modificaţi **numele de coloană DB2**. Serverul generează numele coloanei DB2 dacă acest câmp este lăsat gol. Dacă introduceţi un nume de coloană DB2, trebuie de asemenea să introduceţi un nume tabelă DB2.
    - Modificaţi **Clasă de securitate** selectând **normal**, **sensibil** sau **critic** din lista derulantă.
    - Modificaţi **Reguli de indexare** selectând una din următoarele reguli de indexare. Vedeţi “Reguli de indexare” la pagina 24 pentru informaţii suplimentare despre reguli de indexrare.

      Notă: Ca minim, este recomandabil să specificaţi Indexare egală pe orice atribut care va fi folosit în filtrele de căutare.
13. Apăsaţi **OK** pentru a aplica modificările sau apăsaţi **Anulare** pentru a reveni la **Gestiune atribute** fără a face vreo schimbare.

Notă: Dacă aţi apăsat **OK** în fişa **General** fără a adăuga vreo extensie, puteţi adăuga extensii prin editarea noului atribut.

Linie de comandă

Vizualizare atribute conţinute în schemă lansaţi comanda:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes
IBMAttributeTypes
```

Selectaţi atributul pe care vreţi să o copiaţi. Folosiţi un editor pentru a schimba informaţiile corespunzătoare şi salvaţi modificările în <*filename*>. Apoi lansaţi următoarea comandă:

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

unde <*filename*>conţine:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( <mynewAttribute-oid> NAME
```

```
'<mynewAttribute>' DESC '<A
new
                attribute I copied for my LDAP application> 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 )
```

Ştergerea unui atribut

Nu sunt permise toate modificările de schemă. Vedeţi “Modificări de schemă nepermise” la pagina 28 pentru restricţii de modificare.

Folosiţi una din următoarele metode pentru a şterge un atribut. Unealta de administrare web este metoda preferată.

Administrare Web

Dacă nu aţi făcut asta deja, expandaţi **Gestiune schema** în zona de navigare, apoi apăsaţi pe **Gestiune atribute**. Pentru a şterge un atribut:

1. Apăsaţi butonul radio de lângă atributul pe care vreţi să îl ştergeţi.
2. Apăsaţi **Ştergere**.
3. Vi se va cere să confirmaţi ştergerea atributului. Apăsaţi **OK** pentru a şterge atributul sau apăsaţi **Anulare** pentru a reveni la **Gestiune atribute** fără a face vreo schimbare.

Linie de comandă

```
ldapmodify -D <admindn> -w <adminpw> -i myschemadelete.ldif
```

unde fişierul **myschemadelete.ldif** include:

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

Vedeţi “ldapmodify şi ldapadd” la pagina 159 pentru mai multe informaţii despre această comandă.

Copierea schemei la alte servere

Pentru a copia o schemă la alte servere faceţi următoarele:

1. Folosiţi utilitarul ldapsearch pentru a copia schema într-un fişier:

   ```
   ldapsearch -b cn=schema -L "(objectclass=*)" > schema.ldif
   ```

2. Fişierul schemă va include toate objectclasses şi atributele. Editaţi fişierul LDIF pentru a include doar elementele de schemă pe care le vreţi sau veţi putea filtra ieşirea ldapsearch folosind o comandă precum grep. Asiguraţi-vă că aţi pus atributele înainte de objectclasses care le referă. De exemplu, aţi putea ajunge cu următorul fişier (ţineţi cont că fiecare linie continuată are un singur spaţiu la sfârşit şi linia de continuare are cel puţin un spaţiu la început).

   ```
   attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Some piece of
     information.' 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 'Some piece of
     information.' 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 'Represents
     something.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
   ```

3. Inseraţi linii înaintea fiecărei linii objectclasses sau attributetype pentru a construi directive LDIF pentru a adăuga aceste valori la intrarea cn=schema. Fiecare clasă de obiect şi atribut trebuie să fie adăugat ca o modificare individuală.

```
dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Some piece of
  information.' 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 'Some piece of
  information.' 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 'Represents
  something.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

4. Încărcaţi acea schemă pe alte servere folosind utilitarul ldapmodify:

```
ldapmodify -D cn=administrator -w <password> -f schema.ldif
```

Gestionarea intrărilor în director

Pentru a gestiona intrările director, expandaţi categoria **Gestiune director** din zona de navigare a uneltei de administrare web.

Vedeţi următoarele pentru informaţii suplimentare:

- “Răsfoirea arborelui”
- “Adăugarea unei intrări”
- “Ştergerea unei intrări” la pagina 132
- “Editarea unei intrări” la pagina 132
- “Copierea unei intrări” la pagina 133
- “Editarea listelor de control al accesului” la pagina 133
- “Adăugarea unei clase de obiect auxiliare” la pagina 133
- “Ştergerea unei clase auxiliare” la pagina 134
- “Modificarea apartenenţei la grup” la pagina 134
- “Căutarea intrărilor de director” la pagina 134
- “Modificarea atributelor binare” la pagina 136

Răsfoirea arborelui

Dacă nu aţi făcut asta deja, expandaţi categoria **Gestiune director** din zona de navigare, apoi apăsaţi pe **Gestiune intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea cu care vreţi să lucraţi. Puteţi alege operaţia pe care vreţi să o efectuaţi din bara de unelte din ăartea dreaptă.

Adăugarea unei intrări

Dacă nu aţi făcut asta deja, expandaţi categoria **Gestiune director** din zona de navigare.

1. Apăsaţi **Adăugare intrare**.

2. Selectaţi o **Clasă structurală de obiecte** din lista derulantă.
3. Apăsaţi **Continuare**.
4. Selectaţi orice **Clase de obiecte auxiliare** pe care vreţi să le folosiţi din căsuţa Disponibile şi apăsaţi **Adăugare**. Repetaţi acest proces pentru fiecare clasă de obiecte auxiliare pe care vreţi să o adăugaţi. Puteţi de asemenea şterge o clasă de obiecte auxiliară din căsuţa Selectate prin selectarea ei şi apăsarea pe **Ştergere**.
5. Apăsaţi **Continuare**.
6. În câmpul **DN relativ**, introduceţi DN-ul relativ (RDN) al intrării pe care o adăugaţi, de exemplu, cn=John Doe.
7. În câmpul **DN părinte**, introduceţi numele distinctiv al intrării arbore pe care aţi selectat-o, de exemplu ou=Austin, o=IBM. Puteţi de asemenea să apăsaţi pe **Răsfoire** pentru a selecta DN-ul părinte din listă. Puteţi de asemenea expanda selecţia pentru a vedea alte alegeri de mai jos din subarbore. Specificaţi alegerea dvs. şi apăsaţi **Selectare** pentru a specifica DN-ul părinte pe care îl vreţi. **DN-ul părinte** are valoare implicită intrarea selectată în arbore.

   Notă: Dacă aţi pornit acest task din panoul **Gestiune intrări**, acest câmp este precompletat. Aţi selectat **DN părinte** înainte de a apăsa **Adăugare** pentru a porni procesul de adăugare intrare.
8. În fişa **Atribute obligatorii** introduceţi valorile pentru atributele obligatorii. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
9. Apăsaţi **Atribute opţionale**.
10. În fişa **Atribute opţionale** introduceţi valorile corespunzătoare pentru atributele opţionale. Vedeţi “Modificarea atributelor binare” la pagina 136 pentru informaţii despre adăugarea valorilor binare. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
11. Apăsaţi OK pentru a crea intrarea.
12. Apăsaţi butonul **ACL** pentru a modifica lista de control acces pentru această intrare. Vedeţi “Liste de control al accesului” la pagina 48 pentru informaţii despre ACL-uri.
13. După ce aţi completat cel puţin câmpurile obligatorii, apăsaţi **Adăugare** pentru a adăuga noua intrare sau apăsaţi **Anulare** pentru a reveni la **Răsfoire arbore** fără a face vreo modificare la director.

Ştergerea unei intrări

Dacă nu aţi făcut asta deja, expandaţi categoria **Gestiune director** din zona de navigare, apoi apăsaţi pe **Gestiune intrări**. Puteţi expanda diverşi subarbori şi selecta subarborele, sufixul sau intrarea cu care vreţi să lucraţi. Apăsaţi **Şterge** din bara de unelte din partea dreaptă.

- Vi se va cere să confirmaţi ştergerea. Selectaţi **OK**.
- Intrarea este ştearsă din intrare şi dvs. sunteţi întors la lista de intrări.

Editarea unei intrări

Dacă nu aţi făcut asta deja, expandaţi categoria **Gestiune director** din zona de navigare, apoi apăsaţi pe **Gestiune intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea cu care vreţi să lucraţi. Apăsaţi **Editare atribute** din bara de unelte din partea dreaptă.

1. În fişa **Atribute obligatorii** introduceţi valorile pentru atributele obligatorii. Vedeţi “Modificarea atributelor binare” la pagina 136 pentru informaţii despre adăugarea valorilor binare. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
2. Apăsaţi **Atribute opţionale**.
3. În fişa **Atribute opţionale** introduceţi valorile corespunzătoare pentru atributele opţionale. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
4. Apăsaţi **Apartenenţă**.
5. Dacă aţi creat vreun grup, la fişa **Apartenenţă**:
   - Selectaţi un grup din **Grupuri disponibile** şi faceţi clic pe **Adăugare** pentru a face intrare un membru al **Apartenenţă grup static** selectat.
   - Selectaţi un grup din **Apartenenţe grup spatic** şi faceţi clic pe **Înlăturare** pentru a înlătura intrarea din grupul selectat.

6. Dacă intrarea este o intrare grup, o fişă **Membri** este disponibilă. Fişa **Membri** afişează membrii grupului selectat. Puteţi adăuga şi înlătura membrii din grup.
   - Pentru a adăuga un membru la grup:
     a. Fie faceţi clic pe **Valori multiple** din fişa **Membri** sau la fişa **Membri**, faceţi clic pe **Membri**.
     b. În câmpul Membru, introduceţi DN-ul intrării pe care doriţi să o adăugaţi.
     c. Selectaţi **Adăugare**.
     d. Selectaţi **OK**.
   - Pentru a înlătura un membru din grup:
     a. Fie faceţi clic pe **Valori multiple** din fişa **Membri** sau la fişa **Membri**, faceţi clic pe **Membri**.
     b. Selectaţi intrarea pe care doriţi să o înlăturaţi:
     c. Apăsaţi **Înlăturare**.
     d. Selectaţi **OK**.
   - Pentru a reîmprospăta lista de membri, faceţi clic pe **Actualizare**.
7. Faceţi clic pe **OK** pentru a modifica intrarea.

Copierea unei intrări

Această funcţie este de ajutor în cazul în care creaţi intrări similare. Copia moşteneşte toate atributele originalului. Trebuie să faceţi unele modificări la numele noii intrări.

Dacă nu aţi făcut asta deja, expandaţi categoria **Gestiune director** din zona de navigare, apoi apăsaţi pe **Gestiune intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea, precum John Doe, cu care vreţi să lucraţi. Apăsaţi **Copiere** din bara de unelte din partea dreaptă.

- Modificaţi intrarea RDN din câmpul DN. De exemplu modificaţi cn=John Doe cu cn=Jim Smith.
- În fişa de atribute necesară, modificaţi intrarea cn la noua RDN. În acest exemplu Jim Smith.
- Modificaţi corespunzător celelalte atribute necesare. În acest exemplu modificaţi atributul sn de la Doe la Smith.
- Când aţi terminat de modificat faceţi clic pe **OK** pentru a crea noua intrare.
- Noua intrare Jim Smith este adăugată în josul listei de intrare.

Notă: Această procedură copie doar atributele intrării. Apartenenţele grup ale intrării originale nu sunt copiate la intrarea nouă. Folosiţi funcţia de atribute Editare pentru a adăuga apartenenţă.

Editarea listelor de control al accesului

Pentru a vedea proprietăţile ACL folosind unealta de administrare Web şi să lucraţi cu ACL-uri, vedeţi “Gestionarea listelor de control al accesului (ACL-uri)” la pagina 147.

Vedeţi “Liste de control al accesului” la pagina 48 pentru informaţii suplimentare.

Adăugarea unei clase de obiect auxiliare

Folosiţi butonul **Adăugare clasă auxiliară** din bara de unelte pentru a adăuga o clasă obiect auxiliar unei intrări existente din arborele director. O clasă obiect auxiliar furnizează atribute suplimentare intrării la care este adăugată.

Dacă nu aţi făcut asta deja, expandaţi categoria **Gestiune director** din zona de navigare, apoi apăsaţi pe **Gestiune intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea, precum John Doe, cu care vreţi să lucraţi. Apăsaţi **Adăugare clasă auxiliară** din bara de unelte din partea dreaptă.

1. Selectaţi orice **Clase de obiecte auxiliare** pe care vreţi să le folosiţi din căsuţa Disponibile şi apăsaţi **Adăugare**. Repetaţi acest proces pentru fiecare clasă de obiecte auxiliare pe care vreţi să o adăugaţi. Puteţi de asemenea şterge o clasă de obiecte auxiliară din căsuţa Selectate prin selectarea ei şi apăsarea pe **Ştergere**.
2. În fişa **Atribute obligatorii** introduceţi valorile pentru atributele obligatorii. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.

3. Apăsaţi **Atribute opţionale**.
4. În fişa **Atribute opţionale** introduceţi valorile corespunzătoare pentru atributele opţionale. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
5. Apăsaţi **Apartenenţă**.
6. Dacă aţi creat vreun grup, la fişa **Apartenenţă**:
   - Selectaţi un grup din **Grupuri disponibile** şi faceţi clic pe **Adăugare** pentru a face intrare un membru al **Apartenenţă grup static** selectat.
   - Selectaţi un grup din **Apartenenţe grup spatic** şi faceţi clic pe **Înlăturare** pentru a înlătura intrarea din grupul selectat.
7. Faceţi clic pe **OK** pentru a modifica intrarea.

Ştergerea unei clase auxiliare

Deşi puteţi şterge o clasă auxiliară în timpul procedurii de adăugare de clasă auxiliară, este mai uşor să folosiţi funcţia de şterge clasă auxiliară dacă doriţi să ştergeţi o singură clasă auxiliară dintr-o intrare. Oricum, poate fi mai convenabil să folosiţi procedusa de adăugare clasă auxiliară dacă doriţi să ştergeţi mai multe clase auxiliare din intrare.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestiune director** din zona de navigare, apoi apăsaţi pe **Gestiune intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea, precum John Doe, cu care vreţi să lucraţi. Apăsaţi **Ştergere clasă auxiliară** din bara de unelte din partea dreaptă.
2. Din lista de clase auxiliare, selectaţi pe cea care doriţi să o ştergeţi şi apăsaţi **OK**.
3. Vi se cere să confirmaţi ştergerea, apăsaţi **OK**.
4. Clasa auxiliară este ştearsă din intrare şi dvs. sunteţi întors la lista de intrări.

Repetaţi aceşti paşi pentru fiecare clasă auxiliară pe care doriţi să o ştergeţi.

Modificarea apartenenţei la grup

Dacă nu aţi făcut asta deja, expandaţi categoria **Gestiune director** din zona de navigare.

1. Apăsaţi **Gestiune intrări**.
2. Selectaţi un utilizator din arborele director şi apăsaţi pe pictograma **Editare atribute** din bara de unelte. arbore.
3. Faceţi clic pe fişa **Apartenenţe**.
4. Pentru a modifica apartenenţele pentru utilizator. Panoul **Modificare apartenenţe** afişează **Grupuri disponibile** în care pot fi adăugaţi utilizatori, la fel ca şi **Apartenenţele grup static** ale intrării.
   - Selectaţi un grup din **Grupuri disponibile** şi faceţi clic pe **Adăugare** pentru a face intrarea un membru al grupului selectat.
   - Selectaţi un grup din **Apartenenţe grup static** şi faceţi clic pe **Înlăturare** pentru a înlătura intrarea din grupul selectat.
5. Apăsaţi **OK** penru a salva modificările dvs sau apăsaţi **Anulare** pentru a vă întoarce în panoul anterior fără să salvaţi modificările.

Căutarea intrărilor de director

Există 3 opţiuni pentru căutarea arborelui director:

- O căutare simplă folosind un set predefinit de criterii de căutare:
- O căutare avansată folosind un set definit de utilizator de criterii de căutare.
- O căutare manuală

Opţiunile de căutare sunt disponibile expandând categoria **Gestiune directoare** din zona de navigare, apăsaţi **Căutare intrări**. Selectaţi fie fişa **Căutare filtre**, fie **Opţiuni**.

Notă: Intrările binare, de exemplu parole, nu sunt căutabile.

Filtre de căutare

Selectaţi unul din următoarele tipuri de căutare:

Căutare simplă

O căutare simplă foloseşte un criteriu de căutare implicit:

- DN-ul de bază este **All suffixes**
- Domeniul de căutare este **Subtree**
- Dimensiunea căutarii este **Unlimited**
- Limita de timp este **Unlimited**
- Dereferenţierea de alias este **never**
- Referalii de urmărire sunt deselectaţi (off)

Pentru a executa o căutare simplă:

1. În fişa **Filtru de căutare**, apăsaţi **Căutare simplă**.
2. Selectaţi unele clase obiect din lista derulantă.
3. Selectaţi un atribut specific pentru tipul de intrare selectat. Dacă alegeţi să căutaţi un atribut specific, selectaţi un atribut din lista derulantă şi intrpoduceţi valoarea atributului în caseta **Este egal cu**. Dacă nu specificaţi un atribut, căutarea întoarce toate intrările director ale tipului intrării selectate.

Căutare avansată

O căutare avansată vă permite să specificaţi restricţii de căutare şi să activaţi filtre de căutare. Folosiţi ccăutarea simplă pentru a folosi criterii de căutare implicite.

- Pentru a executa o căutare avansată:
  1. În fişa **Filtru de căutare**, apăsaţi **Căutare avansată**.
  2. Selectaţi un **Atribut** din lista derulantă.
  3. Selectaţi un operator **Comparaţie**
     - Atributul este egal cu valoarea.
     - ! Atributul nu este egal cu valoarea.
     - < Atributul este mai mic sau egal cu valoarea.
     - > Atributul este mai mare sau egal cu valoarea.
     - ~ Atributul este aproximativ egal cu valoarea.
  4. Introduceţi **Valoare** pentru comparaţie.
  5. Folosiţi butoanele de operare căutare pentru interogări complexe.
     - Dacă aţi adăugat deja un filtru de căutare, specificaţi criteriile suplimentare şi apăsaţi **AND**. Comanda **AND** întoarce intrările care se potrivesc cu ambele seturi de criterii de căutare.
     - Dacă aţi adăugat deja un filtru de căutare, specificaţi criteriile suplimentare şi apăsaţi **OR**. Comanda **OR** întoarce intrările care se potrivesc cu unul din seturile de criterii de căutare.
  6.
     - Apăsaţi pe **Adăugare** pentru a adăuga criteriile de filtru de căutare la căutare avansată.
     - Apăsaţi pe **Ştergere** pentru a şterge criteriile de filtru de căutare la căutare avansată.
     - Faceţi clic pe **Reset** pentru a curăţa toate filtrele de căutare.

Căutare manuală

Folosiţi această metodă pentru a crea un filtru de căutare. De exemplu pentru a căuta nume de familie introduceţi sn=* în câmp. În cazul în care căutaţi atribute multiple, folosiţi sintaxa filtrului de căutare: De exemplu, pentru a căuta numele de familie al unui anumit departament, introduceţi:

```
(&(sn=*)(dept=<numedepartament>))
```

Opţiuni

La **fişa Opţiuni**:

- **Căutare DN de bază** - Selectaţi sufixul din lista derulantă pentru a căuta doar în acel sufix.

  Notă: Dacă aţi pornit acest task din panoul **Gestiune intrări**, acest câmp este precompletat. Aţi selectat **DN părinte** înainte de a apăsa **Adăugare** pentru a porni procesul de adăugare intrare.

  Puteţi de asemenea **Toate sufixele** pentru a căuta întregul arbore.
- **Domeniu de căutare**
  - Selectaţi **Obiect** pentru a căuta doar în obiectul selectat.
  - Selectaţi **Nivel singular** pentru a căuta doar în copilul imediat al obiectului selectat.
  - Selectaţi **Subarbore** pentru a căuta toţi descendenţii intrării curente selectate.
- **Limită dimensiune căutare** - Introduceţi numărul maxim de intrări de căutare sau selectaţi **Nelimitat**.
- **Limită timp căutare** - Introduceţi numărul maxim de secunde pentru căutare sau selectaţi **Nelimitat**.
- Selectaţi un tip de **Dereferenţiere alias** din lista derulantă.
  - **Niciodată** - Dacă intrarea selectată este un alias, nu este dereferenţiată pentru căutare, adică căutarea ignoră referinţa la alias.
  - **Găsire** - Dacă intrarea selectată este un alias, căutarea dereferenţiază aliasul şi caută din locaţia aliasului.
  - **Căutare** - Intrarea selectată nu este dereferenţiată, dar orice intrare găsită în căutare este dereferenţiată.
  - **Mereu** - Toate aliasurile întâlnite în căutare sunt dereferenţiate.
- Selectaţi caseta de bifare **Urmare referali** pentru a urma referalii la un alt server, dacă este întors un referal la căutare. Când un referal directează căutarea la un alt server, conexiunea cu serverul foloseşte acreditările curente. Dacă sunteţi logat ca Anonymous aţi putea avea nevoie să vă înregistraţi pe server folosind un DN autentificat.

Vedeţi “Ajustarea setărilor de căutare” la pagina 102 pentru informaţii suplimentare despre căutări.

Modificarea atributelor binare

Dacă un atribut necesită date binare, un buton **Date binare** este afişat lângă câmpul atribut. Dacă atributul nu are date, câmpul este gol. Deoarece atributele binare nu pot fi afişate, dacă un atribut conţine date binare, câmpul afişează **Date binare - 1**. Dacă atributul conţine valori multiple, câmpul este afişat ca listă derulantă.

Faceţi clic pe butonul **Date binare** pentru a lucra cu atribute binare.

Puteţi importa, exporta sau şterge date binare.

Pentru a adăuga date binare la atribut:

1. Faceţi clic pe butonul **Date binare**.
2. Faceţi clic pe **Importare**.
3. Puteţi fie să introduceţi numele cale pentru fişierul pe care doriţi fie să faceţi clic pe **Răsfoire** pentru a localiza şi selecta fişierul binar.
4. Faceţi clic pe **Lansare fişier**. Este afişat un mesaj Fişier încărcat.
5. Clic **Închidere**. **Date binare - 1** este acum afişat sunt **Intrări date binare**.
6. Repetaţi procesul de importare pentru atâtea fişiere binare câte doriţi să adăugaţi. Intrările următoare sunt tipărite ca **Date binare - 2**, **Date binare -3** şamd.
7. Când terminaţi adăugarea de date binare, apăsaţi **OK**.

Pentru a exporta date binare:

1. Faceţi clic pe butonul **Date binare**.
2. Faceţi clic pe **Exportare**.
3. Faceţi clic pe pe legătura **Date binare de descărcat**.

4. Urmaţi direcţiile vrăjitorului dvs fie ca să afişaţi fişierul binar fie să îl salvaţi într-o locaţie nouă.
5. Clic **Închidere**.
6. Repetaţi procesul de importare pentru atâtea fişiere binare câte doriţi să exportaţi.
7. Când terminaţi exportarea de date binare, apăsaţi **OK**.

Pentru a şterge date binare:

1. Faceţi clic pe butonul **Date binare**.
2. Verificaţi fişierul de date binare pe care doriţi să îl ştergeţi. Pot fi selectate fişiere multiple.
3. Apăsaţi **Ştergere**.
4. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**. Datele binare marcate pentru ştergere sunt înlăturare din listă.
5. Când terminaţi ştergerea datelor, apăsaţi **OK**.

Notă: Atributele binare nu sunt căutabile.

Gestionarea utilizatorilor şi grupurilor

Pentru a gestiona utilizatori şi grupuri, expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

Vedeţi următoarele pentru informaţii suplimentare:

- “Gestionarea utilizatorilor”
- “Gestionare grupuri” la pagina 138

Gestionarea utilizatorilor

După ce aţi setat regiunile şi şabloanele dvs, le puteţi popula cu utilizatori. Vedeţi următoarele:

- “Adăugarea de utilizatori”
- “Găsirea de utilizatori în regiune”
- “Editarea informaţiilor unui utilizator” la pagina 138
- “Copierea unui utilizator” la pagina 138
- “Înlăturarea unui utilizator” la pagina 138

Adăugarea de utilizatori

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Adăugare utilizator** sau faceţi clic pe **Gestionare utilizatori** şi faceţi clic pe **Adăugare**.
2. Selectaţi regiunea în care doriţi să adăugaţi utilizatorul din meniul derulant.
3. Apăsaţi **Continuare**. Este afişat şablonul care este asociat cu regiunea. Completaţi câmpurile necesare, notate cu un asterisc (*) şi oricare alte câmpuri de pe fişe. Dacă aţi creat deja grupuri în regiune, puteţi de asemenea să adăugaţi utilizatorul în unul sau mai multe grupuri.
4. Când aţi terminat, faceţi clic pe **Sfârşit**.

Găsirea de utilizatori în regiune

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Găsire utilizator** sau faceţi clic pe **Gestionare utilizatori** şi faceţi clic pe **Găsire**.
2. Selectaţi regiunea în care doriţi să căutaţi din câmpul **Selectare regiune**.
3. Introdceţi şirul de căutare în câmpul **Numire atribute**. Sunt suportate caractere de înlocuire, de exemplu, dacă aţi introdus ***smith** , rezultatul sunt toate căutările care au atributul de numire terminându-se cu smith.
4. Puteţi realiza următoarele operaţii pe un utilizator selectat:
   - **Editare** - Vedeţi “Editarea informaţiilor unui utilizator” la pagina 138.
   - **Copiere** - Vedeţi “Copierea unui utilizator” la pagina 138.

- **Şteregere** - Vedeţi “Înlăturarea unui utilizator”.

5. Când terminaţi faceţi clic pe **OK**.

Editarea informaţiilor unui utilizator

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Gestionare utilizatori**.
2. Selectaţi o regiune din meniul derulant. Faceţi clic pe **Vizualizare utilizatori**, dacă utilizatorii nu sunt afişaţi deja în caseta **Utilizatori**.
3. Selecatţi utilizatorul pe care doriţi să-l editaţi şi faceţi clic pe **Editare**.
4. Modificaţi informaţiile de pe fişe, modificaţi apartenenţa grupului.
5. Când terminaţi faceţi clic pe **OK**.

Copierea unui utilizator

Daca trebuie să creaţi un număr de utilizatori care au informaţii aproape identice, puteţi crea utilizatori suplimentari prin copierea utilizatorului iniţial şi prin modificarea informaţiilor.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Gestionare utilizatori**.
2. Selectaţi o regiune din meniul derulant. Faceţi clic pe **Vizualizare utilizatori**, dacă utilizatorii nu sunt afişaţi deja în caseta **Utilizatori**.
3. Selectaţi utilizatorul pe care doriţi să-l copiaţi şi faceţi clic pe **Copiere**.
4. Modificaţi informaţiile corespunzătoare pentru utilizatorul nou, de exemplu, informaţiile necesare care identifică un anumit utilizator, precum sn sau cn. Nu trebuie modificate informaţiile care sunt comune ambilor utilizatori.
5. Când terminaţi faceţi clic pe **OK**.

Înlăturarea unui utilizator

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Gestionare utilizatori**.
2. Selectaţi o regiune din meniul derulant. Faceţi clic pe **Vizualizare utilizatori**, dacă utilizatorii nu sunt afişaţi deja în caseta **Utilizatori**.
3. Selecatţi utilizatorul pe care doriţi să-l înlăturaţi faceţi clic pe **Ştergere**.
4. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**.
5. Utilizatorul este înlăturat din lista de utilizatori.

Gestionare grupuri

După ce aţi setat regiunile şi şabloanele dvs, puteţi crea grupuri. Vedeţi următoarele:

- “Adăugarea de grupuri”
- “Găsirea grupurilor în regiune” la pagina 139
- “Editarea informaţiilor unui grup” la pagina 139
- “Copierea unui grup” la pagina 139
- “Înlăturarea unui grup” la pagina 139

Adăugarea de grupuri

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Adăugare grup** sau faceţi clic pe **Gestionare grupuri** şi faceţi clic pe **Adăugare**.
2. Introduceţi numele grupului pe care doriţi să-l creaţi.
3. Selectaţi regiunea în care doriţi să adăugaţi utilizatorul din meniul derulant.
4. Faceţi clic pe **Sfârşit** pentru a crea grupul. Dacă aveţi deja utilizatori în regiune puteţi apăsa clic pe **Următorul** şi selectaţi utilizatorii de adăugat la grup. Apoi faceţi clic pe **Sfârşit**.

Vedeţi “Grupuri şi roluri” la pagina 42 pentru informaţii suplimentare.

Găsirea grupurilor în regiune

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Găsire grup** sau faceţi clic pe **Gestionare grupuri** şi faceţi clic pe **Găsire**.
2. Selectaţi regiunea în care doriţi să căutaţi din câmpul **Selectare regiune**.
3. Introdceţi şirul de căutare în câmpul **Numire atribute**. Sunt suportate wildcards, de exemplu, dacă aţi introdus ***club** , rezultatul sunt toate grupurile care au atributul de numire club, de exemplu, Club carte, club şah, club grădină şamd.
4. Puteţi realiza următoarele operaţii pe un utilizator selectat:
   - **Editare** - Vedeţi “Editarea informaţiilor unui grup”.
   - **Copiere** - Vedeţi “Copierea unui grup”.
   - **Ştergere** - Vedeţi “Înlăturarea unui grup”.
5. Când aţi terminat, faceţi clic pe **Sfârşit**.

Editarea informaţiilor unui grup

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Gestiune grupuri**.
2. Selectaţi o regiune din meniul derulant. Faceţi clic pe **Vizualizare grupuri**, dacă utilizatorii nu sunt afişaţi deja în caseta **Grupuri**.
3. Selectaţi grupul pe care doriţi să-l editaţi şi faceţi clic pe **Editare**.
4. Puteţi apăsa clic pe **Filtru** pentru a limita numărul de **Utilizatori disponibili**. De exemplu, introducând *smith în ultimul câmp nume, limitaţi utilizatorii disponibili la cei a căror nume se termină cu smith precum Ann Smith, Bob Smith, Joe Goldsmith, şamd.
5. Puteţi adăuga şi înlătura membrii din grup.
6. Când terminaţi faceţi clic pe **OK**.

Copierea unui grup

Daca trebuie să creaţi un număr de grupuri care au în general aceeaşi membri, puteţi crea grupuri suplimentari prin copierea grupului iniţial şi prin modificarea informaţiilor.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Gestiune grupuri**.
2. Selectaţi o regiune din meniul derulant. Faceţi clic pe **Vizualizare grupuri**, dacă grupurile nu sunt afişaţe deja în caseta **Grupuri**.
3. Selectaţi grupul pe care doriţi să-l copiaţi şi faceţi clic pe **Copiere**.
4. Modificaţi numele grupului din câmpul **Nume grup**. Noul grup are aceeaşi membri cu cel original.
5. Puteţi modifica membrii grupului.
6. Când terminaţi faceţi clic pe **OK**. Noul grup este creat şi conţine aceeaşi membri cu cel original împreună cu orice adăugare sau modificare pe care aţi făcut-o în timpul procedurii de copiere.

Înlăturarea unui grup

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Gestiune grupuri**.
2. Selectaţi o regiune din meniul derulant. Faceţi clic pe **Vizualizare grupuri**, dacă utilizatorii nu sunt afişaţi deja în caseta **Grupuri**.
3. Selectaţi grupul pe care doriţi să-l înlăturaţi faceţi clic pe **Ştergere**.
4. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**.
5. Grupul este înlăturat din lista de utilizatori.

Regiuni şi şabloane utilizator

Pentru a gestiona regiuni şi şabloane utilizator faceţi clic pe **Regiuni şi şabloane utilizator** din zone de navigare a uneltei de administrare Web. Folosiţi regiuni şi şabloane utilizator pentru a le uşura altora introducerea de date în director. Pentru informaţii suplimentare despre conceptele de şablon, vedeţi"Regiuni şi şabloane utilizator" la pagina 39.

Vedeţi următoarele pentru informaţii suplimentare:

- "Crearea unei regiuni"
- "Crearea unui administrator de regiune"
- "Crearea unui şablon" la pagina 141
- "Adăugarea şablonului la o regiune" la pagina 143
- "Crearea de grupuri" la pagina 143
- "Adăugarea unui utilizator la regiune" la pagina 143
- "Gestionarea regiunilor" la pagina 143
- "Gestionarea şabloanelor" la pagina 144

Crearea unei regiuni

Pentru informaţii suplimentare despre conceptele de şablon, vedeţi"Regiuni şi şabloane utilizator" la pagina 39.

Pentru a crea o regiune, faceţi următoarele:

1. Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.
2. Faceţi clic pe **Adăugare regiune**.
   - Introduceţi numele pentru regiune. De exemplu **realm1**.
   - Introduceţi DN-ul părinte care identifică locaţia regiunii. Acesată intrare este forma sufixului, de exemplu o=ibm,c=us. Această intrare poate fi un sufix sau o intrare în altă parte a directorului. Puteţi de asemenea să apăsaţi pe **Răsfoire** pentru a selecta locaţia subarborelui pe care îl douiţi.
3. Faceţi clic pe **Următorul** pentru a continua sau faceţi clic pe **Sfârşit**.
4. Dacă aţi apăsat clic pe **Următorul**, revedeţi informaţiile. În acest moment nu aţi creat efectiv regiunea, deci **Şablon utilizator** şi **Filtru căutare utilizator** pot fi ignorate.
5. Faceţi clic pe **Sfârşit** pentru a crea regiunea.

Crearea unui administrator de regiune

Pentru a crea un administrator de regiune, trebuie mai întâi să creaţi un grup de administrare pentru regiune făcând următoarele:

1. Creaţi grupul de administrare regiune.
   a. Expandaţi categoria **Gestiune director** din zona de navigare a uneltei de administrare web.
   b. Apăsaţi **Gestiune intrări**.
   c. Expandaţi arborele şi selectaţi regiunea pe care tocmai aţi creat-o, **cn=realm1,o=ibm,c=us**.
   d. Faceţi clic pe **Editare ACL**.
   e. Faceţi clic pe fişa **Proprietari**.
   f. Asiguraţi-vă că este bifat **Propagare proprietar**.
   g. Introduceţi DN-ul pentru regiune, **cn=realm1,o=ibm,c=us**.
   h. Modificaţi **Tipul** la grup.
   i. Selectaţi **Adăugare**.
2. Creaţi intrarea administrator. Dacă nu aveţi deja o intrare utilizator pentru administrator, trebuie să creaţi una.
   a. Expandaţi categoria **Gestiune director** din zona de navigare a uneltei de administrare web.
   b. Apăsaţi **Gestiune intrări**.

c. Expandaţi arborele la locaţia unde doriţo să se afle intrarea administrator.

   Notă: Localizarea intrării administrator în afara regiunii evită acordarea administratorului abilitatea de a se şterge accidental. În acest exemplu locaţia poate fi **o=ibm,c=us** .

d. Selectaţi **Adăugare**.
e. Selectaţi **Clasa obiect structurală**, de exemplu **inetOrgPerson**.
f. Apăsaţi **Continuare**.
g. Selectaţi price clasă obiect auxiliară pe care doriţi să o adăugaţi.
h. Apăsaţi **Continuare**.
i. Introduceţi atributele necesare pentru intrare. De exemplu,
   - **RDN** cn=JohnDoe
   - **DN** o=ibm,c=us
   - **cn** John Doe
   - **sn** Doe
j. Pe fişa **Alte atribute** asiguraţi-vă că aţi alocat o parolă.
k. Când aţi terminat, faceţi clic pe **Sfârşit**.

3. Adăugaţi administratorul în grupul de administrare.
   a. Expandaţi categoria **Gestiune director** din zona de navigare a uneltei de administrare web.
   b. Apăsaţi **Gestiune intrări**.
   c. Expandaţi arborele şi selectaţi regiunea pe care tocmai aţi creat-o, **cn=realm1,o=ibm,c=us**.
   d. Apăsaţi **Editare atribute**.
   e. Faceţi clic pe fişa **Membri**.
   f. Apăsaţi **Membri**.
   g. În câmpul **Membri** introduceţi DN-ul administratorului, în acest exmplu **cn=John Doe,o=ibm,c=us**.
   h. Selectaţi **Adăugare**. DN-ul este afişat în lista **Membri**.
   i. Selectaţi **OK**.
   j. Faceţi clic pe **Actualizare**. DN-ul este afişat în lista **Membri actuali**.
   k. Selectaţi **OK**.
4. Aţi creat un administrator care poate gestiona intrări din regiune.

Crearea unui şablon

După ce aţi creat o regiune, următorul pas este să creaţi un şablon utilizator. Un şablon vă ajută să organizaţi informaţiile pe care doriţi să le introduceţi. Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Adăugare şablon utilizator**.
   - Introduceţi numele pentru şablon, de exemplu, **şablon1** .
   - Introduceţi locaţia unde se va afla şablonul. Pentru scopuri de replicare, localizaţi şablonul în subarborele regiunii care va folosi acest şablon. De exemplu, regiunea creată în operaţiile anterioare **cn=realm1,o=ibm,c=us**. De asemenea puteţi apăsa pe **Răsfoire** pentru a to selecta un alt subarbore pentru locaţia şablonului.
2. Apăsaţi **Continuare**. Puteţi apăsa pe **Sfârşit** pentru a crea un nou şablon gol. Puteţi să adăugaţi mai târziu informaţii la şablon, vedeţi “Editarea unui şablon” la pagina 146.
3. Dacă aţi apăsat pe **Continuare**, alegeţi clasa de obiecte structurală pentru şablon, de exemplu **inetOrgPerson**. Puteţi de asemenea să adăugaţi clase de obiecte auxiliare pe care le doriţi.
4. Apăsaţi **Continuare**.
5. A fost creată o fişă **Obligatorii** în acest şablon. Puteţi modifica informaţiile conţinute în această fişă.
   a. Selectaţi **Obligatorii** în meniul de fişe şi apăsaţi **Editare**. Este afişat panoul **Editare fişă**. Vedeţi numele fişei **Obligatorii** şi atributele seletate care sunt obligatorii pentru clasa de obiecte, **inetOrgPerson**:

- *sn - surname
- *cn - common name

Notă: * indică informaţii obligatorii.

b. Dacă vreţi să adăugaţi informaţii suplimentare la această fişă, selectaţi atributul din meniul **Atribute**. De exemplu, selectaţi **departmentNumber** şi apăsaţi **Adăugare**. Selectaţi **employeeNumber** şi apăsaţi **Adăugare**. Selectaţi **title** şi apăsaţi **Adăugare**. Meniul **Atribute selectate** arată acum:
   - title
   - employeeNumber
   - departmentNumber
   - *sn
   - *cn

c. Puteţi rearanja ordinea în care apar aceste câmpuri în şablon prin evidenţierea atributului selectat şi apăsând pe **Mută în sus** sau **Mută în jos**. Aceasta schimbă poziţia atributului cu o poziţie. Repetaţi această procedură până când aţi aranjat atributele în ordinea în care le vreţi. De exemplu,
   - *sn
   - *cn
   - title
   - employeeNumber
   - departmentNumber

d. Puteţi de asemenea modifica fiecare atribut selectat.
   1) Evidenţiaţi atributul în căsuţa **Atribute selectate** şi apăsaţi **Editare**.
   2) Puteţi schimba numele de afişare al câmpului folosit în şablon. De exemplu, dacă vreţi ca **departmentNumber** să fie afişat ca **Număr departament** introduceţi asta în câmpul **Nume afişat**.
   3) Puteţi de asemenea să furnizaţi o valoare implicită care să completeze câmpul atributului în şablon. De exemplu, dacă majoritatea utilizatorilor care vor fi introduşi sunt membri ai Departmentului 789, puteţi introduce 789 ca valoare implicită. Câmpul din şablon este precompletat cu 789. Valoarea poate fi schimbată când adăugaţi informaţiile efective despre utilizator.
   4) Selectaţi **OK**.

e. Selectaţi **OK**.

6. Pentru a crea o altă categorie de fişă pentru informaţii suplimentare, apăsaţi **Adăugare**.
   - Introduceţi numele pentru noua fişă. De exemplu, Informaţii de adresă.
   - Pentru această fişă, selectaţi atributele din meniul **Atribute** . De exemplu, selectaţi **homePostalAddress** şi apăsaţi **Adăugare**. Selectaţi **postOfficeBox** şi apăsaţi **Adăugare**. Selectaţi **telephoneNumber** şi apăsaţi **Adăugare**. Selectaţi **homePhone** şi apăsaţi **Adăugare**. Selectaţi **facsimileTelephoneNumber** şi apăsaţi **Adăugare**. Meniul **Atribute selectate** arată acum:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone
     – facsimileTelephoneNumber
   - Puteţi rearanja ordinea în care apar aceste câmpuri în şablon prin evidenţierea atributului selectat şi apăsând pe **Mută în sus** sau **Mută în jos**. Aceasta schimbă poziţia atributului cu o poziţie. Repetaţi această procedură până când aţi aranjat atributele în ordinea în care le vreţi. De exemplu,
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – facsimileTelephoneNumber

– homePhone
- Selectaţi **OK**.

7. Repetaţi acest proces pentru atâtea fişe câte vreţi să creaţi. Când aţi terminat apăsaţi **Sfârşit** pentru a crea şablonul.

Adăugarea şablonului la o regiune

După ce aţi creat o regiune şi un şablon, trebuie să adăugaţi şablonul la regiune. Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Apăsaţi pe **Gestiune regiuni**.
2. Selectaţi regiunea la care vreţi să adăugaţi şablonul, în acest exemplu, **cn=realm1,o=ibm,c=us** şi apăsaţi **Editare**.
3. Derulaţi în jos la **Şablon utilizator** şi expandaţi meniul derulant.
4. Selectaţi şablonul, în acest exemplu **cn=template1,cn=realm1,o=ibm,c=us**.
5. Selectaţi **OK**.
6. Apăsaţi **Închidere**.

Crearea de grupuri

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Adăugare grup**.
2. Introduceţi numele grupului pe care doriţi să-l creaţi. De exemplu, **group1**.
3. Selectaţi regiunea în care doriţi să adăugaţi utilizatorul din meniul derulant. În acest caz **realm1**.
4. Faceţi clic pe **Sfârşit** pentru a crea grupul. Dacă aveţi deja utilizatori în regiune puteţi apăsa clic pe **Următorul** şi selectaţi utilizatorii de adăugat la group1. Apoi faceţi clic pe **Sfârşit**.

Vedeţi “Grupuri şi roluri” la pagina 42 pentru informaţii suplimentare.

Adăugarea unui utilizator la regiune

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Adăugare utilizator**.
2. Selectaţi regiunea în care doriţi să adăugaţi utilizatorul din meniul derulant. În acest caz **realm1**.
3. Apăsaţi **Continuare**. Este afişat şablonul pe care tocmai l-aţi creat, template1. Completaţi câmpurile necesare, notate cu un asterisc (*) şi oricare alte câmpuri de pe fişe. Dacă aţi creat deja grupuri în regiune, puteţi de asemenea să adăugaţi utilizatorul în unul sau mai multe grupuri.
4. Când aţi terminat, faceţi clic pe **Sfârşit**.

Gestionarea regiunilor

După ce aţi setat şi populat regiunea iniţială, puteţi adăuga mai multe regiuni sau modifica regiuni existente.

Expandaţi categoria **Regiuni şi şabloane** din zona de navigare şi apăsaţi **Gestiune regiuni**. Este afişată o listă cu regiunile existente. Din acest panou puteţi adăuga o regiune, edita o regiune, şterge o regiune sau edita listele de control al accesului (ACL-uri) pentru regiune. Pentru informaţii suplimentare, vedeţi următoarele:

- “Adăugarea unei regiuni”
- “Editarea unei regiuni” la pagina 144
- “Ştergerea unei regiuni” la pagina 144
- “Editarea ACL-urilor din regiune” la pagina 144

Adăugarea unei regiuni

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Adăugare regiune**.
   - Introduceţi numele pentru regiune. De exemplu **realm1**.

- Dacă aveţi regiuni preexistente, de exemplu **realm1**, puteţi selecta o regiune pentru a avea setările copiate la regiunea pe care o creaţi.
- Introduceţi DN-ul părinte care identifică locaţia regiunii. Acesată intrare este forma sufixului, de exemplu **o=ibm,c=us**. Puteţi de asemenea să apăsaţi pe **Răsfoire** pentru a selecta locaţia subarborelui pe care îl douiţi.

2. Faceţi clic pe **Următorul** pentru a continua sau faceţi clic pe **Sfârşit**.
3. Dacă aţi apăsat clic pe **Următorul**, revedeţi informaţiile.
4. Selectaţi un **Şablon utilizator** din meniul derulant. Dacă aţi copiat setările dintr-o regiune preexistentă, şablonul ei este precompletat în acest câmp.
5. Introduceţi un **Filtru de căutare utilizator**.
6. Faceţi clic pe **Sfârşit** pentru a crea regiunea.

Editarea unei regiuni

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

- Apăsaţi pe **Gestiune regiuni**.
- Selectaţi regiunea pe care vreţi să o editaţi din lista de regiuni.
- Apăsaţi **Editare**.
  - Puteţi folosi butoanele de **Răsfoire** pentru a schimba
    - Grupul de administrator
    - Containerul de grup
    - Containerul de utilizator
  - Puteţi selecta alt şablon din meniul derulant.
  - Apăsaţi **Editare** pentru a modifica **Filtrul de căutare utilizator**.
- Apăsaţi **OK** atunci când aţi terminat.

Ştergerea unei regiuni

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Apăsaţi pe **Gestiune regiuni**.
2. Selectaţi regiunea pe care doriţi să o înlăturaţi:
3. Apăsaţi **Ştergere**.
4. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**.
5. Regiunea este înlăturată din lista de regiuni.

Editarea ACL-urilor din regiune

Pentru a vedea proprietăţile ACL folosind unealta de administrare Web şi să lucraţi cu ACL-uri, vedeţi “Gestionarea listelor de control al accesului (ACL-uri)” la pagina 147.

Vedeţi “Liste de control al accesului” la pagina 48 pentru informaţii suplimentare.

Gestionarea şabloanelor

După ce aţi creat şablonul iniţial, puteţi adăuga mai multe şabloane sau să modificaţi şabloane existente.

Expandaţi categoria **Regiuni şi şabloane** din zona de navigare şi apăsaţi **Gestiune şabloane utilizator**. Este afişată o listă cu şabloanele existente. Din acest panou puteţi adăuga un şablon, edita un şablon, şterge un şablon sau edita listele de control al accesului (ACL-uri) pentru şablon. Pentru informaţii suplimentare, vedeţi următoarele:

- “Adăugarea unui şablon de utilizator” la pagina 145
- “Editarea unui şablon” la pagina 146
- “Ştergerea unui şablon” la pagina 146
- “Editarea ACL-urilor pe şablon” la pagina 146

Adăugarea unui şablon de utilizator

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Apăsaţi pe **Adăugare şablon utilizator** sau apăsaţi pe **Gestiune şabloane utilizator** şi apăsaţi **Adăugare**.
   - Introduceţi numele pentru noul şablon. De exemplu **template2** .
   - Dacă aveţi şabloane preexistente, de exemplu **template1**, puteţi selecta un şablon pentru a avea setările copiate la şablonul pe care îl creaţi.
   - Introduceţi DN-ul părinte care identifică locaţia şablonului. Acesată intrare este sub forma unui DN, de exemplu **cn=realm1,o=ibm,c=us**. Puteţi de asemenea să apăsaţi pe **Răsfoire** pentru a selecta locaţia subarborelui pe care îl douiţi.
2. Apăsaţi **Continuare**. Puteţi apăsa pe **Sfârşit** pentru a crea un nou şablon gol. Puteţi să adăugaţi mai târziu informaţii la şablon, vedeţi “Editarea unui şablon” la pagina 146.
3. Dacă aţi apăsat pe **Continuare**, alegeţi clasa de obiecte structurală pentru şablon, de exemplu **inetOrgPerson**. Puteţi de asemenea să adăugaţi clase de obiecte auxiliare pe care le doriţi.
4. Apăsaţi **Continuare**.
5. A fost creată o fişă **Obligatorii** în acest şablon. Puteţi modifica informaţiile conţinute în această fişă.
   a. Selectaţi **Obligatorii** în meniul de fişe şi apăsaţi **Editare**. Este afişat panoul **Editare fişă**. Vedeţi numele fişei **Obligatorii** şi atributele seletate care sunt obligatorii pentru clasa de obiecte, **inetOrgPerson**:
      - *sn - surname
      - *cn - common name

      Notă: * indică informaţii obligatorii.
   b. Dacă vreţi să adăugaţi informaţii suplimentare la această fişă, selectaţi atributul din meniul **Atribute**. De exemplu, selectaţi **departmentNumber** şi apăsaţi **Adăugare**. Selectaţi **employeeNumber** şi apăsaţi **Adăugare**. Selectaţi **title** şi apăsaţi **Adăugare**. Meniul **Atribute selectate** arată acum:
      - title
      - employeeNumber
      - departmentNumber
      - *sn
      - *cn
   c. Puteţi rearanja ordinea în care apar aceste câmpuri în şablon prin evidenţierea atributului selectat şi apăsând pe **Mută în sus** sau **Mută în jos**. Aceasta schimbă poziţia atributului cu o poziţie. Repetaţi această procedură până când aţi aranjat atributele în ordinea în care le vreţi. De exemplu,
      - *sn
      - *cn
      - title
      - employeeNumber
      - departmentNumber
   d. Puteţi de asemenea modifica fiecare atribut selectat.
      1) Evidenţiaţi atributul în căsuţa **Atribute selectate** şi apăsaţi **Editare**.
      2) Puteţi schimba numele de afişare al câmpului folosit în şablon. De exemplu, dacă vreţi ca **departmentNumber** să fie afişat ca **Număr departament** introduceţi asta în câmpul **Nume afişat**.
      3) Puteţi de asemenea să furnizaţi o valoare implicită care să completeze câmpul atributului în şablon. De exemplu, dacă majoritatea utilizatorilor care vor fi introduşi sunt membri ai Departmentului 789, puteţi introduce 789 ca valoare implicită. Câmpul din şablon este precompletat cu 789. Valoarea poate fi schimbată când adăugaţi informaţiile efective despre utilizator.
      4) Selectaţi **OK**.
   e. Selectaţi **OK**.
6. Pentru a crea o altă categorie de fişă pentru informaţii suplimentare, apăsaţi **Adăugare**.

- Introduceţi numele pentru noua fişă. De exemplu, Informaţii de adresă.
- Pentru această fişă, selectaţi atributele din meniul **Atribute** . De exemplu, selectaţi **homePostalAddress** şi apăsaţi **Adăugare**. Selectaţi **postOfficeBox** şi apăsaţi **Adăugare**. Selectaţi **telephoneNumber** şi apăsaţi **Adăugare**. Selectaţi **homePhone** şi apăsaţi **Adăugare**. Selectaţi **facsimileTelephoneNumber** şi apăsaţi **Adăugare**. Meniul **Atribute selectate** arată acum:
  - homePostalAddress
  - postOfficeBox
  - telephoneNumber
  - homePhone
  - facsimileTelephoneNumber
- Puteţi rearanja ordinea în care apar aceste câmpuri în şablon prin evidenţierea atributului selectat şi apăsând pe **Mută în sus** sau **Mută în jos**. Aceasta schimbă poziţia atributului cu o poziţie. Repetaţi această procedură până când aţi aranjat atributele în ordinea în care le vreţi. De exemplu,
  - homePostalAddress
  - postOfficeBox
  - telephoneNumber
  - facsimileTelephoneNumber
  - homePhone
- Selectaţi **OK**.

7. Repetaţi acest proces pentru atâtea fişe câte vreţi să creaţi. Când aţi terminat apăsaţi **Sfârşit** pentru a crea şablonul.

Editarea unui şablon

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

- Apăsaţi **Gestiune şabloane utilizator**.
- Selectaţi regiunea pe care vreţi să o editaţi din lista de regiuni.
- Apăsaţi **Editare**.
- Dacă aveţi şabloane preexistente, de exemplu template1, puteţi selecta un şablon pentru a avea setările copiate la şablonul pe care îl editaţi.
- Apăsaţi **Continuare**.
  - Puteţi folosi meniul derulant pentru a schimba clasa de obiecte structurală a şablonului
  - Puteţi adăuga şi înlătura clase de obiecte auxiliare.
- Apăsaţi **Continuare**.
- Puteţi modifica fişele şi atributele conţinute în şablon. Vedeţi 5 la pagina 145 pentru informaţii despre cum să modificaţi fişele.
- Când aţi terminat, faceţi clic pe **Sfârşit**.

Ştergerea unui şablon

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Gestiune şabloane utilizator**.
2. Selectaţi şablonul pe care vreţi să îl ştergeţi.
3. Apăsaţi **Ştergere**.
4. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**.
5. Şablonul este înlăturat din lista de utilizatori.

Editarea ACL-urilor pe şablon

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Gestiune şabloane utilizator**.
2. Selectaţi şablonul pentru care vreţi să editaţi ACL-urile.

3. Faceţi clic pe **Editare ACL**.

Pentru a vedea proprietăţile ACL folosind unealta de administrare Web şi să lucraţi cu ACL-uri, vedeţi “Gestionarea listelor de control al accesului (ACL-uri)”.

Vedeţi “Liste de control al accesului” la pagina 48 pentru informaţii suplimentare.

Gestionarea listelor de control al accesului (ACL-uri)

Pentru mai multe informaţii despre liste de control al accesului, vedeţi “Liste de control al accesului” la pagina 48.

Pentru a vedea proprietăţile ACL folosind unealta de administrare Web şi să lucraţi cu ACL-uri, faceţi următoarele:

1. Selectaţi o intrare director. De exemplu, cn=John Doe,ou=Advertising,o=ibm,c=US.
2. Apăsaţi pe **Editare ACL**. Este afişat panoul Editare ACL cu fişa **ACL-uri efective** preselectată.

Acest panou are cinci fişe:

- “ACL-uri efective”
- “Proprietari efectivi”
- “ACL-uri nefiltrate” la pagina 148
- “ACL-uri filtrate” la pagina 149
- “Proprietari” la pagina 150

Fişele **ACL-uri efective** şi **Proprietari efectivi** conţin informaţii numai-citire despre ACL-uri.

ACL-uri efective

ACL-urile efective sunt ACL-urile explicite şi moştenite ale intrării selectate. Puteţi vedea drepturile de acces pentru un ACL efectiv specific prin selectarea lui şi apăsarea pe butonul **Vizualizare**. Se deschide panoul **Vizualizare drepturi de acces**.

Vizualizarea drepturilor de acces

- Secţiunea **Drepturi** afişează adăugarea şi ştergerea drepturilor pentru subiect.
  - **Adăugare copil** acordă sau respinge subiectului dreptul de a adăuga o intrare director sub intrarea selectată.
  - **Ştergere intrare** acordă sau respinge subiectului dreptul de a şterge intrarea selectată.
- Secţiunea **Clasă de securitate** defineşte permisiuni pentru clasele de securitate. Atributele sunt grupate în clase de securitate:
  - **Normal** - Clasele de atribute normale necesită cea mai mică securitate, de exemplu, atributul commonName.
  - **Sensibil** - Clasele de atribute sensibile necesită o securitate moderată, de exemplu homePhone.
  - **Critic** - Clasele de atribute critice necesită cea mai mare securitate, de exemplu, atributul userpassword.

  Fiecare clasă de securitate are permisiuni asociate cu ea.
  - **Citire** - subiectul poate citi atributele.
  - **Scriere** - subiectul poate modifica atributele.
  - **Căutare** - subiectul poate căuta atribute.
  - **Comparare** - subiectul poate compara atribute.

Apăsaţi pe **OK** pentru a reveni la fişa ACL-uri efective.

Apăsaţi **Anulare** pentru a reveni la panoul Editare ACL.

Proprietari efectivi

Proprietari efectivi sunt proprietarii expliciţi şi moşteniţi ai intrării selectate.

ACL-uri nefiltrate

Puteţi adăuga noi ACL-uri nefiltrate la o intrare sau să editaţi ACL-uri la o intrare sau să editaţi ACL-uri nefiltrate existente.

ACL-urile nefiltrate pot fi propagate. Aceasta înseamnă că informaţiile de cotrol acces definite pentru o intrare pot fi aplicate la toate intrările subordonate. Sursa ACL este sursa ACL-ului curent pentru intrarea selectată. Dacă intrarea nu are un ACL, el moşteneşte un ACL de la obiectele părinte pe baza setărilor ACL ale obiectelor părinte.

Introduceţi următoarele infos în fişa de ACL-uri **Nefiltrate**:

- Propagaţi ACL-uri - Selectaţi caseta de bifare **Propagare** pentru a permite descendenţilor fără un ACL definit explicit pentru a moşteni această intrare. Dacă caseta de bifare este selectată descendentul moştenesc ACL-urile din această intrare şi dacă ACL-ul este4 explicit definit pentru intrarea copil, atunci ACL-ul care a fost moştenit de la părinte cu noul ACL care a fsot adăugat. Dacă caseta de bifare nu este selectată, intrările descendent fără un ACL definit explicit va moşteni ACL-uri de la un părinte al intrării care are această opţiune activată.
- DN (NUme distinctiv) - Introduceţi **numele distinctiv (DN)** al entităţii care cere acces pentru a executa operaţii pe intrarea selectată, de exemplu, cn=Marketing Group.
- Tip - Introduceţi **Tipul** DN-ului. De exemplu, selectaţi ID-ul de acces dacă DN-ul este un utilizator.

Adăugarea şi editarea drepturilor de acces

Faceţi clic fie pe butonul **Adăugare** pentru a adăuga DN-ul în câmpul DN (Numel distinctiv) în lista ACL fie butonu Editare pentru a modifica ACL-urile unui DN existent.

Panourile **Adăugare drepturi de acces** şi **Editare drepturi de acces** vă permit să setaţi drepturile de acces pentru un ACL (listă de control acces) nou sau existent. Câmpul **Tip** revine la valoarea implicită a tipului pe care l-aţi selectat în panoul **Editare ACL**. Dacă adăugaţi un ACL, toate celelalte câmpuri sunt implicit goale. Dacă editaţi un ACL, câmpurile conţin valorile setate ultima oară când a fost modificat ACL-ul.

Puteţi:

- Modifica tipul ACL-ului
- Seta drepturi de adăugare şi ştergere
- Seta permisiuni pentru clase de securitate

Pentru a seta drepturi de acces:

1. Selectaţi **Tip** al intrării pentru ACL. De exemplu, selectaţi ID-ul de acces dacă DN-ul este un utilizator.
2. Secţiunea **Drepturi** afişează adăugarea şi ştergerea drepturilor pentru subiect.
   - **Adăugare copil** acordă sau respinge subiectului dreptul de a adăuga o intrare director sub intrarea selectată.
   - **Ştergere intrare** acordă sau respinge subiectului dreptul de a şterge intrarea selectată.
3. Secţiunea **Clasă de securitate** defineşte permisiunile pentru clasele de atribute. Atributele sunt grupate în clase de securitate:
   - Normal - Clasele de atribute normale necesită securitatea minimă, de exemplu, atributul commonName.
   - Sensibil - Clasele de atribute sensibile nencesită o securitate moderată, de exemplu, homePhone.
   - Critic - Clasele de atribute critice necesită cea mai mare securitate, de exemplu, atributul userpassword.

   Fiecare clasă de securitate are permisiuni asociate cu ea.
   - Citire - subiectul poate citi atribute.
   - Scriere - subiectul poate modifica atributele.
   - Căutare - subiectul poate căuta atribute.
   - Comparare - subiectul poate compara atribute.

   În plus, puteţi specifica permisiuni pe baza atributului în locul clasei de securitate căreia îi aparţine atributul. Secţiunea de atribute este listată sub **Clasa de securitate critică**.

- Selectaţi un atribut din lista derulantă **Definire atribut**.
- Faceţi clic pe **Definire**. Atributul este afişat cu tabelul de permisiuni.
- Specificaţi dacă să acordaţi sau să refuzaţi fiecare din cele 4 permisiuni de clase de securitate asociate cu atributul.
- Puteţi repeta această procedură pentru atribute multiple.
- Pentru a înlătura un atribut, selectaţi doar atributul şi apăsaţi pe **Ştergere**.
- Când terminaţi, apăsaţi **OK**.

Înlăturare ACL-uri

Puteţi înlătura ACL-urile în fiecare din următoarele 2 modalităţi:

- Selectaţi butonul radio de lângă ACL-ul pe care doriţi să îl ştergeţi. Apăsaţi **Înlăturare**.
- Apăsaţi **Înlăturare toate** pentru a şterge toate DN-urile din listă.

ACL-uri filtrate

Puteţi adăuga noi ACL-uri noi filtrate la o intrare sau să editaţi ACL-uri la o intrare sau să editaţi ACL-uri filtrate existente.

ACL-urile bazate pe filtru implică o comparaţie bazată pe filtru, folosind un filtru de obiect specificat, pentru a corespunde cu obiectele destinaţie cu accesul efectiv care le se aplică.

Comportamentul implicit al ACL-urilor bazate pe filtru este să se acumuleze de la intrarea container cea mai de jos, în sus de-a lungul lanţului de intrări strămoş, până la intrarea container cea mai de sus din DIT. Accesul efectiv este calculat ca reuniune a drepturilor de acces acordate sau negate, de către intrările strămoş constituente. Există totuşi o excepţie de la acest comportament. Pentru compatibilitatea cu facilitatea de replicare a subarborelui şi pentru a permite un control administrativ mai mare, este folosit un atribut plafon ca mijloc de a opri acumularea la intrarea în care este conţinut.

Introduceţi următoarele infos în fişa ACL-uri filtrate.

- Acumulaţi ACL-uri filtrate -
  - Selectaţi butonul radio în **Nespecificat** pentru a înlătura atributul ibm-filterACLInherit din intrarea selectată.
  - Selectaţi butonul radio **Adevărat** pentru a permite ACL-urilor pentru intrarea selectată să se acumuleze din acea intrare în sus de-a lungul lanţului de intrare următor, la cel mai înalt filtru ACL conţinând intrarea în DIT.
  - Selectaţi butonul radio **Fals** pentru a opri acumularea de ACL-uri de filtrare la intrarea selectată.
- DN (NUme distinctiv) - Introduceţi **numele distinctiv (DN)** al entităţii care cere acces pentru a executa operaţii pe intrarea selectată, de exemplu, cn=Marketing Group.
- Tip - Introduceţi **Tipul** DN-ului. De exemplu, selectaţi ID-ul de acces dacă DN-ul este un utilizator.

Adăugarea şi editarea drepturilor de acces

Faceţi clic fie pe butonul **Adăugare** pentru a adăuga DN-ul în câmpul DN (Numel distinctiv) în lista ACL fie butonu Editare pentru a modifica ACL-urile unui DN existent.

Panourile **Adăugare drepturi de acces** şi **Editare drepturi de acces** vă permit să setaţi drepturile de acces pentru un ACL (listă de control acces) nou sau existent. Câmpul Tip revine la valoarea implicită pe care aţi selectat-o în panoul Editare ACL. Dacă adăugaţi un ACL, toate celelalte câmpuri sunt implicit goale. Dacă editaţi un ACL, câmpurile conţin valorile setate ultima oară când a fost modificat ACL-ul.

Puteţi:

- Modifica tipul ACL-ului
- Seta drepturi de adăugare şi ştergere

- Seta filtrul obiect pentru ACL-uri filtrate
- Seta permisiuni pentru clase de securitate

Pentru a seta drepturi de acces:

1. Selectaţi **Tip** al intrării pentru ACL. De exemplu, selectaţi ID-ul de acces dacă DN-ul este un utilizator.
2. Secţiunea **Drepturi** afişează adăugarea şi ştergerea drepturilor pentru subiect.
   - **Adăugare copil** acordă sau respinge subiectului dreptul de a adăuga o intrare director sub intrarea selectată.
   - **Ştergere intrare** acordă sau respinge subiectului dreptul de a şterge intrarea selectată.
3. Seta filtrul obiect pentru o comparaţie bazată pe filtru. În câmpul **Filtru obiect**, introduceţi filtrul de obiect dorit pentru ACL-ul selectat. Faceţi clic pe butonul **Editare filtru** pentru ajutor în compunerea şirul filtrului de căutare. ACL-ul filtrat curent se propagă în fiecare obiect descendent din subarborele asociat care se potriveşte cu filtrul din acel câmp.
4. Secţiunea **Clasă de securitate** defineşte permisiunile pentru clasele de atribute. Atributele sunt grupate în clase de securitate:
   - Normal - Clasele de atribute normale necesită securitatea minimă, de exemplu, atributul commonName.
   - Sensibil - Clasele de atribute sensibile nencesită o securitate moderată, de exemplu, homePhone.
   - Critic - Clasele de atribute critice necesită cea mai mare securitate, de exemplu, atributul userpassword.

   Fiecare clasă de securitate are permisiuni asociate cu ea.
   - Citire - subiectul poate citi atribute.
   - Scriere - subiectul poate modifica atributele.
   - Căutare - subiectul poate căuta atribute.
   - Comparare - subiectul poate compara atribute.

   În plus, puteţi specifica permisiuni pe baza atributului în locul clasei de securitate căreia îi aparţine atributul. Secţiunea de atribute este listată sub **Clasa de securitate critică**.
   - Selectaţi un atribut din lista derulantă **Definire atribut**.
   - Faceţi clic pe **Definire**. Atributul este afişat cu tabelul de permisiuni.
   - Specificaţi dacă să acordaţi sau să refuzaţi fiecare din cele 4 permisiuni de clase de securitate asociate cu atributul.
   - Puteţi repeta această procedură pentru atribute multiple.
   - Pentru a înlătura un atribut, selectaţi doar atributul şi apăsaţi pe **Ştergere**.
   - Când terminaţi, apăsaţi **OK**.

Înlăturare ACL-uri

Puteţi înlătura ACL-urile în fiecare din următoarele 2 modalităţi:

- Selectaţi butonul radio de lângă ACL-ul pe care doriţi să îl ştergeţi. Apăsaţi **Înlăturare**.
- Apăsaţi **Înlăturare toate** pentru a şterge toate DN-urile din listă.

Proprietari

Proprietarii de intrare au permisiuni complete pentru a efectua orice operaţie asupra obiectului. Proprietarii de intrare pot fi expliciţi sau propagaţi (moşteniţi).

Introduceţi următoarele informaţii în fişa de **Proprietari**:

- Selectaţi caseta de bifare **Propagare proprietari** pentru a permite desccendenţilor fără un proprietar definit explicit să moştenească din această intrare. Dacă caseta de bifare nu este selectată, intrările descendent fără un proprietar definit explicit vor moşteni proprietari de la un părinte al intrării care are această opţiune activată.
- DN (NUme distinctiv) - Introduceţi **numele distinctiv (DN)** al entităţii care cere acces pentru a executa operaţii pe intrarea selectată, de exemplu, cn=Marketing Group.

Folosirea cn=this cu obiecte care îşi propagă dreptul de proprietate la alte obiecte face mai uşoară crearea unui subarbore de creare în care fiecare obiect este deţinut de el însuşi.

- Tip - Introduceţi **Tipul** DN-ului. De exemplu, selectaţi ID-ul de acces dacă DN-ul este un utilizator.

Adăugarea proprietar

Faceţi clic pe **Adăugare** pentru a adăuga DN-ul în câmpul **DN (Nume distinctiv)** pentru listă.

Înlăturare proprietar

Puteţi înlătura un proprietar în fiecare din următoarele 2 modalităţi:

- Selectaţi butonul radio de lângă DN-ul proprietarului pe care vreţi să îl ştergeţi. Apăsaţi **Înlăturare**.
- Apăsaţi **Înlăturare toate** pentru a şterge toate DN-urile din listă.

Publicarea informaţiilor pe serverul de directoare

Puteţi configura sistemul dvs să publice anumite informaţii într-un Directory Server din acelaşi sistem sau dintr-un sistem diferit precum şi informaţii definite de utilizator. OS/400 publică automat aceste informaţii în Directory Server când folosiţi Navigator iSeries pentru a modifica aceste informaţii din OS/400. Informaţiile pe care le puteţi publica includ informaţii sistem (sisteme şi imprimante), partajări tipărire şi utilizator şi politicile de serviciu de calitate TCP/IP (pentru informaţii suplimentare vedeţi “Publicare” la pagina 34).

Dacă DN-ul părinte căruia datele îi sunt publicate nu există, Directory Server le creează automat. S-ar putea să aveţi instalat alte aplicaţii OS/400 care publică informaţii într-un director LDAP. În plus, puteţi apela interfeţele de program aplicaţie (API) din programele dvs proprii pentru a publica alte tipuri de informaţii în directorul LDAP.

Notă: Puteţi de asemenea publica informaţii OS/400 într-un server de directoare care nu rulează în OS/400 dacă configuraţi acel server să folosească IBM schema.

Pentru a configura sistemul dumneavoastră să publice informaţii OS/400 într-un server de directoare, urmaţi aceşti paşi :

1. În Navigator iSeries, apăsaşi clic-dreapta pe sistemul dumneavoastră şi selectaţi **Proprietăţi**.
2. Faceţi clic pe fişa **Directory Server**.
3. Apăsaţi pe tipurile de informaţii pe care vreţi să le publicaţi.

   Sugestie:
   Dacă planificaţi să publicaţi mai mult de un tip de informaţie la ceeaşi locaţie puteţi salva timp prin selectarea tipurilor informaţiilor multiple types de configurat la un moment dat. Navigatorul de operaţii va folosi apoi valorile care le introduceţi când configuraţi acel tip de informaţii ca şi valorile implicite când configuraţi tipurile următoare de informaţii.
4. Apăsaţi **Detalii**.
5. Apăsaţi casetă de bifare **Publicare informaţii sistem** .
6. Specificaţi **Metoda de autentificare** care vreţi să o folosească serverul, la fel şi informaţiile corespunzătoare de autentificare.
7. Apsaţi butonul **Editare** de lângă câmpul**Directory Server (Activ)** . În dialogul care apare, introduceţi numele serverului de directoare unde doriţi să publicaţi informaţii OS/400, apoi faceţi clic pe **OK**.
8. În câmpul **Sub DN**, introduceţi numele distinctiv părinte unde doriţi ca informaţiile să fie adăugate în serverul de directoare.
9. Completaţi câmpurile din cadrul **Conexiune server** care sunt corespunzătoare configuraţiei.

   Notă: Pentru a publica informaţii OS/400 la serverul de directoare folosind SSL sau Kerberos, trebuie să aveţi mai întâi serverul de directoare configurat la protocolul corespunzător. Vedeţi “Autentificare Kerberos cu Directory Server” la pagina 41 pentru informaţii despre SSL şi Kerberos.
10. Dacă serverul de directoare nu foloseşte portul implicit, introduceţi numele portului corect în câmpul **Port**.
11. Apăsaţi **Verificare** pentru a vă asigura că DN-ul părinte există pe server şi că informaţiile conexiunii sunt corecte. Dacă calea directorului nu există, un dialog vă va prompta să o creaţi.

Notă: Dacă DN-ul părinte nu există şi nu îl creaţi publicarea nu va fi cu succes.

12. Selectaţi **OK**.

Notă: Puteţi de asemenea publica informaţii i5/OS într-un server de directoare care este pe o platformă diferită. Trebuie să publicaţi informaţii sistem şi utilizator într-un server de directoare care foloseşte o schemă compatibilă cu schema IBM Directory Server. Pentru informaţii suplimentare despre IBM Directory Schema, vedeţi “Schema IBM Directory Server” la pagina 16.

API-uri pentru publicarea OS/400 informaţiilor la serverul de directoare

Directory Server furnizează suport încorporat pentru publicare de informaţii sistem şi utilizator. Aceste elemente sunt menţionate în pagina **Directory Server** din dialogul **Proprietăţi** ale sistemelor. Puteţi configuraţia serverului LDAP şi publicarea API-urilor pentru a activa OS/400 programele care le scrieţi pentru a publica alte tipuri de informaţii. Aceste tipuri de informaţii apar apoi în pagina **Directory Server** de asemenea. Precum sistemele şi utilizatorii, este sunt iniţial dezactivate şi le configuraţi folosind aceeaşi procedură. Programul care adaugă datele la directorul LDAP este numit agentul de publicare. Tipul de informaţii care sunt publicate, după cum apare în pagina **Directory Server**, este numit nume agent.

Următoarele API-uri vă vor permite să încorporaţi pulicarea în propriile dumneavoastră programe:

QgldChgDirSvrA
O aplicaţie foloseşte formatul CSVR0500 pentru a adăuga iniţial un nume de agent care este marcat ca o intrare dezactivată. Instrucţiunile pentru utilizatori din aplicaţie ar trebui să transmită utilizatorilor să folosească Navigator iSeries pentru a merge la pagina de proprietăţi servere de directoare pentru a configura agentul de publicare. Exemple de nume agent sunt numele de agent utilizatori şi sisteme disponibile automat în pagina **Directory Server**.

QgldLstDirSvrA
Folosiţi acest format API LSVR0500 pentru a lista care agenţi sunt disponibili curent pe sistemul dumneavoastră.

QgldPubDirObj
Folosiţi acest API pentru a face publicare aefectivă a informaţiei.

Pentru informaţii detailate despre aceste API-uri, consultaţi subiectul Lightweight Directory Access Protocol (LDAP) sub Programarea în Centru de informare iSeries.

Capitolul 8. Depanarea pentru Directory Server

Din păcate, chiar şi serverele de încredere precum Directory Server au uneori probleme. Când Directory Server are probleme, următoarele informaţii vă pot ajuta să găsiţi problema şi să o rezolvaţi.

Puteţi găsi codurile de întoarcere pentru erorile LDAP în fişierul ldap.h, care este localizat pe sistemul dumneavoastră în QSYSINC/H.LDAP.

"Monitorizarea erorilor şi a accesului cu istoricul jobului Directory Server" la pagina 154
Când obţineţi o eroare în Directory Server şi doriţi detalii suplimentare, o altă acţiune de luat este vizualizarea istoricului de job QDIRSRV.

"Folosirea TRCTCPAPP pentru a ajuta la găsirea problemelor" la pagina 154
Pentru erori ce pot fi reproduse, puteţi folosi comanda TRCTCPAPP APP(*DIRSRV) (Trace TCP/IP Application - Urmărire aplicaţie TCP/IP) pentru a rula o urmărire de erori.

"Folosirea opţiunii LDAP_OPT_DEBUG pentru a urmări erori" la pagina 155
Urmărirea problemelor cu clienţii care folosesc API-uri C LDAP.

"Erori comune client LDAP" la pagina 155
Ştiind cauzele erorile clientului LDAP vă poate ajuta să rezolvaţi probleme cu serverul dumneavoastră.

Pentru informaţii suplimentare despre problemele obişnuite Directory Server, vedeţi pagina home Directory Server  (www.iseries.ibm.com/ldap).

Directory Server foloseşte mai multe servere SQL (Structured Query Language) care sunt joburile iSeries QSQSRVR. Când apare o eroare SQL istoricul jobului QDIRSRV va conţine uzual, următorul mesaj:

```
SQL error -1 occurred
```

În aceste situaţii istoricul jobului QDIRSRV vă va referi la istoricele joburilor server SQL. Totuşi, în unele cazuri QDIRSRV poate să nu conţină acest mesaj şi acest referal, chiar dacă un server SQL este cauza problemei. În aceste instanţe, vă va ajuta să ştiţi ce joburi server SQL a pornit serverul, astfel încât să ştiţi în ce istorice job QSQSRVR să căutaţi pentru erori suplimentare.

Când Directory Server porneşte normal, el generează mesaje similare cu următoarele:

```
                                                      Sistem:   MYISERIES
 Job..:   QDIRSRV       Utilizator..:   QDIRSRV       Număr...:   174440

  >> CALL PGM(QSYS/QGLDSVR)
     Jobul 057448/QUSER/QSQSRVR folosit pentru procesarea mod server SQL.
     Jobul 057340/QUSER/QSQSRVR folosit pentru procesarea mod server SQL.
     Jobul 057448/QUSER/QSQSRVR folosit pentru procesarea mod server SQL.
     Jobul 057166/QUSER/QSQSRVR folosit pentru procesarea mod server SQL.
     Jobul 057279/QUSER/QSQSRVR folosit pentru procesarea mod server SQL.
   Jobul 057288/QUSER/QSQSRVR folosit pentru procesarea mod server SQL.
     Directory Server a pornit cu succes.
```

Mesajele se referă la joburile QSQSRVR care au fost pornite pentru pentru server. Numărul de mesaje pot diferi în serverul dvs în funcţie de configuraţie şi numărul de QSQSRVR necesare pentru executarea pornirii serverului.

Pe pagina Proprietăţi **Bază de date/Sufixe** a serverelor de directoare din Navigator iSeries specificaţi numărul total de servere SQL pe care Directory Server le foloseşte pentru operaţii cu directoare după pornirea serverului. Sunt pornite pentru replicare servere SQL adiţionale.

Monitorizarea erorilor şi a accesului cu istoricul jobului Directory Server

Vizualizarea istoricului de job pentru Directory Server vă poate alerta la erori şi vă poate ajuta să monitorizaţi accesul serverului. Istoricul jobului conţine:

- Mesajele despre operaţia de server şi orice problemă din interiorul serverului precum jobul serverului SQL sau eşuările de replicare.
- Mesajele înrudite cu securitatea care reflectă operaţiile după clienţi precum parole greşite.
- Mesajele care redau detalii despre erorile client precum atribute necesare lipsă.

S-ar putea să nu doriţi să introduceţi în istoric erori client, decât în cazul în care nu depanaţi probleme client. Puteţi controla introducerea în istoric a erorilor client din fişa de proprietăţi **General** din Directory Server din Navigatorul iSeries.

Dacă serverul dumneavoastră este pornit, urmaţi aceşti paşi pentru a vizualiza juranul job QDIRSRV:
1. În Navigator iSeries, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Joburi server**.
5. Din meniul **Fişier**, alegeţi **Istoricul jobului** .

Dacă serverul dumneavoastră este oprit, urmaţi aceşti paşi pentru a vizualiza juranul job QDIRSRV:
1. În Navigator iSeries, expandaţi **Operaţii de bază**.
2. Apăsaţi **Ieşire imprimantă** .
3. QDIRSRV apare în coloana **Utilizator** a panoului din dreapta Navigator iSeries. Pentru a vizualiza juranlul job, faceţi dublu-clic pe **Qpjoblog** în stânga QDIRSRV în aceeaşi linie.

   Notă: Navigator iSeries poate fi configurat pentru a afişa doar fişierele din spool. Dacă QDIRSRV nu apare în listă apăsaţi **Ieşire imprmantă**, apoi alegeţi **Include** din meniul **Opţiuni**. Specificaţi **Toate** din câmpul **Utilizator**, apoi apăsaţi **OK**.

Notă: Directory Server foloseşte alte resurse sistem pentru a realiza unele operaţii. Dacă apare vreo eroare cu una din aceste resurse, istoricul jobului va indica unde să se meargă pentru informaţii. În unele cazuri Directory Server poate sa nu fie capabil să determine unde să caute. În aceste cazuri, căutaţi în juranalele job ale serverelor Structured Query Language (SQL) să vedeţi dacă problema a fost relatat la servere SQL.

Folosirea TRCTCPAPP pentru a ajuta la găsirea problemelor

Serverul dumneavoastră furnizează o urmă de comunicaţie pentru a colecta date p o linie de comunicaţii cum ar fi reţeaua locală (LAN) sau o interfaţă largă de reţea (WAN). Utilizatorul mediu poate să nu înţeleagă întregul conţinut a datelor de urmărire. Totuşi, puteţi folosi intrările de urmărire pentru a determina dacă o dată se schimbă între două puncte.

Comanda TRCTCPAPP (Trace TCP/IP Application - Urmărire aplicaţie TCP/IP) cu opţiunea *DIRSRV poate fi folosită în Directory Server pentru a vă ajuta în găsirea problemelor de aplicaţie sau de client.

Pentru detalii suplimentare despre folosirea comenzii TRCTCPAPP cu LDAP precum şi despre restricţiile asupra autorizărilor necesare, vedeţi Descriere de comandă TRCTCPAPP (Trace TCP/IP Application).

Pentru informaţii generale despre folosirea urmăririi de comunicaţie vedeţi Urmărire de comunicaţii.

Folosirea opţiunii LDAP_OPT_DEBUG pentru a urmări erori

Puteţi folosi opţiunea LDAP_OPT_DEBUG din API-ul **ldap_set_option()** pentru a urmări probleme cu clienţii care folosesc API-uri C LDAP. Opţiunea de depanare are multe setări nivele de depanare care le puteţi folosi penru a vă ajuta în probleme de depanare cu aceste aplicaţii.

Următorul este un exemplu de activare a opţiunii de depanare urmă client.

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

O cale alternativă de setare a nivelului de depanare este de a configura valoarea numerică a variabilei mediu LDAP_DEBUG, pentru job-ul în care aplicaţia client rulează, la aceeaşi valoare numerică la care debugvalue ar fi dacă este folosit API-ul **ldap_set_option()** .

Un exemplu de activare a urmăririi client folosind variabila mediu LDAP_DEBUG este următorul:

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

După rularea clientului care produce problema care o aveţi, tastaţi următoarele la promptul iSeries:

```
DMPUSRTRC    ClientJobNumber
```

unde ClientJobNumber este numărul jobului client.

Pentru a afişa informaţiile interactiv, tastaţi următoarele la promptul iSeries:

```
DSPPFM  QAPOZDMP  QP0Znnnnnn
```

unde QAP0ZDMP conţine un zero şi nnnnnn este un număr de job.

Pentru a salva aceste informaţii pentru a le trimite la service, urmaţi aceşti paşi:

1. Creaţi un fişier SAVF folosind comanda de creare SAVF (CRTSAVF).
2. Tastaţi următoarele la promptul de iSeries comandă.

   ```
   SAVOBJ  OBJ(QAP0ZDMP  LIB(QTEMP)  DEV(*SAVF)  SAVF(xxx)
   ```

   unde QAP0ZDMP conţine un zero şi *xxx* este numel pe care l-aţi specificat pentru fişierul SAVF.

Erori comune client LDAP

Ştiind cauzele erorile clientului LDAP vă poate ajuta să rezolvaţi probleme cu serverul dumneavoastră. Pentru o listă completă de condiţii eroare client, vedeţi subiectul “API-uri Directory Server” de sub Programare în Centru de informare iSeries.

Mesajele de eroare client au următorul format:

```
[Operaţie LDAP eşuată ]:[Condiţii de eroare API client LDAP ]
```

Notă: Explicaţia acestor erori presupune că clientul comunică cu un server LDAP pe i5/OS. Un client ce comunică cu un server pe o platformă diferită poate avea erori similare, dar cauzele şi rezolvările vor fi diferite.

Mesajele comune le includ pe următoarele:

- “ldap_search: Depăşirea limitei de timp” la pagina 156
- “[Operaţie LDAP eşuată]: Eroare operaţii” la pagina 156

- “ldap_bind: Nu există un asemenea obiect”
- “ldap_bind: Autentificare necorespunzătoare”
- “[operaţie LDAP eşuată]: Insuficient acces”
- “[operaţie LDAP eşuată]: Nu se poate contacta serverul LDAP”
- “[operaţie LDAP eşuată]: A eşuat conectarea la serverul SSL.” la pagina 157

ldap_search: Depăşirea limitei de timp

Această eroare apare când căutările ldapsearch sunt realizate încet. Pentru a corecta această eroare, puteţi face una din următoarele:

- Creşteţi limita de timp de căutare pentru Directory Server. Vedeţi “Ajustarea setărilor de performanţă” la pagina 103 pentru informaţii despre realizarea acestui lucru.
- Reduceţi activitatea pe sistemul dumneavoastră. Puteţi de asemenea reduce numărul de joburi client LDAP active care rulează.

[Operaţie LDAP eşuată]: Eroare operaţii

Mai multe lucruri pot genera această eroare. Pentru a prelua informaţii despre cauza acestei erori pentru anumite instanţe, uitaţi-vă în istoricele job QDIRSRV (după cum este descris în “Monitorizarea erorilor şi a accesului cu istoricul jobului Directory Server” la pagina 154) şi istoricele de job ale serverelor SQL (după cum este descris în Capitolul 8, “Depanarea pentru Directory Server”, la pagina 153).

ldap_bind: Nu există un asemenea obiect

O cauză comună a acestei erori este aceea când utilizatorul face o greşeală de tastare când realizează o operaţie. O altă cauză comună este atunci când clientul LDAP încearcă să se lege cu un DN care nu există. Aceasta se întâmplă de obicei când utilizatorul specifică ceea ce crede greşi că este DN-ul administratorului. De exemplu, utilizatorul poate specifica QSECOFR sau Administrator, când actualul DN administrator poate fi ceva ca cn=Administrator.

Pentru detalii despre această eroare, consultaţi istoricul de joburi QDIRSRV cum este descris în “Monitorizarea erorilor şi a accesului cu istoricul jobului Directory Server” la pagina 154.

ldap_bind: Autentificare necorespunzătoare

Serverul întoarce Acreditări invalide când parola sau DN-ul asociat sunt incorecte. Server întoarce Autentificare necorespunzătoare când clientul încearcă să asocieze în unul din felurile următoare:

- O intrare care nu are un atribut userpassword
- O intrare care reprezintă un utilizator i5/OS, care are un atribut UID şi nu un atribut userpassword. Aceasta duce la o comparaţie între parola specificată şi parola utilizator i5/OS, care nu se potrivesc.
- O intrare reprezintă un utilizator proiectat şi o metodă de legare alta decât simplă a fost cerută.

Această eroare eset de obicei generată când clientul încearcă să asocieze cu o parolă care nu este validă. Pentru a obţine detalii despre această eroare, consultaţi istoricul job QDIRSRV cum este descris în “Monitorizarea erorilor şi a accesului cu istoricul jobului Directory Server” la pagina 154.

[operaţie LDAP eşuată]: Insuficient acces

Aceastp eroare este generată de obicei când DN asociat nu are autoritate să facă operaţia (cum ar fi o adăugare sau ştergere) pe care o cere clientul. Pentru a obţine detalii despre această eroare, consultaţi istoricul job QDIRSRV cum este descris în “Monitorizarea erorilor şi a accesului cu istoricul jobului Directory Server” la pagina 154.

[operaţie LDAP eşuată]: Nu se poate contacta serverul LDAP

Cauzele comune pentru această eroare includ următoarele:

- Un client LDAP face o cerere înainte ca serverul LDAP de pe sistemul specificat să fie pornit şi în starea de aşteptare selectare.

- Utilizatorul specifică un număr de port care nu este valid. De exemplu, serverul ascultă pe portul 386 dar încercările clientului folosesc portul 387.

Pentru a obţine detalii despre această eroare, consultaţi istoricul job QDIRSRV cum este descris în “Monitorizarea erorilor şi a accesului cu istoricul jobului Directory Server” la pagina 154. Dacă Directory Server porneşte cu succes, mesajul că Directory Server a pornit cu succes va fi în istoricul de joburi QDIRSRV.

[operaţie LDAP eşuată]: A eşuat conectarea la serverul SSL.

Această eroare apare când serverul LDAP respinge conexiunile client deoarece nu poate fi stabilită o conexiune pe socketi siguri. Aceeastă poate fi cauzată de una din următoarele:

- Suportul pentru Gestiunea certificatelor respinge încercările clienţilor de a se conecta la server. Folosiţi Managerul de certificate digitale pentru a vă asigura că ceritficatele dvs sunt setate corespunzător şi apoi reporniţi serverul şi reîncercaţi conectarea.
- Este posibil ca utilizatorul să nu aibă acces la citire la depozitul de certificate *SYSTEM (implicit /QIBM/userdata/ICSS/Cert/Server/default.kdb).

Pentru aplicaţii C i5/OS, sunt disponibile informaţii de eroare SSL suplimentare. Vedeţi pentru detalii “API-uri Directory Server” din subiectul Programare.

Capitolul 9. Referinţă

Vedeţi următoarele informaţii de referinţe adiţionale.

Utilitare linie de comandă

Această secţiune descrie utilitarele care pot fi rulate din mediul de comandă Qshell din i5/OS. Vedeţi următoarele comenzi pentru informaţii:

Notaţi că unele şiruri trebuie să fie conţinute între ghilimele pentru a fi procesate corect în mediul de comandă Qshell. Aceasta priveşte în general şirurile DN-uri, filtre de căutare şi lista de atribute întoarsă de ldapsearch. Vedeţi următoarea listă pentru următoarele exemple.

- Şirurile care conţin spaţii: "cn=John Smith,cn=users"
- Şirurile care conţin caractere wildcard "*"
- Şirurile care conţin paranteze "(objectclass=person)"

Pentru informaţii suplimentare despre mediul de comandă Qshell, vedeţi subiectul “Qshell”.

ldapmodify şi ldapadd

Uneltele LDAP de modificare şi adăugare intrare.

Sumar

```
ldapmodify [-a] [-b] [-c] [-C charset] [-d debuglevel][-D binddn][-i file]
[-h ldaphost] [-k] [-K keyfile] [-m mechanism] [-M] [-N certificatename]
[-O maxhops] [-p ldapport] [-P keyfilepw] [-r] [-R] [-v] [-V]
[-w passwd | ?] [-Z]


ldapadd [-a] [-b] [-c] [-C charset] [-d debuglevel][-D binddn][-i file]
[-h ldaphost] [-k] [-K keyfile] [-m mechanism] [-M] [-N certificatename]
[-O maxhops] [-p ldapport] [-P keyfilepw] [-r] [-R] [-v] [-V] [-w passwd | ?]
[-Z]
```

Descriere

ldapmodify este o interfaţă de linie de comandă pentru API-urile ldap_modify, ldap_add, ldap_delete şi ldap_modrdn. **ldapadd** este implementat ca versiune redenumită a lui ldapmodify. Când este invocat ca ldapadd, steguleţul **-a** (adăugare intrare nouă) este activat automat.

ldapmodify deschide o conexiune la serverul LDAP şi face legătura la server. Puteţi folosi **ldapmodify** pentru a modifica sau adăuga intrări. Informaţiile de intrare sunt citite de la intrarea standard sau din fişier prin folosirea opţiunii **-i**.

Pentru a afişa ajutorul de sintaxă pentru **ldapmodify** sau pentru **ldapadd**, introduceţi

```
ldapmodify -?
```

sau

```
ldapadd -?
```

Opţiuni

-a Adăugaţi intrări noi. Acţiunea implicită pentru **ldapmodify** este de a modifica intrările existente. Dacă este invocat ca**ldapadd**, acest steguleţ este mereu setat.

-b Presupuneţi că orice valori care încep cu un `/' sunt valori binare şi că valoarea reală este un fişier a cărui cale este specificată în locul evaluatorului.

-c Modul de operare continuu. Erorile sunt raportate, dar **ldapmodify** continuă modificările. Altfel acţiunea implicită este de a ieşi după raportarea unei erori.

-C *charset*
Specifică faptul că şirurile raportate ca intrare utilitarelor **ldapmodify** şi **ldapadd** sunt reprezentate într-un set de caractere local după cum se specifică în setul de caractere şi trebuie să fie convertit la UTF-8. Folosiţi opţiunea **-C** *charset* dacă pagina de cod a şirului de intrare este diferită de valoarea de pagină de cod job. Referiţi-vă la API-ul ldap_set_iconv_local_charset() pentru a vedea valorile set de caractere suportate.

-d *debuglevel*
Setaţi nivelul de depanare LDAP la debuglevel.

-D*binddn*
Folosiţi ***binddn*** pentru a lega la directorul LDAP. ***binddn*** este un DN reprezentat pe şiruri.

-h*ldaphost*
Specificaţi o gazdă alternativă în care rulează serverul ldap.

-i *file* Citiţi informaţiile de intrare de modificare de la un fişier LDIF în locul intrării standard. Dacă nu este specificat un fişier LDIF, trebuie să folosiţi intrarea standard pentru a specifica înregistrările de actualizare în format LDIF.

-k Specificaţi controlul de administrare server.

-K*keyfile*
Specificaţi numele fişierului bază de date de chei SSL cu extensia implicită **kdb**. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat. Dacă numele de fişier bază de date de chei nu este specificat, acest utilitar va căuta prima dată prezenţa unei variabile de mediu SSL_KEYRING cu un nume de fişier asociat. Dacă variabila de mediu SSL_KEYRING nu este definită, fişierul inel de chei sistem va fi folosit, dacă este prezent.

Acest parametru activează efectiv comutatorul **-Z**. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-m*mechanism*
Folosiţi ***mechanism*** pentru a specifica mecanismul SASL de folosit pentru legarea la server. Este folosit API-ul ldap_sasl_bind_s() . Parametrul **-m** este ignorat dacă este setat **-V 2**. Dacă **-m** nu este specificat, este folosită autentificarea simplă. Mecanismele valide sunt:

- CRAM-MD5 - protejează parola trimisă serverului.
- EXTERNAL - foloseşte certificatul SSL. Necesită -Z.
- GSSAPI - foloseşte acreditările Kerberos ale utilizatorului

-M Gestionează obiecte referral ca intrări obişnuite.

-N*certificatename*

Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Dacă serverul LDAP este configurtat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. ***certificatename*** nu este necesar dacă o pereche de chei certificat/privat a fost desemnată ca implicită pentru fişierul bază de date de chei. Similar, ***certificatename*** nu este necesar dacă este o pereche singură de chei certificate/private în fişierul bază de date chei. Acest parametru este ignorat dacă nu sunt specificate **-Z** sau **-K**. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-O *maxhops*

Specificaţi ***maxhops*** pentru a seta numărul maxim de hop-uri pe care le obţine biblioteca client când se urmăresc acreditările. Numărul de hop-uri implicit este 10.

-p *ldapport*

Specificaţi un port TCP alternativ pe care ascultă serverul ldap. Portul LDAP implicit este 389. Dacă **-p** nu este specifcat şi **-Z** este specificat, este folosit portul implicit SSL LDAP.

-P*keyfilepw*

Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile cifrate din fişierul bazei de date, care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-P** nu este necesar. Acest parametru este ignorat dacă nu sunt specificate **-Z** sau **-K**.

-r Înlocuieşte valorile existente cu cele implicite.

-R Specifică faptul că referalii nu trebuiesc automat urmaţi.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-V Specifică versiunea LDAP de folosit de către **ldapmodify** când se leagă la serverul LDAP. Implicit, o conexiune V3 LDAP este stabilită. Pentru a selecta explicit LDAP V3, specificaţi **-V 3**. Specificaţi **-V 2** pentru a rula ca aplicaţie LDAP V2.

-w *passwd* **| ?**

Folosiţi ***passwd*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

-Z Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

Format intrare

Conţinutul fişierului (sau intrării standard dacă nici un steguleţ **-i** nu este dat la linia de comandă) ar trebui să se conformeze formatului LDIF. Vedeţi “LDIF (LDAP Data Interchange Format)” la pagina 184 pentru informaţii suplimentare despre formatul LDIF.

Exemple

Se presupune că fişierul /tmp/entrymods există şi are următorul conţinut:

```
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
-
```

comanda:

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

va înlocui conţinutul atributului de mail a intrării Modify Me cu valoarea modme@student.of.life.edu, adăugaţi un titlu de Grand Poobah şi conţinutul fişierului /tmp/modme.jpeg ca un jpegPhoto şi va înlătura complet atributul de descriere. Aceleaşi modificări pot fi efectuate folosind vechiul format de intrare 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
```

şi comanda:

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

Presupunând că există fişierul /tmp/newentry şi are următorul conţinut:

```
dn: cn=John Doe, o=University of Higher Learning, c=US
objectClass: person
cn: John Doe
cn: Johnny
sn: Doe
titlu: cea mai cunoscută persoană mitică din lume
mail: johndoe@student.of.life.edu
uid: jdoe
```

comanda:

```
 ldapadd -i /tmp/entrymods
```

adaugă o nouă intrare pentru John Doe, folosind valorile pentru fişierul /tmp/newentry.

Note

Dacă informaţiile de intrare nu sunt furnizate din fişier prin folosirea opţiunii **-i**, comanda **ldapmodify** va aştepta să citească intrări pentru introducerea standard.

Diagnostice

Starea de ieşire este 0 dacă nu apar erori. Rezultatele de eroare dintr-o stare de ieşire non-zero şi un mesaj diagnostic au fost scrise la eroarea standard.

ldapdelete

Unealta de ştergere intrare LDAP

Sinopsis

```
ldapdelete [-c] [-C charset] [-d debuglevel][-D binddn][-i file]
[-h ldaphost] [-k] [-K keyfile] [-m mechanism] [-M] [-n] [-N certificatename]
[-O maxops] [-p ldapport] [-P keyfilepw] [-R] [-s][-v] [-V version]
[-w passwd | ?] [-Z] [dn]...
```

Descriere

ldapdelete este o interfaţă linie de comandă la API-ul ldap_delete .

ldapdelete deschide o conexiune la serverul LDAP, face legătura şi şterge una sau mai multe intrări. Dacă sunt furnizate unul sau mai multe argumente nume distinctive (DN), intrările cu acele DN-uri sunt şterse. Fiecare DN este un DN reprezentat prin şir. Dacă nu sunt furnizate argumente DN, o listă de DN-uri este citită din intrarea standard sau dintr-un fişier daca steguleţul **-i** este folosit.

Pentru a afişa sintaxa ajutor pentru **ldapdelete**, introduceţi:

```
ldapdelete -?
```

Opţiuni

-c Modul de operare continuu. Erorile sunt raportate, dar **ldapdelete** continuă modificările. Altfel acţiunea implicită este de a ieşi după raportarea unei erori.

-C *charset*
Specifică faptul că DN-urile furnizate ca intrare la utilitarul **ldapdelete** sunt reprezentate într-un set de caractere local, precum este specificat în setul de caractere. Folosiţi opţiunea **-C** *charset* dacă pagina de cod a şirului de intrare este diferită de valoarea de pagină de cod job. Referiţi-vă la API-ul ldap_set_iconv_local_charset() pentru a vedea valorile set de caractere suportate.

-d *debuglevel*
Setaţi nivelul de depanare LDAP la debuglevel.

-D*binddn*
Folosiţi ***binddn*** pentru a lega la directorul LDAP. ***binddn*** este un DN reprezentat pe şiruri.

-h*ldaphost*
Specifică o gazdă alternativă pe care rulează serverul LDAP.

-i *file* Citiţi o serie de linii din fişier, executând o ştergere LDAP pentru fiecare linie de fişier. Fiecare linie din fişier ar trebui să conţină un singur nume distinctiv.

-k Specificaţi să folosiţi controlul de administrare server.

-K*keyfile*
Specifică nuumele fişierului bază de date de chei SSL. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele complet calificat al fişierului bază de date chei.

Dacă utilitarul nu poate localiza baza de date chei, va folosi un set codificat hardware de rădăcini pentru CA de încredere. Fişierul bază de date chei conţine tipic unul au mai multe certificate de autorităţi de certificare (CA) care sunt crezute de client. Aceste tipuri de certificate X.509 sunt de asemenea cunoscute ca rădăcini de încredere.

Acest parametru activează efectiv comutatorul **-Z**. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-m*mechanism*
Folosiţi ***mechanism*** pentru a specifica mecanismul SASL de folosit pentru legarea la server. Parametrul **-m** este ignorat dacă este setat **-V 2**. Dacă **-m** nu este specificat, este folosită autentificarea simplă.

-M Gestionează obiecte refferal ca intrări obişnuite.

-n Arată ce s-ar face, dar nu modifică efectiv intrările. Folositoare pentru depanare în conjuncţie cu **-v**.

-N*certificatename*
Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Dacă serverul LDAP este configurat pentru a executa doar autentificarea server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. ***certificatename*** nu este necesar, dacă o pereche cheie privată/certificat a fost desemnată ca implicită. Similar, ***certificatename*** nu este necesar dacă este o pereche singură cheie privată/certificat în fişierul bază de date chei desemnat. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-O *maxhops*
Specificaţi ***maxhops*** pentru a seta numărul maxim de hop-uri pe care le obţine biblioteca client când se urmăresc acreditările. Numărul de hop-uri implicit este 10.

-p *ldapport*
Specificaţi un port TCP alternativ pe care ascultă serverul LDAP. Portul LDAP implicit este 389. Dacă **-p** nu este specifcat şi **-Z** este specificat, este folosit portul implicit SSL LDAP.

-P*keyfilepw*
Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile cifrate din fişierul bazei de date, care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-P** nu este necesar. Acest parametru este ignorat dacă nu sunt specificate **-Z** sau **-K**.

-R Specifică faptul că referalii nu trebuiesc automat urmaţi.

-s Folosiţi această opţiune pentru a şterge subarborele din rădăcina intrării specificate.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-V Specifică versiunea LDAP de folosit de către **ldapdelete** când se leagă la serverul LDAP. Implicit, o conexiune V3 LDAP este stabilită. Pentru a selecta explicit LDAP V3, specificaţi **-V 3**. Specificaţi **-V 2** pentru a rula ca aplicaţie LDAP V2.

-w *passwd* **| ?**
Folosiţi ***passwd*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

-Z Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

dn Specifică unul sau mai multe argumente DN. Fiecare DN ar trebui să fie un DN reprezentat de şir.

Exemple

Următoarea comandă,

```
ldapdelete -D cn=administrator -w secret "cn=Delete Me, o=University of Life, c=US"
```

încearcă să şteargă intrarea cu numele de commonName ″Delete Me″ direct sub intrarea Universitatea organizaţională a vieţii.

Note

Dacă nu sunt furnizate argumente DN, comanda **ldapdelete** aşteaptă să citească o listă de DN-uri din intrarea standard.

Diagnostice

Starea de ieşire este 0 dacă nu apar erori. Rezultatele de eroare dintr-o stare de ieşire non-zero şi un mesaj diagnostic au fost scrise la eroarea standard.

ldapexop

Unealta de operaţie extinsă LDAP

Sinopsis

```
ldapexop [-C charset] [-d debuglevel][-D binddn][-e] [-h ldaphost]
[-help][-K keyfile] [-m mechanism] [-N certificatename]
[-p ldapport] [-P keyfilepw] [-?] [-v] [-w passwd | ?] [-Z]
-op {cascrepl | controlqueue | controlrepl |
quiesce | readconfig}
```

Descriere

Utilitarul **ldapexop** este o interfaţă linie de comandă care furnizează capacitatea de a se lega la serverul de directoare şi de a emite o singură operaţie extinsă împreună cu orice date care alcătuiesc valoarea operaţiei extinse.

Utilitarul **ldapexop** suportă gazda standard, portul, SSL-ul şi opţiunile de autentificare de toate utilitarele client LDAP. În plus, un set de opţiuni este definit pentru a sepcifica operaţia de executat şi argumentele pentru fiecare operaţie extinsă.

Pentru a afişa ajutorul de sintaxă pentru **ldapexop**, introduceţi:

```
ldapexop -?
```

sau

```
ldapexop -help
```

Opţiuni

Opţiunile pentru comanda ldapexop sunt împărţite în 2 categorii:

1. Opţiunile generale care specifică modul de conectare la serverul de directoare. Aceste opţiuni trebuie specificat înaintea opţiunilor specifice operaţiei.
2. Opţiunea de operaţie extinsă care identifică operaţia extinsă de realizat.

Opţiuni generale

Aceste opţiuni specifică metodele de conectare la server şi trebuie să fie specificate înaintea opţiunii **-op**.

-C *charset*
: Specifică faptul că DN-urile furnizate ca intrare la utilitarul **ldapexop** sunt reprezentate într-un set de caractere local, precum este specificat în setul de caractere. Folosiţi opţiunea **-C** *charset* dacă pagina de cod a şirului de intrare este diferită de valoarea de pagină de cod job. Referiţi-vă la API-ul ldap_set_iconv_local_charset() pentru a vedea valorile set de caractere suportate.

-d *debuglevel*
: Setaţi nivelul de depanare LDAP la debuglevel.

-D*binddn*
: Folosiţi ***binddn*** pentru a lega la directorul LDAP. ***binddn*** este un DN reprezentat pe şiruri.

-e
: Afişează informaţiile versiunii bibliotecii LDAP şi apoi iese.

-h*ldaphost*
: Specifică o gazdă alternativă pe care rulează serverul LDAP.

-help
: Afişează sintaxa comenzii şi informaţiile de folosire.

-K*keyfile*
: Specifică nuumele fişierului bază de date de chei SSL. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

  Dacă utilitarul nu poate localiza o bază de date de chei, este folosită baza de date de chei sistem. Fişierul bază de date chei conţine tipic unul au mai multe certificate de autorităţi de certificare (CA) care sunt crezute de client. Aceste tipuri de certificate X.509 sunt de asemenea cunoscute ca rădăcini de încredere.

  Acest parametru activează efectiv comutatorul **-Z**. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-m*mechanism*
: Folosiţi ***mechanism*** pentru a specifica mecanismul SASL de folosit pentru legarea la server. Va fi folosit API-ul ldap_sasl_bind_s(). Parametrul **-m** este ignorat dacă este setat **-V 2**. Dacă **-m** nu este specificat, este folosită autentificarea simplă.

-N*certificatename*

Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. ***certificatename*** nu este necesar implicit dacă o pereche de chei implicită certificate/private a fost desemnată ca implicit. Similar, ***certificatename*** nu este necesar dacă este o pereche singură de chei certificate/private în fişierul bază de date chei. Acest parametru este ignorat dacă nu sunt specificate **-Z** sau **-K**. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-p *ldapport*

Specificaţi un port TCP alternativ pe care ascultă serverul LDAP. Portul LDAP implicit este 389. Dacă **-p** nu este specifcat şi **-Z** este specificat, este folosit portul implicit SSL LDAP.

-P*keyfilepw*

Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile cifrate din fişierul bazei de date, care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-P** nu este necesar. Acest parametru este ignorat dacă nu sunt specificate **-Z** sau **-K**.

-? Afişează sintaxa comenzii şi informaţiile de folosire.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-w *passwd* **| ?**

Folosiţi ***passwd*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

-Z Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

Opţiune operaţii extinse

Opţiunea **-op** operaţie extinsă identifică operaţia extinsă de realizat. Operaţia extinsă poate fi una din următoarele valori:

- **cascrepl**: operaţie extinsă de replicare control de cascadare. Acţiunea cerută este aplicată serverul specificat şi de asemenea transmisă tuturor replicilor subarborelui dat. Dacă oricare dintre acestea sunt înaintate ca replici, ele trec operaţia extinsă împreună cu replicile ei. Operaţia se cascadează în întreaga topologie de replicare.

  -action quiesce | unquiesce | replnow | wait

  Acesta este un atribut necesar care specifică acţiunea de realizat.

  quiesce

  Nu sunt permise actualizări viitoare, cu excepţia replicării.

  unquiesce

  Se reia operaţia normală, sunt acceptate actualizările client.

  replnow

  Face replica tuturor modificărilor din coadă la toate serverele replică cât mai curând posibil indiferent de planificare.

  wait Aşteaptă ca toate actualizările să fie replicate la toate replicile.

  -rc *contextDn*

  Acesta este un atribut necesar care specifică rădăcina subarborelui.

  -timeout *secs*

  Acesta este un atribut opţional care, dacă este prezent, specifică perioada de timeout în secunde. Dacă nu este prezent sau este 0, operaţia aşteaptă nedefinit.

  Exemplu:

```
ldapexop -op cascrepl -action -quiesce -rc "o=acme,c=us" -timeout 60
```

- **controlqueue**: operaţia extinsă de replicare coadă de control. Această operaţie vă permite să ştergeţi sau să înlăturaţi modificările în aşteptare din lista de modificări de replicare care a fost pusă în coadă şi unde nu sunt rulate din cauza erorilor de replicare. Această operaţie este folositoare când datele replică sunt fixate manual. Veţi folosi atunci această operaţie pentru a evita realizarea unpr eşuări din coadă.

  -skip all | change-id
  Acesta este un atribut necesar.
  - **all** indică evitarea tuturor modificărilor în aşteptare pentru acest acord.
  - **change-id** identifică singura modificare de evitat. Dacă serverul nu face replicarea aceste modificări acum, cererea eşuează.

  -ra *agreementDn*
  Acesta este un atribut necesar care specifică DN-ul acordului de replicare.

  Exemple:

```
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**: control replication extended operation

  -action suspend | resume | replnow
  Acesta este un atribut necesar care specifică acţiunea de realizat.

  -rc *contextDn* **| -ra** *agreementDn*
  -rc *contextDn* este DN-ul contextului de replicare. Acţiunea este realizată pentru toate acordurile pentru acest context. **-ra** *agreementDn* este DN-ul acordului de replicare. Acţiunea este realizată pentru acordul de replicare specificat.

  Exemplu:

```
ldapexop -op controlrepl -action suspend -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"
```

- **quiesce**: activare sau dezactivare operaţie extinsă de replicare subarbore

  -rc *contextDn*
  Acesta este un atribut necesar care specifică DN-ul contextului (subarbore) replicare pentru a fi activat sau dezactivat.

  -end Acesta este un atribut opţional care, dacă este prezent, specifică dezactivarea subarborelui. Dacă nu este specificat, valoarea implicită este de activare a subarborelui.

  Exemple:

```
ldapexop -op quiesce -rc "o=acme,c=us"

ldapexop -op quiesce -end -rc "o=ibm,c=us"
```

- **readconfig**: operaţia extinsă recitire fişier de configurare

  -scope entire | single<*entry DN***><***attribute***>**
  Acesta este un atribut necesar.
  - **entire** indică recitirea întregului fişier de configurare.
  - **single** înseamnă să citiţi singura intrare şi atributul specificat.

  Exemple:

```
ldapexop -op readconfig -scope entire

ldapexop -op readconfig -scope single "cn=configuration" ibm-slapdAdminPW
```

Notă: Următoarele intrări marcate cu:

- [1] au efect imediat
- [2] au efect în noile operaţii
- [3] au efect imediat ce parola este modificată (nu este necesară readconfig)
- [4] sunt suportate de către utilitarul liniei de comandă din i5/OS, dar nu sunt suportate de Directory Server din i5/OS.

```
cn=Configuraţie
ibm-slapdadmindn[2]
ibm-slapdadminpw[2, 3, 4]
ibm-slapderrorlog[1, 4]
ibm-slapdpwencryption[1]
ibm-slapdsizelimit[1]
ibm-slapdsysloglevel[1, 4]
ibm-slapdtimelimit[1]
cn=Front End, cn=Configuration
ibm-slapdaclcache[1]
ibm-slapdaclcachesize[1]
ibm-slapdentrycachesize[1]
ibm-slapdfiltercachebypasslimit[1]
ibm-slapdfiltercachesize[1]
ibm-slapdidletimeout[1]
cn=Event Notification, cn=Configuration
ibm-slapdmaxeventsperconnection[2]
ibm-slapdmaxeventstotal[2]
cn=Transaction, cn=Configuration
ibm-slapdmaxnumoftransactions[2]
ibm-slapdmaxoppertransaction[2]
ibm-slapdmaxtimelimitoftransactions[2]
cn=ConfigDB, cn=Config Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdreadonly[2]
cn=Directory, cn=RDBM Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdbulkloaderrors[1, 4]
ibm-slapdclierrors[1, 4]
ibm-slapdpagedresallownonadmin[2]
ibm-slapdpagedreslmt[2]
ibm-slapdpagesizelmt[2]
ibm-slapdreadonly[2]
ibm-slapdsortkeylimit[2]
ibm-slapdsortsrchallownonadmin[2]
ibm-slapdsuffix[2]
```

Diagnostice

Starea de ieşire este 0 dacă nu apar erori. Rezultatele de eroare dintr-o stare de ieşire non-zero şi un mesaj diagnostic au fost scrise la eroarea standard.

ldapmodrdn

Unealta RDN de modificare intrare LDAP

Sinopsis

```
ldapmodrdn [-c] [-C charset] [-d debuglevel][-D binddn] [-h ldaphost]
[-i file] [-k] [-K keyfile] [-m mechanism] [-M] [-n]
[-N certificatename] [-O hopcount] [-p ldapport] [-P keyfilepw]
[-r] [-R] [-v] [-V] [-w passwd | ?] [-Z] [dn newrdn | [-i file]]
```

Descriere

ldapmodrdn este o interfaţă linie de comandă la API-ul ldap_modrdn.

ldapmodrdn deschide o conexiune la serverul LDAP, face legătura şi modifică RDN-ul intrărilor. Informaţiile de intrare sunt citite de la intrarea standard sau din fişier prin folosirea opţiunii **-f** sau a perechii linie de comandă DN şi RDN.

Vedeţi “Nume distinctive (DN-uri)” la pagina 11 pentru informaţii despre RDN-uri (Nume distinctive relative) şi DN-uri (Nume distinctive).

Pentru a afişa ajutorul de sintaxă pentru **ldapmodrdn**, introduceţi:

```
ldapmodrdn -?
```

Opţiuni

-c Modul de operare continuu. Erorile sunt raportate, dar **ldapmodrdn** continuă modificările. Altfel acţiunea implicită este de a ieşi după raportarea unei erori.

-C *charset*
Specifică faptul că şirurile furnizate ca intrare la utilitarul **ldapmodrdn** sunt reprezentate într-un set de caractere local, precum este specificat în setul de caractere. Folosiţi opţiunea **-C** *charset* dacă pagina de cod a şirului de intrare este diferită de valoarea de pagină de cod job. Referiţi-vă la API-ul ldap_set_iconv_local_charset() pentru a vedea valorile setului de caractere suportate. Notaţi că valorile suportate pentru setul de caractere sunt aceleaşi valori suportate pentru fişa setului de caractere care este definită opţional în Versiunea 1 a fişierelor LDIF.

-d *debuglevel*
Setaţi nivelul de depanare LDAP la debuglevel.

-D*binddn*
Folosiţi ***binddn*** pentru a lega la directorul LDAP. binddn ar trebui să fie un DN reprezentat pe şiruri.

-h*ldaphost*
Specificaţi o gazdă alternativă în care rulează serverul ldap.

-i *file* Citiţi informaţiile de modificare intrare de un fişier în locul intrării standard sau a liniei de comandă (specificând rdn şi newrdn). Intrarea standard poate fi furnizată dintr-un fişier la fel ca şi (″< file″).

-k Specificaţi controlul de administrare server.

-K*keyfile*
Specifică nuumele fişierului bază de date de chei SSL. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

Dacă utilitarul nu poate localiza baza de date de chei, va folosi un set hard-coded de rădăcina Autorităţii implicită de certificare de înredere. Fişierul bază de date chei conţine tipic unul au mai multe certificate de autorităţi de certificare (CA) care sunt crezute de client. Aceste tipuri de certificate X.509 sunt de asemenea cunoscute ca rădăcini de încredere.

Acest parametru activează efectiv comutatorul **-Z**. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-m*mechanism*
Folosiţi ***mechanism*** pentru a specifica mecanismul SASL de folosit pentru legarea la server. Va fi folosit API-ul ldap_sasl_bind_s(). Parametrul **-m** este ignorat dacă este setat **-V 2**. Dacă **-m** nu este specificat, este folosită autentificarea simplă.

-M Gestionează obiecte refferal ca intrări obişnuite.

-n Arată ce s-ar face, dar nu modifică efectiv intrările. Folositoare pentru depanare în conjuncţie cu **-v**.

-N*certificatename*
Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Notaţi că dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul

LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. ***certificatename*** nu este necesar, dacă o pereche cheie privată/certificat a fost desemnată ca implicită. Similar, ***certificatename*** nu este necesar dacă este o pereche singură cheie privată/certificat în fişierul bază de date chei desemnat. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-O*hopcount*
Specificaţi ***hopcount*** pentru a seta numărul maxim de hopuri pe care le obţine biblioteca client când se urmăresc acreditările. Numărul de hopuri implicit este 10.

-p *ldapport*
Specificaţi un port TCP alternativ pe care ascultă serverul ldap. Portul LDAP implicit este 389. Dacă nu este specificat şi este specificat -Z, este folosit portul SSL LDAP implicit 636.

-P*keyfilepw*
Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile criptate din fişierul bazei de date de chei (care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-P** nu este necesar. Acest parametru este ignorat dacă nu sunt specificate **-Z** sau **-K**.

-r Înlăturaţi vechile valori RDN din intrare. Acţiunea implicită este de a păstra valorile vechi.

-R Specifică faptul că referalii nu trebuiesc automat urmaţi.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-V Specifică versiunea LDAP de folosit de către **ldapmodrdn** când se leagă la serverul LDAP. Implicit, o conexiune V3 LDAP este stabilită. Pentru a selecta explicit LDAP V3, specificaţi **-V 3**. Specificaţi **-V 2** pentru a rula ca aplicaţie LDAP V2. O aplicaţie, ca **ldapmodrdn**, selectează LDAP V3 ca protocol preferat folosind ldap_init în loc de ldap_open.

-w *passwd* **| ?**
Folosiţi ***passwd*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

-Z Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

dn newrdn
Vedeţi următoarea secţiune, “Format de intrare pentru dn newrdn” pentru informaţii suplimentare.

Format de intrare pentru dn newrdn

Dacă argumentele liniei de comandă *dn* şi *newrdn* sunt date, *newrdn* înlocuieşte RDN-ul intrării specificate de DN, *dn*. Altfel, conţinutul fişierului (sau intrarea standard, dacă nu este dat nici un steguleţ **- i**) conţine una sau mai multe intrări:

```
Nume distinctiv (DN)

Nume distinctiv relativ (RDN)
```

Una sau mai multe linii goale pot fi folosite pentru a separa fiecare pereche DN şi RDN.

Exemple

Se presupune că fişierul /tmp/entrymods există şi are conţinutul:

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

comanda:

```
ldapmodrdn -r -i /tmp/entrymods
```

modifică RDN-ul intrării Modify Me din Modify Me la The New Me şi vechiul cn, Modify Me este înlăturat.

Note

Dacă informaţiile de intrare nu sunt furnizate din fişier prin folosirea opţiunii **-i** (perechea linie de comandă *dn* şi *rdn*), comanda **ldapmodrdn** va aştepta să citească intrări din intrarea standard.

Diagnostice

Starea de ieşire este 0 dacă nu apar erori. Rezultatele de eroare dintr-o stare de ieşire non-zero şi un mesaj diagnostic au fost scrise la eroarea standard.

ldapsearch

Unealta de căutare LDAP şi program exemplu

Sinopsis

```
ldapsearch [-a deref] [-A] [-b searchbase] [-B] [-C charset] [-d debuglevel]
[-D binddn] [-F sep] [-h ldaphost] [-i file] [-K keyfile] [-l timelimit] [-L]
[-m mechanism] [-M] [-n] [-N certificatename][-o attr_type] [-O maxhops]
[-p ldapport] [-P keyfilepw] [-q pagesize]  [-R] [-s scope ] [-t] [-T seconds]
[-v] [-V version] [-w passwd | ?] [-z sizelimit] [-Z] filter [attrs...]
```

Descriere

ldapsearch este o interfaţă linie de comandă la API-ul ldap_search.

ldapsearch deschide o conexiune la serverul LDAP, face legătura şi execută o căutare folosind filtru. Filtrul ar trebui să se conformeze la reprezentarea şirului pentru filtrele LDAP (vedeţi ldap_search din API-uri Directory Server pentru informaţii suplimentare despre filtre).

Dacă **ldapsearch** găseşte una sau mai multe intrări, atributele specificate de attrs sunt retrase, iar intrările şi valorile sunt tipărite la ieşirea standard. Dacă nu este listat nici un attrs, toate atributele sunt întoarse.

Pentru a afişa sintaxa ajutor pentru **ldapsearch**, introduceţi ldapsearch -?.

Opţiuni

-a deref
: Specifică cum diferenţierea alias-urilor. deref ar trebui să fie unul dintre niciodată, întotdeauna, căutare sau găsire pentru a specifica că aliasurile nu sunt niciodată dereferenţiate, întotdeauna dereferenţiate, dereferenţiate la căutare sau dereferenţiate doar când se localizează obiectul de bază pentru căutare. Implicit este ca niciodată să nu se diferenţieze alias-urile.

-A
: Extrage doar atributele (fără valori). Aceasta este folositoare când doar vreţi să vedeţi dacă un atribut este prezent într-o intrare şi nu sunteţi interesat de valorile specifice.

-b searchbase
: Folosiţi searchbase ca punct de pornire pentru căutare în locul valorii implicite. Dacă nu este specificat **-b**, acest utilitar va examina variabila de mediu LDAP_BASEDN pentru o definiţie searchbase. Dacă nu este specificat nimic, baza implicită este setată la ″″.

-B
: Nu suprimaţi afişarea valorilor non-ASCII. Aceasta este utilă atunci când lucraţi cu valori care apar în seturi de caractere alternative precum ISO-8859.1. Această opţiune este impusă de opţiunea **-L**.

-C charset
: Specifică faptul că şirurile furnizate ca intrare pentru utilitarul ldapsearch sunt reprezentate într-un set de caractere local (după cum este specificat de charset). Intrarea şir include filtrul, DN-ul de legare şi DN-ul de bază. Similar, când afişaţi date, **ldapsearch** converteşte datele primite de la serverul LDAP la setul de

caractere specificat. Folosiţi opţiunea **-C** *charset* dacă pagina de cod a şirului de intrare este diferită de valoarea de pagină de cod job. Referiţi-vă la API-ul ldap_set_iconv_local_charset() pentru a vedea valorile set de caractere suportate. De asemenea, dacă opţiunile **-C** şi **-L** sunt ambele specificate, intrarea se presupune că este specificată în setul de caractere specificat, dar ieşirea de la **ldapsearch** este mereu păstrată în reprezentarea sa UTF-8 sau o reprezentare codată base-64 a datelor când sunt detectate caractere netipăribile. Aceasta este situaţia dacă fişierele standard LDIF conţin doar reprezentări UTF-8 (sau UTF-8 codat base-64) a datelor şir. Notaţi că valorile suportate pentru charset sunt aceleaşi valori suportate pentru fişa charset care este definită opţional în fişierele LDIF cu Versiunea 1.

-d debuglevel
Setaţi nivelul de depanare LDAP la debuglevel.

-D binddn
Folosiţi binddn pentru legarea la directorul LDAP. binddn ar trebui să fie unDN reprezentat pe şiruri (vedeţi nume distinctive LDAP).

-e Afişaţi informaţiile versiunii bibliotecii LDAP şi apoi ieşiţi.

-F sep Folosiţi sep ca separator de câmp între numele atribut şi valori. Separatorul implicit este `=', doar dacă steguleţul **-L** nu a fost specificat, caz în care această opţiune este ignorată.

-h ldaphost
Specificaţi o gazdă alternativă în care rulează serverul ldap.

-i file Citiţi o serie de linii din fişier, executând o căutare LDAP pentru fiecare linie. În acest caz, filtrul dat în linia de comandă este tratat ca un model unde prima apariţie a %s este înlocuită cu o linie de fişier. Dacă fişierul este un singur caracter ″-″, atunci liniile sunt citite din intrarea standard.

-K keyfile
Specifică nuumele fişierului bază de date de chei SSL. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

Dacă utilitarul nu poate localiza baza de date de chei, va folosi un set hard-coded de rădăcina Autorităţii implicită de certificare de înredere. Fişierul bază de date chei conţine tipic unul au mai multe certificate de autorităţi de certificare (CA) care sunt crezute de client. Aceste tipuri de certificate X.509 sunt de asemenea cunoscute ca rădăcini de încredere.

Acest parametru activează efectiv comutatorul **-Z**. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-l timelimit
Aşteptaţi cel mult secundele specificate în limita de timp pentru terminarea unei căutări.

-L Afişează rezultatele căutării în format LDIF. Această opţiune activează de asemenea opţiunea **-B** şi cauzează opţiunea **-F** să fie ignorată.

-m mechanism
Folosiţi mechanism pentru a specifica mecanismul SASL de folosit pentru legarea la server. Va fi folosit API-ul ldap_sasl_bind_s(). Parametrul **-m** este ignorat dacă este setat **-V 2**. Dacă **-m** nu este specificat, este folosită autentificarea simplă.

-M Gestionează obiecte referal ca intrări obişnuite.

-n Arată ce s-ar face, dar nu modifică efectiv intrările. Folositoare pentru depanare în conjuncţie cu **-v**.

-N certificatename
Specifică eticheta asociată cu certificatul client din fişierul bază de date chei.

Notă: Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. *certificatename* nu este necesar, dacă o pereche cheie privată/certificat a fost desemnată ca implicită. Similar, *certificatename* nu este necesar dacă este o pereche singură cheie privată/certificat în fişierul bază de date chei desemnat. Acest parametru este ignorat dacă nu este

specificat nici **-Z**, nici **-K**.

Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-o *attr_type*

Pentru a sepcifica un atribut de folosit pentru criteriile de sortare a rezultatelor căutării, puteţi folosi parametrul -o (order). Puteţi folosi mai mulţi parametri -o pentru a defini în viitor ordinea de sortare. În exemplul următor, rezultatele de căutare sunt sortate mai întâi după numele de familie (sn), apoi după numele de naştere, cu numele dat (givename) fiind sortat în ordine inversă (descrescătoare) precum a fost specificat de semnul minus predefinit (-):

```
-o sn -o -givenname
```

Astfel, sintaxa parametrului de sortare este după cum urmează:

```
[-]<attribute name>[:<matching rule OID>]
```

unde

- nume atribut este numele atributului după doriţi să sortaţi.
- OID regulă de potrivire este OID-ul opţional al unei reguli de potrivire pe care doriţi să îl folosiţi pentru sortare. Atributul OID al regulii de potrivire nu este suportat de Directory Server, totuşi alte servere LDAP pot suporta acest atribut.
- Semnul minus (-) indică faptul că rezultate trebuie sortate în ordine inversă.
- Starea critică este mereu importantă.

Operaţia implicită ldapsearch nu este de a sorta rezultatele întoarse.

-O maxhops

Specificaţi maxhops pentru a seta numărul maxim de hopuri pe care biblioteca client le foloseşte când urmăreşte referalii. Numărul de hopuri implicit este 10.

-p ldapport

Specificaţi un port TCP alternativ pe care ascultă serverul ldap. Portul LDAP implicit este 389. Dacă nu este specificat şi este specificat -Z, este folosit portul SSL LDAP implicit 636.

-P keyfilepw

Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile criptate din fişierul bazei de date de chei (care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-P** nu este necesar. Acest parametru este ignorat dacă nu sunt specificate **-Z** sau **-K**.

-q *pagesize*

Pentru a specifica paginarea rezultatelor de căutare, pot fi folosiţi 2 parametri: -q (dimensiune pagină de interogare) şi -T (timp între căutări în secunde). În următorul exemplu, rezultatele căutării întoarce o pagină (25 de intrări) la un moment dat, la fiecare 15 secunde, până când toate rezultatele pentru acea căutare sunt întoarse. Clientul ldapsearch tratează toată continuarea de conexiune pentru fiecare cerere de rezultate paginate pentru viaţa operaţiei de căutare.

Aceşti parametri pot fi folositori când clientul are resurse limitate sau când este conectat printr-o conexiune de bandă joasă. În general, vă permite să controlaţi rata la care datele sunt întoarse de o cerere de căutare. În loc să primiţi toate rezultatele o dată, puteţi să obţineţi câteva intrări (o pagină) la un moment dat. În plus, puteţi controla durata întârzierii între fiecare pagină de cerere, dând clientului timp pentru a procesa rezultatele.

```
 -q 25  -T 15
```

Dacă parametrul -v (verbose) este specificat, ldapsearch listează câte intrări au fost întoarse până acum, după fiecare pagină de intrări întoarse de la server, de exemplu, **au fost întoarse 30 de intrări.**

Parametrii multipli -q sunt activaţi pentru a putea specifica diferite dimensiuni de pagină de-a lungul vieţii unei singure operaţii de căutare. În următorul exemplu, prima pagină are 15 intrări, a 2-a are 20 de intrări şi a al 3-lea parametrul termină operaţia paginată de căutare/rezultate.

```
-q 15 -q 20 -q 0
```

În următorul exemplu, prima pagină are 15 de intrări şi restul paginilor au 20 de intrări, continuând cu ultima valoare specificată **-q** până când se completează operaţia de căutare.

```
-q 15 -q 20
```

Operaţia implicită ldapsearch este de a întoarce toate intrările într-o singură cerere. Nici o paginare nu este realizată pentru operaţia implicită ldapsearch.

-R Specifică faptul că referalii nu trebuiesc automat urmaţi.

-s scope
Specifică domeniul căutării. scope ar trebui să fie unul dintre base, one sau sub pentru a specifica un obiect de bază, un nivel 1 sau o căutare de subarbore. Valoare implicită este sub.

-t Scrie valorile extrase într-un set de fişiere temporare. Aceasta este utilă pentru lucrul cu valori non-ASCII cum ar fi jpegPhoto sau audio.

-T *seconde*
Timpul între căutări (în secunde). Opţiunea **-T** este suportată doar când este specificată opţiunea **-q**.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-V Specifică versiunea LDAP de folosit de către ldapmodify când se leagă la serverul LDAP. Implicit, o conexiune V3 LDAP este stabilită. Pentru a selecta explicit LDAP V3, specificaţi ″-V 3″. Specificaţi ″-V 2″ pentru a rula ca o aplicaţie LDAP V2. O aplicaţie, precum ldapmodify, selectează LDAP V3 ca protocol preferat prin folosirea ldap_init în locul ldap_open.

-w *passwd* **| ?**
Folosiţi ***passwd*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă. .

-z sizelimit
Limitaţi rezultatele căutării la intrările care au cel puţin limita de dimensiune. Aceasta face posibil plasarea unei graniţe superioare la numărul de intrări care sunt întoarse pentru o operaţie de căutare.

-Z Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

filter Specifică o reprezentare pe şir a filtrului de aplicare în căutare. Filtrele simple pot fi specificate ca attributetype=attributevalue. Mai multe filtre complexe sunt specificate folosind o notaţie prefix în concordanţă cu următorul Backus Naur Form (BNF):

```
<filter> ::='('<filtercomp>')'
<filtercomp> ::= <and>|<or>|<not>|<simple>
<and> ::= '&' <filterlist>
<or> ::= '|' <filterlist>
<not> ::= '!' <filter>
<filterlist> ::= <filter>|<filter><filterlist>
<simple> ::= <attributetype><filtertype>
<attributevalue>
<filtertype> ::= '='|'~='|'<='|'>='
```

Construcţia '~=' este folosită pentru a specifica potrivirea aproximativă. Reprezentarea pentru <*attributetype*> şi <*attributevalue*> sunt precum în descrierea ″Definiţii sintaxă atribute RFC 2252, LDAP V3″ . În plus, dacă filtertype este '=' atunci <*attributevalue*> poate fi un singur * pentru a realiza un test de existenţă atribut sau poate conţine text şi asterisc(*) împrăştiat pentru realiza o potrivire de subşir.

De exemplu, filtrul ″mail=*″ găseşte orice intrare care are un atribut mail. Filtrul ″mail=*@student.of.life.edu″ găseşte orice intrare care are un atribut mail care se termină cu şirul specificat. Pentru a pune paranteze într-un filtru, însoţiţi-le cu un caracter backslash (\).

Notă: Un filtru ca "cn=Bob *", unde există un spaţiu între Bob şi asterisc (*), se potriveşte cu ″Bob Carter″ dar nu cu ″Bobby Carter″ din Directorul IBM. Spaţiul dintre ″Bob″ şi caracterul wildcard (*) afectează rezultatul unei căutări folosind filtre.

Vedeţi ″RFC 2254, Oreprezentare şir a filtrelor de căutare LDAP  pentru o descriere mai completă a filtrelor permisibile.

Format rezultat

Dacă una sau mai multe intrări sunt găsite, fiecare intrare este scrisă la rezultatul standard în formatul:

```
Nume distinctiv (DN)

attributename=value

attributename=value

attributename=value

...
```

Intrările multiple sunt separate cu o singură linie goală. Dacă opţiunea **-F** este folosită pentru a specifica un caracter separator, va fi folosită în locul caracterului `=’. Dacă este folosită opţiunea **-t**, numele fişierului temporar este folosit în locul valorii actuale. Dacă este dată opţiunea **-A**, este scrisă doar partea ″attributename″.

Exemple

Următoarea comandă:

```
ldapsearch "cn=john doe" cn telephoneNumber
```

execută o căutare de subarbore (folosind baza de căutare implicită) pentru intrările cu un commonName de ″john doe″. Valorile commonName şi telephoneNumber sunt extrase şi tipărite în ieşirea standard. Ieşirea ar putea arăta astfel dacă sunt găsite 2 intrări:

```
  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
```

Comanda:

```
ldapsearch -t "uid=jed" jpegPhoto audio
```

execută o căutare de subarbore (folosind baza de căutare implicită) pentru intrările cu un id de ″jed″. Valorile jpegPhoto şi audio sunt extrase şi scrise în fişiere temporare. Ieşirea poate arăta astfel dacă se găsesşte una dintre intrări a fi o valoare pentru fiecare dintre atributele cerute:

```
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
```

Comanda:

```
ldapsearch -L -s one -b "c=US" "o=university*" o descriere
```

execută o căutare de un nivel la nivelul c=US pentru toate organizaţiile a căror organizationName începe cu University. Rezultatele de căutare vor fi afişate în formatul LDIF (vedeţi Format de interschimbare date LDAP). Valorile atribut organizationName şi descriere vor fi extrase şi tipărite la ieşirea standard, rezultând în ieşire similară cu aceasta:

```
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
```

...

Comanda:

```
ldapsearch -b "c=US" -o ibm-slapdDN "objectclass=person" ibm-slapdDN
```

execută o căutare de un nivel subarbore la nivelul c=US pentru toate persoanele. Acest atribut special (ibm-slapdDN), când este folosit pentru căutări sortate, sortează rezultatele căutării după reprezentarea şir a numelui distinctiv (DN). Ieşirea poate arăta astfel:

```
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
```

Comanda:

```
ldapsearch –h hostname –o sn –b "o=ibm,c=us" "title=engineer"
```

întoarce toate intrările dintr-un director de angajaţi IBM al cărui titlu este ″engineer″, cu rezultatele sortate după numele de familie.

Comanda:

```
ldapsearch –h hostname –o -sn –o cn –b "o=ibm,c=us" "title=engineer"
```

întoarce toate intrările dintr-un director de angajaţi IBM al cărui titlu este ″engineer″, cu rezultatele sortate după numele de familie (în ordine descrescătoare) şi apoi după prenumele (în ordine crescătoare).

Comanda:

```
ldapsearch –h hostname –q 5 –T 3 –b o=ibm,c=us "title=engineer"
```

întoarce 5 intrări per pagină, cu o întârziere de 3 secunde între pagini pentru toate intrările dintr-un director de angajaţi IBM al cărui titlu este ″engineer″.

Acest exemplu demonstrează căutările unde un obiect referal este implicat. Aşa cum s-a discutat în “Referalii directorului LDAP” la pagina 40, directoarele Directory Server LDAP pot conţine obiecte referral cu condiţia să conţină doar următoarele:

- Un nume distinctiv (dn).
- O clasă de obiect (objectClass).
- Un atribut referal (ref).

Se presupune că ’System_A’ deţine intrarea de referal:

```
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
```

Toate atributele asociate cu intrarea ar trebui să existe pe ’System_B’.

System_B conţine o intrare:

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

Când un client emite o cerere la ’System_A’, serverul LDAP de pe System_A răspunde clientului cu URL:

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

Clientul foloseşte aceste informaţii pentru a emite o cerere la System_B. Dacă intrarea de pe System_A conţine atribute suplimentare la dn, objectclass şi ref, serverul ignoră acele atribute (doar dacă specificaţi steguleţul **-R** pentru a indica să nu se urmărească referalii).

Când clientul primeşte un răspuns referal de la un server, acesta emite cererea din nou, de această dată server-ului la care se referă URL-urile returnate. Noua cerere are acelaşi domeniu ca cererea originală. Rezultatele acestei căutări variază depinzând de valoarea pe care o specificaţi pentru domeniul căutării (**-b**).

Dacă specificaţi -s base, după cum este arătat aici:

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

căutarea întoarce toate atributele pentru toate intrările cu ’sn=Jensen’ care există în ’ou=Rochester, o=Big Company, c=US’ pe ambele sisteme System_A şi System_B.

Dacă specificaţi -s sub, cum se arată aici:

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

căutarea întoarce toate atributele pentru toate intrările cu ’sn=Jensen’ care există în sau mai jos de ’ou=Rochester, o=Big Company, c=US’ pe ambele sisteme System_A şi System_B.

Dacă specificaţi -s one, cum se arată aici:

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

căutarea nu întoarce vreo valoare pe acel sistem. În schimb, serverul întoarce clientului URL-ul referal:

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

Clientul în schimb lansează o cerere:

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

Aceasta nu dă nici un rezultat, pentru că intrarea

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
```

se află la

```
ou=Rochester, o=Big Company, c=US
```

O căutare cu -s one încearcă să găsească intrări în nivelul imediat de jos.

```
ou=Rochester, o=Big Company, c=US
```

Diagnostice

Starea de ieşire este 0 dacă nu apar erori. Rezultatele de eroare dintr-o stare de ieşire non-zero şi un mesaj diagnostic au fost scrise la eroarea standard.

ldapchangepwd

Unealta de modificare parolă LDAP.

Sinopsis

```
ldapchangepwd -D binddn -w passwd | ? -n newpassword | ?
[-C charset] [-d debuglevel][-h ldaphost] [-K keyfile]
[-m mechanism] [-M]  [-N certificatename] [-O maxhops]
[-p ldapport] [-P keyfilepw]  [-R] [-v] [-V version]
[-Z] [-?]
```

Descriere

Trimite cereri de modificare parolă unui server LDAP. Permite parolei pentru o intrare director să fie modificată.

Opţiuni

-C *charset*
: Specifică faptul că DN-urile furnizate ca intrare la utilitarul **ldapdelete** sunt reprezentate într-un set de caractere local, precum este specificat în setul de caractere. Folosiţi opţiunea **-C** *charset* dacă pagina de cod a şirului de intrare este diferită de valoarea de pagină de cod job. Referiţi-vă la API-ul ldap_set_iconv_local_charset() pentru a vedea valorile set de caractere suportate.

-d *debuglevel*
: Setaţi nivelul de depanare LDAP la debuglevel.

-D*binddn*
: Folosiţi ***binddn*** pentru a lega la directorul LDAP. ***binddn*** este un DN reprezentat pe şiruri.

-h*ldaphost*
: Specificaţi o gazdă alternativă în care rulează serverul ldap.

-K*keyfile*
: Specifică nuumele fişierului bază de date de chei SSL. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

  Dacă utilitarul nu poate localiza baza de date de chei, va folosi un set hard-coded de rădăcina Autorităţii implicită de certificare de înredere. Fişierul bază de date chei conţine tipic unul au mai multe certificate de autorităţi de certificare (CA) care sunt crezute de client. Aceste tipuri de certificate X.509 sunt de asemenea cunoscute ca rădăcini de încredere.

  Acest parametru activează efectiv comutatorul **-Z**. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-m*mechanism*
: Folosiţi ***mechanism*** pentru a specifica mecanismul SASL de folosit pentru legarea la server. Va fi folosit API-ul ldap_sasl_bind_s(). Parametrul **-m** este ignorat dacă este setat **-V 2**. Dacă **-m** nu este specificat, este folosită autentificarea simplă.

-M Gestionează obiecte referal ca intrări obişnuite.

-n *newpassword* **| ?**
: Specifică noua parolă. Folosiţi ? pentru a genera un prompt de parolă.

-N*certificatename*

Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. ***certificatename*** nu este necesar, dacă o pereche cheie privată/certificat a fost desemnată ca implicită. Similar, ***certificatename*** nu este necesar dacă este o pereche singură cheie privată/certificat în fişierul bază de date chei desemnat. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-O *maxhops*

Specificaţi ***maxhops*** pentru a seta numărul maxim de hop-uri pe care le obţine biblioteca client când se urmăresc acreditările. Numărul de hop-uri implicit este 10.

-p *ldapport*

Specificaţi un port TCP alternativ pe care ascultă serverul ldap. Portul LDAP implicit este 389. Dacă **-p** nu este specifcat şi **-Z** este specificat, este folosit portul implicit SSL LDAP.

-P*keyfilepw*

Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile cifrate din fişierul bazei de date, care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-P** nu este necesar. Acest parametru este ignorat dacă nu sunt specificate **-Z** sau **-K**.

-R Specifică faptul că referalii nu trebuiesc automat urmaţi.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-V *versiune*

Specifică versiunea LDAP de folosit de către **ldapdchangepwd** când se leagă la serverul LDAP. Implicit, o conexiune V3 LDAP este stabilită. Pentru a selecta explicit LDAP V3, specificaţi **-V 3**. Specificaţi **-V 2** pentru a rula ca aplicaţie LDAP V2. O aplicaţie, ca **ldapdchangepwd**, selectează LDAP V3 ca protocol preferat folosind ldap_init în loc de ldap_open.

-w *passwd* **| ?**

Folosiţi ***passwd*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

-Z Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Pentru Directory Server din i5/OS dacă folosiţi -Z şi nu folosiţi -K sau -N, va fi folosit certificatul asociat cu ID-ul de aplicaţie Directory Services Client.

-? Afişează ajutorul sintaxei pentru ldapchangepwd.

Exemple

Următoarea comandă,

```
ldapchangepwd -D cn=John Doe -w a1b2c3d4 -n wxyz9876
```

modifică parola pentru intrarea cu numele commonName ″John Doe″ din a1b2c3d4 la wxyz9876

Diagnostice

Starea de ieşire este 0 dacă nu apar erori. Rezultatele de eroare dintr-o stare de ieşire non-zero şi un mesaj diagnostic au fost scrise la eroarea standard.

ldapdiff

Unealta de sincronizare replică LDAP.

Notă: Această comandă poate rula pentru o perioadă îndelungată în funcţie de numărul de intrări (şi atributele pentru acele intrări) care sunt replicate.

Sinopsis

(Compară şi sincronizează intrările de date între 2 servere dintr-un mediu de replicare).

```
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]
```

sau

(Compară schema între 2 servere).

```
 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]
```

Descriere

Această unealtă sincronizează un server replică cu masterul său. Pentru a afişa ajutorul de sintaxă pentru **ldapdiff**, introduceţi:

```
ldapdiff -?
```

Opţiuni

Următoarele opţiuni se aplică la comanda **ldapdiff**. Există 2 subgrupuri care se aplică specific fie la serverul furnizor fie la cel consumator.

-a Specifică să folosiţi controlul administrare server pentru scrieri la o replică numai citire.

-b *baseDN*
Folosiţi searchbase ca punct de pornire pentru căutare în locul valorii implicite. Dacă nu este specificat **-b**, acest utilitar examinează variabila de mediu LDAP_BASEDN pentru o definiţie searchbase.

-C *countnumber*
Numără numărul de intrări de corectat. Dacă sunt găsite mai multe nepotriviri decât numărul specificat, unealta există.

-F Aceasta este opţiunea de corectare. Dacă este specificată, conţinutul din replica consumator este modificat pentru a se potrivi cu cel al serverului furnizor. Aceasta nu poate fi folosită dacă este specificată de asemenea **-S**.

-L Dacă opţiunea **-F** nu este specificată, folosiţi această opţiune pentru a genera un fişier LDIF pentru ieşire. Fişierul LDIF poate fi folosit pentru a actualiza consumatorul să elimine diferenţele.

-S Specifică să se compare schema pe ambele servere.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

Opţiuni pentru un furnizor de replicare

Următoarele opţiuni se aplică serverului consumator şi denotă dintr-un ’s’ iniţial în numele opţiunii.

-sD *dn* Folosiţi ***dn*** pentru legarea la directorul LDAP. ***dn*** este un DN reprezentat pe şiruri.

-sh *host*
Specifică numele gazdă.

-sK *keyStore*
Specificaţi numele fişierului bază de date de chei SSL cu extensia implicită **kdb**. Dacă acest parametru nu este

specificat sau valoarea este un şir gol, sistemul este un şir gol. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

-sN *keyLabel*
Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Dacă este specificată o etichetă fără specificarea unui depozit de chei (keystore), eticheta este un identificator de aplicaţie din DCM (Digital Certificate Manager). Eticheta implicită (id aplicaţie) este QIBM_GLD_DIRSRV_CLIENT. Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client este necesară. ***keyLabel*** nu este necesar dacă a fost desemnată o pereche implicită certificat/cheie privată. Similar, ***keyLabel*** nu este necesar dacă există o singură pereche certificat/cheie privată în fişierul bază de date cheie desemnat. Acest parametru este ignorat dacă nu sunt specificate **-sZ** sau **-sK**.

-sp *ldapport*
Specificaţi un port TCP alternativ pe care ascultă serverul ldap. Portul LDAP implicit este 389. Dacă **-sp** nu este specifcat şi **-sZ** este specificat, este folosit portul implicit SSL LDAP.

-sP *keyStorePwd*
Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile cifrate din fişierul bazei de date, care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-sP** nu este necesar. Acest parametru este ignorat dacă nu sunt specificate **-sZ** sau **-sK**. Parola nu este folosită dacă există un fişier stash pentru depozitul de chei folosit.

-st *trustStoreType*
Specificaţi eticheta asociată cu certificatul client din fişierul bază de date de încredere. Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. ***trustStoreType*** nu este necesar dacă a fost desemnată o pereche implicită certificat/cheie privată. Similar, ***trustStoreType*** nu este necesar dacă există o singură pereche certificat/cheie privată în fişierul bază de date cheie desemnat. Acest parametru este ignorat dacă nu sunt specificate **-sZ** sau **-sT**.

-sZ Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP.

Opţiuni pentru un consumator de replicare

Următoarele opţiuni se aplică serverului consumator şi denotă dintr-un ’c’ iniţial în numele opţiunii. Pentru uşurinţă, dacă este specificat -cZ fără a specifica valori pentru -cK, -cN sau -cP, aceste opţiuni folosesc aceeaşi valoare specificată pentru opţiunile SSL ale furnizorului. Pentru suprascrie opţiunile furnizorului şi pentru a folosi setările implicite, specificaţi -cK ″″ -cN ″″ -cP ″″.

-cD *dn* Folosiţi ***dn*** pentru legarea la directorul LDAP. ***dn*** este un DN reprezentat pe şiruri.

-ch *host*
Specifică numele gazdă.

-cK *keyStore*
Specificaţi numele fişierului bază de date de chei SSL cu extensia implicită kdb. Dacă valoarea este un şir gol, sistemul este un şir gol. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

-cN *keyLabel*
Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă este specificată o etichetă fără specificarea unui depozit de chei (keystore), eticheta este un identificator de aplicaţie din DCM (Digital Certificate Manager). Eticheta implicită (id aplicaţie) este QIBM_GLD_DIRSRV_CLIENT. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client este necesară. ***keyLabel*** nu este necesar dacă a fost desemnată o pereche implicită certificat/cheie privată. Similar, ***keyLabel*** nu este necesar dacă există o singură pereche certificat/cheie privată în fişierul bază de date cheie desemnat. Acest parametru este ignorat dacă nu sunt specificate **-cZ** sau **-cK**.

-cp *ldapport*
Specificaţi un port TCP alternativ pe care ascultă serverul ldap. Portul LDAP implicit este 389. Dacă **-cp** nu este specifcat şi **-cZ** este specificat, este folosit portul implicit SSL LDAP.

-cP *keyStorePwd*
Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile cifrate din fişierul bazei de date, care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-cP** nu este necesar. Acest parametru este ignorat dacă nu sunt specificate **-cZ** sau **-cK**.

-cw *password* **| ?**
Folosiţi ***password*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

-cZ Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP.

Exemple

```
ldapdiff -b <baseDN> -sh
<supplierhostname> -ch
<consumerhostname> [options]
```

sau

```
ldapdiff -S  -sh <supplierhostname> -ch
<consumerhostname> [options]
```

Diagnostice

Starea de ieşire este 0 dacă nu apar erori. Rezultatele de eroare dintr-o stare de ieşire non-zero şi un mesaj diagnostic au fost scrise la eroarea standard.

Note despre folosirea SSL cu utilitarele liniei de comandă LDAP

Pentru a folosi caracteristicele Secure Sockets Layer (SSL) ale utilitarelor liniei de comandă, trebuie să aveţi instalat unul din produsele Cryptographic Access Provider (5722-ACx).

"SSL (Secure Sockets Layer) şi TLS (Transport Layer Security) cu Directory Server" la pagina 41 discuţii folosind SSL cu serverul Directory Server LDAP. Această informaţie include gestionarea şi crearea Autorităţilor de certificare (CA) de încredere cu Digital Certificate Manager.

Unele din serverele LDAP accesate de client folosesc doar autentificarea server. Pentru aceste servere, aveţi nevoie doar să definiţi unul sau mai multe certificate rădăcină de încredere în memoria de certificate. Cu autentificarea server, clientul poate fi asigurat că serverul LDAP destinaţie a emis un certificat de de către unul din Autorităţi de certificare de încredere (CA-uri). În plus, toate tranzacţiile LDAP care trec prin conexiunea SSL cu serverul sunt cifrate. Aceasta include acreditări LDAP care sunt livrate pe API-uri care sunt folosite pentru a lega la serverul de directoare. De exemplu, dacă serverul LDAP foloseşte un certificat de mare siguranţă Verisign, ar trebui să faceţi una din următoarele:
1. Obţineţi un certificat CA de la Verisign.
2. Folosiţi DCM pentru a-l importa în memoria de certificate.
3. Folosiţi DCM pentru a-l marca ca de încredere.

Dacă serverul LDAP foloseşte un certificat server emis privat, administratorul serverelor vă poate livra o copie a fişierului cerut de certificatele serverului. Importaţi fişierul cerut de certificat în memoria de certificat şi marcaţi-o ca de încredere.

Dacă folosiţi utilitarele shell pentru a accesa serverele LDAP care folosesc şi autentificarea client şi server trebuie să faci următoarele:

- Definiţi unul sau mai multe certificate rădăcină de încredere în memoria sistem de certificate. Aceasta permite clientului să fie asigurat că serverul LDAP destinaţie a fost asigurat cu un certificat de unul din CA-urile de încredere. În plus, toate tranzacţiile LDAP care trec prin conexiunea SSL cu serverul sunt cifrate. Aceasta include acreditări LDAP care sunt livrate pe API-uri care sunt folosite pentru a lega la serverul de directoare.

- Creaţi o pereche de chei şi cereţi un certificat client de la o CA. După primirea certificatului semnat de la CA, primiţi certificatul în fişierul inel de de chei pe client.

LDIF (LDAP Data Interchange Format)

Această documentaţie descrie formatul LDIF (LDAP Data Interchange Format), aşa cum este folosit de utilitarele ldapmodify, ldapsearch şi ldapadd. Formatul LDIF specificat aici este de asemenea suportat de către utilitarele server furnizate cu IBM Directory.

LDIF este folosit pentru a reprezenta intrările LDAP în format text. Forma de bază a unei intrări LDIF este:

```
dn: <distinguished name>
<attrtype> : <attrvalue>
<attrtype> : <attrvalue>
...
```

O linie poate fi continuată prin începerea liniei următoare cu un singur caracter spaţiu sau tab, de exemplu:

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

Sunt specificate valori atribut multiple pe linii separate, de exemplu:

```
cn: John E Doe
cn: John Doe
```

Dacă un <*attrvalue*> conţine un caracter non-US-ASCII sau începe cu un spaţiu sau două puncte ':', atunci <*attrtype*> este urmat de două caractere două puncte şi valoarea este codificată în notaţia base-64. De exemplu, valoarea ″ începe cu spaţiu″ ar fi codificată astfel:

```
cn:: IGJlZ2lucyB3aXRoIGEgc3BhY2U=
```

Intrările multiple din cadrul aceluiaşi fişier LDIF sunt separate de o linie goală. Liniile multiple goale sunt considerate sfârşitul logic al fişierului.

Pentru informaţii suplimentare, vedeţi următoarele:

- "Exemplu LDIF"
- "Suport LDIF Versiunea 1" la pagina 185
- "Exemple LDIF Versiunea 1" la pagina 185

Exemplu LDIF

Acesta este un examplu de fişier LDIF conţinând trei intrări.

```
dn: cn=John E Doe, o=University of High
 er Learning, c=US
cn: John E Doe
cn: John Doe
objectclass: person
sn: Doe

dn: cn=Bjorn L Doe, o=University of High
 er Learning, c=US
cn: Bjorn L Doe
cn: Bjorn Doe
objectclass: person
sn: Doe

dn: cn=Jennifer K. Doe, o=University of High
 er Learning, c=US
cn: Jennifer K. Doe
cn: Jennifer Doe
objectclass: person
sn: Doe
```

```
jpegPhoto:: /9j/4AAQSkZJRgABAAAAAQABAAD/2wBDABALD
 A4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQ
 ERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARESEhgVG
...
```

jpegPhoto din intrarea lui Jennifer Jensen este codificată folosind base-64. Valorile atributului textual pot fi de asemenea specificate în formatul base-64. Totuşi, dacă este cazul, codificarea base-64 trebuie să fie în pagina de cod a formatului fir pentru protocol (adică, pentu LDAP V2, setul de caractere IA5 şi pentru LDAP V3, codificarea UTF-8).

Suport LDIF Versiunea 1

Utilitarele client (ldapmodify şi ldapadd) au fost îmbunătăţite ca să recunoască cea mai recentă versiune de LDIF, care este identificată de prezenţa marcajului ″version: 1″ la începutul fişierului. Spre deosebire de versiunea originală LDIF, versiunea mai nouă de LDIF suportă valori de atribute reprezentată în UTF-8 (în loc de setul limitat US-ASCII).

Totuşi, crearea manuală a unui fişier LDIF care conţine valori UTF-8 poate fi dificilă. Pentru a simplifica acest proces, este suportată o extensie a setului de caractere pentru formatul LDIF. Această extensie permite specificarea unui nume de set de caractere IANA în antetul fişierului LDIF (alături de numărul de versiune). Este suportat un set limitat de caractere IANA.

Versiunea 1 a formatului LDIF suportă de asemenea URL-uri de fişier. Aceasta oferă un mod mai flexibil de a defini specificaţia unui fişier. URL-urile fişier iau următoarea formă:

```
attribute:< file:///path          (unde sintaxa căii depinde de platformă)
```

De exemplu, următoarele sunt adrese web de fişiere valide:

```
jpegphoto:< file:///d:\temp\photos\myphoto.jpg    (căi stil
DOS/Windows)
jpegphoto:< file:///etc/temp/photos/myphoto.jpg   (căi stil Unix)
```

Notă: Utilitarele IBM Directory suportă atât noua specificaţie de URL fişier cât şi stilul mai vechi (″jpegphoto: /etc/temp/myphoto″), indiferent de specificaţia versiunii. Cu alte cuvinte, noul format de URL fişier poate fi folosit fără a adăuga eticheta de versiune la fişierele dvs. LDIF.

Exemple LDIF Versiunea 1

Puteţi folosi marcajul opţional de set de caractere astfel încât utilitarele vor converti automat de la setul de caractere specificat la UTF-8 ca în următorul exemplu:

```
version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, o=University of New Mexico, c=US
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd
title: Associate Dean
title: [title in Spanish]
jpegPhoto:> file:///usr/local/photos/jgriego.jpg
```

În această instanţă, toate valorile care urmează unui nume de atribut şi după un singur caracter două puncte sunt translatate de la setul de caractere ISO-8859-1 la UTF-8. Valorile care urmează unui nume de atribut şi după două caractere două puncte (precum description:: V2hhdCBhIGNhcm...) trebuie să fie codificate în base-64 şi se aşteaptă să fie ori binare ori şiruri de caractere UTF-8. Valorile citite dintr-un fişier precum atributul jpegPhoto specificat de adresa web din exemplul anterior, se aşteaptă de asemenea să fie ori binare, ori UTF-8. Nu este făcută nici o translaţie de la ″charset″-ul specificat la UTF-8 pentru acele valori.

În acest exemplu de fişier LDIF fără eticheta de set de caractere, conţinutul se aşteaptă să fie în UTF-8 sau base-64 codificat UTF-8 sau date binare codificate base-64.

```
# IBM Directorysample LDIF file
 #
 # Sufixul "o=IBM, c=US" ar trebui să fie definit înainte de a încerca
să încărcaţi
 # aceste date.

 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
```

Acest fişier poate fi folosit fără informaţia antet version: 1, ca în ediţiile anterioare ale IBM Directory:

```
 # IBM Directorysample LDIF file
 #
 # Sufixul "o=IBM, c=US" ar trebui să fie definit înainte de a încerca
să încărcaţi
 # aceste date.

 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
```

Notă: Valorile atributului textual pot fi specificate în formatul base-64.

Schema de configurare Directory Server

Aceste informaţii descriu Directory Information Tree (DIT) şi atributele care sunt folosite pentru a configura fişierul ibmslapd.conf. În ediţiile anterioare setările de configurare director erau stocate într-un format proprietar în fişierul de configurare. Setările director sunt stocate acum folosind formatul LDIF în fişierul de configurare.

Fişierul de configurare este denumit ibmslapd.conf. Schema folosită de fişierul de configurare este de asemenea disponibilă acum. Tipurile de atribute pot fi găsite în fişierul v3.config.at şi clasele de obiecte sunt în fişierul v3.config.oc. Atributele pot fi modificate folosind comanda ldapmodify. Pentru mai multe informaţii despre comanda ldapmodify, vedeţi “ldapmodify şi ldapadd” la pagina 159.

- “Arbore informaţii director”
- “Atribute” la pagina 196

Arbore informaţii director

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

Descriere

Aceasta este intrarea de pe nivelul de sus din DIT-ul de configurare. Ea păstrează date de interes global pentru server, deşi în practică ea conţine de asemenea diverse elemente. Fiecare atribut din această intrare vine prima secţiune (global stanza) a ibmslapd.conf.

Număr

1 (necesar)

Clasă Obiect

ibm-slapdTop

Atribute obligatorii

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

Atribute opţionale

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (Deprecated)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion

cn=Admin

DN cn=Admin, cn=Configuration

Descriere
Setări de configurare globală pentru IBM Admin Daemon

Număr
1 (necesar)

Clasă Obiect
ibm-slapdAdmin

Atribute obligatorii
- cn
- ibm-slapdErrorLog
- ibm-slapdPort

Atribute opţionale
- ibm-slapdSecurePort

cn=Event Notification

DN cn=Event Notification, cn=Configuration

Descriere
Setările globale de notificare evenimente pentru Directory Server

Număr
0 sau 1 (opţional; necesar doar dacă vreţi să activaţi notificarea evenimentelor)

Clasă Obiect
ibm-slapdEventNotification

Atribute obligatorii
- cn
- ibm-slapdEnableEventNotification
- objectClass

Atribute opţionale
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

cn=Front End

DN cn=Front End, cn=Configuration

Descriere
Setările globale de mediu pe care serverul le aplică la pornire.

Număr
0 sa 1 (opţional)

Clasă Obiect
ibm-slapdFrontEnd

Atribute obligatorii
- cn
- objectClass

Atribute opţionale
- 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

Descriere
Setările globale de autentificare Kerberos pentru Directory Server.

Număr
0 sa 1 (opţional)

Clasă Obiect
ibm-slapdKerberos

Atribute obligatorii

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

Atribute opţionale

- Nimic

cn=Master Server

DN cn=Master Server, cn=Configuration

Descriere
Când configuraţi o replică, această intrare păstrează acreditările de legare şi URL-ul referal al serverului master.

Număr
0 sa 1 (opţional)

Clasă Obiect
ibm-slapdReplication

Atribute obligatorii

- cn
- ibm-slapdMasterPW (Obligatoriu dacă nu folosiţi autentificare Kerberos.)

Atribute opţionale

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Opţional dacă folosiţi autentificare Kerberos.)
- ibm-slapdMasterReferral
- objectClass

cn=Referral

DN cn=Referral, cn=Configuration

Descriere

Această intrare conţine toate intrările referal din prima secţiune (global stanza) a ibmslapd.conf. Dacă nu există referali (nu există nici unul în mod implicit), această intrare este opţională.

Număr

0 sau 1 (opţional)

Clasă Obiect

ibm-slapdReferral

Atribute obligatorii

- cn
- ibm-slapdReferral
- objectClass

Atribute opţionale

- Nimic

cn=Schemas

DN cn=Schemas, cn=Configuration

Descriere

Această intrare serveşte drept container pentru scheme. Acestă intrare nu este cu adevărat necesară deoarece schemele pot fi distinse după clasa de obiecte ibm-slapdSchema. Este inclusă pentru a îmbunătăţi lizibilitatea DIT.

Doar o intrare schemă este permisă în prezent: cn=IBM Directory.

Număr

1 (necesar)

Clasă Obiect

Container

Atribute obligatorii

- cn
- objectClass

Atribute opţionale

- Nimic

cn=IBM Directory

DN cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere

Această intrare conţine toate datele de configurare schemă din prima secţiune (global stanza) a ibmslapd.conf. Ea serveşte de asemenea drept container pentru toate backend-urile care folosesc schema. Schemele multiple nu sunt suportate în prezent, dar dacă ar fi fost, atunci ar fi fost câte o intrare ibm-slapdSchema per schemă. Notaţi că schemele multiple se presupune că sunt incompatibile. Aşadar, un backend poate fi asociat doar cu o singură schemă.

Număr

1 (necesar)

Clasă Obiect

ibm-slapdSchema

Atribute obligatorii

- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

Atribute opţionale

- ibm-slapdSchemaAdditions

cn=Config Backends

DN cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere

Această intrare serveşte drept container pentru backend-urile Config.

Număr

1 (necesar)

Clasă Obiect

Container

Atribute obligatorii

- cn
- objectClass

Atribute opţionale

Nimic

cn=ConfigDB

DN cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere

Backend configuraţie pentru configuraţia IBM Directory Server

Număr

0 - n (opţional)

Clasă Obiect

ibm-slapdConfigBackend

Atribute obligatorii

- ibm-slapdSuffix
- ibm-slapdPlugin

Atribute opţionale

- ibm-slapdReadOnly

cn=RDBM Backends

DN cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere

Această intrare serveşte drept container pentru backend-urile RDBM. Ea înlocuieşte efectiv linia rdbm din baza de date din ibmslapd.conf prin identificarea tuturor subintrărilor ca backend-uri DB2. Acestă intrare nu este cu adevărat necesară deoarece backend-urile RDBM pot fi distinse după clasa de obiecte ibm-slapdRdbmBackend. Este inclusă pentru a îmbunătăţi lizibilitatea DIT.

Număr

0 sa 1 (opţional)

Clasă Obiect
Container

Atribute obligatorii

- cn
- objectClass

Atribute opţionale

- Nimic

cn=Directory

DN cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere
Această intrare conţine toate setările de configurare baze de date pentru backend-ul implicit baze de date RDBM.

Deşi pot fi create mai multe backend-uri cu nume arbitrare, Server Administration presupune că ″cn=Directory″ este principalul backend director şi că ″cn=Change Log″ este backend-ul changelog opţional. Doar sufixele afişate în ″cn=Directory″ sunt configurabile prin Server Administration (cu excepţia sufixului changelog, care este setat transparent prin activarea changelog).

Număr
0 - n (opţional)

Clasă Obiect
ibm-slapdRdbmBackend

Atribute obligatorii

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Atribute opţionale

- 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

Notă: Dacă folosiţi **ibm-slapdUseProcessIdPw**, trebuie să modificaţi schema pentru a face **ibm-slapdDbUserPW** opţional.

cn=Change Log

DN cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere

Această intrare conţine toate setările de configurare baze de date pentru backend-ul de istoric de modificări.

Număr

0 - n (opţional)

Clasă Obiect

ibm-slapdRdbmBackend

Atribute obligatorii

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Atribute opţionale

- 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

Notă: Dacă folosiţi **ibm-slapdUseProcessIdPw**, trebuie să modificaţi schema pentru a face **ibm-slapdDbUserPW** opţional.

cn=LDCF Backends

DN cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere

Această intrare serveşte drept container pentru backend-urile LDCF. Ea înlocuieşte efectiv linia ldcf bază de date din ibmslapd.conf prin identificarea tuturor subintrărilor drept backend-uri LDCF. Acestă

intrare nu este cu adevărat necesară deoarece backend-urile LDCF pot fi distinse după clasa de obiecte ibm-slapdLdcfBackend. Este inclusă pentru a îmbunătăţi lizibilitatea DIT.

Număr
1 (necesar)

Clasă Obiect
Container

Atribute obligatorii
- cn
- objectClass

Atribute opţionale
- ibm-slapdPlugin

cn=SchemaDB

DN cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere
Această intrare conţine toate datele de configurare bază de date din prima secţiune a ibmslapd.conf.

Număr
1 (necesar)

Clasă Obiect
ibm-slapdLdcfBackend

Atribute obligatorii
- cn
- objectClass

Atribute opţionale
- ibm-slapdPlugin
- ibm-slapdSuffix

cn=SSL

DN cn=SSL, cn=Configuration

Descriere
Setări globale de conexiune SSL pentru Directory Server.

Număr
0 sau 1 (opţional)

Clasă Obiect
ibm-slapdSSL

Atribute obligatorii
- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

Atribute opţionale
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

Notă: **ibm-slapdSslCipherSpecs** este acum depreciat. Folosiţi în schimb **ibm-slapdSslCipherSpec** . Dacă folosiţi **ibm-slapdSslCipherSpecs**, serverul va converti la atributul suportat.

- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW

cn=CRL

DN cn=CRL, cn=SSL, cn=Configuration

Descriere

Această intrare conţine datele de listă revocare certificat din prima secţiune (global stanza) a ibmslapd.conf. Este necesar doar dacă ″ibm-slapdSslAuth = serverclientauth″ din intrarea cn=SSL şi certificatele client au fost emise pentru validarea CRL.

Număr

0 sa 1 (opţional)

Clasă Obiect

ibm-slapdCRL

Atribute obligatorii

- cn
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPort
- objectClass

Atribute opţionale

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword

cn=Transaction

DN cn = Transaction, cn = Configuration

Descriere

Specifică setările globale de suport tranzacţie. Suportul de tranzacţie este oferit folosind plug-in-ul:

```
extendedop /QSYS.LIB/QGLDTRANEX.SRVPGM tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

Serverul (**slapd**) încarcă acest plugin automat la pornire dacă **ibm-slapdTransactionEnable = TRUE**. Pluginul nu necesită să fie adăugat explicit la **ibmslapd.conf**.

Număr

0 sau 1 (opţional; necesar doar dacă vreţi să folosiţi tranzacţii.)

Clasă Obiect

ibm-slapdTransaction

Atribute obligatorii

- cn
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

Atribute opţionale

- Nimic

Atribute

- cn
- ibm-slapdACIMechanism
- ibm-slapdACLAccess
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConcurrentRW
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdEnableEventNotification
- ibm-slapdEntryCacheSize
- ibm-slapdErrorLog
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword
- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdMasterDN
- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions

- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplDbConns
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSuffix
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTransactionEnable
- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- objectClass

cn

Descriere
Acesta este atributul X.500 common Name, care conţine un nume de obiect.

Sintaxă
Şir director

Lungime maximă
256

Valoare
Multi-valoric

ibm-slapdACIMechanism

Descriere

Determină ce model ACL foloseşte serverul. (Suportat doar pe i5/OS începând cu v3.2, ignorat pe alte platforme.)

- 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

Implicit

1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL model

Sintaxă

Şir director

Lungime maximă

256

Valoare

Multi-valoric

ibm-slapdACLAccess

Descriere

Controlează dacă este activat accesul la ACL-uri. Dacă este setat pe TRUE, accesul la ACL-uri este activat. Dacă este setat pe FALSE, accesul la ACL-uri este dezactivat.

Implicit

TRUE

Sintaxă

Boolean

Lungime maximă

5

Valoare

Valoare singulară

ibm-slapdACLCache

Descriere

Controlează dacă serverul stochează sau nu în cache informaţiile ACL.

- Dacă este setat pe TRUE, serverul memorează în cache informaţiile ACL.
- Dacă este setat pe FALSE, serverul nu memorează în cache informaţiile ACL.

Implicit

TRUE

Sintaxă

Boolean

Lungime maximă

5

Valoare

Valoare singulară

ibm-slapdACLCacheSize

Descriere

Numărul maxim de intrări de păstrat în cache-ul ACL.

Implicit

25000

Sintaxă
Intreg

Lungime maximă
11

Valoare
Valoare singulară

ibm-slapdAdminDN

Descriere
DN-ul de legare administrator pentru Directory Server.

Implicit
cn=root

Sintaxă
DN

Lungime maximă
Nelimitat

Valoare
Valoare singulară

ibm-slapdAdminPW

Descriere
Parola de legare administrator pentru Directory Server.

Implicit
secret

Sintaxă
Binar

Lungime maximă
128

Valoare
Valoare singulară

ibm-slapdBulkloadErrors

Descriere
Calea fişierului sau dispozitivul de pe maşina gazdă ibmslapd la care vor fi scrise mesajele de eroare bulkload.

Implicit
/var/bulkload.log

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoare
Valoare singulară

ibm-slapdChangeLogMaxEntries

Descriere

Acest atribut este folosit de un plugin changelog pentru a specifica numărul maxim de intrări din istoricul de modificări din baza de date RDBM. Fiecare changelog are propriul atribut changeLogMaxEntries.

```
Minim = 0 (nelimitat)
Maxim = 2,147,483,647 (32-biţi, întreg înregistrat)
```

Implicit

0

Sintaxă

Intreg

Lungime maximă

11

Valoare

Valoare singulară

ibm-slapdCLIErrors

Descriere

Calea fişierului sau dispozitivul de pe maşina gazdă ibmslapd la care vor fi scrise mesajele de eroare CLI.

Implicit

/var/db2cli.log

Sintaxă

Şir director cu potrivire exactă de majusculă

Lungime maximă

1024

Valoare

Valoare singulară

ibm-slapdConcurrentRW

Descriere

Setând aceasta pe TRUE permite efectuarea căutărilor simultan cu actualizările. Aceasta permite ’citiri murdare’ (’dirty reads’), adică rezultate care ar putea să nu fie consistente cu starea comisă a bazei de date.

Atenţie: Acest atribut este învechit.

Implicit

FALSE

Sintaxă

Boolean

Lungime maximă

5

Valoare

Valoare singulară

ibm-slapdDB2CP

Descriere

Specifică pagina de cod a bazei de date director. 1208 este pagina de cod pentru bazele de date UTF-8.

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
11

Valoare
Valoare singulară

ibm-slapdDBAlias

Descriere
Alias-ul bazei de date DB2.

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
8

Valoare
Valoare singulară

ibm-slapdDbConnections

Descriere
Specifică numărul de conexiuni DB2 pe care serverul le va dedica pentru backend-ul DB2. Valoarea trebuie să fie între 5 & 50 (inclusiv).

Notă: Variabila de mediu ODBCCONS înlocuieşte valoarea acestei directive.
Dacă ibm-slapdDbConnections (sau ODBCCONS) este mai mic decât 5 sau mai mare decât 50, atunci serverul va folosi 5 sau 50, respectiv. Va fi creată 1 conexiune adiţională pentru replicare (chiar dacă nu este definită nici o replicare). Vor fi create 2 conexiuni adiţionale pentru istoricul de modificări (dacă acesta este activat).

Implicit
15

Sintaxă
Intreg

Lungime maximă
50

Valoare
Valoare singulară

ibm-slapdDbInstance

Descriere
Specifică instanţa bază de date DB2 pentru acest backend.

Implicit
ldapdb2

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
8

Valoare
Valoare singulară

Notă: Toate obiectele ibm-slapdRdbmBackend trebuie să folosească acelaşi ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW şi acelaşi set de caractere DB2.

ibm-slapdDbLocation

Descriere
Calea în sistemul de fişiere unde se află baza de date backend.

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoare
Valoare singulară

ibm-slapdDbName

Descriere
Specifică numele bazei de date DB2 pentru acest backend.

Implicit
ldapdb2

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
8

Valoare
Valoare singulară

ibm-slapdDbUserID

Descriere
Specifică numele de utilizator cu care se va lega baza de date DB2 pentru acest backend.

Implicit
ldapdb2

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
8

Valoare
Valoare singulară

Notă: Toate obiectele ibm-slapdRdbmBackend trebuie să folosească acelaşi ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW şi acelaşi set de caractere DB2.

ibm-slapdDbUserPW

Descriere
Specifică parola utilizatorului cu care se va lega baza de date DB2 pentru acest backend. Parola poate fi text întreg sau mască cifrată.

Implicit
ldapdb2

Sintaxă
Binar

Lungime maximă
128

Valoare
Valoare singulară

Notă: Toate obiectele ibm-slapdRdbmBackend trebuie să folosească acelaşi ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW şi acelaşi set de caractere DB2.

ibm-slapdEnableEventNotification

Descriere
Specifică dacă se activează Event Notification. Trebuie să fie setat ori pe TRUE ori pe FALSE.

Dacă este setat pe FALSE, serverul rejectază toate cererile client de înregistrare notificări evenimente cu rezultatul extins LDAP_UNWILLING_TO_PERFORM.

Implicit
TRUE

Sintaxă
Boolean

Lungime maximă
5

Valoare
Valoare singulară

ibm-slapdEntryCacheSize

Descriere
Numărul maxim de intrări de păstrat în cache-ul de intrări.

Implicit
25000

Sintaxă
Intreg

Lungime maximă
11

Valoare
Valoare singulară

ibm-slapdErrorLog

Descriere
Specifică calea fişierului sau dispozitivul de pe maşina Directory Server către care sunt scrise mesajele de eroare.

Implicit
/var/ibmslapd.log

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoare
Valoare singulară

ibm-slapdFilterCacheBypassLimit

Descriere
Filtrele de căutare care se potrivesc cu mai mult de acest număr de intrări nu vor fi adăugate în cache-ul de filtre de căutare. Deoarece lista de Id-uri intrări care s-au potrivit cu filtrul este inclusă în acest cache, această setare ajută la limitarea utilizării memoriei. O valoare 0 indică nici o limită.

Implicit
100

Sintaxă
Intreg

Lungime maximă
11

Valoare
Valoare singulară

ibm-slapdFilterCacheSize

Descriere
Specifică numărul maxim de intrări de ţinut în Search Filter Cache.

Implicit
25000

Sintaxă
Intreg

Lungime maximă
11

Valoare
Valoare singulară

ibm-slapdIdleTimeOut

Descriere
Timpul maxim cât se menţine deschisă o conexiune LDAP când nu este activitate pe conexiune. Timpul de inactivitate pentru o conexiune LDAP este timpul scurs (în secunde) de la ultima activitate de pe conexiune până în momentul curent. Dacă conexiunea a expirat, adică dacă perioada de inactivitate este mai mare decât valoarea acestui atribut, atunci serverul LDAP va curăţa şi va termina conexiunea LDAP, făcând-o astfel disponibilă pentru cereri de intrare.

Implicit
300

Sintaxă
Intreg

Lungime
11

Numărare
Singular

Folosire
Operaţie director

Modificare utilizator
Da

Clasă acces
Critic

Necesar
Nu

ibm-slapdIncludeSchema

Descriere
Specifică o cale de fişier de pe maşina Directory Server care conţine definiţiile schemei.

Implicit
/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

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoare
Multi-valoric

ibm-slapdKrbAdminDN

Descriere
Specifică IDul Kerberos al administratorului LDAP (de exemplu, ibm-kn=admin1@realm1). Folosit când este folosită autentificarea Kerberos pentru a autentifica administratorul când este înregistrat la interfaţa de administrare server. Aceasta ar putea fi specificată în loc de sau în plus faţă de adminDN şi adminPW.

Implicit
Nu este definită nici o valoare implicită.

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
128

Valoare
Valoare singulară

ibm-slapdKrbEnable

Descriere
Specifică dacă serverul suportă Kerberos. Trebuie să fie TRUE sau FALSE.

Implicit
TRUE

Sintaxă
Boolean

Lungime maximă
5

Valoare
Valoare singulară

ibm-slapdKrbIdentityMap

Descriere
Specifică dacă să folosiţi maparea de identităţi Kerberos. Trebuie să fie setat ori pe TRUE ori pe FALSE. Dacă este setat pe TRUE, când un client este autentificat cu un ID Kerberos, serverul caută toţi utilizatorii locali cu acreditări Kerberos corespunzătoare şi adaugă DNurile acelor utilizatori la acreditările de legare ale conexiunii. Aceasta permite ca ACL-urile bazate pe DNuri utilizator LDAP să fie încă utilizabile cu Kerberos.

Implicit
FALSE

Sintaxă
Boolean

Lungime maximă
5

Valoare
Valoare singulară

ibm-slapdKrbKeyTab

Descriere
Specifică fişierul keytab Kerberos de pe serverul LDAP. Acest fişier conţine cheia privată a serverului LDAP, care este asociată cu contul său Kerberos. Acest fişier trebuie să fie protejat (precum fişierul de bază de date chei SSL al serverului).

Implicit
Nu este definită nici o valoare implicită.

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoare
Valoare singulară

ibm-slapdKrbRealm

Descriere
Specifică regiunea Kerberos a serverului LDAP. Este folosit pentru a publica atributul ldapservicename din rădăcina DSE. Luaţi la cunoştinţă că un server LDAP poate servi ca depozitul de informaţii cont pentru multiple KDCs (şi regiuni), dar serverul LDAP, ca un server kerberized, poate fi membru al unei singure regiuni.

Implicit
Nu este definită nici o valoare implicită.

Sintaxă

Şir director cu potrivire inexactă de majusculă

Lungime maximă

256

Valoare

Valoare singulară

ibm-slapdLdapCrlHost

Descriere

Specifică numele gazdă al serverului LDAP care conţine lista de revocare certificate (Certificate Revocation Lists - CRLuri) pentru validarea certificatelor client x.509v3. Acest parametru este necesar când ibm-slapdSslAuth=serverclientauth şi certificatele client au fost emise pentru validarea CRL.

Implicit

Nu este definită nici o valoare implicită.

Sintaxă

Şir director cu potrivire inexactă de majusculă

Lungime maximă

256

Valoare

Valoare singulară

ibm-slapdLdapCrlPassword

Descriere

Specifică parola serverului LDAP care conţine lista de revocare certificate (Certificate Revocation Lists - CRLuri) pentru validarea certificatelor client x.509v3. Acest parametru ar putea fi necesar când ibm-slapdSslAuth=serverclientauth şi certificatele client au fost emise pentru validarea CRL.

Notă: Dacă serverul LDAP care păstrează CRLurile permite accesul neautentificat la CRLuri (adica acces anonim), atunci ibm-slapdLdapCrlPassword nu este necesar.

Implicit

Nu este definită nici o valoare implicită.

Sintaxă

Binar

Lungime maximă

128

Valoare

Valoare singulară

ibm-slapdLdapCrlPort

Descriere

Specifică portul folosit pentru conectarea la serverul LDAP care conţine lista de revocare certificate (Certificate Revocation Lists - CRLuri) pentru validarea certificatelor client x.509v3. Acest parametru este necesar când ibm-slapdSslAuth=serverclientauth şi certificatele client au fost emise pentru validarea CRL. (porturile IP nu sunt marcate, întregi de 16-biţi din intervalul 1 - 65535.)

Implicit

Nu este definită nici o valoare implicită.

Sintaxă

Intreg

Lungime maximă
11

Valoare
Valoare singulară

ibm-slapdLdapCrlUser

Descriere
Specifică binDN-ul pe care SSL server-side îl foloseşte pentru a se lega la serverul LDAP care conţine lista de revocare certificate (Certificate Revocation Lists - CRLuri) pentru validarea certificatelor client x.509v3. Acest parametru ar putea fi necesar când ibm-slapdSslAuth=serverclientauth şi certificatele client au fost emise pentru validarea CRL.

Notă: Dacă serverul LDAP care păstrează CRLurile permite accesul neautentificat la CRLuri (adica acces anonim), atunci ibm-slapdLdapCrlUser nu este necesar.

Implicit
Nu este definită nici o valoare implicită.

Sintaxă
DN

Lungime maximă
1000

Valoare
Valoare singulară

ibm-slapdMasterDN

Descriere
Specifică legarea DN a serverului master. Valoarea trebuie să se potrivească cu replicaBindDN din replicaObject definit pentru un server master. Când este folosit Kerberos pentru a autentifica la replică, ibm-slapdMasterDN trebuie să specifice reprezentarea DN a ID-ului Kerberos (de exemplu, ibm-kn=freddy@realm1). Când este folosit Kerberos, MasterServerPW este ignorat.

Implicit
Nu este definită nici o valoare implicită.

Sintaxă
DN

Lungime maximă
1000

Valoare
Valoare singulară

ibm-slapdMasterPW

Descriere
Specifică parola de legare a serverului replică master. Valoarea trebuie să se potrivească cu replicaBindDN din replicaObject definit pentru un server master. Când este folosit Kerberos pentru a autentifica la replică, ibm-slapdMasterDN trebuie să specifice reprezentarea DN a ID-ului Kerberos (de exemplu, ibm-kn=freddy@realm1). Când este folosit Kerberos, MasterServerPW este ignorat.

Implicit
Nu este definită nici o valoare implicită.

Sintaxă
Binar

Lungime maximă
128

Valoare
Valoare singulară

ibm-slapdMasterReferral

Descriere
Specifică URL-ul serverului replică master. De exemplu:

```
ldap://master.us.ibm.com
```

Pentru securitate setaţi doar pe SSL:

```
ldaps://master.us.ibm.com:636
```

Pentru securitate setaţi pe nimic şi folosiţi un port nonstandard:

```
ldap://master.us.ibm.com:1389
```

Implicit
nimic

Sintaxă
Şir director cu potrivire inexactă de majusculă

Lungime maximă
256

Valoare
Valoare singulară

ibm-slapdMaxEventsPerConnection

Descriere
Specifică numărul maxim de notificări de evenimente care pot fi înregistrate pentru o conexiune.

```
Minim = 0 (nelimitat)
Maxim = 2,147,483,647
```

Implicit
100

Sintaxă
Intreg

Lungime maximă
11

Valoare
Valoare singulară

ibm-slapdMaxEventsTotal

Descriere
Specifică numărul maxim de notificări de evenimente care pot fi înregistrate pentru toate conexiunile.

```
Minim = 0 (nelimitat)
Maxim = 2,147,483,647
```

Implicit
0

Sintaxă
Intreg

Lungime maximă
11

Valoare
Valoare singulară

ibm-slapdMaxNumOfTransactions

Descriere
Specifică numărul maxim de tranzacţii pentru un server.

```
Minim = 0 (nelimitat)
Maxim = 2,147,483,647
```

Implicit
20

Sintaxă
Intreg

Lungime maximă
11

Valoare
Valoare singulară

ibm-slapdMaxOpPerTransaction

Descriere
Specifică numărul maxim de operaţii pentru o tranzacţie.

```
Minim = 0 (nelimitat)
Maxim = 2,147,483,647
```

Implicit
5

Sintaxă
Intreg

Lungime maximă
11

Valoare
Valoare singulară

ibm-slapdMaxPendingChangesDisplayed

Descriere
Numărul maxim de modificări în aşteptare de afişat.

Implicit
200

Sintaxă
Intreg

Lungime maximă
11

Valoare
Valoare singulară

ibm-slapdMaxTimeLimitOfTransactions

Descriere

Specifică, în secunde, valoarea timeout maximă a unei tranzacţii în aşteptare.

```
Minim = 0 (nelimitat)
Maxim = 2,147,483,647
```

Implicit

300

Sintaxă

Intreg

Lungime maximă

11

Valoare

Valoare singulară

ibm-slapdPagedResAllowNonAdmin

Descriere

Indiferent dacă serverul ar trebui să permită sau nu legarea non-administrator pentru cererile rezultate paginate dintr-o cerere de căutare. Dacă valoarea citită din fişierul ibmslapd.conf este FALSE, serverul va procesa doar acele cereri client emise de un utilizator cu autorizarea de administrator. Dacă un client cere rezultate paginate pentru o operaţie de căutare, nu are autorizare de administrator şi valoarea citită din fişierul ibmslapd.conf pentru acest atribut este FALSE, serverul va returna la client codul retur insufficientAccessRights; nu va fi efectuată nici o căutare sau paginare.

Implicit

FALSE

Sintaxă

Boolean

Lungime

5

Numărare

Singular

Folosire

directoryOperation

Modificare utilizator

Da

Clasă acces

critic

Objectclass

ibm-slapdRdbmBackend

Necesar

Nu

ibm-slapdPagedResLmt

Descriere

Numărul maxim de cereri de căutare rezultate paginate remarcabile permise active simultan. Range = 0.... Dacă un client cere o operaţie cu rezultate paginate şi numărul maxim de rezultate paginate remarcabile sunt active, serverul va returna la client codul retur ocupat (busy); nu va fi efectuată nici o căutare sau paginare.

Implicit

3

Sintaxă
Intreg

Lungime
11

Numărare
Singular

Folosire
directoryOperation

Modificare utilizator
Da

Clasă acces
critic

Necesar
Nu

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPageSizeLmt

Descriere
Numărul maxim de intrări de returnat de la o căutare a unei pagini individuale când este specificat controlul rezultatelor paginate, indiferent de orice dimensiune de pagină care ar fi putut fi specificată în cererea de căutare de la client. Range = 0.... Dacă un client a pasat o dimensiune de pagină, atunci va fi folosită valoarea cea mai mică dintre valoarea client şi valorea citită din ibmslapd.conf.

Implicit
50

Sintaxă
Intreg

Lungime
11

Numărare
Singular

Folosire
directoryOperation

Modificare utilizator
Da

Clasă acces
critic

Necesar
Nu

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPlugin

Descriere
Un plugin este o bibliotecă încărcată dinamic care extinde capabilităţile serverului. Un atribut ibm-slapdPlugin specifică serverului cum să încarce şi să iniţializeze o bibliotecă plug-in. Sintaxa este:

nume fişier cuvânt cheie `init_function [`*`args...`*`]`

Sintaxa este uşor diferită pentru fiecare platformă datorită convenţiilor de numire ale bibliotecii.

Majoritatea plug-in-urilor sunt opţionale, dar pluginul backend RDBM este necesar pentru toate backend-urile RDBM.

Implicit
database /bin/libback-rdbm.dll rdbm_backend_init

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
2000

Valoare
Multi-valoric

ibm-slapdPort

Descriere
Specifică portul TCP/IP dolosit pentru conexiuni non-SSL. Nu poate avea aceeaşi valoare ca şi ibm-slapdSecurePort. (porturile IP nu sunt marcate, întregi de 16-biţi din intervalul 1 - 65535.)

Implicit
389

Sintaxă
Intreg

Lungime maximă
5

Valoare
Valoare singulară

ibm-slapdPWEncryption

Descriere
Specifică mecanismul de codificare pentru parolele utilizator înainte de a fi stocate în director. Trebuie să fie specificat ca none, imask, crypt sau sha (trebuie să folosiţi cuvântul cheie **sha** pentru a obţine codificarea SHA-1). Valoarea trebuie să fie setată la none pentru ca legarea SASL cram-md5 să aibă succes.

Implicit
nimic

Sintaxă
Şir director cu potrivire inexactă de majusculă

Lungime maximă
5

Valoare
Valoare singulară

ibm-slapdReadOnly

Descriere
Acest atribut este aplicat în mod normal doar la backend-ul director. El specifică dacă se poate scrie în backend. Trebuie să fie specificat ori pe TRUE ori pe FALSE. Are valoarea implicită FALSE dacă nu este specificat. Dacă este setat pe TRUE, serverul întoarce LDAP_UNWILLING_TO_PERFORM (0x35) ca răspuns la orice cerere client care modifică datele din baza de date readOnly.

Implicit
FALSE

Sintaxă
Boolean

Lungime maximă
5

Valoare
Valoare singulară

ibm-slapdReferral

Descriere
Specifică URL-ul LDAP referal de trimis înapoi când sufixele locale nu corespund cererii. Este folosit pentru referal superior (adică sufixul nu este în cadrul contextului de nume al serverului).

Implicit
Nu este definită nici o valoare implicită.

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
32700

Valoare
Multi-valoric

ibm-slapdReplDbConns

Descriere
Numărul maxim de conexiuni ale bazei de date pentru folosul de către replicare.

Implicit
4

Sintaxă
Intreg

Lungime maximă
11

Valoare
Valoare singulară

ibm-slapdReplicaSubtree

Descriere
Identifică DN-ul unui subarbore replicat

Sintaxă
DN

Lungime maximă
1000

Valoare
Valoare singulară

ibm-slapdSchemaAdditions

Descriere
Atributul ibm-slapdSchemaAdditions este folosit pentru a identifica explicit ce fişier păstrează noile

intrări de schemă. Acesta este setat implicit pe /etc/V3.modifiedschema. Dacă acest atribut nu este definit, serverul revine la folosirea ultimului fişier ibm-slapdIncludeSchema ca în ediţiile anterioare.

Înainte de Version 3.2, ultima intrare includeSchema din **slapd.conf** era fişierul în care erau adăugate de către server orice noi intrări de schemă dacă primea o cerere de adăugare de la un client. În mod normal ultima includeSchema este fişierul V3.modifiedschema, care este un fişier gol instalat doar pentru acest scop.

Notă: Numele modified este înşelător, deoarece stochează doar intrări noi. Schimbările la intrările de schemă existente sunt făcute în fişierele lor originale.

Implicit
/etc/V3.modifiedschema

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoare
Valoare singulară

ibm-slapdSchemaCheck

Descriere
Specifică mecanismul de verificare schemă pentru operaţia de adăugare/modificare/ştergere. Trebuie specificat ca V2, V3 sau V3_lenient.

- V2 - Reţine verificarea v2 şi v2.1. Recomandat pentru migrare.
- V3 - Realizează verificare v3.
- V3_lenient - Nu toate clasele de obiecte părinte sunt necesare. Doar clasa de obiecte imediată este necesară când se adaugă intrări.

Implicit
V3_permisiv

Sintaxă
Şir director cu potrivire inexactă de majusculă

Lungime maximă
10

Valoare
Valoare singulară

ibm-slapdSecurePort

Descriere
Specifică portul TCP/IP folosit de conexiuni SSL. Nu poate avea aceeaşi valoare ca ibm-slapdPort. (porturile IP nu sunt marcate, întregi de 16-biţi din intervalul 1 - 65535.)

Implicit
636

Sintaxă
Intreg

Lungime maximă
5

Valoare
Valoare singulară

ibm-slapdSecurity

Descriere
Activează conexiuni SSL. Trebuie să fie nimic, SSL sau SSLOnly.
- none - serverul ascultă doar la portul non-ssl.
- SSL - serverul ascultă atât la portul ssl cât şi non-ssl.
- SSLOnly - server ascultă doar la portul ssl.

Implicit
nimic

Sintaxă
Şir director cu potrivire inexactă de majusculă

Lungime maximă
7

Valoare
Valoare singulară

ibm-slapdServerId

Descriere
Identifică serverul de folosit în replicare.

Sintaxă
Şir IA5 cu potrivire sensibilă la majusculă

Lungime maximă
240

Valoare
Valoare singulară

ibm-slapdSetenv

Descriere
Serverul rulează **putenv()** pentru toate valorile lui ibm-slapdSetenv la pornire pentru a modifica mediul de exeecuţie al serverului. Variabilele shell (precum %PATH% sau $LANG) nu sunt expandate.

Implicit
Nu este definită nici o valoare implicită.

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
2000

Valoare
Multi-valoric

ibm-slapdSizeLimit

Descriere
Specifică numărul maxim de intrări de returnat de la o căutare, indiferent de orice dimensiune limită care ar fi putut fi specificată în cererea de căutare de la client (Range = 0...). Dacă un client a pasat o limită, atunci va fi folosită cea mai mică valoare dintre valoarile client şi valorea citită din **ibmslapd.conf**. Dacă un client nu a pasat o limită şi s-a legat ca DN admin, limita este considerată nelimitată. Dacă clientul nu a pasat o limită şi nu s-a legat ca DN admin, atunci limita este cea care a fost citită din fişierul **ibmslapd.conf**. 0 = nelimitat.

Implicit
500

Sintaxă
Intreg

Lungime maximă
12

Valoare
Valoare singulară

ibm-slapdSortKeyLimit

Descriere
Numărul maxim de condiţii (chei) de sortare care pot fi specificate la o singură cerere de căutare. Range = 0.... Dacă un client a pasat o cerere de căutare cu mai multe chei de sortare decât permite limita şi criticalitatea de control căutare sortată este FALSE, atunci serverul va onora valoarea citită din fişierul ibmslapd.conf şi va ignora orice chei de sortare întâlnite după ce a fost atinsă limita - căutarea şi sortarea vor fi efectuate. Dacă un client a pasat o cerere de căutare cu mai multe chei decât permite limita şi criticalitatea de control căutare sortată este TRUE, atunci serverul va returna clientului codul de retur **adminLimitExceeded** - nu va fi realizată nici o căutare sau sortare.

Implicit
3

Sintaxă
cis

Lungime
11

Numărare
Singular

Folosire
directoryOperation

Modificare utilizator
Da

Clasă acces
critic

Objectclass
ibm-slapdRdbmBackend

Necesar
Nu

ibm-slapdSortSrchAllowNonAdmin

Descriere
Dacă serverul ar trebui să permită sau nu legarea non-administrator pentru sortare într-o cerere de căutare. Dacă valoarea citită din fişierul ibmslapd.conf este FALSE, serverul va procesa doar acele cereri client emise de un utilizator cu autorizarea de administrator. Dacă un client cere sortare pentru o operaţie de căutare, nu are autorizare de administrator şi valoarea citită din fişierul ibmslapd.conf pentru acest atribut este FALSE, serverul va returna la client codul retur insufficientAccessRights; nu va fi efectuată nici o căutare sau paginare.

Implicit
FALSE

Sintaxă
Boolean

Lungime
5

Numărare
Singular

Folosire
directoryOperation

Modificare utilizator
Da

Clasă acces
critic

Objectclass
ibm-slapdRdbmBackend

Necesar
Nu

ibm-slapdSslAuth

Descriere
Specifică tipul de autentificare pentru conexiunea SSL, ori serverauth ori serverclientauth.

- serverauth - suportă autentificarea server la client. Aceasta este valoarea implicită.
- serverclientauth - suportă atât autentificarea server cât şi client.

Implicit
serverauth

Sintaxă
Şir director cu potrivire insensibilă la majuscule

Lungime maximă
16

Valoare
Valoare singulară

ibm-slapdSslCertificate

Descriere
Specifică eticheta care identifică Certificatul personal al serverului în fişierul bază de date chei. Această etichetă este specificată când cheia privată a serverului şi certificatul sunt create cu aplicaţia **gsk4ikm**. Dacă nu este definit ibm-slapdSslCertificate, atunci cheia privată implicită, aşa cum este definită în fişierul bază de date chei, este folosită de către serverul LDAP pentru conexiuni SSL.

Implicit
Nu este definită nici o valoare implicită.

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
128

Valoare
Valoare singulară

ibm-slapdSslCipherSpec

Specifică metoda de criptare SSL pentru clienţii care accesează serverul. Trebuie setată la una din următoarele:

Tabela 5. Metode de criptare SSL

Atribut	Nivel criptare
TripleDES-168	Criptare Triple DES cu o cheie de 168-biţi şi SHA-1 MAC
DES-56	Criptare DES cu o cheie de 56-biţi şi SHA-1 MAC
RC4-128-SHA	Criptare RC4 cu o cheie de 128-biţi şi SHA-1 MAC
RC4-128-MD5	Criptare RC4 cu o cheie de 128-biţi şi MD5 MAC
RC2-40-MD5	Criptare RC4 cu o cheie de 40-biţi şi MD5 MAC
RC4-40-MD5	Criptare RC4 cu o cheie de 40-biţi şi MD5 MAC
AES	Criptare AES

Sintaxă
Şir IA5

Lungime maximă
30

ibm-slapdSslKeyDatabase

Descriere
Specifică calea fişierului către fişierul bază de date chei SSL ale serverului LDAP. Acest fişier bază de date chei este folosit pentru tratarea conexiunilor SSL de la clienţii LDAP precum şi pentru crearea conexiunilor securizate SSL cu serverele LDAP replică.

Implicit
/etc/key.kdb

Sintaxă
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoare
Valoare singulară

ibm-slapdSslKeyDatabasePW

Descriere
Specifică parola asociată cu fişierul bază de date chei SSL ale serverului LDAP, aşa cum este specificată în parametrul ibm-slapdSslKeyDatabase. Dacă fişierul bază de date chei server LDAP are asociat un fişier stash parole, atunci parametrul ibm-slapdSslKeyDatabasePW poate fi omis sau setat pe none.

Notă: Fişierul stash parole trebuie să se afle în acelaşi director ca şi fişierul baze de date chei şi trebuie să aibă acelaşi nume ca şi fişierul baze de date chei, dar cu extensia .sth în loc de .kdb.

Implicit
nimic

Sintaxă
Binar

Lungime maximă
128

Valoare
Valoare singulară

ibm-slapdSslKeyRingFile

Descriere
Calea către fişierul baze de date chei SSL ale serverului LDAP. Acest fişier bază de date chei este folosit pentru tratarea conexiunilor SSL de la clienţii LDAP precum şi pentru crearea conexiunilor securizate SSL cu serverele LDAP replică.

Implicit
key.kdb

Sintaxă
Şir director cu potrivire sensibilă la majusculă

Lungime maximă
1024

Valoare
Valoare singulară

ibm-slapdSuffix

Descriere
Specifică un context de numire de memorat în acest back-end.

Notă: Acesta are acelaşi nume cu clasa obiectului.

Implicit
Nu este definită nici o valoare implicită.

Sintaxă
DN

Lungime maximă
1000

Valoare
Multi-valoric

ibm-slapdSupportedWebAdmVersion

Descriere
Acest atribut defineşte cea mai veche versiune a uneltei de administrare care suportă acest server de cn=configuration.

Implicit

Sintaxă
Şir director

Lungime maximă

Valoare
Valoare singulară

ibm-slapdSysLogLevel

Descriere
Specifică nivelul la care statisticele de depanare şi de operaţii sunt înregistrate în istoricul fişierului slapd.errors. Trebuie specificat ca l, m sau h.

- h - înalt (high)(furnizează cele mai multe informaţii)
- m - mediu (medium)(valoarea implicită)
- l - jos (low) (furnizează cele mai puţine informaţii)

Implicit
m

Sintaxă
Şir director cu potrivire insensibilă la majuscule

Lungime maximă
1

Valoare
Valoare singulară

ibm-slapdTimeLimit

Descriere
Specifică numărul maxim de secunde pentru o cerere de căutare, indiferent de orice limită de timp care ar fi putut fi specificată în cererea de la client. Dacă un client a pasat o limită, atunci va fi folosită cea mai mică valoare dintre valoarile client şi valorea citită din **ibmslapd.conf**. Dacă un client nu a pasat o limită şi s-a legat ca DN admin, limita este considerată nelimitată. Dacă clientul nu a pasat o limită şi nu s-a legat ca DN admin, atunci limita este cea care a fost citită din fişierul **ibmslapd.conf**. 0 = nelimitat.

Implicit
900

Sintaxă
Intreg

Lungime maximă

Valoare
Valoare singulară

ibm-slapdTransactionEnable

Descriere
Dacă plug-in-ul de tranzacţii este încărcat, dar ibm-slapdTransactionEnable este setat pe FALSE, serverul rejectează toate cererile StartTransaction cu răspunsul LDAP_UNWILLING_TO_PERFORM.

Implicit
TRUE

Sintaxă
Boolean

Lungime maximă
5

Valoare
Valoare singulară

ibm-slapdUseProcessIdPw

Descriere
Dacă este setat pe TRUE, serverul ignoră atributele ibm-slapdDbUserID şi ibm-slapdDbUserPW şi foloseşte propriile acreditări de proces pentru autentificarea DB2.

Implicit
FALSE

Sintaxă
Boolean

Lungime maximă
5

Valoare
Valoare singulară

ibm-slapdVersion

Descriere
Număr versiune IBM Slapd

Implicit

Sintaxă
Şir director cu potrivire sensibilă la majusculă

Lungime maximă

Valoare
Valoare singulară

objectClass

Descriere
Valorile atributului objectClass descriu tipul de obiect pe care îl reprezintă o intrare.

Sintaxă
Şir director

Lungime maximă
128

Valoare
Multi-valoric

Capitolul 10. Informaţii înrudite

Menţionate mai jos sunt IBM Redbooks (în format PDF), site-uri Web şi subiecte ale Centrului de informare care le înrudeşte cu subiectul Directory Server. Puteţi vizualiza sau tipări oricare dintre PDF-uri.

Manuale Redbooks (www.redbooks.ibm.com)

- *Understanding LDAP*, SG24-4986 .
- *Using LDAP for Directory Integration: A Look at IBMSecureWay Directory, Active Directory, and Domino*, SG24-6163 .
- *Implementation and Practical Use of LDAP on the iSeries Server*, SG24-6193 .

Site-uri Web

- Situl Web IBM Directory Server for iSeries (www.ibm.com/servers/eserver/iseries/ldap)
- Situl Web Java Naming and Directory Interface (JNDI) Tutorial (java.sun.com/products/jndi/tutorial/)

Alte informaţii

“API-uri Directory Server” din subiectul Programare.

Anexa. Observaţii

Aceaste informaţii au fost dezvoltate pentru produse şi servicii oferite în U.S.A.

Este posibil ca IBM să nu ofere produsele, serviciile sau caracteristicile discutate în acest document în alte ţări. Consultaţi reprezentantul dvs. local IBM pentru informaţii despre produse şi servicii disponibile în zona dvs. Orice referal la un produs IBM, program sau serviciu nu are ca scop enunţarea sau implicarea că doar acel produs IBM, program sau serviciu poate fi folosit. Orice produs echivalent funcţional, produs sau serviciu care nu încalcă vreun drept de proprietate intelectuală a IBM poate fi folosit în schimb. Totuşi, este în responsabilitatea utilizatorului să evalueze şi să verifice operarea oricărui produs non-IBM, program sau serviciu.

IBM poate avea patente sau aplicaţii de patente în aşteptare referitoare la subiectele descrise în acest document. Oferirea acestui document nu vă conferă nici o licenţă cu privire la aceste patente. Puteţi trmite cereri de licenţă, în scris, la:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pentru cereri de licenţă privitoare la informaţiile dublu-octet (DBCS), contactaţi IBM Intellectual Property Department din ţara dvs. sau trimiteţi cererile în scris la:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Următorul paragraf nu se aplică la Regatul Unit sau la alte ţări în care aceste furnizări sunt inconsistente cu legea locală: INTERNATIONAL BUSINESS MACHINES CORPORATION FURNIZEAZĂ ACEASTĂ PUBLICAŢIE "AŞA CUM ESTE" FĂRĂ NICI O GARANŢIE, FIE EXPRESĂ SAU IMPLICATĂ, INCLUSIV, DAR NU LIMITATĂ LA, GARANŢIILE IMPLICATE DE NE-ÎNCĂLCARE, MARCANTIBILITATE SAU POTRIVIRE PENTRU UN ANUMIT SCOP. Unele state nu permit declinarea responsabilităţii pentru garaţii exprese sau implicate în anumite tranzacţii, aşadar, această declaraţie s-ar putea să nu vi se aplice.

Aceste informaţii pot include neconcordanţe tehnice sau erori tipografice. Sunt făcute periodic modificări la informaţiile de aici; aceste modificări vor fi încorporate în noile ediţii ale publicaţiei. IBM poate face îmbunătăţiri şi/sau schimbări în produs(e) şi/sau programul(ele) descrise în această publicaţie în orice moment fără notificare.

Orice referinţe din aceste informaţii la situri Web non-IBM sunt furnizate doar pentru comoditate şi nu servesc în nici un mod ca o aprobare a acelor situri web. Materialele din acele situri Web nu fac parte din materialele pentru acest produs IBM şi folosirea acelor situri Web este pe riscul dvs.

IBM poate folosi sau distribui orice informaţie pe care o furnizaţi în orice mod considerat corespunzător fără a atrage asupra dvs. nici o obligaţie.

Deţinătorii de licenţe ale acestui program care doresc să aibă informaţii pentru scopul de a activa: (i) schimbul de informaţii dintre programe create independent şi alte programe (inclusiv acesta) şi (ii) folosirea mutuală a informaţiei care a fost schimbată, ar trebui să contacteze:

IBM
Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Aceste informaţii pot fi disponibile, subiectul unor termeni şi condiţii corespunzătoare, inclusiv în unele cazuri plătirea unor taxe.

Programul licenţiat descris în această publicaţie şi toate materialele licenţiate disponibile pentru el sunt furnizate de IBM conform termenilor din IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code sau orice acord echivalent între noi.

Orice date de performanţă conţinute aici au fost determinate într-un mediu controlat. Aşadar, rezultatele obţinute în alte medii de operare pot varia considerabil. Este posibil ca unele măsuri să fi fost făcute pe sisteme de nivel dezvoltare şi nu există nici o garanţie că aceste măsurători vor fi la fel pe sisteme disponibile general. Mai mult, unele măsurători se poate să fi fost estimate prin extrapolare. Rezultatele reale pot varia. Utilizatorii acestui document ar trebui să verifice datele aplicabile pentru mediul lor specifict.

Informaţiile referitoare la produsele non-IBM au fost obţinute de la furnizorii acestor produse, anunţurile lor publice sau alte surse disponibile public. IBM nu a testat acele produse şi nu poate confirma acurateţea sau performanţa, compatibilitatea sau alte cereri înrudite cu produse non-IBM. Întrebările despre capabilităţile produselor non-IBM ar trebui adresate furnizorilor acelor produse.

Toate declaraţiile cu privire la direcţia sau scopul viitor a IBM pot fi schimbate sau retrase fără notificare şi reprezintă doar scopuri şi obiective.

Toate preţurile IBM arătate sunt preţurile cu amănuntul sugerate de IBM, sunt curente şi pot fi modificate fără notificare. Preţurile dealer-ului pot fi diferite.

Aceste informaţii sunt doar în scop de planificare. Informaţiile menţionate aici se pot modifica înainte ca produsele descrise să devină disponibile pe piaţă.

Aceste informaţii conţin exemple de date şi rapoarte utilizate în operaţii de afaceri zilnice. Pentru a le ilustra cât mai complet posibil, exemplele includ numele de indivizi, companii, mărci şi produse. Toate aceste nume sunt fictive şi orice similaritate cu numele şi adresele folosite de o întreprindere reală sunt pure coincidenţe.

LICENŢĂ - COPYRIGHT:

Aceste informaţii conţin exemple de programe de aplicaţii în limbaje sursă, care ilustrează tehnici de programare pe diferite platforme de operare. Puteţi copia, modifica şi distribui aceste exemple de programe sub orice formă fără plată către IBM, în scopul dezvoltării, folosirii, promovării şi distribuirii programelor de aplicaţii conform cu interfaţa de programare aplicaţii pentru platforma de operare pentru care au fost scrise exemplele de program. Aceste exemple nu au fost testate temeinic pentru toate condiţiile. De aceea, IBM nu poate garanta sau sugera fiabilitatea, suportul pentru service sau funcţionarea acestor programe.

EXCEPTÂND GARANŢIILE OBLIGATORII, CARE NU POT FI EXCLUSE, IBM, DEZVOLTATORII DE PROGRAME ŞI FURNIZORII SĂI NU ACORDĂ NICI O GARANŢIE SAU CONDIŢIE, EXPRESĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE SAU CONDIŢIILE IMPLICITE DE VANDABILITATE, DE POTRIVIRE PENTRU UN ANUMIT SCOP SAU DE NEÎNCĂLCARE A UNUI DREPT, REFERITOARE LA PROGRAM SAU LA SUPORTUL TEHNIC, DACĂ ESTE CAZUL.

ÎN NICI O ÎMPREJURARE IBM, DEZVOLTATORII SĂI DE PROGRAME SAU FURNIZORII NU VOR FI RESPONSABILI PENTRU ORICARE DINTRE URMĂTOARELE PAGUBE, CHIAR DACĂ AU FOST INFORMAŢI ÎN LEGĂTURĂ CU POSIBILITATEA PRODUCERII LOR:

1. PIERDEREA SAU DETERIORAREA DATELOR;
2. PAGUBE SPECIALE, ACCIDENTALE SAU INDIRECTE SAU PREJUDICII ECONOMICE DE CONSECINŢĂ; SAU

3. PIERDERI REFERITOARE LA PROFIT, AFACERI, BENEFICII, REPUTAŢIE SAU ECONOMII PLANIFICATE.

UNELE JURISDICŢII NU PERMIT EXCLUDEREA SAU LIMITAREA PREJUDICIILOR INCIDENTALE SAU INDIRECTE, CAZ ÎN CARE ESTE POSIBIL CA UNELE SAU TOATE LIMITĂRILE SAU EXCLUDERILE DE MAI SUS SĂ NU FIE VALABILE PENTRU DUMNEAVOASTRĂ.

Fiecare copie sau orice porţiune din aceste exemple de pogram sau orice lucrare derivată din acestea trebuie să includă un anunţ de copyright de genul următor:

© (numele companiei dumneavoastră) (anul). Părţi din acest cod sunt derivate din IBM Corp. Sample Programs. © Copyright IBM Corp. _introduceţi anul sau anii_. Toate drepturile rezervate.

Dacă vizualizaţi aceste informaţii softcopy, fotografiile sau ilustraţiile color s-ar putea să nu apară.

Mărci comerciale

Următorii termeni sunt mărci comerciale ale International Business Machines Corporation din Statele Unite, alte ţări sau ambele:

AIX
AIX 5L
e(logo)server
eServer
i5/OS
IBM
iSeries
pSeries
xSeries
zSeries

Intel, Intel Inside (logo-uri), MMX şi Pentium sunt mărci comerciale ale Intel Corporation în Statele Unite, în alte ţări sau în ambele.

Microsoft, Windows, Windows NT şi emblema Windows sunt mărci comerciale ale Microsoft Corporation în Statele Unite, în alte ţări sau ambele.

Java şi toate mărcile comerciale bazate pe Java sunt mărci comerciale ale Sun Microsystems, Inc. în Statele Unite, în alte ţări sau ambele.

Linux este marcă comercială a Linus Torvalds în Statele Unite, în alte ţări sau ambele.

UNIX este o marcă comercială înregistrată, deţinută de The Open Group în Statele Unite şi în alte ţări.

Şi alte nume de companii, produse sau servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

Termeni şi condiţii pentru descărcarea şi tipărirea informaţiilor

Permisiunile pentru folosirea informaţiilor pe care le-aţi selectat pentru descărcare sunt acordate în următorii termeni şi condiţii şi cu indicarea acceptării lor de către dumneavoastră.

Uz personal: Puteţi reproduce aceste informaţii pentru uzul dumneavoastră personal şi necomercial cu condiţia ca toate notele de proprietate să fie păstrate. Nu puteţi distribui, afişa sau face lucrări derivative din aceste informaţii sau orice alte porţiuni din ele, fără acordul explicit al IBM.

Uz comercial: Puteţi reproduce, distribui şi afişa aceste informaţii doar în întreprinderea dumneavoastră cu condiţia ca toate notele de proprietate să fie păstrate. Nu puteţi face lucrări derivative ale acestor informaţii sau să reproduceţi, să distribuiţi sau să afişaţi aceste informaţii sau orice alte porţiuni din ele în afara întreprinderii dumneavoastră, fără acordul explicit al IBM.

Cu excepţia acestei permisiuni explicite, nici o altă permisiune, licenţă sau drepturi nu sunt acordate, fie explicite sau implicite, pentru informaţii sau alte date, software sau alte proprietăţi intelectuale conţinute în acestea.

IBM îşi păstrează dreptul de a retrage permisiunile acordate aici oricând, la discreţia sa, dacă folosirea Publicaţiilor este în detrimentul intereselor sale sau, după cum este determinat de IBM sau dacă instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu aveţi voie să descărcaţi, să exportaţi sau să reexportaţi aceste informaţii decât în deplină conformitate cu toate legile şi reglementările aplicabile, inclusiv toate legile şi reglementările de export ale Statelor Unite. IBM NU ACORDĂ NICI O GARANŢIE PENTRU CONŢINUTUL ACESTOR INFORMAŢII. PUBLICAŢIILE SUNT FURNIZATE ″AŞA CUM SUNT″ ŞI FĂRĂ GARANŢIE DE NICI UN FEL, FIE EXPLICITĂ, FIE IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE SUBÎNŢELESE DE NEÎNCĂLCARE A UNUI DREPT, DE VANDABILITATE SAU DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Prin descărcarea sau tipărirea de informaţii de pe acest sit, v-aţi dat acordul pentru aceşti termeni şi aceste condiţii.

Tipărit în S.U.A.